DE GRUYTER

Yakov Berkovich, Zvonimir Janko

GROUPS OF PRIME POWER ORDER

VOLUME 3

EXPOSITIONS IN MATHEMATICS 56

DE G

De Gruyter Expositions in Mathematics 56

Editors

Victor P. Maslov, Moscow, Russia
Walter D. Neumann, New York, USA
Markus J. Pflaum, Boulder, USA
Dierk Schleicher, Bremen, Germany
Raymond O. Wells, Bremen, Germany

Yakov Berkovich
Zvonimir Janko

Groups of Prime Power Order

Volume 3

De Gruyter

Mathematical Subject Classification 2010: 20-02, 20D15, 20E07.

ISBN 978-3-11-020717-0
e-ISBN 978-3-11-025448-8
ISSN 0938-6572

Library of Congress Cataloging-in-Publication Data

Berkovich, IA. G., 1938−
Groups of prime power order / by Yakov Berkovich, Zvonimir Janko.
p. cm. − (De Gruyter expositions in mathematics ; < >-56)
Description based on v. 3, copyrighted c2011.
Includes bibliographical references and index.
ISBN 978-3-11-020717-0 (v. 3 : alk. paper)
1. Finite groups. 2. Group theory. I. Janko, Zvonimir, 1932− II. Title.
QA177.B469 2011
512'.23−dc22
2011004438

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

© 2011 Walter de Gruyter GmbH & Co. KG, Berlin/New York

Typesetting: Dimler & Albroscheit, Müncheberg
Printing and binding: Hubert & Co. GmbH & Co. KG, Göttingen
∞ Printed on acid-free paper

Printed in Germany

www.degruyter.com

Contents

List of definitions and notations ix

Preface xv

Prerequisites from Volumes 1 and 2 xvii

§93 Nonabelian 2-groups all of whose minimal nonabelian subgroups are metacyclic and have exponent 4 1

§94 Nonabelian 2-groups all of whose minimal nonabelian subgroups are nonmetacyclic and have exponent 4 8

§95 Nonabelian 2-groups of exponent 2^e which have no minimal nonabelian subgroups of exponent 2^e 10

§96 Groups with at most two conjugate classes of nonnormal subgroups . . . 12

§97 p-groups in which some subgroups are generated by elements of order p 24

§98 Nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic to $\mathrm{M}_{2^{n+1}}$, $n \geq 3$ fixed 31

§99 2-groups with sectional rank at most 4 34

§100 2-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian 46

§101 p-groups G with $p > 2$ and $\mathrm{d}(G) = 2$ having exactly one maximal subgroup which is neither abelian nor minimal nonabelian 66

§102 p-groups G with $p > 2$ and $\mathrm{d}(G) > 2$ having exactly one maximal subgroup which is neither abelian nor minimal nonabelian 77

§103 Some results of Jonah and Konvisser 93

§104 Degrees of irreducible characters of p-groups associated with finite algebras 97

§105 On some special p-groups 102

§106 On maximal subgroups of two-generator 2-groups 110

§107 Ranks of maximal subgroups of nonmetacyclic two-generator 2-groups . 113

§108 p-groups with few conjugate classes of minimal nonabelian subgroups . . 120

§109 On p-groups with metacyclic maximal subgroup without cyclic subgroup of index p 122

§110 Equilibrated p-groups 125

§111 Characterization of abelian and minimal nonabelian groups 134

§112 Non-Dedekindian p-groups all of whose nonnormal subgroups have the same order 140

§113 The class of 2-groups in §70 is not bounded 148

§114 Further counting theorems 152

§115 Finite p-groups all of whose maximal subgroups except one are extraspecial 157

§116 Groups covered by few proper subgroups 162

§117 2-groups all of whose nonnormal subgroups are either cyclic or of maximal class 176

§118 Review of characterizations of p-groups with various minimal nonabelian subgroups 179

§119 Review of characterizations of p-groups of maximal class 185

§120 Nonabelian 2-groups such that any two distinct minimal nonabelian subgroups have cyclic intersection 192

§121 p-groups of breadth 2 197

§122 p-groups all of whose subgroups have normalizers of index at most p . . 204

§123 Subgroups of finite groups generated by all elements in two shortest conjugacy classes 237

§124 The number of subgroups of given order in a metacyclic p-group 239

§125 p-groups G containing a maximal subgroup H all of whose subgroups are G-invariant 269

§126 The existence of p-groups $G_1 < G$ such that $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G)$ 272

§127 On 2-groups containing a maximal elementary abelian subgroup of order 4 275

§128 The commutator subgroup of p-groups with the subgroup breadth 1 . . . 277

§129 On two-generator 2-groups with exactly one maximal subgroup which is not two-generator 285

§130 Soft subgroups of p-groups 287

§131 p-groups with a 2-uniserial subgroup of order p 292

§132 On centralizers of elements in p-groups 295

§133 Class and breadth of a p-group 300

§134 On p-groups with maximal elementary abelian subgroup of order p^2 . . . 304

§135 Finite p-groups generated by certain minimal nonabelian subgroups . . . 315

§136 p-groups in which certain proper nonabelian subgroups are two-generator 328

§137 p-groups all of whose proper subgroups have its derived subgroup of order at most p 338

§138 p-groups all of whose nonnormal subgroups have the smallest possible normalizer 343

§139 p-groups with a noncyclic commutator group all of whose proper subgroups have a cyclic commutator group 355

§140 Power automorphisms and the norm of a p-group 363

§141 Nonabelian p-groups having exactly one maximal subgroup with a noncyclic center 368

§142 Nonabelian p-groups all of whose nonabelian maximal subgroups are either metacyclic or minimal nonabelian 370

§143 Alternate proof of the Reinhold Baer theorem on 2-groups with nonabelian norm 373

§144 p-groups with small normal closures of all cyclic subgroups 376

A.27 Wreathed 2-groups 384

A.28 Nilpotent subgroups 393

A.29 Intersections of subgroups 405

A.30 Thompson's lemmas 416

A.31 Nilpotent p'-subgroups of class 2 in $\mathrm{GL}(n, p)$ 428

A.32 On abelian subgroups of given exponent and small index 434

A.33 On Hadamard 2-groups 437

A.34 Isaacs–Passman's theorem on character degrees 440

A.35 Groups of Frattini class 2 446

A.36 Hurwitz' theorem on the composition of quadratic forms 449

A.37 On generalized Dedekindian groups 452

A.38 Some results of Blackburn and Macdonald 457

A.39 Some consequences of Frobenius' normal p-complement theorem 460

A.40 Varia 472

A.41 Nonabelian 2-groups all of whose minimal nonabelian subgroups have cyclic centralizers 514

A.42 On lattice isomorphisms of p-groups of maximal class 516

A.43 Alternate proofs of two classical theorems on solvable groups and some related results 519

A.44 Some of Freiman's results on finite subsets of groups with small doubling 527

Research problems and themes III 536

Author index 630

Subject index 632

List of definitions and notations

Set theory

$|M|$ is the cardinality of a set M (if G is a finite group, then $|G|$ is called its order).

$x \in M$ ($x \notin M$) means that x is (is not) an element of a set M. $N \subseteq M$ ($N \not\subseteq M$) means that N is (is not) a subset of the set M; moreover, if $M \neq N \subseteq M$, we write $N \subset M$.

$\varnothing$ is the empty set.

N is called a nontrivial subset of M if $N \neq \varnothing$ and $N \subset M$. If $N \subset M$, we say that N is a proper subset of M.

$M \cap N$ is the intersection and $M \cup N$ is the union of sets M and N. If M, N are sets, then $N - M = \{x \in N \mid x \notin M\}$ is the difference of N and M.

Number theory and general algebra

p is always a prime number.

π is a set of primes; π' is the set of all primes not contained in π.

m, n, k, r, s are, as a rule, natural numbers.

$\pi(m)$ is the set of prime divisors of m; then m is a π-number if $\pi(m) \subseteq \pi$.

n_p is the p-part of n, n_π is the π-part of n.

GCD(m, n) is the greatest common divisor of m and n.

$m \mid n$ should be read as: m divides n.

GF(p^m) is the finite field containing p^m elements.

F* is the multiplicative group of a field F.

$\mathfrak{L}(G)$ is the lattice of all subgroups of a group G.

If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is the standard prime decomposition of n, then $\lambda(n) = \sum_{i=1}^{k} \alpha_i$.

Groups

We consider only finite groups which are denoted, with a few exceptions, by uppercase Latin letters.

If G is a group, then $\pi(G) = \pi(|G|)$.

G is a p-group if $|G|$ is a power of p; G is a π-group if $\pi(G) \subseteq \pi$.

G is, as a rule, a finite p-group.

$H \leq G$ means that H is a subgroup of G.

$H < G$ means that $H \leq G$ and $H \neq G$ (in that case, H is called a proper subgroup of G). $\{1\}$ denotes the group containing only one element.

H is a nontrivial subgroup of G if $\{1\} < H < G$.

H is a maximal subgroup of G if $H < G$ and it follows from $H \leq M < G$ that $H = M$.

If H is a proper normal subgroup of G, then we write $H \lhd G$. Expressions 'normal subgroup of G' and 'G-invariant subgroup' are synonyms.

A normal subgroup of G is nontrivial provided $G > H > \{1\}$.

H is a minimal normal subgroup of G if (a) H is normal in G; (b) $H > \{1\}$; (c) $N \lhd G$ and $N < H$ implies $N = \{1\}$. Thus the group $\{1\}$ has no minimal normal subgroup.

G is simple if it is a minimal normal subgroup of G (so $|G| > 1$).

H is a maximal normal subgroup of G if $H < G$ and G/H is simple.

The subgroup generated by all minimal normal subgroups of G is called the socle of G and denoted by $\mathrm{Sc}(G)$. We put, by definition, $\mathrm{Sc}(\{1\}) = \{1\}$.

$\mathrm{N}_G(M) = \{x \in G \mid x^{-1}Mx = M\}$ is the normalizer of a subset M in G.

$\mathrm{C}_G(x)$ is the centralizer of an element x in G: $\mathrm{C}_G(x) = \{z \in G \mid zx = xz\}$.

$\mathrm{C}_G(M) = \bigcap_{x \in M} \mathrm{C}_G(x)$ is the centralizer of a subset M in G.

If $A \leq B$ and A, B are normal in G, then $\mathrm{C}_G(B/A) = H$, where $H/A = \mathrm{C}_{G/A}(B/A)$.

$A \operatorname{wr} B$ (or $A \wr B$) is the wreath product of the 'passive' group A and the transitive permutation group B (in what follows we assume that B is regular); B is called the active factor of the wreath product). Then the order of that group is $|A|^{|B|}|B|$.

$\mathrm{Aut}(G)$ is the group of automorphisms of G (the automorphism group of G).

$\mathrm{Inn}(G)$ is the group of all inner automorphisms of G.

$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is the outer automorphism group of G.

$\mathcal{N}(G)$ is the norm of G, the intersection of normalizers of all subgroups of G.

If $a, b \in G$, then $a^b = b^{-1}ab$.

An element $x \in G$ inverts a subgroup $H \leq G$ if $h^x = h^{-1}$ for all $h \in H$.

If $M \subseteq G$, then $\langle M \rangle = \langle x \mid x \in M \rangle$ is the subgroup of G generated by M.

$M^x = x^{-1}Mx = \{y^x \mid y \in M\}$ for $x \in G$ and $M \subseteq G$.

$[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$ is the commutator of elements x, y of G. If $M, N \subseteq G$, then $[M, N] = \langle [x, y] \mid x \in M, y \in N \rangle$ is a subgroup of G.

$o(x)$ is the order of an element x of G.

An element $x \in G$ is a π-element if $\pi(o(x)) \subseteq \pi$.

G is a π-group, if $\pi(G) \subseteq \pi$. Obviously, G is a π-group if and only if all of its elements are π-elements.

G' is the subgroup generated by all commutators $[x, y]$, $x, y \in G$ (i.e., $G' = [G, G]$), $G^{(2)} = [G', G'] = G'' = (G')'$, $G^{(3)} = [G'', G''] = (G'')'$ and so on. G' is called the commutator (or derived) subgroup of G.

$\mathrm{Z}(G) = \bigcap_{x \in G} \mathrm{C}_G(x)$ is the center of G.

$\mathrm{Z}_i(G)$ is the i-th member of the upper central series of G; in particular, $\mathrm{Z}_0(G) = \{1\}$, $\mathrm{Z}_1(G) = \mathrm{Z}(G)$.

$\mathrm{K}_i(G)$ is the i-th member of the lower central series of G; in particular, $\mathrm{K}_2(G) = G'$. We have $\mathrm{K}_i(G) = [G, \ldots, G]$ ($i \geq 1$ times). We set $\mathrm{K}_1(G) = G$.

If G is nonabelian, then $\eta(G)/\mathrm{K}_3(G) = \mathrm{Z}(G/\mathrm{K}_3(G))$.

$\mathcal{M}(G) = \langle x \in G \mid \mathrm{C}_G(x) = \mathrm{C}_G(x^p) \rangle$ is the Mann subgroup of a p-group G.

$\mathrm{Syl}_p(G)$ is the set of p-Sylow subgroups of an arbitrary finite group G.

S_n is the symmetric group of degree n.

A_n is the alternating group of degree n.

Σ_{p^n} is a Sylow p-subgroup of S_{p^n}.

$\mathrm{GL}(n, \mathrm{F})$ is the set of all nonsingular $n \times n$ matrices with entries in a field F, the n-dimensional general linear group over F, $\mathrm{SL}(n, \mathrm{F}) = \{A \in \mathrm{GL}(n, \mathrm{F}) \mid \det(A) = 1 \in \mathrm{F}\}$, the n-dimensional special linear group over F.

If $H \leq G$, then $H_G = \bigcap_{x \in G} x^{-1}Hx$ is the core of the subgroup H in G and H^G, the intersection of all normal subgroups of G containing H, is the normal closure or normal hull of H in G. Obviously, H_G is normal in G.

If G is a p-group, then $p^{\mathrm{b}(x)} = |G : \mathrm{C}_G(x)|$; $\mathrm{b}(x)$ is said to be the breadth of $x \in G$, where G is a p-group; $\mathrm{b}(G) = \max\{\mathrm{b}(x) \mid x \in G\}$ is the breadth of G.

If $H \leq G$ and $|G : \mathrm{N}_G(H)| = p^{\mathrm{sb}(H)}$, then $\mathrm{sb}(H)$ is said to be the subgroup breadth of H. Next, $\mathrm{sb}(G) = \max\{\mathrm{sb}(H) \mid H \leq G\}$.

$\Phi(G)$ is the Frattini subgroup of G (= the intersection of all maximal subgroups of G), $\Phi(\{1\}) = \{1\}$, $p^{\mathrm{d}(G)} = |G : \Phi(G)|$

$\Gamma_i = \{H < G \mid \Phi(G) \leq H, |G : H| = p^i\}, i = 1, \ldots, \mathrm{d}(G)$, where $G > \{1\}$.

If $H < G$, then $\Gamma_1(H)$ is the set of all maximal subgroups of H.

$\exp(G)$ is the exponent of G (the least common multiple of the orders of elements of G). If G is a p-group, then $\exp(G) = \max\{o(x) \mid x \in G\}$.

$\mathrm{k}(G)$ is the number of conjugacy classes of G (= G-classes), the class number of G.

K_x is the G-class containing an element x (sometimes we also write $\mathrm{ccl}_G(x)$).

C_m is the cyclic group of order m.

G^m is the direct product of m copies of a group G.

$A \times B$ is the direct product of groups A and B.

$A * B$ is a central product of groups A and B, i.e., $A * B = AB$ with $[A, B] = \{1\}$.

$\mathrm{E}_{p^m} = \mathrm{C}_p^m$ is the elementary abelian group of order p^m. G is an elementary abelian p-group if and only if it is a p-group $> \{1\}$ and G coincides with its socle. Next, $\{1\}$ is elementary abelian for each prime p.

A group G is said to be homocyclic if it is a direct product of isomorphic cyclic subgroups (obviously, elementary abelian p-groups are homocyclic).

$\mathrm{ES}(m, p)$ is an extraspecial group of order p^{1+2m} (a p-group G is said to be extraspecial if $G' = \Phi(G) = \mathrm{Z}(G)$ is of order p). Note that for each positive integer m, there are exactly two nonisomorphic extraspecial groups of order p^{2m+1}.

$S(p^3)$ is a nonabelian group of order p^3 and exponent $p > 2$.

A special p-group is a nonabelian p-group G such that $G' = \Phi(G) = \mathrm{Z}(G)$ is elementary abelian. Direct products of extraspecial p-groups are special.

D_{2m} is the dihedral group of order $2m$, $m > 2$. Some authors consider E_{2^2} as the dihedral group D_4.

Q_{2^m} is the generalized quaternion group of order $2^m \geq 2^3$.

SD_{2^m} is the semidihedral group of order $2^m \geq 2^4$.

M_{p^m} is a nonabelian p-group containing exactly p cyclic subgroups of index p.

$\mathrm{cl}(G)$ is the nilpotence class of a p-group G.

$\mathrm{dl}(G)$ is the derived length of a p-group G.

$\mathrm{CL}(G)$ is the set of all G-classes.

A p-group of maximal class is a nonabelian group G of order p^m with $\mathrm{cl}(G) = m-1$.

$\Omega_m(G) = \langle x \in G \mid o(x) \leq p^m \rangle$, $\Omega_m^*(G) = \langle x \in G \mid o(x) = p^m \rangle$ and $\mathfrak{V}_m(G) = \langle x^{p^m} \mid x \in G \rangle$.

A p-group G is said to be regular if for any $x, y \in G$ there exists $z \in \langle x, y \rangle'$ such that $(xy)^p = x^p y^p z^p$.

A p-group is absolutely regular if $|G/\mathfrak{V}_1(G)| < p^p$.

A p-group is thin if it is either absolutely regular or of maximal class.

$G = A \cdot B$ is a semidirect product with kernel B and complement A.

A group G is an extension of a normal subgroup N by a group H if $G/N \cong H$. A group G splits over N if $G = H \cdot N$ with $H \leq G$ and $H \cap N = \{1\}$ (in that case, G is a semidirect product of H and N with kernel N).

$H^\# = H - \{e_H\}$, where e_H is the identity element of the group H. If $M \subseteq G$, then $M^\# = M - \{e_G\}$.

An automorphism α of G is regular (= fixed-point-free) if it induces a regular permutation on $G^\#$ (a permutation is said to be regular if it has no fixed points).

An involution is an element of order 2 in a group.

A group G is said to metacyclic if it contains a normal cyclic subgroup C such that G/C is cyclic.

A group G is said to be minimal nonmetacyclic if it is nonmetacyclic but all its proper subgroups are metacyclic.

A subgroup A of a group G is said to be soft if $\mathrm{C}_G(A) = A$ and $|\mathrm{N}_G(A) : A| = p$.

A section of a group G is an epimorphic image of some subgroup of G.

If $\mathrm{F} = \mathrm{GF}(p^n)$, then we may write $\mathrm{GL}(m, p^n), \mathrm{SL}(m, p^n), \ldots$ instead of $\mathrm{GL}(m, \mathrm{F})$, $\mathrm{SL}(m, \mathrm{F}), \ldots$.

$\mathrm{c}_n(G)$ is the number of cyclic subgroups of order p^n in a p-group G.

$\mathrm{s}_n(G)$ is the number of subgroups of order p^n in a p-group G.

$e_n(G)$ is the number of subgroups of order p^n and exponent p in G.

A group G is said to be minimal nonabelian if it is nonabelian but all its proper subgroups are abelian.

$\mathcal{A}_n$-group is a p-group G all of whose subgroups of index p^n are abelian but G contains a nonabelian subgroup of index p^{n-1}. In particular, $\mathcal{A}_1$-group is a minimal nonabelian p-group for some p.

$\alpha_n(G)$ is the number of $\mathcal{A}_n$-subgroups in a p-group G.

$\mathcal{MA}(G)$ is the set of minimal nonabelian subgroups of a p-group G.

$\mathcal{MA}_k(G) = \{H \in \mathcal{MA}(G) \mid \Omega_k(H) = H\}$.

$\mathrm{D}_k(G) = \langle \mathcal{MA}_k(G) \rangle = \langle H \mid H \in \mathcal{MA}_k(G) \rangle$.

$L_n = |\{x \in G \mid x^n = 1\}|$.

Characters and representations

$\mathrm{Irr}(G)$ is the set of all irreducible characters of G over complex numbers.

A character of degree 1 is said to be linear.

$\mathrm{Lin}(G)$ is the set of all linear characters of G (obviously, $\mathrm{Lin}(G) \subseteq \mathrm{Irr}(G)$).

$\mathrm{Irr}_1(G) = \mathrm{Irr}(G) - \mathrm{Lin}(G)$ is the set of all nonlinear irreducible characters of G; $\mathrm{n}(G) = |\mathrm{Irr}_1(G)|$.

$\chi(1)$ is the degree of a character χ of G.

χ_H is the restriction of a character χ of G to $H \leq G$.

χ^G is the character of G induced from the character χ of some subgroup of G.

$\bar{\chi}$ is a character of G defined as follows: $\bar{\chi}(x) = \overline{\chi(x)}$ (here $\bar{w}$ is the complex conjugate of a complex number w).

$\mathrm{Irr}(\chi)$ is the set of irreducible constituents of a character χ of G.

1_G is the principal character of G.

$\mathrm{Irr}^{\#}(G) = \mathrm{Irr}(G) - \{1_G\}$.

If χ is a character of G, then $\ker(\chi) = \{x \in G \mid \chi(x) = \chi(1)\}$ is the kernel of a character χ.

$\mathrm{Z}(\chi) = \{x \in G \mid |\chi(x)| = \chi(1)\}$ is the quasikernel of χ.

If N is normal in G, then $\mathrm{Irr}(G \mid N) = \{\chi \in \mathrm{Irr}(G) \mid N \not\leq \ker(\chi)\}$.

$\langle \chi, \tau \rangle = |G|^{-1} \sum_{x \in G} \chi(x)\tau(x^{-1})$ is the inner product of characters χ and τ of G.

$\mathrm{I}_G(\phi) = \langle x \in G \mid \phi^x = \phi \rangle$ is the inertia subgroup of $\phi \in \mathrm{Irr}(H)$ in G, where $H \lhd G$.

1_G is the principal character of G ($1_G(x) = 1$ for all $x \in G$).

$\mathrm{M}(G)$ is the Schur multiplier of G.

$\mathrm{cd}(G) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$.

$\mathrm{mc}(G) = \mathrm{k}(G)/|G|$ is the measure of commutativity of G.

$\mathrm{T}(G) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)$, $\mathrm{f}(G) = \mathrm{T}(G)/|G|$.

Preface

This is the third volume of the book devoted to elementary parts of p-group theory. Sections 93–95, 98–102, 113, 117, 118, 120–123, 125–133, 137, 139, 140–142, 144 are written by the second author, Sections 107, 138 and Appendix 41 are jointly written by both authors, all other material, apart from Appendices 33 and 44, is written by the first author. All exercises and about all problems are due to the first author. All material of this part is appeared in the book form for the first time.

Some interesting problems of elementary p-group theory are solved in this volume:

(i) classification of p-groups containing exactly one maximal subgroup which is neither abelian nor minimal nonabelian,
(ii) classification of groups all of whose nonnormal subgroups have the same order (independently, this result was obtained by Guido Zappa),
(iii) classification of p-groups all of whose nonnormal subgroups have normalizers of index p,
(iv) computation of the number of subgroups of given order in metacyclic p-groups (for $p > 2$ this was done by Avinoam Mann),
(v) computation of the order of the derived subgroup of a group with subgroup breadth 1,
(vi) classification of p-groups all of whose subgroups have derived subgroups of order $\leq p$ (so-called $\mathcal{A}_2$-groups satisfy this condition),
(vii) classification of p-groups G all of whose maximal abelian subgroups containing a non-G-invariant cyclic subgroup of minimal order, say p^ν, have order $\leq p^{\nu+1}$.

Some results proved in this part have no analogs in existing books devoted to finite p-groups. We list only a few such results:

(a) study the p-groups G all of whose minimal nonabelian subgroups have exponent $< \exp(G)$,
(b) study the groups admitting an irredundant covering by few proper subgroups,
(c) study of some 2-groups with sectional rank 4,
(d) study the p-groups which do not generated by certain minimal nonabelian subgroups,
(e) study the p-groups, $p > 3$, in which certain nonabelian subgroups are generated by two elements,
(f) study the p-groups with nonnormal maximal elementary abelian subgroup of order p^2 (this is a continuation of the paper of Glauberman–Mazza),
(g) classification of p-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian,

(h) classification of p-groups all of whose proper subgroups have derived subgroups of orders $\leq p$,
(i) classification of p-groups all of whose nonnormal cyclic subgroups of minimal possible order have index p is their normalizers,
(j) classification of p-groups G all of whose maximal abelian subgroups containing non-G-invariant cyclic subgroup of minimal order, say p^v, have order $\leq p^{n+1}$,
(k) classification of p-groups all of whose maximal subgroups have cyclic derived subgroups,
(l) characterizations of abelian and minimal nonabelian groups,
(m) describing all possible sets of numbers of generators of maximal subgroups of two-generator 2-groups,
(n) study the equilibrated p-groups,
(o) classification of nonabelian 2-groups in which any two distinct minimal nonabelian subgroups have cyclic intersection,
(p) study the p-groups of breadth 2,
(q) study groups containing a soft subgroup,
(r) proof of the Schenkman theorem on the norm of a finite group and a new proof of Baer's theorem on an arbitrary 2-group with nonabelian norm.

For further information, see the Contents.

Essential part of this volume is devoted to investigation of impact of minimal nonabelian subgroups on the structure of a p-group.

Some appendices are devoted to nilpotent subgroups of nonnilpotent groups.

The section 'Research problems and themes III', written by the first author, contains about 900 research problems and themes some of which are solved by the second author. There are in the text approximately 200 exercises most of which are solved.

Avinoam Mann (Hebrew University of Jerusalem) analyzed the list of problems and made a great number of constructive comments and corrections. He also read a number of sections and made numerous useful remarks. Moshe Roitman (University of Haifa) wrote Appendix 44 and helped with LaTeX. Noboru Ito wrote Appendix 33. We are indebted to these three mathematicians.

We are grateful to the publishing house of Walter de Gruyter and all its workers for supporting and promoting the publication of our book and especially to Simon Albroscheit and Kay Dimler.

Prerequisites from Volumes 1 and 2

In this section we state some results from Volumes 1 and 2 which we use in what follows. If we formulate Lemma 1.4 from Volume 1, then it is named below also as Lemma 1.4.

Lemma INTR. (a) *If $M, N \lhd G$, then the quotient group $G/(M \cap N)$ is isomorphic to a subgroup of $G/M \times G/N$.*

(b) *If Z is a cyclic subgroup of maximal order in an abelian p-group, then Z is a direct factor of G. In particular, an abelian p-group is a direct product of cyclic subgroups.*

(c) (Fitting's lemma) *If M and N are nilpotent normal subgroups of a group G, then* $\mathrm{cl}(MN) \leq \mathrm{cl}(M) + \mathrm{cl}(N)$.

(d) *If G is a p-group, then $G/\Phi(G)$ is elementary abelian of order, say d. Every minimal set of generators of G contains exactly d members.*

(e) *If G is a p-group, then $\Phi(G) = G'\mho_1(G)$.*

Lemma 1.1. *If A is an abelian subgroup of index p in a nonabelian p-group G, then $|G| = p|G'||\mathrm{Z}(G)|$.*

Theorem 1.2. *Suppose that a nonabelian p-group has a cyclic subgroup of index p. Then one of the following holds:*

(a) $G = \langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{-1}\rangle \cong \mathrm{D}_{2^n}$ *is of class $n-1$, all elements of the set $G - \langle a\rangle$ are involutions.*

(b) $G = \langle a, b \mid a^{2^{n-1}} = 1,\ a^{2^{n-2}} = b^2,\ a^b = a^{-1}\rangle \cong \mathrm{Q}_{2^n}$ *is of class $n-1$, all elements of the set $G - \langle a\rangle$ have the same order* 4.

(c) $G = \langle a, b \mid a^{2^{n-1}} = 1,\ a^{2^{n-2}} = b^2,\ a^b = a^{-1}\rangle \cong \mathrm{SD}_{2^n}$ *is of class $n-1$,* $\Gamma_1 = \{D \cong \mathrm{D}_{2^{n-1}},\ Q \cong \mathrm{Q}_{2^{n-1}}, \langle a\rangle \cong \mathrm{C}_{2^{n-1}}\}$, $\Omega_1(G) = D$, $\Omega_2^*(G) = Q$.

(d) $G = \langle a, b \mid a^{p^{n-1}} = b^p = 1,\ a^b = a^{1+p^{n-2}}\rangle \cong \mathrm{M}_{p^n}$ *is of class* 2, *where $n > 3$ if $p = 2$,* $\mathrm{Z}(G) = \langle a^p\rangle$, $\Omega_1(G) = \langle a^{p^{n-2}}, b\rangle \cong \mathrm{E}_{p^2}$.

The groups D_{2^n}, Q_{2^n}, SD_{2^n} are called dihedral, generalized quaternion, semidihedral, respectively.

Proposition 1.3. *If a p-group has only one subgroup of order p, then it is either cyclic or a generalized quaternion group.*

Lemma 1.4. *Let N be a normal subgroup of a p-group G. If N has no G-invariant abelian subgroup of type (p, p), then it is either cyclic or a 2-group of maximal class.*

It follows from Lemma 1.4 that if $\mathrm{Z}_2(G)$ is cyclic, then G is either cyclic or a 2-group of maximal class.

Lemma 1.6 (Taussky). *If a nonabelian 2-group G satisfies $|G : G'| = 4$, then it is a 2-group of maximal class.*

Exercise 1.6(a). The number of abelian maximal subgroups in a nonabelian p-group G is either 0 or 1 or $p + 1$.

Exercise P1. If a nonabelian p-group G has two distinct abelian maximal subgroups, then $|G'| = p$.

Proposition 1.8 (Suzuki). *If a nonabelian p-group G has a self-centralizing abelian subgroup of order p^2, then G is of maximal class. (For the converse assertion, see Theorem 9.6(c).)*

Exercise 1.8(a). If a p-group G is minimal nonabelian, then

$$|G'| = p, \quad \mathrm{d}(G) = 2, \quad |G : \mathrm{Z}(G)| = p^2,$$

and one of the following holds:

(a) $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}} \rangle$ is metacyclic.

(b) $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, [a, b] = c, c^p = 1, [a, c] = [b, c] = 1 \rangle$ is nonmetacyclic. In that case, $\mho_1(G) = \langle a^p \rangle \times \langle b^p \rangle$, $G/\mho_1(G)$ is nonabelian of order p^3 and exponent p unless $p = 2$ (if $p = 2$, then $G/\mho_1(G) \cong \mathrm{E}_4$).

(c) $G \cong \mathrm{Q}_8$.

Next, a group G is nonmetacyclic if and only if G' is a maximal cyclic subgroup of G. The group G is metacyclic if and only if $|\Omega_1(G)| \leq p^2$. No noncentral cyclic subgroup is normal in G.

Theorems 1.10 and 1.17. *Suppose that a p-group G is neither cyclic nor a 2-group of maximal class. Then*

(a) $\mathrm{c}_1(G) \equiv 1 + p \pmod{p^2}$.

(b) *If $k > 1$, then* $\mathrm{c}_k(G) \equiv 0 \pmod{p}$.

Theorem 1.20. *If all subgroups of a nonabelian p-group G are normal, then we have $G = Q \times E$, where $Q \cong \mathrm{Q}_8$ and $\exp(E) \leq 2$.*

Exercise 1.69(a). Let G be a p-group and let $H \neq K$ be two distinct maximal subgroups of G. Then $|G' : H'K'| \leq p$. In particular, if G' is cyclic, there is $A \in \Gamma_1$ such that $|G' : A'| \leq p$.

Lemma 4.2. *Let G be a p-group with $|G'| = p$. Then $G = (A_1 * A_2 * \cdots * A_s)\mathrm{Z}(G)$, the central product, where $A_1, \ldots, A_s$ are minimal nonabelian, so $G/\mathrm{Z}(G)$ is elementary abelian of even rank. In particular, if G/G' is elementary abelian, then we have $|A_1| = \cdots = |A_s| = p^3$, $E = A_1 * \cdots * A_s$ is extraspecial and $G = E\mathrm{Z}(G)$.*

Lemma 4.3. *Let E be a subgroup of a p-group G with $|E'| = p$ and $\mathrm{Z}(E) = \Phi(E)$. If $[G, E] = E'$, then $G = E * \mathrm{C}_G(E)$.*

Theorem 5.2 (Hall's enumeration principle). *Let G be a p-group and $\mathcal{M}$ be a set of proper subgroups of G. Given $H \leq G$, let $\alpha(H)$ be the number of members of the set $\mathcal{M}$ contained in H. Then*

$$\alpha(G) \equiv \sum_{H \in \Gamma_1} \alpha(H) \pmod{p}.$$

Theorems 5.3 and 5.4. *Suppose that a p-group G of order p^m is neither cyclic nor a 2-group of maximal class and $1 \leq n < m$. Then $\mathrm{s}_n(G) \equiv 1 + p \pmod{p^2}$.*

Theorem 5.8. *Let G be a group of order $p^m > p^3$ and exponent p, $2 < n < m$. Let $\mathcal{M}$ denote the set of all 2-generator subgroups of order p^n in G and $\alpha(K)$ the number of elements of the set $\mathcal{M}$ contained in $K \leq G$.*

(a) *If $n = m - 1$, then $\alpha(G) \in \{0, p, p^2\}$.*

(b) *p divides $\alpha(G)$.*

Theorem 7.1. *Let G be a p-group.*

(a) *Regularity is inherited by sections.*

(b) *If $\mathrm{cl}(G) < p$ or $|G| \leq p^p$ or $\exp(G) = p$, then G is regular.*

(c) *If $\mathrm{K}_{p-1}(G)$ is cyclic, then G is regular.*

Theorem 7.2. *Suppose that G is a regular p-group.*

(b) $\exp(\Omega_n(G)) \leq p^n$.

(c) $\mathfrak{V}_n(G) = \{x^{p^n} \mid x \in G\}$.

(d) $|\Omega_n(G)| = |G : \mathfrak{V}_n(G)|$.

Theorem 9.5. *Let G be a group of maximal class and order p^m, $m \leq p+1$. Then $\Phi(G)$ and $G/\mathrm{Z}(G)$ have exponent p. If $m = p + 1$, then G is irregular and $|\mathfrak{V}_1(G)| = p$.*

Theorem 9.6. *Let G be a group of maximal class and order p^m, $p > 2$, $m > p + 1$. Then G is irregular and*

(a) $|G : \mathfrak{V}_1(G)| = p^p$. *In particular,* $\mathfrak{V}_1(G) = \mathrm{K}_p(G)$.

(b) *There is $G_1 \in \Gamma_1$ such that $|G_1 : \mathfrak{V}_1(G_1)| = p^{p-1}$.*

(c) *G has no normal subgroups of order p^p and exponent p (here the condition that $m > p+1$ is essential). Moreover, if $N \lhd G$ and $|G:N| > p$, then N is absolutely regular since $N < G_1$. Next, if $N \lhd G$ of order p^{p-1}, then* $\exp(N) = p$. *In particular, G has no normal cyclic subgroups of order p^2.*

(d) *Let $Z_2 = \mathrm{Z}_2(G)$ be a normal subgroup of order p^2 in G, $G_0 = \mathrm{C}_G(Z_2)$. Then G_0 is regular such that $|\Omega_1(G_0)| = p^{p-1}$.*

(e) *Let $\Gamma_1 = \{M_1 = G_0, M_2, \ldots, M_{p+1}\}$, where G_0 is defined in* (d). *Then the subgroups $M_2, \ldots, M_{p+1}$ are of maximal class (and so irregular; see Theorem 9.5). Thus the subgroups G_1 from* (b) *and G_0 from* (d) *coincide. In what follows we call G_1 the fundamental subgroup of G.*

(f) *In this part, $m \geq 3$ (i.e., we do not assume as in other parts that $m > p+1$). The group G has an element a such that $|\mathrm{C}_G(a)| = p^2$, i.e., $\mathrm{C}_G(a) = \langle a, \mathrm{K}_{m-1}(G)\rangle$.*

Theorem 9.7. *A nonabelian p-group G is of maximal class if and only if $G/\mathrm{K}_{p+1}(G)$ is of maximal class.*

Theorem 9.8. (a) *Absolutely regular p-groups G (i.e., G with $|G/\mathfrak{V}_1(G)| < p^p$) are regular.*

(b) *If a p-group G is such that $|G'/\mathfrak{V}_1(G')| < p^{p-1}$, then G is regular.*

(c) *Any irregular p-group G has a characteristic subgroup R of order $\geq p^{p-1}$ and exponent p such that $R \leq G'$.*

Theorem 9.11. *A p-group G, $p > 2$, is metacyclic if and only if $|G/\mathfrak{V}_1(G)| \leq p^2$.*

Exercise 9.13. Let G be a p-group of maximal class, $p > 2$, and $H < G$. Then $\mathrm{d}(H) \leq p$. If $\mathrm{d}(H) = p$, then $G \cong \Sigma_{p^2} \in \mathrm{Syl}_p(\mathrm{S}_{p^2})$. In particular (Blackburn), if G is a p-group of maximal class, $p > 2$, $N \lhd G$ and $G/N \cong \Sigma_{p^2}$, then $N = \{1\}$.

Theorem 10.1. *Let $p^n > 2$ and let $A < G$ be abelian of exponent p^n. Then the number of abelian subgroups $B \leq G$ of order $p|A|$ that contain A is congruent to* 1 *modulo p.*

Corollary 10.2. *Let N be a normal subgroup of a p-group G and let $A < N$ be a maximal G-invariant abelian subgroup of exponent $\leq p^n$, where $p^n > 2$. Then we have $\Omega_n(\mathrm{C}_N(A)) = A$.*

Theorems 10.4 and 10.5. *Suppose that G is a p-group, $p > 2$. Let $\epsilon_n(G)$ be the number of elementary abelian subgroups of order p^n in G. If $k \in \{3, 4\}$ and $\epsilon_k(G) > 0$, then we have $\epsilon_k(G) \equiv 1 \pmod{p}$.*

Exercise P2. Let G and k be such as in the previous theorem.

(a) If $\mathrm{Z}_k(G)$ has no G-invariant elementary abelian subgroup of order p^k, then we have $\epsilon_k(G) = 0$.

(b) If a G-invariant subgroup N of G has no G-invariant elementary abelian subgroup of order p^k, then $\epsilon_k(N) = 0$.

Lemma 10.8. *Suppose that G is a minimal nonnilpotent group. Then $G = PQ$, where $P \in \mathrm{Syl}_p(G)$, $Q = G' \in \mathrm{Syl}_q(G)$ and*

(a) *P is cyclic, $|P : (P \cap \mathrm{Z}(G)| = p$.*

(b) *Q is either elementary abelian or special, $|Q/\Phi(Q)| = q^b$, where b is the order of q modulo p.*

(c) *If Q is special, then b is even and $\Phi(Q) = \mathrm{Z}(Q) \leq \mathrm{Z}(G)$, $|\Phi(Q)| \leq p^{b/2}$.*

Theorem (Frobenius' normal p-complement theorem). *If a group G has no p-closed minimal nonnilpotent subgroup of order divisible by p, then G has a normal p-complement ($= p$-nilpotent).*

Theorem (Burnside's normal p-complement theorem). *If a Sylow p-subgroup of a group G is contained in the center of its normalizer, then G is p-nilpotent.*

Proposition 10.17. *If $B \leq G$ is a nonabelian subgroup of order p^3 in a p-group G and $C_G(B) < B$, then G is of maximal class.*

Remark 10.5. Let $H < G$ and assume that $\mathrm{N}_G(H)$ is of maximal class. Then G is also of maximal class.

Proposition 10.19. *Suppose that H is a nonabelian subgroup of order p^3 in a metacyclic p-group G. If $p > 2$, then $G = H$. If $p = 2$, then G is of maximal class.*

Proposition 10.28. *A nonabelian p-group G is generated by minimal nonabelian subgroups. In particular, if, in addition, G is not minimal nonabelian, it contains two nonconjugate minimal nonabelian subgroups.*

Theorem 10.33. *If all minimal nonabelian subgroups of a nonabelian 2-group G are generated by involutions, then $G = \langle x \rangle \cdot A$, where $A \in \Gamma_1$ is abelian and all elements in $G - A$ are involutions (such G is said to be* generalized dihedral*).*

Theorem 12.1. (a) *If a p-group G has no normal subgroup of order p^p and exponent p, then G is either absolutely regular or irregular of maximal class.*

(b) *If an irregular p-group G has an absolutely regular maximal subgroup H, then it is either of maximal class or $G = H\Omega_1(G)$, where $\Omega_1(G)$ is of order p^p (and, of course, of exponent p).*

Exercise P3. If $\Omega_p(G)$ has no G-invariant subgroup of order p^p and exponent p, then G is either absolutely regular or of maximal class.

Theorem 12.12. *Let a group G of order p^m be neither absolutely regular nor of maximal class and suppose that $H \in \Gamma_1$ is of maximal class. Then*

(a) $\mathrm{d}(G) = 3$.

(b) *Set $\nu = m - 2$ if $m \leq p + 1$ and $\nu = p$ if $m > p + 1$. Then $G/\mathrm{K}_\nu(G)$ is of order $p^{\nu+1}$ and, if $m > 4$, it is of exponent p.*

(c) *Exactly p^2 maximal subgroups of G are of maximal class. If, in addition, $p > 2$ and $m > 4$, then the remaining $p + 1$ maximal subgroups of G have no two generators and their intersection $\eta(G)$ has index p^2 in G.*

Theorem 13.2. *Suppose that a p-group G is neither absolutely regular nor of maximal class. Then*

(a) $\mathrm{c}_1(G) \equiv 1 + p + \cdots + p^{p-1} \pmod{p^p}$.

(b) *If $k > 1$, then $\mathrm{c}_k(G) \equiv 0 \pmod{p^{p-1}}$.*

Corollary 13.3. *Suppose that an irregular p-group G is neither absolutely regular nor of maximal class and $k < p$. Then it has a normal subgroup M of order p^k and exponent p, and the number of subgroups in G of order p^{k+1} and exponent p containing M is $\equiv 1 \pmod{p}$.*

Theorem 13.5. *If a p-group G is neither absolutely regular nor of maximal class, then $e_p(G) \equiv 1 \pmod{p}$ (here $e_n(G)$ is the number of subgroups of order p^n and exponent p in G).*

Exercise P4. Let N be a normal subgroup of a p-group G. If N has no G-invariant subgroup of order p^p and exponent p, then it is either absolutely regular or of maximal class.

Theorem 13.6. *Let a group G of order p^m be neither absolutely regular nor of maximal class, let n be a natural number with $m > n \geq p+1$. Denote by $\alpha(G)$ the number of subgroups of maximal class and order p^n in G. Then p^2 divides $\alpha(G)$.*

Theorem 13.7. *Let $p > 2$ and suppose that a p-group has no normal elementary abelian subgroup of order p^3. Then one of the following holds:*

(a) *G is metacyclic.*

(b) *G is a 3-group of maximal class not isomorphic to a Sylow 3-subgroup of the symmetric group of degree 9.*

(c) *$G = \Omega_1(G)C$, where $|\Omega_1(G)| = p^3$ and C is cyclic.*

Exercise P5. Let G be a p-group, $p > 2$, and suppose that $\Omega_1(G)$ has no G-invariant elementary abelian subgroup of order p^3. Then G is one of the groups from Theorem 13.7.

Exercise 13.10(a). Let $H < G$, where G is a p-group. If every subgroup of G of order $p|H|$ containing H is of maximal class, then G is also of maximal class.

Proposition 13.18. *Let G be a p-group, and let $M < G$ be of maximal class.*

(a) *Set $D = \Phi(M)$, $N = \mathrm{N}_G(M)$ and $C = \mathrm{C}_N(M/D)$. Let t be the number of subgroups $K \leq G$ of maximal class such that $M < K$ and $|K : M| = p$. Then $t = \mathrm{c}_1(N/M) - \mathrm{c}_1(C/M)$. If G is not of maximal class, then $t \equiv 0 \pmod{p}$.*

(b) *Suppose, in addition, that M is irregular and G is not of maximal class and a positive integer k is fixed. Then the number t of the subgroups $L < G$ of maximal class and order $p^k|M|$ such that $M < L$ is a multiple of p.*

Theorem 36.1. *Let G be a nonabelian p-group and $R < G'$ be a G-invariant subgroup of index p. Then G is metacyclic if and only if G/R is metacyclic.*

Corollary 36.6 (Blackburn). *Suppose that a nonabelian p-group G and all its maximal subgroups are two-generator. Then G is either metacyclic or $p > 2$ and $\mathrm{K}_3(G) = \mho_1(G)$ has index p^3 in G (in the last case, $|G : G'| = p^2$).*

Theorem 36.16. *Suppose that a p-group G is such that $G/\mho^2(G)$ is of maximal class. Then G is also of maximal class.*

Exercise P6. If a p-group G is such that $G/\mho_2(G)$ is of maximal class, then G is also of maximal class.

Lemma 42.1. *Let G be a group of order p^m satisfying $|\Omega_2(G)| \le p^{p+1} < |G|$. Then one of the following holds:*

(a) *G is an L_p-group.*

(b) *G is absolutely regular.*

(c) *$p = 2$, G is metacyclic and*

$$G = \langle a, b \mid a^{2^{m-2}} = b^8 = 1,\ a^b = a^{-1},\ a^{2^{m-3}} = b^4,\ m > 4\rangle.$$

Here $\mathrm{Z}(G) = \langle b^2\rangle$, $G' = \langle a^2\rangle$ and G/G' is abelian of type $(4, 2)$, $\Phi(G) = \langle a^2, b^2\rangle$, $\Omega_2(G) = \langle a^{2^{m-4}}, b^4\rangle$.

Corollary 44.6. *A p-group is metacyclic if and only if one of the following quotient groups is metacyclic:*

$$G/\Phi(G'), \quad G/\mathrm{K}_3(G), \quad G/\mho_1(G'), \quad \text{and, if } p > 2, \text{ then } G/\mho_1(G).$$

Corollary 44.9. *If $G/\mho_2(G)$ is a metacyclic 2-group, then G is also metacyclic.*

Theorem 44.12. *Suppose that N is a two-generator normal subgroup of a p-group G. If $N \le \Phi(G)$, then N is metacyclic.*

Theorem 50.1. *Let G be a 2-group which has no normal elementary abelian subgroup of order 8. Then G has a normal metacyclic subgroup N such that G/N is isomorphic to a subgroup of D_8.*

Lemma 57.1. *Let G be a nonabelian p-group and let A be a maximal abelian normal subgroup of G. Then for any $x \in G-A$, there is a $a \in A$ such that $[a, x] \ne 1$, $[a, x]^p = 1$, and $[a, x, x] = 1$ which implies that $\langle a, x\rangle$ is minimal nonabelian. Therefore G is generated by its minimal nonabelian subgroups.*

In particular, if all minimal nonabelian subgroups of a nonabelian p-group G, $p > 2$, have exponent p, then $\mathrm{H}_p(G)$ is abelian. (For a stronger result, see Mann's commentary to Problem 115.)

Lemma 57.2. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are of exponent 4 and let A be a maximal normal abelian subgroup of G. Then all elements in $G-A$ are of order ≤ 4 and so either $\exp(A)=2$ or $\exp(A)=\exp(G)$. If $x \in G-A$ with $x^2 \in A$, then x inverts each element in $\mho_1(A)$ and in $A/\Omega_1(A)$. If $\exp(G)>4$, then either G/A is cyclic of order ≤ 4 or $G/A \cong Q_8$.*

Lemma 65.2(a). *If G is a nonabelian two-generator p-group and $G' \leq \Omega_1(Z(G))$, then G is minimal nonabelian.*

Theorems 66.1 and 69.1. *If G is a minimal nonmetacyclic p-group, then one of the following holds:*

(a) *G is of order p^3 and exponent p.*

(b) *G is a 3-group of maximal class and order 3^4.*

(c) *$G \cong D_8 * C_4 = Q_8 * C_4$ is of order 16.*

(d) *$G = Q_8 \times C_2$.*

(e) *G is special of order 2^5 with $|Z(G)|=4$, exactly one maximal subgroup of G is abelian.*

It follows from the previous theorem that a p-group G is metacyclic in any of the following cases: (i) every subgroup of G of exponent $\leq p^2$ is metacyclic (in particular, if $\Omega_2(G)$ is metacyclic), (ii) every three-generator subgroup of G is metacyclic.

Exercise P7. A p-group is metacyclic if one of the following holds:

(a) $\Omega_2(G)$ is metacyclic.

(b) $G/\mho_2(G)$ is metacyclic.

(c) $G/K_3(G)\Phi(G')$ is metacyclic.

Exercise P8. If a 2-group G and all its maximal subgroups are two-generator, then G is metacyclic.

Propositions 71.3–71.5. *If a two-generator p-group is a nonmetacyclic $\mathcal{A}_2$-group, then $p>2$.*

Theorems 82.1–82.3. *Let G be a 2-group with exactly three involutions and assume that $Z(G)$ is noncyclic. Then G has a normal metacyclic subgroup M such that G/M is elementary abelian of order at most 4.*

Theorem 90.1. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to D_8 or Q_8. Then G is one of the following groups:*

(a) *G is generalized dihedral (i.e., $|G : H_2(G)| = 2$).*

(b) *$G = HZ(G)$, where H is of maximal class and $\mho_1(Z(G)) \leq Z(H)$.*

(c) *$G = HZ(G)$, where H is extraspecial and $\mho_1(Z(G)) \leq Z(H)$.*

Corollary 90.2. *Let G be a nonabelian 2-group in which any two noncommuting elements generate a subgroup of maximal class. Then G is one of the groups* (a), (b) *or* (c) *from Theorem 90.1. Conversely, each group in* (a), (b) *or* (c) *of Theorem 90.1 satisfies the assumption of our corollary.*

Exercise P9. Let $H = \langle a, b\rangle$ be a two-generator p-group with H' of order p. Then $\Phi(H) = \langle a^p, b^p, [a, b]\rangle$ and H is minimal nonabelian.

Exercise P10. Let G be a p-group with $|G'| = p$. If H is a minimal nonabelian subgroup of G, then $G = H\mathrm{C}_G(H)$.

Exercise P11. All $p^2 + p + 1$ subgroups of order p^2 in an elementary abelian group $E = \langle a, b, c\rangle$ of order p^3 are: $\langle a, b\rangle$, $\langle a, b^i c\rangle$ ($p + 1$ subgroups containing $\langle a\rangle$) and $\langle a^j b, a^k c\rangle$ (p^2 subgroups not containing $\langle a\rangle$), where i, j, k are any integers modulo p.

Corollary 92.7. *Let G be a non-Dedekindian p-group and let $R(G)$ be the intersection of all nonnormal subgroups. If $R(G) > \{1\}$, then $p = 2$, $|R(G)| = 2$ and G is one of the following groups:*

(a) $G \cong \mathrm{Q}_8 \times \mathrm{C}_4 \times \mathrm{E}_{2^s}$, $s \geq 0$.

(b) $G \cong \mathrm{Q}_8 \times \mathrm{Q}_8 \times \mathrm{E}_{2^s}$, $s \geq 0$.

(c) *G has an abelian maximal subgroup A of exponent > 2 and an element $x \in G - A$ of order 4 which inverts each element in A.*

§93

Nonabelian 2-groups all of whose minimal nonabelian subgroups are metacyclic and have exponent 4

We shall determine the structure of nonabelian 2-groups all of whose minimal nonabelian subgroups are metacyclic and have exponent 4, i.e., they are isomorphic to D_8, Q_8 or $H_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1}\rangle$. In Theorem 90.1 we have determined the nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic to D_8 or Q_8. The nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic to Q_8 or H_2 are identified in Theorem 92.6. Here we determine the title 2-groups G which possess as subgroups both D_8 and H_2 (and possibly Q_8). It turns out, as a surprise, that such 2-groups G must be of exponent > 4. More precisely, we prove the following result.

Theorem 93.1. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are metacyclic and have exponent 4 and assume that D_8 and $H_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1}\rangle$ (and possibly Q_8) actually appear as subgroups of G. Then G has a unique abelian maximal subgroup A of exponent > 4 and an involution $t \in G - A$ such that t inverts each element in $A/\Omega_1(A)$ and in $\Omega_2(A)$ and there is an element $a \in A$ of order > 4 such that $a^t = a^{-1}\zeta$ with $1 \neq \zeta \in \Omega_1(A)$, where in case that $\mathfrak{V}_1(A)$ is cyclic we have $\zeta \notin \mathfrak{V}_1(A)$.*

Conversely, all these 2-groups satisfy the assumptions of the theorem.

Proof. Let G be a 2-group satisfying the assumptions of Theorem 93.1 and suppose that A is a maximal normal abelian subgroup of G. We shall freely use Lemmas 57.1, 57.2 and 65.2(a). It follows that all elements in $G - A$ are of order ≤ 4.

(i) We show that G/A is elementary abelian.

Suppose that this is false. Then there is an element v of order 4 in $G - A$ such that $v^2 = t \notin A$. Set $T = A\langle v\rangle$, $A_0 = C_A(v)$ and $T_0 = A_0 \times \langle v\rangle$ so that $A \neq A_0$ and $T \neq T_0$. Let $T_1 \leq T$ be such that $T_1 > T_0$ and $|T_1 : T_0| = 2$. Set $A_1 = T_1 \cap A$ so that $|A_1 : A_0| = 2$. Note that $T_1' \leq A \cap T_0 = A_0 \leq Z(T_1)$ and so $\mathrm{cl}(T_1) = 2$. Let a be any element in $A_1 - A_0$ so that $a^2 \in A_0$. We get $1 \neq [a, v] \in A_0$ and $[a, v]^2 = [a^2, v] = 1$ and so $[a, v]$ is an involution in $Z(T_1)$. This implies that $\langle a, v\rangle' = \langle [a, v]\rangle$ and so $\langle a, v\rangle$ is minimal nonabelian. Set $\langle a, v\rangle \cap A = A^* \geq \langle a\rangle$ so that $\langle a, v\rangle = A^*\langle v\rangle$ satisfying $A^* \cap \langle v\rangle = \{1\}$. If $|A^*| = 2$, then $\langle a, v\rangle = A^* \times \langle v\rangle$ is abelian, a contradiction.

Hence $|A^*| = 4$ so that $\langle a, v\rangle \cong \mathrm{H}_2$ and $A^* = \langle a\rangle \cong \mathrm{C}_4$ with $a^v = a^{-1}$. We have proved that all elements in $A_1 - A_0$ are of order 4 and they are inverted by v. Since $\langle A_1 - A_0\rangle = A_1$, v inverts A_1 so that $A_0 = \mathrm{C}_A(v)$ is elementary abelian and $t = v^2$ centralizes A_1.

Set $A_2 = \mathrm{C}_A(t)$ so that $A_2 \geq A_1$, $A_2 \neq A$ and A_2 is $\langle v\rangle$-invariant which gives that $T_2 = A_2\langle v\rangle$ is a subgroup of T, $T_2 \neq T$ and $T_2 \cap A = A_2$. Let T_3 be a subgroup of T such that $T_3 > T_2$ and $|T_3 : T_2| = 2$ and set $A_3 = T_3 \cap A$ so that $|A_3 : A_2| = 2$. Let b be any element in $A_3 - A_2$ so that $b^2 \in A_2 = \mathrm{C}_A(t)$. It follows that

$$1 \neq [b, t] \in A \cap T_2 = A_2 \quad \text{and} \quad 1 = [b^2, t] = [b, t]^b[b, t] = [b, t]^2$$

so that $\langle b, t\rangle$ is minimal nonabelian with a noncentral involution t which yields that $\langle b, t\rangle \cong \mathrm{D}_8$ and $o(b) \leq 4$. All elements in the set $A_3 - A_2$ are of order ≤ 4 so that $A_3 = \langle A_3 - A_2\rangle$ is of exponent 4. If $o(b) = 2$, then $o(ba) = 4$, where $a \in A_1 - A_0$ and $o(a) = 4$. In any case, there is an element $w \in A_3 - A_2$ of order 4 which together with $\langle w, t\rangle \cong \mathrm{D}_8$ gives $w^t = w^{-1}$.

Suppose that there is an involution u in $A_2 - A_1$. Then $1 \neq [u, v] \in A$ and we get

$$1 = [u^2, v] = [u, v]^u[u, v] = [u, v]^2 \quad \text{and} \quad 1 = [u, v^2] = [u, v][u, v]^v$$

so that $[u, v]$ is a central involution in $\langle u, v\rangle$. Hence $\langle u, v\rangle$ is minimal nonabelian with a noncentral involution u which gives $\langle u, v\rangle \cong \mathrm{D}_8$. But then $v^u = v^{-1}$ and so $[u, v] \notin A$, a contradiction. We have proved that all element in $A_2 - A_0$ are of order 4. In particular, $w^2 \in A_0 = \mathrm{C}_A(v)$. We compute

$$1 = [w^2, v] = [w, v]^w[w, v] = [w, v]^2$$

and so $[w, v] \in T_2 \cap A = A_2$ is an involution in A_2 and therefore $[w, v] \in A_0 = \mathrm{C}_A(v)$. It follows that $[w, v] \in \mathrm{Z}(\langle w, v\rangle)$ and thus $\langle w, v\rangle$ is minimal nonabelian satisfying $\langle w, v\rangle \cap A \geq \langle w\rangle \cong \mathrm{C}_4$ so that $\langle w, v\rangle \cong \mathrm{H}_2$ and $\langle w, v\rangle \cap A = \langle w\rangle$ which implies $w^v = w^{-1}$. But then $w^t = w^{v^2} = w$, which contradicts a result from the previous paragraph.

(ii) We prove that $\exp(G) > 4$.

Suppose that this is false. In what follows we assume that $\exp(G) = 4$. In that case, $G' \leq \mho_1(G) \leq \Omega_1(A)$ and so $\mho_1(G)$ is elementary abelian. Since H_2 is a subgroup of G, we have $|\mho_1(G)| \geq 4$.

(ii1) If $a \in A$ and $x \in G$ with $[a, x] \neq 1$, then $\langle a, x\rangle$ is minimal nonabelian. In that case, $\langle a, x\rangle \cong \mathrm{D}_8$ if and only if a or x (or both) is an involution.

Indeed, $1 = [a, x^2] = [a, x][a, x]^x$ and so $[a, x] \in \Omega_1(A)$ is an involution which commutes with a and x. Hence $\langle a, x\rangle' = \langle [a, x]\rangle$ and so, by Lemma 65.2(a), $\langle a, x\rangle$ is minimal nonabelian.

(ii2) We have $\mho_1(A) \neq \{1\}$ and $\mho_1(A) \leq \mathrm{Z}(G)$.

Assume that A is elementary abelian. Let

$$H = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1},\ a^2 = z,\ b^2 = u\rangle$$

be a subgroup of G so that $H \cap A = \langle u, z\rangle \cong \mathrm{E}_4$. Let t be an involution in the set

$A - (\mathrm{C}_A(a) \cup \mathrm{C}_A(b))$. By (ii1), we have $\langle t, a\rangle \cong \langle t, b\rangle \cong \mathrm{D}_8$ and so $a^t = a^{-1} = az$ and $b^t = b^{-1} = bu$. We get $(ab)^t = (ab)zu$ and so $[t, ab] \neq 1$. Again by (ii1), we obtain $\langle t, ab\rangle \cong \mathrm{D}_8$ and so $(ab)^t = (ab)^{-1} = (ab)(ab)^2 = (ab)u$, a contradiction. We have proved that $\mho_1(A) \neq \{1\}$. Let $a \in A$ and assume that $a^2 \notin \mathrm{Z}(G)$. Then there is $g \in G$ such that $[a^2, g] \neq 1$. But then $[a, g] \neq 1$ and so (ii1) implies that $\langle a, g\rangle$ is minimal nonabelian. In that case, $a^2 \in \Phi(\langle a, g\rangle) = \mathrm{Z}(\langle a, g\rangle)$ and so $[a^2, g] = 1$, a contradiction. We have proved that $\mho_1(A) \leq \mathrm{Z}(G)$.

(ii3) We have $\mho_1(G) \leq \mathrm{Z}(G)$ which implies that each maximal abelian subgroup of G is also normal in G. Whenever $x, y \in G$ with $[x, y] \neq 1$, then $\langle x, y\rangle$ is minimal nonabelian.

Suppose that this is false. Then there is an element $v \in G - A$ such that $v^2 \notin \mathrm{Z}(G)$ and $v^2 \in \Omega_1(A)$. In that case, there is $w \in G - (A\langle v\rangle)$ such that $[w, v^2] \neq 1$. By (ii1), $\langle w, v^2\rangle \cong \mathrm{D}_8$ and so (replacing w with wv^2 if necessary), we see that there is an involution $t \in G - (A\langle v\rangle$ such that $\langle t, v^2\rangle \cong \mathrm{D}_8$. We study the two-generator subgroup $H = \langle t, v\rangle$ and set $A_0 = H \cap A$. Since $H/A_0 \cong \mathrm{E}_4$, we have $\Phi(H) = A_0$ and A_0 is elementary abelian. Hence $[t, v]$ is an involution in A_0 and $1 = [t^2, v] = [t, v]^t[t, v]$ shows that t commutes with $[t, v]$. If $[t, v]$ also commutes with v or tv, then we get $[t, v] \in \mathrm{Z}(H)$, $\langle t, v\rangle' = \langle [t, v]\rangle$ and so $\langle t, v\rangle$ is minimal nonabelian. But in that case, we conclude $v^2 \in \Phi(H) = \mathrm{Z}(H)$ and $[t, v^2] = 1$, a contradiction. We have proved that $\mathrm{C}_H(A_0) = A_0$ and so A_0 (being elementary abelian) is a maximal normal abelian subgroup of H.

We have already seen that $\mathrm{D}_8 \cong \langle t, v^2\rangle$ is a subgroup of H. Suppose that H_2 is not a subgroup of H. In that case, we are in a position to use Theorem 90.1. If H is quasidihedral, then $\langle v\rangle$ is normal in H in which case $v^2 \in \mathrm{Z}(H)$, a contradiction. It follows that $H = H_0\mathrm{Z}(H)$, where H_0 is extraspecial and $\mho_1(\mathrm{Z}(H)) \leq \mathrm{Z}(H_0)$. But in the last case, $A_0 = \mho_1(H) \leq \mathrm{Z}(H)$, a contradiction. We have shown that H has both D_8 and H_2 as subgroups. By (ii2) applied to H and A_0, we get $\mho_1(A_0) \neq \{1\}$, contrary to the fact that A_0 is elementary abelian.

We have proved that $\mho_1(G) \leq \mathrm{Z}(G)$ and so G is of class 2 which implies that each maximal abelian subgroup of G is also normal in G. Let $x, y \in G$ with $[x, y] \neq 1$. Then $[x, y] \in \mho_1(G) \leq \mathrm{Z}(G)$ and $\mho_1(G) \leq \Omega_1(A)$ so that $\langle x, y\rangle' = \langle [x, y]\rangle$ is of order 2 and so $\langle x, y\rangle$ is minimal nonabelian.

(ii4) $\mathrm{D}_8 \times \mathrm{C}_4$ is not a subgroup of G.

Indeed, assume that $\langle a, t \mid a^4 = t^2 = 1, a^t = a^{-1}\rangle \times \langle b\rangle$, where $\langle b\rangle \cong \mathrm{C}_4$, is a subgroup of G. Then $[t, ab] = [t, a] \neq 1$ and (ii3) implies $\langle t, ab\rangle \cong \mathrm{D}_8$. It follows $(ab)^t = (ab)^{-1} = a^{-1}b^{-1}$ and $(ab)^t = a^tb^t = a^{-1}b$, a contradiction.

(ii5) Each maximal abelian subgroup A is of type $(4, 2, \ldots, 2)$. In particular, $\mathrm{C}_4 \times \mathrm{C}_4$ is not a subgroup of G.

By (ii2) and (ii3), A is not elementary abelian, A is normal in G, and assume that A has a subgroup $\langle a\rangle \times \langle b\rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$. Since D_8 is a subgroup of G, there is an involution $t \in G - A$. By (ii1) and (ii4), t either centralizes $\langle a, b\rangle$ or t inverts each element of $\langle a, b\rangle$. Suppose that t centralizes $\langle a, b\rangle$ and let x be any element of order 4

in A. By (ii1), t normalizes $\langle x\rangle$ (since $[t,x]\neq 1$ implies that $\langle t,x\rangle\cong \mathrm{D}_8$) and again by (ii4), t centralizes x. But elements of order 4 in A generate A and so t centralizes A, a contradiction. Hence t inverts $\langle a,b\rangle$ and by (ii4), t inverts each element of order 4 in A. It follows that t inverts A. This implies that each minimal nonabelian subgroup of $A\langle t\rangle$ is isomorphic to D_8 and so $A\langle t\rangle\neq G$ and there are no involutions in $G-(A\langle t\rangle)$. We have $G=(A\langle t\rangle)S$ with $(A\langle t\rangle)\cap S=A$, where $S\neq A$ and all elements in $S-A$ are of order 4. Let $v\in S-A$. If $[v,t]\neq 1$, then (ii3) implies that $\langle v,t\rangle\cong \mathrm{D}_8$. But then $vt\in G-(A\langle t\rangle)$ and vt is an involution, a contradiction. It follows that t commutes with each element in $S-A$ and so $[S,t]=1$ and t centralizes A, a contradiction. We have proved that any maximal abelian subgroup A of G is of type $(4,2,\ldots,2)$.

(ii6) If $v\in G-A$ is such that $v^2\notin \mathfrak{V}_1(A)$, then v centralizes $\Omega_1(A)$.

Suppose that a is an element of order 4 in A so that (by (ii5)) $A=\langle a\rangle\Omega_1(A)$ with $\langle a\rangle\cap\Omega_1(A)=\langle a^2\rangle=\mathfrak{V}_1(A)$. Further, suppose that there exists $t\in\Omega_1(A)$ such that $[v,t]\neq 1$. Then $\langle v,t\rangle\cong \mathrm{D}_8$ and so $v^t=v^{-1}$ and $t'=vt$ is an involution in Av. By (ii5), we get $[a,v]\neq 1$ and so $\langle a,v\rangle\cong \mathrm{H}_2$. We have $[av,t]=[v,t]=v^2\neq 1$ and so $\langle av,t\rangle\cong \mathrm{D}_8$ which gives

$$v^2=[av,t]=(av)^2=a^2v^2[v,a],\quad [v,a]=a^2,\quad a^v=a^{-1}$$

and $(av)^2=v^2$. We compute

$$(av)^{t'}=(av)^{vt}=(a^{-1}v)^t=a^{-1}v^{-1}=(av)a^2v^2\neq av$$

since $a^2\neq v^2$ and so $\langle av,t'\rangle\cong \mathrm{D}_8$ which implies

$$(av)^{t'}=(av)^{-1}=(av)(av)^2=(av)v^2,$$

a contradiction with the above.

(ii7) If t is any involution in $G-A$, then t does not centralize $\Omega_1(A)$.

Suppose that t centralizes $\Omega_1(A)$ so that $\mathrm{C}_A(t)=\Omega_1(A)$. In that case, t inverts each element in A. If v is an element of order 4 in A, then $A=\langle v\rangle\Omega_1(A)$ with

$$\langle v\rangle\cap\Omega_1(A)=\langle v^2\rangle=\mathfrak{V}_1(A)\quad\text{and}\quad v^t=v^{-1}.$$

Since $|\mathfrak{V}_1(G)|\geq 4$, there is an element $g\in G-(A\langle t\rangle)$ such that $g^2\neq v^2$. By (ii6), g centralizes $\Omega_1(A)$ and so $[g,v]\neq 1$ which implies that $\langle g,v\rangle\cong \mathrm{H}_2$. If $v^g=v^{-1}$, then $v^{gt}=(v^{-1})^t=v$ and gt centralizes A, a contradiction. It follows that $v^g=vg^2$ and so

$$v^{gt}=(vg^2)^t=v^{-1}g^2=v(v^2g^2).$$

If $[g,t]\neq 1$, then we get $\langle g,t\rangle\cong \mathrm{D}_8$, gt is an involution which does not normalize $\langle v\rangle$, a contradiction. Hence $[g,t]=1$, $o(gt)=4$, $(gt)^2=g^2$ and so $\langle v,gt\rangle\cong \mathrm{H}_2$ with $\langle v,gt\rangle'=\langle v^2g^2\rangle$ which implies that v^2g^2 is a square in $\langle v,gt\rangle$. This is a contradiction since g^2 and v^2 are the only involutions in $\langle v,gt\rangle$ which are squares in $\langle v,gt\rangle$.

(ii8) We consider a final configuration which will produce a contradiction.

Let $H = \langle g, v \mid g^4 = v^4 = 1,\ v^g = v^{-1}\rangle$ be a subgroup of G. Let A be a maximal abelian subgroup of G containing $\langle v, g^2\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$. Since g centralizes $\Omega_1(A)$ (by (ii6)), g inverts on A, all elements in Ag are of order 4, and $A\langle g\rangle \cong \mathrm{H}_2 \times \mathrm{E}_{2^s}$, $s \geq 0$. Since D_8 is a subgroup of G, there is an involution $t \in G - (A\langle g\rangle)$. By (ii7), t does not centralize $\Omega_1(A)$ and we see that also gt and vgt do not centralize $\Omega_1(A)$. If $[g,t] = 1$, then $(gt)^2 = g^2 \notin \mathfrak{V}_1(A)$ and then (ii6) gives a contradiction. Similarly, if $[vg,t] = 1$, then $(vgt)^2 = (vg)^2 = g^2 \notin \mathfrak{V}_1(A)$ and again (ii6) gives a contradiction. We have proved that

$$[g,t] \neq 1, \quad [vg,t] \neq 1, \quad \text{and so } \langle g,t\rangle \cong \langle vg,t\rangle \cong \mathrm{D}_8$$

which gives $g^t = g^{-1}$ and $(vg)^t = (vg)^{-1}$. We compute

$$(vg)^t = (vg)^{-1} = (vg)(vg)^2 = (vg)g^2 = vg^{-1} = v^t g^t = v^t g^{-1},$$

and so $v^t = v$. Let $s \in \Omega_1(A) - \mathrm{C}_{\Omega_1(A)}(t)$ so that $\langle s,t\rangle \cong \mathrm{D}_8$, $w = ts$ is an element of order 4 in the coset At and $w^t = w^{-1}$. Since w commutes with v, (ii5) implies that $w^2 = v^2$ and $\langle w, g\rangle \cong \mathrm{H}_2$ with $g^w = g^{ts} = g^{-1}$. Hence gw is an element of order 4 and

$$(gw)^t = g^{-1}w^{-1} = (gg^2)(ww^2) = (gw)(g^2v^2) \neq gw.$$

By (ii3), $\langle gw, t\rangle \cong \mathrm{D}_8$ which implies $(gw)^t = (gw)^{-1}$. On the other hand,

$$(gw)^t = (gw)^{-1} = (gw)(gw)^2 = (gw)w^2 = (gw)v^2,$$

which contradicts the above result $(gw)^t = (gw)(g^2v^2)$. We have thus proved that $\exp(G) > 4$.

(iii) It remains to determine the structure of G in case $\exp(G) > 4$.

By (i) and Lemma 57.2, A is a maximal subgroup of G, all elements in $G - A$ are of order ≤ 4, $\exp(A) \geq 8$ and for each $g \in G - A$, g inverts $A/\Omega_1(A)$ and on $\mathfrak{V}_1(A)$. If $a \in A$ with $o(a) = 8$ and $g \in G - A$, then $a^g = a^{-1}\zeta$, $\zeta \in \Omega_1(A)$ and so $[a,g] = a^{-1}a^g = a^{-2}\zeta$, where $o(a^{-2}\zeta) = 4$ and therefore $|G'| > 2$. This gives together with $|G| = 2|\mathrm{Z}(G)||G'|$ (Lemma 1.1) that A is a unique abelian maximal subgroup of G. Since D_8 is a subgroup of G, there is an involution $t \in G - A$.

Let v be an element of order 4 in A. Then $v^t = v^{-1}\eta$, $\eta \in \Omega_1(A)$, and so

$$[v,t] = v^{-2}\eta \in \Omega_1(A) \quad \text{and} \quad 1 = [v,t^2] = [v,t][v,t]^t$$

which gives $[v,t]^t = [v,t]$. If $[v,t] \neq 1$, then $[v,t]$ is an involution commuting with v and t and so $\langle v,t\rangle' = \langle [v,t]\rangle$ which implies that $\langle v,t\rangle$ is minimal nonabelian (Lemma 65.2(a)). Hence in that case, $\langle [v,t]\rangle \cong \mathrm{D}_8$ and so $v^t = v^{-1}$. We have proved that t either centralizes or inverts each element of order 4 in A.

Assume that $A_0 = \mathrm{C}_A(t) = \mathrm{Z}(G)$ is not elementary abelian in which case we have $\exp(A_0) = 4$. Since t inverts $\mathfrak{V}_1(A)$, there is an element v of order 4 in $A - A_0$ such

that $v^t = v^{-1}$ and $v^2 \in A_0$. Let w be an element of order 4 in A_0. If $w^2 \neq v^2$, then vw is an element of order 4 in $A - A_0$ and so

$$(vw)^t = (vw)^{-1} = v^{-1}w^{-1} = v^t w^t = v^{-1}w^t$$

which implies $w^t = w^{-1}$, a contradiction. Hence $w^2 = v^2$, A_0 is of type $(4, 2, \ldots, 2)$ and $\mho_1(A_0\langle v\rangle) = \langle v^2\rangle$.

Suppose that there is an element y of order 4 in $A - (A_0\langle v\rangle)$ so that $y^t = y^{-1}$ and $y^2 \in A_0$. If $y^2 = v^2$, then yv is an involution in $A - (A_0\langle v\rangle)$ centralized by t, a contradiction. If there exists an involution $u \in A - (A_0\langle v\rangle)$, then $o(uv) = 4$ and $uv \in A - (A_0\langle v\rangle)$. Hence in case that $\Omega_2(A) > (A_0\langle v\rangle)$ we have an element y of order 4 in $\Omega_2(A) - (A_0\langle v\rangle)$ with $y^2 \in A_0$ and $y^2 \neq v^2$. For each $l \in A_0\langle v\rangle$ we obtain $(yl)^2 = y^2l^2$ with $l^2 \in \langle v^2\rangle$, and so all elements in $y(A_0\langle v\rangle)$ are of order 4 and they are inverted by t. Since $\langle y(A_0\langle v\rangle)\rangle = A_0\langle y, v\rangle$, t inverts $A_0\langle v\rangle$. This is a contradiction because for an element w of order 4 in A_0, we have $w^t = w$. We have proved that

$$\Omega_2(A) = A_0\langle v\rangle \quad \text{and} \quad A_0\langle v, t\rangle = A_0 * \langle v, t\rangle$$

with

$$\langle v, t\rangle \cong \mathrm{D}_8, \quad A_0 \cap \langle v, t\rangle = \langle v^2\rangle = \mathrm{Z}(\langle v, t\rangle) \quad \text{and} \quad \mho_1(A_0) = \langle v^2\rangle$$

so that each minimal nonabelian subgroup in $A_0\langle v, t\rangle$ is isomorphic to D_8 or Q_8.

Since H_2 is a subgroup of G, there is $a \in A - (A_0\langle v\rangle)$ such that $(at)^2 \in A_0 - \langle v^2\rangle$ and $v^{at} = v^{-1}$ so that $\langle at, v\rangle \cong \mathrm{H}_2$ with $\langle at, v\rangle' = \langle v^2\rangle$. Note that vw (with $w \in A_0$ and $w^2 = v^2$) is an involution in $(A_0\langle v\rangle) - A_0$ and $(vw)^{at} = (vw)^t = (vw)v^2$ and so $\langle at, vw\rangle$ is the nonmetacyclic minimal nonabelian of order 2^4, a contradiction.

We have proved that $A_0 = \mathrm{C}_A(t) = \mathrm{Z}(G)$ is elementary abelian. Then all elements of order 4 in $\Omega_2(A)$ are inverted by t and so t inverts $\Omega_2(A)$ and therefore we have $\mathrm{C}_A(t) = \mathrm{Z}(G) = \Omega_1(A)$. Since H_2 is not a subgroup of $\Omega_2(A)\langle t\rangle$, there are elements $a \in A - \Omega_2(A)$ and $v \in \Omega_2(A) - \Omega_1(A)$ such that

$$(at)^2 = \zeta \neq 1, \quad \zeta \in \Omega_1(A), \quad v^{at} = v^{-1} \quad \text{and} \quad \zeta \neq v^2.$$

We have $atat = \zeta$ and so $a^t = a^{-1}\zeta$. If $\mho_1(A)$ is cyclic, then $v^2 \in \mho_1(A)$ and so we must have in that case $\zeta \notin \mho_1(A)$.

(iv) We have obtained 2-groups stated in Theorem 93.1.

It is easy to check that all these 2-groups satisfy the assumptions of our theorem. Indeed, let G be a 2-group described in the second paragraph of Theorem 93.1. Since t inverts each element in $\Omega_2(A)$, we have $\mathrm{C}_A(t) = \Omega_1(A) = \mathrm{Z}(G)$. Let xt be any element in $G - A$, where $x \in A$. Then xt also inverts $\Omega_2(A)$ and on $A/\Omega_1(A)$. We get $(xt)^2 = xtxt = xx^t = x(x^{-1}s) = s$, where $s \in \Omega_1(A)$ so that $o(xt) \leq 4$. Let w be an element of order 4 in $\mho_1(A)$ such that $\zeta \notin \langle w\rangle$. From $a^t = a^{-1}\zeta$ we deduce $(at)^2 = \zeta \neq 1$ and so $\langle w\rangle \cap \langle at\rangle = \{1\}$ together with $w^{at} = w^t = w^{-1}$ implies that

$\langle at, w\rangle \cong \mathrm{H}_2$. Also, $\langle w, t\rangle \cong \mathrm{D}_8$ and therefore we have proved that both D_8 and H_2 actually appear as subgroups of G.

Let H be any minimal nonabelian subgroup of G so that $H \not\leq A$. Let $c \in H - A$ and $d \in (H \cap A) - \Phi(H)$ so that $H = \langle c, d\rangle$ and $o(c) \leq 4$. Suppose that $o(d) \geq 8$. In that case, $d^c = d^{-1}r$ with $r \in \Omega_1(A)$ so that $[d, c] = d^{-2}r$ is of order ≥ 4, a contradiction. Hence $o(d) \leq 4$ and in fact $o(d) = 4$ since $\Omega_1(A) \leq \mathrm{Z}(G)$. Since c inverts $\Omega_2(A)$, we have $d^c = d^{-1}$. If $o(c) = 2$, then $H = \langle c, d\rangle \cong \mathrm{D}_8$. In case $o(c) = 4$ and $c^2 = d^2$, we get $H \cong \mathrm{Q}_8$. If $o(c) = 4$ and $c^2 \neq d^2$, then $H \cong \mathrm{H}_2$ and we are done. □

§94

Nonabelian 2-groups all of whose minimal nonabelian subgroups are nonmetacyclic and have exponent 4

We consider here nonabelian 2-groups G all of whose minimal nonabelian subgroups are nonmetacyclic and have exponent 4. Then it is easy to prove that $\exp(G) = 4$. In fact, we prove the following result.

Theorem 94.1. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are nonmetacyclic and have exponent 4. Then $\exp(G) = 4$, $\Omega_1(G)$ is elementary abelian and if A is a maximal normal abelian subgroup of G containing $\Omega_1(G)$, then $\Phi(G) \leq \Omega_1(A)$ is elementary abelian and $\mho_1(A) \leq \mathrm{Z}(G)$.*

Proof. Since D_8 is not a subgroup of G, $\Omega_1(G)$ is elementary abelian. Let A be a maximal normal abelian subgroup of G containing $\Omega_1(G)$. Suppose that $\exp(G) > 4$. By Lemma 57.2, $|G : A| = 2$, all elements in $G - A$ are of order 4 and if x is one of them, then x inverts $\mho_1(A)$. Let y be an element of order 4 in $\mho_1(A)$. Then $y^x = y^{-1}$ which implies that $\langle x, y\rangle \cong \mathrm{Q}_8$ or $\langle x, y\rangle \cong \mathrm{H}_2$, a contradiction.

We have proved that $\exp(G) = 4$ and so $\exp(A) \leq 4$ and G/A is elementary abelian. Then $\Phi(G) = \mho_1(G) \leq \Omega_1(A)$ and so $\Phi(G)$ is elementary abelian. If $a \in A$ and $g \in G$ with $[a, g] \neq 1$, then $\langle a, g\rangle$ is minimal nonabelian. Indeed, $[a, g]$ is an involution in $\Omega_1(A)$ and $1 = [a, g^2] = [a, g][a, g]^g$ so that $[a, g]$ commutes with a and g and therefore $\langle a, g\rangle' = \langle [a, g]\rangle$. By Lemma 65.2(a), $\langle a, g\rangle$ is minimal nonabelian.

We prove that $\mho_1(A) \leq \mathrm{Z}(G)$. Indeed, let $a \in A$ be such that $a^2 \notin \mathrm{Z}(G)$. Then there is $g \in G$ with $[a^2, g] \neq 1$. But then $[a, g] \neq 1$ and so, by the previous paragraph, $\langle a, g\rangle$ is minimal nonabelian. In that case, $a^2 \in \Phi(\langle a, g\rangle) = \mathrm{Z}(\langle a, g\rangle)$ and so $[a^2, g] = 1$, a contradiction. □

Remark. It is easy to see that the group $\mathrm{H}_{16} \times \mathrm{C}_4$ contains both nonmetacyclic minimal nonabelian 2-groups of exponent 4, namely,

$$\mathrm{H}_{16} = \langle a, b \mid a^4 = b^2 = 1,\ [a, b] = z,\ z^2 = [a, z] = [b, z] = 1\rangle$$

(of order 16) and

$$\mathrm{H}_{32} = \langle a, b \mid a^4 = b^4 = 1,\ [a, b] = z,\ z^2 = [a, z] = [b, z] = 1\rangle$$

(of order 32) and each minimal nonabelian subgroup of $\mathrm{H}_{16} \times \mathrm{C}_4$ is nonmetacyclic.

We prove a lemma for $p = 2$ which might be useful for future similar investigations. The corresponding case for $p > 2$ was treated in Lemma 28.2.

Lemma 94.2. *Let G be a 2-group such that all subgroups of $\Phi(G)$ are normal in G. Then $\Phi(G)$ is abelian and $|G : \mathrm{C}_G(\Phi(G))| \leq 2$. If $|G : \mathrm{C}_G(\Phi(G))| = 2$, then each element $x \in G - (\mathrm{C}_G(\Phi(G))$ is of order ≤ 4 and x inverts each element in $\Phi(G)$.*

Proof. By assumption, $\Phi(G)$ is Dedekindian. Suppose that $\Phi(G)$ is nonabelian. Then $\Phi(G)$ possesses a subgroup $Q \cong \mathrm{Q}_8$. Since Q is normal in G and each cyclic subgroup of Q is normal in G, it follows that no element in G induces an outer automorphism on Q and so $G = Q\mathrm{C}_G(Q)$ with $Q \cap \mathrm{C}_G(Q) = \mathrm{Z}(Q)$. If M is a maximal subgroup of G containing $\mathrm{C}_G(Q)$, then $Q \not\leq M$, which contradicts the fact that $Q \leq \Phi(G)$. We have proved that $\Phi(G)$ is abelian.

Suppose that $\Phi(G)$ is cyclic. Let P be a cyclic subgroup of G which contains $\Phi(G)$ with $|P : \Phi(G)| = 2$. Let $x \in G - P$ so that $x^2 \in \Phi(G)$ and P is a maximal cyclic subgroup of index 2 in $P\langle x\rangle$. By the structure of such groups, x either centralizes $\Phi(G)$ or inverts $\Phi(G)$.

Now assume that $\Phi(G)$ is noncyclic so that $\Phi(G) = Z_1 \times \cdots \times Z_n$, where Z_i are cyclic and $n > 1$. Set

$$Z_i = \langle a_i\rangle \quad \text{and} \quad K = Z_1 \times \cdots \times Z_{i-1} \times Z_{i+1} \times \cdots \times Z_n$$

and consider G/K. By the above, for each $x \in G$ we have $a_i^x = a_i k$ or $a_i^x = a_i^{-1}k$ for some $k \in K$. But Z_i is normal in G and so $k = 1$. We have proved that each $x \in G$ either centralizes or inverts each Z_i, $i = 1, 2, \ldots, n$.

Suppose that $\Phi(G)$ possesses a subgroup $\langle v, w\rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$ such that for an element $x \in G$ we have $v^x = v^{-1}$ and $w^x = w$. In that case, $(vw)^x = v^{-1}w = v^2(vw)$, which contradicts the fact that $\langle vw\rangle$ is normal in G.

We have proved that each element $x \in G$ either centralizes $\Phi(G)$ or inverts each element in $\Phi(G)$. This gives $|G : \mathrm{C}_G(\Phi(G))| \leq 2$. Suppose that $|G : \mathrm{C}_G(\Phi(G))| = 2$ and let $x \in G - (\mathrm{C}_G(\Phi(G))$. Since x inverts $\Phi(G)$ and $x^2 \in \Phi(G)$, it follows that $\mathrm{o}(x^2) \leq 2$ which gives $\mathrm{o}(x) \leq 4$. The proof is complete. □

§95

Nonabelian 2-groups of exponent 2^e which have no minimal nonabelian subgroups of exponent 2^e

Here we solve a general problem (Nr. 1475 for $p = 2$) by classifying the title groups. More precisely, we prove the following result.

Theorem 95.1. *Let G be a nonabelian 2-group of exponent 2^e ($e \geq 3$) which does not possess a minimal nonabelian subgroup of exponent 2^e. Then G has a unique maximal normal abelian subgroup A. The factor group G/A is either cyclic or generalized quaternion and each element in $G - A$ is of order $< 2^e$. Also, G possesses at least one metacyclic minimal nonabelian subgroup and $|\mathrm{C}_G(\Omega_1(A)) : A| \leq 2$.*

Proof. Let G be a 2-group satisfying the assumptions of Theorem 95.1 and let A be any maximal normal abelian subgroup of G and $g \in G - A$. Set

$$2^m = \max\{\exp(H) \mid H < G \text{ is minimal nonabelian}\}$$

so that $m \geq 2$ and $m < e$. Further, set $T = A\langle g\rangle$, $A_0 = \mathrm{C}_A(g)$ so that $A_0 < A$ and $T_0 = A_0\langle g\rangle$ is abelian, $T_0 < T$ and T/A is cyclic. Let $T_1 \leq T$ with $T_1 > T_0$ and $|T_1 : T_0| = 2$. Set $A_1 = T_1 \cap A$ so that $T_1 = A_1\langle g\rangle$. Let $a \in A_1 - A_0$ so that $a^2 \in A_0$ and $[a, g] \in A \cap T_0 = A_0 \leq \mathrm{Z}(T_1)$. We have

$$1 = [a^2, g] = [a, g]^a[a, g] = [a, g]^2$$

so that $[a, g]$ is an involution commuting with a and g and therefore $\langle a, g\rangle$ is minimal nonabelian (Lemma 65.2(a)). In particular, we get $o(a) \leq 2^m$ and $o(g) \leq 2^m$. Since $A_1 = \langle A_1 - A_0\rangle$ and A_1 is abelian, we have $\exp(A_1) \leq 2^m$. We have proved that for each $g \in G - A$, $o(g) \leq 2^m$ and $A_0 = \mathrm{C}_A(g)$ is of exponent $\leq 2^m$.

Suppose at the moment that $g^2 \in A$ and let x be an element in A. Then we have also $(xg)^2 \in A$. Set $x^g = x^{-1}w$ for some $w \in A$. In that case,

$$w = xx^g = x(g^{-1}xg) = xg^{-2}gxg = g^{-2}(xg)^2$$

is an element of order $\leq 2^{m-1}$ in A. We have shown that an element $g \in G - A$ with $g^2 \in A$ inverts $A/\Omega_{m-1}(A)$. Thus for each $x \in A$,

$$(x^{2^{m-1}})^g = (x^g)^{2^{m-1}} = (x^{-1}w)^{2^{m-1}} = x^{-2^{m-1}}$$

and so g inverts $\mho_{m-1}(A)$. Since $\exp(A) = \exp(G) = 2^e$ and $e > m$, it follows that $\mho_{m-1}(A)$ contains elements of order ≥ 4. Hence G/A contains only one subgroup of order 2 which implies that G/A is either cyclic of order $\leq 2^m$ or generalized quaternion of order $\leq 2^{m+1}$ ($m \geq 2$).

Since $g \in G - A$ with $g^2 \in A$ inverts a cyclic subgroup of order 4 in $\mho_{m-1}(A)$, it follows that G possesses a metacyclic minimal nonabelian subgroup.

Suppose that G possesses another maximal normal abelian subgroup B, $B \neq A$. Then all elements in $G - A$ are of order $< 2^e$, all elements in $A - B = A - (A \cap B)$ are of order $< 2^e$ and since an element $b \in B - (A \cap B)$ centralizes $A \cap B$, we have also $\exp(A \cap B) < 2^e$. But then $\exp(G) < 2^e$, a contradiction.

Suppose that A satisfies $|\mathrm{C}_G(\Omega_1(A)) : A| \geq 4$. Let $H/A \cong \mathrm{C}_4$ be a subgroup of order 4 in $\mathrm{C}_G(\Omega_1(A))/A$ and let g be an element in $H - A$ such that $\langle g \rangle$ covers H/A. Set $A_0 = \mathrm{C}_A(g)$, $T_0 = A_0\langle g \rangle$ so that T_0 is abelian and $A_0 \geq \Omega_1(A)$. Further, set $S = \Omega_2(\mho_{m-1}(A))$ so that S is normal in H, $\exp(S) = 4$ and g^2 inverts S. Therefore $S \cap A_0 = \Omega_1(S)$ and ST_0 is a subgroup of H. Let T^* be a subgroup of ST_0 containing T_0 such that $|T^* : T_0| = 2$. Suppose that w is an element in $(T^* \cap S) - \Omega_1(S)$ so that $o(w) = 4$ and $w^2 \in \Omega_1(S) \leq A_0$ and $w^{g^2} = w^{-1}$. We now study the subgroup $\langle w, g \rangle$, where $1 \neq [w, g] \in T_0 \cap A = A_0$. Also,

$$1 = [w^2, g] = [w, g]^w [w, g] = [w, g]^2$$

and so $[w, g]$ is an involution commuting with both w and g. It now follows from Lemma 65.2(a) that $\langle w, g \rangle$ is minimal nonabelian. But then $g^2 \in \Phi(\langle w, g \rangle) = \mathrm{Z}(\langle w, g \rangle)$ and so g^2 centralizes w, a contradiction. The theorem is proved. □

Theorem 95.2. *Let G be a nonabelian 2-group of exponent 2^e ($e \geq 3$) which does not possess a minimal nonabelian subgroup of exponent 2^e. Let A be a unique maximal normal abelian subgroup of G (Theorem 95.1). Suppose that G possesses a cyclic subgroup Z with $Z \cap A = \{1\}$. Then G also possesses a nonmetacyclic minimal nonabelian subgroup.*

Proof. Set $Z = \langle v \rangle$, $v^2 = t$ and $A_0 = \mathrm{C}_A(v)$ so that the subgroup $T_0 = A_0 \times \langle v \rangle$ is abelian. By Theorem 95.1, $\Omega_1(A) \not\leq A_0$ and set $T_1 = \Omega_1(A)T_0$. Let T_2 be a subgroup of T_1 containing T_0 such that $|T_2 : T_0| = 2$. We have $T_2 = (\Omega_1(A) \cap T_2)T_0$ and take an involution $u \in (\Omega_1(A) \cap T_2) - \Omega_1(A_0)$. Then $[u, v] \in \Omega_1(A) \cap T_0 = \Omega_1(A_0)$ so that $[u, v]$ is an involution commuting with u and v and therefore $\langle u, v \rangle$ is minimal nonabelian. We have $t = v^2 \in \mathrm{Z}(\langle u, v \rangle)$ so that $\langle u, [u, v], t \rangle \cong \mathrm{E}_8$ and thus $\langle u, v \rangle$ is nonmetacyclic. □

§96

Groups with at most two conjugate classes of nonnormal subgroups

The non-Dedekindian p-groups all of whose nonnormal subgroups are conjugate were classified in §58. Below we offer another proof. Next we classify the p-groups with exactly two conjugate classes of nonnormal subgroups. Both these results are due to Otto Schmidt.

If G is a minimal nonabelian p-group, then (see Exercise 1.8(a) or Lemma 65.1) $G = \langle a, b\rangle$, where

(MA1) $a^{p^m} = b^{p^n} = c^p = 1$, $[a,b] = c$, $[a,c] = [b,c] = 1$, $|G| = p^{m+n+1}$, $G = \langle b\rangle\cdot(\langle a\rangle\times\langle c\rangle) = \langle a\rangle\cdot(\langle b\rangle\times\langle c\rangle)$ is nonmetacyclic with kernels $\langle a\rangle\times\langle c\rangle$, $\langle b\rangle\times\langle c\rangle$, respectively.

(MA2) $a^{p^m} = b^{p^n} = 1$, $a^b = a^{1+p^{m-1}}$, $|G| = p^{m+n}$ and $G = \langle b\rangle\cdot\langle a\rangle$ is metacyclic with kernel $\langle a\rangle$, $m > 1$.

(MA3) $G \cong \mathrm{Q}_8$, the ordinary quaternion group.

Let $\mathrm{nc}(G)$ be the number of conjugate classes of nonnormal subgroups of a group G and let $\mathrm{no}(G)$ be the number of orders of nonnormal subgroups of G. To facilitate the proof, we first prove some lemmas.

Lemma 96.1. *Let $G = \langle a, b\rangle$ be a minimal nonabelian p-group as in* (MA1) *or* (MA2).

(a) *All nonnormal cyclic subgroups of G have the same order if and only if one of the following holds:*

(a1) *G is as in* (MA2) *with $m \geq n$.*

(a2) *G is as in* (MA1) *with $m = n$.*

(b) *All nonnormal subgroups of G have the same order if and only if one of the following holds:*

(b1) *$G \in \{\mathrm{D}_8, S(p^3)\}$.*

(b2) *G is as in* (MA2) *with $m \geq n$.*

(c) *All nonnormal cyclic subgroups of G of same order are conjugate if and only if $G \cong M_{p^t}$.*

(d) *All nonnormal subgroups of G are conjugate if and only if $G \cong M_{p^t}$.*

Proof. We use the same notation as in (MA1) and (MA2). Write $A = \langle a \rangle$ and $B = \langle b \rangle$. Let $H < G$ be nonnormal; then $G' \not\leq H$ so that $H \cap G' = \{1\}$ since $|G'| = p$.

(a) Suppose that all nonnormal cyclic subgroups of G have the same order.

Let G be metacyclic as in (MA2) and let H be cyclic. If $n > m$ and $\Omega_m(B) = \langle x \rangle$, then $(ax)^b = (ax)a^{p^{m-1}} \notin \langle ax \rangle$ hence B and $D = \langle ax \rangle$ are not G-invariant, and they are cyclic of orders p^n and $p^m \neq p^n$, respectively, a contradiction. It remains to show that if $n \leq m$, then G satisfies the hypothesis. We have $H \cap A = \{1\}$ since $G' < A$ has order p and A is cyclic, so H, being isomorphic to a subgroup of G/A, has order $\leq p^n$. Since $\Omega_{n-1}(G) \leq \mathrm{Z}(G)$, our G satisfies the hypothesis and so it is as in (a1).

Suppose that G is nonmetacyclic as in (MA1). Since A and B are not G-invariant, we must have $m = n$ and G is as in (a2). Conversely, if G is as in (a2) with $m = n$, then, since $\Omega_{m-1}(G) \leq \mathrm{Z}(G)$, our G satisfies the hypothesis.

(b) Suppose that all nonnormal subgroups of G have the same order; then H is cyclic since it is not generated by its G-invariant maximal subgroups. Thus one can use (a).

Let G be metacyclic as in (a1); then $m \geq n$. It remains to show that such G satisfies the hypothesis. In view of $H \cap A = \{1\}$, we obtain that $|H| \leq |G : A| = p^n$. Since $\Omega_{n-1}(G) \leq \mathrm{Z}(G)$, we have $|H| = p^n$, and G is as in (b2).

Now let G be nonmetacyclic as in (a2) so $m = n$. Assume that $m > 1$. Then we see that $B \times \Omega_1(A)$ is nonnormal and noncyclic, a contradiction. Thus G is as in (b1).

(c) Suppose that all nonnormal cyclic subgroups of G of same order are conjugate; then these subgroups have the same order.

Let G be nonmetacyclic as in (MA1) and let $m, n > 1$. Assume that $m > n$. Let $\Omega_n(A) = \langle x \rangle$. Then the cyclic subgroups B and $\langle bx \rangle$ of the same order p^n are not normal, and since $B_G \neq \langle bx \rangle_G$, we conclude that B and $\langle bx \rangle$ are not conjugate. Thus $m \leq n$. Similarly, $n \leq m$ so $m = n$. Then the cyclic subgroups A and B of the same order p^m are neither normal nor conjugate, a contradiction.

Now let G be nonmetacyclic as in (MA1) and $m > n = 1$. Then G has exactly p^2 nonnormal subgroups of order p. Since any nonnormal subgroup has p conjugates, there are in G two nonconjugate subgroups of order p.

Let G be metacyclic as in (MA2). If $n = 1$, then $G \cong \mathrm{M}_{p^{m+1}}$ satisfies the condition. Now let $n > 1$. If $n < m$, set $\Omega_n(A) = \langle x \rangle$; then the cyclic subgroups B and $\langle bx \rangle$ of order p^n are neither G-invariant (otherwise, $G = A \times \langle bx \rangle$ is abelian) nor conjugate since their cores in G are different. If $n \geq m$, then the cyclic subgroups B and $\langle a^p b \rangle$ of order p^n are neither G-invariant nor conjugate since their cores in G are different, a contradiction.

Statement (d) follows from (c). □

Below we present an alternate proof of Theorem 1.23.

Lemma 96.2 (= Theorem 1.23 (Passman)). *Assume G is a non-Dedekindian p-group. Then there is a G-invariant subgroup R of index p in G' such that G/R is non-Dedekindian.*

Proof. If $p > 2$, the result is obvious as Dedekindian groups of odd order are abelian.

Now let $p = 2$. Assume that for every G-invariant subgroup K of index 2 in G', the quotient group G/K is Dedekindian. We want to prove that G is itself Dedekindian. One may assume that $K > \{1\}$. Assuming that G is a minimal counterexample, we get $|K| = 2$ (this is due to the fact that the derived subgroup of a nonabelian Dedekindian group is of order 2; see Theorem 1.20) so $|G'| = 4$. It follows that G is not minimal nonabelian (Lemma 65.1) and there is in G/K a subgroup $Q/K \cong \mathrm{Q}_8$ (Theorem 1.20). Since Q is not of maximal class (Theorem 1.2), we get $|Q'| = 2$ (Proposition 1.6), and so $G' = Q' \times K \cong \mathrm{E}_4$ and $G' \le \mathrm{Z}(G)$.

Let $A < G$ be minimal nonabelian. Assume that $|A| > 8$; then $K < A$ (otherwise, A is isomorphic to a subgroup of G/K, which is impossible since all minimal nonabelian subgroups of the nonabelian Dedekindian group G/K are isomorphic to Q_8 by Theorem 1.20). Assume that A/K is abelian; then it is of type $(4, 2)$ (here we use Theorem 1.20 again), and hence $A' = K$. In this case, $G'/K = \mho_1(G/K) < A/K$, and we conclude that $G' < A$, and so $A \lhd G$. Then A/Q' is nonabelian in view of $Q' \cap K = \{1\}$, hence $A/Q' \cong \mathrm{Q}_8$ by hypothesis. Thus one can assume from the start that $A/K \cong \mathrm{Q}_8$. In this case,

$$A \cong \mathscr{H}_{2,2} = \langle x, y \mid x^4 = y^4 = 1,\ x^y = x^3 \rangle$$

since $|\Omega_1(A)| = 4$ and $\exp(A) = 4$ (see Lemma 65.1 or (MA1) and (MA2)). We know that all subgroups of order 2 are characteristic in A so normal in G. Then $A/\langle y^2 \rangle \cong \mathrm{D}_8$ so $G/\langle y^2 \rangle$ is not Dedekindian, contrary to the assumption. Thus $|A| = 8$ so that any minimal nonabelian subgroup of G has order 8.

Assume that $A \cong \mathrm{D}_8$. Let $L < G'$ of order 2 be such that $L \not\le A$. Then $AL/L \cong \mathrm{D}_8$ so G/L is not Dedekindian, a contradiction. Thus $A \cong \mathrm{Q}_8$.

Then $A \lhd G$ (indeed, any abelian subgroup of type $(2, 2)$ of a Dedekindian group G/A' is normal). Write $C = \mathrm{C}_G(A)$. Then G/C is a subgroup of a Sylow 2-subgroup of $\mathrm{Aut}(A) \cong \mathrm{S}_4$, which is isomorphic to D_8. It follows that $G/C \cong \mathrm{E}_4$, and we conclude that $G = A * C$. Since $|G'| = 4$, C is nonabelian. Let $B < C$ be minimal nonabelian; then, by the above, $B \cong \mathrm{Q}_8$. If $A \cap B > \{1\}$, then $A * B$ is extraspecial so it contains a subgroup $\cong \mathrm{D}_8$ (Appendix 16), contrary to what has been proved above. Thus we get $A \cap B = \{1\}$. If $U < A' \times B' = G'$ is of order 2 and $A' \ne U \ne B'$, then AB/U is an extraspecial subgroup of order 2^5 of the Dedekindian group G/U, a final contradiction. □

The presented proof of Lemma 96.2 is longer than the original one. Our aim here was to show an application of minimal nonabelian subgroups.

The following lemma is a partial case of Theorem 96.7.

Lemma 96.3. *Let G be a p-group with $|G'| = p$ and* $\mathrm{nc}(G) = 1$. *Then* $G \cong \mathrm{M}_{p^n}$.

Proof. We use induction on $|G|$. In view of Lemma 96.1(c), one may assume that G is not minimal nonabelian. Let $H < G$ be minimal nonabelian. Then $G = H\mathrm{C}_G(H)$

(Lemma 4.3) so $C_G(H) \not\leq H$. Since $\mathrm{nc}(H) \leq \mathrm{nc}(G) = 1$ (see the decomposition of G in the previous sentence), we get $H \in \{Q_8, M_{p^n}\}$ by induction.

(i) $H \cong Q_8$. Since G is non-Dedekindian, we get $\exp(C_G(H)) > 2$. Suppose that $L = \langle x \rangle \leq C_G(H)$ is cyclic of order 4. If $L \cap H = \{1\}$ and $\langle a \rangle$, $\langle b \rangle$ are distinct cyclic subgroups of order 4 in H, then the nonnormal subgroups $\langle ax \rangle$, $\langle bx \rangle$ do not belong to the same G-class[1], and this is a contradiction. Now assume that $L \cap H = Z(H)$. Then the central product $L * H$ (of order 16) has exactly six nonnormal subgroups of order 2, and these subgroups do not belong to the same conjugate class since 6 is not a power of 2 (note that $HL \lhd G$ since $G' < H < HL$), a contradiction. Thus G has no subgroups $\cong Q_8$.

(ii) Let $H \cong M_{p^n}$. Assume that there is in G a subgroup L of order p with $L \not\leq H$. Since H has a nonnormal subgroup B of order p, $\mathrm{nc}(G) = 1$ and $H \lhd G$, we get $L \lhd G$. Then $HL = H \times L$, and this subgroup has exactly p^2 nonnormal subgroups of order p which do not belong to the same G-class (indeed, every nonnormal subgroup of G of order p has exactly p conjugates). We get a contradiction since $HL \lhd G$. Thus we have $\Omega_1(G) = \Omega_1(H) \cong E_{p^2}$. If $p > 2$, then, by Theorem 13.7 or Theorem 69.4, G is metacyclic. By Lemma 65.2(a), since $|G'| = p$, the group G is minimal nonabelian, contrary to the assumption.

Now let $p = 2$. By Lemma 65.2(a), G is nonmetacyclic (see the previous paragraph). Therefore, by Theorem 66.1, $\Omega_2(G) \not\leq H$. It follows that there is a cyclic $L < G$ of order 4 such that $L \not\leq H$. Then $L \lhd G$ by hypothesis so $L \cap H = H'$ (recall that $Z(H)$ is cyclic). Write $F = L\Omega_2(H)$. Then $F/H' \cong E_8$. Since $|\Omega_1(F)| = 4$, it follows that F is nonabelian. Then it contains a minimal nonabelian subgroup of order 8, contrary to what has been proved above. □

If G is nilpotent and $\mathrm{nc}(G) = 1$, then, as is easily seen, G is primary. Therefore, in Theorem 96.4 we consider p-groups.

Theorem 96.4 (O. Schmidt [Sch3]). *Let G be a p-group. If $\mathrm{nc}(G) = 1$, then we have $G \cong M_{p^{n+1}}$.*

Proof. We proceed by induction on G. In view of Lemma 96.3, one may assume that $|G'| > p$; then G is neither Dedekindian nor minimal nonabelian. Therefore, by Lemma 96.2, there is in G' a G-invariant subgroup R of order p such that G/R is not Dedekindian. By induction, $G/R \cong M_{p^n}$. Let U/R and V/R be two distinct cyclic subgroups of index p in G/R. Then $U, V \in \Gamma_1$ are distinct abelian so $U \cap V = Z(G)$. Since $R < G' \leq \Phi(G)$, we get

$$d(G) = d(G/R) = 2$$

so G is minimal nonabelian (Lemma 65.2(a)), a final contradiction. □

Below we freely use properties of minimal nonnilpotent groups which are listed in Theorem A.22.1.

[1] We have $\langle ax \rangle^b = \langle a^{-1}x \rangle \notin \{\langle ax \rangle, \langle bx \rangle\}$, and the same is true for $\langle bx \rangle^a$.

Supplement to Theorem 96.4 (O. Schmidt [Sch3]). *Let G be a nonnilpotent group. Then* $\mathrm{nc}(G) = 1$ *if and only if G is minimal nonabelian with derived subgroup of prime order.*

Proof. Let $H \leq G$ be minimal nonnilpotent. Then $H = PQ$, where $P \in \mathrm{Syl}_p(G)$ is cyclic and $H' = Q \in \mathrm{Syl}_q(G)$, $p \neq q$. In this case, all nonnormal subgroups of G are conjugate with P. It follows that P is maximal in H and all subgroups of Q are normal in G so $|Q| = q$. Since $\mathrm{N}_G(P)$ is nonnormal in G, we get $\mathrm{N}_G(P) = P$ so $H = G$ as H is normal in G and, by Frattini's lemma, $G = H\mathrm{N}_G(P) = HP = H$. □

Next we classify the p-groups G with $\mathrm{nc}(G) = 2$.

Lemma 96.5. *If $G = \langle a, b\rangle$ is a minimal nonabelian p-group and the number of conjugate classes of nonnormal subgroups of G is equal to* $\mathrm{nc}(G) = 2$*, then $p = 2$ and $G \in \{\mathrm{D}_8, \mathcal{H}_{2,m},\ m \geq 2\}$. Here $\mathcal{H}_{2,m} = \langle a, b \mid a^{2^m} = b^4 = 1,\ a^b = a^{1+2^{m-1}}\rangle$.*

Proof. Let G be as in (MA1) or (MA2). Write $A = \langle a\rangle$, $B = \langle b\rangle$.

(i) Let G be nonmetacyclic as in (MA1). The subgroups A and B are neither G-invariant nor conjugate. The normal closures $A^G = A \times G'$, $B^G = B \times G'$ are of order $p|A|$, $p|B|$, respectively. Suppose that $m > 1$. Then $H = B\Omega_1(G) = B \times E$, where $E \cong \mathrm{E}_{p^2}$. Let $L < E$ be of order p such that $B \times L \neq B \times G'$. Then $B \times L$ is not normal in G (otherwise, $B = (B \times L) \cap (B \times G') \lhd G$), and we get $\mathrm{nc}(G) > 2$, a contradiction. Similarly, we consider the case $n = 1$ so that $|G| = p^3$. But D_8 is metacyclic and $\mathrm{nc}(S(p^3)) = p > 2$ (recall that $S(p^3)$ is nonabelian of order p^3 and exponent $p > 2$).

(ii) Now let G be metacyclic as in (MA2); $n > 1$ (otherwise, $G \cong \mathrm{M}_{p^{m+1}}$ and $\mathrm{nc}(G) = 1$). Since $G' < \Omega_1(G) \cong \mathrm{E}_{p^2}$, every nonnormal subgroup of G being abelian is cyclic. If $H < G$ is cyclic of order p^n such that $G' \not\leq H$, then $G = H \cdot A$ is a semidirect product so H is not normal in G.

(ii1) Assume that $n > m$. Then $B_1 = \langle ab\rangle$ of order p^n is neither a-invariant (otherwise, $G = \langle a\rangle \times B_1$ would be abelian) nor conjugate with B since $B_1 \not\leq B^G = B \times G'$. Suppose that $\Omega_m(B) = \langle y\rangle$; then $A_1 = \langle ay\rangle$ of order p^m is not b-invariant and $|A_1| < |B| = |B_1|$ so $\mathrm{nc}(G) \geq 3$, a contradiction.

(ii2) Let $n = m$. If $U/G' < G/G'$ is cyclic of order p^m, then $U = G' \times V$ so the cyclic subgroup V is not normal in G since $G' \not\leq V$ so that $A \cap V = \{1\}$. There are in G/G' exactly

$$\frac{p^{2m-1} - p^{2m-2}}{p^{m-1} \cdot (p-1)} = p^{m-1}$$

distinct cyclic subgroups U_i/G' of order p^m. If $U_i = G' \times V_i$, then the subgroups $V_1, \ldots, V_{p^{m-1}}$ that have trivial intersections with A are not G-invariant and pairwise nonconjugate in G since all $U_i/G' \lhd G/G'$ are distinct. It follows that $p^{m-1} \leq 2$ so $p = 2 = m$; then $G \cong \mathcal{H}_{2,2}$.

(ii3) Let $n < m$. As we have noticed, $n > 1$. The subgroup $\Omega_n(G)$ is abelian of type (p^n, p^n) so it contains exactly

$$\frac{p^{2n} - p^{2n-2}}{p^{n-1}(p-1)} = p^{n-1}(p+1)$$

cyclic subgroups of order p^n and exactly p^{n-1} of them contain G'. It follows that G has exactly $p^{n-1}(p+1) - p^{n-1} = p^n$ nonnormal cyclic subgroups of order p^n which are partitioned in p^{n-1} classes of conjugate subgroups. We have $\mathrm{nc}(G) = 2 \geq p^{n-1}$ so $n = 2$ and $p = 2$, and we get $G = \mathscr{H}_{2,m}$. □

Let $G = M \times C$, where $M = \langle a, b \mid a^{p^{n-1}} = b^p = 1, a^b = a^{1+p^{n-2}} \rangle \cong \mathrm{M}_{p^n}$ and $C = \langle c \rangle$. Set $\sigma = a^{p^{n-2}}$. Then $\mathrm{Z}(G) = \langle \sigma \rangle \times \langle c \rangle$ contains exactly $p+1$ subgroups of order p and $\mathrm{c}_1(G) = p^2 + p + 1$. Therefore exactly $\mathrm{c}_1(G) - (p+1) = p^2$ subgroups of order p of G are non-G-invariant so they belong to p distinct G-classes. Also the subgroup $\langle b \rangle \times \langle c \rangle$ of order p^2 is non-G-invariant so that $\mathrm{nc}(G) \geq 1 + p > 2$.

Lemma 96.6. *If G is a p-group such that $|G'| = p$ and $\mathrm{nc}(G) = 2$, then $p = 2$ and $G \in \{\mathrm{D}_8, \mathscr{H}_{2,\mathrm{m}}\}$.*

Proof. In view of Lemmas 96.3 and 96.5, one may assume that G is not minimal nonabelian. Let $A < G$ be minimal nonabelian; then $A \lhd G$ since $A' = G'$ in view of $|A'| = p = |G'|$, so $G = A * C$, where $C = \mathrm{C}_G(A)$ (Lemma 4.3). By assumption, we have $C \not\leq A$. Two subgroups of A are G-conjugate if and only if they are A-conjugate. Therefore $\mathrm{nc}(A) \leq \mathrm{nc}(G) = 2$ so $A \in \{\mathrm{Q}_8, \mathrm{M}_{p^n}, \mathrm{D}_8, \mathscr{H}_{2,m}\}$ by Lemma 96.3 and Theorem 96.5.

(i) Let $A \cong \mathrm{D}_8$. Then A contains two nonnormal subgroups L_1, L_2 of order 2 which are not conjugate in A, and so neither in G. If L of order 2 is such that $L \not\leq A$ (L exists by Theorem 1.17(b) since G is not of maximal class), then $L \lhd G$; then $L_3 = L_1 \times L$ is not normal in G since $A \cap L_3 = L_1$, and we get $\mathrm{nc}(G) > 2$, a contradiction. Thus G has no subgroup $\cong \mathrm{D}_8$.

(ii) Let $A \cong \mathrm{Q}_8$. Since G is not Dedekindian, $\exp(C) > 2$. Let $\langle l \rangle = L \leq C$ be cyclic of order 4. If $A \cap L = \mathrm{Z}(A)$, then $A * L \cong \mathrm{D}_8 * L$ contains a subgroup $\cong \mathrm{D}_8$, contrary to (i). Thus $A \cap L = \{1\}$ hence $H = AL = A \times L$. Let $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$ be distinct (cyclic) subgroups of order 4 in A. Then the subgroups $\langle al \rangle$, $\langle bl \rangle$ are not c-invariant and $\langle cl \rangle$ is not a-invariant; since these three subgroups are not G-conjugate in pairs, we get $\mathrm{nc}(G) > 2$, a contradiction. Thus G has no subgroup $\cong \mathrm{Q}_8$.

(iii) Suppose that

$$A = \langle a, b \mid a^4 = b^{2^m} = 1, a^b = a^3 \rangle \cong \mathscr{H}_{2,m}.$$

Then $B = \langle b \rangle$ and $B_1 = \langle ba^2 \rangle$ are neither conjugate nor A-invariant so are not G-invariant. Assume that there is $L < G$ of order 2 such that $L \not\leq A$. Then $L < \mathrm{Z}(G)$. Since $B \times L$ and $B_1 \times L$ are not G-invariant (for example, $A \cap (B \times L) = B$ is not A-invariant), we get $\mathrm{nc}(G) > 2$. Thus L does not exist so $\Omega_1(G) = \Omega_1(A) \cong \mathrm{E}_4$.

Since $C \not\leq A$ and $A \cap C = \mathrm{Z}(A) = \Phi(A)$, it follows that $\mathrm{d}(G) > 2$ so G is nonmetacyclic. Let $M < G$ be minimal nonmetacyclic. Since $|\Omega_1(M)| \leq |\Omega_1(G)| = 4$ and all minimal nonabelian subgroups of G have order > 8, we obtain that $|M| = 2^5$ (Lemma 66.1(d)). Because of $|M'| = 4 > 2 = |G'|$, we get a contradiction. Next we assume that G has no subgroup $\cong \mathscr{H}_{2,m}$.

(iv) Now suppose that A is as in (MA2) with $n = 1$; then $A \cong \mathrm{M}_{p^{m+1}}$, and $B = \langle b \rangle$ is not G-invariant. Let $L < G$ be a subgroup of order p not contained in A. Write $H = L\Omega_1(A)$; then $|H| = p^3$. By (i), we have $\exp(H) = p$. Assume that H is nonabelian. Then $p^2 + p$ noncentral subgroups of H of order p belong to $p + 1$ distinct G-classes so $\mathrm{nc}(G) \geq p + 1 > 2$, a contradiction. Now assume that $H \cong \mathrm{E}_{p^3}$. Then we get $|H \cap \mathrm{Z}(G)| \in \{p, p^2\}$. In the first case, we obtain a contradiction as above. Let $|H \cap \mathrm{Z}(G)| = p^2$. Then p^2 subgroups of H of order p that are not contained in $\mathrm{Z}(G)$ belong to p distinct G-classes, and we conclude that $p = 2$. As $H \not\leq \mathrm{Z}(G)$, it contains also a non-G-invariant subgroup of order 4; then $\mathrm{nc}(G) \geq 2 + 1 > 2$, a contradiction. Thus $\Omega_1(G) = \Omega_1(A) \cong \mathrm{E}_{p^2}$. Now it follows from (i) and (ii) that C is cyclic. Since $A \cap C = \mathrm{Z}(A) = \mathfrak{V}_1(A)$, we get $\mathfrak{V}_1(A) < C$.

Let $C_0 \leq C$ be (cyclic) of order $o(a)$ (note that $\langle a^p \rangle < C$ and C is cyclic). Write $F = A_0C_0$. Then $F = A_0 \times K$, where $|K| = p$ (basic theorem on abelian p-groups). It follows from $F \not\leq A$ that $K \not\leq A$. Since $|K| = p$, we get a contradiction to the result of the previous paragraph. □

Theorem 96.7 (O. Schmidt [Sch4]). *If a group G is nilpotent and $\mathrm{nc}(G) = 2$, then either $p = 2$ and $G \in \{\mathrm{D}_8, \mathrm{Q}_{16}, \mathscr{H}_{2,m}\}$ or $G \cong \mathrm{M}_{p^n} \times \mathrm{C}_q$, where $q \neq p$ are any primes.*

Proof. It is easily checked that the groups from the conclusion satisfy the hypothesis.

Let $G = P \times Q$, where $P \in \mathrm{Syl}_p(G)$ with $\mathrm{nc}(P) > 0$ and $Q > \{1\}$ is a p'-group. If $\{1\} \leq L \leq Q$ and $U < P$ is not P-invariant, then $L_1 = U \times L$ is not G-invariant since $P \cap L_1 = U$. It follows that $|Q| = q$, a prime, and $\mathrm{nc}(P) = 1$ so $P \cong \mathrm{M}_{p^n}$ by Theorem 96.4. If $G = P \times Q$ is a p-group, $Q > \{1\}$, then $\mathrm{nc}(G) > 2$ (Lemma 96.6).

Next we assume that G is a p-group; then G has no nontrivial direct factors by the previous paragraph. If G has a cyclic subgroup of index p, then $G \in \{\mathrm{D}_8, \mathrm{Q}_{16}\}$ (note that $\mathrm{nc}(\mathrm{SD}_{16}) = 3$). Next we assume that G has no cyclic subgroup of index p.

In view of Lemma 96.6, one may assume that $|G'| > p$. By Lemma 96.2, there exists in G' a G-invariant subgroup R of index p such that G/R is not Dedekindian. Then we have $|(G/R)'| = p$ and $1 \leq \mathrm{nc}(G/R) \leq \mathrm{nc}(G) = 2$ so, by Theorem 96.4 and Lemma 96.6, $G/R \in \{\mathscr{H}_{2,m}\ (p = 2), \mathrm{M}_{p^n}, \mathrm{D}_8\}$. Since $R < G' \leq \Phi(G)$, we get $\mathrm{d}(G) = \mathrm{d}(G/R) = 2$. Below we consider these three possibilities.

(i) If $G/R \cong \mathrm{D}_8$, then $|G : G'| = 4$ so G is of maximal class by Taussky's theorem, a contradiction since, by assumption, G has no cyclic subgroup of index 2.

(ii) Let $p = 2$ and $G/R \cong \mathscr{H}_{2,m}$, $m \geq 2$. To obtain a contradiction, one may assume that $|R| = 2$. Then G/R has two nonnormal and not conjugate subgroups S_1/R and S_2/R of order 2^m; then S_1 and S_2 are not conjugate in G. Since, in view of $\mathrm{nc}(G) = 2$, all subgroups of order 2^m are normal in G, S_1 and S_2 are cyclic of or-

der 2^{m+1}. As $\bar{G} = G/(S_1)_G \cong \mathrm{D}_8$ has exactly four nonnormal subgroups of order 2, and among of them $\bar{S}_1$ and $\bar{S}_2$, the inverse images in G of these four subgroups must be cyclic. It follows that $Z = (S_1)_G = \mathrm{Z}(G)$ (if $Z < \mathrm{Z}(G)$, then $|G : \mathrm{Z}(G)| = 4$ hence $|G'| = 2$ by Lemma 1.1, a contradiction). Let $S_1 < M \in \Gamma_1$. Then S_1 is cyclic of index 2 in M so $M \in \{\mathrm{C}_2 \times \mathrm{C}_{2^m}, \mathrm{M}_{2^{m+1}}\}$ (Theorem 1.2). In the second case, M has a nonnormal subgroup of order $2 < 2^{m+1}$ so $\mathrm{nc}(G) > 2$, a contradiction. Thus M is abelian. Similarly, the remaining two members of the set Γ_1 are abelian; then G is minimal nonabelian since $\mathrm{d}(G) = 2$. We have $|G'| = 2$, and this is a contradiction.

(iii) Let $G/R \cong \mathrm{M}_{p^n}$. To obtain a contradiction, it suffices to assume that $|R| = p$. Let A/R and B/R be two distinct cyclic subgroups of index p in G/R. Then A and B are distinct abelian maximal subgroups of G so $A \cap B = \mathrm{Z}(G)$ has index p^2 in G and G is minimal nonabelian; then $|G'| = p$, contrary to the assumption. □

The 2-groups $\mathcal{H}_{2,m}$ are not presented in [Sch4] so Schmidt's proof is not full.

O. Schmidt [Sch4] also classified the nonnilpotent groups G with $\mathrm{nc}(G) = 2$. His proof is very long and not full (at first, this fact was noticed in [SU]). This question is the subject of the recent paper [M] as well. For related results see also [PR]. Below we offer another approach to prove that theorem. In the nonnilpotent case we show an essentially stronger result, namely, we classify the nonnilpotent groups G with $\mathrm{no}(G) = 2$, where $\mathrm{no}(G)$ is the number of orders of non-G-invariant subgroups in G.

Write

$$\Delta(G) = \{|H| \mid H < G \text{ is nonnormal in } G\}$$

so that $|\Delta(G)| = \mathrm{no}(G)$.

(MNN) (O. Schmidt, Y. Gol'fand; see Lemma A.22.1) Let G be a minimal nonnilpotent group. Then $|G| = p^a q^\beta$, where p and q are distinct prime numbers. Let $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$. Then the following statements hold:

(a) One of the subgroups P, Q (say Q) is normal and coincides with G'.

(b) If Q is abelian, then $Q \cap \mathrm{Z}(G) = \{1\}$ and $\exp(Q) = p$.

(c) P is cyclic and $|P : (P \cap \mathrm{Z}(G))| = p$.

(d) Let Q be nonabelian. Then Q is special (i.e., $\mathrm{Z}(Q) = Q' = \Phi(Q)$ is elementary abelian) and $|Q/Q'| = q^b$, where b is the order of $q \pmod p$, $Q \cap \mathrm{Z}(G) = \mathrm{Z}(Q)$. If $L < \mathrm{Z}(Q)$ is of index p, then Q/L is extraspecial so that b is even.

A group from (MNN) is said to be an $\mathrm{S}(p, q)$-*group*.

In Theorem 96.8, p, q are distinct primes.

Theorem 96.8. *Let G be a nonnilpotent group such that* $\mathrm{no}(G) = 2$. *Then G is solvable and one of the following holds:*

(a) $G = H \times C$, *where either*

(a1) H *is minimal nonabelian of order* $p^a q$ *and* $|C| = r \neq q$, $\Delta(G) = \{p^a, p^a r\}$, *or*

(a2) H *is nonabelian of order* pq *and* $|C| = p$, $\Delta(G) = \{p, p^2\}$.

In what follows, $G = P \cdot Q$, where $P \in \mathrm{Syl}_p(G)$ is non-G-invariant, $Q \in \mathrm{Syl}_q(G)$ and $Q \lhd G$.

(b) *G is minimal nonabelian of order pq^2, $\Delta(G) = \{p, q\}$.*

(c) *We have $|Q| = q$, P is cyclic of order p^a, $a > 1$, $G/\mathrm{Z}(G)$ is a Frobenius group of order p^2q, $\Delta(G) = \{p^a, p^{a-1}\}$.*

(d) *One has $G = P \cdot Q$ with Q of order q^2 and cyclic P of order p^a, $\mho_1(P) = \mathrm{Z}(G)$, $G/\mathrm{Z}(G)$ is a Frobenius group of order pq^2, all subgroups of Q are G-invariant, $\Delta(G) = \{p^a, p^aq\}$.*

(e) *One has $P \cong \mathrm{Q}_8$, $|Q| = q$, G has exactly one cyclic subgroup of index 2 and $\Delta(G) = \{4, 8\}$.*

Proof. By Burnside's two-prime theorem, G is solvable since it has at most two non-normal Sylow subgroups of distinct orders. Let $H < G$. Then $\mathrm{no}(H) \le \mathrm{no}(G) = 2$. If, in addition, H is not G-invariant, then even $\mathrm{no}(H) \le 1$.

Suppose that $G = P \cdot Q$ is an $\mathrm{S}(p, q)$-group as in (MNN). Then $|Q| > q$ (otherwise, $\mathrm{no}(G) = 1$) and P is not G-invariant. If $Q' > \{1\}$, then PK, where $\{1\} < K \le Q'$, is not normal in G so $|Q'| \le q$. Assume that $|Q'| = q$; then $|Q/Q'| \ge q^2$ and PQ' is not normal in G. If $Q' < Q_1 < Q$, then Q_1 is not normal in G so $\mathrm{no}(G) > 2$, a contradiction. Thus $Q' = \{1\}$ so Q is elementary abelian and G is minimal nonabelian. Since every nontrivial subgroup of Q is not normal in G, we get $|Q| = q^2$. Assume that $|P| > p$. If $\{1\} < Q_1 < Q$, then $\mho_1(P)Q_1$ is not normal in G so $\mathrm{no}(G) > 2$, a contradiction. Thus G is an minimal nonabelian subgroup of order pq^2 as in (b).

In what follows we assume that G is not minimal nonnilpotent.

Next let $P \cdot Q = H < G$ be an $\mathrm{S}(p, q)$-subgroup as in (MNN). Then $\mathrm{no}(H) \le 2$ hence H is minimal nonabelian by the above, so either $\mathrm{no}(H) = 1$ with $|Q| = q$ (Supplement to Theorem 96.4) or $\mathrm{no}(H) = 2$ and H is of order pq^2, $H \lhd G$.

Suppose that $r \in \pi(G) - \pi(H)$ and let $R \in \mathrm{Syl}_r(G)$. Since G is solvable, one may assume that $PR < G$. If R is not normal in G, then P, R and PR are not normal in G and have different orders hence $\mathrm{no}(G) > 2$, a contradiction. Thus $R \lhd G$. If $R_1 < R$ is G-invariant, then PR_1 is not normal in G since $PR_1 \cap H = P$. We conclude that R is a minimal normal subgroup of G. Since P and RP are not normal in G, we get $H \lhd G$ so $G = H \times R$, and we conclude that $|R| = r$. Thus G is as in (a).

In what follows we assume that $\pi(G) = \pi(H) = \{p, q\}$, where H here and below is a proper $\mathrm{S}(p, q)$-subgroup of G chosen above.

(i) Suppose that H is not normal in G; then $\mathrm{no}(H) = 1$ so $H' = Q \lhd G$ is of order q and $\mho_1(P) \lhd G$. All subgroups of G of order $\ne |P|, |H|$ are G-invariant hence $P \in \mathrm{Syl}_p(G)$ and $\Delta(G) = \{|P|, |P|q\}$. Then $\mathrm{N}_G(P)$ is not G-invariant and $Q_0 \in \mathrm{Syl}_q(G)$ is normal in the group G since $|Q_0| > |Q| = q$ in view of $H < G$. Next, $|\mathrm{N}_G(P)| \in \{|P|, |P|q\}$.

(i1) Assume that Q_0 is noncyclic of order $q^c > q^2$. Then there exist in Q_0 two distinct maximal subgroups Q_1 and Q_2 (of order $q^{c-1} > q = |Q|$). In this case,

$Q_1, Q_2 \lhd G$ and PQ_1 and PQ_2 are distinct subgroups of G of order $|P|q^{c-1} > |H|$ so these subgroups are G-invariant. It follows that $P \leq L = PQ_1 \cap PQ_2 \lhd G$ and $|G : L| = q^2$. By Frattini's lemma, we obtain $G = L\mathrm{N}_G(P)$ hence $P < \mathrm{N}_G(P)$, $|\mathrm{N}_G(P)| > |H|$ so that $\mathrm{no}(G) > 2$ since $\mathrm{N}_G(P)$ is nonnormal in G, a contradiction.

(i2) Let Q_0 be cyclic of order $q^c > q^2$; then $\mathrm{N}_G(P)$ is abelian so $\mathrm{N}_G(P) = P$ since Q is a unique subgroup of order q in G. If $Q_1 < Q_0$ is of index q in Q, then $PQ_1 = \mathrm{N}_G(P)Q_1 \lhd G$, a contradiction since $\mathrm{N}_G(P) > PQ_1$.

Thus $|Q_0| = q^2$. By hypothesis, all subgroups of order q are G-invariant. In this case, $\Delta(G) = \{|P|, |P|q|\}$.

(i3) Assume that $P < \mathrm{N}_G(P)$. Then $\mathrm{N}_G(P) = P \times Q_1$, where $|Q_1| = q$, $Q_1 \lhd G$ and $\mathrm{C}_G(Q_1) \geq PQ_0 = G$ so $G = H \times Q_1$, and hence $H \lhd G$, contrary to the assumption. Thus $\mathrm{N}_G(P) = P$. We have $\mho_1(P) \lhd G$ so $\mho_1(P) = \mathrm{Z}(G)$, and we conclude that $G/\mho_1(P)$ is a Frobenius group of order pq^2. As we have noticed, all subgroups of $Q_0 (\in \mathrm{Syl}_q(G))$ are G-invariant; then G is as in (d).

(ii) Now suppose that $H \lhd G$; then $|H| \in \{p^a q, pq^2\}$.

(ii1) Assume that $|H| = pq^2$ is minimal nonabelian with $|H'| = q^2$; then we have $\mathrm{no}(H) = 2 = \mathrm{no}(G)$ so $\Delta(G) = \Delta(H) = \{p, q\}$ and $P \in \mathrm{Syl}_p(G)$ since a Sylow p-subgroup of G is not G-invariant (consider its intersection with H). By Frattini's lemma, $G = \mathrm{N}_G(P)H = \mathrm{N}_G(P)PQ = \mathrm{N}_G(P) \cdot Q$ so $P < \mathrm{N}_G(P)$. Since $\mathrm{N}_G(P)$ is not normal in G and $|\mathrm{N}_G(P)| \notin \{p, q\} = \Delta(G)$, we get a contradiction.

(ii2) Let $|H| = p^a q$ and $p \mid |G : H|$. If $P < P_0 \in \mathrm{Syl}_p(G)$, then P_0 is not normal in G and $|P_0 : P| = p$ (otherwise, every subgroup lying between P and P_0 is not G-invariant so $\mathrm{no}(G) > 2$); then $\Delta(G) = \{|P|, |P_0|\} = \{|P|, p|P|\}$. Next, $\mathrm{N}_G(P)$ is not normal in G since $\mathrm{N}_G(P) \cap H = P$. It follows that $\mathrm{N}_G(P) = P_0$ is of order $p|P| = p^{a+1}$. On the other hand, $G = \mathrm{N}_G(P)H = \mathrm{N}_G(P) \cdot Q = P_0 \cdot Q$ (Frattini's lemma). It follows that $|G| = p|H| = p^{a+1}q$.

If P_0 is cyclic, then $\mho_2(P) = \mathrm{Z}(G)$ and $G/\mathrm{Z}(G)$ is a Frobenius group of order $p^2 q$ so G is as in (c).

In what follows we assume that P_0 is noncyclic.

There is $L < P_0$ of order p such that $L \not\leq P$. Suppose that L is not normal in G. Then we have $p = |L| = |P|$ so $P_0 \cong \mathrm{E}_{p^2}$. In this case, $G = H \times \mathrm{C}_P(Q)$, where $|\mathrm{C}_P(Q)| = p$, contrary to the assumption. If $L \lhd G$, then $G = H \times L$ as above. Then $\Delta(G) = \{|P|, p|P|\}$ is as in (a).

Now assume that $\Omega_1(P_0) \leq P$. In this case, P_0 is generalized quaternion since it is noncyclic by assumption. Then $P_0 \cong \mathrm{Q}_8$ (if $|P_0| > 8$, then $\mathrm{no}(G) > 2$). Such G has a unique cyclic subgroup $\mathrm{C}_G(Q)$ of index 2 so it is as in (e) (indeed, $G/\mathrm{C}_G(Q) > \{1\}$ is cyclic of order dividing $q - 1$). We have $\Delta(G) = \{4, 8\}$.

(ii3) Next assume that $P \in \mathrm{Syl}_p(G)$, i.e., (ii2) does not hold. Then

$$G = \mathrm{N}_G(P)H = \mathrm{N}_G(P)PQ = \mathrm{N}_G(P) \cdot Q,$$

$\mathrm{N}_G(P)$ is not normal in G and $P < \mathrm{N_G(P)}$. In this case, $|\mathrm{N}_G(P) : P| = q$. It follows

that $Q_0 \cong \mathrm{E}_{q^2}$, where $Q_0 \in \mathrm{Syl}_q(G)$, and $\Delta(G) = \{|P|, |P|q\}$. Since $q \notin \Delta(G)$, every $Q_1 < Q_0$ is G-invariant. If $Q_1 \neq Q$, then $G = H \times Q_1$ so $Q_1 \leq \mathrm{Z}(G)$. It follows that $Q_0 \leq \mathrm{Z}(G)$ since Q_0 has $q + 1 > 2$ subgroups of order q, and then G is nilpotent, a final contradiction. □

Corollary 96.9 (O. Schmidt [S2]). *If G is a nonnilpotent group with* $\mathrm{nc}(G) = 2$*, then one of the following holds:*

(i) $G \cong \mathrm{A}_4$*, the alternating group of degree* 4*.*

(ii) $G = P \cdot Q$*, where* $P \in \mathrm{Syl}_p(G)$ *and* $G' = Q \in \mathrm{Syl}_q(G)$ *are cyclic satisfying* $\mho_1(P) = \mathrm{Z}(G)$*, and* $G/\mathrm{Z}(G)$ *is a Frobenius group of order* pq^2*.*

(iii) $G = H \times C$*, where H is a minimal nonabelian subgroup of order* $p^a q$ *with* $|H'| = q$ *and* $|C| = r$ *is a prime different from* p *and* q*.*

(iv) $G = P \cdot Q$ *(semidirect product with kernel Q), where* $|Q| = q$*, P is cyclic,* $|G : \mathrm{C}_G(Q)| = p^2$ *and* $G/\mathrm{Z}(G)$ *is a Frobenius group of order* $p^2 q$*.*

Proof. As $1 \leq \mathrm{no}(G) \leq \mathrm{nc}(G) = 2$, G is one of the groups from Theorem 96.4, the Supplement to Theorem 96.4 and Theorem 96.8. Since the nonnilpotent groups G with $\mathrm{no}(G) = 1$ satisfy $\mathrm{nc}(G) = 1$ as well, by the Supplement to Theorem 96.4, we need only consider the groups from Theorem 96.8. As in the proof of Theorem 96.8, let $H = PQ \leq G$ be an $\mathrm{S}(p, q)$-subgroup, $P \in \mathrm{Syl}_p(H)$ and $Q = H' \in \mathrm{Syl}_q(H)$.

(a) Let $G = H \times C$ be as in Theorem 96.8(a2), $|C| = r \neq q$. If also $r \neq p$, then $\mathrm{nc}(G) = 2$. Now let $r = p$. Then $P_0 = P \times C \in \mathrm{Syl}_p(G)$ is not G-invariant. Let $\mathrm{Syl}_p(G) = \{P_0, P_1, \ldots, P_q\}$. For $i = 1, \ldots, q$, let $P_i = C \times S_i$, where $S_i \neq P_i \cap H$, and set $H_i = S_i \cdot Q$, $S_0 = P$. The subgroups $S_0, \ldots, S_p$ are not normal in G. The pairwise distinct (by construction) subgroups $H = H_0, H_1, \ldots, H_q$, being direct factors of G, are G-invariant. Since $S_i^G = H_i$ for all i, we get $\mathrm{nc}(G) \geq q + 1 > 2$, a contradiction. Thus $r \neq p$ so G is as in (iii).

(b) Let $G = PQ$ be minimal nonabelian of order pq^2 as in Theorem 96.8(b). Since the $q + 1$ subgroups of order q must be conjugate under P, we get $p = q + 1$ so $q = 2$, $p = 3$ and therefore $G \cong \mathrm{A}_4$ is as in (i).

(c) The group of Theorem 96.8(c) satisfies the hypothesis, and G is as in (iv).

(d) Let the group $G = P \cdot Q$ be as in Theorem 96.8(d). Then, provided $Q \cong \mathrm{E}_{q^2}$, G does not satisfy the hypothesis. Indeed, if $Q_1, \ldots, Q_{q+1}$ are all the subgroups of order q in Q, then, for $i \neq j$, we have

$$PQ_i \neq (PQ_i)_G = \mho_1(P)Q_i \neq (PQ_j)_G = \mho_1(P)Q_j \neq PQ_j$$

so that the subgroups $P, PQ_1, \ldots, PQ_{q+1}$ are not G-invariant and not conjugate to each other, i.e., $\mathrm{nc}(G) \geq q + 2 > 2$, a contradiction. If Q is cyclic of order q^2, then G satisfies the hypothesis, and G is as in (ii).

(e) The group from Theorem 96.8(e) does not satisfy the hypothesis. Indeed, if M_1 and M_2 are distinct nonnilpotent maximal subgroups of G and $P_i < M_i \cap P$ of order 4,

$i = 1, 2$, then $P_1^G = M_1 \neq M_2 = P_2^G$ so P, P_1, P_2 are neither normal nor conjugate in pairs so $\mathrm{nc}(G) > 2$. □

Problem 1. Classify the p-groups G which satisfy $\mathrm{no}(G) = 2$ (the p-groups G satisfying $\mathrm{no}(G) = 1$ are classified in §112).

Problem 2. Classify the p-groups G, $p > 2$, satisfying $\mathrm{nc}(G) = p$.

Problem 3. Classify the p-groups G with exactly two conjugate classes of nonnormal cyclic subgroups.

§97

p-groups in which some subgroups are generated by elements of order p

The 2-groups all of whose nonmetacyclic subgroups are generated by involutions are classified in §84. Corollary 97.4 contains a stronger version of the main theorem from §84 for $p > 2$.

Definition. A p-group G is said to be an L_n*-group* if $\Omega_1(G)$ is of order p^n and exponent p and $G/\Omega_1(G)$ is cyclic of order greater than p (see §§17, 18).

In what follows we consider L_n-groups only for $n = p$.

Exercise. Let G be an L_p-group of exponent p^e; then $e > 2$ and $|G| = p^{p+e-1}$. Prove that $\mathfrak{V}_1(G)$ is cyclic of order p^{e-1} and $G = \langle x \in G \mid o(x) = p^e \rangle$.

Solution. We have

$$p^e = \exp(G) \le \exp(\mathfrak{V}_1(G)) \exp(G/\mathfrak{V}_1(G)) = p \cdot \exp(\mathfrak{V}_1(G))$$

so $|\mathfrak{V}_1(G)| \ge \exp(\mathfrak{V}_1(G)) \ge p^{e-1}$. Therefore it suffices to show that $|\mathfrak{V}_1(G)| \le p^{e-1}$. If G is regular, then $|\mathfrak{V}_1(G)| = |G/\Omega_1(G)| = p^{e-1}$. In case that G is irregular, then, by Theorem 9.8(a), we have $|G/\mathfrak{V}_1(G)| \ge p^p$ so $|\mathfrak{V}_1(G)| \le p^{-p}|G| = p^{e-1}$, and we conclude that $|\mathfrak{V}_1(G)| = p^{p-1}$, as required. Next, $\exp(\Omega_{e-1}(G)) = p^{e-1}$ so

$$\langle x \in G \mid o(x) = p^e \rangle = \langle G - \Omega_{e-1}(G) \rangle = G.$$

The main result of this section is the following

Theorem 97.1 ([Ber40]). *Let a p-group G of exponent $p^e > p$ be neither absolutely regular nor of maximal class. Then G contains a subgroup H of order p^{p+e-1} such that $|\Omega_1(H)| = p^p$, $H/\Omega_1(H)$ is cyclic of order p^{e-1} and $\Omega_2(H)$ is regular (so if $e > 2$, then H is an L_p-group).*

Our proof of Theorem 97.1 is based on some consequences of Blackburn's theory of p-groups of maximal class (see §§9, 12, 13; proofs of some of them are reproduced below; see Lemmas 97.J(d), 97.5 and 97.6).

If a p-group G is either absolutely regular or of maximal class and order $> p^{p+1}$, then it has no subgroup H such as in conclusion of Theorem 97.1 (in the second case

this follows from the description of members of the set Γ_1 and some other subgroups given in Lemma 97.J(h)). Therefore absolutely regular p-groups and p-groups of maximal class are excluded from the hypothesis of Theorem 97.1.

Corollary 97.2. *Suppose that a p-group G of exponent greater than p is not absolutely regular. If all proper not absolutely regular subgroups of G are generated by elements of order p, then one and only one of the following holds:*

(a) $|G| = p^{p+1}$ *and* $|\Omega_1(G)| > p^{p-1}$ *so if G is regular, then* $|\Omega_1(G)| = p^p$.

(b) $|G| = p^{p+1}$, $\mathrm{cl}(G) = p$, $|\Omega_1(G)| = p^{p-1}$ *(in this case, all proper subgroups of G are absolutely regular).*

(c) *G has maximal class,* $|G| > p^{p+1}$ *and every irregular member of the set* Γ_1 *has two distinct subgroups of order* p^p *and exponent p.*

Corollary 97.3. *Let G be an irregular p-group, $p > 2$. Suppose that whenever $H < G$ is neither absolutely regular nor of maximal class, then $\Omega_1(H) = H$. Then G is of maximal class.*

Corollary 97.4. *Let $p > 2$ and suppose that M is a maximal metacyclic subgroup of a nonmetacyclic p-group G, where $|M| > p^2$. Suppose that whenever $M < N \leq G$ and $|N : M| = p$, then $\Omega_1(N) = N$. Then $p = 3$ and G is of maximal class.*

In particular, if $p > 2$ and a p-group G of exponent greater than p is nonmetacyclic and such that all proper nonmetacyclic subgroups of G are generated by elements of order p, then one and only one of the following assertions holds:

(a) G is regular of order p^4 and $|\Omega_1(G)| = p^3$.

(b) G is of maximal class and order 3^4.

(c) $p = 3$, G is of maximal class, $|G| > 3^4$ and every irregular member of the set Γ_1 has two distinct (nonabelian) subgroups of order 3^3 and exponent 3.

Note that if a p-group of maximal class, $p > 2$, has an elementary abelian subgroup of order p^p, then G is isomorphic to a Sylow p-subgroup of the symmetric group of degree p^2 (Exercise 9.13). Therefore a group of Corollary 97.4 has no abelian subgroups of order 3^3 and exponent 3 unless $|G| = 3^4$.

In Lemma 97.J we collect some known results which are used in what follows.

Lemma 97.J. *Let $G > \{1\}$ be a p-group, $p > 2$.*

(a) (Theorems 7.1 and 7.2) *If G is regular, then* $\exp(\Omega_1(G)) = p$ *and* $|\Omega_1(G)| = |G/\mathfrak{V}_1(G)|$. *Absolutely regular p-groups, groups of exponent p and p-groups of class $< p$ are regular.*

(b) (Exercise 9.1(b)) *If G is of maximal class and order p^m, then it has exactly one normal subgroup of order p^i for all $1 \leq i < m - 1$.*

(c) (Proposition 1.8) *If $H < G$ is of order p^2 and $|\mathrm{C}_G(H)| = p^2$, then G is of maximal class.*

(d) (Exercise 13.10(a)) *If $A < G$ and all subgroups of G of order $p|A|$ containing A are of maximal class (so that $|A| > p$), then G is also of maximal class.*

(e) (Theorem 12.12) *Suppose that $M < G$ is an irregular subgroup of maximal class and index p. If G is not of maximal class, then $G/\mathrm{K}_p(G)$ is of order p^{p+1} and exponent p and $\Gamma_1 = \{M = M_1, \ldots, M_{p^2}, T_1, \ldots, T_{p+1}\}$, where all M_i's are of maximal class and all T_j's are not of maximal class (T_i are also not absolutely regular since $|G/\mathfrak{V}_1(G)| \geq p^{p+1}$), $\eta(G) = \bigcap_{i=1}^{p+1} T_i = D$ has index p^2 in G and $G/\eta(G)$ is abelian of type (p, p) so $\bigcup_{i=1}^{p+1} T_i = G$.*[1]

(f) (Theorem 12.1(b)) *If G is neither absolutely regular nor of maximal class and $H \in \Gamma_1$ is absolutely regular, then $G = H\Omega_1(G)$, where $\Omega_1(G)$ is of order p^p and exponent p (in particular, $|\Omega_1(H)| = p^{p-1}$).*

(g) (Theorem 13.5) *If G is neither absolutely regular nor of maximal class, then the number$e_p(G)$ of subgroups of order p^p and exponent p in G is $\equiv 1 \pmod{p}$.*

(h) (Theorem 9.6) *If G is of maximal class and order $> p^{p+1}$, then*

$$\Gamma_1 = \{G_1, G_2, \ldots, G_{p+1}\},$$

where G_1 is absolutely regular with $|\Omega_1(G_1)| = p^{p-1}$ (G_1 is called the fundamental subgroup of G*), and the subgroups $G_2, \ldots, G_{p+1}$ are irregular of maximal class. All p-groups of maximal class and order p^{p+1} are irregular.*

A p-group G of maximal class and order $> p^{p+1}$ has no normal subgroup of order p^p and exponent p. Assume that this is false, and let $R \lhd G$ be of order p^p and exponent p. Then, by Lemma 97.J(b), $R \leq \Phi(G) < G_1$, a contradiction since the fundamental subgroup G_1 is absolutely regular.

If a p-group G satisfies $\exp(\Omega_1(G)) > p$, then it is irregular (Lemma 97.J(a)).

To facilitate the proof of Theorem 97.1, we prove the following three assertions which have been proved in previous sections of the book.

Lemma 97.5. *Suppose that $H < G$ is such that $N = \mathrm{N}_G(H)$ is of maximal class. Then the p-group G is also of maximal class.*

Proof. We use induction on $|G|$. One may assume that $N < G$; then H is not characteristic in N (otherwise, $N = G$). In this case, by Lemma 97.J(b), we have $|N : H| = p$ hence $|H| > p$. As $|\mathrm{Z}(N)| = p$ and $\mathrm{Z}(G) < N$, we get $\mathrm{Z}(G) = \mathrm{Z}(N)$ so $|\mathrm{Z}(G)| = p$ and $\mathrm{Z}(G) \leq \Phi(N) < H$. Set $\bar{G} = G/\mathrm{Z}(G)$. If $|\bar{H}| = p$, then $\mathrm{C}_{\bar{G}}(\bar{H}) = \bar{N}$ is of order p^2 so $\bar{G}$ is of maximal class (Lemma 97.J(c)). Now let $|\bar{H}| > p$; then $\bar{N}$ is of maximal class so $\bar{G}$ is also of maximal class by induction, and we are done since $|\mathrm{Z}(G)| = p$. □

Lemma 97.6. *Suppose that $A \in \Gamma_1$ is absolutely regular and $M < G$ is irregular of maximal class. Then G is of maximal class.*

[1] It follows from the last equality that $\exp(T_i) = \exp(G)$ for some $i \leq p + 1$.

Proof. Assume that G is not of maximal class. Then, by Lemma 97.J(d), one can take $H \leq G$ such that $M < H \leq G$, where $|H : M| = p$ and H is not of maximal class. In this case, by Lemma 97.J(e), $H/\mathrm{K}_p(H)$ is of order p^{p+1} and exponent p. It follows that H has no absolutely regular maximal subgroups. However, $A \cap H$ is an absolutely regular maximal subgroup of H, and this is a contradiction. □

Lemma 97.7. *All proper subgroups of an* L_p*-group* G *are regular; in particular, the subgroup* $\Omega_2(G)$ *is regular.*

Proof. It suffices to show that all maximal subgroups of an L_p-group G are regular. This is true for $p = 2$ since then G is either abelian or $\cong \mathrm{M}_{p^n}$ which is minimal nonabelian. In what follows we assume that $p > 2$. Take $M \in \Gamma_1$.

Suppose that $\Omega_1(G) \not\leq M$; then $\Omega_1(M) = M \cap \Omega_1(G)$ is of order p^{p-1} and exponent p. Since M is not of maximal class (indeed, $M/\Omega_1(M) \cong G/\Omega_1(G)$ is cyclic of order $> p$), it follows that M is absolutely regular so regular (Lemma 97.J(g,a)).

Now let $\Omega_1(G) < M$. Let $D < \Omega_1(G)$ be a G-invariant subgroup of index p^2. Set $C = \mathrm{C}_G(\Omega_1(G)/D)$; then $|G : C| \leq p$. Take in $C/\Omega_1(G)$ a subgroup $H/\Omega_1(G)$ which is maximal in $G/\Omega_1(G)$; then H/D is abelian so $\mathrm{cl}(H) < p$, and hence H is regular (Lemma 97.J(a)). Since $G/\Omega_1(G)$ has only one maximal subgroup, we get $H = M$. It is clear now that $\Omega_2(G)(< G)$ is regular. □

Remark. Suppose that $p > 2$ and G is an irregular L_p-group of exponent p^e. Assume that there is in G a normal cyclic subgroup C of order p^e. Set $D = C \cap \Omega_1(G)$; then $C\Omega_1(G) = G$ and $|D| = p$ by the product formula, and $G/D = (C/D) \times (\Omega_1(G)/D))$ so $\mathrm{d}(G) > 2$ (it is important that $p > 2$). By Lemma 97.7, all proper subgroups of G are regular. It follows that $\mathrm{d}(G) = 2$, contrary to what has just been proved. Thus all cyclic subgroups of order p^e are not normal in G.

Proof of Theorem 97.1. First consider the case $p = 2$. Note that absolutely regular 2-groups are cyclic. Since G is not of maximal class, there is in G a normal abelian subgroup R of type $(2, 2)$ (Lemma 97.J(g)). Put $C = \mathrm{C}_G(R)$; then $|G : C| \leq 2$ so $\exp(C) \geq 2^{e-1}$. Suppose that $\exp(C) = 2^e$; then there is in $C - R$ an element x of order 2^e. In this case, $A = \langle x, R\rangle$ is abelian of type $(2^e, 2)$ or $(2^e, 2, 2)$. In any case, A contains an abelian subgroup H of type $(2^e, 2)$, and H is the desired subgroup. Now let $\exp(C) = 2^{e-1}$. Take $y \in G - C$ of order 2^e. Suppose that $U = \mathrm{C}_G(y)$ is cyclic; then $\mathrm{C}_G(U) = U$ and $\mathrm{Z}(G)$ is cyclic. If $e = 2$, then G is of maximal class (Lemma 97.J(c)), contrary to the hypothesis. Thus $e > 2$. In this case, $U \cap R$ is of order 2 so $H = RU$ is an L_2-subgroup of exponent 2^e. If $\mathrm{C}_G(y)$ is noncyclic, then there is an involution $x \in \mathrm{C}_G(y) - \langle y\rangle$; in this case, $H = \langle x, y\rangle = \langle x\rangle \times \langle y\rangle$ is abelian of type $(2^e, 2)$ so H is the desired subgroup.

In what follows we assume that $p > 2$. We use induction on $|G|$. Take an element $x \in G$ of order p^e. Let $x \in L < G$, where L is either absolutely regular or irregular of maximal class such that if $L < M \leq G$, then M is neither absolutely regular nor of maximal class (L exists by hypothesis and Lemma 97.J(d)). Let $L < F \leq G$ and

$|F : L| = p$; then F is neither absolutely regular nor of maximal class by the choice of L. Therefore if $F < G$, then F contains the desired subgroup H. Next assume that $F = G$; then $|G : L| = p$.

(i) Let L be absolutely regular. Then, by Lemma 97.J(f), we have $G = L\Omega_1(G)$, where $\Omega_1(G)(< G)$ is of order p^p and exponent p. Set $H = \langle x, \Omega_1(G)\rangle$, where $x \in L$ has order p^e; then $\Omega_1(H) = \Omega_1(G)$ is of order p^p and $|H| = p^{p+e-1}$ by the product formula. If $e > 2$, then H is an L_p-group so $\Omega_2(H)$ is regular by Lemma 97.7. It remains to show that if $e = 2$, then H is regular. This is true provided that $H = G$ since, by hypothesis, G of order p^{p+1} is not of maximal class, so $\mathrm{cl}(G) < p$ (Lemma 97.J(a)). Now let $H < G$ and assume, by way of contradiction, that H is irregular. Then H is of maximal class since $|H| = p^{p+1}$ (Lemma 97.J(a) again) and, by assumption, L is absolutely regular of index p in G. It follows from Lemma 97.6 that G is of maximal class, contrary to the hypothesis. Thus H is the desired subgroup.

(ii) Now let L be irregular of maximal class. If $F > L$ is as in the paragraph preceding (i), then, by Lemma 97.J(e),

$$\Gamma_1(F) = \{L = L_1, L_2, \ldots, L_{p^2}, T_1, \ldots, T_{p+1}\},$$

where $L_1, \ldots, L_{p^2}$ are of maximal class and $T_1, \ldots, T_{p+1}$ are neither absolutely regular nor of maximal class and $G = \bigcup_{i=1}^{p+1} T_i$. It follows that one of the T_i's, say T_1, has exponent p^e. Therefore, by induction, there is $H \leq T_1$ of exponent p^e such that $\Omega_1(H)$ is of order p^p and exponent p, $H/\Omega_1(H)$ is cyclic of order p^{e-1} and $\Omega_2(H)$ is regular. □

Lemma 97.8. *Suppose that A is a proper absolutely regular subgroup of a p-group G, $\exp(A) > p$ and whenever $A < B \leq G$ and $|B : A| = p$, then $\Omega_1(B) = B$. Then G is of maximal class.*

Proof. By Lemma 97.J(a), B is irregular so G is also irregular. Assume that G is not of maximal class. Let $|G : A| = p$; then $\Omega_1(G) = G$ by hypothesis. However, by Lemma 97.J(f), $G = A\Omega_1(G)$, where $|\Omega_1(G)| = p^p < |G| = |\Omega_1(G)|$, a contradiction. Now let $|G : A| > p$. If $A < B < G$, where $|B : A| = p$, then, by what has just been proved, B is of maximal class so G is also of maximal class by Lemma 97.J(d). □

Proof of Corollary 97.2. Suppose that G is regular and set $L = \Omega_1(G)$; then $|L| \geq p^p$ since G is not absolutely regular. However, G (of exponent $> p$) has a maximal subgroup of exponent $> p$ so it is absolutely regular, and this implies $|L| = p^p$. By Lemma 97.J(a), $|G : L| = p$ (otherwise, if $L < M < G$, then $\Omega_1(M) = L < M$, contrary to the hypothesis) so G is as in (a).

Next we assume that G is irregular. Since, by hypothesis, G has no regular subgroup H of order p^{p+1} and exponent p^2 such that $\Omega_1(H) < H$ is of order p^p, it follows that G is of maximal class (Theorem 97.1). If all maximal subgroups of G are absolutely regular, then G is as in (b) by Lemma 97.J(h). Obviously, every group of maximal class and order p^{p+1} satisfies the hypothesis. Now let $|G| > p^{p+1}$. If $M \in \Gamma_1$

is irregular, then $\Omega_1(M) = M$ by hypothesis. If $L = \Omega_1(\Phi(M))$, then L is of order p^{p-1} and exponent p (Lemma 97.J(h,a,b)). Take an element $x \in M - L$ of order p and set $U_1 = \langle x, L\rangle$. Pick an element $y \in M - U_1$ of order p and set $U_2 = \langle y, L\rangle$. Then U_1 and U_2 are distinct of order p^p and exponent p (Lemma 97.J(a)), and the proof is complete. □

Proof of Corollary 97.3. Assume that G is not of maximal class. Then there is in G a subgroup H such as in Theorem 97.1. Since H is neither absolutely regular nor of maximal class and $\Omega_1(H) \neq H$, we get a contradiction. □

Proof of Corollary 97.4. Let M and N be as in the statement of the corollary. Then M is absolutely regular since $p > 2$ so, by Lemma 97.J(f), N is of maximal class. By Lemma 97.J(d), G is also of maximal class. Since $p^{p-1} = |\Omega_1(M)| \leq p^2$ and $p > 2$, we get $p = 3$. □

Here we offer another proof of Theorem 97.1 in the case $\exp(G) = p^e > p^2$. We have to prove that G contains an L_p-subgroup of order p^{p+e-1}. To this end, we use induction on $|G|$. By Lemma 97.J(g), there is $M \lhd G$ of order p^p and exponent p. Take a cyclic $X < G$ of order p^e and set $F = MX$; then F of exponent $p^e > p^2$ is neither absolutely regular nor of maximal class. Therefore if $F < G$, the result follows by induction. Now let $F = G$. Suppose that $X \cap M > \{1\}$; then $|G| = p^{p+e-1}$. We claim that G is an L_p-group. It suffices to show that $\Omega_1(G) = M$. Assume that this is false. Since G/M is cyclic, we conclude that $|\Omega_1(G)| \leq p^{p+1}$. Assume that $|\Omega_1(G)| = p^{p+1}$. Then $X \cap \Omega_1(G)$ is cyclic of order p^2 hence $\Omega_1(G)$ is irregular and we conclude that it is of maximal class (Lemma 97.J(a)). Since the group G is not of maximal class, the number $e_p(G)$ of subgroups of order p^p and exponent p in G is $\equiv 1 \pmod p$ (Lemma 97.J(g)), and all these subgroups lie in $\Omega_1(G)$. As $e_p(G) > 1$ and $\mathrm{d}(\Omega_1(G)) = 2$, it follows that all maximal subgroups of $\Omega_1(G)$ have exponent p so $\exp(\Omega_1(G)) = p$ and $\Omega_1(G)$ is regular (Lemma 97.J(a)), a contradiction. Thus, in the case under consideration, G is an L_p-group. Now let $X \cap M = \{1\}$. Let $R < M$ be a G-invariant subgroup of index p. Set $H = RX$. Let us show that H is an L_p-group. Indeed, H is not absolutely regular since $\Omega_1(X)R$ is of order p^p and exponent p (Lemma 97.J(a)). Next, H/R is cyclic of order $p^e > p^2$ so H is not of maximal class. If $K/R < H/R$ is of order p, then $\Omega_1(H) \leq K \leq \Omega_1(H)$ so $\Omega_1(H) = \Omega_1(X)R = K$ is of order p^p and exponent p whence H is an L_p-subgroup. By Lemma 97.7, $\Omega_2(H)$ is regular.

Proposition 97.9. *Let H be a normal absolutely regular subgroup of a p-group G, $|H| > p^{p-1}$ and $\Omega_1(G) \not\leq H$.*

(a) *If for every $z \in G - H$ of order p the subgroup $V = \langle z, H\rangle$ is of maximal class, then G is also of maximal class.*

(b) *If for every $z \in G - H$ of order p we have $\Omega_1(\langle z, H\rangle) = \langle z, H\rangle$, then G is of maximal class.*

Proof. By hypothesis, $\exp(H) > p$. It follows from Lemma 97.J(a) and Theorem 9.5 that G is irregular. Assume, by way of contradiction, that G is not of maximal class.

Let $H \leq H_0 < G$, where H_0 is absolutely regular such that $|H_0|$ is as large as possible. By Lemma 97.J(d), $H_0 < B \leq G$, where $|B : H_0| = p$ and B is not of maximal class. Then, by Lemma 97.J(f), we have $B = H_0\Omega_1(B)$, where $\Omega_1(B)$ is of order p^p and exponent p so there exists an element $x \in \Omega_1(B) - H_0$ of order p. Set $U = \langle H, x\rangle$; then, by hypothesis, U is of maximal class and order $> p^p$ so irregular. We have $H_0, U < B$, H_0 is absolutely regular of index p in B and U is irregular of maximal class. Therefore, by Lemma 97.6, B is of maximal class, contrary to its choice. The above argument also proves (b). □

It is possible to change the condition $\Omega_1(G) \not\leq H$ in Proposition 97.9 to the following one: G is not absolutely regular. Indeed, assume that $\Omega_1(G) < H$. Then, by Lemma 97.J(f), G must be of maximal class.

Problems

Below G is a p-group.

Problem 1. Classify the p-groups all of whose proper nonabelian subgroups that are nonmetacyclic are generated by elements of order p.

Problem 2. Study the p-groups G containing a proper abelian subgroup M of exponent $> p$ such that whenever $M < N \leq G$ and $|N : M| = p$, then $\Omega_1(N) = N$ ($\Omega_2^*(N) = N$).

Problem 3. Let A be a subgroup of index $> p^k$ in a p-group G. Suppose that all subgroups of G containing A as a subgroup of index p^k, are of maximal class. Is it true that G also of maximal class? (Compare this with Lemma 97.J(d).)

Problem 4. Study the 2-groups G containing a metacyclic subgroup M and such that whenever $M < N \leq G$ and $|N : M| = 2$, then $\mathrm{d}(N) = 2$.

Problem 5. Study the p-groups G containing a minimal nonabelian subgroup M such that whenever $M < N \leq G$ and $|N : M| = p$, then $\Omega_1(N) = N$.

§98

Nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic to $\mathrm{M}_{2^{n+1}}$, $n \geq 3$ fixed

Here we classify completely the title groups. This classification for an arbitrary $n \geq 3$ (fixed) is quite involved and shows that our technique with minimal nonabelian subgroups is efficient.

Theorem 98.1. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to $\mathrm{M}_{2^{n+1}}$, $n \geq 3$ fixed. Then $E = \Omega_1(G)$ is elementary abelian. Let A be a maximal normal abelian subgroup of G containing E. Then $A = \mathrm{C}_G(E)$, all elements in $G - A$ are of order 2^n, G/A is elementary abelian of order ≤ 4, and if $x \in G - A$, then $|E : \mathrm{C}_E(x)| = 2$, $A_0 = \mathrm{C}_A(x) = \mathrm{C}_E(x)\langle x^2\rangle$, A/A_0 is cyclic, $\langle A, x\rangle'$ is cyclic of order $|A/A_0|$, $\langle A, x\rangle' \cap A_0 = \Omega_1(\langle x\rangle)$, x inverts A/A_0 and $\mathfrak{V}_{n-2}(A)$. We have two possibilities:*

(a) $\exp(A) = 2^m \geq 2^n$ *in which case* $|G : A| = 2$ *and A is of type* $(2^m, 2^{n-2}, 2, \ldots, 2)$.

(b) $\exp(A) \leq 2^{n-1}$ *in which case A is of type* $(2^{n-1}, 2^r, 2, \ldots, 2)$ *with* $1 \leq r \leq n-2$ *and either* $|G : A| = 2$ *or* $|G : A| = 4$, *where in the last case* $G/\Omega_{n-2}(A) \cong \mathrm{Q}_8$.

Conversely, if G is a 2-group of type (a) *or* (b), *then each minimal nonabelian subgroup of G is isomorphic to $\mathrm{M}_{2^{n+1}}$, $n \geq 3$ fixed.*

Proof. Let G be a title group with $n \geq 3$ fixed. Since G has no dihedral subgroups, $E = \Omega_1(G)$ is elementary abelian. Set $A = \mathrm{C}_G(E)$ so that A is normal in G. If A is nonabelian, then consider a minimal nonabelian subgroup $X \cong \mathrm{M}_{2^{n+1}}$ in A. But then all three involutions in X are central in X, which contradicts the structure of $\mathrm{M}_{2^{n+1}}$. Hence A is abelian and so $A = \mathrm{C}_G(E)$ is a unique maximal abelian subgroup of G containing E.

Let x be any element in $G - A$ so that $o(x) \geq 4$ and set $\langle z\rangle = E \cap \langle x\rangle$, where z is an involution. Set $T = E\langle x\rangle$ and $E_0 = \mathrm{C}_E(x)$ so that $E > E_0$ and $T_0 = \mathrm{C}_T(x) = E_0\langle x\rangle$ is abelian. Let $T_1 \leq T$ be such that $T_1 > T_0$ and $|T_1 : T_0| = 2$. Set $E_1 = T_1 \cap E$ so that $T_1 = E_1\langle x\rangle$, $|E_1 : E_0| = 2$ and let e be an involution in $E_1 - E_0$. Then we have $1 \neq [e, x] \in T_0 \cap E = E_0$ and so $[e, x]$ is an involution commuting with e and x and therefore $\langle e, x\rangle' = \langle [e, x]\rangle$ which implies that $\langle e, x\rangle$ is minimal nonabelian (Lemma 65.2(a)) and so $\langle e, x\rangle \cong \mathrm{M}_{2^{n+1}}$. In particular, $\langle [e, x]\rangle = \Omega_1(\Phi(\langle e, x\rangle)) = \langle z\rangle$,

$e^x = ez$ and $\langle e\rangle$ normalizes $\langle x\rangle$ which gives $o(x) = 2^n$. We have proved that all elements in $G - A$ are of order 2^n and so G/A is elementary abelian. In particular, $x^2 \in A$ and so x induces an involutory automorphism on E. Hence x centralizes E/E_0 and so T_0 is normal in T with $T/T_0 \cong E/E_0$. Suppose that $|E/E_0| > 2$ and let $f \in E - E_1$. Then considering $T_2 = \langle f\rangle T_0$, we get in the same way as above that $\langle f, x\rangle \cong \mathrm{M}_{2^{n+1}}$ and so $f^x = fz$. But then $ef \notin E_0$ and $(ef)^x = (ez)(fz) = ef$, a contradiction. We have proved that $|E : E_0| = 2$ and $[E, x] = \langle z\rangle = \Omega_1(\langle x\rangle)$.

Let $t \in E - E_0$ so that $t^x = tz$ and $\langle t, x\rangle \cong \mathrm{M}_{2^{n+1}}$. Let s be an arbitrary element in A. We may set $s^x = s^{-1}w$ for some $w \in A$. Note that $o(x) = 2^n$, $o(sx) = 2^n$ and $t^{sx} = t^x = tz$ so that $[t, sx] = z$ with $z \in \mathrm{Z}(A\langle x\rangle)$ and so $\langle t, sx\rangle \cong \mathrm{M}_{2^{n+1}}$. In particular, $\langle sx\rangle > \langle z\rangle$ and so $(sx)^{2^{n-1}} = (x)^{2^{n-1}} = z$. We compute (noting that $x^{-2} \in A$ and $(sx)^2 \in A$)

$$w = ss^x = s(x^{-1}sx) = sx^{-2}xsx = x^{-2}(sx)(sx) = x^{-2}(sx)^2.$$

Therefore $w^{2^{n-2}} = x^{-2^{n-1}}(sx)^{2^{n-1}} = zz = 1$ and so $s^x = s^{-1}w$ implies that x inverts $A/\Omega_{n-2}(A)$. Since

$$(s^{2^{n-2}})^x = (s^x)^{2^{n-2}} = (s^{-1}w)^{2^{n-2}} = s^{-2^{n-2}} = (s^{2^{n-2}})^{-1},$$

we see that x also inverts each element in $\mathfrak{V}_{n-2}(A)$.

We shall determine the structure of $A_0 = \mathrm{C}_A(x)$, where $A_0 \geq E_0\langle x^2\rangle$. Suppose that there is an element v of order 4 in A_0 such that $v^2 = z' \neq z$. Taking an involution $t \in E - E_0$, we get $(vt)^2 = z'$ and $[vt, x] = [v, x]^t[t, x] = [t, x] = z$ and so $\langle vt, x\rangle$ is minimal nonabelian. But $\Phi(\langle vt, x\rangle) \geq \langle z, z'\rangle \cong E_4$, which contradicts the structure of $\mathrm{M}_{2^{n+1}}$. Hence A_0 is of type $(2^{s_0}, 2, \ldots, 2)$ with $s_0 \geq n - 1$ and $\Omega_1(A_0) = E_0$. Suppose that A_0 contains an element y of order 2^n. Then $\mathfrak{V}_{n-2}(\langle y\rangle) \cong \mathrm{C}_4$ is inverted by x, a contradiction. Hence $s_0 = n - 1$ and so $A_0 = E_0\langle x^2\rangle$. Also, $A_1 = EA_0$ is of type $(2^{n-1}, 2, \ldots, 2)$ with $\mathfrak{V}_{n-2}(A_1) = \langle z\rangle$. For each $l \in A_1 - A_0$, $l^2 \in \langle x^2\rangle$, $[l, x] = z$ and so $\langle l, x\rangle \cong \mathrm{M}_{2^{n+1}}$.

For each $y \in Ax$ $(x \in G - A)$, $\mathrm{C}_A(y) = A_0$ and so $y^2 \in A_0$. This implies that x inverts A/A_0. Let A^*/A_0 be a subgroup of order 2 in A/A_0 and let a^* be an element in $A^* - A_0$. We have $(a^*)^x = a^*s$ with $1 \neq s \in A_0$ since x inverts A/A_0. Then we get $a^* = (a^*)^{x^2} = (a^*s)^x = a^*s^2$ and so $s^2 = 1$ and s is an involution in $E_0 = \Omega_1(A_0)$. The involution $s = [a^*, x]$ commutes with a^* and x and so $\langle a^*, x\rangle$ is minimal nonabelian. Hence $\langle a^*, x\rangle \cong \mathrm{M}_{2^{n+1}}$ with $\Phi(\langle a^*, x\rangle) = \langle x^2\rangle$ and so $[a^*, x] = s = z$. If $\langle a^*, x^2\rangle$ is cyclic, then we obtain that $o(a^*) = 2^n$ and x inverts $\mathfrak{V}_{n-2}(\langle a^*\rangle) \cong \mathrm{C}_4$ with $\mathfrak{V}_{n-2}(\langle a^*\rangle) \leq A_0$, a contradiction. Hence $\langle a^*, x^2\rangle$ is noncyclic and so $i = a^*y$ is an involution for a suitable $y \in \langle x^2\rangle$, where $i \in E - E_0$. Thus $E \leq A^*$ and so $A^* = E\langle x^2\rangle = A_1$. We have proved that $E\langle x^2\rangle/A_0$ is a unique subgroup of order 2 in A/A_0 and so A/A_0 is cyclic. The mapping $a \to a^{-1}a^x$ $(a \in A)$ is a homomorphism from A onto $\langle A, x\rangle'$ with the kernel $A_0 = \mathrm{Z}(\langle A, x\rangle)$. Thus $A/A_0 \cong \langle A, x\rangle'$. Since x inverts the cyclic group A/A_0, we have $|A : (\langle A, x\rangle' A_0)| = 2$ and therefore $\langle A, x\rangle' \cap A_0 = \langle z\rangle$ noting that $[A_1, x] = \langle z\rangle$.

(i) Suppose that A possesses an element a of order 2^n. Then each element $x \in G-A$ inverts $\mho_{n-2}(\langle a\rangle) = \langle v\rangle \cong C_4$ which implies that $|G : A| = 2$, $v \notin A_0 = C_A(x)$ and $v^2 \in E_0$. Since $A_1 = E\langle x^2\rangle$ is of type $(2^{n-1}, 2, \dots, 2)$, we have $v^2 = z$ and $v \in A_1 - A_0$. This implies that $|A/A_0| \geq 2^{n-1}$. Let y be an element in the set $A - A_0$ such that $\langle y\rangle$ covers A/A_0 and so $o(y) \geq 2^{n-1}$. Suppose that $o(y) = 2^{n-1}$ in which case $|A/A_0| = 2^{n-1}$, A splits over A_0 and $y^{2^{n-2}} = e \in E - E_0$. But then x inverts $\mho_{n-2}(\langle y\rangle) = \langle e\rangle$ and so x centralizes e, contrary to $C_E(x) = E_0$. It follows that $o(y) = 2^m \geq 2^n$. By the above, we get $\langle y\rangle \cap A_0 = \langle z\rangle$. Since $\langle y\rangle$ covers A/A_0 and $\langle x^2\rangle$ covers A_0/E_0, we get $A = E\langle y\rangle\langle x^2\rangle$, where $\langle y\rangle \cap \langle x^2\rangle = \langle z\rangle$. Let $y_0 \in \langle y\rangle$ be of order 2^{n-1}. Then we obtain $o(y_0x^2) = 2^{n-2}$, $\Omega_1(\langle y_0x^2\rangle)^\sharp \in E - E_0$ and $\langle y, x^2\rangle = \langle y\rangle \times \langle y_0x^2\rangle$ so that A is of type $(2^m, 2^{n-2}, 2, \dots, 2)$. We have obtained the groups of type (a) of our theorem.

(ii) Suppose that $\exp(A) = 2^{n-1}$. In that case, $\langle x^2\rangle$ is a cyclic subgroup in A of the maximal possible order. Let C be a complement of $\langle x^2\rangle$ in A so that $A = C \times \langle x^2\rangle$. Set $C_0 = A_0 \cap C$, $C_1 = A_1 \cap C$ so that C_1 is elementary abelian since $A_1/\langle x^2\rangle$ is elementary abelian. Hence we have $A_1 = C_1 \times \langle x^2\rangle$, $A_0 = C_0 \times \langle x^2\rangle$, $|C_1 : C_0| = 2$, $E = C_1 \times \langle z\rangle$ and $E_0 = C_0 \times \langle z\rangle$. We know that $A/A_0 \cong C/C_0$ is cyclic of order 2^r, $r \geq 1$. Let $c \in C$ be such that $\langle c\rangle$ covers C/C_0. Then $c^{2^{r-1}} = e$ is an involution in the set $C_1 - C_0$ so that $o(c) = 2^r$, $r \leq n-1$. Suppose that $r = n-1$. Since x inverts $\mho_{n-2}(\langle c\rangle) = \langle e\rangle$, we infer that x centralizes $e \notin E_0$, a contradiction. We have proved that $r \leq n-2$ and so A is of type $(2^{n-1}, 2^r, 2, \dots, 2)$, where $1 \leq r \leq n-2$. It follows that $\Omega_{n-2}(A) = \langle c, E, x^4\rangle$ is of index 2 in A, $\Omega_{n-2}(A)$ is normal in G and all elements in $A - \Omega_{n-2}(A)$ are of order 2^{n-1}.

Assume, in addition, that G/A is elementary abelian of order ≥ 4. Let $B/\Omega_{n-2}(A)$ be a subgroup of order 2 in $G/\Omega_{n-2}(A)$ distinct from $A/\Omega_{n-2}(A)$. But then each element $d \in B - \Omega_{n-2}(A)$ is of order 2^n, but $d^2 \in \Omega_{n-2}(A)$ is of order $\leq 2^{n-2}$, a contradiction. Hence $A/\Omega_{n-2}(A)$ is a unique subgroup of order 2 in $G/\Omega_{n-2}(A)$. Since $G/\Omega_{n-2}(A)$ cannot be cyclic (noting that G/A is elementary abelian of order ≥ 4), it follows that $G/\Omega_{n-2}(A)$ is generalized quaternion. But then $d(G/\Omega_{n-2}(A)) = 2$ and so $|G/A| = 4$ and $G/\Omega_{n-2}(A) \cong Q_8$. We have obtained the groups of type (b) of our theorem.

It remains to show that all obtained groups G of type (a) or (b) have the property that each minimal nonabelian subgroup M of G is isomorphic to $M_{2^{n+1}}$, $n \geq 3$ fixed. First suppose that $|M : (M \cap A)| = 2$ and let $x \in M - A$. Then $M \cap A \not\leq A_0 = C_A(x)$. Since A/A_0 is cyclic, it follows that $(M \cap A) - A_0$ contains an element $l \in A_1 - A_0$, where $A_1 = E\langle x^2\rangle$. But then we know that $\langle l, x\rangle \cong M_{2^{n+1}}$ and so $\langle l, x\rangle = M$. Now suppose that $|M : (M \cap A)| > 2$ in which case $|G/A| = 4$ and $G/\Omega_{n-2}(A) \cong Q_8$. In this case, M covers Q/A. But for any $m \in M - A$ we obtain that $o(m^2) = 2^{n-1}$ and so $m^2 \in A - \Omega_{n-2}(A)$. Thus the subgroup M covers also $G/\Omega_{n-2}(A)$ and so $M/(M \cap \Omega_{n-2}(A)) \cong Q_8$. Hence M' covers $(M \cap A)/(M \cap \Omega_{n-2}(A))$. But we have $|M'| = 2$ which gives a contradiction since all elements in the set $A - \Omega_{n-2}(A)$ are of order $2^{n-1} \geq 4$. Our theorem is proved. □

§99

2-groups with sectional rank at most 4

Here we give some results of K. Harada from [Har], where in case of 2-groups of sectional rank at most 4 we simplify some of his proofs. Recall that the sectional rank $\mathrm{r}(G)$ of a p-group G is $\mathrm{r}(G) = \max\{\mathrm{d}(H) \mid H \leq G\}$. The most impressive result is Theorem 99.9 stating that a 2-group which possesses a self-centralizing abelian subgroup of order 8 is of sectional rank at most 4. For related results see §51, where the 2-groups containing a self-centralizing subgroup isomorphic to E_8 are studied.

Lemma 99.1. *Suppose that $G = A \cdot B$ is a 2-group, where $A \cong \mathrm{E}_8$, $A \trianglelefteq G$, $B \cong \mathrm{E}_4$, $A \cap B = \{1\}$ and $\mathrm{C}_G(A) = A$. Then one of the following holds:*

(i) $\mathrm{C}_A(B) = [A, B] \cong \mathrm{C}_2$ *and* $G \cong \mathrm{Q}_8 * \mathrm{Q}_8$.

(ii) $\mathrm{C}_A(B) = [A, B] \cong \mathrm{E}_4$ *and* $G \cong \mathrm{E}_4 \wr \mathrm{C}_2$.

Proof. We know that $\mathrm{Aut}(A) \cong \mathrm{GL}(3, 2)$ has exactly two conjugacy classes of four-subgroups. Therefore there exist at most two possible structures for $A \cdot B$. Indeed, $\mathrm{Q}_8 * \mathrm{Q}_8$ (the extraspecial group of order 2^5 and "type +") and $\mathrm{E}_4 \wr \mathrm{C}_2$ are those two possibilities. In the first case, $\mathrm{C}_A(B) = [A, B] \cong \mathrm{C}_2$ and in the second case, $\mathrm{C}_A(B) = [A, B] \cong \mathrm{E}_4$. □

Lemma 99.2. *Let G be a 2-group with an elementary abelian subgroup A of order 16 and index 2. If $|\mathrm{Z}(G)| = 4$, then $G \cong \mathrm{E}_4 \wr \mathrm{C}_2$. In particular, each involution in $\mathrm{Z}(G)$ has exactly four square roots in $G - A$ so G contains exactly six cyclic subgroups of order 4 (it follows that G has exactly 19 involutions).*

Proof. Let g be an element of order 4 in $G - A$. Then $\mathrm{C}_A(g) = Z \cong \mathrm{E}_4$ and $g^2 \in Z$ which implies $Z = \mathrm{Z}(G)$, $\Phi(G) \leq Z$ and therefore $G' \leq Z$ and so $\langle Z, g\rangle \trianglelefteq G$. Hence all four conjugates of g in G lie in $\{gZ\}$ and so $G' = \Phi(G) = \mathrm{Z}(G)$ and G is special. Let $g' \in G - A$ be such that $(g')^2 = g^2$. Then $g' = ga$ for some $a \in A$ and $g^2 = (g')^2 = (ga)^2 = gaga = g^2 a^g a$ which gives $a^g = a$ and so $a \in Z$ and $g' \in \{gZ\}$. Hence $g^2 \in Z$ has exactly four square roots and they are all conjugate to g in G. If i is an involution in $G - A$, then we see (as above) that $\{iZ\}$ is the set of all involutions in $G - A$ and they form a single conjugate class of involutions in $G - A$. It follows that $G - A$ must contain exactly four square roots of each of the three involutions in Z. But this gives exactly 12 elements of order 4 in $G - A$ and so the remaining four elements in $G - A$ must be involutions forming a single conjugate

class. The structure of G is uniquely determined and so $G \cong \mathrm{E}_4 \wr \mathrm{C}_2$. Indeed, let t be an involution in $G - A$ and let X be a complement of Z in A. Then $X \cap X^t \trianglelefteq G$ so that $X \cap X^t = \{1\}$. □

Lemma 99.3. *Let G be a 2-group containing a subgroup $R \cong \mathrm{Q}_8 * \mathrm{Q}_8$ of order 2^5. If $\mathrm{C}_G(R) \leq R$, then $\mathrm{r}(G) \leq 4$.*

Proof. Set $R = Q_1 * Q_2$, where Q_1 and Q_2 are the only two quaternion subgroups of R and $Q_1 \cap Q_2 = \mathrm{Z}(R) = \langle z \rangle$. Let U be a normal four-subgroup of G and assume that $U \not\leq R$. Then $U \cap R = \langle z \rangle$, $|(RU) : R| = 2$ so that $[R, U] \leq \langle z \rangle$ and so if $u \in U - \langle z \rangle$, then $Q_1^u = Q_2$ is not possible. If u induces an outer automorphism on Q_i ($i \in \{1, 2\}$), then $[Q_i, u] \cong \mathrm{C}_4$, a contradiction. Thus u induces on both Q_1 and Q_2 inner automorphisms and so u induces an inner automorphism on R, contrary to $\mathrm{C}_G(R) \leq R$. Hence $U \leq R$.

If G does not have a normal elementary abelian subgroup of order 8, then $\mathrm{r}(G) \leq 4$ (Theorem 50.3). Hence we may assume that G possesses a normal elementary abelian subgroup X of order 8. Assume that $X \not\leq R$. By the previous paragraph, $X \cap R = X_1 \cong \mathrm{E}_4$, X_1 is a normal four-subgroup in G and $z \in X_1$. We have $|(RX) : R| = 2$ and so $[R, X] \leq X_1$ which shows that X cannot interchange Q_1 and Q_2. But $[R, X]$ is elementary abelian and so X induces on both Q_1 and Q_2 inner automorphisms and so X induces an inner automorphism group on R, a contradiction. We have proved that $X \leq R$ with $z \in X$.

Set $V = \mathrm{N}_G(R)$. Since $\mathrm{Q}_8 * \mathrm{Q}_{16}$ and $\mathrm{Q}_8 * \mathrm{SD}_{16}$ do not possess an elementary abelian normal subgroup of order 8, no element of $V - R$ induces an inner automorphism on Q_1 or on Q_2. Hence any element of $V - R$ must either interchange Q_1 and Q_2 or induce an outer automorphism on both Q_1 and Q_2. Note that a Sylow 2-subgroup of the outer automorphism group of $\mathrm{Q}_8 * \mathrm{Q}_8$ is isomorphic to D_8 and so we get $|V/R| \leq 4$ since $X \leq R$.

Suppose that $G > V$. Set $\bar{G} = G/\langle z \rangle$ where $\mathrm{Z}(R) = \langle z \rangle = \mathrm{Z}(G)$. Then $\bar{V}$ contains a normal elementary abelian subgroup $\bar{T}$ of order 16 which is distinct from $\bar{R}$, where $T = R^y$ with an element $y \in G - V$ which normalizes V. By the action of elements of $\bar{V} - \bar{R}$ on $\bar{R}$, we have $\mathrm{C}_{\bar{R}}(\bar{t}) \cong \mathrm{E}_4$ for $\bar{t} \in \bar{T} - \bar{R}$. Therefore $\bar{T} \cap \bar{R} \cong \mathrm{E}_4$ and $\bar{T}/(\bar{T} \cap \bar{R}) \cong \mathrm{E}_4$ so that $T \cap R = X \cong \mathrm{E}_8$ since X is normal in G and $T/X \cong \mathrm{E}_4$. Therefore there is $t \in T - R$ which induces an outer automorphism on both Q_1 and Q_2 and so $[t, R]$ is not elementary abelian. On the other hand, $[t, R] \leq X$ and so $[t, R]$ is elementary abelian, a contradiction. Hence we have $V = G$ and so $|G| \leq 2^7$.

By the action of the elements of $G - R$ on R, we see that $\mathrm{r}(G) \leq 4$. Indeed, let A/B be a section of G such that $A/B \cong \mathrm{E}_{2^5}$. If $B = \{1\}$, then $A \cong \mathrm{E}_{2^5}$ and so A covers $G/R \cong \mathrm{E}_4$ and so $|G| = 2^7$. Let u be an involution in $A - R$ which induces an involutory outer automorphism on both Q_1 and Q_2 in which case $\mathrm{C}_R(u) \cong \mathrm{E}_4$. On the other hand, $A \cap R \cong \mathrm{E}_8$, a contradiction. Hence $B \neq \{1\}$. If $|B| = 4$, then $A = G$ is of order 2^7 and $|\Phi(G)| \leq 4$. But in this case, there is $v \in G - R$ such that $Q_1^v = Q_2$ and so $|\Phi(G)| \geq 8$, a contradiction. Hence we may assume $|B| = 2$ and since G cannot

have an elementary abelian subgroup of order 2^6, we obtain that $\Phi(A) = B \cong \mathrm{C}_2$. If $G = A$ is of order 2^6, then $B = \mathrm{Z}(G) = \mathrm{Z}(R)$ and if $x \in A - R$, then x centralizes $R/\mathrm{Z}(R)$, a contradiction. Hence we have $|G| = 2^7$, A is a maximal subgroup of G with $\Phi(A) = B \leq \mathrm{Z}(G)$ and so $B = \mathrm{Z}(R) = \mathrm{Z}(G) = \langle z \rangle$. Since $A > R$ is obviously not possible (as before), we conclude that A covers $G/R \cong \mathrm{E}_4$. But then considering again $\bar{G} = G/\langle z \rangle$, we have for elements $\bar{t} \in \bar{A} - \bar{R}$ that $\bar{t}$ centralizes a subgroup of order 8 in $\bar{R}$, contrary to the established fact that $\mathrm{C}_{\bar{R}}(\bar{t}) \cong \mathrm{E}_4$. We have proved that $\mathrm{r}(G) \leq 4$. □

Lemma 99.4. *Suppose that G is a 2-group which contains a subgroup $R \cong \mathrm{E}_4 \wr \mathrm{C}_2$. If $\mathrm{C}_G(\mathrm{Z}(R)) = R$, then $\mathrm{r}(G) \leq 4$.*

Proof. Since $\mathrm{r}(R) \leq 4$, we may assume $R < G$. Let A be a unique elementary abelian subgroup of order 16 in R and let D be a subgroup of G containing R satisfying $|D : R| = 2$. Since A char R, we have $A \trianglelefteq D$. Also, $\mathrm{C}_G(A) \leq \mathrm{C}_G(\mathrm{Z}(R)) = R$ and so $\mathrm{C}_G(A) = A$. We study $V = \mathrm{N}_G(A)$ and set $\bar{V} = V/A$ so that $\bar{V}$ is a subgroup of $\mathrm{GL}(4, 2)$. Let a be an involution in $R - A$ and set $\bar{X} = \mathrm{C}_{\bar{V}}(\bar{a})$ so that $X \geq D$. Then X normalizes R and so $\mathrm{Z}(R) \trianglelefteq X$. But $\mathrm{C}_G(\mathrm{Z}(R)) = R$ and so $X = D$. Thus $|\mathrm{C}_{\bar{V}}(\bar{a})| = 4$ which implies (noting that $\exp(\bar{V}) \leq 4$) $\bar{V} \cong \mathrm{C}_4$, E_4 or D_8. Suppose that $\bar{V} \cong \mathrm{C}_4$ which gives $V = D$. But then A char D which gives $D = G$. If in this case H is a subgroup of G containing A, then either $H = R$ and $\mathrm{d}(H) \leq 4$ or $H = G$ and $\Phi(H) \geq \mathrm{Z}(R) = R'$ and so $\mathrm{d}(H) \leq 4$. If $H \not\geq A$, then $\mathrm{d}(H \cap A) \leq 3$ and $H/(H \cap A)$ is cyclic and so $\mathrm{d}(H) \leq 4$. It follows that we may assume that $\bar{V} \cong \mathrm{E}_4$ or $\bar{V} \cong \mathrm{D}_8$ and so in both cases $D/A \cong \mathrm{E}_4$ since $|\mathrm{C}_{\bar{V}}(\bar{a})| = 4$.

Since $R - A$ has exactly four involutions and they are all conjugate in R to a, we conclude that $T = \mathrm{C}_D(a)$ covers D/R and $T \cap R = \langle a \rangle \times \mathrm{Z}(R)$. If $x \in T - R$, then $T/\mathrm{Z}(R) \cong \mathrm{E}_4$ implies that $x^2 \in \mathrm{Z}(R)$ and so $\langle x, \mathrm{Z}(R) \rangle \cong \mathrm{D}_8$. Therefore there is an involution $t \in T - R$ so that $\langle a, t \rangle \cong \mathrm{E}_4$ and $\mathrm{C}_{\mathrm{Z}(R)}(t) = \langle z \rangle \cong \mathrm{C}_2$ which gives $\mathrm{Z}(D) = \langle z \rangle$ and D splits over A. Let $t' \in \{t, ta\}$ so that $\mathrm{C}_{\mathrm{Z}(R)}(t') = \langle z \rangle$ and suppose that $|\mathrm{C}_A(t')| = 8$ in which case $\mathrm{C}_A(t')$ covers $A/\mathrm{Z}(R)$. But then $\mathrm{C}_A(t')$ is $\langle a \rangle$-admissible and $\mathrm{C}_{\mathrm{C}_A(t')}(a) > \langle z \rangle$, a contradiction. It follows that $\mathrm{C}_A(t') \cong \mathrm{E}_4$ so that by Lemma 99.2 we have $\langle A, t' \rangle \cong \mathrm{E}_4 \wr \mathrm{C}_2$ and this together with $\mathrm{Z}(D) = \langle z \rangle$ gives A char D because A is a unique elementary abelian subgroup of order 16 in D.

Now set $Q = \langle a, t \rangle \langle \mathrm{C}_A(a), \mathrm{C}_A(t) \rangle$, where the four-group $\langle a, t \rangle$ acts faithfully on $E = \mathrm{C}_A(a)\mathrm{C}_A(t) \cong \mathrm{E}_8$ and $\mathrm{Z}(Q) = \langle z \rangle$. By Lemma 99.1, we have $Q \cong \mathrm{Q}_8 * \mathrm{Q}_8$. Suppose that $\mathrm{C}_G(Q) \not\leq Q$. Then, as A normalizes $\mathrm{C}_G(Q)$, we can find a subgroup B in $\mathrm{C}_G(Q)$ of order 4 with $B > \mathrm{Z}(Q) = \langle z \rangle$ and A normalizes B. It follows that $[A, B] \leq \mathrm{Z}(Q) = \mathrm{Z}(D) = \langle z \rangle$ and so B normalizes A. On the other hand, B also centralizes Q and so B normalizes $R = A\langle a \rangle$, where $a \in Q$. By the above, $\mathrm{C}_{\bar{V}}(\bar{a}) = \bar{D}$ and so $B \leq D$. This is a contradiction since $\mathrm{C}_D(Q) = \mathrm{Z}(Q) = \langle z \rangle$. We have proved that $\mathrm{C}_G(Q) \leq Q$. From Lemma 99.3 it follows that $\mathrm{r}(G) \leq 4$. □

Lemma 99.5. *Let $A \cong \mathrm{C}_8$ be self-centralizing in a 2-group G. Then $\mathrm{r}(G) \leq 4$.*

Proof. We set $A = \langle a\rangle$ and $a^4 = c$. Assume that G possesses a normal elementary abelian subgroup E of order 8 (because otherwise, Theorem 50.3 implies $\mathrm{r}(G) \le 4$). We set $E = \langle c, x, y\rangle$, where $E \cap \mathrm{Z}(G) = \langle c\rangle$ and $\mathrm{Z}(G) < A$. If $[a^2, E] = 1$, then a would centralize a four-subgroup of E, contrary to $\mathrm{C}_G(A) = A$. Hence $[a^2, E] \ne 1$ and so $\mathrm{Z}(G) = \langle c\rangle$. Since $\mathrm{GL}(3,2)$ has only one class of elements of order 4, we may assume that $x^a = xc$ and $y^a = yx$. This yields that $a^x = ac = a^5$ and $a^y = ax$ and the structure of AE is uniquely determined. In particular, $\langle A, x\rangle \cong \mathrm{M}_{16}$ has exactly two cyclic subgroups of order 8: $A = \langle a\rangle$ and $\langle ax\rangle = A^y$. We obtain $(ay)^2 = a^2x$ and AE has only two further cyclic subgroups of order 8: $\langle ay\rangle$ and $\langle ay \cdot x\rangle$, where $(ay)^y = ay \cdot x$. Also, $\Omega_2(AE) = E\langle a^2\rangle = \langle x\rangle \times \langle a^2y, y\rangle \cong \mathrm{C}_2 \times \mathrm{D}_8$. We know that $\mathrm{Aut}(A) \cong \mathrm{E}_4$ and we have $\mathrm{N}_{AE}(A) = \langle A, x\rangle$ since $y \notin \mathrm{N}_{AE}(A)$. Moreover, $\langle c, x\rangle$ is a unique normal four-subgroup of G which is contained in E. Since $\exp(AE) = 8$, we may assume that $|G : (AE)| \ge 4$ (because otherwise, obviously $\mathrm{r}(G) \le 4$).

Assume that $A_1 = \mathrm{N}_G(A) = \langle A, x\rangle$ is of order 16. Then $A_2 = \mathrm{N}_G(A_1) = AE$ and set $A_3 = \mathrm{N}_G(A_2)$ so that $|A_3 : A_2| = 2$. Since $\Omega_2(A_2)$ char A_2, we get $\Omega_2(A_2) = E\langle a^2\rangle \trianglelefteq A_3$. If $\mathrm{C}_{A_3}(E) = E$, then $A_3/E \cong \mathrm{D}_8$ and so $\mathrm{C}_4 \cong A_2/E$ char A_3/E which implies that an element in $G - A_3$ normalizing A_3 also normalizes E and A_2, contrary to $\mathrm{N}_G(A_2) = A_3$. Hence $\mathrm{C}_{A_3}(E)/E \cong \mathrm{C}_2$ so that $A_3/E \cong \mathrm{C}_4 \times \mathrm{C}_2$ is abelian. Set $E^* = \mathrm{C}_{A_3}(E)$ so that E^* is abelian of type $(2,2,2,2)$ or $(4,2,2)$. Since $\langle a\rangle$ normalizes E^* and $\mathrm{C}_E(a) = \langle c\rangle$, it follows that $\mho_1(E^*) \le \langle c\rangle$. Take an element $t \in E^* - E$. Then t centralizes E and $t^2 \in \langle c\rangle$. We have $\Phi(A_2) = \langle a^2, x\rangle$ and $A_3/E\langle a^2\rangle \cong \mathrm{E}_4$ and so $\Phi(A_3) = E\langle a^2\rangle$ since our element $t \in A_3 - A_2$ fuses $\langle a\rangle$ to $\langle ay\rangle$ or $\langle ayx\rangle$. There are three maximal subgroups of A_3 (containing $E\langle a^2\rangle$): A_2, $E\langle a^2, at\rangle$ and $E\langle a^2, t\rangle$. Since $(E\langle a^2\rangle)/E$ and $(E\langle t\rangle)/E$ are two distinct subgroups of order 2 in $(E\langle a^2, t\rangle)/E$, it follows that $(E\langle a^2, t\rangle)/E \cong \mathrm{E}_4$ which gives that $\exp(E\langle a^2, t\rangle) = 4$. As all elements in $A_2 - \langle E, a^2\rangle$ are of order 8, $A_2^l = \langle E, a^2, at\rangle$ for some $l \in G - A_3$ normalizing A_3. Hence all elements in $\langle E, a^2, at\rangle - \langle E, a^2\rangle$ are of order 8 and, in particular, the element at is of order 8. Since $A_3 = A_2E^*$, $A_2 \trianglelefteq A_3$, $E^* \trianglelefteq A_3$ and $A_2 \cap E^* = E$, we have $[a, t] \in A_2 \cap E^* = E$, where $t^2 \in \langle c\rangle = \mathrm{Z}(G)$ and E^* is abelian. We get $a^{-1}t^{-1}at = e \in E$ and so $a^t = ae$. On the other hand, $t \in A_3 - A_2$ and so $a^t \notin A_1 = \langle A, x\rangle$ which implies that $e = yc^ix^j$, $i, j = 0, 1$. We compute

$$(at)^2 = atat = at^2(t^{-1}at) = at^2 \cdot ayc^ix^j = a^2t^2yc^ix^j$$

and so

$$\begin{aligned}(at)^4 &= a^2t^2yc^ix^j \cdot a^2t^2yc^ix^j = a^2ya^2x^jyx^j\\ &= a^2ya^2y = a^2y \cdot ya^2c = a^4c = cc = 1,\end{aligned}$$

a contradiction.

It remains to treat the case where $A_1 = \mathrm{N}_G(A)$ is of order 32. We have $A_1/A \cong \mathrm{E}_4$ and $x \in A_1$. Choose an element $t \in A_1 - \langle A, x\rangle$ such that $a^t = a^{-1}$. Then we see that t satisfies $t^2 \in \mathrm{C}_G(A) = A$ and so $t^2 \in \langle c\rangle$. It follows that $\langle A, t\rangle \cong \mathrm{D}_{16}$ or Q_{16}

and $\langle A, tx\rangle \cong \mathrm{SD}_{16}$ with $(tx)^2 \in \langle c\rangle$. Also, A is a unique cyclic subgroup of order 8 in $\langle A, t\rangle$ and in $\langle A, tx\rangle$. Thus A_1 contains exactly two cyclic subgroups of order 8: $\langle a\rangle$ and $\langle ax\rangle = A^y$. This forces that $|A_2 : A_1| = 2$, where $A_2 = \mathrm{N}_G(A_1)$ and so $A_2 = A_1E$. Since t inverts A, $A_2/E \cong \mathrm{D}_8$. Moreover, $\mathrm{C}_{A_2}(E) = E$ as $[E, a^2] \neq 1$. By the structure of $\mathrm{GL}(3,2)$, A_2/E contains a four-subgroup D/E with $\mathrm{C}_E(D) \cong \mathrm{C}_2$ and so $\mathrm{C}_E(D) = \langle c\rangle$. We have $D = E\langle a^2, t\rangle$ or $D = E\langle a^2, at\rangle$, where $t^2 \in \langle c\rangle$ and $(at)^2 \in \langle c\rangle$. Since $[D, E] = \langle c\rangle$, we get also $\Phi(D) = \langle c\rangle$ and so $D \cong \mathrm{Q}_8 * \mathrm{Q}_8$. If $\mathrm{C}_G(D) \not\leq D$, then we can find a group V of $\mathrm{C}_G(D)$ of order 4 which contains $\langle c\rangle$ and is normalized by A. But then $[a, V] \leq \langle c\rangle$ and so V normalizes A and so $V \leq A_2$. On the other hand, $\mathrm{C}_{A_2}(D) \leq \mathrm{C}_{A_2}(E) = E$ and so $\mathrm{C}_{A_2}(D) = \langle c\rangle$, a contradiction. Hence $\mathrm{C}_G(D) \leq D$ and then Lemma 99.3 gives $\mathrm{r}(G) \leq 4$. □

Lemma 99.6. *Let G be a 2-group with a self-centralizing abelian subgroup A of order 8. If $\mathrm{r}(G) > 4$, then $|G| \geq 2^7$, G has a normal elementary abelian subgroup E of order 8 and A is not normal in G.*

Proof. Obviously, $|G| \geq 2^6$. Suppose that $|G| = 2^6$. Then G has subgroups $H > K$ with $K \trianglelefteq H$ and $H/K \cong \mathrm{E}_{2^5}$. If $K = \{1\}$, then H is a maximal subgroup of G and $H \cong \mathrm{E}_{2^5}$. But then $|\mathrm{Z}(G)| \geq 8$ and $\mathrm{Z}(G) \leq A$, a contradiction. Hence $H = G$ and $K \cong \mathrm{C}_2$ so that $\Phi(G) = G' = K$. Since G cannot be extraspecial, we have $\mathrm{Z}(G) > K$. But $\mathrm{Z}(G) < A$ and so $|\mathrm{Z}(G)| = 4$. Let $a \in A - \mathrm{Z}(G)$. On the other hand, $|G'| = 2$ implies that $|G : \mathrm{C}_G(a)| = 2$ so that $\mathrm{C}_G(A) > A$, a contradiction. We get $|G| \geq 2^7$ and Theorem 50.3 implies that G has a normal elementary abelian subgroup E of order 8. Also, an S_2-subgroup of $\mathrm{Aut}(A)$ is of order at most 8 which together with $\mathrm{C}_G(A) = A$ implies that A is not normal in G. □

Lemma 99.7. *Suppose that G is a 2-group which contains a self-centralizing subgroup $A \cong \mathrm{E}_8$. Then $\mathrm{r}(G) \leq 4$.*

Proof. Suppose that $\mathrm{r}(G) > 4$. Then Lemma 99.6 implies that $|G| \geq 2^7$, A is not normal in G, G possesses a normal elementary abelian subgroup E of order 8 and $A \neq E$.

(i) We show that $|A \cap E| = 4$ which implies $E \leq \mathrm{N}_G(A)$.

Since $\mathrm{Z}(G) < A$, $A \cap E$ is a nontrivial central subgroup of AE. Suppose that $A \cap E \cong \mathrm{C}_2$. Then A contains a four-subgroup A_1 with $A_1 \cap E = \{1\}$. If $x \in A_1$ is an involution which centralizes E, then taking $y \in A_1 - \langle x\rangle$ we get $|\mathrm{C}_E(y)| \geq 4$, contrary to $\mathrm{C}_G(A) = A$. This yields that A_1 acts faithfully on E. Since $\mathrm{C}_E(A_1) = A \cap E \cong \mathrm{C}_2$, Lemma 99.1(i) yields that $AE \cong \mathrm{Q}_8 * \mathrm{Q}_8$. But then $\mathrm{C}_G(AE) \leq \mathrm{C}_G(A) = A$ and so Lemma 99.3 gives a contradiction.

(ii) Let B be any elementary abelian subgroup of order 8 in $\mathrm{N}_G(A)$. Then we have $|A \cap B| \geq 4$.

As $\mathrm{C}_G(A) = A$, we have $A \cap B \neq \{1\}$ and assume that $A \cap B \cong \mathrm{C}_2$. Let $B_1 \cong \mathrm{E}_4$ be a complement of $A \cap B$ in B. Obviously, B_1 acts faithfully on A and so Lemma 99.1 implies $AB \cong \mathrm{Q}_8 * \mathrm{Q}_8$ or $AB \cong \mathrm{E}_4 \wr \mathrm{C}_2$. Clearly, $\mathrm{C}_G(AB) \leq \mathrm{C}_G(A) = A$ in both

cases. By Lemma 99.3, we get $AB \cong \mathrm{E}_4 \wr \mathrm{C}_2$ and let V be a unique elementary abelian subgroup of order 16 in AB so that $AB = AV$ with $V \cap A = Z = \mathrm{Z}(AB) \cong \mathrm{E}_4$. Assume that $\mathrm{C}_G(Z) > AB$ and let T be a subgroup of $\mathrm{C}_G(Z)$ containing AB with $|T : (AB)| = 2$. Then V is normal in T and if $a \in A - Z$, then $(AB) - V$ contains exactly four involutions and they are all conjugate to a in AB since $\mathrm{C}_{AB}(a) = A$. Hence $\mathrm{C}_G(a)$ covers $T/(AB)$, contrary to $\mathrm{C}_G(A) = A$. We have proved that $\mathrm{C}_G(Z) = AB$. But then Lemma 99.4 implies that $\mathrm{r}(G) \leq 4$, a contradiction.

(iii) $\mathrm{N}_G(A)/A$ is not isomorphic to D_8.

Suppose that $\mathrm{N}_G(A)/A \cong \mathrm{D}_8$. Since $G > \mathrm{N}_G(A)$, $\mathrm{N}_G(A)$ contains a conjugate $B = A^t \neq A$ of A, where $t \notin \mathrm{N}_G(A)$ and $(\mathrm{N}_G(A))^t = \mathrm{N}_G(A)$. Since $B \trianglelefteq \mathrm{N}_G(A)$ and $A \cap B \cong \mathrm{E}_4$, B maps into the center of $\mathrm{N}_G(A)/A$. Hence $AE = AB$ and note that $AE \cong \mathrm{C}_2 \times \mathrm{D}_8$ and so A and E are the only two elementary abelian subgroups of order 8 in AE. Then $B = A$ or $B = E$ and this is a contradiction in both cases.

(iv) $\bar{G} = G/E$ is isomorphic to D_{2^n}, $n \geq 3$, or to SD_{2^m}, $m \geq 4$.

We investigate the structure of $\bar{G} = G/E$. Obviously, $\mathrm{N}_G(AE)$ normalizes A since $E \trianglelefteq G$ and A and E are the only two elementary abelian subgroups of order 8 in AE. Hence $|\mathrm{N}_G(AE)/E| = 4$ which means that $|\mathrm{C}_{\bar{G}}(\bar{A})| = 4$. This fact together with $G > \mathrm{N}_G(AE)$ implies that $\bar{G} \cong \mathrm{D}_{2^n}$ or $\bar{G} \cong \mathrm{SD}_{2^m}$.

(v) Now we obtain a final contradiction.

Since $\mathrm{r}(G) > 4$, G contains subgroups G_0 and U with $G_0/U \cong \mathrm{E}_{32}$. If $E \not\leq G_0$, then $\mathrm{d}(E \cap G_0) \leq 2$ and (by (iv)) $\mathrm{d}(G_0/E \cap G_0) \leq 2$, a contradiction. Hence $E \leq G_0$. Since $\mathrm{d}(G_0/E) \leq 2$, we must have $E \cap U = \{1\}$. Hence $[E, G_0] \leq E \cap U = \{1\}$ and so $E \leq \mathrm{Z}(G_0)$. Since $|G_0/E| \geq 4$, G_0 contains the inverse image K of $\mathrm{Z}(G/E)$ in G. As $K \leq G_0 \leq \mathrm{C}_G(E)$, we have $K \cong \mathrm{E}_{16}$ or $K \cong \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$. The latter case does not occur as $\Phi(G_0) \cap E \leq U \cap E = \{1\}$. Thus $K \cong \mathrm{E}_{16}$. Let $a \in A - (A \cap E)$ so that $a \notin K$ and $\mathrm{C}_K(a) \cong \mathrm{E}_4$. Hence Lemma 99.2 implies that $\langle a, K\rangle \cong \mathrm{E}_4 \wr \mathrm{C}_2$. As $A = \langle a, \mathrm{C}_K(a)\rangle$ is normal in $\langle a, K\rangle$, we can find an elementary abelian subgroup B of K of order 8 with $|A \cap B| = 2$ and $B \leq \mathrm{N}_G(A)$. This contradicts (ii) and our lemma is proved. □

Lemma 99.8. *Let G be a 2-group with a self-centralizing subgroup $A \cong \mathrm{C}_4 \times \mathrm{C}_2$. Then* $\mathrm{r}(G) \leq 4$.

Proof. Suppose that $\mathrm{r}(G) > 4$. Then Lemma 99.6 implies that $|G| \geq 2^7$, A is not normal in G and G possesses a normal elementary abelian subgroup E of order 8.

We set $A = \langle a, b \mid a^4 = b^2 = 1, [a, b] = 1, a^2 = c\rangle$. It is well known that $\mathrm{Aut}(A) \cong \mathrm{D}_8$, $\mathrm{C}_A(\mathrm{Aut}(A)) = \langle c\rangle$ and if ζ is the unique central involution in $\mathrm{Aut}(A)$, then ζ inverts A.

(i) We have $|A \cap E| = 4$.

Suppose that $|A \cap E| \leq 2$. Then $A \cap E \cong \mathrm{C}_2$ and $A \cap E = \langle c\rangle$, $\langle bc\rangle$ or $\langle b\rangle$.

Suppose first that $A \cap E = \langle c\rangle$. As $A/\langle c\rangle \cong \mathrm{E}_4$, each element x in $A - \langle c\rangle$ induces an involutory automorphism on E with $|\mathrm{C}_E(x)| = 4$ and $\langle E, x\rangle' = [E, x] = \langle c\rangle$.

Indeed, if x centralizes E, then for an element $y \in A - \langle c, x\rangle$ we have $|\mathrm{C}_E(y)| \geq 4$, which contradicts $\mathrm{C}_G(A) = A$. If $\langle E, x\rangle' = \langle e\rangle$ with $e \in E - \langle c\rangle$, then $\langle e\rangle$ is normal in AE and A centralizes $\langle e\rangle$, a contradiction. Hence we get $(AE)' = [A, E] = \langle c\rangle$ and $(AE)/\langle c\rangle \cong \mathrm{E}_{16}$. Then we obtain that $\mathrm{Z}(AE) = (AE)' = \Phi(AE) = \langle c\rangle$ and so AE is extraspecial with an elementary abelian subgroup of order 8 which implies that $AE \cong \mathrm{Q}_8 * \mathrm{Q}_8$. As $\mathrm{C}_G(AE) \leq \mathrm{C}_G(A) = A \leq AE$, Lemma 99.3 yields that $\mathrm{r}(G) \leq 4$, a contradiction.

We next treat the case $A \cap E = \langle bc\rangle$ or $\langle b\rangle$. Without loss of generality we may assume that $A \cap E = \langle b\rangle$. We have $(AE)/E \cong \langle a\rangle \cong \mathrm{C}_4$. If $[c, E] = 1$, then a centralizes a four-subgroup in E, a contradiction. Therefore $\langle a\rangle$ acts faithfully on E and this forces $\mathrm{Z}(AE) = \mathrm{Z}(G) = \langle b\rangle$. Set $E = \langle b, x, y\rangle$. Without loss of generality we may set $x^a = xb$, $y^a = yx$ and so $a^x = ab$, $[c, x] = 1$, $a^y = ax$, and $x \in \mathrm{N}_G(A)$. Clearly $\langle b, x\rangle$ is a unique normal four-subgroup of G contained in E. Hence x maps into the center of $\mathrm{N}_G(A)/A$. Since x does not invert A, $\mathrm{N}_G(A)/A \cong \mathrm{C}_2$ or $\mathrm{N}_G(A)/A \cong \mathrm{E}_4$.

First suppose that $\mathrm{N}_G(A)/A \cong \mathrm{E}_4$, where $\mathrm{N}_{AE}(A) = \langle A, x\rangle$. Then $\mathrm{N}_G(A) - (AE)$ contains an element t which inverts A. We have $\mathrm{N}_G(A) = \langle A, x, t\rangle$ and $t^2 \in \langle b, c\rangle$ so that $\langle t, A\rangle/\langle b\rangle \cong \mathrm{D}_8$ or Q_8. Setting $F = \mathrm{N}_G(A)E$, we see that $F/E \cong \mathrm{D}_8$ or Q_8 and F/E is faithful on E, inasmuch as c maps onto the center of F/E and does not centralize E. In that case, $F/E \cong \mathrm{D}_8$ and so $\langle t, A\rangle/\langle b\rangle \cong \mathrm{D}_8$, $t^2 \in \langle b\rangle$ and $(ta)^2 \in \langle b\rangle$. By the structure of $\mathrm{GL}(3, 2)$, F/E must contain a four-subgroup F_1/E with $\mathrm{C}_E(F_1) \cong \mathrm{C}_2$. Interchanging t and ta if necessary, we may assume that $F_1 = \langle E, c, t\rangle$ with $\mathrm{Z}(F_1) = \langle b\rangle$. But then $[\langle t, c\rangle, E] = F_1' = \langle b\rangle$ and $F_1/\langle b\rangle \cong \mathrm{E}_{16}$ so that F_1 is extraspecial and $F_1 \cong \mathrm{Q}_8 * \mathrm{Q}_8$. Suppose that $\mathrm{C}_G(F_1) \not\leq F_1$. Since a normalizes $\mathrm{C}_G(F_1)$, we can find a subgroup V of order 4 in $\mathrm{C}_G(F_1)$ which contains $\langle b\rangle$ and is normalized by $\langle a\rangle$. But then $[a, V] \leq \langle b\rangle$ and so V normalizes A which implies that $V \leq F$. On the other hand, $\mathrm{C}_F(F_1) = \mathrm{Z}(F_1) = \langle b\rangle$. This contradiction forces $\mathrm{C}_G(F_1) \leq F_1$ and then Lemma 99.3 implies $\mathrm{r}(G) \leq 4$, a contradiction.

It remains to treat the case $A_1 = \mathrm{N}_G(A) = \langle A, x\rangle$, where A_1 is the nonmetacyclic minimal nonabelian group of order 16. Also, we set $A_2 = \mathrm{N}_G(A_1)$ and $A_3 = \mathrm{N}_G(A_2)$. As $\Phi(A_1) = \langle b, c\rangle$, A_1 has exactly three maximal subgroups: A, $A^y = \langle ax, b\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$ and $\langle c, b, x\rangle \cong \mathrm{E}_8$ and A_2 permutes A and A^y and so $A_2 = AE = \langle A, x, y\rangle$ is of order 2^5. Also, $A_3 > A_2$ since $|G| \geq 2^7$. On the other hand, as $\Phi(A_2) = \langle b, c, x\rangle$, A_2 has exactly three maximal subgroups: A_1, $\langle c, E\rangle \cong \mathrm{C}_2 \times \mathrm{D}_8$ and $\langle ay, b, c, x\rangle$, where A_1 cannot be conjugate to $\langle c, E\rangle$. Hence $|A_3 : A_2| = 2$, $|A_3| = 2^6$ and A_3 contains an element $t \in A_3 - A_2$ such that $A_1^t = \langle ay, b, c, x\rangle$, $(ay)^2 = a(yay) = a \cdot ax = cx$.

If $\mathrm{C}_{A_3}(E) = E$, then $A_3/E \cong D_8$ and $A_2/E \cong \mathrm{C}_4$ is characteristic in A_3/E. Therefore if $s \in G - A_3$ is such that $s^2 \in A_3$ and $A_3^s = A_3$, then s normalizes A_2, contrary to $A_3 = \mathrm{N}_G(A_2)$. Thus E satisfies $\mathrm{C}_{A_3}(E) > E$ and since A_2/E is faithful on E, we get $\mathrm{C}_{A_3}(E) = \langle E, t\rangle$, where $[E, t] = 1$, $t^2 \in E$ and $t \in A_3 - A_2$. We have $A_3 = A_2\langle E, t\rangle$, where A_2 and the abelian subgroup $\langle E, t\rangle$ (of order 16) are normal in

A_3 and $A_2 \cap \langle E, t\rangle = E$ so that $A_3/E \cong \mathrm{C}_4 \times \mathrm{C}_2$ and so

$$\Omega_1(A_3) \leq \langle E, c, t\rangle.$$

We shall show that $B = \langle b, c, x\rangle$ is a unique normal self-centralizing elementary abelian subgroup of order 8 in A_3. Since $B = \Phi(A_2)$, we see that B is normal in A_3. Since t normalizes A_2 but does not normalize A_1, we have $a^t \equiv ay \pmod{B}$, where $A_2/B \cong \mathrm{E}_4$ and so $A_3/B \cong \mathrm{D}_8$. The element y maps onto $\mathrm{Z}(A_3/B)$ and y does not centralize B and so $\mathrm{C}_{A_3}(B) = B$.

Suppose that $\langle E, t\rangle \cong \mathrm{E}_{16}$. Then the four-group $\langle y, t\rangle$ acts faithfully on B and $\langle y, t\rangle$ centralizes $\langle b, x\rangle$ so that $\mathrm{C}_{\langle E,t\rangle}(c) = \langle b, x\rangle \cong \mathrm{E}_4$ and so by Lemma 99.1, we obtain $\langle E, c, t\rangle \cong \mathrm{E}_4 \wr \mathrm{C}_2$. Since all involutions in $\langle E, c, t\rangle - \langle E, t\rangle$ are contained in B, it follows that in this case B is a unique normal self-centralizing elementary abelian subgroup of order 8 in A_3.

Now suppose that $\langle E, t\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$. Since a centralizes $\mho_1(\langle E, t\rangle) = \langle t^2\rangle$, we get $t^2 = b$. Suppose that c inverts an element $t_1 \in \langle E, t\rangle - E$ in which case $t_1^2 = b$ and $c^{t_1} = cb$. Hence t_1 normalizes $\langle b, c\rangle$ so t_1 normalizes $\mathrm{C}_{A_2}(\langle b, c\rangle) = \langle A, x\rangle = A_1$. As $t_1 \notin A_2 = \mathrm{N}_G(A_1)$, this is a contradiction. Thus all involutions in $\langle E, c, t\rangle - \langle E, t\rangle$ are contained in B and so B has the required property also in this case.

Now we get a final contradiction which will finally prove our statement (i). Let l be an element in $G - A_3$ such that $A_3^l = A_3$ and $l^2 \in A_3$. Since B is characteristic in A_3, B is normal in $\langle A_3, l\rangle$ and so $\langle A_3, l\rangle/B \cong \mathrm{D}_8 \times \mathrm{C}_2$. Set $F = \mathrm{C}_{\langle A_3,l\rangle}(B)$ so that $F/B \cong \mathrm{C}_2$ and F is normal $\langle A_3, l\rangle = A_3F$ with $A_3 \cap F = B$. Let $l' \in F - B$ so that $l' \notin A_3$, $l'^2 \in B$ and $[l', A_3] \leq A_3 \cap F = B$. Hence l' centralizes B and A_2/B and so l' normalizes A_2, contrary to $A_3 = \mathrm{N}_G(A_2)$.

(ii) We have $|\mathrm{N}_G(A)| \leq 2^5$.

By (i), $|A \cap E| = 4$ and so we may set $E = \langle b, c, x\rangle$, where $A \cap E = \langle b, c\rangle$.

Suppose that $|\mathrm{N}_G(A)| = 2^6$. Since $\mho_1(A) = \langle c\rangle$, we get $\langle c\rangle = \mathrm{Z}(\mathrm{N}_G(A)) = \mathrm{Z}(G)$. We have $E \leq \mathrm{N}_G(A)$ and $E \trianglelefteq G$ and so x maps into the center of $\mathrm{N}_G(A)/A \cong \mathrm{D}_8$. Thus x inverts A. In particular, $x^a = xc$. Let e be an element of $\mathrm{N}_G(A)$ such that $a^e = a$ and $b^e = bc$. Then $e^2 \in \mathrm{C}_G(A) = A$.

First suppose that $o(e) \leq 4$. Then $e^2 \in \langle b, c\rangle$ and so $\langle e, b, c\rangle \cong \mathrm{D}_8$. Thus we may assume that $o(e) = 2$. As $|\mathrm{C}_E(e)| = 4$, we may also assume that $[e, x] = 1$. We claim that $\langle A, e, x\rangle \cong \mathrm{Q}_8 * \mathrm{Q}_8$. Indeed, we have $\langle A, e, x\rangle' = \langle c\rangle$ and $\Phi(\langle A, e, x\rangle) = \langle c\rangle = \mathrm{Z}(\langle A, e, x\rangle)$ and so $\langle A, e, x\rangle$ is extraspecial of order 2^5 containing $E \cong \mathrm{E}_8$ and so $\langle A, e, x\rangle \cong \mathrm{Q}_8 * \mathrm{Q}_8$. Since $\langle A, e, x\rangle$ is self-centralizing in G, Lemma 99.3 yields that $\mathrm{r}(G) \leq 4$, a contradiction.

Now suppose that $o(e) = 8$ so that we may assume $e^2 = a$. There is an element $d \in \mathrm{N}_G(A)$ with $a^d = ab$ and $b^d = b$ and so $\Phi(\mathrm{N}_G(A)) \geq A$. On the other hand, we have $\mathrm{N}_G(A)/A \cong \mathrm{D}_8$ and so x maps into $\Phi(\mathrm{N}_G(A)/A)$ which implies that

$$\Phi(\mathrm{N}_G(A)) = \langle A, x\rangle = AE.$$

As x inverts A, $\langle A, x\rangle \cong \mathrm{C}_2 \times \mathrm{D}_8$ and so A is a unique abelian maximal subgroup of

$\langle A, x\rangle$ which is not elementary abelian. It follows that A is characteristic in $N_G(A)$ which forces $N_G(A) = G$, contrary to the fact that $|G| \geq 2^7$(Lemma 99.6).

(iii) Set $\bar{G} = G/E$. Then $|C_{\bar{G}}(\bar{a})| > 4$.

Suppose that $|C_{\bar{G}}(\bar{a})| \leq 4$, where $|\bar{G}| \geq 2^4$. This implies that $\bar{G} \cong D_{2^n}$ or that $\bar{G} \cong SD_{2^n}$, $n \geq 4$. It follows that $C_G(E) > E$ and so if K is the inverse image of $Z(\bar{G})$, then K is an abelian normal subgroup of order 16.

Since $r(G) > 4$, G contains subgroups $T > U$ with $U \trianglelefteq T$ and $T/U \cong E_{2^5}$. Clearly, $E \leq T$ because otherwise $d(T) \leq 4$. In this case, $d(T/E) \leq 2$ which implies $E \cap U = \{1\}$. Hence $[T, E] \leq E \cap U = \{1\}$ and so E is central in T. But $|T/E|$ is of order at least 4 and this implies that T also contains the inverse image K of $Z(\bar{G})$. Also, $\Phi(T) \leq U$ and $\Phi(K) \leq E$ and so $K \cong E_{16}$. Since $C_K(a) = \langle b, c\rangle$, we get (Lemma 99.2) $\langle a, K\rangle \cong E_4 \wr C_2$ with $Z(\langle a, K\rangle) = \langle b, c\rangle \cong E_4$.

By Lemma 99.4, $C_G(\langle b, c\rangle) > \langle a, K\rangle$ and let X be a subgroup of $C_G(\langle b, c\rangle)$ containing $\langle a, K\rangle$ as a subgroup of index 2. Note that (Lemma 99.2) $\langle a, K\rangle - K$ contains exactly four square roots of c and they form a single conjugate class in $\langle a, K\rangle$ which is also X-invariant (since X centralizes $\langle b, c\rangle$). This shows that $C_G(a)$ must cover $X/\langle a, K\rangle$, contrary to $C_G(A) = A$.

(iv) We are now in a position to get a final contradiction.

We set again $\bar{G} = G/E$. By (iii), the inverse image D of $C_{\bar{G}}(\bar{a})$ is of order $\geq 2^6$. Since D normalizes $\langle A, x\rangle = AE$ and (by (ii)) $|N_G(A)| \leq 2^5$, it follows that $\langle A, x\rangle \ncong C_2 \times D_8$ (because otherwise, A would be characteristic in AE). Therefore x does not invert A. Without loss of generality we may assume (replacing b with bc if necessary) $a^x = ab$ and so $\Phi(AE) = \langle b, c\rangle$. We have

$$(ax)^2 = a(xax) = a(ab) = a^2b = cb$$

and so $A = \langle a, b\rangle$ and $\langle ax, b\rangle$ are the only subgroups of AE which are isomorphic to $C_4 \times C_2$. This implies that $|D| = 2^6$, $|N_G(A)| = 2^5$, $N_G(A)/A \cong E_4$ and if $t \in D - N_G(A)$, then $A^t = \langle ax, b\rangle$ and $c^t = cb$ which gives $Z(G) = Z(D) = \langle b\rangle$.

Let d be an element in $N_G(A)$ which inverts A. Then $d \in N_G(A) - (AE)$ and since d^2 centralizes A, we have $d^2 \in A$ and so $d^2 \in \langle b, c\rangle$. Since $|G| \geq 2^7$ (Lemma 99.6), we obtain $C_G(E) > E$. Hence $\bar{a}$ (which does not centralize E) centralizes a subgroup E_0/E of order 2 in $C_G(E)/E$, where E_0 is normal in G. This in turn implies that $C_D(E) > E$. Since any element of $D - N_G(A)$ sends c onto cb, we have $C_D(E) \leq N_G(A)$. Thus $C_D(E) = \langle E, d\rangle$ or $C_D(E) = \langle E, ad\rangle$. Noting that both d and ad inverts A, we may assume without loss of generality that $C_D(E) = \langle E, d\rangle$.

Setting $K = \langle E, d\rangle$, we first assume that K satisfies $K \cong E_{16}$. As $C_K(a) = \langle b, c\rangle$, $\langle a, K\rangle \cong E_4 \wr C_2$ with $Z(\langle a, K\rangle) = \langle b, c\rangle$ (Lemma 99.2). If $C_G(Z(\langle a, K\rangle)) > \langle a, K\rangle$, then take a subgroup Y in $C_G(Z(\langle a, K\rangle))$ containing $\langle a, K\rangle$ with $|Y : \langle a, K\rangle| = 2$. Since $\langle a, K\rangle$ contains exactly four square roots of c and they are all conjugate to a in $\langle a, K\rangle$ (Lemma 99.2), we get that $C_G(a)$ covers $Y/\langle a, K\rangle$, contrary to $C_G(A) = A$. Hence we have $C_G(Z(\langle a, K\rangle)) = \langle a, K\rangle$ and then Lemma 99.4 gives that $r(G) \leq 4$, a contradiction.

It remains to treat the case $K \cong \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$. Since $\mho_1(K)$ is central in D, we get $d^2 = b$. We compute

$$(adx)^2 = (adx)(adx) = ax(dad)x = axd^2a^dx$$
$$= axba^{-1}x = ab(xa^{-1}x) = ab(ab)^{-1} = 1.$$

Setting $C = \langle b, c, adx\rangle$, we shall argue that C is a normal self-centralizing elementary abelian subgroup of order 8 in D. There are three nontrivial cosets in $\mathrm{N}_G(A)$ modulo E: aE, dE, $adxE$. All elements in aE are of order 4 (noting that $\Phi(\langle a, E\rangle) = \langle b, c\rangle$ and the three maximal subgroups of $\langle a, E\rangle$ are $A \cong \mathrm{C}_4 \times \mathrm{C}_2$, $\langle ax, b\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$, and E, where $(ax)^2 = cb$) and all elements in dE are of order 4 since $d^2 = b$ and d centralizes E. Finally, in the coset $adxE$ there are exactly four involutions forming the set $\{adx\langle b, c\rangle\}$ since $\mathrm{C}_E(adx) = \langle b, c\rangle$. Hence all involutions in $\mathrm{N}_G(A)$ are contained in E or C. As $E \trianglelefteq D$ and $\mathrm{N}_G(A) \trianglelefteq D$, we have $C \trianglelefteq D$. Since each $t \in D - \mathrm{N}_G(A)$ has the property $c^t = cb$, we get $\mathrm{C}_D(C) \leq \mathrm{N}_G(A) = \mathrm{C}_D(\langle b, c\rangle)$ and no one of d, x, dx centralizes adx, where dC, xC and dxC are three nontrivial cosets of C in $\mathrm{N}_G(A)$. Hence $\mathrm{C}_D(C) = C$, as required.

Suppose that D contains another such subgroup C_1, namely $C_1 \cong \mathrm{E}_8$, $C_1 \trianglelefteq D$, and $\mathrm{C}_D(C_1) = C_1$. Then $b \in C_1$ since $\langle b\rangle = \mathrm{Z}(D)$. Suppose that $C \cap C_1 = \langle b\rangle$. Let $C_1^* \cong \mathrm{E}_4$ be a complement of $\langle b\rangle$ in C_1 so that C_1^* acts faithfully on C and $\mathrm{C}_C(C_1^*) = \langle b\rangle = \mathrm{Z}(CC_1)$. By Lemma 99.1, $CC_1 \cong \mathrm{Q}_8 * \mathrm{Q}_8$. We have $a \notin CC_1$ since $a^2 = c$ and $\mho_1(CC_1) = \langle b\rangle$. Since $|D : (CC_1)| = 2$, we conclude that a normalizes CC_1 and $D = CC_1\langle a\rangle$. Suppose that $\mathrm{C}_G(CC_1) \not\leq CC_1$. Since $\langle a\rangle$ normalizes $\mathrm{C}_G(CC_1)$, there is an $\langle a\rangle$-invariant subgroup V of order 4 in $\mathrm{C}_G(CC_1)$ which contains $\langle b\rangle$. But then $[\langle a\rangle, V] \leq \langle b\rangle$ and so V normalizes $\langle a, b\rangle = A$ and therefore $V \leq D$, where $(CC_1) \cap V = \langle b\rangle$. In that case, V centralizes C, contrary to the fact that C is self-centralizing in D. Thus $\mathrm{C}_G(CC_1) \leq CC_1$ and so Lemma 99.3 implies $\mathrm{r}(G) \leq 4$, a contradiction. Hence we may assume that $|C \cap C_1| = 4$. Since $\langle b, c\rangle = C \cap E$ is a normal four-subgroup of D and $D/C \cong \mathrm{D}_8$, it follows that four involutions in $C - \langle b, c\rangle$ are conjugate in D and so $\langle b, c\rangle$ is a unique normal four-subgroup of D contained in C. This implies $C \cap C_1 = \langle b, c\rangle$. Consequently, $C_1 \leq \mathrm{C}_D(\langle b, c\rangle) = \mathrm{N}_G(A)$. Thus $C_1 = C$, contrary to $C_1 \neq C$. Hence C is the unique subgroup in D with the required property which implies that C is characteristic in D.

Let $F \leq G$ be a subgroup of G containing D so that $|F : D| = 2$. Then C is normal in F and $D/C \cong \mathrm{D}_8$. Let $H = \mathrm{C}_F(C)$ so that $H \trianglelefteq F$, $|H : C| = 2$ and H is abelian. We get $F = DH$ with $D \cap H = C$ and $[D, H] \leq D \cap H = C$. Let $h \in H - C$ so that $h^2 \in C$ and h centralizes C and D/C. We get $a^h = ay$ with $y \in C$. If $y \in \langle b, c\rangle$, then h normalizes $A = \langle a, b\rangle$, contrary to $\mathrm{N}_G(A) \leq D$. We get $y \notin \langle b, c\rangle$ and so $y = adx \cdot b^i c^j$ with $i, j = 0, 1$. Then

$$a^h = a \cdot adxb^i c^j = a^2 dxb^i c^j = cdxb^i c^j = dxb^i c^{j+1} \in K$$

and h centralizes $\langle b, c\rangle$. Thus $A^h \leq K$, where K is abelian of order 16. This is a final contradiction since $\mathrm{C}_G(A^h) = A^h$. Our lemma is proved. □

Now Lemmas 99.5, 99.7 and 99.8 give the following remarkable result.

Theorem 99.9 (K. Harada). *Let G be a 2-group with a self-centralizing abelian subgroup of order 8. Then each subgroup of G is generated by at most four elements, i.e., the sectional rank of G is at most 4.*

Theorem 99.10 (K. Harada). *Let G be a 2-group containing a subgroup $T = U \times W$, where $U \cong \mathrm{E}_4$ and $W \cong \mathrm{E}_4$, D_{2^n}, $n \geq 3$, or SD_{2^m}, $m \geq 4$. Suppose that for each involution $x \in U$, $\mathrm{C}_G(x) = T$. Then the sectional rank $\mathrm{r}(G)$ of G is 4.*

Proof. Since $\mathrm{r}(T) = 4$, we may assume that $G > T$. We have $\mathrm{Z}(T) = U \times \mathrm{Z}(W) \cong \mathrm{E}_8$ or E_{16}. Let $x \in \mathrm{N}_G(T) - T$ with $x^2 \in T$. If $U \cap U^x \neq \{1\}$, then x normalizes $U \cap U^x$ and so x centralizes an involution in $U \cap U^x$, a contradiction. Hence we have $U \cap U^x = \{1\}$ which implies $\mathrm{Z}(W) \cong \mathrm{E}_4$ and so $W \cong \mathrm{E}_4$ and $T \cong \mathrm{E}_{16}$. For any element $s \in \mathrm{N}_G(T) - T$ with $s^2 \in T$, $U \cap U^s = \{1\}$ and so $\langle s, T\rangle \cong \mathrm{E}_4 \wr \mathrm{C}_2$ (Lemma 99.2). In particular, $\langle s, T\rangle - T$ contains an involution. Let $k = |\mathrm{N}_G(T) : T|$ and $R = \mathrm{N}_G(T)$. Then any element $u \in U$ has exactly k conjugates in T by the action of R. This gives $2 \leq k \leq 8$.

Suppose that $k = 2$. Then $R \cong \mathrm{E}_4 \wr \mathrm{C}_2$. This forces $G = R = \mathrm{N}_G(T)$ as T is characteristic in R. Thus $\mathrm{r}(G) = 4$ by Lemma 99.4. Hence we may assume that $k > 2$.

Suppose next that $k = 8$. Since there cannot be two orbits of length 8 (under the action of R), all involutions in U are conjugate in R. Let a be an involution in $R - T$ which maps into the center of R/T. Since all involutions of $\langle a, T\rangle - T$ are conjugate in $\langle a, T\rangle$ (as $\langle a, T\rangle \cong \mathrm{E}_4 \wr \mathrm{C}_2$), we have $R = \mathrm{C}_R(a)T$. Hence $\mathrm{C}_T(a)$ is normal is R. Moreover, $U \cap \mathrm{C}_T(a) = \{1\}$. Let L be an R-invariant subgroup with $\mathrm{C}_T(a) < L < T$ and $|L : \mathrm{C}_T(a)| = 2$. Then $|L \cap U| = 2$ and so all involutions in U cannot be conjugate in R, a contradiction.

We have proved that $k = 4$. If $G = R = \mathrm{N}_G(T)$, then $|G| = 2^6$ and it is easy to see that in that case $\mathrm{r}(G) = 4$. Indeed, let $A/B \cong \mathrm{E}_{2^5}$ be a section of G. If $B = \{1\}$, then A is an elementary abelian subgroup of index 2 in G. But then $U \cap A \neq \{1\}$, contrary to $|\mathrm{C}_G(U \cap A)| = 2^4$. Hence we have $B \cong \mathrm{C}_2$ and $A = G$. But in this case, $G' = B \cong \mathrm{C}_2$ and so an involution in U cannot have $k = 4$ conjugates in $R = G$. Hence we have $\mathrm{r}(G) = 4$ in this case. It follows that we may assume that $G > R$. This implies that using an element $h \in G - \mathrm{N}_G(R)$ with $h^2 \in R$, we get another elementary abelian subgroup $T_1 = T^h$ of order 16. As $\mathrm{C}_G(u) = T$ for any involution in U, we have $T_1 \cap U = \{1\}$. Hence $R = T_1 T$ as $|R| = 2^6$ and $T_1 \cap T = \mathrm{Z}(R) \cong \mathrm{E}_4$. This in turn implies that R is a split extension of E_{16} by E_4. Then $U_1 = U^h$ is a complement of T in R and $\mathrm{C}_T(b) = T_1 \cap T$ for any involution b in U_1 and, in addition, $\langle b, T\rangle \cong \mathrm{E}_4 \wr \mathrm{C}_2$ which shows that all elements in $R - (T \cup T_1)$ are of order 4 and $R' = \Phi(R) = \mathrm{Z}(R) = T \cap T_1$. Hence R has exactly two elementary abelian subgroups T an T_1 of order 16. This forces that $|\mathrm{N}_G(R) : R| = 2$. Setting $P = \mathrm{N}_G(R)$, we shall argue that $P = G$. It suffices to show that T and T_1 are the only subgroups of P which are isomorphic to E_{16}. Indeed, let $t \in P - R$ so that $T^t = T_1$ and therefore

$\Omega_1(\mathrm{C}_R(t)) \leq T \cap T_1$. This implies that any elementary abelian subgroup of P which is not contained in R is of order at most 8. Thus $G = P$, as required.

It remains to be shown that $\mathrm{r}(G) \leq 4$. For this, it suffices to prove that G does not possess a normal elementary abelian subgroup of order 8. Suppose that this is false and let A be such a subgroup. If $A \leq R$, then $A \leq T$ or $A \leq T_1$. However, as $T^t = T_1$ ($t \in G - R$) and $A \not\leq T \cap T_1$, A cannot be t-invariant. Hence $A \not\leq R$ and $A \cap R$ is a normal four-subgroup of $G = P$ which gives $A \cap R = T \cap T_1$. Let $a \in A - R$. Then $T^a = T_1$ and so $G/T \cap T_1 \cong \mathrm{E}_4 \wr \mathrm{C}_2$ which shows that a does not map into the center of $G/(T \cap T_1)$. This contradicts the fact that $A/(T \cap T_1) \trianglelefteq G/(T \cap T_1)$. Our theorem is proved. □

It is interesting to notice that if a p-group G has a nonabelian subgroup B of order p^3 such that $\mathrm{C}_G(B) < B$, then G is of maximal class (Proposition 10.17(a)); then every subgroup of G is generated by p elements.

§100

2-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian

Suppose that G is a p-group all of whose maximal subgroups are metacyclic except one (which is nonmetacyclic). If $p > 2$ and $|G| > p^4$, then Y. Berkovich has shown (with a short and elegant proof) that G must be a so-called L_3-group, i.e., $\Omega_1(G)$ is of order p^3 and exponent p and $G/\Omega_1(G)$ is cyclic of order $\geq p^2$ (see Proposition A.40.12). However, if $p = 2$, then the problem of determination of such groups is much more difficult and this was done in §87. All these results will be used very heavily in this section.

Here we continue with this idea of classifying p-groups all of whose maximal subgroups, but one, have a certain strong property. In this section we determine up to isomorphism the 2-groups G all of whose maximal subgroups, but one, are abelian or minimal nonabelian. We begin with the case $\mathrm{d}(G) = 2$ (Theorems 100.1, 100.2 and 100.3). Actually, a detailed investigation of such groups has already begun in Lemma 76.5. Then we determine such groups satisfying $\mathrm{d}(G) > 2$ (Theorems 100.4, 100.5 and 100.6). All resulting groups will be presented in terms of generators and relations, but we shall also describe all important characteristic subgroups of these groups for two reasons. One reason is that only the knowledge of the subgroup structure of these groups will make our theorems useful for applications. Another reason is that with this knowledge we see that 2-groups appearing in distinct theorems are nonisomorphic.

Conversely, it is easy to check that all groups given in these theorems indeed possess exactly one maximal subgroup which is neither abelian nor minimal nonabelian.

The corresponding problem for $p > 2$ is open, but we think that this problem is within the reach of the present methods in finite p-group theory.

Theorem 100.1. *Let G be a two-generator 2-group with exactly one maximal subgroup H which is neither abelian nor minimal nonabelian. If G has an abelian maximal subgroup A, then $\Gamma_1 = \{A, M, H\}$ is the set of the maximal subgroups of G, where M is minimal nonabelian, A and M are both metacyclic,* $\mathrm{d}(H) = 3$ *and we have more precisely:*

$$G = \langle a, x \mid [a, x] = v,\ v^4 = 1,\ v^2 = z,\ v^x = v^{-1},$$
$$v^a = v^{-1},\ x^2 \in \langle z \rangle,\ a^{2^m} \in \langle z \rangle,\ m \geq 2 \rangle,$$

where

$$G' = \langle v \rangle \cong \mathrm{C}_4, \quad \mathrm{K}_3(G) = [G, G'] = \langle z \rangle \cong \mathrm{C}_2, \quad E = \langle v, x \rangle \cong \mathrm{D}_8 \text{ or } \mathrm{Q}_8,$$
$$E \trianglelefteq G, \quad G = E\langle a \rangle, \quad G/E \cong \mathrm{C}_{2^m}, \quad \Phi(G) = G'\langle a^2 \rangle \text{ is abelian},$$
$$H = E\langle a^2 \rangle, \quad \mathrm{Z}(G) = \langle a^2, z \rangle,$$

$A = \langle ax, v \rangle$ is an abelian maximal subgroup of G, $M = \langle v, a \rangle$ is metacyclic minimal nonabelian of order 2^{m+2} and $|G| = 2^{m+3}$, $m \geq 2$.

Proof. If G has more than one abelian maximal subgroup, then all three maximal subgroups of G are abelian, a contradiction. Hence A is a unique abelian maximal subgroup of G. It follows that $\Gamma_1 = \{A, M, H\}$, where M is minimal nonabelian. The subgroup $A \cap M = \Phi(G)$ is abelian, $\Phi(M) < \Phi(G)$ and $|\Phi(G) : \Phi(M)| = 2$. Also, $\Phi(M) = \mathrm{Z}(M) \leq \mathrm{Z}(G)$ so that for an element $m \in M - A$, $\mathrm{C}_{\Phi(G)}(m) = \mathrm{Z}(M)$. If $\mathrm{C}_A(m) > \mathrm{Z}(M)$, then $G = M * C$ with $C = \mathrm{C}_G(M)$ and $M \cap C = \mathrm{Z}(M)$, contrary to $\mathrm{d}(G) = 2$. It follows that $\mathrm{C}_A(m) = \mathrm{Z}(M) = \mathrm{Z}(G)$ and so $|G : \mathrm{Z}(G)| = 8$. From $|G| = 2|\mathrm{Z}(G)||G'|$ (Lemma 1.1) follows that $|G'| = 4$. For each $x \in G - A$, $\mathrm{C}_A(x) = \mathrm{Z}(M)$ and so $x^2 \in \mathrm{Z}(M) = \mathrm{Z}(G)$ which implies that x inverts $A/\mathrm{Z}(M)$. If $A/\mathrm{Z}(M) \cong \mathrm{E}_4$, then $\Phi(G) = \mho_1(G) \leq \mathrm{Z}(M)$, a contradiction. Hence we obtain that $A/\mathrm{Z}(M) \cong \mathrm{C}_4$ and since $m \in M - A$ inverts $A/\mathrm{Z}(M)$, we have $G/\mathrm{Z}(M) \cong \mathrm{D}_8$. Let $a \in A - \Phi(G)$. Then $\langle a \rangle$ covers $A/\mathrm{Z}(M)$ and so $v = [a, m] \in \Phi(G) - \mathrm{Z}(M)$. We get

$$1 = [a, m^2] = [a, m][a, m]^m = vv^m \quad \text{and so} \quad v^m = v^{-1}$$

which implies that $o(v) = 4$. Indeed, if $o(v) = 2$, then $[v, m] = 1$, which contradicts the fact that $\mathrm{C}_{\Phi(G)}(m) = \mathrm{Z}(M)$. We get $G' = \langle v \rangle \cong \mathrm{C}_4$ and $[v, m] = v^2$ implies that $M' = \langle v^2 \rangle$. Since v^2 is a square in M, it follows that M is metacyclic (Lemma 65.1). In particular, $|\Omega_1(\Phi(G))| \leq 4$ which together with $A/\mathrm{Z}(M) \cong \mathrm{C}_4$ gives $\Omega_1(A) \leq \Phi(G)$ and so A is also metacyclic. Here $H = \Phi(G)\langle am \rangle$ is our third maximal subgroup of G. From $\mathrm{C}_{\Phi(G)}(am) = \mathrm{Z}(M)$ follows that H is nonabelian with $\mathrm{Z}(H) = \mathrm{Z}(M)$ and so Lemma 1.1 yields $|H'| = 2$. If $\mathrm{d}(H) = 2$, then Lemma 65.2 gives that H would be minimal nonabelian, a contradiction. Hence $\mathrm{d}(H) \geq 3$ and so H is the only maximal subgroup of G which is nonmetacyclic. In fact, $\mathrm{d}(H) = 3$ since $\Phi(G)$ is metacyclic. We are in a position to use Theorem 87.12 for $n = 2$ since $G' \cong \mathrm{C}_4$. This gives the generators and relations described in our theorem, where we have used the notation from Theorem 87.12. □

Theorem 100.2. *Let G be a 2-group with $\mathrm{d}(G) = 2$ which has exactly one maximal subgroup H which is neither abelian nor minimal nonabelian. If the other two maximal subgroups H_1 and H_2 are minimal nonabelian with $H_1' = H_2'$, then one of the following holds:*

(a) *G is one of the groups given in Theorem 87.10.*

(b) *G is the group of order 2^5 given in Theorem 87.14.*

(c) $G = \langle h, x \mid h^{2^n} = 1, n \geq 2, [h,x] = s, s^2 = 1, [s,h] = z, z^2 = [z,h] = [z,x] = [x,s] = 1, x^2 \in \langle z \rangle \rangle$, *where*

$$|G| = 2^{n+3}, \quad G' = \langle z, s \rangle \cong \mathrm{E}_4, \quad \mathrm{K}_3(G) = [G, G'] = \langle z \rangle \cong \mathrm{C}_2,$$

$\Phi(G) = G'\langle h^2 \rangle$ *is abelian and the maximal subgroups of* G *are* $H_1 = \langle G', h \rangle$, $H_2 = \langle G', xh \rangle$ *(both are nonmetacyclic minimal nonabelian) and* $H = \langle x, s, h^2 \rangle$ *with* $\mathrm{d}(H) = 3$ *and* $H_1' = H_2' = H' = \langle z \rangle$.

Proof. Here $A = H_1 \cap H_2 = \Phi(G)$ is a maximal normal abelian subgroup of G. Set $H_1' = H_2' = \langle z \rangle \leq A$ so that $H_1/\langle z \rangle$ and $H_2/\langle z \rangle$ are two distinct abelian maximal subgroups in $G/\langle z \rangle$. It follows that $H/\langle z \rangle$ is also abelian and so $H' = \langle z \rangle$ since H is nonabelian. If $\mathrm{d}(H) = 2$, then, by Lemma 65.2(a), H would be minimal nonabelian, a contradiction. Thus $\mathrm{d}(H) \geq 3$.

If $G/\langle z \rangle$ is abelian, then $G' = \langle z \rangle$ and so $G = H_1 \mathrm{C}_G(H_1)$ which gives $\mathrm{d}(G) = 3$, a contradiction. Hence $G/\langle z \rangle$ is nonabelian and so $(G/\langle z \rangle)' \cong \mathrm{C}_2$ since $G/\langle z \rangle$ has three distinct abelian maximal subgroups. Thus $|G'| = 4$ and $G' \leq A = \Phi(G)$. Taking $h_1 \in H_1 - A$ and $h_2 \in H_2 - A$, we get $\langle h_1, h_2 \rangle = G$ and so $s = [h_1, h_2] \in G' - \langle z \rangle$. If $G' \cong C_4$, then z is a square in H_1 and H_2 and so both H_1 and H_2 are metacyclic (Lemma 65.1). Since $\mathrm{d}(H) \geq 3$, G has exactly one nonmetacyclic maximal subgroup. But then Theorem 87.12 for $n = 2$ implies that G has an abelian maximal subgroup, a contradiction. Thus $G' = \langle s, z \rangle \cong \mathrm{E}_4$, where s is an involution. If $s \in \mathrm{Z}(G)$, then $G/\langle s \rangle$ would be abelian (because $\langle h_1, h_2 \rangle = G$ and $s = [h_1, h_2]$), a contradiction. Hence $s \notin \mathrm{Z}(G)$ and so $s \notin \mathrm{Z}(H_1)$ or $s \notin \mathrm{Z}(H_2)$. Without loss of generality we may assume that $s \notin \mathrm{Z}(H_1)$.

Suppose that z is a square in H_1, i.e., there is $v \in H_1$ such that $v^2 = z$. Suppose at the moment that $v \in H_1 - A$ in which case $\langle v, G' \rangle = \langle v, s \rangle \cong \mathrm{D}_8$ since $s^v = sz$. It follows that $\langle v, G' \rangle = H_1$. Since $\mathrm{C}_G(H_1) \leq H_1$ (otherwise, $\mathrm{d}(G) = 3$), G would be of maximal class (Proposition 10.17), a contradiction (noting that 2-groups of maximal class have a cyclic maximal subgroup). Thus $v \in A = \Phi(G)$. In that case, both H_1 and H_2 are metacyclic (Lemma 65.1) which together with $\mathrm{d}(H) \geq 3$ allows us to use §87, part 2^o. If G has a normal elementary abelian subgroup of order 8, then we get the groups in part (a) of our theorem. If G has no normal elementary abelian subgroup of order 8, then we get the group of order 2^5 given in part (b) of our theorem.

Now we assume that z is not a square in H_1 which implies that H_1 is nonmetacyclic (Lemma 65.1). If h_1 is an involution, then $s^{h_1} = sz$ shows that $\langle h_1, s \rangle \cong \mathrm{D}_8$ and so $\langle h_1, s \rangle = H_1$ is metacyclic, a contradiction. Hence $o(h_1) = 2^n, n \geq 2$. Set $u = h_1^{2^{n-1}}$ so that $u \in \mathrm{Z}(H_1)$ and $u \notin G'$ since z is not a square in H_1 and $s^{h_1} = sz$. We have

$$E = \Omega_1(H_1) = \langle z, s, u \rangle \cong \mathrm{E}_8, \quad E \trianglelefteq G \quad \text{and} \quad E \leq A$$

which implies that H_2 is nonmetacyclic and therefore z is also not a square in H_2. Since $H_1 = E\langle h_1 \rangle = \langle h_1, s \rangle$, we have $|H_1| = 2^{n+2}$, $|G| = 2^{n+3}$ and $A = \langle h_1^2, s, z \rangle$ is abelian of order 2^{n+1} and type $(2^{n-1}, 2, 2)$. Also, H_1 is a splitting extension of G'

by $\langle h_1\rangle \cong \mathrm{C}_{2^n}$, $n \geq 2$. As $\mathrm{d}(G/G') = 2$, we get that G/G' is abelian of type $(2^n, 2)$. We obtain $G = FH_1$, where $F \cap H_1 = G'$ and $|F : G'| = 2$ so that $F = \langle G', x\rangle$ with $o(x) \leq 4$. In fact, we have $x^2 \in \langle z\rangle$. Indeed, if F is not elementary abelian, then $\mho_1(F) \cong \mathrm{C}_2$ and $\mho_1(F) \leq G'$. But $F \trianglelefteq G$ and so $\mho_1(F) \leq \mathrm{Z}(G)$ which implies that $\mho_1(F) = \langle z\rangle$ as $G' \not\leq \mathrm{Z}(G)$. Since $\langle xh_1\rangle G'/G'$ is another cyclic subgroup of index 2 in G/G' (distinct from H_1/G'), $M = \langle G', xh_1\rangle$ is a maximal subgroup of G distinct from H_1 and $M' = \langle z\rangle$ (since $H_2' = H' = \langle z\rangle$). If $G' \leq \mathrm{Z}(M)$, then M would be abelian, a contradiction. We get $s^{xh_1} = sz$ and so $M = \langle xh_1, s\rangle$ is minimal nonabelian which yields that $M = H_2$. We may set $h_2 = xh_1$, where $[h_1, h_2] = s$ and $G' = \langle s, z\rangle$. From $s^{xh_1} = sz$ it follows

$$s^x = (s^{xh_1})^{h_1^{-1}} = (sz)^{h_1^{-1}} = s^{h_1^{-1}} z = (sz)z = s$$

and so F is abelian. As $s = [h_1, h_2]$, we get

$$s = [h_1, h_2] = [h_1, xh_1] = [h_1, h_1][h_1, x]^{h_1} = [h_1, x]^{h_1}$$

and so

$$[h_1, x] = sz.$$

We conclude that $\Phi(G) = G'\langle h_1^2\rangle$ is abelian and $H = F\langle h_1^2\rangle$, where

$$[h_1^2, x] = [h_1, x]^{h_1}[h_1, x] = (sz)^{h_1}(sz) = (szz)(sz) = z.$$

Since $H/\langle z\rangle = H/H'$ is abelian of type $(2, 2, 2^{n-1})$, we have $\mathrm{d}(H) = 3$. Replacing s with $s' = sz$, we get $[h_1, x] = s'$ and writing again s instead of s', we may write $[h_1, x] = s \in G' - \langle z\rangle$. Also, writing h instead of h_1, we obtain the relations of part (c) of our theorem. □

Theorem 100.3. *Let G be a 2-group with $\mathrm{d}(G) = 2$ which has exactly one maximal subgroup H which is neither abelian nor minimal nonabelian. If the other two maximal subgroups H_1 and H_2 are minimal nonabelian with $H_1' \neq H_2'$, then one of the following holds:*

(a) *G is a group of order 2^6 with $n = 2$ given in Theorem 87.15*(a).

(b) *G is a group of order 2^{m+4} ($m \geq 2$) with $n = 2$ given in Theorem 87.16.*

(c) $G = \langle h, x \mid [h, x] = v,\ v^4 = 1,\ v^h = vz_1,\ v^x = v^{-1}\ v^2 = z_1z_2,\ z_1^2 = z_2^2 = 1,$ $[z_1, h] = [z_1, x] = [z_2, h] = [z_2, x] = 1,\ x^2 \in \langle z_1, z_2\rangle,\ h^{2^m} = (z_1z_2)^{\epsilon}\rangle$, *where*

$$\epsilon = 0, 1, \quad m \geq 2, \quad |G| = 2^{m+4}, \quad G' = \langle v, z_1\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2,$$
$$\mathrm{K}_3(G) = [G, G'] = \langle z_1, z_2\rangle \cong \mathrm{E}_4 \quad \textit{and} \quad \langle z_1, z_2\rangle \leq \mathrm{Z}(G).$$

Moreover, the maximal subgroups of the group G are $H_1 = G'\langle h\rangle$, $H_2 = G'\langle hx\rangle$ and $H = G'\langle x, h^2\rangle$, where H_1 and H_2 are both nonmetacyclic minimal nonabelian with $H_1' = \langle z_1\rangle$, $H_2' = \langle z_2\rangle$ and $H' = \langle z_1, z_2\rangle \cong \mathrm{E}_4$ ($\mathrm{d}(H) = 3$).

Proof. Set $\langle z_1\rangle = H_1'$ and $\langle z_2\rangle = H_2'$ so that $W = \langle z_1, z_2\rangle \cong \mathrm{E}_4$, $W \leq \mathrm{Z}(G)$ and $W \leq A = H_1 \cap H_2 = \Phi(G)$, where A is abelian. Here $\{H_1/\langle z_1\rangle, H_2/\langle z_1\rangle, H/\langle z_1\rangle\}$ is the set of maximal subgroups of $G/\langle z_1\rangle$ and $H_1/\langle z_1\rangle$ is abelian and two-generated, $H_2/\langle z_1\rangle$ is minimal nonabelian and so $H/\langle z_1\rangle$ must be nonabelian. If $H/\langle z_1\rangle$ is minimal nonabelian, then by a result of N. Blackburn (Theorem 44.5), $G/\langle z_1\rangle$ would be metacyclic. But then, by another result of N. Blackburn (Lemma 44.1 and Corollary 44.6), G is also metacyclic, contrary to $W \leq G'$ and $W \cong \mathrm{E}_4$. Hence $H/\langle z_1\rangle$ is neither abelian nor minimal nonabelian. By Theorem 100.1,

$$\mathrm{d}(H/\langle z_1\rangle) = 3, \quad (H/\langle z_1\rangle)' \cong \mathrm{C}_2, \quad G'/\langle z_1\rangle \cong \mathrm{C}_4.$$

Similarly, considering $G/\langle z_2\rangle$, we obtain that $(H/\langle z_2\rangle)' \cong \mathrm{C}_2$ and $G'/\langle z_2\rangle \cong \mathrm{C}_4$. It follows that G' is abelian of type $(4, 2)$ with $\mho(G') = \langle z_1 z_2\rangle$. On the other hand, $\{H_1/W, H_2/W, H/W\}$ is the set consisting of the maximal subgroups of the nonabelian group G/W, where both H_1/W and H_2/W are abelian. Hence H/W is also abelian and so $H' \leq W$. By the above, H' is distinct from $\langle z_1\rangle$ and $\langle z_2\rangle$ and so either $H' = W$ or $H' = \langle z_1 z_2\rangle$.

Suppose that $H' = \langle z_1 z_2\rangle$. Then

$$\{H_1/\langle z_1 z_2\rangle, H_2/\langle z_1 z_2\rangle, H/\langle z_1 z_2\rangle\}$$

is the set of maximal subgroups of $G/\langle z_1 z_2\rangle$, where $H_1/\langle z_1 z_2\rangle$ and $H_2/\langle z_1 z_2\rangle$ are minimal nonabelian and $H/\langle z_1 z_2\rangle$ is abelian. By Theorem 106.3 (or by results of §71), we deduce that $G/\langle z_1 z_2\rangle$ is metacyclic, contrary to $G'/\langle z_1 z_2\rangle \cong \mathrm{E}_4$. We have thus proved that $H' = W = \langle z_1, z_2\rangle$. Take $h_1 \in H_1 - A$, $h_2 \in H_2 - A$ so that we have $\langle h_1, h_2\rangle = G$. If $v = [h_1, h_2] \in W$, then v is an involution in $\mathrm{Z}(G)$ and $G/\langle v\rangle$ is abelian, $G' \leq \langle v\rangle$, a contradiction. Hence $v \notin W$ and so $v \in G' - W$ is of order 4 with $v^2 = z_1 z_2$ and $\langle v\rangle$ is not normal in G (and so also $\langle v z_1\rangle$ is not normal in G). Indeed, if $\langle v\rangle$ is normal in G, then $G/\langle v\rangle$ would be abelian since $[h_1, h_2] = v$ and $\langle h_1, h_2\rangle = G$. In particular, $\langle v\rangle$ cannot be normal in both H_1 and H_2 and so we may assume without loss of generality that $\langle v\rangle$ is not normal in H_1. Hence $[h_1, v] = z_1$ which gives $v^{h_1} = v z_1$ and $H_1 = \langle h_1, v\rangle$.

Suppose that H_1 is metacyclic. Then there exists $h_1' \in H_1$ such that $(h_1')^2 = z_1$. If $h_1' \in H_1 - A$, then $v^{h_1'} = v z_1$ and so $H_1 = \langle h_1', v\rangle$ is of order 2^4. But then $|G| = 2^5$ and $|G'| = 2^3$ imply (using a result of O. Taussky) that G is of maximal class, a contradiction. It follows that $h_1' \in A$ and then

$$(h_1' v)^2 = (h_1')^2 v^2 = z_1(z_1 z_2) = z_2$$

which implies that H_2 is also metacyclic. We are in a position to use §87, 2^o. By Theorems 87.9 and 87.10, G has no normal elementary abelian subgroup of order 8 (since $|G'| = 8$). We have $\Phi(G') \neq \{1\}$ and $\mathrm{Z}(G) \geq W$ is noncyclic. If $G/\Phi(G')$ has no normal elementary abelian subgroup of order 8, then G is isomorphic to a group of

order 2^6 given in Theorem 87.15(a) for $n = 2$. If $G/\Phi(G')$ has a normal elementary abelian subgroup of order 8, then G is a group of order 2^{m+4}, $m \geq 2$, given in Theorem 87.16 for $n = 2$.

Suppose that H_1 is nonmetacyclic. If there exists an element $l \in H_1 - A$ such that $l^2 \in G'$, then $v^l = vz_1$ gives that $H_1 = \langle l, v\rangle = G'\langle l\rangle$ is nonmetacyclic minimal nonabelian of order 2^4. But in that case, $|G| = 2^5$ and $|G'| = 2^3$ imply (using a result of O. Taussky) that G is of maximal class, a contradiction. It then follows that $\Omega_1(H_1) = \Omega_1(A) \cong \mathrm{E}_8$ and so H_2 is also nonmetacyclic minimal nonabelian. Since $h_2^2 \in H_1$, we have

$$[h_1, h_2^2] = z_1^\eta, \quad \eta = 0, 1.$$

We compute

$$z_1^\eta = [h_1, h_2^2] = [h_1, h_2][h_1, h_2]^{h_2} = vv^{h_2},$$

and so

$$v^{h_2} = v^{-1}z_1^\eta = v(z_1z_2)z_1^\eta = vz_1^{\eta+1}z_2.$$

If $\eta = 0$, then $v^{h_2} = v(z_1z_2)$, contrary to $H_2' = \langle z_2\rangle$. Thus $\eta = 1$ and so $v^{h_2} = vz_2$ which implies $H_2 = \langle h_2, v\rangle = G'\langle h_2\rangle$. Also, $v^{h_1} = vz_1$ gives $H_1 = \langle h_1, v\rangle = G'\langle h_1\rangle$ and since $h_1^2 \notin G'$, we have $H_1/G' \cong \mathrm{C}_{2^m}$, $m \geq 2$, and then also $H_2/G' \cong \mathrm{C}_{2^m}$.

Since $\mathrm{d}(G/G') = 2$, we see that G/G' is abelian of type $(2^m, 2)$, $m \geq 2$. We may set $G = FH_1$ with $F \cap H_1 = G'$ and $|F : G'| = 2$. Since $\langle h_1\rangle$ covers $H_1/G' \cong \mathrm{C}_{2^m}$, $v^{h_1} = vz_1$ and neither z_1 nor z_2 are squares of any element in $A = G'\langle h_1^2\rangle = \Phi(G)$, we get $h_1^{2^m} = (z_1z_2)^\epsilon$, $\epsilon = 0, 1$. We may set $h_2 = h_1x$ with $x \in F - G'$ so that from $v^{h_2} = vz_2$ follows

$$vz_2 = v^{h_2} = (v^{h_1})^x = (vz_1)^x = v^xz_1$$

and so $v^x = v(z_1z_2) = v^{-1}$ which gives $x^2 \in \langle z_1, z_2\rangle \leq \mathrm{Z}(G)$. It then follows from $v = [h_1, h_2]$ that

$$v = [h_1, h_1x] = [h_1, x][h_1, h_1]^x = [h_1, x].$$

Finally, we have $H_2 = G'\langle h_1x\rangle$ and $H = F\langle h_1^2\rangle$, where $F' = \langle [v, x]\rangle = \langle z_1z_2\rangle$ and

$$[h_1^2, x] = [h_1, x]^{h_1}[h_1, x] = v^{h_1}v = (vz_1)v = z_1v^2 = z_1(z_1z_2) = z_2$$

and so indeed $H' = \langle z_1, z_2\rangle \cong \mathrm{E}_4$ which shows that H is neither abelian nor minimal nonabelian. Writing h instead of h_1, we have obtained the relations given in part (c) of our theorem. □

We turn now to the case $\mathrm{d}(G) \geq 3$. Since G possesses at least one minimal nonabelian maximal subgroup, it follows that in this case $\mathrm{d}(G) = 3$. It is well known that the number of abelian maximal subgroups in a nonabelian 2-group G is 0, 1 or 3. According to this fact, we shall subdivide our study of the title groups with $\mathrm{d}(G) = 3$.

Theorem 100.4. *Let G be a 2-group with $\mathrm{d}(G) = 3$ which has exactly one maximal subgroup which is neither abelian nor minimal nonabelian. If G possesses more than one abelian maximal subgroup, then one of the following holds:*

(a) $G = Q * Z$, *where* $Q \cong \mathrm{Q}_8$, $Z \cong \mathrm{C}_{2^n}$, $n \geq 3$ *and* $Q \cap Z = \mathrm{Z}(Q)$.

(b) $G = Q \times Z$, *where* $Q \cong \mathrm{Q}_8$ *and* $Z \cong \mathrm{C}_{2^n}$, $n \geq 2$.

(c) $G = D \times Z$, *where* $D \cong \mathrm{D}_8$ *and* $Z \cong \mathrm{C}_{2^n}$, $n \geq 2$.

Proof. By our assumption, G has exactly three abelian maximal subgroups. This implies $|G'| = 2$ and G possesses exactly three maximal subgroups which are minimal nonabelian. Suppose that H is a minimal nonabelian maximal subgroup of G. Since $H' = G' \cong \mathrm{C}_2$, we get $G = H\mathrm{Z}(G)$, where

$$\mathrm{Z}(G) \cap H = \mathrm{Z}(H) = \Phi(H) = \Phi(G).$$

All three maximal subgroups of G, containing $\mathrm{Z}(G)$, are abelian.

Let G be a title group with $|G'| = 2$. Then G possesses a maximal subgroup H which is minimal nonabelian. From $H' = G' \cong \mathrm{C}_2$ follows that $G = H\mathrm{Z}(G)$ with $|G : \mathrm{Z}(G)| = 4$. In that case, $\mathrm{d}(G) = 3$ and all three maximal subgroups of G containing $\mathrm{Z}(G)$ are abelian. It follows that for a title group G the assumption $G' \cong \mathrm{C}_2$ is equivalent with the assumption that G has more than one abelian maximal subgroup.

In what follows H will denote a fixed maximal subgroup of G which is minimal nonabelian. Suppose that there is an involution $c \in \mathrm{Z}(G) - \mathrm{Z}(H)$. Then $G = H \times \langle c \rangle$ and so each maximal subgroup of G which does not contain $\langle c \rangle$ is isomorphic to $G/\langle c \rangle \cong H$ and so is minimal nonabelian, a contradiction. Hence there are no involutions in $\mathrm{Z}(G) - H$ which implies that $\Omega_1(\mathrm{Z}(H)) = \Omega_1(\mathrm{Z}(G))$ so that $\mathrm{d}(\mathrm{Z}(H)) = \mathrm{d}(\mathrm{Z}(G))$. It follows that for each $x \in \mathrm{Z}(G) - H$, $x^2 \in \mathrm{Z}(H) - \Phi(\mathrm{Z}(H))$. Suppose that $|G| = 2^4$. Then each nonabelian maximal subgroup of G is isomorphic to D_8 or Q_8 and so is minimal nonabelian, a contradiction. Hence $|G| \geq 2^5$ and, in particular, H is not isomorphic to Q_8 or D_8.

(i) First assume that H is metacyclic. Since H is not isomorphic to Q_8, it follows that H is a "splitting" metacyclic group and so we may set

$$H = \langle a, b \mid a^{2^m} = b^{2^n} = 1,\ a^b = az,\ z = a^{2^{m-1}} \rangle,$$

where

$$m \geq 2, \quad n \geq 1, \quad m + n \geq 4, \quad H' = \langle z \rangle, \quad |H| = 2^{m+n}, \quad |G| = 2^{m+n+1}.$$

We see that $\mathrm{Z}(H) = \langle a^2 \rangle \times \langle b^2 \rangle = \Phi(H) = \Phi(G)$ and, for each $x \in \mathrm{Z}(G) - H$, $x^2 \in \langle a^2, b^2 \rangle - \langle a^4, b^4 \rangle$ since $\langle a^4, b^4 \rangle = \Phi(\mathrm{Z}(H))$.

Suppose that $n = 1$ so that b is an involution, $m \geq 3$, $H \cong \mathrm{M}_{2^{m+1}}$, $\mathrm{Z}(H) = \langle a^2 \rangle$. Hence $\mathrm{Z}(G) \cong \mathrm{C}_{2^m}$ is cyclic and therefore we may choose $c \in \mathrm{Z}(G) - H$ such that $c^2 = a^{-2}$ which gives $(ca)^2 = c^2a^2 = 1$. As $[ca, b] = z$, we get $D = \langle ca, b \rangle \cong \mathrm{D}_8$,

$\langle ca, b\rangle \cap \mathrm{Z}(G) = \langle z\rangle$ which together with $|G : \mathrm{Z}(G)| = 4$ gives $G = D\mathrm{Z}(G)$. But $D * \Omega_2(\mathrm{Z}(G))$ contains a subgroup $Q \cong \mathrm{Q}_8$ and so $G = Q * \mathrm{Z}(G)$ with $\mathrm{Z}(G) \cong \mathrm{C}_{2^m}$, $m \geq 3$, $Q \cap \mathrm{Z}(G) = \mathrm{Z}(Q) = \langle z\rangle$ and we have obtained the groups stated in part (a) of our theorem.

It remains to treat the case $n \geq 2$. Suppose that there is an involution $x \in G - H$. We know that $x \notin \mathrm{Z}(G)$ and so $[a, x] \neq 1$ or $[b, x] \neq 1$. Obviously, $\langle a, b, x\rangle = G$.

Suppose that $[a, x] \neq 1$. As $\langle a\rangle \trianglelefteq G$, $\langle a, x\rangle$ is minimal nonabelian of order 2^{m+1}. Because $|G| = 2^{m+n+1}$ and $n \geq 2$, $\Phi(G)\langle a, x\rangle = \langle a, x, b^2\rangle$ is a maximal subgroup of G which is neither abelian nor minimal nonabelian. Assume at the moment that $[b, x] \neq 1$. In that case, $\langle b\rangle \times \langle z\rangle$ is normal in G and so $\langle b, x\rangle$ is a nonmetacyclic minimal nonabelian subgroup of G of order 2^{n+2}. It follows that $\langle b, x\rangle$ must be maximal in G with $|G| = 2^{n+3}$ (and so $m = 2$). But the case of a nonmetacyclic minimal nonabelian maximal subgroup in G will be studied in part (ii) of this proof. Hence we may assume $[x, b] = 1$ so that $[x, ab] = [x, a][x, b] = z$ which implies that $\langle x, ab\rangle$ is minimal nonabelian and so $\langle x, ab\rangle$ must be maximal in G. Now, $\langle ab\rangle$ covers $H/\langle a\rangle \cong \mathrm{C}_{2^n}$, $n \geq 2$, and so $o(ab) \geq 2^n$. We get

$$(ab)^{2^n} = a^{2^n} b^{2^n} [b, a]^{2^{n-1}(2^n-1)} = a^{2^n}.$$

If $n \geq m$, then we have $(ab)^{2^n} = 1$ and so $o(ab) = 2^n$ and $\langle ab\rangle \cap \langle a\rangle = \{1\}$. Since $\langle ab, z\rangle \trianglelefteq G$, we see that $\langle ab, x\rangle$ is a nonmetacyclic minimal nonabelian subgroup of order 2^{n+2}. In that case, $\langle ab, x\rangle$ must be maximal in G (with $m = 2$) and again this will be studied in part (ii) of this proof. It follows that we may assume $n < m$ and we set in that case $s = m - n \geq 1$. From $(ab)^{2^n} = a^{2^n}$ and $o(a^{2^n}) = 2^s$ we infer that $o(ab) = 2^{n+s} = 2^m$ and $\langle ab\rangle \geq \langle z\rangle$ so that $\langle ab\rangle \trianglelefteq G$. Hence $\langle ab, x\rangle$ is metacyclic minimal nonabelian of order 2^{m+1} and so $\langle ab, x\rangle$ must be maximal in the group G. From $|G| = 2^{m+n+1}$ follows $n = 1$, contrary to our assumption.

We may assume $[a, x] = 1$ and so we must have $[b, x] \neq 1$. Since $\langle b\rangle \times \langle z\rangle \trianglelefteq G$, $\langle b, x\rangle$ is nonmetacyclic minimal nonabelian of order 2^{n+2}. If $\langle b, x\rangle$ is maximal in G, then this case will be treated in part (ii) of this proof. Thus we may assume that $\langle b, x\rangle$ is not maximal in G and so $M = \Phi(G)\langle b, x\rangle$ is maximal in G and M is neither abelian nor minimal nonabelian. It then follows that the subgroup $\langle ab, x\rangle$ (with $[ab, x] = z$), which is minimal nonabelian, must be also a maximal subgroup in G. Since $\langle ab\rangle$ covers $H/\langle a\rangle$, we have $o(ab) \geq 2^n$, $n \geq 2$ and $(ab)^{2^n} = a^{2^n}$. If $n \geq m$, then we get $o(ab) = 2^n$ and $\langle ab\rangle \cap \langle a\rangle = \{1\}$ and so $\langle ab, x\rangle$ is nonmetacyclic minimal nonabelian of order 2^{n+2}. In that case, $\langle ab, x\rangle$ is maximal in G (with $m = 2$) and again this will be treated in part (ii) of this proof. We may assume that $n < m$ and then $o(ab) = 2^m$, $\langle ab\rangle \geq \langle z\rangle$ and so $\langle ab, x\rangle$ is metacyclic minimal nonabelian of order 2^{m+1}. But then $|G| = 2^{m+n+1}$ implies $n = 1$, contrary to our assumption.

We have proved that we may assume that there are no involutions in $G - H$. If there is $c \in \mathrm{Z}(G) - H$ such that $c^2 = h^2$ for some $h \in H$, then the abelian subgroup $\langle h, c\rangle$ is noncyclic since $\langle h\rangle$ and $\langle c\rangle$ are two distinct cyclic subgroups of $\langle h, c\rangle$ of the same order. But $\langle h, c\rangle \cap H = \langle h\rangle$ and so there is an involution in $\langle h, c\rangle - H$, a contradiction.

It follows that not every element in $\mho_1(H) = \mathrm{Z}(H)$ is a square of an element in H. By Proposition 26.23, H is not a powerful 2-group which implies $H' = \langle z\rangle \not\leq \mho_2(H)$. This forces $m = 2$ and c^2 is not a square in H for any $c \in \mathrm{Z}(G) - H$. We compute for any integers i, j

$$(a^i b^j)^2 = a^{2i} b^{2j} [b^j, a^i] = a^{2i} b^{2j} z^{ij}.$$

We get that $a^{2i} b^{2j} \in \mho_1(H) = \mathrm{Z}(H)$ is a square in H if and only if i or j is even. Therefore for any $c \in \mathrm{Z}(G) - H$, $c^2 = a^{2i} b^{2j}$, where both i and j are odd, and then (since $m = 2$ and so $a^2 = z$) $c^2 = z b^{2j}$, where j is odd. Consider the nonabelian subgroup $S = \langle a, b^{-j} c\rangle$, where

$$(b^{-j} c)^2 = b^{-2j} c^2 = b^{-2j} z b^{2j} = z,$$

and so $S \cong \mathrm{Q}_8$. Hence we conclude that $G = \langle S, c\rangle = S \times \langle c\rangle \cong \mathrm{Q}_8 \times \mathrm{C}_{2^n}$ with $n \geq 2$, where $S \times \langle b^2\rangle \cong \mathrm{Q}_8 \times \mathrm{C}_{2^{n-1}}$ is a unique maximal subgroup of G which is neither abelian nor minimal nonabelian. We have obtained the groups stated in part (b) of our theorem.

(ii) It remains to consider the case where H is nonmetacyclic minimal nonabelian. We may set

$$H = \langle a, b \mid a^{2^m} = b^{2^n} = 1,\ [a, b] = z,\ z^2 = [a, z] = [b, z] = 1\rangle,$$

where we may assume $m \geq 2$, $n \geq 1$ as $|H| \geq 2^4$. Here $H' = \langle z\rangle$, $|H| = 2^{m+n+1}$ and so $|G| = 2^{m+n+2}$. Also, z is not a square in H, $\mathrm{Z}(H) = \langle a^2\rangle \times \langle b^2\rangle \times \langle z\rangle = \Phi(H) = \Phi(G)$ and for each $x \in \mathrm{Z}(G) - H$, $x^2 \in \mathrm{Z}(H) - \Phi(\mathrm{Z}(H))$.

(ii1) First assume $n = 1$ so that $\mathrm{Z}(H) = \langle a^2\rangle \times \langle z\rangle$ and for a $c \in \mathrm{Z}(G) - H$, $c^2 = a^{2i} z^j$. Suppose that i is even and then j must be odd and so we may set in that case $c^2 = a^{4i'} z$ and compute for an element $c' = a^{-2i'} c \in \mathrm{Z}(G) - H$

$$(c')^2 = (a^{-2i'} c)^2 = a^{-4i'} c^2 = a^{-4i'} a^{4i'} z = z.$$

This gives $G = H * \langle c'\rangle$ with $(c')^2 = z$, where $\langle z\rangle = H'$, and it is easy to see that in that case G is an A_2-group (see Proposition 71.1), a contradiction.

We have proved that i must be odd. The subgroup $D = \langle a^{-i} c, b\rangle$ is minimal nonabelian since $[a^{-i} c, b] = [a, b]^{-i} = z$. We have also

$$(a^{-i} c)^2 = a^{-2i} c^2 = a^{-2i} a^{2i} z^j = z^j$$

which shows that $D \cong \mathrm{D}_8$. But $\langle c\rangle \cap \langle z\rangle = \{1\}$, where $\langle z\rangle = \mathrm{Z}(D)$, and so $\langle D, c\rangle = \langle a^{-i} c, b, c\rangle = G = D \times \langle c\rangle$ with $o(c) = 2^m$, $m \geq 2$. The subgroup $D \times \langle c^2\rangle$ is a unique maximal subgroup of G which is neither abelian nor minimal nonabelian and we have obtained the groups stated in part (c) of our theorem.

(ii2) It remains to consider the case $n \geq 2$. In this case, for an element $c \in \mathrm{Z}(G) - H$ we have $c^2 = a^{2i} b^{2j} z^k$, where at least one of the integers i, j, k is odd.

Suppose that both i and j are even so that in this case k is odd and we may set $c^2 = a^{4i'}b^{4j'}z$. For the element $c' = a^{-2i'}b^{-2j'}c$, we get

$$(c')^2 = a^{-4i'}b^{-4j'}c^2 = a^{-4i'}b^{-4j'}a^{4i'}b^{4j'}z = z,$$

and so $G = H * \langle c' \rangle$ with $(c')^2 = z$ and $\langle z \rangle = H'$ which gives that G is an A_2-group from Proposition 71.1, a contradiction.

Now assume that one of the integers i, j is even and the other one is odd. Note that i, j occur symmetrically and so we may assume that i is odd and j is even. In that case, the subgroup $T = \langle a^{-i}b^{-j}c, b \rangle$ is minimal nonabelian since $[a^{-i}b^{-j}c, b] = [a, b]^{-i} = z$. Using the fact that $b^{-j} \in \mathrm{Z}(G)$, we get

$$(a^{-i}b^{-j}c)^2 = a^{-2i}b^{-2j}c^2 = a^{-2i}b^{-2j}a^{2i}b^{2j}z^k = z^k.$$

Since $\Phi(T) = \langle b^2 \rangle \times \langle z \rangle$, we have $|T| = 2^{n+2}$. On the other hand, $|G| = 2^{m+n+2}$ with $m \geq 2$ and so $\Phi(G)T$ is a maximal subgroup of G which is neither abelian nor minimal nonabelian. Consider now the minimal nonabelian subgroup $U = \langle ab, ac \rangle$, where $[ab, ac] = z$. We have

$$(ab)^2 = a^2b^2z, \quad (ac)^2 = a^2c^2 = a^2 \cdot a^{2i}b^{2j}z^k = a^{2(i+1)}b^{2j}z^k,$$

where both $i + 1$ and j are even, and

$$\Phi(U) = \langle a^2b^2z, a^{2(i+1)}b^{2j}z^k, z \rangle \leq \langle a^2b^2, z \rangle \Phi(\mathrm{Z}(H))$$

since $a^{2(i+1)}b^{2j} \in \Phi(\mathrm{Z}(H))$. But

$$\mathrm{Z}(H) = \langle a^2 \rangle \times \langle b^2 \rangle \times \langle z \rangle$$

and so $\mathrm{d}(\mathrm{Z}(H)) = 3$ which gives $\Phi(U) < \mathrm{Z}(H) = \Phi(G)$. This shows that $\Phi(G)U$ is another maximal subgroup of G which is neither abelian nor minimal nonabelian, a contradiction.

It remains to consider the possibility that both i and j are odd. Then we consider the minimal nonabelian subgroup $V = \langle a^{-i}b^{-j}c, b \rangle$, where $[a^{-i}b^{-j}c, b] = [a, b]^{-i} = z$. We get

$$\begin{aligned}(a^{-i}b^{-j}c)^2 &= (a^{-i}b^{-j})^2c^2 = a^{-2i}b^{-2j}z^{ij}c^2 \\ &= a^{-2i}b^{-2j}z \cdot a^{2i}b^{2j}z^k = z^{k+1}\end{aligned}$$

which shows that $|V| = 2^{n+2}$. But $|G| = 2^{m+n+2}$ with $m \geq 2$ and so $\Phi(G)V$ is a maximal subgroup of G which is neither abelian nor minimal nonabelian. Now we consider a minimal nonabelian subgroup $W = \langle a, bc \rangle$, where $[a, bc] = z$. We compute

$$(bc)^2 = b^2c^2 = b^2 \cdot a^{2i}b^{2j}z^k = a^{2i}b^{2(1+j)}z^k,$$

where i is odd and $1 + j$ is even. Then we have

$$\Phi(W) = \langle a^2, (bc)^2, z\rangle = \langle a^2, a^{2i}b^{2(1+j)}z^k, z\rangle = \langle a^2, z\rangle\Phi(\mathrm{Z}(H)) < \mathrm{Z}(H) = \Phi(G)$$

since $b^{2(1+j)} \in \Phi(\mathrm{Z}(H))$. Hence $\Phi(G)W$ is another maximal subgroup of G which is neither abelian nor minimal nonabelian, a contradiction. □

In the rest of this section we shall assume that G is a title group with $\mathrm{d}(G) = 3$ which possesses at most one abelian maximal subgroup. We know that in that case $|G : \mathrm{Z}(G)| \geq 8$ and $|G'| > 2$. Let H be a maximal subgroup of G which is minimal nonabelian. Then $\Phi(H) = \mathrm{Z}(H) \leq \Phi(G)$ and $|H : \Phi(H)| = 4$. As $|G : \Phi(H)| = 8$, we must also have $\Phi(H) = \Phi(G)$. Let $K \neq H$ be another maximal subgroup of G which is minimal nonabelian. Then $\mathrm{Z}(K) = \Phi(K) = \Phi(G)$ which implies $\Phi(G) \leq \mathrm{Z}(G)$ and so $\Phi(G) = \mathrm{Z}(G)$. Let M be the unique maximal subgroup of G which is neither abelian nor minimal nonabelian. Since $|M : \Phi(G)| = 4$ and $\Phi(G) = \mathrm{Z}(G)$, we have $M = S * \Phi(G)$, where S is minimal nonabelian, $S \cap \Phi(G) = \Phi(S) < \Phi(G)$ and so $M' = S' \cong \mathrm{C}_2$ with $\mathrm{d}(M) \geq 3$.

Theorem 100.5. *Let G be a 2-group with $\mathrm{d}(G) = 3$ which has exactly one maximal subgroup M which is neither abelian nor minimal nonabelian. If G possesses exactly one abelian maximal subgroup A, then*

$$\Phi(G) = \mathrm{Z}(G), \quad G' \cong \mathrm{E}_4, \quad M' \cong \mathrm{C}_2, \quad \mathrm{d}(M) \geq 3$$

and one of the following holds:

(a) *If G has no normal elementary abelian subgroup of order 8, then G is one of the groups given in Theorem 87.8*(e).

(b) *If G has a normal subgroup $E \cong \mathrm{E}_8$ but $\Omega_1(G) > E$, then*

$$G = \langle t, t', c \mid t^2 = t'^2 = c^4 = 1,\ [t,t'] = c^2 = z,\ [c,t] = u,\ u^2 = [c,t'] = [u,t] = [u,t'] = [u,c] = [z,t] = [z,t'] = 1\rangle,$$

where

$$|G| = 2^5, \quad G' = \Phi(G) = \mathrm{Z}(G) = \langle z, u\rangle \cong \mathrm{E}_4,$$
$$\Omega_1(G) = M = \langle t, t'\rangle G' \cong \mathrm{C}_2 \times \mathrm{D}_8,$$

the subgroup $A = \langle t', c\rangle G'$ is abelian of type $(4,2,2)$ and the other five maximal subgroups of G are nonmetacyclic minimal nonabelian.

(c) *If G has a normal subgroup $E \cong \mathrm{E}_8$, $\Omega_1(G) = E$ and $E \not\leq A$, then*

$$G = \langle a, b, t \mid a^{2^{m+1}} = b^4 = t^2 = 1,\ a^{2^m} = z,\ b^2 = u,\ [a,t] = u,\ [b,t] = z,\ [u,a] = [u,t] = [a,b] = [z,t] = 1\rangle,$$

where

$$|G| = 2^{m+4},\ m \geq 2, \quad G' = \langle z, u\rangle \cong \mathrm{E}_4,$$
$$\Phi(G) = \mathrm{Z}(G) = \langle a^2, u\rangle \cong \mathrm{C}_{2^m} \times \mathrm{C}_2, \quad E \not\leq \mathrm{Z}(G),$$
$$A = \langle a, b\rangle \text{ is abelian of type } (2^{m+1}, 4), \quad M = \langle b, t\rangle * \langle a^2\rangle,$$

where $\langle b, t\rangle$ is the nonmetacyclic minimal nonabelian group of order 2^4 and the other five maximal subgroups of G are minimal nonabelian.

(d) *If G has a normal subgroup $E \cong \mathrm{E}_8$, $\Omega_1(G) = E$ and $E \leq A$, then*

$$G = \langle a, b, d \mid a^4 = b^2 = d^4 = 1,\ a^2 = d^2 = z,\ [a, d] = z,$$
$$[a, b] = c,\ c^2 = [c, d] = [c, a] = [c, b] = [b, d] = 1\rangle,$$

where

$$|G| = 2^5, \quad G' = \Phi(G) = \mathrm{Z}(G) = \langle z, c\rangle \cong \mathrm{E}_4, \quad A = \langle b, d\rangle\Phi(G),$$
$$M = \langle a, d, c\rangle \cong \mathrm{Q}_8 \times \mathrm{C}_2, \quad E \not\leq \mathrm{Z}(G)$$

and the other five maximal subgroups of G are minimal nonabelian.

Proof. Let $\Gamma_1 = \{M, A, H_1, \ldots, H_5\}$ be the set of maximal subgroups of G, where $H_1, \ldots, H_5$ are minimal nonabelian. By Exercise 1.69(a), we have $|G' : (A'H_1')| = |G' : H_1'| \leq 2$ and so $|G'| = 4$ (since $|G'| > 2$). If $G' = \langle v\rangle \cong \mathrm{C}_4$, then we get $H_1' = \cdots = H_5' = \langle v^2\rangle$. But then $G/\langle v^2\rangle$ is a nonabelian group with at least five abelian maximal subgroups $H_i/\langle v^2\rangle$, $i = 1, \ldots, 5$, a contradiction. Hence we obtain that $G' \cong \mathrm{E}_4$. Since A/M' and M/M' are two abelian maximal subgroups of the nonabelian group G/M', it follows that there is exactly one minimal nonabelian maximal subgroup of G, say H_5, such that $H_5' = M'$. With similar arguments we see that we may assume that $H_1' = H_2'$, $H_3' = H_4'$, $H_5' = M'$ are three pairwise distinct subgroups of order 2 in $G' \cong \mathrm{E}_4$.

Suppose that the group G has no normal elementary abelian subgroup of order 8. Then $A, H_1, \ldots, H_5$ are metacyclic and so M is the only maximal subgroup of G which is nonmetacyclic. Since $\mathrm{d}(G) = 3$ and $G' \cong \mathrm{E}_4$, we see that G is isomorphic to one of the groups stated in Theorem 87.8(e) which gives part (a) of our theorem.

From now on we assume that G has a normal elementary abelian subgroup E of order 8. Suppose at the moment that G possesses an elementary abelian subgroup F of order 16. Obviously, F is a maximal elementary abelian subgroup in G. Indeed, if X is an elementary abelian subgroup of order 32 in G, then $|X \cap H_1| = 16$, a contradiction. Since $G' \leq \mathrm{Z}(G)$, we have $G' \leq F$ and so $F \trianglelefteq G$. If G/F is noncyclic, then there are at least three distinct maximal subgroups of G containing F and so at least one of them is minimal nonabelian, a contradiction. Hence G/F is cyclic and let $a \in G - F$ be such that $\langle a\rangle$ covers G/F. Suppose that $|G : F| = 2$ holds so that F is an abelian

maximal subgroup in G. Since $\mathrm{C}_F(a) = \mathrm{Z}(G) = \Phi(G)$ and $|G/\Phi(G)| = 8$, we get $\mathrm{C}_F(a) = G' \cong \mathrm{E}_4$. By Lemma 99.2, $G \cong \mathrm{E}_4 \wr \mathrm{C}_2$ and so we may assume that a is an involution. Let $f_1, f_2 \in F - G'$ so that $F = \langle f_1, f_2\rangle \times G'$ and $G = \langle f_1, f_2, a\rangle$. We have $\langle a, f_1\rangle \cong \langle a, f_2\rangle \cong \mathrm{D}_8$ and $\langle a, f_1\rangle G'$ and $\langle a, f_2\rangle G'$ are two distinct maximal subgroups of G which are isomorphic to $\mathrm{D}_8 \times \mathrm{C}_2$ (and so they are neither abelian nor minimal nonabelian), a contradiction. We have proved that $G/F \cong \mathrm{C}_{2^m}$, $m \geq 2$. Since $a^2 \in \Phi(G) = \mathrm{Z}(G)$, a induces an involutory automorphism on F which together with $|G : \mathrm{Z}(G)| = 8$ implies $\mathrm{C}_F(a) = G'$. As $a^2 \notin F$ and $\Omega_1(\langle a\rangle) \leq \mathrm{Z}(G)$, we must have $\Omega_1(\langle a\rangle) \leq F$ (because E_{32} is not a subgroup of G). Hence $\langle a\rangle \cap F = \langle a\rangle \cap G' = \langle z\rangle \cong \mathrm{C}_2$ and so

$$o(a) = 2^{m+1}, \quad m \geq 2, \quad |G| = 2^{m+4}, \quad \mathrm{Z}(G) = \Phi(G) = G'\langle a^2\rangle.$$

We may set $F = \langle x, y, u, z\rangle$, where $G' = \langle u, z\rangle$, $[a, x] = u$, $[a, y] = z$, $G = \langle x, y, a\rangle$ and so the structure of G is completely determined. Now, $\langle a, y\rangle \cong \langle ax, y\rangle \cong \mathrm{M}_{2^{m+2}}$ so that $\langle u\rangle \times \langle a, y\rangle$ and $\langle u\rangle \times \langle ax, y\rangle$ are two distinct maximal subgroups of G which are neither abelian nor minimal nonabelian, a contradiction.

We have proved that G does not possess an elementary abelian subgroup of order 16. Since $G' \leq \mathrm{Z}(G)$, we have $G' < E \cong \mathrm{E}_8$. Next suppose that $E < \Omega_1(G)$ so that there is an involution $t \in G - E$ with $\mathrm{C}_E(t) = G'$ and $S = \langle E, t\rangle \trianglelefteq G$. If G/S is noncyclic, then S is contained in a maximal subgroup of G which is minimal nonabelian, a contradiction (to the structure of minimal nonabelian 2-groups). Hence G/S is cyclic and let $c' \in G - S$ be such that $\langle c'\rangle$ covers G/S. Let $t' \in E - G'$ so that $1 \neq [t, t'] = z \in G'$ and $\langle t, t'\rangle = D \cong \mathrm{D}_8$. Also, $E_1 = \langle G', t\rangle$ is another elementary abelian normal subgroup of order 8 in G. All elements in $S - (E \cup E_1)$ are of order 4 and $v = tt'$ is one of them. We infer that $v^2 = z$, $S = D \times \langle u\rangle \cong \mathrm{D}_8 \times \mathrm{C}_2$, where $u \in G' - \langle z\rangle$, and also $\mathrm{Z}(S) = G'$ with $\mathrm{Z}(G) = \Phi(G) = G'\langle c'^2\rangle$ so that $G = \langle t, t', c'\rangle$ and $M = S\langle c'^2\rangle$ must be a unique maximal subgroup of G which is neither abelian nor minimal nonabelian. If $x \in G - M$, then x is either an involution or $\Omega_1(\langle x\rangle) \leq G'$. If x is an involution, then $[t, x] \neq 1$ (because E_{16} is not a subgroup of G) and so $\langle t, x\rangle \cong \mathrm{D}_8$, $|G : S| = 2$, $|G| = 2^5$, and $\langle t, x\rangle G'$ would be another maximal subgroup of G which is neither abelian nor minimal nonabelian, a contradiction. We have proved that x is not an involution and so $\Omega_1(\langle x\rangle) \leq G'$. Indeed, $\Omega_1(\langle x\rangle) \leq \mathrm{Z}(G)$ and so $\Omega_1(\langle x\rangle) \leq S$ which implies that $\Omega_1(\langle x\rangle) \leq \mathrm{Z}(S) = G'$.

Now, $A \cap M$ is equal to one of three abelian maximal subgroups of M (containing $\Phi(G) = \mathrm{Z}(G)$): $\langle E_1, c'^2\rangle$, $\langle E, c'^2\rangle$, $\langle G'\langle v\rangle, c'^2\rangle$, where A is the unique abelian maximal subgroup of G. We choose $c \in A - M$ (instead of c'), where $\langle c\rangle$ also covers G/S, $o(c) \geq 4$, $\Omega_1(\langle c\rangle) \leq G'$, $\Phi(G) = \mathrm{Z}(G) = G'\langle c^2\rangle$, and c centralizes exactly one of the elements in the set $\{t, t', v = tt'\}$. Indeed, otherwise, $G/\langle z\rangle$ would be abelian since c generates G together with any two elements in the above set. But then $G' = \langle z\rangle$, a contradiction. Interchanging t and t' (if necessary), we may assume that $[c, t'] = 1$ or $[c, tt'] = 1$. In that case, $[c, t] \neq 1$ and if $[c, t] = z$, then again $G/\langle z\rangle$ would be abelian, a contradiction. It follows that we may set $[c, t] = u \in G' - \langle z\rangle$.

First assume $[c, tt'] = 1$ which gives $[c, t'] = u$. We have $M = \langle t, t'\rangle\Phi(G)$ and $A = \langle c, tt'\rangle\Phi(G)$. It follows that the other five maximal subgroups $\Phi(G)T$ of G must be minimal nonabelian, where T is one of the following minimal nonabelian subgroups:

$$\langle t, c\rangle, \quad \langle t', c\rangle, \quad \langle t, t'c\rangle, \quad \langle t', tc\rangle, \quad \langle tt', tc\rangle.$$

We have to show that in each of these cases $\Phi(T) \geq \Phi(G) = \langle G', c^2\rangle = \langle u, z, c^2\rangle$. Note that $[t, c] = u$ and so $\Phi(\langle t, c\rangle) = \langle c^2, u\rangle$ which implies $\Omega_1(\langle c\rangle) \in \{\langle z\rangle, \langle uz\rangle\}$. We have $[t, t'c] = zu$ and so $\Phi(\langle t, t'c\rangle) = \langle (t'c)^2 = c^2u, zu\rangle$. Here if $o(c) \geq 8$, then $\Omega_1(\langle t'c\rangle) = \Omega_1(\langle c\rangle)$ and then $\Omega_1(\langle c\rangle) \in \{\langle z\rangle, \langle u\rangle\}$ which together with the above result gives $\Omega_1(\langle c\rangle) = \langle z\rangle$, and if $o(c) = 4$, then $c^2 = uz$. We have $[tt', tc] = z$ and so

$$\Phi(\langle tt', tc\rangle) = \langle (tt')^2 = z, (tc)^2 = c^2u, z\rangle = \langle c^2u, z\rangle.$$

If $o(c) = 4$, then by the above $c^2 = uz$ and then $\Phi(\langle tt', tc\rangle = \langle z\rangle$, a contradiction. In case $o(c) \geq 8$, then by the above $\Omega_1(\langle c\rangle) = \langle z\rangle$ and as $\Omega_1(\langle c^2u\rangle) = \Omega_1(\langle c\rangle) = \langle z\rangle$, we get again $\Phi(\langle tt', tc\rangle) = \langle c^2u\rangle \not\geq \Phi(G)$, a contradiction.

Now assume $[c, t'] = 1$ and from before we know that $[t, t'] = z$ and $[c, t] = u$. We have here $M = \langle t, t'\rangle\Phi(G)$ and $A = \langle c, t'\rangle\Phi(G)$ so that the other five maximal subgroups must be minimal nonabelian. Since $[t, c] = u$, we get $\Phi(\langle t, c\rangle) = \langle c^2, u\rangle$ which gives $\Omega_1(\langle c\rangle) \in \{\langle z\rangle, \langle uz\rangle\}$. Further, $[t, t'c] = zu$ and so we conclude that $\Phi(\langle t, t'c\rangle) = \langle (t'c)^2 = c^2, zu\rangle$ which implies that $\Omega_1(\langle c\rangle) \in \{\langle u\rangle, \langle z\rangle\}$. This fact together with our previous result gives $\Omega_1(\langle c\rangle) = \langle z\rangle$. We have $[t', tc] = z$ and so $\Phi(\langle t', tc\rangle) = \langle (tc)^2 = c^2u, z\rangle$. If $o(c) \geq 8$, then $(c^2u)^2 = c^4$ and $\langle c^4\rangle \geq \langle z\rangle$ since $\Omega_1(\langle c\rangle) = \langle z\rangle$. In this case, $\Phi(\langle t', tc\rangle) \not\geq \Phi(G)$, a contradiction. Hence $o(c) = 4$ and so $c^2 = z$. We have obtained a uniquely determined group of order 2^5 given in part (b) of our theorem.

From now on we may assume that $\Omega_1(G) = E \cong \mathrm{E}_8$.

(i) Assume that $\Omega_1(G) = E \not\leq \mathrm{Z}(G) = \Phi(G)$ and $E \not\leq A$, where A is the unique abelian maximal subgroup of G.

Then $A \cap E = G'$, A covers G/E and A is metacyclic. Since there are three maximal subgroups of G containing E, there exists at least one of them, denoted by H, which is minimal nonabelian. If H/E is noncyclic, then there are two distinct maximal subgroups $X_1 \neq X_2$ of H containing E. In that case, $E \leq X_1 \cap X_2 = \Phi(H) = \Phi(G) = \mathrm{Z}(G)$, a contradiction. Hence H/E is cyclic. Since $\mathrm{d}(G/E) = 2$, G/E is abelian of type $(2^m, 2)$, $m \geq 1$. Therefore $A/G' \cong G/E$ is of type $(2^m, 2)$, where $A \cap H/G' \cong \mathrm{C}_{2^m}$. Let a be an element in $A \cap H$ such that $\langle a\rangle$ covers $A \cap H/G'$. Noting that $\Omega_1(G) = E$, we have $o(a) = 2^{m+1}$ and $\Omega_1(\langle a\rangle) = \langle z\rangle \leq G'$, where $z = a^{2^m}$. If $t \in E - G'$, then $[t, a] = u \in G' - \langle z\rangle$ because H is nonmetacyclic and therefore u is not a square in H. Since $A/G' \cong \mathrm{C}_{2^m} \times \mathrm{C}_2$, there is an element $b \in A - H$ such that $1 \neq b^2 \in G'$ and $b^2 \neq z$. Indeed, if $b^2 = z$, then taking an element v of order 4 in $\langle a\rangle$, we get $(bv)^2 = b^2v^2 = z^2 = 1$, where $bv \in A - H$, a contradiction. Hence we get that $b^2 \in \{u, uz\}$. We have $\Phi(H) = \Phi(G) = \langle a^2, u\rangle$

and $G = \langle a, b, t\rangle$. If $[b, t] \in \langle u\rangle$, then $G/\langle u\rangle$ is abelian, a contradiction. Hence we obtain $[b, t] \in \{z, uz\}$, $o(b) = 4$ and A is abelian of type $(4, 2^{m+1})$. We set $[b, t] = zu^{\epsilon}$ and $b^2 = uz^{\eta}$, $\epsilon, \eta = 0, 1$.

First suppose that $o(a) > 4$ so that $\langle a^4\rangle \geq \langle z\rangle$. In that case,

$$\Phi(\langle b, t\rangle) = \langle b^2, [b, t]\rangle \leq G' < \Phi(G) = \langle a^2, u\rangle$$

and so $M = \langle b, t\rangle\Phi(G)$. The fact that

$$\Phi(\langle ab, t\rangle) = \langle (ab)^2 = a^2uz^{\eta},\ [ab, t] = zu^{\epsilon+1}\rangle = \Phi(G)$$

gives $\epsilon = 0$. We may assume that $b^2 = u$, i.e., $\eta = 0$. Indeed, if $b^2 = uz = u'$, then we replace $H = \langle a, t\rangle$ with $H_1 = \langle a' = ab, t\rangle$, where $o(a') = o(a)$, $\langle a'\rangle \geq \langle z\rangle$ and $[a', t] = uz = u'$ and so writing again a and u instead of a' and u', respectively, we have obtained the relations for groups G of order 2^{m+4} given in part (c) of our theorem.

It remains to examine the case $o(a) = 4$. In this case, $m = 1$, $a^2 = z$, G is a special group of order 2^5, where $\Phi(G) = \langle u, z\rangle$. We have $A = \langle a, b\rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$ and $\langle a, t\rangle = H$ is the nonmetacyclic minimal nonabelian group of order 2^4. Further,

$$\begin{aligned}
[b, t] &= zu^{\epsilon} \quad \text{with} \quad \Phi(\langle b, t\rangle) = \langle uz^{\eta}, zu^{\epsilon}\rangle,\\
[ab, t] &= zu^{\epsilon+1} \quad \text{with} \quad \Phi(\langle ab, t\rangle) = \langle uz^{\eta+1}, zu^{\epsilon+1}\rangle,\\
[b, at] &= zu^{\epsilon} \quad \text{with} \quad \Phi(\langle b, at\rangle) = \langle uz^{\eta}, uz, zu^{\epsilon}\rangle\\
\text{and} \quad [ab, at] &= zu^{\epsilon+1} \quad \text{with} \quad \Phi(\langle ab, at\rangle) = \langle uz^{\eta+1}, uz, zu^{\epsilon+1}\rangle.
\end{aligned}$$

If $\epsilon = \eta = 0$, then $\Phi(\langle ab, t\rangle) = \langle uz\rangle$ and $\Phi(\langle ab, at\rangle) = \langle uz\rangle$. In case $\epsilon = \eta = 1$, we get $\Phi(\langle b, t\rangle) = \langle uz\rangle$ and $\Phi(\langle b, at\rangle) = \langle uz\rangle$. It follows that in the above two cases our group G has two distinct maximal subgroups which are neither abelian nor minimal nonabelian, a contradiction. Therefore we must have $\epsilon \neq \eta$ in which case we may set $\eta = \epsilon + 1$. But in this case, we check that each nonabelian maximal subgroup of G is minimal nonabelian and so G would be an $\mathcal{A}_2$-group, a contradiction.

(ii) Assume that $\Omega_1(G) = E \not\leq \mathrm{Z}(G) = \Phi(G)$ and $E \leq A$, where A is the unique abelian maximal subgroup of G.

Since there are three maximal subgroups of G containing E, there is a maximal subgroup H of G containing E which is minimal nonabelian. Then H is nonmetacyclic with $\mathrm{Z}(H) \cap E = G'$ and H/E is cyclic. Taking an element $b \in E - G'$, we may set

$$H = \langle a, b \mid a^{2^{\alpha}} = b^2 = 1,\ \alpha \geq 2,\ [a, b] = c,\ c^2 = [a, c] = [b, c] = 1\rangle,$$

where $\langle c\rangle = H'$, $\mathrm{Z}(H) = \langle c\rangle \times \langle a^2\rangle$, $|G| = 2^{\alpha+3}$, and setting $a^{2^{\alpha-1}} = z$ we have $G' = \langle z, c\rangle \cong \mathrm{E}_4$ since c is not a square in H. Here $\langle a, c\rangle$ (containing G') is an abelian normal subgroup of type $(2^{\alpha}, 2)$ in G having exactly two cyclic subgroups $\langle a\rangle$ and $\langle ac\rangle$ of order 2^{α}. Since $a^b = ac$, we obtain that $\mathrm{N}_H(\langle a\rangle) = \langle a, c\rangle$ which implies that

$N = \mathrm{N}_G(\langle a\rangle)$ covers G/H and $N \cap H = \langle a, c\rangle$. It follows that N is a nonabelian maximal subgroup of G (because $A \geq E$), where $N/G' \cong G/E$ is noncyclic abelian and so N/G' is of type $(2, 2^\alpha)$. Hence there is $d \in N - H$ with $1 \neq d^2 \in G'$ and so $o(d) = 4$. But d normalizes $\langle a\rangle$ and therefore $[d, a] \in \langle a\rangle \cap G' = \langle z\rangle$ which gives $[d, a] = z$. There exist exactly three maximal subgroups of G containing E: $H = \langle a, b\rangle$, $\langle d, b\rangle\Phi(H)$, $\langle ad, b\rangle\Phi(H)$, where exactly one of two last subgroups is abelian. It follows that either $[d, b] = 1$ or $[ad, b] = 1$ in which case $[d, b] = c$ (since $[a, b] = c$). We may set $[d, b] = c^\epsilon$, where $\epsilon = 0, 1$, and note that $G = \langle a, b, d\rangle$.

First assume that $\alpha \geq 3$. If $d^2 = z$, then $\langle d, a\rangle \cong \mathrm{M}_{2^{\alpha+1}}$ and there are involutions in $\langle d, a\rangle - \langle a\rangle$, a contradiction. Thus $d^2 \in G' - \langle z\rangle$ in which case $\langle d, a^{2^{\alpha-2}}\rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$ since $a^{2^{\alpha-2}} \in \mathrm{Z}(G)$. Hence, replacing d with $da^{2^{\alpha-2}}$ (if necessary), we may assume that $d^2 = c$. If $\epsilon = 0$, then $A = \langle d, b\rangle\Phi(G)$ is an abelian maximal subgroup of G and we check that all other six maximal subgroups of G are minimal nonabelian and so G is an A_2-group, a contradiction. Hence we must have $\epsilon = 1$. We have $[b, d] = c$ and $\Phi(\langle b, d\rangle) = \langle c\rangle < \Phi(G)$. Also, $[ab, ad] = z$ and

$$\Phi(\langle ab, ad\rangle) = \langle a^2c, a^2cz, z\rangle = \langle a^2c\rangle < \Phi(G)$$

since $(a^2c)^2 = a^4$ and $\langle a^4\rangle \geq \langle z\rangle$. Hence $\langle b, d\rangle\Phi(G)$ and $\langle ab, ad\rangle\Phi(G)$ are two distinct maximal subgroups of G which are neither abelian nor minimal nonabelian, a contradiction.

We have proved that we must have $\alpha = 2$ so that $a^2 = z$, G is special satisfying $\Phi(G) = \langle z, c\rangle$ and $|G| = 2^5$. We have $[d, b] = c^\epsilon$ and if $\epsilon = 1$, then we replace d with $d' = ad$ so that $[d', b] = 1$ and $[a, d'] = z$. Writing again d instead of d', we may assume that $[d, b] = 1$ and $[a, d] = z$ (as before). If $d^2 = z$, then we obtain the group of order 2^5 given in part (d) of our theorem. It remains to analyze the cases $d^2 \in \{c, cz\}$. If $d^2 = c$, then we infer that $\langle b, ad\rangle \cong \mathrm{D}_8$ since $[b, ad] = c$ and $(ad)^2 = a^2d^2[d, a] = zcz = c$. This is a contradiction since $\Omega_1(G) \cong E_8$. Suppose that $d^2 = cz$. In that case, we replace a with $a' = ab$, z with $z' = zc$ and d with $d' = db$. Then we get

$$a'^2 = (ab)^2 = zc = z', \quad d'^2 = (db)^2 = d^2 = cz = z', \quad [a', b] = [ab, b] = c,$$
$$[a', d'] = [ab, db] = zc = z', \quad [b, d'] = [b, db] = 1,$$

and so, writing again a, z, d instead of a', z', d', respectively, we obtain again the group given in part (d) of our theorem.

(iii) We turn now to the difficult case, where $\Omega_1(G) = E \leq \mathrm{Z}(G) = \Phi(G)$.

Let $H_1 = H$ be a maximal subgroup of G which is minimal nonabelian and such that $H' \neq M'$. Since $\mathrm{Z}(H) = \mathrm{Z}(G) \geq E$, H is nonmetacyclic and we may set

$$H = \langle a, b \mid a^{2^\alpha} = b^{2^\beta} = 1,\ [a, b] = c,\ c^2 = [a, c] = [b, c] = 1\rangle,$$

where $\alpha \geq 2$, $\beta \geq 2$, $\langle c\rangle = H'$, $\mathrm{Z}(H) = \Phi(G) = \langle c\rangle \times \langle a^2\rangle \times \langle b^2\rangle$ is abelian of type $(2^{\alpha-1}, 2^{\beta-1}, 2)$, and $|G| = 2^{\alpha+\beta+2}$. We have $G' < E = \langle a^{2^{\alpha-1}}, a^{2^{\beta-1}}, c\rangle \cong \mathrm{E}_8$.

We consider the group G/M', where $(G/M')' = G'/M' \cong \mathrm{C}_2$, $\mathrm{d}(G/M') = 3$, G/M' has exactly three abelian maximal subgroups A/M', M/M' and H_5/M' (since $H_5' = M'$) and the other four maximal subgroups H_i/M', $i = 1, \ldots, 4$, are minimal nonabelian. Thus G/M' is an A_2-group of Proposition 71.1 which implies that there is an element $d \in G - H$ such that $[d, G] = M'$ and $1 \neq d^2 \in G'$. Since there are exactly three maximal subgroups of G containing $\langle d \rangle \cong \mathrm{C}_4$, at least one of them H^* is minimal nonabelian, where $H^* \geq E$ and so H^* is nonmetacyclic. Thus $(H^*)'$ is a maximal cyclic subgroup in H^* and so $(H^*)' \neq \langle d^2 \rangle$ which gives $G' = \langle (H^*)', d^2 \rangle$. Taking an element $a^* \in (H \cap H^*) - \Phi(G)$, we conclude that $H^* = \langle a^*, d \rangle$ and so $\Phi(H^*) = \langle (a^*)^2, d^2, (H^*)' \rangle = \langle (a^*)^2, G' \rangle = \Phi(G)$ and $E = \langle \Omega_1(\langle a^* \rangle), G' \rangle$. Set $o(a^*) = 2^\gamma$, $\gamma \geq 2$, so that $\Phi(H^*) = \Phi(G)$ is of type $(2^{\gamma-1}, 2, 2)$. On the other hand, $\Phi(G)$ is of type $(2^{\alpha-1}, 2^{\beta-1}, 2)$. Interchanging the elements a and b (if necessary), we may assume that $\beta = 2$ and then $\gamma = \alpha$ so that $\Phi(G)$ is of type $(2^{\alpha-1}, 2, 2)$ and $o(b) = 4$. Since $[d, G] = M'$, we have $\langle [d, a^*] \rangle = M'$ and so $(H^*)' = M'$ and therefore $H^* = H_5$ and $d^2 \in G' - M'$. Because H^*/E is abelian of type $(2^{\alpha-1}, 2)$, it follows that $H \cap H^*/E$ is cyclic of order $2^{\alpha-1}$ and so $\langle a^* \rangle$ covers $H \cap H^*/E$. Since $H \cap H^* = \langle a^* \rangle \times G'$, it follows that H/G' is abelian of type $(2^\alpha, 2)$ which implies that $H = H_0(H \cap H^*)$ with $H_0 \cap (H \cap H^*) = G'$ and $|H_0 : G'| = 2$. Hence there is an element $b^* \in H - H^*$ with $1 \neq (b^*)^2 \in G'$, $\langle a^*, b^* \rangle = H$, $(b^*)^2 \neq c$ (since $H' = \langle c \rangle$ and so c is not a square in H) and so $[a^*, b^*] = c$ and $o(b^*) = 4$. In addition, from $[d, G] = M'$ follows that either $[d, b^*] = m$ with $\langle m \rangle = M'$ or $[d, b^*] = 1$. Also $d^2 = cm^\epsilon$ and $(b^*)^2 = c^\eta m$, where $\epsilon, \eta = 0, 1$.

Assume that $[d, b^*] = 1$ in which case $d^2 \neq (b^*)^2$ (because if $d^2 = (b^*)^2$, then db^* is an involution in $G - H$, a contradiction) and so $\langle d, b^* \rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$ and $\langle d^2, (b^*)^2 \rangle = G'$. In that case, $[b^*a^*, d] = m$ since $[a^*, d] = m$ and we get

$$\begin{aligned}\Phi(\langle b^*a^*, d \rangle) &= \langle (b^*a^*)^2 = c^\eta m \cdot (a^*)^2 \cdot c = (a^*)^2 c^{\eta+1} m, d^2 = cm^\epsilon, m \rangle \\ &= G' \langle (a^*)^2 \rangle = \Phi(G),\end{aligned}$$

and so $\langle b^*a^*, d \rangle$ is a minimal nonabelian maximal subgroup of G which satisfies $\langle b^*a^*, d \rangle' = \langle m \rangle$ and $\langle b^*a^*, d \rangle \neq H^*$. This is a contradiction since $H^* = H_5$ is the only maximal subgroup of G which is minimal nonabelian and $(H^*)' = M' = \langle m \rangle$.

We have proved that $[d, b^*] = m$ which together with $\langle b^*, d \rangle \neq H^*$ implies that $\langle b^*, d \rangle \Phi(G) = M$ must be the unique maximal subgroup of G which is neither abelian nor minimal nonabelian. If $\epsilon = 0$ and $\eta = 1$, then $(b^*)^2 = cm$, $d^2 = c$ and therefore $(b^*d)^2 = cm \cdot c \cdot m = 1$ and b^*d would be an involution in $G - H$, a contradiction. Hence we have either $\epsilon = \eta$ or $\epsilon = 1$ and $\eta = 0$. In this case, $[a^*, b^*d] = cm$ and $\Phi(\langle a^*, b^*d \rangle) = \langle (a^*)^2, c^{\eta+1} m^\epsilon, cm \rangle = \Phi(G)$ implies that $\epsilon = 1$ and $\eta = 0$ is not possible and so $\epsilon = \eta$. Further, we have $[b^*, a^*d] = cm$ and so $\Phi(\langle b^*, a^*d \rangle) = \langle c^\epsilon m, (a^*)^2 cm^{\epsilon+1}, cm \rangle$ forces that $\epsilon = \eta = 0$. But then $[a^*b^*, a^*d] = c$ shows together with $\Phi(\langle a^*b^*, a^*d \rangle) = \langle (a^*)^2 cm, c \rangle < \Phi(G)$ that $\langle a^*b^*, a^*d \rangle \Phi(G)$ is another maximal subgroup of G which is neither abelian nor minimal nonabelian, a contradiction. Our theorem is proved. □

Theorem 100.6. *Let G be a 2-group with $\mathrm{d}(G) = 3$ which has exactly one maximal subgroup M which is neither abelian nor minimal nonabelian. If G has no abelian maximal subgroups, then we get*

$$\begin{aligned} G = \langle a, b, c \mid\ & a^4 = b^4 = c^{2^n} = 1,\ a^2 = x,\ b^2 = y,\ c^{2^{n-1}} = z, \\ & [a,b] = z,\ [a,c] = y,\ [b,c] = xy, \\ & [x,b] = [x,c] = [y,a] = [y,c] = [z,a] = [z,b] = 1\rangle, \end{aligned}$$

where $|G| = 2^{n+4}$, $n \geq 3$, $G' = \langle x, y, z\rangle \cong \mathrm{E}_8$, $\mathrm{Z}(G) = \Phi(G) = G'\langle c^2\rangle$ is abelian of type $(2^{n-1}, 2, 2)$, $M = \Phi(G)\langle a, b\rangle = \langle c^2\rangle * \langle a, b\rangle$ with $\langle c^2\rangle \cap \langle a, b\rangle = \langle z\rangle = \langle a, b\rangle'$, $\langle c^2\rangle \cong \mathrm{C}_{2^{n-1}}$ and $\langle a, b\rangle$ is the nonmetacyclic minimal nonabelian group of exponent 4 and order 2^5 and the other six maximal subgroups of G are nonmetacyclic minimal nonabelian.

Proof. We put $\Gamma_1 = \{H_1, H_2, \ldots, H_6, M\}$ to be the set of maximal subgroups of G, where $H_1, \ldots, H_6$ are minimal nonabelian. We know that $|M'| = 2$ and $\mathrm{d}(M) \geq 3$ (see the remark preceding Theorem 100.5). By a result of A. Mann, $|G' : (H_1'H_2')| \leq 2$ and so $|G'| \leq 8$. However, if $|G'| = 2$, then we know that G has three abelian maximal subgroups (see the second paragraph of the proof of Theorem 100.4), a contradiction. Hence $|G'| = 4$ or $|G'| = 8$.

Suppose that for some $H_i \neq H_j$ we have $H_i' = H_j'$. Then by a result of A. Mann, we get $|G'| = 4$ and moreover $G' \cong \mathrm{E}_4$. Indeed, if $G' \cong \mathrm{C}_4$, then the nonabelian group $G/\Omega_1(G')$ would possess at least six abelian maximal subgroups $H_i/\Omega_1(G')$, $i = 1, \ldots, 6$, a contradiction. The group G/M' is obviously an A_2-group satisfying $(G/M')' \cong \mathrm{C}_2$. By Proposition 71.1, G/M' has exactly three abelian maximal subgroups so that we may set $H_5' = H_6' = M' = \langle u\rangle$. In that case, H_i', $i = 1, \ldots, 4$, cannot be all pairwise distinct and so we may set $H_2' = H_3' = H_4' = \langle v\rangle$ with $\langle u, v\rangle = G'$ and $G/\langle v\rangle$ has exactly three abelian maximal subgroups $H_i/\langle v\rangle$, $i = 2, 3, 4$. It follows that we must have $H_1' = \langle uv\rangle$ so that $G/\langle uv\rangle$ with $(G/\langle uv\rangle)' \cong \mathrm{C}_2$ has exactly one abelian maximal subgroup $H_1/\langle uv\rangle$. If $\mathrm{d}(M/\langle uv\rangle) = 2$, then $M/\langle uv\rangle$ is minimal nonabelian so that $G/\langle uv\rangle$ would be an A_2-group. But in that case (Proposition 71.1), $G/\langle uv\rangle$ would have three abelian maximal subgroups, a contradiction. Hence we must have $\mathrm{d}(M/\langle uv\rangle) \geq 3$ in which case $M/\langle uv\rangle$ is a unique maximal subgroup of $G/\langle uv\rangle$ which is neither abelian nor minimal nonabelian. By Theorem 100.5, we must have $(G/\langle uv\rangle)' \cong \mathrm{E}_4$, a contradiction.

We have proved that all H_i' are pairwise distinct subgroups of order 2 in G'. This implies that $G' \cong \mathrm{E}_8$. If $M' = H_i'$ for some $i \in \{1, 2, \ldots, 6\}$, then considering G/M' we see that there must exist a maximal subgroup H_j, $j \neq i$, such that $M' = H_i' = H_j'$, a contradiction. Hence $\{H_1', \ldots, H_6', M'\}$ is the set of seven pairwise distinct subgroups of order 2 in G'. Since $G' \leq H_i$, all H_i ($i = 1, \ldots, 6$) are nonmetacyclic minimal nonabelian. The group G/G' is abelian of rank 3. Suppose that there is an involution $t \in G - G'$. Then $F = G' \times \langle t\rangle \cong \mathrm{E}_{16}$ and G/F is noncyclic. But then there is a maximal subgroup H of G such that $H \geq F$ and H is minimal nonabelian,

a contradiction. We have proved that $G' = \Omega_1(G)$. Set $T/G' = \Omega_1(G/G') \cong \mathrm{E}_8$. If G/T is noncyclic, then there is a maximal subgroup K of G such that $K \geq T$ and K is minimal nonabelian. But then $\mathrm{d}(K/G') = 3$, a contradiction. Hence G/T is cyclic and so G/G' is abelian of type $(2^m, 2, 2)$, $m \geq 1$.

(i) First assume $m = 1$, i.e., $T = G$, $G/G' \cong \mathrm{E}_8$ and G is a special group with $G' = \Omega_1(G) \cong \mathrm{E}_8$.

We shall determine the structure of $M > G'$. We have $M = G'S$, where $S = \langle a, b\rangle$ is minimal nonabelian and $G' \cap S = \Phi(S) < G'$. Set $\langle z\rangle = S' = M' \cong \mathrm{C}_2$. Suppose at the moment that $\Phi(S) = \langle z\rangle$ so that $S \cong \mathrm{Q}_8$. Then $G/\langle z\rangle$ is an A_2-group, where $M/\langle z\rangle \cong \mathrm{E}_{16}$ is a unique abelian maximal subgroup of $G/\langle z\rangle$ and $\mathrm{E}_4 \cong (G/\langle z\rangle)' \leq \mathrm{Z}(G/\langle z\rangle)$. But then Proposition 71.4(b) implies that $\Omega_1(G/\langle z\rangle) \cong \mathrm{E}_8$, a contradiction. We have proved that $\Phi(S) \cong \mathrm{E}_4$ and $\Omega_1(S) = \Phi(S)$. Hence S is the metacyclic minimal nonabelian group of order 16 and exponent 4. We choose $a, b \in S - \Phi(S)$ so that $a^2 = z$, $b^2 = y$, $[a, b] = z$ and $\langle y, z\rangle = \Phi(S) = \Phi(M)$. Since $G' = \Phi(G)$, there is $c \in G - M$ such that $c^2 = x \in G' - \langle y, z\rangle$. We obtain $\langle x, y, z\rangle = G'$ and $\langle a, b, c\rangle = G$. All other six maximal subgroups (distinct from M) are nonmetacyclic minimal nonabelian. We have $\Phi(\langle a, c\rangle) = \langle z, x, [a, c]\rangle = G'$ so that $[a, c] = x^\alpha y z^\beta$. Also, $\Phi(\langle b, c\rangle) = \langle y, x, [b, c]\rangle = G'$ gives $[b, c] = x^\gamma y^\delta z$. Further,

$$\Phi(\langle ab, c\rangle) = \langle y, x, [ab, c] = x^{\alpha+\gamma} y^{\delta+1} z^{\beta+1}\rangle = G'$$

which implies $\beta = 0$. From

$$\Phi(\langle b, ac\rangle) = \langle y, x^{\alpha+1} yz, [b, ac] = x^\gamma y^\delta\rangle = G'$$

we get $\gamma = 1$, and from

$$\Phi(\langle ab, ac\rangle) = \langle y, x^{\alpha+1} yz, [ab, ac] = x^{\alpha+1} y^{\delta+1}\rangle = G'$$

it follows $\alpha = 0$. Finally,

$$\Phi(\langle a, bc\rangle) = \langle z, y^{\delta+1} z, [a, bc] = zy\rangle = \langle y, z\rangle < G'$$

gives a contradiction since $G'\langle a, bc\rangle$ is another maximal subgroup of G (distinct from the subgroup M) which is neither abelian nor minimal nonabelian.

(ii) Suppose that $T < G$, where $T/G' = \Omega_1(G/G') \cong \mathrm{E}_8$ and $\{1\} \neq G/T$ is cyclic so that G/G' is abelian of type $(2^m, 2, 2)$, $m \geq 2$.

The unique maximal subgroup of G containing T must be equal to M. There are normal subgroups U and V of G such that $G = UV$, $U \cap V = G'$, $U/G' \cong \mathrm{E}_4$ and V/G' is cyclic of order 2^m, $m \geq 2$. Let c be an element in $V - G'$ such that $\langle c\rangle$ covers V/G'. We have $o(c) = 2^n$, $n \geq 3$, where $n = m+1$ (noting that $\Omega_1(G) = G'$). Set $\langle z\rangle = \Omega_1(\langle c\rangle)$ so that $z = c^{2^{n-1}}$ and $z \in G'$. Then we conclude that $M = U\langle c^2\rangle$, $\Phi(G) = \mathrm{Z}(G) = G'\langle c^2\rangle$ is abelian of type $(2^{n-1}, 2, 2)$ and $|G| = 2^{n+4}$. Suppose that $a, b \in U - G'$ satisfy $U = G'\langle a, b\rangle$, where $a^2, b^2 \in G'$ and $G = \langle a, b, c\rangle$. Since each maximal subgroup H_i $(i = 1, \ldots, 6)$ is nonmetacyclic and contains $\Phi(G)$ and z

is a square in $\Phi(G)$, it follows that $H_i' \neq \langle z\rangle$ for all $i = 1, \ldots, 6$. This implies that $M' = \langle z\rangle$ and therefore $[a, b] = z$.

Now, $G/\langle z\rangle$ has the unique maximal abelian subgroup $M/\langle z\rangle$ and six minimal nonabelian maximal subgroups $H_i/\langle z\rangle$, $i = 1, \ldots, 6$, and so $G/\langle z\rangle$ is an A_2-group with the following properties. We have $d(G/\langle z\rangle) = 3$ and so $G/\langle z\rangle$ is nonmetacyclic of order $2^{n+3} > 2^4$ since $n \geq 3$, $(G/\langle z\rangle)' \cong E_4$, $G'/\langle z\rangle \leq Z(G/\langle z\rangle)$ (as $G' \leq Z(G)$) and $G/\langle z\rangle$ has a normal elementary abelian subgroup $\langle G', \Omega_2(\langle c\rangle)\rangle/\langle z\rangle$ of order 8. Hence $G/\langle z\rangle$ is an A_2-group from Proposition 71.4(b) which implies the fact that $\langle G', \Omega_2(\langle c\rangle)\rangle/\langle z\rangle = \Omega_1(G/\langle z\rangle)$. Set $a^2 = x$ and $b^2 = y$ and consider the abelian group $M/\langle z\rangle$. If the abelian subgroup $U/\langle z\rangle$ of order 16 and exponent ≤ 4 has rank greater than 2, then we get $\Omega_1(U/\langle z\rangle) > G'/\langle z\rangle$, which contradicts the above fact. Hence we must have $U/\langle z\rangle \cong C_4 \times C_4$ which implies that $G' = \langle x, y, z\rangle$. Since all H_i are minimal nonabelian (containing $\Phi(G) = \langle c^2, x, y\rangle$), we get $[a, c] = x^\alpha y z^\beta$ and $[b, c] = x y^\gamma z^\delta$, where $\alpha, \beta, \gamma, \delta = 0, 1$. From

$$\Phi(\langle ab, c\rangle) = \langle (ab)^2 = xyz, c^2, [ab, c] = x^{\alpha+1} y^{\gamma+1} z^{\beta+\delta}\rangle = \Phi(G)$$

and the fact that $\Omega_1(\langle c^2\rangle) = \langle z\rangle$ it follows that $\alpha + 1 \neq \gamma + 1$ which gives $\gamma = \alpha + 1$ and $[b, c] = x y^{\alpha+1} z^\delta$.

Interchanging a and b respectively x and y, i.e., writing $a' = b$, $b' = a$, $x' = y$, $y' = x$, we get

$$\begin{aligned} a'^2 = b^2 = y = x', \quad b'^2 = a^2 = x = y', \\ [a', b'] = [b, a] = z, \\ [a', c] = [b, c] = x y^{\alpha+1} z^\delta = (x')^{\alpha+1} y' z^\delta, \\ [b', c] = [a, c] = x^\alpha y z^\beta = x' y'^\alpha z^\beta. \end{aligned}$$

Writing again a, b, x, y instead of a', b', x', y', respectively, we obtain

$$\begin{gathered} a^2 = x, \quad b^2 = y, \quad [a, b] = z, \\ [a, c] = x^{\alpha+1} y z^\delta, \quad [b, c] = x y^\alpha z^\beta, \quad \beta, \delta = 0, 1, \end{gathered}$$

which are the old relations in which α is replaced with $\alpha + 1$. This shows that we may assume $\alpha = 0$ and so we get $[a, c] = y z^\beta$ and $[b, c] = x y z^\delta$, $\beta, \delta = 0, 1$.

Finally, replacing c with $c' = c a^\delta b^\beta$, we get

$$c'^2 = c^2 (a^\delta b^\beta)^2 [a^\delta b^\beta, c] = c^2 l$$

with $l \in G'$ and so $c'^4 = c^4$, $\langle c'\rangle$ covers G/U and $\langle c'\rangle \cap G' = \langle z\rangle$. In addition, we have

$$\begin{aligned} [a, c'] = [a, c a^\delta b^\beta] = [a, c][a, b]^\beta = y z^\beta z^\beta = y, \\ [b, c'] = [b, c a^\delta b^\beta] = [b, c][b, a]\delta = x y z^\delta z^\delta = x y. \end{aligned}$$

Writing again c instead of c', we obtain the relations stated in our theorem. □

§102

p-groups G with $p > 2$ and $\mathrm{d}(G) > 2$ having exactly one maximal subgroup which is neither abelian nor minimal nonabelian

In this section we determine up to isomorphism the title groups (Theorems 102.1, 102.3 and 102.5). It is obvious that for such groups G we have $\mathrm{d}(G) = 3$. All resulting groups will be presented in terms of generators and relations. But we shall also state all important characteristic subgroups of these groups so that the results could be useful for applications. In §§100, 101 and 102 the difficult problem Nr. 861 stated by the first author is completely solved.

Theorem 102.1. *Let G be a p-group, $p > 2$, which possesses exactly one maximal subgroup which is neither abelian nor minimal nonabelian. Suppose that* $\mathrm{d}(G) = 3$ *and G has more than one abelian maximal subgroup. Then we have one of the following possibilities:*

(a) $G = U * Z$, *where* $U \cong \mathrm{S}(p^3)$, $Z \cong \mathrm{C}_{p^m}$, $m \geq 3$, *and* $U \cap Z = \mathrm{Z}(U)$. *Here G is an* L_3*-group.*

(b) $G = U \times Z$, *where* $U \cong \mathrm{S}(p^3)$ *or* $U \cong \mathrm{M}_{p^3}$ *and* $Z \cong \mathrm{C}_{p^m}$, $m \geq 2$.

Conversely, the groups in (a) *and* (b) *satisfy the assumptions of our theorem.*

Proof. Our assumptions imply that $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ and G has exactly $p + 1$ abelian maximal subgroups (Exercise 1.6(a)). By Lemma 1.1, $|G| = p|G'||\mathrm{Z}(G)|$ gives that $|G'| = p$.

Conversely, assume that G is a title group with $|G'| = p$. Since G has at most $p+1$ abelian maximal subgroups, there is a minimal nonabelian maximal subgroup H. From $|G'| = p$ we conclude that $G = H\mathrm{C}_G(H)$ (Exercise P10), where $H \cap \mathrm{C}_G(H) = \mathrm{Z}(H) = \Phi(H) = \Phi(G)$ and $\mathrm{C}_G(H) = \mathrm{Z}(G)$. We have $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ and so all $p + 1$ maximal subgroups of G containing $\mathrm{Z}(G)$ are abelian.

In what follows H will denote a fixed maximal subgroup of G which is minimal nonabelian. Suppose that there exists an element $c \in \mathrm{Z}(G) - H$ of order p. Then we have $G = H \times \langle c \rangle$ and so each maximal subgroup of G which does not contain $\langle c \rangle$ is isomorphic to $G/\langle c \rangle \cong H$ and so is minimal nonabelian, a contradiction. Hence there are no elements of order p in $\mathrm{Z}(G) - H$ which implies $\Omega_1(\mathrm{Z}(H)) = \Omega_1(\mathrm{Z}(G))$ so that $\mathrm{d}(\mathrm{Z}(H)) = \mathrm{d}(\mathrm{Z}(G))$. It follows that for each $x \in \mathrm{Z}(G) - H$, $x^p \in \mathrm{Z}(H) - \Phi(\mathrm{Z}(H))$.

Obviously, $|G| \geq p^5$ since the exceptional maximal subgroup M (which is neither abelian nor minimal nonabelian) is of order $\geq p^4$.

(i) First assume that H is metacyclic. We may set

$$\langle a, b \mid a^{p^m} = b^{p^n} = 1,\ a^b = az,\ z = a^{p^{m-1}} \rangle,$$

where $m \geq 2, n \geq 1, m+n \geq 4$, $H' = \langle z \rangle = G'$, $|H| = p^{m+n}$, and $|G| = p^{m+n+1}$. We see that $\mathrm{Z}(H) = \langle a^p \rangle \times \langle b^p \rangle = \Phi(H) = \Phi(G)$ and for each $x \in \mathrm{Z}(G) - H$, $x^p \in \langle a^p, b^p \rangle - \langle a^{p^2}, b^{p^2} \rangle$ since $\langle a^{p^2}, b^{p^2} \rangle = \Phi(\mathrm{Z}(H))$.

Suppose that $n = 1$ so that $o(b) = p$, $m \geq 3$, $H \cong \mathrm{M}_{p^{m+1}}$ and $\mathrm{Z}(H) = \langle a^p \rangle$. Here $\mathrm{Z}(G) \cong \mathrm{C}_{p^m}$ is cyclic and so there is $c \in \mathrm{Z}(G) - H$ such that $c^p = a^{-p}$ which gives $(ca)^p = c^p a^p = 1$ and $o(ca) = p$. Since $[ca, b] = z$, it follows that $U = \langle ca, b \rangle \cong \mathrm{S}(p^3)$, $U \cap \mathrm{Z}(G) = \langle z \rangle$ which together with $|G : \mathrm{Z}(G)| = p^2$ gives $G = U\mathrm{Z}(G)$. We have obtained the groups stated in part (a) of our theorem. Here $M = U * \langle c^p \rangle$, all $p+1$ maximal subgroups of G containing $\langle c \rangle$ are abelian and we have to show that all subgroups $\langle c^i a, c^j b \rangle$ are minimal nonabelian maximal subgroups of G for all integers $i, j \pmod p$ unless $i \equiv 1 \pmod p$ and $j \equiv 0 \pmod p$. Indeed, $[c^i a, c^j b] = [a, b] = z$ and so, by Exercise P9, $\langle c^i a, c^j b \rangle$ is minimal nonabelian and

$$\begin{aligned}\Phi(\langle c^i a, c^j b \rangle) &= \langle (c^i a)^p = c^{pi} a^p = a^{-pi} a^p = a^{p(-i+1)},\ (c^j b)^p = a^{-pj},\ z \rangle \\ &= \langle a^p \rangle = \Phi(G)\end{aligned}$$

if and only if either $i \not\equiv 1 \pmod p$ or $j \not\equiv 0 \pmod p$.

It remains to treat the case $n \geq 2$. Suppose, in addition, that there exists an element $x \in G - H$ of order p. We know that $x \notin \mathrm{Z}(G)$ and so $[a, x] \neq 1$ or $[b, x] \neq 1$. Obviously, $\langle a, b, x \rangle = G$.

First suppose $[a, x] \neq 1$. Since $\langle a \rangle \trianglelefteq G$, $\langle a, x \rangle \cong \mathrm{M}_{p^{m+1}}$ is minimal nonabelian of order p^{m+1}. But $|G| = p^{m+n+1}$ and $n \geq 2$ which implies that $M = \Phi(G)\langle a, x \rangle = \langle a, x \rangle \times \langle b^p \rangle$ is a maximal subgroup of G which is neither abelian nor minimal nonabelian. Assume at the moment that also $[x, b] \neq 1$. In that case, we get $\langle b \rangle \times \langle z \rangle \trianglelefteq G$ and so $\langle b, x \rangle$ is nonmetacyclic minimal nonabelian of order p^{n+2}. Then it follows that $\langle b, x \rangle$ must be a maximal subgroup of G with $|G| = p^{n+3}$ (and so $m = 2$). But this case will be studied in part (ii) of this proof (where G possesses a nonmetacyclic minimal nonabelian maximal subgroup). Hence we may assume $[x, b] = 1$. This gives $[x, ab] = [x, a] = z^r$, $r \not\equiv 0 \pmod p$ and so $\langle x, ab \rangle$ is minimal nonabelian which forces that $\langle x, ab \rangle$ must be a maximal subgroup of G. Now, $\langle ab \rangle$ covers $H/\langle a \rangle \cong \mathrm{C}_{p^n}$ and so $o(ab) \geq p^n$, where $n \geq 2$. We have $(ab)^{p^n} = a^{p^n} b^{p^n} = a^{p^n}$. If $n \geq m$, then $o(ab) = p^n$ and $\langle ab \rangle \cap \langle a \rangle = \{1\}$. Since $\langle ab, z \rangle \trianglelefteq G$, we see that $\langle ab, x \rangle$ is a nonmetacyclic minimal nonabelian subgroup of order p^{n+2}. In that case, $\langle ab, x \rangle$ must be a maximal subgroup of G (with $m = 2$) and again this will be studied in part (ii) of the proof. It follows that we may assume $n < m$. In that case, $o(ab) = p^m$ and $\langle ab \rangle \geq \langle z \rangle$ so that $\langle ab \rangle \trianglelefteq G$. Hence $\langle ab, x \rangle$ is metacyclic minimal nonabelian of order p^{m+1} and so $\langle ab, x \rangle$ must be a maximal subgroup of G. From $|G| = p^{m+n+1}$ follows $n = 1$, contrary to our assumption.

We may assume that $[a, x] = 1$ and then $[b, x] \neq 1$. Since $\langle b\rangle \times \langle z\rangle \trianglelefteq G$, $\langle b, x\rangle$ is nonmetacyclic minimal nonabelian of order p^{n+2}. If $\langle b, x\rangle$ is a maximal subgroup of G, then this case will be treated in part (ii) of this proof. Thus we may assume that $\langle b, x\rangle$ is not a maximal subgroup of G and so $M = \Phi(G)\langle b, x\rangle$ with $m > 2$. It follows that $\langle ab, x\rangle$, which is minimal nonabelian, must be a maximal subgroup of G. Since $\langle ab\rangle$ covers $H/\langle a\rangle$, we obtain that $o(ab) \geq p^n$, $n \geq 2$, and $(ab)^{p^n} = a^{p^n}$. If $n \geq m$, then $o(ab) = p^n$ and $\langle ab\rangle \cap \langle a\rangle = \{1\}$ and so $\langle ab, x\rangle$ is nonmetacyclic minimal nonabelian of order p^{n+2}. In that case, $\langle ab, x\rangle$ must be a maximal subgroup of G with $m = 2$, a contradiction. We may assume that $n < m$ and then $o(ab) = p^m$ with $\langle ab\rangle \geq \langle z\rangle$ and so $\langle ab, x\rangle$ is metacyclic minimal nonabelian of order p^{m+1}. But then $|G| = p^{m+n+1}$ implies $n = 1$, contrary to our assumption.

Therefore we may assume that there are no elements of order p in $G - H$. We know that for an element $c^{-1} \in \mathrm{Z}(G) - H$, $c^{-p} \in \mathrm{Z}(H) - \Phi(\mathrm{Z}(H))$ and so c^{-p} is not a p-th power of any element in $\mathrm{Z}(H)$. But $\mathfrak{V}_1(H) = \mathrm{Z}(H) \geq H' = \langle z\rangle$ and so H is a powerful group. Then $c^{-p} = h^p$ for some element $h \in H - \mathrm{Z}(H)$ (see Proposition 26.10). It follows $hc \in G - H$ and $(hc)^p = h^p c^p = 1$ and so hc is of order p, a contradiction.

(ii) It remains to consider the case where H is nonmetacyclic minimal nonabelian. We may set

$$\langle a, b \mid a^{p^m} = b^{p^n} = 1,\ [a, b] = z,\ z^p = [a, z] = [b, z] = 1\rangle,$$

where we may assume $m \geq 2$, $n \geq 1$ since $|G| \geq p^5$. Here we have $H' = \langle z\rangle$, $|H| = p^{m+n+1}$, and $|G| = p^{m+n+2}$. Also, $\langle z\rangle$ is a maximal cyclic subgroup in H, $\mathrm{Z}(H) = \langle a^p\rangle \times \langle b^p\rangle \times \langle z\rangle = \Phi(H) = \Phi(G)$ and for each $x \in \mathrm{Z}(G) - H$ we have $x^p \in \mathrm{Z}(H) - \Phi(\mathrm{Z}(H))$.

(ii1) First assume $n = 1$ so that $\mathrm{Z}(H) = \langle a^p\rangle \times \langle z\rangle$ and for an element $c \in \mathrm{Z}(G) - H$ we have $c^p = a^{pr} z^s$, where both integers r, s are not divisible by p. Suppose that $r \equiv 0 \pmod p$ and then $s \not\equiv 0 \pmod p$. Replacing c with another suitable generator of $\langle c\rangle$, we may assume that $c^p = a^{p^2 r'} z$ for some integer r'. Take the element $c' = a^{-pr'} c \in \mathrm{Z}(G) - H$; then we get $(c')^p = a^{-p^2 r'} c^p = z$. Thus $G = H * \langle c'\rangle$ with $(c')^p = z$ and $\langle z\rangle = H'$ and so we have obtained a p-group from Proposition 71.1(ii) which is an A_2-group, a contradiction. We have proved that $c^p = a^{pr} z^s$ with $r \not\equiv 0 \pmod p$. Set $a' = a^{-r}$ so that

$$o(a') = p^m, \quad [a', b] = z^{-r} \quad \text{and} \quad (ca')^p = c^p (a')^p = z^s,$$

where $\langle a', b\rangle = H$. Consider the subgroup $U = \langle ca', b\rangle$. Since $[ca', b] = z^{-r}$ and $o(b) = p$, we have in case $s \not\equiv 0 \pmod p$ that $U \cong \mathrm{M}_{p^3}$ and in case $s \equiv 0 \pmod p$ that $U \cong \mathrm{S}(p^3)$. However, $c^p = (a')^{-p} z^s$, $G = \langle a', b, c\rangle$, $o(c) = p^m$, $m > 1$, and $\langle c\rangle \cap U = \{1\}$ and so we get $G = U \times \langle c\rangle$ which are the groups stated in part (b) of our theorem. Here $M = U \times \langle c^p\rangle$ and all $p + 1$ maximal subgroups containing $\langle c\rangle$ are abelian.

We have to show that all subgroups $\langle c^i a', c^j b\rangle$ are minimal nonabelian maximal subgroups of G (not containing $\langle c\rangle$) for all integers $i, j \pmod p$ unless $i \equiv 1 \pmod p$ and $j \equiv 0 \pmod p$ holds. Indeed, $[c^i a', c^j b] = [a', b] = z^{-r}$ and

$$\begin{aligned}\Phi(\langle c^i a', c^j b\rangle) &= \langle c^{pi}(a')^p = a^{pri} z^{si} a^{-pr} = a^{pr(i-1)} z^{si},\ c^{pj} = a^{prj} z^{sj},\ z^{-r}\rangle \\ &= \Phi(G) = \Phi(H)\end{aligned}$$

if either $i \not\equiv 1 \pmod p$ or $j \not\equiv 0 \pmod p$.

(ii2) It remains to consider the case $n \geq 2$. In this case, for an element $c \in \mathrm{Z}(G) - H$ we have $c^p = a^{pi} b^{pj} z^k$, where at least one of the integers i, j, k is $\not\equiv 0 \pmod p$.

First suppose that $i \equiv 0 \pmod p$ and $j \equiv 0 \pmod p$ so that $k \not\equiv 0 \pmod p$. We may define $c^p = a^{p^2 i'} b^{p^2 j'} z^k$ for some integers i', j'. Considering the element $c' = a^{-pi'} b^{-pj'} c \in \mathrm{Z}(G) - H$, we get

$$(c')^p = a^{-p^2 i'} b^{-p^2 j'} c^p = z^k, \quad k \not\equiv 0 \pmod p,$$

and so $G = H * \langle c'\rangle$ with $\langle c'\rangle \cap H = \langle z\rangle = H'$ and this is an A_2-group from Proposition 71.1(ii), a contradiction.

Now assume that one and only one of the integers i, j is $\equiv 0 \pmod p$. Because of the symmetry, we may assume $i \not\equiv 0 \pmod p$ and $j \equiv 0 \pmod p$. We have

$$\Phi(\langle a^{-i} b^{-j} c, b\rangle) = \langle a^{-pi} b^{-pj} c^p = z^k,\ b^p,\ [a^{-i} b^{-j} c, b] = z^{-i} \neq 1\rangle < \Phi(G)$$

and

$$\Phi(\langle ab, a^r c\rangle) = \langle a^p b^p,\ a^{pr} c^p = a^{p(i+r)} b^{pj} z^k,\ [ab, a^r c] = z^{-r} \neq 1\rangle < \Phi(G)$$

for some suitable $r \not\equiv 0 \pmod p$ such that $i + r \equiv 0 \pmod p$. Hence we deduce that $\Phi(G)\langle a^{-i} b^{-j} c, b\rangle$ and $\Phi(G)\langle ab, a^r c\rangle$ are two distinct maximal subgroups of G which are neither abelian nor minimal nonabelian, a contradiction.

Finally, we consider the case where both i and j are $\not\equiv 0 \pmod p$. We have

$$\Phi(\langle a^{-i} b^{-j} c, b\rangle) = \langle a^{-pi} b^{-pj} c^p = z^k,\ b^p,\ [a^{-i} b^{-j} c, b] = z^{-i} \neq 1\rangle < \Phi(G)$$

and

$$\Phi(\langle a, b^r c\rangle) = \langle a^p,\ b^{pr} c^p = a^{pi} b^{p(j+r)} z^k,\ [a, b^r c] = z^r \neq 1\rangle < \Phi(G)$$

for some suitable $r \not\equiv 0 \pmod p$ such that $j + r \equiv 0 \pmod p$. Hence we deduce that $\Phi(G)\langle a^{-i} b^{-j} c, b\rangle$ and $\Phi(G)\langle a, b^r c\rangle$ are two distinct maximal subgroups of G which are neither abelian nor minimal nonabelian, a contradiction. Our theorem is proved. □

Lemma 102.2. *Let G be a p-group, $p > 2$, which possesses exactly one maximal subgroup M which is neither abelian nor minimal nonabelian. Suppose that* $\mathrm{d}(G) = 3$ *and G has at most one abelian maximal subgroup. Then $\Phi(G) = \mathrm{Z}(G) = \Phi(H)$ for each minimal nonabelian maximal subgroup H of G. Also, $|G'| > p$, $|M'| = p$ and* $\mathrm{d}(M) \geq 3$ *which implies $|G| \geq p^5$.*

Proof. From the first two paragraphs of the proof of Theorem 102.1 we know that $|G : \mathrm{Z}(G)| \geq p^3$ and $|G'| > p$. Let H be a maximal subgroup of G which is minimal nonabelian. Then $\Phi(H) = \mathrm{Z}(H) \leq \Phi(G)$ and $|H : \Phi(H)| = p^2$ which gives that $\Phi(H) = \Phi(G)$. Let $K \neq H$ be another maximal subgroup of G which is minimal nonabelian. Then $\mathrm{Z}(K) = \Phi(K) = \Phi(G)$ which implies $\mathrm{C}_G(\Phi(G)) \geq \langle H, K\rangle = G$ and so $\Phi(G) = \mathrm{Z}(G)$. Since $|M : \Phi(G)| = p^2$ and $\Phi(G) = \mathrm{Z}(G)$, we have $M = S * \Phi(G)$, where S is minimal nonabelian and $S \cap \Phi(G) = \Phi(S) < \Phi(G) = \mathrm{Z}(M)$. This implies $M' = S' \cong \mathrm{C}_p$ and $\mathrm{d}(M) \geq 3$. □

Theorem 102.3. *Let G be a p-group, $p > 2$, satisfying $\mathrm{d}(G) = 3$ which has exactly one maximal subgroup M which is neither abelian nor minimal nonabelian. Suppose that G has exactly one abelian maximal subgroup A. Then we have $\Phi(G) = \mathrm{Z}(G)$, $G' \cong \mathrm{E}_{p^2}$, $|M'| = p$, $\mathrm{d}(M) \geq 3$, $\Omega_1(G) = E \cong \mathrm{E}_{p^3}$, and $E \not\leq \Phi(G)$.*

If $E \not\leq A$, then we have the following possibilities:

(a) $G = \langle a, b, t \mid a^{p^{m+1}} = b^{p^2} = t^p = 1,\ [b,t] = z,\ a^{p^m} = z^n,\ b^p = u,\ [t,a] = u,\ [u,a] = [u,t] = [a,b] = [z,t] = 1\rangle$, *where $m \geq 2$ and $n \not\equiv 0 \pmod p$. We have*

$$|G| = p^{m+4}, \quad G' = \langle u, z\rangle \cong \mathrm{E}_{p^2},$$

$$\Phi(G) = \mathrm{Z}(G) = \langle a^p, u\rangle \cong \mathrm{C}_{p^m} \times \mathrm{C}_p, \quad \Omega_1(G) = E = \langle u, z, t\rangle \cong \mathrm{E}_{p^3},$$

$A = \langle a, b\rangle$ is abelian of type (p^{m+1}, p^2), $M = \langle b, t\rangle * \langle a^p\rangle$, where $\langle b, t\rangle$ is a nonmetacyclic minimal nonabelian group of order p^4, and all other $p^2 + p - 1$ maximal subgroups of G are minimal nonabelian.

(b) $G = \langle a, b, t \mid a^{p^2} = b^{p^2} = t^p = 1,\ a^p = z,\ u = [t,a],\ [b,t] = u^l z,\ b^p = u^n z^s,\ [u,a] = [u,t] = [a,b] = [z,t] = 1\rangle$, *where l, n, s are integers* mod p, *$n \not\equiv 0 \pmod p$, n is a square (in* $\mathrm{GF}(p)$*) and $(l+s)^2 \equiv 4n \pmod p$. The group G is a special group of order p^5 with*

$$G' = \langle u, z\rangle \cong \mathrm{E}_{p^2}, \quad \Omega_1(G) = E = \langle u, z, t\rangle \cong \mathrm{E}_{p^3},$$

$A = \langle a, b\rangle \cong \mathrm{C}_{p^2} \times \mathrm{C}_{p^2}$, $M = \langle a^j b, t\rangle G'$, where $j \equiv (1/2)(l - s) \pmod p$, and all other maximal subgroups of G are minimal nonabelian.

If $E \leq A$, then we have:

(c) $G = \langle a, b, d \mid a^{p^\alpha} = b^p = d^{p^2} = 1,\ a^{p^{\alpha-1}} = z,\ c = [a,b],\ z = [d,a],\ d^p = c^n z^r,\ [d,b] = c^s,\ c^p = [c,d] = [c,a] = [c,b] = 1\rangle$, *where $\alpha \geq 2$, n, r, s are integers* mod p, *$n \not\equiv 0 \pmod p$. We have*

$$|G| = p^{\alpha+3}, \quad G' = \langle z, c\rangle \cong \mathrm{E}_{p^2}, \quad \Phi(G) = \mathrm{Z}(G) = \langle a^p, c\rangle \cong \mathrm{C}_{p^{\alpha-1}} \times \mathrm{C}_p$$

and $A = \Phi(G)\langle b, a^{-s}d\rangle$.

- *If $\alpha \geq 3$, then $M = \Phi(G)\langle b, d\rangle$ with $s \not\equiv 0 \pmod p$.*
- *If $\alpha = 2$, then $M = \Phi(G)\langle b, a^{-r}d\rangle$ with $r \not\equiv s \pmod p$.*

All other maximal subgroups of G (distinct from A and M) are minimal nonabelian.

Proof. From Lemma 102.2 we conclude that $\Phi(G) = \mathrm{Z}(G)$ (and so G is of class 2), $|M'| = p$, $\mathrm{d}(M) \geq 3$, $|G'| > p$ and $|G| \geq p^5$. By Exercise 1.69(a), we get that $|G' : (A'H')| = |G' : H'| \leq p$, where H is a minimal nonabelian maximal subgroup of G. Hence $|G'| \leq p^2$ and so $|G'| = p^2$. If $G' = \langle v \rangle \cong \mathrm{C}_{p^2}$, then all $p^2 + p + 1$ maximal subgroups of the nonabelian group $G/\langle v^2 \rangle$ are abelian, a contradiction (see Exercise 1.6(a)). Hence $G' \cong \mathrm{E}_{p^2}$. We see also that each of the $p + 1$ subgroups of order p in G' is the commutator group of exactly p nonabelian maximal subgroups of G.

For each $x, y \in G$ we have $(xy)^p = x^p y^p [y, x]^{\binom{p}{2}} = x^p y^p$ and so G is regular. By Theorem 7.2, $\Omega_1(G)$ is of exponent p and $|\Omega_1(G)| = |G : \mathfrak{V}_1(G)|$. Suppose that $|\Omega_1(G)| \geq p^5$. Let H be a minimal nonabelian maximal subgroup of G. Then we obtain that $|H \cap \Omega_1(G)| \geq p^4$, contrary to the structure of H. We have proved that $|\Omega_1(G)| \leq p^4$.

Suppose that G has no normal elementary abelian subgroup of order p^3. Then we get $|\Omega_1(A)| \leq p^2$ and so A is metacyclic. If H is any minimal nonabelian maximal subgroup of G, then $|H| \geq p^4$ and the fact that $\Omega_1(H) \cong \mathrm{E}_{p^3}$ is not possible imply that H is metacyclic. In that case, M (with $\mathrm{d}(M) \geq 3$) is the only maximal subgroup of G which is not metacyclic. By Proposition A.40.12 of Berkovich, G is an L_3-group. In this case, $\Omega_1(G) \cong \mathrm{S}(p^3)$ (the nonabelian group of order p^3 and exponent p) and $G/\Omega_1(G)$ is cyclic of order $\geq p^2$. But then $\mathrm{E}_{p^2} \cong G' \leq \Omega_1(G)$, contrary to the fact that $G' \leq \mathrm{Z}(G)$.

We have proved that G possesses a normal elementary abelian subgroup $E \cong \mathrm{E}_{p^3}$ of order p^3. Suppose that G has an elementary abelian subgroup F of order p^4. Since $G' \cong \mathrm{E}_{p^2}$ and $G' \leq \mathrm{Z}(G)$, we have $G' \leq F$ and so $F \trianglelefteq G$. Also, $|\Omega_1(G)| \leq p^4$ implies that $F = \Omega_1(G)$. If G/F is noncyclic, then there is a minimal nonabelian maximal subgroup K of G containing F, contrary to the structure of K. Hence G/F is cyclic of order $\geq p$. Let $a \in G - F$ be such that $\langle a \rangle$ covers G/F. Then $o(a) = p^m$, $m \geq 2$, which implies that $\Omega_1(\langle a \rangle) = \langle z \rangle \leq \Phi(G) = \mathrm{Z}(G)$ and so $z \in F$. On the other hand, G/G' is abelian of rank 3 which forces $z \in G'$. Set $F = G'\langle f_1, f_2 \rangle$ for some $f_1, f_2 \in F - G'$ so that $\langle a, f_1, f_2 \rangle = G$ and $\Phi(G) = G'\langle a^p \rangle$. As $[F, \langle a \rangle] = G'$, we may choose $f_1 \in F - G'$ so that $[f_1, a] = z$ and thus $\langle f_1, a \rangle \cong \mathrm{M}_{p^{m+1}}$. This gives $\langle f_1, a \rangle G' \cong \mathrm{C}_p \times \mathrm{M}_{p^{m+1}}$. Since $[f_1, f_2 a] = z$ and $(f_2 a)^p = f_2^p a^p [a, f_2]^{\binom{p}{2}} = a^p$, it follows that $\Omega_1(\langle f_2 a \rangle) = \Omega_1(\langle a \rangle) = \langle z \rangle$ and $\langle f_1, f_2 a \rangle \cong \mathrm{M}_{p^{m+1}}$. Hence we conclude that $\langle f_1, f_2 a \rangle G' \cong \mathrm{C}_p \times \mathrm{M}_{p^{m+1}}$ is another maximal subgroup of G (distinct from $\langle f_1, a \rangle G'$) which is neither abelian nor minimal nonabelian, a contradiction. We have proved that G does not possess an elementary abelian subgroup of order p^4.

Assume that $\Omega_1(G) = S$ is a nonabelian subgroup of order p^4 and exponent p. Then we have $\mathrm{Z}(S) = G'$. If G/S is noncyclic, then there is a minimal nonabelian maximal subgroup H of G containing S, which contradicts the structure of H. Hence G/S is cyclic of order $\geq p$. Let $t, t' \in S - G'$ so that $S = G'\langle t, t' \rangle$ and then we have $1 \neq [t', t] = z \in G'$, $\langle t, t' \rangle \cong \mathrm{S}(p^3)$ and $S \cong \mathrm{S}(p^3) \times \mathrm{C}_p$. Let M be the unique maximal subgroup of G containing S so that M is neither abelian nor minimal

nonabelian and let A be the unique abelian maximal subgroup of G. Then $A > G'$ and $A \cap S \cong \mathrm{E}_{p^3}$ so that we may assume that $A \cap S = G'\langle t'\rangle$. Also, A covers G/S and so if $c \in A - M$, then $\langle c\rangle$ covers $A/(A \cap S) \cong G/S$ and $o(c) \geq p^2$ which implies

$$\Omega_1(\langle c\rangle) \leq \Phi(G) \cap S = \mathrm{Z}(G) \cap S = \mathrm{Z}(S) = G'.$$

We have $\Phi(G) = G'\langle c^p\rangle$, and so $G = \langle c, t, t'\rangle$ and $[c, t'] = 1$. If $[c, t] \in \langle z\rangle$, then $G/\langle z\rangle$ is abelian, a contradiction. Hence $[c, t] = u \in G' - \langle z\rangle$ so that $G' = \langle u, z\rangle$. The other $p^2 + p - 1$ maximal subgroups of G (which are distinct from A and M) are of the form $T\Phi(G)$, where T is one of the following minimal nonabelian subgroups: $\langle c, (t')^i t\rangle$ and $\langle c^j t', c^k t\rangle$, where i, j, k are integers mod p and both j and k cannot be congruent 0 (mod p) (see Exercise P9 and P11). Here $T\Phi(G)$ must be minimal nonabelian and this will be the case if and only if $\Phi(T) \geq \Phi(G) = G'\langle c^p\rangle$. It is enough to consider $\langle c, t\rangle$ and $\langle c^j t', ct\rangle$ for any integer j mod p. We have

$$\Phi(\langle c, t\rangle) = \langle c^p, [c, t] = u\rangle = \Phi(G)$$

if and only if $\Omega_1(\langle c\rangle) \neq \langle u\rangle$ which gives $\Omega_1(\langle c\rangle) = \langle u^l z\rangle$ for some integer l mod p. Further, we get

$$\begin{aligned}\Phi(\langle c^j t', ct\rangle) &= \langle c^{pj}(t')^p = c^{pj},\ (ct)^p = c^p t^p = c^p,\ [c^j t', ct] = u^j z\rangle \\ &= \langle c^p, u^j z\rangle.\end{aligned}$$

But $\Omega_1(\langle c\rangle) = \Omega_1(\langle c^p\rangle) = \langle u^l z\rangle$ and so for $j = l$, $\Phi(\langle c^l t', ct\rangle) = \langle c^p\rangle < \Phi(G)$ which shows that $\langle c^l t', ct\rangle\Phi(G)$ is another maximal subgroup of G (distinct from M) which is neither abelian nor minimal nonabelian, a contradiction. We have proved that $\Omega_1(G) = E \cong \mathrm{E}_{p^3}$.

(i) Assume that $\mathrm{E}_{p^3} \cong E = \Omega_1(G) \not\leq \mathrm{Z}(G) = \Phi(G)$ and $E \not\leq A$, where A is the unique abelian maximal subgroup of G. Then we see that $A \cap E = G'$, A covers G/E and A is metacyclic. Since G/G' is abelian of rank 3, we have $\mathrm{d}(G/E) = 2$ and so there exists at least one maximal subgroup H of G which is minimal nonabelian. If H/E is noncyclic, then $E \leq \Phi(H) = \Phi(G) = \mathrm{Z}(G)$, a contradiction. Hence we have $H/E \cong (H \cap A)/G' \cong \mathrm{C}_{p^m}$, $m \geq 1$. Since $\mathrm{d}(G/E) = 2$, $G/E \cong A/G'$ is abelian of type (p^m, p). Let $a \in H \cap A$ be such that $\langle a\rangle$ covers $(H \cap A)/G'$. Noting that $\Omega_1(G) = E$, we have $o(a) = p^{m+1}$ and $1 \neq z = a^{p^m} \in G'$. Let $t \in E - G'$ so that $[t, a] = u \in G' - \langle z\rangle$ and so $G' = \langle u, z\rangle$ since H is nonmetacyclic and so $H' = \langle u\rangle$ is a maximal cyclic subgroup in H. Since $A/G' \cong \mathrm{C}_{p^m} \times \mathrm{C}_p$, there is an element $b \in A - H$ such that $1 \neq b^p \in G'$, $b^p \in G' - \langle z\rangle$ and $[a, b] = 1$. Indeed, if $b^p \in \langle z\rangle$, then the subgroup $\langle b, \Omega_2(\langle a\rangle)\rangle$ contains elements of order p in $A - H$, a contradiction. We have $\Phi(H) = \Phi(G) = \langle a^p, u\rangle$, $G = \langle a, b, t\rangle$ and $A = \langle a\rangle \times \langle b\rangle$ is abelian of type (p^{m+1}, p^2), $m \geq 1$. If $[b, t] \in \langle u\rangle$, then $G/\langle u\rangle$ would be abelian, a contradiction. Hence $[b, t] \in G' - \langle u\rangle$ and so replacing b with $b' = b^s$ (with some $s \not\equiv 0$ (mod p)), we may assume from the start that $[b, t] = u^l z$ for some integer l mod p.

We have $A = \langle a, b\rangle$ and so we have to check the $p^2 + p$ other maximal subgroups of G which are of the form $T\Phi(G)$, where T is one of the minimal nonabelian subgroups: $\langle a, b^i t\rangle$, $\langle a^j b, a^k t\rangle$, where i, j, k are any integers mod p (see Exercise P11).

(i1) First assume $m \geq 2$ so that $\Phi(G) > G'$. Consider $T = \langle b, t\rangle$, where

$$\Phi(\langle b, t\rangle) = \langle b^p, [b, t]\rangle \leq G' < \Phi(G)$$

and so $M = \langle b, t\rangle\Phi(G)$ must be our unique maximal subgroup of G which is neither abelian nor minimal nonabelian. All other maximal subgroups of G (which are distinct from A and M) must be minimal nonabelian. Indeed,

$$\Phi(\langle a, b^i t\rangle) = \langle a^p, b^{ip} t^p = b^{ip}, [a, b^i t] = u^{-1}\rangle = \Phi(G).$$

Further, for $j \not\equiv 0 \pmod{p}$ we have

$$\Phi(\langle a^j b, t\rangle) = \langle a^{pj} b^p, [a^j b, t] = u^{-j} u^l z\rangle.$$

Here $\langle a^{pj} b^p\rangle$ covers $\Phi(G)/G'$ and $\Omega_1(\langle a^{pj} b^p\rangle) = \langle z\rangle$. Hence if $l \not\equiv 0 \pmod{p}$, then $\Phi(\langle a^l b, t\rangle) = \langle a^{pl} b^p\rangle < \Phi(G)$, a contradiction (since $\langle a^l b, t\rangle\Phi(G)$ will be another maximal subgroup which is neither abelian nor minimal nonabelian). Therefore we conclude that $l \equiv 0 \pmod{p}$ and so $[b, t] = z$. Finally, if both j and k are not congruent $0 \pmod{p}$, then we have

$$\Phi(\langle a^j b, a^k t\rangle) = \langle a^{pj} b^p, a^{pk}, \quad [a^j b, a^k t] = u^{-j} z\rangle = \Phi(G).$$

We have $b^p \in G' - \langle z\rangle$ and so $b^p = u^n z^s$, where n and s are some integers mod p with $n \not\equiv 0 \pmod{p}$. Then we replace a with $a' = a^n b^{-s}$ and u with $u' = u^n z^s$ and get

$$(a')^{p^m} = z^n, \quad b^p = u', \quad [t, a'] = [t, a^n b^{-s}] = u^n z^s = u'.$$

Writing again a instead a' and u instead u', we see that we have obtained the relations stated in part (a) of our theorem.

(i2) Now assume $m = 1$ so that $|G| = p^5$ and $G' = \mathrm{Z}(G) = \Phi(G) = \langle u, z\rangle$ and therefore G is a special p-group. In this case, we have

$$a^p = z, \quad [t, a] = u, \quad [a, b] = 1, \quad [b, t] = u^l z, \quad b^p = u^n z^s,$$

where l, n, s are some integers mod p with $n \not\equiv 0 \pmod{p}$. Also, A is abelian of type (p^2, p^2). For all integers $i \bmod p$ we have

$$\Phi(\langle a, b^i t\rangle) \geq \langle a^p = z, [a, b^i t] = u^{-1}\rangle = G' = \Phi(G)$$

and so all subgroups $\langle a, b^i t\rangle$ are minimal nonabelian maximal subgroups of G. Hence among the rest of the p^2 nonabelian maximal subgroups $\langle a^j b, a^k t\rangle G'$ (j, k are any integers mod p) there is exactly one which is not minimal nonabelian. We have

$$\Phi(\langle a^j b, a^k t\rangle) = \langle u^n z^{s+j}, z^k, u^{l-j} z\rangle,$$

and so if $k \not\equiv 0 \pmod{p}$, then $\Phi(\langle a^j b, a^k t\rangle) = \langle u, z\rangle = G'$. It remains to examine the case $k \equiv 0 \pmod{p}$, where we must have

$$\Phi(\langle a^j b, t\rangle) = \langle u^n z^{s+j}, u^{l-j} z\rangle \neq G' = \langle u, z\rangle$$

for exactly one j. It follows that the quadratic congruence

$$\begin{vmatrix} n & s+j \\ l-j & 1 \end{vmatrix} = j^2 + j(s-l) + (n-sl) \equiv 0 \pmod{p}$$

must have exactly one solution in j. This occurs if and only if

$$(s-l)^2 - 4(n-sl) \equiv 0 \pmod{p}$$

or, equivalently, $(s+l)^2 \equiv 4n \pmod{p}$. In this case, $j \equiv (1/2)(l-s) \pmod{p}$ and for that integer j the maximal subgroup $M = \langle a^j b, t\rangle G'$ is the only one which is neither abelian nor minimal nonabelian. We have obtained the groups from part (b) of our theorem.

(ii) Assume that $\mathrm{E}_{p^3} \cong E = \Omega_1(G) \not\leq \mathrm{Z}(G) = \Phi(G)$ and $E \leq A$, where A is the unique abelian maximal subgroup of G. Since $\mathrm{d}(G/E) = 2$, there exists (at least one) maximal subgroup H containing E which is minimal nonabelian. Then H is nonmetacyclic, $H/E \neq \{1\}$ is cyclic and $\mathrm{Z}(H) \cap E = G'$. Indeed, if H/E is noncyclic, then we have $E \leq \Phi(H) = \Phi(G) = \mathrm{Z}(G)$, contrary to our assumption. Taking an element $a \in H - E$ such that $\langle a\rangle$ covers H/E and an element $b \in E - G'$, we get $\Omega_1(\langle a\rangle) \leq G'$ and

$$H = \langle a, b \mid a^{p^\alpha} = b^p = 1,\ c = [a, b],\ c^p = [a, c] = [b, c] = 1\rangle,$$

where $\alpha \geq 2$, $H' = \langle c\rangle$, $\mathrm{Z}(H) = \Phi(H) = \langle a^p\rangle \times \langle c\rangle$, and $|G| = p^{\alpha+3}$. Setting $a^{p^{\alpha-1}} = z$, we have $G' = \langle c, z\rangle$, $E = \langle b\rangle \times G' \cong \mathrm{E}_{p^3}$ because $\langle c\rangle$ is a maximal cyclic subgroup in H and therefore $\langle c\rangle \neq \langle z\rangle$.

Now, $\langle a, c\rangle$ is an abelian normal subgroup of G of type (p^α, p) which possesses exactly p cyclic subgroups $\langle ac^i\rangle$ (i any integer mod p) of order p^α. But $[a, b^i] = c^i$ and so we get $\mathrm{N}_H(\langle a\rangle) = \langle a, c\rangle$ and all subgroups $\langle ac^i\rangle$ are conjugate in H. Therefore $N = \mathrm{N}_G(\langle a\rangle)$ covers G/H and so $G = NH$ with $N \cap H = \langle a, c\rangle$. As $N/G' \cong G/E$ is abelian of rank 2, it follows that N/G' is abelian of type (p^α, p). Hence there exists an element $d \in N - H$ such that $1 \neq d^p \in G'$ and $\langle d\rangle$ normalizes $\langle a\rangle$. But N is a maximal subgroup of our group G which does not contain E and so N is nonabelian (noting that in our case $E \leq A$). This gives $1 \neq [d, a] \in \langle z\rangle$ and so replacing d with a suitable power d^j ($j \not\equiv 0 \pmod{p}$), we may assume from the start that $[d, a] = z$. If $d^p \in \langle z\rangle$, then we get $\langle d, a\rangle \cong \mathrm{M}_{p^{\alpha+1}}$ in which case there are elements of order p in $\langle d, a\rangle - H$, a contradiction. We have proved that $d^p \in G' - \langle z\rangle$ so that $\langle d, a\rangle$ is a metacyclic minimal nonabelian maximal subgroup of $G = \langle a, b, d\rangle$. Now, $H = \langle a, b\rangle$ is a minimal nonabelian maximal subgroup of G containing E and the other p maximal subgroups of G containing E are $\langle b, a^i d\rangle\Phi(G)$, where i is any integer mod p and

$\Phi(G) = G'\langle a^p\rangle$. For exactly one i, $\langle b, a^i d\rangle\Phi(G)$ is the unique abelian maximal subgroup A of G, i.e., $[a^i d, b] = 1$ and then $c^i[d, b] = 1$ and so we may set $[d, b] = c^s$ for some integer s mod p. Since $d^p \in G' - \langle z\rangle$, we may set $d^p = c^n z^r$ for some integers n, r mod p with $n \not\equiv 0 \pmod p$.

All p^2 maximal subgroups of G which do not contain E are $\langle b^j a, b^k d\rangle\Phi(G)$, where j, k are any integers mod p. They are all metacyclic minimal nonabelian since

$$\Phi(\langle b^j a, b^k d\rangle) = \langle a^p,\ d^p = c^n z^r,\ [b^j a, b^k d] = c^{-sj+k} z^{-1} \neq 1\rangle = \Phi(G),$$

where we have used the facts $\langle a^p\rangle \geq \langle z\rangle$ and $n \not\equiv 0 \pmod p$.

We obtain that $A = \langle b, a^{-s} d\rangle\Phi(G)$ is the unique abelian maximal subgroup of G and in the set of the $p - 1$ nonabelian maximal subgroups $\langle b, a^i d\rangle\Phi(G)$ for $i \not\equiv -s \pmod p$ there is exactly one which is not minimal nonabelian. We compute for all $i \not\equiv -s \pmod p$

$$\begin{aligned}\Phi(\langle b, a^i d\rangle) &= \langle b^p = 1,\ (a^i d)^p = a^{pi} c^n z^r,\ [b, a^i d] = c^{-i-s} \neq 1\rangle \\ &= \langle a^{pi} z^r, c\rangle.\end{aligned}$$

If $\alpha \geq 3$, then $\langle z^r\rangle \leq \langle a^p\rangle$ and so in this case $\Phi(\langle b, a^i d\rangle) \neq \Phi(G)$ if and only if $i \equiv 0 \pmod p$. Then we have $M = \langle b, d\rangle\Phi(G)$ and in this case $s \not\equiv 0 \pmod p$.

If $\alpha = 2$, then $\Phi(\langle b, a^i d\rangle) = \langle z^{i+r}, c\rangle$ since $a^p = z$. Hence in this case we have $\Phi(\langle b, a^i d\rangle) \neq \Phi(G)$ if and only if $i \equiv -r \pmod p$. Then $M = \langle b, a^{-r} d\rangle\Phi(G)$ and in this case we must have $r \not\equiv s \pmod p$. We have obtained the groups stated in part (c) of our theorem.

(iii) It remains to consider the case $\mathrm{E}_{p^3} \cong E = \Omega_1(G) \leq \mathrm{Z}(G) = \Phi(G)$. We shall show that this difficult case cannot occur.

If H_i is any minimal nonabelian maximal subgroup of G, then $\Phi(H_i) = \Phi(G) \geq E \cong \mathrm{E}_{p^3}$ and so $|H_i| \geq p^5$ which implies $|G| \geq p^6$. By the first paragraph of this proof, we know that there are exactly p nonabelian maximal subgroups of G whose commutator subgroup is equal to $M' = \langle m\rangle$. Obviously, G/M' is an A_2-group of order $\geq p^5$ with $(G/M')' = G'/M' \cong \mathrm{C}_p$ and G/M' has exactly $p+1$ abelian maximal subgroups. By Proposition 71.1, there is a minimal nonabelian maximal subgroup H/M' of G/M' and an element $d \in G - H$ with $1 \neq d^p \in G'$ and $[\langle d\rangle, G] = M'$. We have $H' = \langle c\rangle$ with $c \in G' - M'$ and $G' = \langle c, m\rangle$ which implies that H is a minimal nonabelian maximal subgroup of G (noting that $H \neq M$ since $H' \neq M'$).

There are exactly $p + 1$ maximal subgroups X_i of G ($i = 1, 2, \ldots, p + 1$) which contain $\langle d\rangle$. Then $X_i \cap H$ is an abelian maximal subgroup of H. Further, we obtain that $X_i' = [\langle d\rangle, (X_i \cap H)] \leq M'$ and so X_i is either abelian or $X_i' = \langle m\rangle$. It follows that $\{X_1, \ldots, X_{p+1}\} = \{A, M, H_1^*, \ldots, H_{p-1}^*\}$, where H_j^* ($j = 1, 2, \ldots, p - 1$) are minimal nonabelian with $(H_j^*)' = \langle m\rangle = M'$. But H_j^* (containing E) is nonmetacyclic and so M' is a maximal cyclic subgroup in H_j^* which implies $d^p \in G' - M'$ and we may set $d^p = c^s m^t$, where s, t are some integers (mod p) with $s \not\equiv 0 \pmod p$.

Consider $H^* = H_1^*$ so that H^* is a minimal nonabelian maximal subgroup of G containing $\langle d\rangle$ and $(H^*)' = \langle m\rangle$. Choose an element $a^* \in (H \cap H^*) - \Phi(G)$ so that $H^* = \langle d, a^*\rangle$ and $[d, a^*] = m$. By Exercise P9,

$$\Phi(H^*) = \langle d^p, [d, a^*] = m\rangle\langle (a^*)^p\rangle = G'\langle (a^*)^p\rangle,$$

and we know that $\Phi(H^*) = \Phi(G)$. If $\Omega_1(\langle a^*\rangle) \leq G'$, then $E \not\leq \Phi(G)$, a contradiction. Hence we have $\Omega_1(\langle a^*\rangle) \not\leq G'$ which implies $\Phi(H^*) = \Phi(G) = \langle (a^*)^p\rangle \times G'$ and this is an abelian group of type $(p, p, p^{\gamma-1})$, where $o(a^*) = p^\gamma$, $\gamma \geq 2$ and $H \cap H^* = \langle a^*\rangle \times G'$. It follows that $(H \cap H^*)/G' \cong \mathrm{C}_{p^\gamma}$ and since H/G' is noncyclic abelian, there exists $b^* \in H - (H \cap H^*)$ such that $1 \neq (b^*)^p \in G'$ and $\langle a^*, b^*\rangle = H$. We may set $[a^*, b^*] = c$, where $\langle c\rangle = H'$. Also, $\langle c\rangle$ is a maximal cyclic subgroup in H which gives $(b^*)^p \in G' - \langle c\rangle$ and we have $G = \langle a^*, b^*, d\rangle$, $|G| = p^{\gamma+4}$, $\gamma \geq 2$. We may set $(b^*)^p = c^v m^w$, where v, w are some integers (mod p) with $w \not\equiv 0 \pmod p$.

Suppose that $[d, b^*] = 1$ so that $A = \langle d, b^*\rangle\Phi(G)$. Also, $\langle d, a^*\rangle = H^*$ and so we investigate other maximal subgroups $\langle d, (a^*)^i b^*\rangle\Phi(G)$ containing $\langle d\rangle$, where $i \not\equiv 0 \pmod p$. We get

$$\begin{aligned}\Phi(\langle d, (a^*)^i b^*\rangle) &= \langle d^p \in G' - \langle m\rangle,\ [d, (a^*)^i b^*] = m^i,\ (a^*)^{pi}(b^*)^p\rangle \\ &= \Phi(G).\end{aligned}$$

But then there is no subgroup M in the set of maximal subgroups of G containing $\langle d\rangle$, a contradiction. Hence we have $[d, b^*] = m^r$ with $r \not\equiv 0 \pmod p$.

Since the maximal subgroups A and M are contained in the set of the $p + 1$ maximal subgroups of G which contain $\langle d\rangle$, it follows that all p^2 maximal subgroups $\langle d^i a^*, d^j b^*\rangle\Phi(G)$ of G (i, j are any integers mod p) which do not contain $\langle d\rangle$ must be minimal nonabelian.

For each integer i mod p we must have

$$\Phi(\langle d^i a^*, b^*\rangle) = \langle d^{pi}(a^*)^p,\ (b^*)^p = c^v m^w,\ [d^i a^*, b^*] = cm^{ri}\rangle = \Phi(G)$$

and this will be the case if and only if $\langle c^v m^w, cm^{ri}\rangle = G' = \langle c, m\rangle$ or, equivalently,

$$\begin{vmatrix} v & w \\ 1 & ri \end{vmatrix} = vri - w \not\equiv 0 \pmod p.$$

But $r \not\equiv 0 \pmod p$ and so if $v \not\equiv 0 \pmod p$, then the congruence $vri - w \equiv 0 \pmod p$ would have a solution in i, a contradiction. Hence $v \equiv 0 \pmod p$ and so $(b^*)^p = m^w$.

For each integer i mod p we must have

$$\begin{aligned}\Phi(\langle d^i a^*, db^*\rangle) &= \langle d^{pi}(a^*)^p,\ d^p(b^*)^p = c^s m^{t+w},\ [d^i a^*, db^*] = cm^{ri-1}\rangle \\ &= \Phi(G)\end{aligned}$$

and this will be the case if and only if $\langle c^s m^{t+w}, cm^{ri-1}\rangle = G' = \langle c, m\rangle$ or, equivalently,

$$\begin{vmatrix} s & t+w \\ 1 & ri-1 \end{vmatrix} = (sr)i - s - t - w \not\equiv 0 \pmod{p}.$$

But $sr \not\equiv 0 \pmod{p}$ and so the congruence $(sr)i - s - t - w \equiv 0 \pmod{p}$ would have a solution in i, a final contradiction. Our theorem is proved. □

Lemma 102.4. *Let P be a p-group with $|P'| = p$. If P possesses a minimal nonabelian maximal subgroup H, then P has exactly $p+1$ abelian maximal subgroups.*

Proof. By Exercise P.10, $P = H\mathrm{C}_P(H)$ and in our case $\mathrm{C}_P(H)$ is abelian so that $\mathrm{C}_P(H) = \mathrm{Z}(P)$. But then all $p+1$ maximal subgroups of P containing $\mathrm{Z}(P)$ are abelian and so we are done (see Exercise 1.6(a)). □

Theorem 102.5. *Let G be a p-group, $p > 2$, with $\mathrm{d}(G) = 3$ which has exactly one maximal subgroup M which is neither abelian nor minimal nonabelian. Suppose that G has no abelian maximal subgroups. Then $\Phi(G) = \mathrm{Z}(G)$, $\Omega_1(G) = G' \cong \mathrm{E}_{p^3}$, $|M'| = p$, $\mathrm{d}(M) \geq 3$ and we have one of the following possibilities:*

(a) $G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^{p^2} = 1,\ a^p = z,\ b^p = y,\ c^p = x,\ [a,b] = z,\ [a,c] = yz^\beta,\ [b,c] = x^{-1}y^\delta z^\eta,\ [x,b] = [x,a] = [y,a] = [y,c] = [z,b] = [z,c] = 1\rangle$, *where β, δ, η are integers* mod p, *$\eta \not\equiv 0 \pmod{p}$ and $(\beta-\delta)^2 + 4\eta$ is not a square in* $\mathrm{GF}(p)$. *We have $|G| = p^6$, $\Omega_1(G) = G' = \Phi(G) = \mathrm{Z}(G) = \langle x, y, z\rangle \cong \mathrm{E}_{p^3}$ and so G is a special p-group. Also, $M = \langle a, b\rangle G'$ and all other maximal subgroups of G are nonmetacyclic minimal nonabelian.*

(b) $G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^{p^n} = 1,\ a^p = x,\ b^p = y,\ c^{p^{n-1}} = z,\ [a,b] = z,\ [c,a] = x^\alpha y^\eta z^\beta,\ [c,b] = x^\xi y^\gamma z^\delta,\ [x,b] = [x,c] = [y,a] = [y,c] = [z,a] = [z,b] = 1\rangle$, *where $n \geq 3$, $\alpha, \beta, \gamma, \delta, \eta, \zeta$ are integers* mod p, *$\eta \not\equiv 0 \pmod{p}$, $\zeta \not\equiv 0 \pmod{p}$, and $(\alpha-\gamma)^2 + 4\eta\zeta$ is not a square in* $\mathrm{GF}(p)$. *In this case, we have $|G| = p^{n+4}$, $\Omega_1(G) = G' = \langle x, y, z\rangle \cong \mathrm{E}_{p^3}$ and $\Phi(G) = \mathrm{Z}(G) = \langle c^p, x, y\rangle$ is abelian of type (p^{n-1}, p, p). Also, $M = \langle a, b\rangle\Phi(G)$ and all other maximal subgroups of G are nonmetacyclic minimal nonabelian.*

Proof. Let $\Gamma_1 = \{H_1, H_2, \ldots, H_{p^2+p}, M\}$ be the set of maximal subgroups of G, where H_i $(i = 1, \ldots, p^2+p)$ are minimal nonabelian and M is neither abelian nor minimal nonabelian. From Lemma 102.2 we get $\Phi(G) = \mathrm{Z}(G) = \mathrm{Z}(H_i) = \mathrm{Z}(M)$, $\mathrm{d}(M) \geq 3$, $|M'| = p$ and $|G'| > p$. By a result of A. Mann (see Exercise 1.69(a)), $|G : (H_1'H_2')| \leq p$ and so $p^2 \leq |G'| \leq p^3$.

Suppose that for some $H_i \neq H_j$ we have $H_i' = H_j'$ or $H_i' = M'$. Then, by Exercise 1.69(a), $|G'| \leq p^2$ and so $|G'| = p^2$. If $G' \cong \mathrm{C}_{p^2}$, then the nonabelian group $G/\Omega_1(G')$ has $p^2 + p + 1$ abelian maximal subgroups, which is a contradiction by Exercise 1.6(a). Hence $G' \cong \mathrm{E}_{p^2}$. Let X be any fixed subgroup of order p in G'. Then there is a minimal nonabelian maximal subgroup H_i $(i \in \{1, \ldots, p^2+p\})$ such that $H_i' \neq X$ so that H_i/X is minimal nonabelian. By Lemma 102.4, G/X has exactly

$p + 1$ abelian maximal subgroups. Hence there are exactly $p + 1$ maximal subgroups of G whose commutator subgroup is equal X. But G' has $p + 1$ subgroups of order p and so G must have $(p + 1)^2 = p^2 + 2p + 1$ maximal subgroups, a contradiction.

We have proved that $\{H_1', H_2', \ldots, H_{p^2+p}', M'\}$ is the set of $p^2 + p + 1$ pairwise distinct subgroups of order p in G' and so, in particular, $G' \cong \mathrm{E}_{p^3}$. Assume that there is an element $t \in G - G'$ of order p. Since G/G' is abelian of rank 3, $G/(G' \times \langle t \rangle)$ is noncyclic. But then there is a maximal subgroup Y of G containing $G' \times \langle t \rangle$ which is minimal nonabelian, a contradiction (with the structure of Y). We have proved that $\Omega_1(G) = G' \cong \mathrm{E}_{p^3}$ and all minimal nonabelian maximal subgroups of G are nonmetacyclic.

Set $T/G' = \Omega_1(G/G') \cong \mathrm{E}_{p^3}$. If G/T is noncyclic, then there is a maximal subgroup K of G containing T which is minimal nonabelian. Since $K > T$, T is abelian of type (p^2, p^2, p^2). But $K' < G'$ and so K' is not a maximal cyclic subgroup in K, contrary to the fact that K is nonmetacyclic minimal nonabelian. We have proved that G/T is cyclic.

(i) First assume that $T = G$, i.e., $G/G' \cong \mathrm{E}_{p^3}$ and so in this case G is a special group of order p^6 with $G' = \Omega_1(G) \cong \mathrm{E}_{p^3}$.

We determine the structure of M. We have $M = G' * S$, where $S = \langle a, b \rangle$ is minimal nonabelian and $G' \cap S = \Phi(S) < G'$ since $\mathrm{d}(M) \geq 3$. Set $S' = M' = \langle z \rangle \cong \mathrm{C}_p$. If $\Phi(S) = \langle z \rangle$, then $\langle z \rangle$ is a unique subgroup of order p in S which implies that S would be cyclic, a contradiction. Hence $\Phi(S) = \Omega_1(S) \cong \mathrm{E}_{p^2}$ and so S is metacyclic of order p^4 and exponent p^2. We may choose $a, b \in S - G'$ so that $a^p = z$, $b^p = y \in \Phi(S) - \langle z \rangle$ and $[a, b] = z$. Since $\mathfrak{V}_1(M) = \mathfrak{V}_1(S) = \langle y, z \rangle \geq M' = \langle z \rangle$, it follows that M is a powerful group. By Proposition 26.10, each element in $\langle y, z \rangle$ is a p-th power of an element in M. Let c be an element in $G - M$. Suppose that $c^p \in \langle y, z \rangle$. Then there is $m \in M$ such that $m^p = c^{-p}$. We get

$$(mc)^p = m^p c^p [c, m]^{\binom{p}{2}} = 1,$$

contrary to the fact that $\Omega_1(G) = G'$. Hence we have $c^p = x \in G' - \langle y, z \rangle$ and so $G' = \langle x, y, z \rangle$ and $G = \langle a, b, c \rangle$. All $p^2 + p$ maximal subgroups of G which are distinct from M must be minimal nonabelian.

We obtain $\Phi(\langle a, c \rangle) = \langle z, x, [a, c] \rangle = G'$ and so $[a, c] = y^r y'$, where $r \not\equiv 0 \pmod{p}$ and $y' \in \langle x, z \rangle$. Replacing c with $c' = c^{r'}$, where $r' \not\equiv 0 \pmod{p}$ is such that $rr' \equiv 1 \pmod{p}$, we get

$$[a, c'] = [a, c^{r'}] = [a, c]^{r'} = y^{rr'} (y')^{r'} = y (y')^{r'},$$

where $c' \in G - M$, $(y')^{r'} \in \langle x, z \rangle$ and $(c')^p = (c^p)^{r'} = x^{r'} = x' \in G - \langle y, z \rangle$. Writing again c and x instead of c' and x', respectively, we see that we may assume from the start $[a, c] = yy''$ and $c^p = x$, where $y'' \in \langle x, z \rangle$ and so we may set $[a, c] = x^\alpha y z^\beta$ for some integers $\alpha, \beta \bmod p$. From $\Phi(\langle b, c \rangle) = \langle y, x, [b, c] \rangle = G'$ follows that $[b, c] = x^\gamma y^\delta z^\eta$, where γ, δ, η are some integers mod p with $\eta \not\equiv 0 \pmod{p}$.

Maximal subgroups of G containing $\langle c\rangle$ are $\langle a, c\rangle G'$ and $\langle a^i b, c\rangle G'$. Therefore we must have for all integers $i \bmod p$

$$\Phi(\langle a^i b, c\rangle) = \langle yz^i, x, [a^i b, c] = x^{\alpha i+\gamma} y^{i+\delta} z^{\beta i+\eta}\rangle = G'$$

which is equivalent to

$$\begin{vmatrix} 0 & 1 & i \\ 1 & 0 & 0 \\ \alpha i+\gamma & i+\delta & \beta i+\eta \end{vmatrix} = i^2 + (\delta-\beta)i - \eta \not\equiv 0 \pmod p.$$

Hence the quadratic congruence $i^2 + (\delta-\beta)i - \eta \equiv 0 \pmod p$ should not have any solution in i which is equivalent to the requirement that $(\beta-\delta)^2 + 4\eta$ is not a square in GF(p).

We have to examine the p^2 maximal subgroups $\langle c^j a, c^k b\rangle G'$ of G (j, k are integers mod p) which do not contain $\langle c\rangle$. For all $k \not\equiv 0 \pmod p$ we get

$$\Phi(\langle a, c^k b\rangle) = \langle z, x^k y, [a, c^k b] = x^{k\alpha} y^k z^{k\beta+1}\rangle = G'$$

which is equivalent to

$$\begin{vmatrix} 0 & 0 & 1 \\ k & 1 & 0 \\ k\alpha & k & k\beta+1 \end{vmatrix} m = k^2 - k\alpha = k(k-\alpha) \not\equiv 0 \pmod p.$$

Hence we must have $\alpha \equiv 0 \pmod p$ and so $[a, c] = yz^\beta$.

For all $j \not\equiv 0 \pmod p$ we obtain

$$\Phi(\langle c^j a, b\rangle) = \langle x^j z, y, [c^j a, b] = x^{-\gamma j} y^{-\delta j} z^{-\eta j+1}\rangle = G'$$

which is equivalent to

$$\begin{vmatrix} j & 0 & 1 \\ 0 & 1 & 0 \\ -\gamma j & -\delta j & -\eta j+1 \end{vmatrix} = j(-\eta j + \gamma + 1) \not\equiv 0 \pmod p.$$

Since $\eta \not\equiv 0 \pmod p$, we must have $\gamma \equiv -1 \pmod p$ and so $[b, c] = x^{-1} y^\delta z^\eta$. We have obtained the groups of order p^6 stated in part (a) of our theorem.

It remains to check that all maximal subgroups $\langle c^j a, c^k b\rangle G'$ are minimal nonabelian unless $j \equiv k \equiv 0 \pmod p$ in which case $\langle a, b\rangle G' = M$. Indeed,

$$\Phi(\langle c^j a, c^k b\rangle) = \langle x^j z, x^k y, [c^j a, c^k b] = x^j y^{-\delta j+k} z^{-\eta j+\beta k+1}\rangle < G'$$

if and only if

$$\begin{vmatrix} j & 0 & 1 \\ k & 1 & 0 \\ j & -\delta j+k & -\eta j+\beta k+1 \end{vmatrix} = k^2 + k(\beta j - \delta j) - \eta j^2 \equiv 0 \pmod p.$$

The quadratic congruence in k

$$k^2 + kj(\beta - \delta) - \eta j^2 \equiv 0 \pmod{p}$$

(where $j \in \mathrm{GF}(p)$ is fixed) has a solution in k if and only if the discriminant

$$(*) \qquad j^2(\beta - \delta)^2 + 4\eta j^2 = ((\beta - \delta)^2 + 4\eta) j^2$$

is a square in $\mathrm{GF}(p)$. But we know that $(\beta - \delta)^2 + 4\eta$ is not a square in $\mathrm{GF}(p)$ and so we must have $j \equiv 0 \pmod{p}$. From $(*)$ we then get $k^2 \equiv 0 \pmod{p}$ and so also $k \equiv 0 \pmod{p}$ and we are done.

(ii) Now assume that $T < G$, where $T/G' = \Omega_1(G/G') \cong \mathrm{E}_{p^3}$ and T/G' is cyclic. Hence G/G' is abelian of type (p^m, p, p), $m \geq 2$, and the unique maximal subgroup of G containing T is obviously equal to M. There are normal subgroups U and V of G such that $G = UV$, $U \cap V = G'$, $U/G' \cong \mathrm{E}_{p^2}$ and $V/G' \cong \mathrm{C}_{p^m}$, $m \geq 2$. Let c be an element in $V - G'$ such that $\langle c \rangle$ covers V/G'. We have $o(c) = p^n$, $n \geq 3$, where $n = m + 1$ (noting that $\Omega_1(G) = G'$). Set $c^{p^{n-1}} = z$, where $z \in G'$. Then $M = \langle c^p \rangle U$, $\Phi(G) = \mathrm{Z}(G) = G'\langle c^p \rangle$ is abelian of type (p^{n-1}, p, p) and $|G| = p^{n+4}$. Let $a, b \in U - G'$ be such that $U = G'\langle a, b \rangle$, where $a^p, b^p \in G'$ and $G = \langle a, b, c \rangle$. Since each minimal nonabelian maximal subgroup H_i of G ($i = 1, \ldots, p^2 + p$) is nonmetacyclic and contains $\Phi(G)$ and $\langle z \rangle$ is not a maximal cyclic subgroup in $\Phi(G)$, it follows that $H_i' \neq \langle z \rangle$ (for all i) and so $M' = \langle z \rangle$. Therefore $1 \neq [a, b] \in \langle z \rangle$ and so we may assume $[a, b] = z$.

Now, $G/\langle z \rangle$ has the unique abelian maximal subgroup $M/\langle z \rangle$ and all other maximal subgroups of the factor group $G/\langle z \rangle$ are minimal nonabelian. Hence $G/\langle z \rangle$ is an A_2-group with $\mathrm{d}(G/\langle z \rangle) = 3$ and of order $p^{n+3} > p^4$ (since $n \geq 3$), $G'/\langle z \rangle \cong \mathrm{E}_{p^2}$, $G'/\langle z \rangle \leq \mathrm{Z}(G/\langle z \rangle)$ and $G/\langle z \rangle$ has a normal elementary abelian subgroup of order p^3, namely $\langle G', \Omega_2(\langle c \rangle) \rangle / \langle z \rangle$. Therefore $G/\langle z \rangle$ is an A_2-group from Proposition 71.4(b) which implies $\Omega_1(G/\langle z \rangle) = \langle G', \Omega_2(\langle c \rangle) \rangle / \langle z \rangle$. Set $a^p = x$ and $b^p = y$ and consider the abelian group $M/\langle z \rangle$. If the abelian subgroup $U/\langle z \rangle$ of order p^4 and exponent $\leq p^2$ has rank > 2, then $\Omega_1(U/\langle z \rangle) > G'/\langle z \rangle$, which contradicts the above fact. Hence we get $U/\langle z \rangle \cong \mathrm{C}_{p^2} \times \mathrm{C}_{p^2}$ which implies $G' = \langle x, y, z \rangle$.

Since $\Phi(\langle c, a \rangle) = \langle c^p, x, [c, a] \rangle = \Phi(G)$ and $\Phi(\langle c, b \rangle) = \langle c^p, y, [c, b] \rangle = \Phi(G)$, we must have

$$[c, a] = x^\alpha y^\eta z^\beta, \quad [c, b] = x^\xi y^\gamma z^\delta$$

for some integers $\alpha, \beta, \gamma, \delta, \eta, \zeta \bmod p$ with $\eta \not\equiv 0 \pmod{p}$ and $\zeta \not\equiv 0 \pmod{p}$.

The maximal subgroups of G containing $\langle c \rangle$ are $\langle a, c \rangle \Phi(G)$ and $\langle a^i b, c \rangle \Phi(G)$. Therefore we must have for all integers $i \bmod p$

$$\Phi(\langle c, a^i b \rangle) = \langle c^p, x^i y, [c, a^i b] = x^{\alpha i + \xi} y^{\eta i + \gamma} z^{\beta i + \delta} \rangle = \Phi(G)$$

which is equivalent to

$$\begin{vmatrix} 0 & 0 & 1 \\ i & 1 & 0 \\ \alpha i + \zeta & \eta i + \gamma & \beta i + \delta \end{vmatrix} = \eta i^2 + (\gamma - \alpha) i - \zeta \not\equiv 0 \pmod{p}.$$

Hence the quadratic congruence $\eta i^2 + (\gamma - \alpha)i - \zeta \equiv 0 \pmod{p}$ should not have any solution in i which is equivalent to the requirement that $(\gamma - \alpha)^2 + 4\eta\zeta$ is not a square in GF(p). We have obtained the groups stated in part (b) of our theorem.

It remains to check that all maximal subgroups $\langle c^j a, c^k b\rangle\Phi(G)$ are minimal non-abelian unless $j \equiv k \equiv 0 \pmod{p}$ in which case $\langle a, b\rangle\Phi(G) = M$. Note that

$$\Phi(G) = \langle c^p\rangle \times \langle x\rangle \times \langle y\rangle \quad \text{and} \quad \Phi(\Phi(G)) = \langle c^{p^2}\rangle \geq \langle z\rangle,$$

where $\Phi(G)/\Phi(\Phi(G)) \cong \mathrm{E}_{p^3}$. We have

$$\Phi(\langle c^j a, c^k b\rangle) = \langle c^{pj} x, c^{pk} y, [c^j a, c^k b] = x^{\zeta j - \alpha k} y^{\gamma j - \eta k} z^{\delta j - \beta k + 1}\rangle < \Phi(G)$$

if and only if

$$\begin{vmatrix} j & 1 & 0 \\ k & 0 & 1 \\ 0 & \zeta j - \alpha k & \gamma j - \eta k \end{vmatrix} = \eta k^2 + (\alpha - \gamma) jk - \zeta j^2 \equiv 0 \pmod{p}.$$

The quadratic congruence in k

$$(**) \qquad \eta k^2 + (\alpha - \gamma) jk - \zeta j^2 \equiv 0 \pmod{p}$$

(where $j \in \mathrm{GF}(p)$ is fixed) has a solution in k if and only if the discriminant

$$j^2(\alpha - \gamma)^2 + 4\eta\zeta j^2 = ((\alpha - \gamma)^2 + 4\eta\zeta) j^2$$

is a square in GF(p). But we know that $(\alpha - \gamma)^2 + 4\eta\zeta$ is not a square in GF(p) and so we must have $j \equiv 0 \pmod{p}$. From $(**)$ we then get $\eta k^2 \equiv 0 \pmod{p}$ and so (noting that $\eta \not\equiv 0 \pmod{p}$) $k \equiv 0 \pmod{p}$ and we are done. □

§101

p-groups G with $p > 2$ and $\mathrm{d}(G) = 2$ having exactly one maximal subgroup which is neither abelian nor minimal nonabelian

Here we determine up to isomorphism the title groups (Theorems 101.1 and 101.2). As a result we get a complete classification of p-groups (which are not A_2-groups) from Lemma 76.5 (Theorems 100.1 and 101.1). Also, p-groups of Lemma 76.13 are completely determined (Theorems 100.2, 100.3 and 101.2).

Theorem 101.1. *Let G be a two-generator p-group, $p > 2$, with exactly one maximal subgroup M which is neither abelian nor minimal nonabelian. If G has an abelian maximal subgroup A, then we have*

$$G = \langle h, k \mid [h,k] = v,\ [v,k] = z,\ [v,h] = z^{\rho},$$
$$v^p = z^p = [z,h] = [z,k] = 1,\ h^p = z^{\sigma},\ k^{p^{n+1}} = z^{\tau}\rangle,$$

where $n \geq 1$ and ρ, σ, τ are integers mod p *with* $\rho \not\equiv 0 \pmod{p}$.

We have

$$|G| = p^{n+4}, \quad G' = \langle v, z\rangle \cong \mathrm{E}_{p^2}, \quad \mathrm{Z}(G) = \langle k^p, z\rangle, \quad \Phi(G) = \mathrm{Z}(G)G',$$
$$G' \cap \mathrm{Z}(G) = \langle z\rangle \cong \mathrm{C}_p, \quad [G', G] = \langle z\rangle$$

and so G is of class 3. *Also, $S = \langle v, h\rangle \cong \mathrm{S}(p^3)$ (if $\sigma \equiv 0 \pmod{p}$) or $S \cong \mathrm{M}_{p^3}$ (if $\sigma \not\equiv 0 \pmod{p}$), S is normal in G,*

$$G = S\langle k\rangle, \quad S \cap \langle k\rangle \leq \langle z\rangle, \quad G/S \cong \mathrm{C}_{p^{n+1}}, \quad G/\mathrm{Z}(G) \cong \mathrm{S}(p^3),$$
$$M = S\langle k^p\rangle, \quad \mathrm{d}(M) = 3, \quad M' = \langle z\rangle,$$
$$A = \mathrm{C}_G(G'), \quad \Gamma_1 = \{A, M, M_1, \ldots, M_{p-1}\},$$

where all M_i are minimal nonabelian with $M_1' = \cdots = M_{p-1}' = \langle z\rangle$. Finally, G is an L_3*-group if and only if $\tau \not\equiv 0 \pmod{p}$ and in that case $\Omega_1(G) \cong \mathrm{S}(p^3)$, $G/\Omega_1(G)$ is cyclic of order p^{n+1} ($n \geq 1$) and $\mathrm{Z}(G) = \langle k^p\rangle \cong \mathrm{C}_{p^{n+1}}$ is cyclic.*

Proof. Obviously, A is a unique abelian maximal subgroup of G (otherwise, by Exercise 1.6(a), all $p+1$ maximal subgroups of G would be abelian). By Exercise 1.69(a),

$|G' : (A'M_1')| \leq p$, where M_1 is a minimal nonabelian maximal subgroup of G and so $|G'| \leq p^2$. But if $|G'| = p$, then this fact together with $\mathrm{d}(G) = 2$ would imply (Exercise P9) that G is minimal nonabelian, a contradiction. Hence $|G'| = p^2$. Then it follows from $|G| = p|G'||Z(G)|$ (Lemma 1.1) that $|G : \mathrm{Z}(G)| = p^3$. Set $\Gamma_1 = \{A, M, M_1, \ldots, M_{p-1}\}$, where all M_i $(i = 1, \ldots, p-1)$ are minimal nonabelian. We have $\mathrm{Z}(G) \leq M_i$ (otherwise $\mathrm{d}(G) = 3$) and so $\mathrm{Z}(G) = \mathrm{Z}(M_i) = \Phi(M_i)$ for all $i = 1, \ldots, p-1$. Also, $\Phi(M_i) < \Phi(G) < M_i$ and so $\Phi(G)$ is abelian. For each $x \in G - A$, $\mathrm{C}_A(x) = \mathrm{Z}(G)$ and so $x^p \in \mathrm{Z}(G)$. Hence $G/\mathrm{Z}(G)$ is generated by its elements of order p and so $G/\mathrm{Z}(G) \cong \mathrm{S}(p^3)$ because $\mathrm{d}(G) = 2$ and so $G/\mathrm{Z}(G)$ cannot be elementary abelian. This implies

$$G' \cap \mathrm{Z}(G) \cong \mathrm{C}_p, \quad \Phi(G) = \mathrm{Z}(G)G', \quad \mathrm{cl}(G) = 3.$$

Also, $M_i' = M' = G' \cap \mathrm{Z}(G)$ for all $i = 1, \ldots, p-1$. If $\mathrm{d}(M) = 2$, then $M' \cong \mathrm{C}_p$ would imply that M is minimal nonabelian, a contradiction. Hence we get $\mathrm{d}(M) \geq 3$. In particular, $|M| \geq p^4$ and so $|G| \geq p^5$.

(i) First assume that $G' = \langle v \rangle \cong \mathrm{C}_{p^2}$ is cyclic. Since $\langle v^p \rangle = M_i'$ is not a maximal cyclic subgroup in $M_i > \Phi(G) = \mathrm{Z}(G)G'$, it follows that all M_i $(i = 1, \ldots, p-1)$ are metacyclic. In particular, $|\Omega_1(\Phi(G))| \leq p^2$. Suppose that A is also metacyclic so that M (with $\mathrm{d}(M) \geq 3$) is the only nonmetacyclic maximal subgroup of G. By a result of Y. Berkovich (see Proposition A.40.12), G is an L_3-group. But then we have $G' \leq \Omega_1(G)$, where $\Omega_1(G)$ is of order p^3 and exponent p and so $G' \cong \mathrm{E}_{p^2}$, a contradiction. It follows that A must be nonmetacyclic in which case $\Omega_1(A) \not\leq \Phi(G)$. Let a be an element of order p in $A - \Phi(G)$ and let $k \in G - A$ be such that $\langle \Phi(G), k \rangle = M_1$. Since $[k, v] \neq 1$, we may replace k with another generator of $\langle k \rangle$ so that we may assume that $[k, v] = v^p$. As $\langle k, v \rangle' = \langle v^p \rangle \leq \mathrm{Z}(G)$, it follows that $\langle k, v \rangle$ is minimal nonabelian and so $\langle k, v \rangle = M_1$. By Exercise P9, we have

$$\mathrm{Z}(G) = \Phi(M_1) = \langle k^p, v^p, [k, v] = v^p \rangle = \langle k^p, v^p \rangle.$$

All maximal subgroups of G distinct from $A = \Phi(G)\langle a \rangle$ are

$$\Phi(G)\langle a^i k \rangle = \mathrm{Z}(G)\langle a^i k, v \rangle,$$

where i is any integer mod p. Since $[a^i k, v] = [a^i, v]^k [k, v] = v^p \in \mathrm{Z}(G)$, it follows that $\langle a^i k, v \rangle$ is minimal nonabelian. Again, by Exercise P9,

$$\Phi(\langle a^i k, v \rangle) = \langle (a^i k)^p, v^p, [a^i k, v] = v^p \rangle = \langle (a^i k)^p, v^p \rangle.$$

The factor group $G/\langle v^p \rangle$ is minimal nonabelian (since we have $\mathrm{d}(G/\langle v^p \rangle) = 2$ and $(G/\langle v^p \rangle)' \cong \mathrm{C}_p$) and so computing in $G/\langle v^p \rangle$, we get

$$(a^i k)^p = a^{ip} k^p [k, a^i]^{\binom{p}{2}} x, \quad \text{where } x \in \langle v^p \rangle.$$

But $a^{ip} = 1$ and $[k, a^i] \in \langle v \rangle$ so that $[k, a^i]^{\binom{p}{2}} \in \langle v^p \rangle$ which gives $(a^i k)^p = k^p y$ for some $y \in \langle v^p \rangle$. By the above,

$$\Phi(\langle a^i k, v \rangle) = \langle k^p y, v^p \rangle = \langle k^p, v^p \rangle = \mathrm{Z}(G)$$

and so we conclude that $\Phi(G)\langle a^i k \rangle = \mathrm{Z}(G)\langle a^i k, v \rangle = \langle a^i k, v \rangle$ is minimal nonabelian for all $i = 1, \ldots, p-1$. It follows that G is an A_2-group, a contradiction.

(ii) We have proved that $G \cong \mathrm{E}_{p^2}$. Since $[G, G'] = G' \cap \mathrm{Z}(G) \cong \mathrm{C}_p$, we get by the Hall–Petrescu formula (Appendix 1) for any $x, y \in G$, $(xy)^p = x^p y^p l$ for some $l \in G' \cap \mathrm{Z}(G)$.

We have $A = \mathrm{C}_G(G')$ and we take an element $k \in G - A$ such that $\Phi(G)\langle k \rangle = M_1$ is a minimal nonabelian maximal subgroup of G. Then for any element $v \in G' - \mathrm{Z}(G)$, we get $[v, k] = z$, where $\langle z \rangle = G' \cap \mathrm{Z}(G)$. Since $\langle k, v \rangle' = \langle z \rangle$, $\langle k, v \rangle$ is minimal nonabelian and so $\langle k, v \rangle = M_1$. In particular,

$$\Phi(\langle k, v \rangle) = \langle k^p, v^p, [v, k] \rangle = \langle k^p, z \rangle = \Phi(M_1) = \mathrm{Z}(G).$$

Thus $\langle k^p \rangle$ covers $\mathrm{Z}(G)/\langle z \rangle$, where $|\mathrm{Z}(G)| \geq p^2$. Set $\mathrm{Z}(G)/\langle z \rangle \cong \Phi(G)/G' \cong \mathrm{C}_{p^n}$ with $n \geq 1$ so that $|G| = p^{n+4}$. Consider the abelian group G/G' of rank 2. Since $(G'\langle k \rangle)/G' \cong \mathrm{C}_{p^{n+1}}$, there is a subgroup S/G' of order p such that $G = S\langle k \rangle$ and $S \cap \langle k \rangle \leq \langle z \rangle$. Let $h \in S - G'$ so that $h^p \in \langle z \rangle$ since $h^p \in \mathrm{Z}(G) \cap G' = \langle z \rangle$.

Assume that $S \leq A$ in which case $h \in A - \Phi(G)$ and $G = \langle h, k \rangle$. We may assume that $[h, k] = v$ and examine all maximal subgroups $\Phi(G)\langle h^i k \rangle$ of G (i is any integer mod p) which are distinct from A. We have $[v, h^i k] = [v, k][v, h^i]^k = [v, k] = z$ and so $\langle v, h^i k \rangle$ is minimal nonabelian. On the other hand,

$$\Phi(\langle v, h^i k \rangle) = \langle v^p = 1, (h^i k)^p = h^{ip} k^p l, [v, h^i k] = z \rangle = \langle k^p, z \rangle = \mathrm{Z}(G)$$

(where $l \in \langle z \rangle$) since $(h^i k)^p = k^p l'$ for some $l' \in \langle z \rangle$. This means that $\Phi(G)\langle h^i k \rangle = \langle v, h^i k \rangle$ and so all these p maximal subgroups of G are minimal nonabelian. But then G is an A_2-group, a contradiction.

We have proved that $S \not\leq A = \mathrm{C}_G(G')$ and so $1 \neq [v, h] \in \langle z \rangle$. Since $G = \langle h, k \rangle$, we may set $[h, k] = v$ and $[v, k] = z$, where $v \in G' - \mathrm{Z}(G)$ and $\langle z \rangle = G' \cap \mathrm{Z}(G)$. Also, $[v, h] = z^\rho$, $h^p = z^\sigma$, and $k^{p^{n+1}} = z^\tau$, where ρ, σ, τ are integers mod p with $\rho \not\equiv 0 \pmod{p}$. Here $S = \langle v, h \rangle \cong \mathrm{S}(p^3)$ or M_{p^3}, S is normal in G, $G = S\langle k \rangle$ with $\langle k \rangle \cap S \leq \langle z \rangle$ and $M = S\mathrm{Z}(G) = S\langle k^p \rangle$ with $\mathrm{d}(M) = 3$.

It remains to examine all p maximal subgroups $\Phi(G)\langle h^i k \rangle$ ($i = 0, 1, \ldots, p-1$) of G which are distinct from $M = \Phi(G)\langle h \rangle = S\langle k^p \rangle$. We compute

$$[v, h^i k] = [v, k][v, h]^i = z z^{\rho i} = z^{\rho i + 1},$$

where the congruence $\rho i + 1 \equiv 0 \pmod{p}$ has exactly one solution i' for i (noting that $\rho \not\equiv 0 \pmod{p}$). Hence $A = \Phi(G)\langle h^{i'} k \rangle$ is an abelian maximal subgroup of G

and for all other $i \not\equiv i' \pmod p$ we see that $\langle v, h^i k\rangle$ is minimal nonabelian and moreover,

$$\Phi(\langle v, h^i k\rangle) = \langle v^p = 1, (h^i k)^p = h^{ip} k^p l, [v, h^i k] = z^{\rho i+1} \neq 1\rangle$$

for some $l \in \langle z\rangle$. Hence $\Phi(\langle v, a^i k\rangle) = \langle k^p, z\rangle = \mathrm{Z}(G)$ and so $\Phi(G)\langle h^i k\rangle = \langle v, h^i k\rangle$ is a minimal nonabelian maximal subgroup of G. Our theorem is proved. □

Theorem 101.2. *Let G be a two-generator p-group, $p > 2$, with exactly one maximal subgroup H which is neither abelian nor minimal nonabelian. If G has no abelian maximal subgroup, then $\Gamma_1 = \{H, H_1, \ldots, H_p\}$, where H_i $(i = 1, \ldots, p)$ are nonmetacyclic minimal nonabelian, $G' \cong \mathrm{E}_{p^3}$, $W = [G, G'] \cong \mathrm{E}_{p^2}$, $W \leq \mathrm{Z}(G)$ (and so G is of class 3) and $\mathrm{C}_G(G') = \Phi(G)$ is abelian. Moreover, $\{H', H_1', \ldots, H_p'\}$ is the set of $p + 1$ subgroups of order p in W and the following holds.*

(a) *If $|G| \geq p^6$, then we have*

$$G = \langle h, x \mid h^{p^{m+1}} = 1,\ [h, x] = v,\ h^{p^m} = u,\ [v, h] = z,$$
$$[v, x] = u^\alpha,\ v^p = z^p = [u, x] = [z, h] = [z, x] = 1,\ x^p \in \langle u, z\rangle\rangle,$$

where $m \geq 2$ and α is an integer mod p *with $\alpha \not\equiv 0 \pmod p$. Here*

$$|G| = p^{m+4}, \quad G' = \langle u, z, v\rangle \cong \mathrm{E}_{p^3}, \quad W = [G, G'] = \langle u, z\rangle \leq \mathrm{Z}(G),$$
$$\mathrm{Z}(G) = \langle h^p\rangle \times \langle z\rangle \cong \mathrm{C}_{p^m} \times \mathrm{C}_p, \quad \Phi(G) = \mathrm{Z}(G) \times \langle v\rangle.$$

Finally, $H = \Phi(G)\langle x\rangle$, where in case $x^p \in W - \langle u\rangle$ we have $\mathrm{d}(H) = 3$ and in case $x^p \in \langle u\rangle$ we have $\mathrm{d}(H) = 4$ and $H_i = \langle v, x^i h\rangle$ $(i = 1, \ldots, p)$ is the set of p nonmetacyclic minimal nonabelian maximal subgroups of G.

(b) *If $|G| = p^5$, then*

$$G = \langle h, x \mid h^{p^2} = 1,\ [h, x] = v,\ h^p = u^\alpha,\ [v, h] = z,$$
$$[v, x] = u,\ v^p = z^p = [u, x] = [z, h] = [z, x] = 1,\ h^p = u^\beta z^\gamma\rangle,$$

where α, β, γ are integers mod p *with $\beta \not\equiv 0 \pmod p$. We have $\Phi(G) = G' = \langle u, z, v\rangle \cong \mathrm{E}_{p^3}$ and $W = [G, G'] = \langle u, z\rangle = \mathrm{Z}(G) \cong \mathrm{E}_{p^2}$.*

If $p \geq 5$, then we have $\gamma \equiv \alpha \pmod p$. In that case, $\alpha \equiv 0 \pmod p$ implies $\mho_1(G) = \langle u\rangle$ and $\Omega_1(G) = H \cong \mathrm{S}(p^3) \times \mathrm{C}_p$ and $\alpha \not\equiv 0 \pmod p$ implies $\mho_1(G) = W$, $\Omega_1(G) = G'$ and $H \cong \mathrm{M}_{p^3} \times \mathrm{C}_p$. Also, all p maximal subgroups $H_i = G'\langle x^i h\rangle$ $(i$ integer mod $p)$ are nonmetacyclic minimal nonabelian.*

If $p = 3$, then either $\beta = 1$ and $\gamma \not\equiv \alpha \pmod 3$) or $\beta = -1$ and $\gamma \equiv \alpha \pmod 3$. In that case, $H = G'\langle x\rangle \cong \mathrm{S}(27) \times \mathrm{C}_3$ or $H \cong \mathrm{M}_{27} \times \mathrm{C}_3$ and all three maximal subgroups $H_i = G'\langle x^i h\rangle$ $(i$ integer mod $p)$ are nonmetacyclic minimal nonabelian.*

Proof. We set $\Gamma_1 = \{H, H_1, \ldots, H_p\}$, where H_i $(i = 1, \ldots, p)$ are minimal nonabelian. Since H is neither abelian nor minimal nonabelian, we have $|H| \geq p^4$ and so $|G| \geq p^5$.

First suppose that two distinct minimal nonabelian maximal subgroups of G have the same commutator subgroup, say, $H_1' = H_2'$. Then considering G/H_1' (see Exercise 1.6(a)), we see that all maximal subgroups of G/H_1' are abelian and so we get

$$H' = H_1' = \cdots = H_p' = \langle z \rangle \cong \mathrm{C}_p.$$

By Exercise 1.69(a), we have $|G' : (H_1'H_2')| = |G' : H_1'| \leq p$, and so $|G'| \leq p^2$. But if $|G'| = p$, then this fact together with $\mathrm{d}(G) = 2$ implies (see Exercise P9) that G is minimal nonabelian, a contradiction. Hence $|G'| = p^2$. Also, $\mathrm{d}(H) \geq 3$ and so H is nonmetacyclic. Indeed, if $\mathrm{d}(H) = 2$, then (noting that $|H'| = p$) H would be minimal nonabelian, a contradiction.

Suppose for a moment that $G' = \langle v \rangle \cong \mathrm{C}_{p^2}$ is cyclic. Then $H_1' = \cdots = H_p' = \langle v^2 \rangle$ and $G' = \langle v \rangle \leq H_i$ so that H_i' is not a maximal cyclic subgroup in H_i and therefore H_i is metacyclic for all $i = 1, \ldots, p$. By Proposition A.40.12, G is an L_3-group. But in that case, G' is of exponent p, a contradiction. We have proved that $G' \cong \mathrm{E}_{p^2}$.

We notice that $\Phi(G) = H_1 \cap H_2$ is a maximal normal abelian subgroup of G. Taking elements $h_1 \in H_1 - \Phi(G)$ and $h_2 \in H_2 - \Phi(G)$, we have $\langle h_1, h_2 \rangle = G$ and so $s = [h_1, h_2] \in G' - \langle z \rangle$ and $s \notin \mathrm{Z}(G)$. Indeed, if $s \in \mathrm{Z}(G)$, then $G/\langle s \rangle$ would be abelian, a contradiction. In particular, $[G, G'] = \langle z \rangle = H_1'$ and so G is of class 3. Since $s \notin \mathrm{Z}(G)$, we have $s \notin \mathrm{Z}(H_1)$ or $s \notin \mathrm{Z}(H_2)$ and we may assume without loss of generality that $s \notin \mathrm{Z}(H_1)$. Suppose that there is an element $x \in H_1 - \Phi(G)$ such that $x^p \in \langle z \rangle$. Then $G'\langle x \rangle$ is minimal nonabelian of order p^3 and so $G'\langle x \rangle = H_1$, contrary to $|G| \geq p^5$. Assume that $\langle z \rangle = H_1'$ is not a maximal cyclic subgroup in H_1. Then there is $v \in \Phi(G)$ such that $v^2 = z$. This implies that all H_i, $i = 1, \ldots, p$, are metacyclic. Again by Proposition A.40.12, G is an L_3-group. This means that the subgroup $U = \Omega_1(G)$ is of order p^3 and exponent p and G/U is cyclic of order $\geq p^2$. We have $G' \leq U$ and so if U is nonabelian, then $\mathrm{C}_G(G')$ covers G/U and $\mathrm{C}_G(G')$ is an abelian maximal subgroup of G, a contradiction. If U is elementary abelian, then $|G : \mathrm{C}_G(U)| = p$ since a Sylow p-subgroup of $\mathrm{GL}_3(p)$ is isomorphic to $\mathrm{S}(p^3)$ and so is of exponent p. But in that case, $\mathrm{C}_G(U)$ is an abelian maximal subgroup of G, a contradiction. Hence $\langle z \rangle = H_1'$ is a maximal cyclic subgroup in H_1 which yields that H_1 is nonmetacyclic. Noting that $|H_1| \geq p^4$, we get

$$E = \Omega_1(H_1) = \Omega_1(\Phi(G)) \cong \mathrm{E}_{p^3}$$

which also implies that all H_i are nonmetacyclic.

By the previous paragraph, $\Omega_1(\langle h_1 \rangle) = \langle u \rangle \leq E$ and $u \in E - G'$. Further, we have $H_1 = E\langle h_1 \rangle$ and so H_1 is a splitting extension of G' by $\langle h_1 \rangle$, where $o(h_1) = p^n$, $n \geq 2$. Since G/G' is abelian of rank 2, we get $G = H_1F$ with $H_1 \cap F = G'$ and $|F : G'| = p$. We have $G/F \cong H_1/G' \cong \mathrm{C}_{p^n}$. If F is nonabelian, then $\mathrm{C}_G(G')$

covers G/F and so $\mathrm{C}_G(G')$ is an abelian maximal subgroup of G, a contradiction. Hence F is abelian. Assume that $\mho_1(F) \not\leq \langle z\rangle$. Then we obtain that $|\mho_1(F)| = p$ and $G' = \langle z\rangle \times \mho_1(F) \leq \mathrm{Z}(G)$, a contradiction. Hence $\mho_1(F) \leq \langle z\rangle$ and so for an element $x \in F - G'$ we have $x^p \in \langle z\rangle$.

Since G satisfies $G = \langle h_1, x\rangle$, we may set $[x, h_1] = s \in G' - \langle z\rangle$ and $[s, h_1] = z$, where $H_1' = \langle z\rangle \leq \mathrm{Z}(G)$. Then $x^{h_1} = xs$, $s^{h_1} = sz$ and $s^{h_1^i} = sz^i$ for all $i \geq 1$. We get

$$x^{h_1^2} = (xs)^{h_1} = (xs)(sz) = xs^2z$$

and claim that we have $x^{h_1^i} = xs^i z^{\binom{i}{2}}$ for all $i \geq 2$. Indeed, by induction on i,

$$x^{h_1^{i+1}} = (x^{h_1})^{h_1^i} = (xs)^{h_1^i} = (xs^i z^{\binom{i}{2}})(sz^i) = xs^{i+1}z^{\binom{i}{2}+i} = xs^{i+1}z^{\binom{i+1}{2}}.$$

Our formula gives $x^{h_1^p} = xs^p z^{\binom{p}{2}} = x$ and so $F\langle h_1^p\rangle$ is an abelian maximal subgroup of G, a contradiction.

We have proved that $H_1' = \langle z_1\rangle$, $H_2' = \langle z_2\rangle, \ldots, H_p' = \langle z_p\rangle$ are pairwise distinct subgroups of order p in $G' \cap \mathrm{Z}(G)$. By Exercise 1.69(a), we get $|G' : (H_1'H_2')| \leq p$ and so $|G'| \leq p^3$. Set $W = \langle z_1, \ldots, z_p\rangle$ so that W is an elementary abelian subgroup of order $\geq p^2$ contained in $G' \cap \mathrm{Z}(G)$ which implies that G' is abelian of exponent $\leq p^2$. We have $G = \langle x, y\rangle$ for some $x, y \in G$. If $[x, y] \in \mathrm{Z}(G)$, then $G/\langle [x, y]\rangle$ is abelian which implies that $G' = \langle [x, y]\rangle$ is cyclic, contrary to the fact that $W \leq G'$. Thus $[x, y] \in G' - W$ which gives

$$|G'| = p^3, \quad W \cong \mathrm{E}_{p^2}, \quad \{1\} \neq [G, G'] \leq W \leq \mathrm{Z}(G)$$

and so G is of class 3. Let $\langle z_{p+1}\rangle$ be the subgroup of order p in W with $\langle z_{p+1}\rangle \neq \langle z_i\rangle$ for all $i = 1, \ldots, p$.

For any fixed $i \in \{1, \ldots, p\}$ we consider $G/\langle z_i\rangle$, where $H_i/\langle z_i\rangle$ is abelian (and two-generated) and $H_j/\langle z_i\rangle$ is minimal nonabelian for all $j \neq i$, $j \in \{1, \ldots, p\}$. This implies that $H/\langle z_i\rangle$ must be nonabelian (Exercise 1.6(a)). If $G/\langle z_i\rangle$ is metacyclic, then Theorem 36.1 gives that G is also metacyclic, contrary to $\mathrm{E}_{p^2} \cong W \leq G'$. Hence $G/\langle z_i\rangle$ is nonmetacyclic. Suppose that $H/\langle z_i\rangle$ is minimal nonabelian. Then $G/\langle z_i\rangle$ is a nonmetacyclic A_2-group. If $|G/\langle z_i\rangle| > p^4$, then Theorem 65.7(a) implies that $G'/\langle z_i\rangle \cong \mathrm{E}_{p^2}$. Suppose that $|G/\langle z_i\rangle| = p^4$ and $G'/\langle z_i\rangle \cong \mathrm{C}_{p^2}$. In that case, each maximal subgroup of $G/\langle z_i\rangle$ is metacyclic and so $G/\langle z_i\rangle$ is minimal nonmetacyclic. By Theorem 69.1, $G/\langle z_i\rangle$ is a group of maximal class and order 3^4. But in that case, $G'/\langle z_i\rangle$ cannot be cyclic (see Exercise 9.1(c)). We have proved that in any case $G'/\langle z_i\rangle \cong \mathrm{E}_{p^2}$. Assume now that $H/\langle z_i\rangle$ is not minimal nonabelian and we know already that $H/\langle z_i\rangle$ is nonabelian. By Theorem 101.1, we have again $G'/\langle z_i\rangle \cong \mathrm{E}_{p^2}$. As a consequence we get $[x, y]^p \in \langle z_i\rangle$ for each $i = 1, \ldots, p$ which implies that $[x, y]^p = 1$ and so $G' \cong \mathrm{E}_{p^3}$ is elementary abelian.

By Lemma 36.5(b), $G'/[G, G']$ is cyclic and so $[G, G'] = W$ (since $[G, G'] \leq W$). Since $(G/W)' \cong \mathrm{C}_p$ and $\mathrm{d}(G/W) = 2$, G/W is minimal nonabelian (Exercise P9)

and so H/W is abelian which implies $\{1\} \neq H' \leq W$. Suppose that $H' = \langle z_j \rangle$ for some $j \in \{1, \ldots, p\}$. Then $G/\langle z_j \rangle$ is nonabelian with at least two distinct abelian maximal subgroups $H_j/\langle z_j \rangle$ and $H/\langle z_j \rangle$. But then $(G/\langle z_j \rangle)' \cong \mathrm{C}_p$ (Exercise P1), a contradiction. We have proved that $H' = \langle z_{p+1} \rangle$ or $H' = W$.

Suppose that $H' = W \leq \mathrm{Z}(G)$. In that case, $\mathrm{d}(H) \geq 3$. Indeed, if $\mathrm{d}(H) = 2$, then H is a two-generator group of class 2 in which case H' must be cyclic (Proposition 36.5(a)), a contradiction. Consider $G/\langle z_{p+1} \rangle$ with $\mathrm{d}(G/\langle z_{p+1} \rangle) = 2$ and having minimal nonabelian maximal subgroups $H_i/\langle z_{p+1} \rangle$ for all $i = 1, \ldots, p$. The remaining maximal subgroup $H/\langle z_{p+1} \rangle$ is neither abelian nor minimal nonabelian since $\mathrm{d}(H/\langle z_{p+1} \rangle) \geq 3$. But $(H_i/\langle z_{p+1} \rangle)' = W/\langle z_{p+1} \rangle$ for all $i = 1, \ldots, p$, contrary to the first part of this proof. Hence we must have $H' = \langle z_{p+1} \rangle$.

We have proved that $H', H_1', \ldots, H_p'$ are $p+1$ pairwise distinct subgroups of order p in W. Since H is not minimal nonabelian, we have $\mathrm{d}(H) \geq 3$ and so $|H| \geq p^4$ and $|G| \geq p^5$. Also, $\Omega_1(H_i) = G' \leq \Phi(G)$ for all $i = 1, \ldots, p$, where $\Phi(G)$ is abelian. Therefore we have either $\mathrm{C}_G(G') = \Phi(G)$ or $\mathrm{C}_G(G')$ is a maximal subgroup of G. In any case, there exist two minimal nonabelian maximal subgroups of G, say H_1 and H_2, such that $G' \not\leq \mathrm{Z}(H_1)$ and $G' \not\leq \mathrm{Z}(H_2)$. Then $H_1 \cap H_2 = \Phi(G)$ and taking some elements $h_1 \in H_1 - \Phi(G)$ and $h_2 \in H_2 - \Phi(G)$, we have $\langle h_1, h_2 \rangle = G$ and so $v = [h_1, h_2] \in G' - W$. Indeed, if $v \in W$, then $G/\langle v \rangle$ is abelian, a contradiction. We may set $[v, h_1] = z_1$ and $[v, h_2] = z_2$ so that $H_1' = \langle z_1 \rangle$, $H_2' = \langle z_2 \rangle$ and $W = \langle z_1 \rangle \times \langle z_2 \rangle$. All maximal subgroups of G are $H_1 = \Phi(G)\langle h_1 \rangle$ and $\Phi(G)\langle h_1^i h_2 \rangle$, where i is any integer mod p. We compute

$$[v, h_1^i h_2] = [v, h_2][v, h_1^i]^{h_2} = z_2 (z_1^i)^{h_2} = z_1^i z_2 \neq 1$$

which shows $\mathrm{C}_G(v) = \Phi(G)$ and so $\mathrm{C}_G(G') = \Phi(G)$. As $\langle v, h_1 \rangle$ (with $[v, h_1] = z_1$) is minimal nonabelian, we have $\langle v, h_1 \rangle = H_1 = G'\langle h_1 \rangle$. Hence $H_1/G' \cong \mathrm{C}_{p^m}$ is cyclic of order p^m, $m \geq 1$, and $h_1^{p^m} \in W - \langle z_1 \rangle$. The abelian group G/G' is of rank 2 and so G/G' is of type (p^m, p) and $|G| = p^{m+4}$. Finally,

$$\Phi(G) = G'\langle h_1^p \rangle = \langle h_1^p \rangle \times \langle v \rangle \times \langle z_1 \rangle$$

is abelian of type (p^m, p, p).

(i) First suppose that $m \geq 2$. Set $u = h_1^{p^m}$ so that $u \in W - H_1'$, $o(h_1) = p^{m+1} \geq p^3$ and $\Phi(G)/G'$ is cyclic of order $p^{m-1} \geq p$ since $H_1/G' \cong \mathrm{C}_{p^m}$. Consider any H_i for $2 \leq i \leq p$ so that $H_i \cap H_1 = \Phi(G)$. Let $h_i \in H_i - \Phi(G)$ and $v \in G' - W$ so that $1 \neq [h_i, v] = z_i$ and $H_i' = \langle z_i \rangle$. Since $\langle h_i, v \rangle$ is minimal nonabelian, we have $\langle h_i, v \rangle = H_i = G'\langle h_i \rangle$ and so H_i/G' is also cyclic of order p^m. Further, we have $h_i^p \in \Phi(G) - G'$ and $\langle h_i^p \rangle$ covers $\Phi(G)/G'$. It follows $h_i^p = h_1^{\delta p} k$ for some $k \in G'$ and $\delta \not\equiv 0 \pmod{p}$. Then

$$h_i^{p^2} = h_1^{\delta p^2} \quad \text{and so} \quad \langle h_i^{p^m} \rangle = \langle u \rangle, \quad \text{where } u = h_1^{p^m},$$

and this implies that $u \in W - H_i'$. We have proved that $u \notin H_i'$ for all $i = 1, \ldots, p$ which forces $\langle u \rangle = H'$.

Since G/G' is abelian of type (p^m, p), $m \geq 2$, we get $G = H_1 F$ with $H_1 \cap F = G'$ and $|F : G'| = p$. For the maximal subgroup $\Phi(G)F$ of G we have

$$(\Phi(G)F)/G' = (\Phi(G)/G') \times (F/G') \cong \mathrm{C}_{p^{m-1}} \times \mathrm{C}_p$$

and so $(\Phi(G)F)/G'$ is not cyclic which implies that $\Phi(G)F = H$. Taking the elements $h_1 = h \in H_1 - \Phi(G)$ and $x \in F - \Phi(G)$, we have $o(x) \leq p^2$, $G = \langle h, x \rangle$ and so $v = [h, x] \in G' - W$. We set again $u = h^{p^m}$ and we know that $H' = \langle u \rangle$. Also set $[v, h] = z_1 = z$, where $H_1' = \langle z \rangle$, $W = \langle u \rangle \times \langle z \rangle$, $v^h = vz$ and $v^{h^j} = vz^j$ for $j \geq 1$. Since $\mathrm{C}_G(G') = \mathrm{C}_G(v) = \Phi(G)$, we have $x^p \in W = \langle u, z \rangle$ and $[v, x] = u^\alpha$ with $\alpha \not\equiv 0 \pmod{p}$. We have obtained all relations stated in part (a) of our theorem. From $[h, x] = v$ we get

$$[h^2, x] = [h, x]^h [h, x] = v^h v = (vz)v = v^2 z.$$

We prove by induction on $j \geq 2$ that $[h^j, x] = v^j z^{\binom{j}{2}}$. Indeed,

$$\begin{aligned}[h^{j+1}, x] &= [hh^j, x] = [h, x]^{h^j} [h^j, x] = v^{h^j} (v^j z^{\binom{j}{2}}) = (vz^j)(v^j z^{\binom{j}{2}}) \\ &= v^{j+1} z^{j + \binom{j}{2}} = v^{j+1} z^{\binom{j+1}{2}}.\end{aligned}$$

In particular, $[h^p, x] = v^p z^{\binom{p}{2}} = 1$ and so $h^p \in \mathrm{Z}(G)$ since $G = \langle h, x \rangle$. We get

$$\mathrm{Z}(G) = \langle h^p \rangle \times \langle z \rangle \cong \mathrm{C}_{p^m} \times \mathrm{C}_p \quad \text{and} \quad \Phi(G) = \mathrm{Z}(G) \times \langle v \rangle.$$

Further, we have $H = F * \langle h^p \rangle$ with $F \cap \langle h^p \rangle = \langle u \rangle$. If $x^p \in W - \langle u \rangle$, then F is minimal nonabelian and so $\mathrm{d}(H) = 3$. If $x^p \in \langle u \rangle$, then $F = \langle v, x \rangle \times \langle z \rangle$, where $\langle u \rangle = \mathrm{Z}(\langle v, x \rangle)$ and $\langle v, x \rangle \cong \mathrm{S}(p^3)$ or M_{p^3} and so $\mathrm{d}(H) = 4$.

Finally, we have to check all p maximal subgroups $H_i = \Phi(G)\langle x^i h \rangle$ of G which are distinct from H and we have to show that they are minimal nonabelian. We have

$$[v, x^i h] = [v, h][v, x^i]^h = z(u^{\alpha i})^h = zu^{\alpha i},$$

where $\langle zu^{\alpha i} \rangle$ are pairwise distinct subgroups of order p in W for $i = 1, \ldots, p$ since $\alpha \not\equiv 0 \pmod{p}$). Thus $\langle v, x^i h \rangle$ is minimal nonabelian with $\langle v, x^i h \rangle' = \langle zu^{\alpha i} \rangle \neq \langle u \rangle$. By the Hall–Petrescu formula (Appendix 1), we get for all $r, s \in G$,

$$(rs)^{p^m} = r^{p^m} s^{p^m} c_2^{\binom{p^m}{2}} c_3^{\binom{p^m}{3}},$$

where $c_2 \in G'$ and $c_3 \in W = [G, G']$. But $m \geq 2$ and so $(rs)^{p^m} = r^{p^m} s^{p^m}$. We get

$$(x^i h)^{p^m} = (x^i)^{p^m} h^{p^m} = h^{p^m} = u$$

and so $o(x^i h) = p^{m+1}$ which together with $\langle v, x^i h \rangle = G' \langle x^i h \rangle$ and $G' \cap \langle x^i h \rangle = \langle u \rangle$ implies that $|\langle v, x^i h \rangle| = p^{m+3}$. But $|G| = p^{m+4}$ and so $\langle v, x^i h \rangle = H_i$ is minimal nonabelian and we are done.

(ii) Suppose that $m = 1$. Then $|G| = p^5$ and $G' = \Phi(G)$ with $\mathrm{C}_G(G') = G'$. We have $H_1 \cap H = G'$ and since $\Omega_1(H_1) = G'$, we get

$$1 \neq h^p \in W = [G, G'] = \mathrm{Z}(G) \cong \mathrm{E}_{p^2}$$

for an element $h \in H_1 - G'$. Also, we have $\mho_1(G) \leq W$. Take an element $x \in H - G'$ so that $x^p \in W$, $G = \langle h, x\rangle$ and $v = [h, x] = G' - W$. Set $[v, x] = u$ so that $1 \neq u \in W$ and $\langle u\rangle = H'$. Then $[v, h] = z \notin \langle u\rangle$ from which we conclude that $H_1' = \langle z\rangle$ and $W = \langle u\rangle \times \langle z\rangle$. Since $\langle v, x\rangle$ is minimal nonabelian, we have $\langle v, x\rangle \neq H$ which implies $x^p = u^\alpha$ (for some integer $\alpha \bmod p$) and $H = \langle v, x\rangle \times \langle z\rangle$, where $\langle v, x\rangle \cong \mathrm{S}(p^3)$ or M_{p^3}. Since H_1 is nonmetacyclic minimal nonabelian, $\langle z\rangle$ is a maximal cyclic subgroup in H_1 which implies $h^p = u^\beta z^\gamma$ with $\beta \not\equiv 0 \pmod p$. All p maximal subgroups $H_i = G'\langle x^i h\rangle$ (i is any integer mod p) of G which are distinct from H must be minimal nonabelian. Since

$$[v, x^i h] = [v, h][v, x^i]^h = z(u^i)^h = zu^i \neq 1$$

and $\langle v, x^i h\rangle$ is minimal nonabelian with $\langle v, x^i h\rangle' = \langle u^i z\rangle$ and so we must have that $H_i = \langle v, x^i h\rangle$, we get $\langle (x^i h)^p\rangle \neq \langle u^i z\rangle$ or, equivalently,

$$(*) \qquad \langle (x^i h)^p, u^i z\rangle = \langle u, z\rangle$$

for all integers $i \pmod p$.

(ii1) First we assume $p \geq 5$ in which case G is regular. By the Hall–Petrescu formula (Appendix 1), we have in our case for all $r, s \in G$,

$$(rs)^p = r^p s^p c_2^{\binom{p}{2}} c_3^{\binom{p}{3}},$$

where $c_2 \in G'$ and $c_3 \in W = [G, G']$ and so $(rs)^p = r^p s^p$. Hence

$$(x^i h)^p = x^{pi} h^p = u^{\alpha i}(u^\beta z^\gamma) = u^{\alpha i + \beta} z^\gamma.$$

Our condition $(*)$ is equivalent to

$$\begin{vmatrix} \alpha i + \beta & \gamma \\ i & 1 \end{vmatrix} = (\alpha - \gamma)i + \beta \not\equiv 0 \pmod p$$

for all integers $i \pmod p$, where we know that $\beta \not\equiv 0 \pmod p$. This is equivalent to $\alpha - \gamma \equiv 0 \pmod p$ and so $\gamma \equiv \alpha \pmod p$. If $\alpha \equiv 0 \pmod p$, then

$$\mho_1(G) = \langle u\rangle \quad \text{and} \quad \Omega_1(G) = H \cong \mathrm{S}(p^3) \times \mathrm{C}_p.$$

In case $\alpha \not\equiv 0 \pmod p$ we get $\mho_1(G) = W$ and $\Omega_1(G) = G'$ so that $H \cong \mathrm{M}_{p^3} \times \mathrm{C}_p$.

(ii2) Finally, we suppose $p = 3$. In that case, the Hall–Petrescu formula gives for all $r, s \in G$, $(rs)^3 = r^3 s^3 c_3$, where $c_3 \in W$. This is not a sufficient information because

we have to know exactly the element c_3. Using the usual commutator identities (see §7, p. 98) together with $xy = yx[x, y]$, we compute exactly $(rs)^3$. We get

$$\begin{aligned}(rs)^2 &= r(sr)s = r(rs[s, r])s = r^2s(s[s, r][s, r, s]) = r^2s^2[s, r][s, r, s],\\ (rs)^3 &= r^2s^2[s, r][s, r, s] \cdot rs = r^2s^2 \cdot r[s, r]s[s, r, r][s, r, s]\\ &= r^2(s^2r)s[s, r][s, r, s][s, r, r][s, r, s].\end{aligned}$$

But we have

$$\begin{aligned}r^2(s^2r)s[s, r] &= r^2(rs^2[s^2, r])s[s, r] = r^3s^3[s^2, r][s^2, r, s][s, r]\\ &= r^3s^3[s, r][s, r]^s[s^2, r, s][s, r] = r^3s^3[s, r]([s, r][s, r, s])[s^2, r, s][s, r]\\ &= r^3s^3[s, r, s][s^2, r, s]\end{aligned}$$

and so

$$(1)\qquad (rs)^3 = r^3s^3[s, r, s][s^2, r, s][s, r, s][s, r, r][s, r, s] = r^3s^3[s^2, r, s][s, r, r].$$

Also, we get

$$[s^2, r] = [s, r]^s[s, r] = [s, r][s, r, s][s, r] = [s, r]^2[s, r, s]$$

and then

$$[s^2, r, s] = [[s, r]^2[s, r, s], s] = [[s, r]^2, s] = [s, r, s]^{[s,r]}[s, r, s] = [s, r, s]^2$$

which together with (1) yields

$$(rs)^3 = r^3s^3[s, r, s]^2[s, r, r] = r^3s^3[s, r, s]^{-1}[s, r, r] = r^3s^3[s, [s, r]][[s, r], r].$$

Thus we have obtained the formula

$$(**)\qquad (rs)^3 = r^3s^3[s, [s, r]][[s, r], r].$$

Since $\langle h^p, z\rangle = \langle u^\beta z^\gamma, z\rangle = \langle u, z\rangle$ (noting that $\beta \not\equiv 0 \pmod 3$),we have to use our condition $(*)$ only for $i = 1, 2$. By $(**)$,

$$(xh)^3 = x^3h^3[h, [h, x]][[h, x], x] = u^\alpha u^\beta z^\gamma [h, v][v, x] = u^{\alpha+\beta+1}z^{\gamma-1},$$

and so from $\langle u^{\alpha+\beta+1}z^{\gamma-1}, uz\rangle = \langle u, z\rangle$ we get

$$(2)\qquad \begin{vmatrix}\alpha+\beta+1 & \gamma-1\\ 1 & 1\end{vmatrix} = \alpha+\beta-\gamma-1 \not\equiv 0 \pmod 3.$$

We compute $[h, x^2] = [h, x][h, x]^x = vv^x = v(vu) = v^2u$ and so by $(**)$,

$$(x^2h)^3 = x^6h^3[h, v^2u][v^2u, x^2] = u^{2\alpha}(u^\beta z^\gamma)z^{-2}u = u^{-\alpha+\beta+1}z^{\gamma+1}.$$

From our condition $(*)$ for $i = 2$ we get $\langle u^{-\alpha+\beta+1}z^{\gamma+1}, u^2 z\rangle = \langle u, z\rangle$ or, equivalently,

$$\begin{vmatrix} -\alpha+\beta+1 & \gamma+1 \\ -1 & 1 \end{vmatrix} = -\alpha+\beta+\gamma-1 \not\equiv 0 \pmod 3. \tag{3}$$

Now, (2) and (3) hold if and only if

$$(\alpha+\beta-\gamma-1)(-\alpha+\beta+\gamma-1) \not\equiv 0 \pmod 3.$$

This is equivalent to

$$((\beta-1)+(\alpha-\gamma))((\beta-1)-(\alpha-\gamma)) \not\equiv 0 \pmod 3 \quad \text{or}$$
$$(\beta-1)^2-(\alpha-\gamma)^2 \not\equiv 0 \pmod 3.$$

Hence if $\beta = 1$, then $\gamma \not\equiv \alpha \pmod 3$ and if $\beta = -1$, then $\gamma \equiv \alpha \pmod 3$.

We have obtained the groups stated in part (b) of our theorem which is now completely proved. □

§103

Some results of Jonah and Konvisser

In this section we will present another approach to counting theorems due to Jonah and Konvisser [KonJ, JKon].

Definition 1. Let G be a p-group. The line $\overline{M_1M_2}$ determined by two distinct maximal subgroups M_1 and M_2 of G is the set of all maximal subgroups of G containing $M_1 \cap M_2$.

Obviously, $|\overline{M_1M_2}| = p + 1$, i.e., every line contains exactly $p + 1$ points.

Proposition 103.1. *Let Π be a finite projective space in which each line contains $p+1$ points and let f be a function from the points of Π to the set of integers. Suppose that there is a point $m_0 \in \Pi$ with the following property:*

If m_1 and m_2 are two points different from m_0 on the same line through m_0, then $f(m_1) \equiv f(m_2) \pmod{p}$.

Then $\sum_{m\in\Pi} f(m) \equiv f(m_0) \pmod{p}$.

Proof. We have

$$\sum_{m\in\Pi} f(m) = f(m_0) + \sum_{L'\subset\Pi}\Big(\sum_{m\in L'} f(m)\Big),$$

where L runs over all lines of Π through m_0 and $L' = L - \{m_0\}$. Furthermore,

$$\sum_{m\in L'} f(m) \equiv |L'|f(m) \equiv 0 \pmod{p}$$

since f is constant (mod p) on the points of L' and $|L'| = p$ by hypothesis. The two displayed formulas yield the result. □

Applying these ideas to p-groups, we get the following

Theorem 103.2. *Let G be a p-group, $\mathcal{C}$ be a nonempty set of proper subgroups of G and $\alpha(H)$ be the number of elements of $\mathcal{C}$ contained in $H \leq G$. Suppose that:*

(i) *For each proper normal subgroup M of G which contains an element of $\mathcal{C}$, one has $\alpha(M) \equiv 1 \pmod{p}$.*

(ii) *There is a maximal subgroup M_0 of G with the property: if a maximal subgroup $M_1 \neq M_0$ contains an element of $\mathcal{C}$, then so do all maximal subgroups on the line $\overline{M_0M_1}$.*

Then $\alpha(G) \equiv 1 \pmod{p}$ or, what is the same, $|\mathcal{C}| \equiv 1 \pmod{p}$ since $\alpha(G) = |\mathcal{C}|$.

Proof. By Hall's enumeration principle and Proposition 103.1, we have

$$\alpha(G) \equiv \sum_{M \in \Gamma_1} \alpha(M) \equiv \alpha(M_0)|\Gamma_1| \equiv 1 \pmod{p}$$

since, by hypothesis, if $M \in \Gamma_1 - \{M_0\}$, then $\alpha(M) \equiv \alpha(M_0) \equiv 1 \pmod{p}$ and $|\Gamma_1| \equiv 1 \pmod{p}$. □

At this point it is appropriate to give the following

Definition 2. Let $\mathcal{C}$ be a nonempty set of proper subgroups of a p-group G.

(a) A maximal subgroup M_0 of G which satisfies Lemma 103.2(ii) is called an *origin* (for $\mathcal{C}$).

(b) A proper subgroup L of G is called a *local origin* if for each $M \in \Gamma_1$ the intersection $L \cap M$ contains an element of $\mathcal{C}$.

(c) A pair E_1, E_2 of distinct elements of the set $\mathcal{C}$ is said to *support good lines* if each maximal subgroup $M < G$ containing $E_1 \cap E_2$ also contains an element of $\mathcal{C}$.

Proposition 103.3 (Method of locating origins). *Let $\mathcal{C}$ be a nonempty set, closed under conjugation, of proper subgroups of a p-group G satisfying $\alpha(M) = 0$ or $\alpha(M) \equiv 1 \pmod{p}$ for each $M \in \Gamma_1$. Then G contains an origin M_0 if any at least one of the following three conditions is satisfied:*

(a) *G contains a local origin L, in which case any maximal subgroup $M \geq L$ is an origin.*

(b) *Each pair of distinct G-invariant elements $E_1, E_2 \in \mathcal{C}$ supports good lines, in which case any maximal subgroup M of G containing an element of $\mathcal{C}$ is an origin.*

(c) *A maximal subgroup M of G contains a family $E_1, \ldots, E_m$ of G-invariant elements of the set $\mathcal{C}$ satisfying: if E is a G-invariant element of the set $\mathcal{C}$, then for some $i \in \{1, \ldots, m\}$, the pair E, E_i supports good lines, in which case M is an origin.*

Proof. Statement (a) follows from the definitions. Indeed, let $L \leq M_0 \in \Gamma_1$ and let $M \in \Gamma_1 - \{M_0\}$. Then $\alpha(M_0) \equiv 1 \pmod{p}$ and $\alpha(M) \equiv 1 \pmod{p}$ since L is a local origin. It follows that M_0 is an origin.

(b) Let $M_0 \in \Gamma_1$ contain an element of the set $\mathcal{C}$. Then M_0 contains a G-invariant element $E_0 \in \mathcal{C}$ since $\alpha(M_0) \equiv 1 \pmod{p}$ in view of $\alpha(M_0) > 0$. For the same

reasons, each $M_1 \in \Gamma_1$ contains a G-invariant element E_1 of the set $\mathcal{C}$ whenever M_1 contains an element of the set $\mathcal{C}$. Thus each M on the line $\overline{M_0 M_1}$ contains an element of the set $\mathcal{C}$ for $M > M_0 \cap M_1 \geq E_0 \cap E_1$, which in turn implies that M contains a G-invariant element of $\mathcal{C}$ because the G-invariant pair E_0, E_1 supports good lines by hypothesis.

Statement (c) follows as (b). □

Exercise 1 coincides with the case $n = 2$ of Theorem 1.10(b).

Exercise 1. Let G be a noncyclic p-group, $p > 2$. Then the number of noncyclic subgroups of order p^2 in G is congruent to 1 (mod p).

Solution. We use induction on $|G|$. Let $\mathcal{C}$ be the set of all abelian subgroups of type (p, p) in G; then $\mathcal{C}$ is nonempty (Lemma 1.4) and G-invariant. By induction, if $\mathrm{E}_{p^2} \cong E \leq M_1 \in \Gamma_1$, then $\alpha(M_1) \equiv 1 \pmod{p}$ so that M_1 contains a G-invariant abelian subgroup E_1 of type (p, p). One may assume that $\alpha(G) > 1$. Let $E_2 \neq E_1$ be a G-invariant element of the set $\mathcal{C}$ (if E_2 does not exist, the result is obvious). Then the product $E_1 E_2$ is a group of order $\leq p^4$ and exponent p since $p > 2$. Since $(E_1 E_2) \cap M$ contains an abelian subgroup of type (p, p) for all $M \in \Gamma_1$, it follows that $E_1 E_2$ is a local origin; then M is an origin. By Lemma 103.2, $\alpha(G) \equiv 1 \pmod{p}$.

Exercise 2 (Sylow). Let G be a group of order p^m and $n < m$. Then the number of subgroups of order p^n in G is congruent to 1 (mod p).

Hint. Let $\mathcal{C}$ be the set of all subgroups of order p^n in G. As above, $\mathcal{C}$ contains a G-invariant element E_1. If $E_2 \neq E_1$ is another G-invariant element of the set $\mathcal{C}$ (if E_2 does not exist, the result is obvious), then, obviously, $E_1 E_2$ is a local origin (indeed, $M \cap E_1 E_2$ contains an element from $\mathcal{C}$ for $M \in \Gamma_1$). Now the result follows from Lemma 103.2.

In the previous two exercises one can take as $\mathcal{C}$ the set of all G-invariant subgroups of the set $\mathcal{C}$ defined in these exercises.

The following result is also known (see Theorem 10.4).

Proposition 103.4. *Let G be a p-group, $p > 2$. If G contains an elementary abelian subgroup of order p^3, then the number of such subgroups in G is congruent to* 1 (mod p).

Proof. We use induction on $|G|$. Let $\mathcal{C}$ be the set of all elementary abelian subgroups of order p^3 in G. Then, as above, there exists a G-invariant element $E_1 \in \mathcal{C}$. Let $E_2 \neq E_1$ be a G-invariant element in $\mathcal{C}$ (see Exercises 1 and 2). Set $H = E_1 E_2$; then $\exp(H) = p$ since $p > 2$ and $\mathrm{cl}(H) \leq 2$ (see Theorems 7.1(b) and 7.2(b)). Then one of the following assertions holds:

(i) $|H| = p^4$. Then $E_1 \cap E_2 \leq \mathrm{Z}(H)$. Let a maximal subgroup M of G contain $E_1 \cap E_2$. If $H \leq M$, then H and so M contains an element of $\mathcal{C}$. If $H \not\leq M$, then

$H \cap M$ is an element of $\mathcal{C}$ since $|H \cap M| = p^3$ and $E_1 \cap E_2 < H \cap M < H$ so $H \cap M$ is elementary abelian of order p^3 since $E_1 \cap E_2 \leq \mathrm{Z}(H)$ and $\exp(H \cap M) = p$. We see that the pair E_1, E_2 supports good lines.

(ii) $|H| \geq p^5$. If $M \in \Gamma_1$, then $|M \cap H| \geq p^4$ so $M \cap H$ contains an abelian subgroup of order p^3 which is an element of the set $\mathcal{C}$ hence the pair E_1, E_2 supports good lines.

Now the result follows from Proposition 103.3 and Lemma 103.2. □

Exercise 3. Suppose that a p-group G has order $> p^3$, $p > 2$. Then the number of abelian subgroups of order p^3 in G is congruent to 1 (mod p).

Using the above approach, the following results are established in [KonJ].

Theorem 103.5. *Let G be a p-group, $p > 2$, and let $\mathcal{C}$ be any one of the following classes of abelian subgroups of G:*

(i) *elementary abelian subgroups of order p^k for some fixed $k \leq 5$.*

(ii) *abelian subgroups of order p^k for some fixed $k \leq 5$.*

(iii) *abelian subgroups of fixed index p or p^2.*

Suppose that the set $\mathcal{C}$ is nonempty.

Then $|\mathcal{C}| \equiv 1$ (mod p) except in the index p^2 case (case (iii)*) where the number can also be exactly* 2.

Corollary 103.6 ([Alp2]). *If G is a p-group, $p > 2$, having an abelian subgroup of index p^3, then there is a normal abelian subgroup of the same index in G.*

Proof. Indeed, let A be an abelian subgroup of index p^3 in G, and let $A < M \in \Gamma_1$; then $|M : A| = p^2$. Then, by Theorem 103.5, the number of subgroups of index p^2 in M is not divisible by p since $p > 2$, and so one of these subgroups is normal in G. □

Corollary 103.7. *Suppose that a p-group G possesses an elementary abelian subgroup E_k of order p^k, $p > 2$, $k < 6$. Then the normal closure E_k^G of E_k in G contains a G-invariant elementary abelian subgroup of order p^k.*

Indeed, the number of elementary abelian subgroups of order p^k in E_k^G is not divisible by p so one of them is G-invariant.

Exercise 4. Suppose that a 2-group G contains an abelian subgroup E of type $(2, 2)$. Then one of the following holds:

(a) E^G is dihedral or semidihedral.

(b) E^G contains a G-invariant abelian subgroup of type $(2, 2)$.

(*Hint.* Use Theorem 1.17(b).)

§104

Degrees of irreducible characters of p-groups associated with finite algebras

All results of this section are due to Isaacs [Isa11]

In what follows q is a power of a prime p, $\mathrm{F} = \mathrm{GF}(q)$ (the field of cardinality q, where q is a power of a prime), R a finite dimensional F-algebra (as always, with the identity element). Let $J = \mathrm{J}(R)$ be the Jacobson radical of R (= the maximal nilpotent two-sided ideal of R; see [Lang, p. 658]); then $1 + J = \{1 + x \mid x \in J\}$ is a p-subgroup of R^*, the group of units in R (Theorem 34.6). We refer to the group $1 + J$ arising in this way from an F-algebra R as an F-*algebra group* G. Let $x \in G$; then $x = 1 + a$ for some $a \in J$. Observe that $|G| = |J|$ so G is a p-group.

The upper unitriangular group $\mathrm{UT}(n, q)$ is a Sylow p-subgroup of $\mathrm{GL}(n, q)$ and it has the form $1 + J$, where J is the space of strictly $n \times n$ upper-triangular matrices over F; then J is the radical of the F-algebra $\mathrm{F} \cdot 1 + J$. Thompson conjectured that the degrees of complex irreducible characters of the group $\mathrm{UT}(n, q)$ are degrees of q. This conjecture is a corollary of the following general Isaacs' theorem which is the main result of this section:

Theorem 104.1 ([Isa11, Theorem A]). *Let G be an* F*-algebra group. Then the degrees of all irreducible complex characters of G are powers of q.*

The theorem is a consequence of the following six lemmas.

Lemma 104.2. *Let N be a normal subgroup of a group G and suppose that G/N is abelian. Let $\chi \in \mathrm{Irr}(G)$ and suppose that $\chi_N = \phi \in \mathrm{Irr}(N)$. Then every irreducible constituent of ϕ^G has the form $\lambda\chi$ for some $\lambda \in \mathrm{Lin}(G/N)$.*[1]

Proof. Note that $(1_N)^G = \rho_{G/N}$, the regular character of G/N, and so the irreducible constituents of $(1_N)^G\chi$ are exactly the characters $\lambda\chi$ as in the statement of the lemma. Since (see [BZ, Theorem 5.1.2])

$$\mathrm{Irr}(\phi^G) \subseteq \mathrm{Irr}((\chi_N)^G) \quad \text{and} \quad (\chi_N)^G = (1_N\chi_N)^G = (1_N)^G\chi,$$

the result follows. □

[1] In particular, all irreducible constituents of ϕ^G are extensions of ϕ to G. The lemma is a particular case of a known result of Gallagher.

Lemma 104.3. *Let G, N and G/N be such as in Lemma* 104.2. *Let $\phi \in \mathrm{Irr}(N)$ be G-invariant and suppose that $\chi \in \mathrm{Irr}(\phi^G)$. Then there exists a subgroup M of G with $N \leq M \leq G$ and $\theta \in \mathrm{Irr}(M)$ such that $\theta_N = \phi$ and $\chi_M = e\theta$, where $e^2 = |G : M|$. Furthermore, χ vanishes on the set $G - M$.*

Proof. Take M to be the unique smallest subgroup of G containing N such that χ vanishes on $G - M$ and let $\theta \in \mathrm{Irr}(\chi_M)$ be arbitrary. To see that $\chi_M = e\theta$ for some integer $e > 0$, let $\psi \in \mathrm{Irr}(\chi_M)$ be arbitrary. Then $\psi, \theta \in \mathrm{Irr}(\phi^M)$ and so, by Lemma 104.2, $\psi = \lambda\theta$ for some $\lambda \in \mathrm{Lin}(M/N)$ since M/N is abelian. Let $K = \ker(\lambda)$; then $N \leq K \leq M$.

Since G/N is abelian, λ extends to a character μ of G/N and $\mu\chi \in \mathrm{Irr}((\lambda\theta)^G) = \mathrm{Irr}(\psi^G)$ (consider $(\mu\chi)_M$). Now, ψ is an irreducible constituent of $\chi_M = (\mu\chi)_M$, and Lemma 104.2 then tells us that $\mu\chi = \nu\chi$ for some $\nu \in \mathrm{Lin}(G/M)$. For the elements $x \in M - K$ we see that $\mu(x) = \lambda(x) \neq 1 = \nu(x)$ and thus $\chi(x) = 0$. By the definition of M, then $K = M$ and hence $\lambda = 1_M$. We conclude that $\psi = \theta$, i.e., $\chi_M = e\theta$, as claimed.

Now

$$e^2 = \langle e\theta, e\theta \rangle = \langle \chi_M, \chi_M \rangle = |G : M|,$$

where the third equality holds since χ vanishes on $G - M$. It remains to show that θ_N is irreducible. If this is false, it follows from the fact that M/N is abelian that θ is induced from a character of some subgroup T with $N \leq T < M$ [BZ, Theorem 7.2.2]. Next, T is normal in M, and thus θ vanishes on $M - T$. It follows that χ vanishes on $G - T$, a contradiction since $T < M$. □

For an arbitrary positive integer q we shall say that G is a *q-power-degree group* if all of its irreducible characters have degrees that are powers of q.

Lemma 104.4. *Fix a positive integer q and let G be a finite group. Let $M \lhd G$ and suppose that $\mathcal{H}$ is a collection of subgroups of G. Assume the following:*

(1) *M is the intersection of any two distinct members of the set $\mathcal{H}$.*

(2) *$G = \bigcup_{H \in \mathcal{H}} H$ (i.e., $G/M = \bigcup_{H \in \mathcal{H}} H/M$ is a nontrivial partition).*

(3) *$|G : H| = q$ for each $H \in \mathcal{H}$.*

(4) *G/M is abelian of order q^2.*

(5) *M and all members of the set $\mathcal{H}$ are q-power-degree groups.*

Then G is a q-power-degree group.

Proof. By (1)–(4), $|\mathcal{H}| = \frac{q^2-1}{q-1} = q + 1$ and if H and K are any distinct members of the set $\mathcal{H}$, we have $HK = G$ by the product formula.

To show that G is a q-power-degree group, let $\chi \in \mathrm{Irr}(G)$ be arbitrary. We choose $\phi \in \mathrm{Irr}(\chi_M)$ and let $T = \mathrm{I}_G(\phi)$, the inertia subgroup of ϕ in G. Let $H \in \mathcal{H}$ and $\alpha \in \mathrm{Irr}(\phi^H)$. Then

$$\phi(1) \leq \alpha(1) \leq \phi^H(1) = |H : M|\phi(1) = q\phi(1).$$

Since M and H are q-power-degree groups, however, and so $\phi(1) \mid \alpha(1)$, it follows that

$$\alpha(1) \in \{\phi(1), q\phi(1)\}.$$

In the first case, $\alpha_M = \phi$ and thus $H \leq T$. Otherwise, we get $\phi^H = \alpha$ and this forces $H \cap T = M$.

If $M < T$, then since T is partitioned by subgroups $T \cap H$ ($H \in \mathcal{H}$), we must have $T \cap H > M$ for some $H \in \mathcal{H}$. Therefore, by the result of the previous paragraph, $H \leq T$. If, in fact, $H < T$, then $T \cap K > M$ for some other member $K \in \mathcal{H}$ different from H, and in this case $T \geq HK = G$. We see, therefore, that the only possibilities are $T = M$, $T = G$ or $T \in \mathcal{H}$.

Suppose that $T < G$. By the Clifford Correspondence Theorem 7.2.2, we know that $\chi = \alpha^G$ for some $\alpha \in \mathrm{Irr}(T)$. Since either $T = M$ or $T \in \mathcal{H}$, it follows that T is a q-power-degree group, and so $\alpha(1)$ is a q-power. As

$$\chi(1) = |G : T|\alpha(1) \quad \text{and} \quad |G : T| \in \{q, q^2\},$$

the result follows in this case.

We are left with the situation where $T = G$ so ϕ is G-invariant. In this case, Lemma 104.3 yields the existence of a subgroup Q with $M \leq Q \leq G$ and a character $\theta \in \mathrm{Irr}(Q)$ such that $\chi_Q = e\theta$ and $\theta_M = \phi$. Since $\theta(1) = \phi(1)$ is a q-power and $\chi(1) = e\theta(1)$, it suffices to show that e is either 1 or q. To this end, we shall use the additional information (from Lemma 104.3) that $e^2 = |G : Q|$ and that χ vanishes on the set $G - Q$.

Let $H \in \mathcal{H}$ and consider $\alpha \in \mathrm{Irr}(\chi_H)$. Since ϕ is H-invariant and both ϕ and α have q-power degrees, we have seen that $\alpha(1) < |H : M|\phi(1) = q\phi(1)$ so we get $\alpha(1) = \phi(1)$. We know that $\chi(1) = e\phi(1)$ and it follows that χ_H is a sum of exactly e irreducible constituents and so $\langle \chi_H, \chi_H \rangle \geq e$.

Write $S = H \cap Q$ and note that χ_H vanishes on $H - S$ since it vanishes on $H - Q$. Also, θ_S is irreducible since $\theta_M = \phi \in \mathrm{Irr}(M)$ and $M \leq S$. We thus have

$$e|H : S| \leq \langle \chi_H, \chi_H \rangle |H : S| = \langle \chi_S, \chi_S \rangle = \langle e\theta_S, e\theta_S \rangle = e^2.$$

It follows that $e \geq |H : S|$ and so $|S/M| = q/|H : S| \geq q/e$.

Now Q/M is covered by subgroups $(Q \cap H)/M$ as H runs over $\mathcal{H}$, and we have just seen that each of these subgroups has order at least $\frac{q}{e}$. Since the pairwise intersections of these subgroups are trivial and $|G/Q| = e^2$, we have

$$|Q/M| = \frac{|Q|q^2}{|G|} = \frac{q^2}{|G : Q|} = \frac{q^2}{e^2}$$

and so

$$\begin{aligned} \frac{q^2}{e^2} - 1 = |Q/M| - 1 &= \sum_{H \in \mathcal{H}} (|(Q \cap H)/M| - 1) \\ &\geq |\mathcal{H}| \left(\frac{q}{e} - 1\right) = (q + 1)\left(\frac{q}{e} - 1\right). \end{aligned}$$

If $e < q$, we can divide by $\frac{q}{e} - 1$ to get $\frac{q}{e} + 1 \geq q + 1$ and this yields $e = 1$. We have now shown that either $e = 1$ or $e = q$, and the proof is complete. □

Note that G/M in Lemma 104.4 has a prime exponent since this quotient group is equally partitioned (see §68).

The following lemma resembles the known Nakayama's lemma.

Lemma 104.5. *Let $J = \mathrm{J}(R)$ and suppose that $U \subseteq J$ is a multiplicatively closed subspace. If $J = U + J^2$, then $U = J$.*

Proof. We show by induction on m that $J = U + J^m$ for any positive integer m. Since J is nilpotent, the result will follow. We can assume that $m > 2$ and $J = U + J^{m-1}$. Then, since $U \subseteq J$ is a multiplicatively closed subspace, we get

$$J^2 = J(U + J^{m-1}) \leq JU + J^m,$$
$$JU = (U + J^{m-1})U \leq U + J^m$$

and so $J^2 \subseteq U + J^m$. It follows that

$$J = U + J^2 \subseteq U + J^m \subseteq U + J^{m-1} = J$$

and we conclude that $J = U + J^m$. □

Lemma 104.6. *Let $J = \mathrm{J}(R)$ and suppose that $U \subseteq J$ is an ideal of R. Set $G = 1 + J$ and $N = 1 + U$. Then N is a normal algebra subgroup of G and G/N is naturally isomorphic to the algebra group corresponding to R/U.*

Proof. Write $\bar{R}$ to denote the F-algebra R/U and, as usual, let $\bar{r} \in \bar{R}$ denote the image of $r \in R$. Observe that $\bar{G} = 1 + \bar{J}$ and so $\bar{G}$ is an F-algebra group and the image of G under the group homomorphism $g \mapsto \bar{g}$. The result now follows from the observation that $N = 1 + U$ is the kernel of this homomorphism. □

Before stating the next lemma, we introduce a bit more notation. If $G = 1 + J$ is an F-algebra group, it is clear that the collection of the F-algebra subgroups of G is closed under intersection. It follows that for each element $x \in G$ there is a unique smallest F-algebra subgroup containing x, and we write $A(x)$ to denote this subgroup. In fact, it is easy to construct $A(x)$ explicitly. Write $x = 1 + u$ and observe that the smallest multiplicatively closed F-subspace of J containing u is $u\mathrm{F}[u]$. It follows that $A(x) = 1 + u\mathrm{F}[u]$. The key observation here is that $A(x)$ is abelian for all $x \in G$. This follows since the multiplication in $u\mathrm{F}[u]$ is clearly commutative.

Lemma 104.7. *Let G be an* F*-algebra group for R that is not of the form $A(x)$ for any element $x \in G$. (In particular, this holds if G is nonabelian.) Then there exists an* F*-algebra subgroup $M \lhd G$ and a family $\mathcal{H}$ of* F*-algebra subgroups of G satisfying properties* (1)–(4) *of Lemma* 104.4.

Proof. We have $G = 1+J$, where $J = \mathrm{J}(R)$ for some finite dimensional F-algebra R, and we can assume that $R = \mathrm{F} \cdot 1 + J$. If J^2 has codimension 1 in J, we can write $J = J^2 + \mathrm{F}u$ for some element $u \in J$. It follows that $J = J^2 + u\mathrm{F}[u]$ and hence, by Lemma 104.6, we have $J = u\mathrm{F}[u]$ and $A(u) = A(1+u)$, a contradiction. We conclude that the codimension of J^2 in J is at least 2.

Now let U be an F-subspace of J having codimension 2 and containing J^2. Note that U and all F-subspaces of J containing U are ideals of R and that the multiplication in $\mathrm{J}(R/U)$ is trivial. Let $M = 1 + U$ and let $\mathcal{H}$ be the collection of the subgroups $1 + V$, where V runs over all hyperplanes of J that contain U. By Lemma 104.6, M is normal in G and G/M is isomorphic to $1 + \mathrm{J}(R/U)$, which is abelian. All of the assertions are now clear. □

We mention that Lemma 104.7 essentially continues to hold even if the field F is infinite. Obviously, we need to delete the assertion about the indices of the members $H \in \mathcal{H}$ and M, but everything else goes through without change.

Proof of Theorem 104.1. We are given an F-algebra group G, where $|\mathrm{F}| = q$ (q being a power of a prime), and we show by induction on $|G|$ that G is a q-power-degree group. We can certainly assume that G is nonabelian and thus, by Lemma 104.7, we get a normal algebra subgroup M and a collection of algebra subgroups $\mathcal{H}$ satisfying certain properties. In particular, all of these subgroups are proper in G and thus each is a q-power-degree group by the inductive hypothesis. It follows from Lemma 104.4 that G is a q-power-degree group, as required. □

It follows from Theorem 104.1 that $\mathrm{UT}(n, q)$ is a q-power-degree group.

The important paper [Isa11] contains a number of related results.

§105

On some special p-groups

This section was inspired by a letter of Isaacs in which he disproved one problem posed by the first author on character degrees (see below). Most main results of this section are also due to Isaacs.

1^o. Here we repeat some considerations from §46. Let $s > 2$ be a positive integer, $\mathrm{F} = \mathrm{GF}(p^s)$, F_0 be the prime subfield of F and

$$\mathcal{S} = \mathrm{Gal}(\mathrm{F}/\mathrm{F}_0) = \langle\theta\rangle,$$

the set of all automorphisms of F. It is known that $o(\theta) = s$ and if $\theta(x) = x$ for some $x \in \mathrm{F}$, then $x \in \mathrm{F}_0$.

We will construct a special p-group $P = \mathrm{A}_p(s, \theta)$ (see §46) and study its structure. For $x, y \in \mathrm{F}$, write (x, y) to denote the matrix (a_{ij}) with

$$a_{ii} = 1,\ i = 1, 2, 3,\ \ a_{12} = x,\ \ a_{13} = y,\ \ a_{23} = \theta(x),\ \ a_{21} = a_{31} = a_{32} = 0.$$

The set of matrices (x, y) $(x, y \in \mathrm{F})$ is a group (denote it by $P = \mathrm{A}_p(s, \theta)$) with respect to matrix multiplication; obviously, $|P| = |\mathrm{F}|^2 = \mathrm{p}^{2s}$. The identity element of P is $(0, 0)$. It is easy to check that

(i) We have

$$(1)\ \ (x, y)(x_1, y_1) = (x + x_1, y + y_1 + x\theta(x_1)), \quad (x, y)^{-1} = (-x, -y + x\theta(x))$$

and the commutator

$$(2) \qquad [(x, y), (x_1, y_1)] = (0, x\theta(x_1) - x_1\theta(x)).$$

If $(x_1, y_1)(x, y) = (x, y)(x_1, y_1)$, then by (2) we get $x\theta(x_1) = x_1\theta(x)$ or, if $x_1 \neq 0$, $x_1^{-1}x = \theta(x_1^{-1}x)$. In that case, $x = x_1x_0$, where $x_0 \in \mathrm{F}_0$. Thus

(ii) If $x \neq 0$, then

$$(3)\ \ \mathrm{C}_P((x, y)) = \{(xx_0, y'),\ x_0 \in \mathrm{F}_0,\ y' \in \mathrm{F}\}, \quad |\mathrm{C}_P((x, y))| = |\mathrm{F}_0||\mathrm{F}| = p^{s+1}.$$

Obviously, $\mathrm{Z}(P) = \{(0, y), y \in \mathrm{F}\}$, and so $|\mathrm{Z}(P)| = |\mathrm{F}| = p^s$ and $\mathrm{Z}(P) \cong \mathrm{F}^+$, the additive group of the field F. In particular, $\mathrm{Z}(P) \cong \mathrm{E}_{p^s}$. It follows that G is a group with small abelian subgroups (see §20).

By induction on n, we get

$$(x, y)^n = \Big(nx, ny + \frac{1}{2}n(n-1)x\theta(x)\Big). \tag{4}$$

Setting in the above formula $n = p$, we obtain

$$(x, y)^p = (0, p(p-1)/2 \cdot x\theta(x)). \tag{5}$$

If $p > 2$, then $(x, y)^p = (0, 0)$ is the identity element of P. In case $p = 2$, we get $(x, y)^2 = (0, x\theta(x))$. If $p = 2$ and (x, y) is an involution, then we obtain $x = 0$ so $(x, y) \in \mathrm{Z}(P)$. Thus

(iii) $\exp(P) = p$ if $p > 2$ and $\exp(P) = 4$ if $p = 2$; in the last case, we have $\mathrm{Z}(P) = \Omega_1(P)$.

It follows from (3) and (iii) that if $(x, y) \in P - \mathrm{Z}(P)$, then

$$\mathrm{C}_P((x, y)) = \langle (x, y), \mathrm{Z}(P) \rangle$$

is isomorphic to $\mathrm{C}_{p^2} \times \mathrm{E}_{p^{s-1}}$ if $p = 2$ and is isomorphic to $\mathrm{E}_{p^{s+1}}$ if $p > 2$. Therefore, if $p = 2$ and $o((x, y)) = 4$, then $(x, y)^2$ is contained in exactly $\frac{2^{s+1}-2^s}{2(2-1)} = 2^{s-1}$ cyclic subgroups of order 4. It follows from (iii) that if $p = 2$, then P has exactly

$$\frac{2^{2s} - 2^s}{2(2-1)} = 2^{s-1}(2^s - 1)$$

cyclic subgroups of order 2^2 and $2^s - 1$ subgroups of order 2. Therefore

(iv) If $p = 2$, then $\mathfrak{V}_1(P) = \mathrm{Z}(P)$. In particular, $\Phi(P) = \mathfrak{V}_1(P)P' = \mathrm{Z}(P)$ (by (i), $P' \leq \mathrm{Z}(P)$).

It follows from (ii) that $|P'| \geq p^{s-1}$ (since $|P'|$ is at least the size of a conjugacy class). We will prove that $|P'| = p^s$.

Let $x_1, \ldots, x_s$ be a normal basis of the extension F/F_0 consisting of primitive elements of F.[1] Then, by (ii), the commutators

$$c_i = [(x_i, 0), (1, 0)] = (0, x_i - \theta(x_i)), \quad i = 1, \ldots, s.$$

We claim that $c_1, \ldots, c_s$ are linearly independent. Indeed, assume $c_1^{a_1} \ldots c_s^{a_s} = (0, 0)$ for some $a_1, \ldots, a_s \in \{0, \ldots, p-1\}$. Set $u_i = x_i - \theta(x_i)$, $i = 1, \ldots, s$. Then $a_2u_2 + \cdots + a_su_s = 0$ or, what is the same,

$$\theta(a_1x_1 + \cdots + a_sx_s) = a_1x_1 + \cdots + a_su_s.$$

[1] The elements $x_1, \ldots, x_s$ constitute a normal basis of the extension F/F_0 if $\sigma(x_i) \in \{x_1, \ldots, x_s\}$ for all i and $\sigma \in \mathrm{Gal}(\mathrm{F}/\mathrm{F}_0)$. A normal basis consisting of primitive elements does always exists; see [Ward, Kapitel 8].

This implies $a_1x_1 + \cdots + a_sx_s \in \mathrm{F}_0$ and so $a_1 = \cdots = a_s = 0$, proving our claim. Therefore $|\langle c_1, \ldots, c_s\rangle| = p^s$ and so $P' = \mathrm{Z}(P)$. Thus

(v) P is special, $P' = \mathrm{Z}(P) = \Phi(P)$ is elementary abelian of order p^s.

By (3) and (v), we obtain

(vi) The class number of P is

$$\mathrm{k}(P) = |\mathrm{Z}(P)| + \frac{|P| - |\mathrm{Z}(P)|}{p^{s-1}} = p^s + p^{s+1} - p.$$

Next,

$$|\mathrm{Lin}(P)| = |P : P'| = p^s \quad \text{and} \quad |\mathrm{Irr}_1(P)| = \mathrm{k}(G) - |\mathrm{Lin}(P)| = p^{s+1} - p,$$

where $\mathrm{Irr}_1(P)$ is the set of nonlinear characters of P.

Let s be odd. If $\chi \in \mathrm{Irr}(P)$, then $\chi(1)^2 \le |P : \mathrm{Z}(P)| = p^s$ and so $\chi(1)^2 \le p^{s-1}$. In this case,

$$p^{2s} - p^s = |P| - |P : P'| = \sum_{\chi \in \mathrm{Irr}_1(P)} \chi(1)^2 \le p^{s-1}(p^{s+1} - p) = p^{2s} - p^s$$

and so

(vii) If s is odd, then the degree of any nonlinear irreducible character of P is equal to $p^{\frac{1}{2}(s-1)}$, i.e., $\mathrm{cd}(P) = \{1, p^{\frac{1}{2}(s-1)}\}$.

It is easy to check that if s is even, then $|\mathrm{cd}(P)| > 2$. According to §46, in this case, $|\mathrm{cd}(G)| = 3$.

An automorphism ϕ of a group G is said to be *central* or *normal*, if it centralizes $\mathrm{Inn}(G)$, the group of inner automorphisms of G. In this case, for any $x, g \in G$ one has

$$\phi(x)^{-1}\phi(g)\phi(x) = \phi(x^{-1}gx) = x^{-1}\phi(g)x$$

and so

$$\phi(g)(\phi(x)x^{-1}) = (\phi(x)x^{-1})\phi(g)$$

hence, since $\mathrm{im}(\phi) = G$, we get $\phi(x) = xz_x$, where $z_x \in \mathrm{Z}(G)$ for all $x \in G$, and we conclude that ϕ induces the identity automorphism on $G/\mathrm{Z}(G)$. Conversely, if $\phi \in \mathrm{Aut}(G)$ induces the identity automorphism of $G/\mathrm{Z}(G)$, it is central. The set $\mathrm{Aut}_c(G)$ of central automorphisms of a group G is a normal subgroup of $\mathrm{Aut}(G)$.[2]

(viii) (L. Kazarin) Let $p = 2$ and let $s > 1$ be odd, $P = \mathrm{A}_2(s, \theta)$, where θ is a generator of $\mathrm{Gal}(\mathrm{F}/\mathrm{F}_0)$, $\phi \in \mathrm{Aut}_c(P)$. Then $(a, b)^\phi = (a, b + \lambda(a))$ for all $(a, b) \in P$, where $\lambda = \lambda_\phi$ is a linear operator of the s-dimensional vector space $\mathrm{GF}(2^s)/\mathrm{GF}(2)$.

[2]Indeed, if $\alpha \in \mathrm{Aut}(G)$, $\phi \in \mathrm{Aut}_c(G)$ and $g \in G$, then

$$(\alpha^{-1}\phi\alpha)(g) = \alpha^{-1}(\phi(\alpha(g)) = \alpha^{-1}(\alpha(g)z) = g\alpha(z)$$

for some $z \in \mathrm{Z}(G)$, and we conclude that $\alpha^{-1}\phi\alpha \in \mathrm{Aut}_c(G)$.

We claim that $|\mathrm{Aut}_c(P)| = 2^{s^2}$. Indeed, $(a,b) = (a,0)(0,b)$. Let us show that

$$\{a\theta(a) \mid a \in \mathrm{GF}(2^s)\} = \mathrm{GF}(2^s).$$

In fact, if $a\theta(a) = a_1\theta(a_1)$ $(a, a_1 \in \mathrm{GF}(2^s))$, then $\theta(a_1a^{-1}) = (a_1a^{-1})^{-1}$ so that $a = a_1$ in view of $o(\theta) = s$ is odd. It follows that for each $b \in \mathrm{GF}(2^s)$ there exists a unique $a \in \mathrm{GF}(2^s)$ such that $b = a\theta(a)$, and so $(0,b) = (a,0)^2$. Therefore ϕ is defined uniquely by its action on elements of the form $(a,0)$. Let $(a,0)^\phi = (a,\lambda(a))$, where $\lambda : \mathrm{GF}(2^s) \to \mathrm{GF}(2^s)$. Since $(a,0)^2 = (0,a\theta(a))$, then for $b = a\theta(a)$ we have

$$(0,b)^\phi = ((a,0)^2)^\phi = ((a,0)^\phi)^2 = (a,\lambda(a))^2 = (0,a\theta(a)) = (0,b),$$

i.e., ϕ fixes all elements of $\mathrm{Z}(P)$. In this case,

$$(a,b)^\phi = ((a,0)(0,b))^\phi = (a,\lambda(a))(0,b) = (a,b+\lambda(a)).$$

If $(a,b)^\phi = (0,0)$ and $\lambda = \lambda_\phi$ is linear, then $a = 0$ and $b = \lambda(a) = \lambda(0) = 0$, and so λ is an injection so a surjection. We claim that λ is linear. We have

$$(a,0)^\phi(c,0)^\phi = (a,\lambda(a)(c,\lambda(c)) = (a+c,\lambda(a)+\lambda(c)+a\theta(c)).$$

On the other hand, $(a,0)(c,0) = (a+c,a\theta(c))$ and

$$((a,0)(c,0))^\phi = (a+c,\lambda(a+c)+a\theta(c)).$$

Since ϕ is an automorphism, we get $\lambda(a+c) = \lambda(a)+\lambda(c)$. It is easy to check that the mapping $\phi : (a,b) \mapsto (a,b+\lambda(a))$ is an automorphism of P for every linear map

$$\lambda : \mathrm{GF}(2^s)/\mathrm{GF}(2) \to \mathrm{GF}(2^s)/\mathrm{GF}(2).$$

Thus,

$$(a,b)^\phi = (a,b+\lambda(a)) = (a,b)(0,\lambda(a)),$$

and $\phi \in \mathrm{Aut}_c(P)$ since $(0,\lambda(a)) \in \mathrm{Z}(P)$. It is easy to see that for every λ there is a unique central automorphism of P corresponding to λ. Since the number of λ's is equal to the number of $s \times s$ matrices over GF(2) (every such matrix contains s^2 entries equal 0 or 1), the claim (viii) follows.

2^o. Let P, F, θ and p^s be as in the previous subsection. Set

$$b = \frac{p^s-1}{p-1} = 1 + p + \cdots + p^{s-1}.$$

The multiplicative cyclic group F* of order p^s-1 has a unique subgroup C of order b since $b \mid p^s-1$. We define an action of C on P as follows:

$$(x,y)^c = (xc, yc^{p+1}) \quad (c \in C).$$

Note that $\theta(c) = c^p$ for all $c \in \mathrm{F}$ (θ is a generator of Aut(F)). We have

$$\begin{aligned}(x, y)^c(u, v)^c &= (xc, yc^{1+p})(uc, vc^{1+p}) \\ &= ((x + u)c, (y + v + x\theta(u))c^{1+p}) = ((x, y)(u, v))^c,\end{aligned}$$

and we conclude that $(x, y) \mapsto (xc, yc^{p+1})$ is an action. If $(x, y)^c = (x, y)$, then $c = 1$, i.e., every element of C induces a fixed-point-free automorphism of P. Therefore $CP = (C, P)$ is a Frobenius group with kernel P and cyclic complement C of order b.

We will construct a p-solvable group G such that $\mathrm{b}(Q)$ does not divide $\chi(1)$ for all $\chi \in \mathrm{Irr}(G)$, where $Q \in \mathrm{Syl}_p(G)$ and $\mathrm{b}(Q) = \max\{\phi(1), \phi \in \mathrm{Irr}(Q)\}$. This example is taken from Isaacs' unpublished note.

We retain the above notation. In what follows we will assume that $s = p > 2$. Then $o(\theta) = p$. We define an action of $\mathcal{S} = \langle\theta\rangle$ on $P = \mathrm{A}_p(p, \theta)$ as follows:

$$(x, y)^\theta = (\theta(x), \theta(y)).$$

Set $G = (C\mathcal{S}) \cdot P$. If $(x, y)^\theta = (x, y)$, then $x, y \in \mathrm{F}_0$, and so

$$|\mathrm{C}_P(\theta)| = |\mathrm{F}_0|^2 = p^2, \quad |\mathrm{C}_{\mathrm{Z}(P)}(\theta)| = p.$$

Thus θ fixes exactly p classes of $\mathrm{Z}(P)$ and p^2 classes of P and p classes of $P/P' = P/\mathrm{Z}(P)$. By Brauer's permutation Lemma 10.3.1(c), θ fixes exactly p linear characters of both groups $\mathrm{Z}(P)$ and P. If $\lambda \neq 1_{\mathrm{Z}(P)}$ is one of them in $\mathrm{Lin}(\mathrm{Z}(P))$ and $H = \ker(\lambda)$, then θ fixes all linear characters of $\mathrm{Z}(P)$ with kernel H. It follows that θ fixes exactly one maximal subgroup of $\mathrm{Z}(P)$. We choose θ so that $\theta(c) = c^p$ for all $c \in \mathrm{F}$. If $c \in C$ and $\theta(c) = c$, then we have $c = 1$ since $(|C|, p) = 1$. Therefore $\mathcal{S} \cdot C = (\mathcal{S}, C)$ is a Frobenius group with kernel C and complement $\mathcal{S} = \langle\theta\rangle$. The group $(\mathcal{S}, C)$ has exactly $|C| = b$ subgroups of order $|\mathcal{S}| = s = p$ and all of them are conjugate in $\mathcal{S}C$ (Sylow). If T is a subgroup of order p in $(\mathcal{S}, C) = (T, C)$, then T fixes exactly one maximal subgroup H_T of $\mathrm{Z}(P)$. Since b is equal to the number of maximal subgroups of $\mathrm{Z}(P)$ and to the number of subgroups of order p in $(\mathcal{S}, C)$, there is a one-to-one correspondence $T \leftrightarrow H_T$, where T and H_T are as above.

By the result of the previous paragraph, $\mathcal{S}$ fixes exactly $p^2 - p = p(p - 1)$ nonlinear irreducible characters of P (these characters are irreducible constituents of α^P, where α runs over all $p - 1$ nonprincipal linear characters of $\mathrm{Z}(P)/H_{\mathcal{S}}$ and $H_{\mathcal{S}}$ is the unique maximal subgroup of $\mathrm{Z}(P)$ fixed by $\mathcal{S}$). It follows that $\alpha^{\mathcal{S}P}$ is the sum of p^2 irreducible characters of $\mathcal{S}P$ of degree $p^{(p-1)/2}$. In particular, the inertia subgroup $\mathrm{I}_G(\alpha) = \mathcal{S}P$, and so all irreducible constituents of α^G have degree $bp^{(p-1)/2}$. If T is a subgroup of order p in $\mathcal{S}C$, then it is conjugate to $\mathcal{S}$ in $\mathcal{S}C$. Therefore, if H_T is the unique maximal subgroup of $\mathrm{Z}(P)$ fixed by T and β is a nonprincipal linear character of $\mathrm{Z}(P)/H_T$, then $\mathrm{I}_G(\beta) = TP$. If χ is a nonlinear irreducible character of $G/\mathrm{Z}(P)$, then $\chi(1)$ divides $|G : P| = bp$. Therefore, the p-part of the degree of every irreducible character of G does not exceed $p^{(p-1)/2}$.

The Sylow p-subgroup $\mathcal{S}P$ of G has an irreducible character of degree $p^{(p+1)/2}$, however. This is because $\mathcal{S}$ definitely does not stabilize all nonlinear irreducible characters of P. (It stabilizes only those that have a particular fixed maximal subgroup of $\mathrm{Z}(P)$ as kernel.) This proves that $\mathrm{b}(\mathcal{S}P)$ does not divide $\chi(1)$ for all $\chi \in \mathrm{Irr}(G)$.

The same question is open for $p = 2$.

Isaacs [Isa4] proved that for every set $\mathcal{S}$ of powers of a prime p containing $p^0 = 1$ there exists a p-group P such that $\mathrm{cd}(P) = \mathcal{S}$ (see Theorem 105.2 below). Next, he showed that for every p-group P there exists a group G with cyclic Sylow p-subgroup C such that $\mathrm{cd}(G) = \mathrm{cd}(P)$. We will prove this result. More exactly, we will show that for every set $\mathcal{S}$ of powers of a prime p containing $1 = p^0$ and with maximum member p^a there exists a group G having a cyclic Sylow p-subgroup C of order p^a such that $\mathrm{cd}(G) = \mathcal{S}$. For each member $p^e \in \mathcal{S}$, let V_e be an elementary abelian q-group on which a cyclic group of order p^e acts faithfully and irreducibly. Let C act on V_e with kernel of order p^{a-e} (in that case, C acts on V_e irreducibly), and let W be the direct product of the groups V_e for all $p^e \in \mathcal{S}$ so that C acts on W. Let $G = C \cdot W$ be the semidirect product of W with C. We claim that $\mathrm{cd}(G) = \mathcal{S}$. Obviously, it is enough to prove that $p^a \in \mathrm{cd}(G)$ (by Ito's theorem (see Introduction, Theorem 17), the set $\mathrm{cd}(D)$ contains only powers of p not exceeding $|C| = p^a$). Let

$$W = V_{e_1} \times \cdots \times V_{e_s}, \quad \text{where } \mathcal{S} = \{1, p^{e_1}, \ldots, p^{e_s} = p^a\}.$$

Let $x_i \in V_{e_i}^{\#}$, $i = 1, \ldots, s$, $x = x_1 \ldots x_s$. Then the normal closure of $\langle x \rangle$ in G is equal to W, the socle of G. Therefore, by [BZ, Corollary 9.6] (Gaschütz' theorem), $\mathrm{Irr}(G)$ has a faithful character χ. We claim that $\chi(1) = p^{e_s} = p^a$. Note that $C \cdot V_a$ is a Frobenius group. As $V_a \not\leq \ker(\chi)$, it follows that χ_{V_a} has a nonlinear constituent, and so $\chi(1) \geq p^a$ in view of $\mathrm{cd}(C \cdot V_a) = \{1, p^a\}$. Since $\chi(1)$ divides p^a by Ito's theorem (see Introduction, Theorem 17), we get $\chi(1) = p^a$, as desired.

Of course, if $\mathrm{cd}(G) = \mathcal{S}$, where $\mathcal{S}$ is as in the previous paragraph, then G has an abelian normal p-complement.

Problem 1. Let P be a Sylow p-subgroup of a p-solvable group G. Study $\mathrm{cd}(P)$ in the case where p^2 does not divide $\chi(1)$ for all $\chi \in \mathrm{Irr}(G)$.

Problem 2. Let $P = \mathrm{A}_p(s, \theta)$, where θ is a generator of $\mathrm{Aut}(\mathrm{GF}(p^s))$, $s > 2$ is even. Find $\mathrm{cd}(P)$.

Exercise. Let G be a group of class two of maximal order generated by $n > 1$ elements of order p (for the matrix construction of this group, see [Macd3]). Prove that

(a) $\exp(G) = p$ if $p > 2$ and $\exp(G) = 4$ if $p = 2$, $|G| = p^{n(n+1)/2}$.

(b) G is special and $|\mathrm{Z}(G)| = p^{n(n-1)/2}$.

(c) If $x \in G - \mathrm{Z}(G)$, then $|G : \mathrm{C}_G(x)| = p^{n-1}$, i.e., G is a p-group with small abelian subgroups; see §20.

(d) $\mathrm{k}(G) = p^{n(n-1)/2} + p^{n(n+1)/2-(n-1)} - p^{n(n-1)/2-(n-1)}$.

(e) For any positive integer n such that $2r \leq n$, $\mathrm{Irr}(G)$ has a character χ of degree p^r.

(f) Find $\mathrm{T}(G) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)$.

(g) (Mann) If $p > 2$, then we have $\mathrm{Aut}(G)/\mathrm{Aut}_c(G) \cong \mathrm{Aut}(G/G') \cong \mathrm{GL}(n, p)$, $|\mathrm{Aut}_c(G)| = |G'|^n$ and $\mathrm{Aut}_c(G)$ is elementary abelian.

(h) (Mann) If $p = 2$, then $\mathrm{Aut}(G)/\mathrm{Aut}_c(G) \cong \mathrm{S}_n$.

(i) If $n > 5$, then G' has non-commutators. (In fact, this is true in the case $n > 3$. Moreover, if $n = 4$, then G has an epimorphic image H of order p^8 such that not all elements of H' are commutators [Macd3]. Numerous examples of groups, in which not all elements of G' are commutators, have been published; see, for example, [Fit], [Isa6] and [Macd3].)

3^o. Let X be a set of powers of p such that $1 \in X$. We will prove that there exists a p-group G such that $\mathrm{cd}(G) = X$. As we know (see the exercise, this is the case if $X = \{1, p, \ldots, p^e\}$. Isaacs [Isa4] has shown that such a G exists for any X; moreover, G may be taken to be of class ≤ 2.

Let U be an abelian group which acts on an abelian group A. Set $\widehat{A} = \mathrm{Lin}(A)$, the group of linear characters of A. As we know (see [BZ, §1.9]), there exists a natural isomorphism of $\widehat{A}$ onto A. If $\alpha \in \widehat{A}$, $u \in U$ and $a \in A$, then, setting

$$\alpha^u(a) = \alpha(uau^{-1}),$$

we can define an action of U on $\widehat{A}$.

The following lemma is of independent interest.

Lemma 105.1 ([Isa4]). *Let U be an abelian group which acts on an abelian group A and $\mathcal{S}$ be the set of the sizes of the orbits in this action. Write $G = U \cdot \widehat{A}$, where the semidirect product is constructed with respect to the action of U on $\widehat{A}$, induced by the given action of U on A. Then* $\mathrm{cd}(G) = \mathcal{S}$. *Furthermore, if $[A, U, U] = \{1\}$, then G has the nilpotence class ≤ 2.*

Proof. Let $\lambda \in \mathrm{Lin}(\widehat{A})$ and let T be the stabilizer of λ in U. Since the cyclic group $\widehat{A}/\ker(\lambda)$ is centralized by an abelian subgroup T, it follows that $\widehat{A}T/\ker(\lambda)$ is abelian and thus every $\psi \in \mathrm{Irr}(\lambda^{\widehat{A}T})$ is linear. Obviously, $\widehat{A}T = \mathrm{I}_G(\lambda)$, the inertia subgroup of λ in G, and thus every $\chi \in \mathrm{Irr}(\lambda^G)$ has degree $|G : \widehat{A}T| = |U : T|$. Therefore,

$$\mathrm{cd}(G) = \{|U : T| \mid T \text{ is a stabilizer in } U \text{ of some } \lambda \in \mathrm{Lin}(\widehat{A})\}.$$

However, there is a natural correspondence between $\mathrm{Lin}(\widehat{A})$ and A, and this defines a permutation isomorphism of the actions of U on A and $\mathrm{Lin}(\widehat{A})$, respectively, and we conclude that $\mathrm{cd}(G) = \mathcal{S}$, as required.

Now suppose that $[A, U, U] = \{1\}$. If $\alpha \in \widehat{A}$, we have for $u \in U$ and $a \in A$ that

$$[\alpha, u](a) = (\alpha^{-1}\alpha^u)(a) = \alpha(a^{-1})\alpha(uau^{-1}) = \alpha([a, u^{-1}]).$$

Therefore, if $v \in U$, we get by the above displayed formula,

$$[\alpha, u, v](a) = [\alpha, u]([a, v^{-1}]) = \alpha([a, v^{-1}, u^{-1}]) = \alpha(1) = 1$$

and so $[\widehat{A}, U, U] = \{1\}$. Since $\widehat{A}$ is abelian and $[\widehat{A}, U] \leq \widehat{A}$, this yields $\mathrm{C}_G([\widehat{A}, U]) \geq U\widehat{A} = G$, i.e., $[\widehat{A}, U] \leq \mathrm{Z}(G)$. As $G/[\widehat{A}, U] = U\widehat{A}/[\widehat{A}, U]$ is abelian, it follows that $\mathrm{cl}(G) \leq 2$, completing the proof. □

Now we are ready to prove the main result of this section.

Theorem 105.2 ([Isa4]). *Let p be a prime and let $0 = e_0 < e_1 < \cdots < e_m$ be integers. Then there exists a p-group that is generated by elements of order p and has nilpotence class ≤ 2 such that* $\mathrm{cd}(G) = \{p^{e_i} \mid 1 \leq i \leq m\}$.

Proof. Suppose that U is an elementary abelian p-group of rank e_m with generators $u_1, \ldots, u_{e_m}$. Let A be an elementary abelian p-group with basis

$$a_1, z_{1,1}, \ldots, z_{1,e_1}, \ldots, a_m, z_{m,1}, \ldots, z_{m,e_m}$$

(m blocks of sizes $e_1, \ldots, e_m$, respectively) and define an action of U on A as follows.

Put $(z_{i,\mu})^{u_\nu} = z_{i,\mu}$ for all i, μ, ν and $(a_i)^{u_\nu} = a_i$ if $\nu > e_i$ and $(a_i)^{u_\nu} = a_i z_{i,\nu}$ if $\nu \leq e_i$. Since the automorphisms of A defined this way all have order p and commute pairwise, this does define an action of U on A.

Let us compute the sizes of the orbits of this action. Write

$$Z = \langle z_{i,\mu} \mid \mu \leq e_i \rangle \leq A$$

and let $a \in A$. Obviously, $Z \leq \mathrm{Z}(G)$, where $G = U \cdot \widehat{A}$ is defined as in Lemma 105.1. Assume that $a \in A - Z$. Then there exists a unique subscript i such that we can write $a = bcz$, where

$$b \in \langle a_j \mid j < i \rangle, \quad 1 \neq c \in \langle a_i \rangle, \quad z \in Z.$$

Suppose that $u \in U$. If u involves the generator u_μ with $\mu \leq e_i$, the exponents of $z_{i,\mu}$ in a and in a^u will not be equal, and u does not centralize a. Thus we obtain that $\mathrm{C}_U(a) \leq \langle u_\nu \mid \nu > e_i \rangle$. Since the reverse inclusion is obvious, we finally obtain $\mathrm{C}_G(a) = \langle u_\nu \mid \nu > e_i \rangle$.

We now have $|U : \mathrm{C}_U(a)| = p^{e_i}$ and we see that the orbit sizes of the action of U on A are precisely the numbers p^{e_i} for $0 \leq i \leq m$. Since $[A, U] \leq Z \leq \mathrm{Z}(G)$, we have $[A, U, U] = \{1\}$ and the result follows by Lemma 105.1. □

§106

On maximal subgroups of two-generator 2-groups

To facilitate the proof of Theorem 106.3, we first prove Lemmas 106.1 and 106.2. The lemma below follows from Propositions 71.3, 71.4 and 71.5, but we prefer to give an independent proof.

Lemma 106.1. *If a nonmetacyclic $\mathcal{A}_2$-group G is two-generator, then $p > 2$.*[1]

Proof (Berkovich). Assume that this is false, i.e., there exists a nonmetacyclic two-generator 2-group G which is an $\mathcal{A}_2$-group. Since G is not metacyclic, it has a maximal subgroup, say A, such that $\mathrm{d}(A) > 2$ (Corollary 36.6); then $\mathrm{d}(A) = 3$ (Schreier; see Appendix 25). From Lemma 65.1 we deduce that A is not an $\mathcal{A}_1$-group so it is abelian. Let $\Gamma_1 = \{M, N, A\}$. If one of the subgroups M, N, say M, is abelian, then $A \cap M = \mathrm{Z}(G)$ so $\mathrm{Z}(G) = \Phi(G)$ since $G/\mathrm{Z}(G) \cong \mathrm{E}_4 \cong G/\Phi(G)$, and we conclude that G is an $\mathcal{A}_1$-group, contrary to the hypothesis. Thus M and N are $\mathcal{A}_1$-subgroups. We have $\mathrm{Z}(M) = \Phi(M) < \Phi(G) < A$ so $\mathrm{C}_G(\mathrm{Z}(M)) \geq AM = G$, and we conclude that $\mathrm{Z}(M) = \mathrm{Z}(G)$ since $\mathrm{Z}(G) < \Phi(G)$ (otherwise, G is an $\mathcal{A}_1$-group). Similarly, $\mathrm{Z}(N) = \mathrm{Z}(G)$. Since the two-generator group $G/\mathrm{Z}(G)$ of order 8 has two noncyclic subgroups $M/\mathrm{Z}(G)$ and $N/\mathrm{Z}(G)$ of order 4, it is generated by involutions. It follows that $G/\mathrm{Z}(G) \cong \mathrm{D}_8$.

Suppose that $R \lhd G$ satisfies $G/R \cong \mathrm{D}_8$. We claim that then $R = \mathrm{Z}(G)$. Indeed, it follows from $\mathrm{d}(G) = 2$ that $R < \Phi(G)$. Since G/R has exactly one cyclic subgroup of order 4, one may assume, without loss of generality, that $M/R \cong \mathrm{E}_4$ holds so $R = \Phi(M) = \mathrm{Z}(M)$. In that case, $\mathrm{C}_G(R) \geq AM = G$ so that $R = \mathrm{Z}(G)$ (compare indices). Thus there is in G only one normal subgroup, namely $\mathrm{Z}(G)$, such that the corresponding quotient group is isomorphic to D_8.

Set $\bar{G} = G/\mathfrak{V}_1(A)$. Then $\bar{G}$ is nonabelian of order 16 since $\bar{A} \cong \mathrm{E}_8$ and $\mathrm{d}(\bar{G}) = \mathrm{d}(G) = 2$. As $\exp(\bar{G}) = 4$, $\bar{G}$ is not of maximal class. Then, by Proposition 10.17, $\bar{G}$ has no nonabelian subgroup of order 8 (otherwise, $\mathrm{d}(G) > 2$) so it is an $\mathcal{A}_1$-group. It follows that $\mathrm{Z}(\bar{G}) \cong \mathrm{E}_4$. In this case, there exists $\bar{R} < \mathrm{Z}(\bar{G})$ of order 2 such that $\bar{R} \neq \bar{G}'$; then $\bar{G}/\bar{R} \cong \mathrm{D}_8$ since a *nonabelian* group $\bar{G}/\bar{R}$ has a subgroup $\bar{A}/\bar{R} \cong \mathrm{E}_4$. By the first paragraph, $R = \mathrm{Z}(G)$. Let $B/\mathrm{Z}(G) < G/\mathrm{Z}(G)$ be cyclic of order 4; then

[1] Thus a 2-group G which is a two-generator $\mathcal{A}_2$-group is metacyclic; this will be the case if and only if $|G'| = p^2$ by Corollary 65.3.

B is abelian. As $B \neq A$ (indeed, $A/\mathrm{Z}(G) \cong \mathrm{E}_4$), we get a contradiction since, by the above, there is in G only one abelian maximal subgroup. □

Lemma 106.2 ([BJ3, Lemma 2.1]). *Let G be a nonmetacyclic p-group and let $R < G'$ be G-invariant of order p. If G/R is minimal nonabelian and all nonabelian maximal subgroups of G are two-generator, then G is an $\mathcal{A}_2$-group and $p > 2$.*

Proof. By hypothesis, $|G'| > p$ so G is not an $\mathcal{A}_1$-group (Lemma 65.1). We also have $\mathrm{d}(G) = \mathrm{d}(G/R) = 2$ since $R < G' \leq \Phi(G)$.

Let $M \in \Gamma_1$ be nonabelian. Then $\mathrm{d}(M) = 2$ by hypothesis, and M/R, as a maximal subgroup of the $\mathcal{A}_1$-group G/R, is abelian which implies in view of $|R| = p$ that $M' = R$. Hence M is an $\mathcal{A}_1$-group (Lemma 65.2(a)) and so G is an $\mathcal{A}_2$-group. By Lemma 106.1, $p > 2$. □

Note that if $R < G'$ is G-invariant of order p and G/R is a metacyclic $\mathcal{A}_1$-group, then G is a metacyclic $\mathcal{A}_2$-group. Indeed, G is metacyclic by Theorem 36.1. Since $|G'| = p^2$, G is an $\mathcal{A}_2$-group by Corollary 65.3.

Now we are ready to prove our main result.

Theorem 106.3 ([BJ3, Theorem 2.2]). *If a 2-group G and all its nonabelian maximal subgroups are two-generator, then G is either metacyclic or minimal nonabelian.*

Proof. Assume that G is a counterexample of minimal order. Then G is nonabelian (otherwise, G is metacyclic since, by hypothesis, $\mathrm{d}(G) \leq 2$).

Assume that $|G'| = 2$. Then, since we have $\mathrm{d}(G/G') = 2$, G is an $\mathcal{A}_1$-group by Lemma 65.2(a), contrary to the assumption. It follows that $|G'| > 2$.

Let $R < G'$ be G-invariant of order 2; then $\bar{G} = G/R$ is nonabelian. Since $\bar{G}$ satisfies the hypothesis and $|\bar{G}| < |G|$, it is either metacyclic or minimal nonabelian by induction.

If $\bar{G}$ is metacyclic, then G is also metacyclic by Theorem 36.1, contrary to the assumption.

Thus $\bar{G} = G/R$ is a nonmetacyclic $\mathcal{A}_1$-group. By hypothesis, G and all its nonabelian maximal subgroups are two-generator. Then, by Lemma 106.2, G is an $\mathcal{A}_2$-group and $p > 2$, a final contradiction. □

Let a nonabelian 2-group be neither metacyclic nor minimal nonabelian. If all nonabelian maximal subgroups of G are two-generator, then $\mathrm{d}(G) = 3$ (Theorem 106.3).

If G is a 2-group with $\mathrm{d}(G) > 2$ and all maximal subgroups of G are two-generator, then the quotient group $G/\mathrm{K}_4(G)$, where $\mathrm{K}_n(G)$ is the n-th member of the lower central series of G, is described up to isomorphism in §71 (the order of such quotient group does not exceed 2^9). However, see §113 which shows that there exist such groups of arbitrary class.

Remark. Let G be a two-generator p-group, $p > 2$, possessing an abelian maximal subgroup, say A, and suppose that all nonabelian maximal subgroups of G are two-generator. Suppose that $|G'| > p$ (if $|G'| = p$, then G is minimal nonabelian by Lem-

ma 65.2(a)). Let $R < G'$ be a G-invariant subgroup of order p and let G/R be of maximal class. We claim that then G is also of maximal class. Indeed, since $R < \Phi(G)$, we get $p^2 = |(G/R) : (G'/R)| = |G : G'| = p|\mathrm{Z}(G)|$ by Lemma 1.1, i.e., $\mathrm{Z}(G)$ is of order p so coincides with R. It follows that G is of maximal class, as was to be shown. Conversely, if a p-group G of maximal class and order $> p^3$ has an abelian maximal subgroup, say A, then all nonabelian subgroups of G are of maximal class so two-generator. Indeed, if $H \in \Gamma_1$ is nonabelian, then H is of maximal class by Fitting's lemma. Next, if $F < G$ is nonabelian, then $F \leq H \in \Gamma_1$, and since $H \cap A$ is maximal abelian in H, we conclude that F is of maximal class by induction in H, completing the proof. If all nonabelian maximal subgroups of a p-group G are two-generator and $|G/\mathfrak{V}_1(G)| \geq p^4$, then G has an abelian maximal subgroup. Indeed, $G/\mathfrak{V}_1(G)$ has a maximal subgroup, say $A/\mathfrak{V}_1(G)$, which is not generated by two elements (Theorem 5.8(b)); then $\mathrm{d}(A) > 2$ so A is abelian by hypothesis.

§107

Ranks of maximal subgroups of nonmetacyclic two-generator 2-groups

Let G be a nonmetacyclic two-generator 2-group. By Theorem 44.5, there is in G a maximal subgroup C such that $\mathrm{d}(C) > 2$ (in fact, by Schreier's theorem on the number of generators of subgroups, $\mathrm{d}(C) = 3$; see Appendix 25). Let A, B, C be all maximal subgroups of G. It is important to know all possibilities for $\mathrm{d}(A)$ and $\mathrm{d}(B)$ and also on the structure of A and B. As Theorem 107.1 asserts, there are exactly two possibilities: $\mathrm{d}(A) = \mathrm{d}(B) = 2$ and $\mathrm{d}(A) = \mathrm{d}(B) = 3$.

Theorem 107.1 ([BJ3, Theorem 5.1]). *Suppose that G is a nonmetacyclic two-generator 2-group. Then the number of two-generator maximal subgroups of G is even.*

Proof. By hypothesis, G is nonabelian. If $A \in \Gamma_1$, then $\exp(G/\mho_1(A)) \leq 4$ so that $\mho_2(G) \leq \mho_1(A) = \Phi(A)$ and hence $\mathrm{d}(A/\mho_2(G)) = \mathrm{d}(A)$. Therefore, without loss of generality, one may assume that $\mho_2(G) = \{1\}$; then $\exp(G) = 4$. It follows that G/G' is abelian either of type $(4,2)$ or $(4,4)$. Since G is not metacyclic, at least one maximal subgroup of G is not two-generator by Corollary 36.6. Let $\Gamma_1 = \{A, B, C\}$ and $\mathrm{d}(C) = 3$ (see the paragraph preceding the theorem).

Assume that the statement of the theorem is false. Then one may assume $\mathrm{d}(A) = 2$ and $\mathrm{d}(B) = 3 (= \mathrm{d}(C))$. Let R be a G-invariant subgroup of index 2 in G'. Then G/R is minimal nonabelian and nonmetacyclic (Theorem 36.1). By what has just been said, $|G/R| \leq 2^5$. If $|G/R| = 2^5$, then all maximal subgroups of G/R are not generated by two elements (see Lemma 65.1), contrary to the assumption. Thus $|G/R| = 2^4$. In this case, G/G' is abelian of type $(4,2)$ and $|\Omega_1(G/R)| = 2^3$ (Lemma 65.1). All maximal subgroups of G/R which are different from $C/R = \Omega_1(G/R)$ are abelian of type $(4,2)$. Hence B/R is abelian of type $(4,2)$ and so it is two-generator. By assumption, we have on the one hand $\mathrm{d}(B) = 3$ implying that $R \neq \Phi(B)$ (note that $|R| = |\Phi(B)|$), and on the other hand that $\Phi(B)$ is a G-invariant subgroup of index 2^3 in B. Write $\bar{G} = G/\Phi(B)$; then $\bar{G}$ (of order 2^4) is not of maximal class since it contains a subgroup $\bar{B} \cong \mathrm{E}_8$. It follows that $|\bar{G} : \bar{G}'| = 8 = |G/G'|$ so $\Phi(B) < G'$ (this also follows from Taussky's theorem), and we conclude that $|G' : \Phi(B)| = 2$. Since G' has only one G-invariant subgroup of index 2 (Lemma 36.5), we conclude that $\Phi(B) = R$. This is a contradiction since, by the above, $R \neq \Phi(B)$. Thus $\mathrm{d}(B) = 2$ so that the number of two-generator maximal subgroups of G is even, as was to be

shown. (There exists an $\mathcal{A}_2$-group G of order 2^6 and $\mathrm{d}(G) = 3$ all of whose seven maximal subgroups are $\mathcal{A}_1$-groups so two-generator (see §71).) □

Thus, if the number of two-generator maximal subgroups of a 2-group G is odd, then either G is metacyclic or $\mathrm{d}(G) = 3$.

Exercise. Let G be a p-group such that $|G/G'| = p^2$. Then G has no maximal subgroup of rank $p + 1$. If $A \in \Gamma_1$ with $\mathrm{d}(A) = p$, then $G/\Phi(A) \cong \Sigma_{p^2}$, a Sylow p-subgroup of the symmetric group of degree p^2.

Solution. Let $A \in \Gamma_1$. Then $G/\Phi(A)$ is of maximal class (to prove, use Lemma 1.1 and induction) so that $\mathrm{d}(A) < p + 1$ (Theorem 9.5). Now let $A \in \Gamma_1$ with $\mathrm{d}(A) = p$. Then $G/\Phi(A) \cong \Sigma_{p^2}$ (Exercise 9.13).

Theorem 107.2 ([BJ3, Theorem 5.2]). *Suppose that G is a nonmetacyclic two-generator 2-group. Then one of the following holds:*

(a) *Every maximal subgroup of G is not generated by two elements if and only if G/G' has no cyclic subgroup of index 2.*

(b) *Exactly one maximal subgroup of G is not generated by two elements if and only if G/G' has a cyclic subgroup of index 2.*

Proof. (a) Suppose that all maximal subgroups of a given nonmetacyclic two-generator 2-group G are not two-generator (then their ranks are equal to 3 by Appendix 25). We claim that, in this case, G/G' has no cyclic subgroup of index 2. Assume that this is false. As in the proof of Theorem 107.1, one may assume that $\mho_2(G) = \{1\}$ hence $\exp(G) = 4$ and G is nonabelian. Let R be a G-invariant subgroup of index 2 in G'. Then G/R is a nonmetacyclic $\mathcal{A}_1$-group (Theorem 36.1 and Lemma 65.2(a)). As in the proof of Theorem 107.1, $2^3 < |G/R| \le 2^5$ and R is the unique G-invariant subgroup of index 2 in G'.

Assume that $|G/R| = 2^4$; then G/G' is abelian of type $(4, 2)$ and the maximal subgroups of G/R are abelian of types $(4, 2)$, $(4, 2)$ and $(2, 2, 2)$. Let $B/R < G/R$ be abelian of type $(4, 2)$. By hypothesis, we have $B/\Phi(B) \cong \mathrm{E}_8$. Since $G/\Phi(B)$ is not of maximal class (indeed, it contains a subgroup $\cong \mathrm{E}_8$, namely $B/\Phi(B)$), it follows that $|G/\Phi(B) : (G/\Phi(B))'| = 8$ (Taussky's theorem) and so $G' \cap \Phi(B) = R$ which yields $\Phi(B) > R$, and this is a contradiction (recall that $\mathrm{d}(B/R) = 2$). As in the proof of Theorem 107.1, we get $R = \Phi(B)$, and this is a contradiction.

Thus $|G/R| = 2^5$ so G/G' is abelian of type $(4, 4)$. It follows that, in the case under consideration, G/G' has no cyclic subgroup of index 2.

Now suppose that G/G' has no cyclic subgroup of index 2. Let R be (the unique) G-invariant subgroup of index 2 in G'. Write $\bar{G} = G/R$. Then $\bar{G}$ is a nonmetacyclic $\mathcal{A}_1$-group by Theorem 36.1 and Lemma 65.2(a) so $\Omega_1(\bar{G}) \cong \mathrm{E}_8$ (Lemma 65.1). Since G/G' has no cyclic subgroup of index 2, it is abelian of type $(2^m, 2^n)$, $m, n > 1$, therefore it follows that $\bar{G}/\Omega_1(\bar{G})$ is abelian of type (p^{m-1}, p^{n-1}) hence noncyclic. Therefore $\Omega_1(\bar{G}) \le \Phi(\bar{G})$ since $\mathrm{d}(\bar{G}) = \mathrm{d}(G) = 2$. Thus, if $\bar{A}/\Omega_1(\bar{G})$ is maximal

in $\bar{G}/\Omega_1(\bar{G})$, then $\mathrm{d}(A/R) = 3$ since A/R is abelian and contains $\Omega_1(\bar{G}) \cong \mathrm{E}_8$, and we conclude that $\mathrm{d}(A) = 3$. Since $A \in \Gamma_1$ is arbitrary, the proof of (a) is complete.

Statement (b) follows from (a) and Theorem 107.1. □

Suppose that a nonmetacyclic two-generator p-group G contains a metacyclic abelian maximal subgroup A. If G has a normal elementary abelian subgroup E of order p^3, then A has a cyclic subgroup of index p. Indeed, $G = AE$ and $G/(A \cap E) \cong (A/(A \cap E)) \times (E/(A \cap E))$. Since $\mathrm{d}(G) = 2$, we conclude that $A/(A \cap E)$ is cyclic, and our claim follows in view of $A \cap E = \Omega_1(A)$. We have $G' \leq A \cap E$.

In the following two theorems we shall consider the nonmetacyclic two-generator 2-groups G containing exactly one non-two-generator maximal subgroup.

Theorem 107.3 ([BJ3, Theorem 5.3]). *Suppose that G is a nonmetacyclic two-generator 2-group which possesses exactly one maximal subgroup K which is not two-generator. If $\Gamma_1 = \{M, N, K\}$ is the set of maximal subgroups of G, then $|G' : K'| = 2$, G/K' is nonmetacyclic minimal nonabelian, both M and N are either metacyclic or nonmetacyclic and G/G' has a cyclic subgroup of index 2.*

Proof. By Theorem 107.2, G/G' has a cyclic subgroup of index 2.

We know that $\mathrm{d}(M) = 2 = \mathrm{d}(N)$ and $\mathrm{d}(K) = 3$. If $K' = \{1\}$, then Theorem 106.3 implies that G is minimal nonabelian in which case both M and N are metacyclic since, in the case under consideration, $\Omega_1(M) \cong \Omega_1(N) \cong \mathrm{E}_4$ and M, N are abelian.

Therefore one may assume that G is not minimal nonabelian and hence $|G'| > 2$ (Lemma 65.2(a)); then $K' > \{1\}$. We have $K/\Phi(K) \cong \mathrm{E}_8$ so that $\mathrm{d}(G/\Phi(K)) = 2$ implies that $G/\Phi(K)$ is nonmetacyclic minimal nonabelian of order 2^4 (this follows from the previous paragraph; this also follows from Proposition 10.17). Hence we get $K' \leq G' \cap \Phi(K)$ and $|G' : (G' \cap \Phi(K))| = 2$. Assume that $K' < G' \cap \Phi(K)$. In this case, consider $G/K' = \bar{G}$, where $\bar{G}, \bar{M}, \bar{N}$ are two-generator groups and $\bar{K}$ is abelian with $\mathrm{d}(\bar{K}) = 3$. By Theorem 106.3, $\bar{G}$ must be minimal nonabelian. This is a contradiction since $\bar{G}' = (\bar{G})'$ is of order > 2. We have proved that $K' = G' \cap \Phi(K)$, and so, by the above, $|G' : K'| = 2$ and therefore $\bar{G} = G/K'$ is nonmetacyclic minimal nonabelian (recall that $\mathrm{d}(\bar{K}) = 3$).

Now assume that M is nonmetacyclic but N is metacyclic. Then $M' \neq \{1\}$ since $\mathrm{d}(M) = 2$, and let $R < M'$ be a G-invariant subgroup with $|M' : R| = 2$. In this case, we consider $\bar{G} = G/R$ so that $\bar{M}$ is nonmetacyclic minimal nonabelian (Theorem 36.1 and Lemma 65.2(a)). Note that $\bar{N}$ is metacyclic and we set $\bar{E} = \Omega_1(\bar{M}) \cong \mathrm{E}_8$ (Lemma 65.1). If $\bar{G}/\bar{E}$ is noncyclic, then $\bar{E} \leq \Phi(\bar{G})$ since $\mathrm{d}(\bar{G}) = 2$, and so $\bar{E} \cong \mathrm{E}_8$ is contained in metacyclic subgroup $\bar{N}$, a contradiction. Hence $\bar{G}/\bar{E}$ is cyclic of order ≥ 4 since $\bar{M} > \bar{E}$ in view of $\mathrm{d}(\bar{M}) = 2 < 3 = \mathrm{d}(\bar{E})$. Let $\bar{a} \in \bar{G} - \bar{M}$ be such that $\langle \bar{a} \rangle$ is cyclic of order ≥ 8, $\langle \bar{a} \rangle$ covers $\bar{G}/\bar{E}$ and $\langle \bar{z} \rangle = \langle \bar{a} \rangle \cap \bar{E} \cong \mathrm{C}_2$ so that, in particular, $\langle \bar{z} \rangle \in \mathrm{Z}(\bar{G})$ since $\langle \bar{a}, \bar{E} \rangle = \bar{G}$ (recall that $\bar{G}$ is not split over $\bar{E}$). We have $\bar{M} = \langle \bar{a}^2 \rangle \bar{E}$ and $\bar{M}' = [\bar{a}^2, \bar{E}] = \langle \bar{u} \rangle$, where $\bar{u} \in \bar{E} - \langle \bar{z} \rangle$ since $\bar{u}$ is not a square in $\bar{M}$ by Lemma 65.1, and so $\langle \bar{z}, \bar{u} \rangle \leq Z(\bar{G})$ (recall that $\bar{M}$ is minimal nonabelian).

Let $\bar{v} \in \bar{E} - \langle \bar{z}, \bar{u} \rangle$ so that $\bar{v}^{\bar{a}} = \bar{v}\bar{\zeta}$ with $\bar{\zeta} \in \langle \bar{z}, \bar{u} \rangle$ hence $\bar{\zeta} \in \mathrm{Z}(\bar{G})$. But then

$$\bar{v}^{\bar{a}^2} = (\bar{v}\bar{\zeta})^{\bar{a}} = (\bar{v}\bar{\zeta})\bar{\zeta}^{\bar{a}} = \bar{v}\bar{\zeta}^2 = \bar{v}$$

and so $[\bar{a}^2, \bar{E}] = \{1\}$, a contradiction since $\bar{M} = \langle \bar{a}^2, \bar{E} \rangle$ is nonabelian. The proof is complete. □

It follows from Theorem 107.3 and Corollary 36.6 that the number of metacyclic maximal subgroups in any nonmetacyclic two-generator 2-group is even.

Let us show that provided X is a nonmetacyclic two-generator 2-group of minimal possible order, then it is an $\mathcal{A}_1$-group of order 16 which is uniquely determined. Since $X/\mho_2(X)$ is nonmetacyclic two-generator (Corollary 44.9), we get $\mho_2(X) = \{1\}$ so that $\exp(X) = 4$. By Taussky's theorem and Theorem 36.1, X/X' is abelian of type $(4, 2)$. If $R < X'$ is X-invariant of index 2, then X/R is nonmetacyclic and minimal nonabelian (Theorem 36.1) so that $R = \{1\}$. It follows that X is nonmetacyclic minimal nonabelian of order 16 so it is determined uniquely (Lemma 65.1).

Theorem 107.4 ([BJ3, Theorem 5.4]). *Let G be a smallest group from Theorem 107.3, where maximal subgroups M and N of G are both nonmetacyclic. Then G is uniquely determined as follows:*

$$G = \langle a, b \mid a^2 = b^4 = 1,\ [a, b] = c,\ [b, c] = m,$$
$$c^2 = m^2 = [m, a] = [m, b] = [a, c] = 1 \rangle,$$

where

$$|G| = 2^5, \quad G' = \langle c, m \rangle \cong \mathrm{E}_4, \quad \mathrm{K}_3(G) = \mathrm{Z}(G) = \langle m \rangle$$

and so $\mathrm{cl}(G) = 3$. *The three maximal subgroups of G are*

$$M = \langle G', b \rangle, \quad N = \langle G', ab \rangle$$

(which are both nonmetacyclic minimal nonabelian of order 2^4) and

$$K = \langle G', a, b^2 \rangle \cong \mathrm{C}_2 \times \mathrm{D}_8.^{1}$$

Our group G exists as a subgroup of the alternating group A_8.

Proof. By the paragraph preceding the theorem, a smallest possibility for two-generator nonmetacyclic subgroups M and N is the nonmetacyclic minimal nonabelian group

$$\mathrm{H}_{16} = \langle x, y \mid x^2 = y^4 = 1,\ [x, y] = z,\ z^2 = [z, x] = [z, y] = 1 \rangle$$

of order 2^4. Therefore we try to construct our two-generator group G under the assumption that $|G| = 2^5$ and the set of maximal subgroups $\{M, N, K\}$ is such that

[1] Thus G is an $\mathcal{A}_3$-group.

$M \cong N \cong \mathrm{H}_{16}$ and K is a nonabelian group of order 2^4 with $\mathrm{d}(K) = 3$ (indeed, K must be nonabelian by Theorem 106.3). Since G is neither of maximal class (and so $|G'| < 2^3$ by Taussky's theorem) nor minimal nonabelian (and so $|G'| > 2$ by Lemma 65.2(a)), we have $|G'| = 4$. As $\mathrm{d}(G) = 2$, we conclude that G/G' is abelian of type $(4, 2)$ so $G = AB$, where $A \cap B = G'$, $A/G' \cong \mathrm{C}_2$ and $B/G' \cong \mathrm{C}_4$. Let $a \in A - G'$ and $b \in B - G'$ be such that $A = \langle G', a\rangle$ and $B = \langle G', b\rangle$. We have $\Phi(G) = G'\langle b^2\rangle$ so that $G = \langle a, b, G'\rangle = \langle a, b\rangle$, and we set $c = [a, b] \neq 1$. By Proposition 10.17, since K is neither of maximal class nor minimal nonabelian, we get $K = U\mathrm{Z}(K)$, where U is nonabelian of order 8. Note that $K/\Phi(K) \cong \mathrm{E}_8$. We obtain

$$G = M \cup N \cup K \quad \text{and} \quad \exp(M) = \exp(N) = \exp(K) = 4 \quad \text{so} \quad \exp(G) = 4$$

since $G = M \cup N \cup K$. It follows from $|\Phi(G)| = 8$ that $\Phi(G)$ is abelian. Assume that $\Phi(G)$ is abelian of type $(4, 2)$; then every set of generators of $\Phi(G)$ contains an element of order 4 so, since $\Phi(G) = \mho_1(G)$, we get $\exp(G) = 8$, which is a contradiction. Thus $\Phi(G) \cong \mathrm{E}_8$ so $G' \cong \mathrm{E}_4$ and $K \cong \mathrm{D}_8 \times \mathrm{C}_2$ since $\mathrm{Z}(K) \cong \mathrm{E}_4$. It follows that $|G' : K'| = 2$ so G/K' is nonmetacyclic $\mathscr{A}_1$-group (of order 2^4 and hence we get $G/K' \cong \mathrm{H}_{16}$ by Lemmas 65.1 and 65.2(a)); in particular, $M' = N' = K'$ since M/K' and N/K' are abelian. Since $|K'| = 2$, we have $K' = \langle m\rangle \leq \mathrm{Z}(G)$ and so $G' = \langle c, m\rangle (\cong \mathrm{E}_4)$, where $o(c) = 2$.

As we have shown, G/K' is a nonmetacyclic $\mathscr{A}_1$-group. Therefore, by Lemma 65.1, the generator of G'/K' is not a square in G/K', and we conclude that $a^2 \in \langle m\rangle$. Since $K/G' \cong \mathrm{E}_4$ and G/G' is abelian of type $(4, 2)$, we get $K/G' = \Omega_1(G/G')$ so that $M/G' \cong \mathrm{C}_4 \cong N/G'$. It follows from $\Phi(G) \cong \mathrm{E}_8$ that $\Phi(G) = \langle b^2\rangle \times G'$ so that $A\langle b^2\rangle/\langle m\rangle \cong \mathrm{E}_8$ and so we must have $K = A\langle b^2\rangle$ with $\Phi(K) = \langle m\rangle$. The other two maximal subgroups are $G'\langle b\rangle$ and $G'\langle ab\rangle$ so that we may set $M = B = G'\langle b\rangle$ and $N = G'\langle ab\rangle$. We have $M = \langle b, c, m\rangle = \langle b, c\rangle$ since $m \in \Phi(M)$, and similarly $N = \langle ab, c\rangle$, so that $[b, c] = [ab, c] = m$ since $M' = N' = K' = \langle m\rangle$. We compute

$$m = [ab, c] = [a, c]^b[b, c] = [a, c]^b m$$

which gives $[a, c] = 1$ and therefore $A = \langle a, c, m\rangle$ is abelian of order 8. Further,

$$[a, b^2] = [a, b][a, b]^b = cc^b = c(cm) = m.$$

If $a^2 = m$, then $\langle a, b^2\rangle \cong \mathrm{D}_8$, and then $a' = ab^2$ is an involution. Replacing a with a' (if necessary), we may assume from the start that a is an involution, and then $A = \langle a, c, m\rangle \cong \mathrm{E}_8$ (see the above two displayed formulas; recall that A is abelian since $[a, c] = 1 = [a, m] = [c, m]$). We get $K = \langle c\rangle \times \langle a, b^2\rangle \cong \mathrm{C}_2 \times \mathrm{D}_8$ and the structure of G is uniquely determined as given in the statement of the theorem. It is easy to see that $\mathrm{Z}(G) = \langle m\rangle = \mathrm{K}_3(G)$ so $\mathrm{cl}(G) = 3$.

The existence of G as a subgroup of A_8 is established if we set

$$a = (2, 7)(3, 8) \quad \text{and} \quad b = (1, 2, 3, 4)(5, 6, 7, 8).$$

It is enough to check that the permutations a and b satisfy all the above relations. Since we get $m = (1,6)(2,7)(3,8)(4,5) \neq 1_G$ and $\langle m \rangle = \mathrm{Z}(G)$, our permutation representation is faithful. □

Theorem 107.5 ([BJ3, Theorem 5.5]). *Suppose that G is a nonmetacyclic two-generator 2-group and let M, N, K be all its maximal subgroups such that M, N are nonmetacyclic two-generator and $\mathrm{d}(K) = 3$ (see Theorem 107.3). Then there is $R \lhd G$ such that G/R is isomorphic to the group from Theorem 107.4.*

Proof. We may assume that $|G| > 2^5$ (otherwise, in view of Theorem 107.4, there is nothing to prove). Since two-generator abelian 2-groups are metacyclic, the (nonmetacyclic two-generator) subgroups M and N are nonabelian. It follows that G is neither abelian nor minimal nonabelian; in particular, $|G'| > 2$ (Lemma 65(a)). In view of Theorem 106.3, K is nonabelian. Let L_1 be a G-invariant subgroup of index 2 in M' (since $\mathrm{d}(M) = 2$, the quotient group $M'/\mathrm{K}_3(M)$ is cyclic so L_1 is uniquely determined). By Theorem 36.1, M/L_1 is not metacyclic and neither is G/L_1. We also have $L_1 < \Phi(M) < \Phi(G) = N \cap K$. Since $\mathrm{d}(N/L_1) = 2 = \mathrm{d}(G/L_1)$, it follows that $\mathrm{d}(K/L_1) = 3$ (Corollary 36.6). By Theorem 107.3, N/L_1 is nonmetacyclic so nonabelian. Thus the group G/L_1 satisfies the hypothesis. Therefore, without loss of generality, one may assume that $L_1 = \{1\}$.

Let L_2 be a G-invariant subgroup of index 2 in N'. As above, N/L_2 is not metacyclic so is M/L_2, and $\mathrm{d}(K/L_2) = 3$, so again G/L_2 satisfies the hypothesis, and we may assume that $L_2 = \{1\}$. By Lemma 65.2(a), M and N are $\mathfrak{A}_1$-groups since, by construction, $|M'| = 2 = |N'|$.

Now set $L_3 = \mathfrak{V}_2(M)$. Then, by Supplement to Corollary 36.6, M/L_3 is not metacyclic and, as above, G/L_3 satisfies the hypothesis so, arguing as above, one may assume that $L_3 = \{1\}$. Similarly, one may assume that $\mathfrak{V}_2(N) = \{1\}$. In that case, we get $\exp(M) = \exp(N) = 4$. Since M and N are nonmetacyclic two-generator, they are nonabelian so $\mathfrak{A}_1$-groups as epimorphic images of $\mathfrak{A}_1$-groups. From Lemma 65.1 we deduce $|M| \leq 2^5$ (indeed, an $\mathfrak{A}_1$-group of exponent 2^n has order $\leq 2^{2n+1}$). By assumption, we must have $|G| > 2^5$ so $|M| = 2^5$ and M/M' is abelian of type $(4,4)$, $|G| = 2^6$. In that case, by Lemma 65.1,

$$\mathrm{Z}(M) = \Phi(M) = \Omega_1(M) \cong \mathrm{E}_8 \cong \Omega_1(N) = \mathrm{Z}(N) = \Phi(N).$$

Since

$$\mathrm{Z}(M) = \Phi(M) < \Phi(G) < N \quad \text{and} \quad \mathrm{Z}(N) < \Phi(G) < M,$$

it follows that $\mathrm{Z}(M) = \mathrm{Z}(N) = \mathrm{Z}(G) (\cong \mathrm{E}_8)$ (indeed, we have $\mathrm{Z}(G) < M$ in view of $\mathrm{d}(G) = 2$). The quotient group $G/\mathrm{Z}(G)$ of order 8 is not elementary abelian since $\mathrm{d}(G) = 2$. It follows that $G/\mathrm{Z}(G)$ contains a cyclic subgroup, say $C/\mathrm{Z}(G)$, of order 4. In that case, C is abelian so $\mathrm{d}(C) = 3$. Since K is a unique maximal subgroup of G not generated by two elements, we get $C = K$ so that K is abelian. This is a final contradiction: by the above, G has no abelian maximal subgroups. □

Let G be a two-generator 2-group all of whose maximal subgroups are not two-generator (in that case all those subgroups are three-generator by Appendix 25); then G is nonabelian. Denote by H_{32} the unique $\mathcal{A}_1$-group of order 32 and exponent 4 (see Lemma 65.1; all maximal subgroups of H_{32} are abelian of type $(4,2,2)$).

Supplement to Theorem 107.5 ([BJ3]). *If all maximal subgroups of a two-generator 2-group G are not two-generator, then there is $R \lhd G$ such that $G/R \cong \mathrm{H}_{32}$.*

Proof. Indeed, if $M < G$ is maximal, then $\Phi(M) = \mho_1(M) \geq \mho_2(G)$ so that, as we have noticed, $\mathrm{d}(M/\mho_2(G)) = \mathrm{d}(M) = 3$. Thus $G/\mho_2(G)$ satisfies the hypothesis so one may assume that $\mho_2(G) = \{1\}$ holds. By Theorem 107.2(a), G/G' is abelian of type $(4,4)$. If R is G-invariant of index 2 in G', then $G/R \cong \mathrm{H}_{32}$ (Lemmas 65.2(a) and 65.1), as desired. □

It follows that if a group G from the supplement has minimal possible order, then $G \cong \mathrm{H}_{32}$.

Remark 1. Suppose that a nonabelian two-generator p-group G, $p > 2$, has an abelian subgroup A of index p. (i) If $\Omega_1(G) = G$, then $\exp(G/G') = p$ so $|G/G'| = p^2$ and G is of maximal class (to prove this, we use Lemma 1.1 and induction). (ii) If $\Omega_1(G) \not\leq A$, then $|G : G'\mho_1(A)| = |G : \Phi(G)| = p^2$ (indeed, $A\Omega_1(G) = G$, $G'\mho_1(A) \leq G'\mho_1(G) = \Phi(G)$ and $G/G'\mho_1(A)$ is elementary abelian since it is abelian of rank 2 and generated by elements of order p as an epimorphic image of $G/\mho_1(A) = A\Omega_1(G)/\mho_1(A)$). Thus $|G/\mho_1(A) : (G/\mho_1(A))'| = p^2$. It follows from (i) that $G/\mho_1(A)$ is of maximal class; then $\mathrm{d}(A) = \mathrm{d}(A/\mho_1(A) \leq p$ by Exercise 9.13.

Remark 2. Let $p > 2$ and let G be a two-generator p-group containing a maximal subgroup M such that $\mathrm{d}(M) = p+1$ (see Appendix 25). Let us study the structure of $G/\Phi(M)$. To simplify our task, one may assume that $\Phi(M) = \{1\}$; then $M \cong \mathrm{E}_{p^{p+1}}$ so G is not of maximal class (Theorems 9.5 and 9.6). It follows that $|\mathrm{Z}(G)| > p$ (if $|\mathrm{Z}(G)| = p$, then $|G : G'| = p|\mathrm{Z}(G)| = p^2$ by Lemma 1.1, so G is of maximal class contrary to what has just been said). Thus we have $|G/G'| = p|\mathrm{Z}(G)| \geq p^3$. If $G/G'| > p^3$, then, in view of $M \cong \mathrm{E}_{p^{p+1}}$, $p+1 \geq 4$, $M/G' < G/G'$ and $\mathrm{d}(M/G') > 2 = \mathrm{d}(G/G') = \mathrm{d}(G)$, we get a contradiction. Thus $|G/G'| = p^3$ hence $\exp(G/G') = p^2$ since $\mathrm{d}(G/G') = \mathrm{d}(G)) = 2$, and we conclude that G/G' is abelian of type (p^2, p). Write $H/G' = \Omega_1(G/G')$; then $M \leq \Omega_1(G) \leq H$ so that $M = H = \Omega_1(G)$ since $M \in \Gamma_1$. Let $x \in G - M$; then $G = \langle x, M\rangle$, $o(x) = p^2$ and $x^p \in \mathrm{Z}(G)$ since M is abelian. Write $\bar{G} = G/\langle x^p\rangle$. Since $\Omega_1(\bar{G}) = \bar{G}$, the group $\bar{G}$ is of maximal class (Remark 1(i)), isomorphic to Σ_{p^2}, a Sylow p-subgroup of the symmetric group of degree p^2 by Exercise 9.13. If $\bar{K} < \bar{G}$ is maximal and nonabelian, then $\bar{K}$ is of maximal class (Fitting's lemma). However, K is not of maximal class since $\mathrm{d}(G) = 2$ (here we use Theorem 12.12(a)), so $|\mathrm{Z}(K)| > p$. We have $\mathrm{Z}(K) < M$ (otherwise, $G = M\mathrm{Z}(K)$ so $\mathrm{cl}(G) = 2$, a contradiction). Thus $\mathrm{C}_G(\mathrm{Z}(K)) \geq MK = G$ so $\mathrm{Z}(K) = \mathrm{Z}(G)$ since $\mathrm{Z}(G) < \Phi(G) < K$ in view of $\mathrm{d}(G) = 2$.

§108

p-groups with few conjugate classes of minimal nonabelian subgroups

Let $\kappa_1(G)$ be the number of conjugate classes of $\mathcal{A}_1$-subgroups (= minimal nonabelian subgroups) of a p-group G (see §76). If $\kappa_1(G) \leq 1$, then G is either abelian or an $\mathcal{A}_1$-group (Theorem 10.28). Therefore only the case where $\kappa_1(G) > 1$ is interesting. It follows from Remark 76.1 that if a p-group G is neither abelian nor minimal nonabelian, then $\kappa_1(G) \geq p$.

Proposition 108.1. *Suppose that a p-group G contains a normal nonabelian subgroup N of index p^n such that G/N is noncyclic. Then we have $\kappa_1(G) \geq n + p$. If, in addition, $\kappa_1(G) = n + p$, then all proper G-invariant subgroups of N are abelian.*

Proof. By hypothesis, $n \geq 2$. Let $N = N_0 < N_1 < \cdots < N_n = G$ be a chain of G-invariant subgroups such that G/N_{n-2} is noncyclic; then all indices of this chain are equal to p. Since a nonabelian p-group is generated by its minimal nonabelian subgroups (Theorem 10.28), there is a minimal nonabelian subgroup $S_i < N_i$ such $S_i \not\leq N_{i-1}$, $i = 1, \ldots, n-2$. We have $G/N_{n-2} \cong \mathrm{E}_{p^2}$. Let $S_0 \leq N_0 = N$ be minimal nonabelian and $N_{n-1} = N_{n-1,1}, \ldots, N_{n-1,p+1}$ all (nonabelian) maximal subgroups of G containing N_{n-2}. Let $S_{n-1,i} < N_{n-1,i}$ be minimal nonabelian not contained in N_{n-2}, $i = 1, 2, \ldots, p+1$. Since $(n-2) + 1 + (p+1) = n + p$ minimal nonabelian subgroups $S_0, S_1, \ldots, S_{n-2}, S_{n-1,1}, \ldots, S_{n-1,p+1}$ are not conjugate in pairs (indeed, normal closures of these subgroups in G are pairwise distinct), we get $\kappa_1(G) \geq n + p$.

Now suppose that $\kappa_1(G) = n + p$. Assume that there is in N a proper nonabelian G-invariant subgroup R; then G/R is noncyclic of order $\geq p^{n+1}$. By the previous paragraph, $\kappa_1(G) \geq (n+1) + p > n + p$, a contradiction. Thus all proper G-invariant subgroups of N are abelian. □

Proposition 108.2. *Suppose that a p-group G of order $p^m > p^3$ is of maximal class with abelian $A \in \Gamma_1$. Then $\kappa_1(G) = p$.*

Proof. It is well known that all nonabelian subgroups of G are of maximal class so all minimal nonabelian subgroups of G have the same order p^3, and the number of minimal nonabelian subgroups in G equals p^{m-3}. Indeed, $\Gamma_1 = \{H_1, \ldots, H_p, A\}$, where $H_1, \ldots, H_p$ are of maximal class (Fitting's lemma). Then, by induction, H_i contains

$p^{m-1-3} = p^{m-4}$ minimal nonabelian subgroups, and $H_i \cap H_j = \Phi(G)(< A)$ is abelian for all $i \neq j$, so the number of minimal nonabelian subgroups in G is equal to $p \cdot p^{m-1-3} = p^{m-3}$, as asserted. If $S_i \leq H_i$ is minimal nonabelian, $i = 1, \ldots, p$, then $S_1, \ldots, S_p$ are pairwise nonconjugate since $S_i^G = H_i$ for $i = 1, \ldots, p$ (indeed, if a G-invariant subgroup has index $> p$ in G, then it is contained in $\Phi(G)$; see Exercise 9.1(b)). We have $|G : \mathrm{N}_G(S_i)| = p^{m-4}$ for all $i = 1, \ldots, p$. Indeed, $\mathrm{N}_G(S_i)$ is nonabelian hence of maximal class. Since all normal subgroups of $\mathrm{N}_G(S_i)$ of index $> p$ are abelian, we get $|\mathrm{N}_G(S_i)| = p|S_i| = p^4$, proving our claim. Thus all minimal nonabelian subgroups of H_i are conjugate in G for $i = 1, \ldots, p$ and do not lie in G_j $(j \neq i)$ hence $\kappa_1(G) = p$. □

Proposition 108.3. *Suppose that G is a group of exponent p. Then $\kappa_1(G) = p$ if and only if G is of maximal class and order $> p^3$ with an abelian subgroup of index p. In this case, $|G| \leq p^p$, and so we must have $p > 3$.*

Proof. By hypothesis, $|G| > p^3$. If G is of maximal class with an abelian subgroup of index p, then $\kappa_1(G) = p$ (Proposition 108.2).

Now let $\kappa_1(G) = p$. Then, by Theorem 76.17, $\mathrm{d}(G) = 2$ and G has an abelian maximal subgroup. As $\Phi(G) = G'$, we get $|G : G'| = p^2$. It follows that G is of maximal class so $|G| \leq p^p$ (Theorem 9.5). Since G is not of maximal class, we get $p > 3$. □

Let $\xi(G)$ be the number of conjugate classes of maximal cyclic subgroups of a p-group G. Then $\xi(G) \geq k = 1 + p + \cdots + p^{\mathrm{d}(G)-1}$. Indeed, if $x \in G - \Phi(G)$, then $\langle x \rangle$ is a maximal cyclic subgroup of G. The group $G/\Phi(G)$ has exactly k subgroups of order p, say $M_1/\Phi(G), \ldots, M_k/\Phi(G)$. Let $C_i \leq M_i$ be cyclic such that $C_i \not\leq \Phi(G)$ for all i. Then $C_1, \ldots, C_k$ are maximal cyclic subgroups in G. Since we have $C_i^G \leq C_i\Phi(G) = M_i$ for all i and $M_i \cap M_j = \Phi(G)$ $(i \neq j)$, it follows that $C_1, \ldots, C_k$ are pairwise nonconjugate in G so that $\xi(G) \geq k$. It is interesting to classify the p-groups G satisfying $\xi(G) = k$ (all 2-groups of maximal class satisfy this condition).

Exercise. If G is a nonabelian p-group, then $\kappa_1(G) \geq d(G) - 1$. Improve this estimate in the case $\mathrm{d}(G) > 3$. (*Hint*. If A is minimal nonabelian, then the subgroup $A\Phi(G)$ is nonabelian of index $\geq p^{\mathrm{d}(G)-2}$ in G and G-invariant. Apply Proposition 108.1.)

Problems

Problem 1. Estimate the maximal possible number of conjugate classes of minimal nonabelian subgroups in a p-group of maximal class and order p^m.

Problem 2. Estimate the maximal possible number of conjugate classes of minimal nonabelian subgroups in representation groups of elementary abelian group E_{p^n}.

Problem 3. Estimate the maximal possible number of conjugate classes of minimal nonabelian subgroups in metacyclic groups of order p^m.

§109

On p-groups with metacyclic maximal subgroup without cyclic subgroup of index p

According to [MS, Lemma 4.9], if $p > 3$ is a prime and if a is an automorphism of order p of the abelian group L of type (p^2, p^2), then a centralizes $\Omega_1(L)$ (the proof of this result is also reproduced in [AS, Lemma A.1.30]). We offer a generalization of this result. Our proof is based on entirely other ideas.

Theorem 109.1. *Suppose that $p > 2$ and L is a metacyclic p-group without cyclic subgroup of index p. An element $a \in \mathrm{Aut}(L)$ of order p does not centralize $\Omega_1(L)$ if and only if $p = 3$, the partial holomorph $G = \langle a \rangle \cdot L$ is a 3-group of maximal class and one of the following holds:*

(a) *L is abelian of type $(3^m, 3^n)$, $m > 1, n > 1$ and $|m - n| \leq 1$.*

(b) *$L = \langle a, b \mid a^{3^m} = b^{3^n} = 1,\ a^b = a^{1+3^{m-1}} \rangle$ is minimal nonabelian, $|m-n| \leq 1$.*

Proof. Suppose that $G = \langle x, G_1 \rangle$ is a 3-group of maximal class and order $> 3^4$ with regular subgroup G_1 of index 3 such that $o(x) = 3$. Then G_1, the fundamental subgroup of G, is metacyclic so $\mathrm{d}(G_1) = 2$ (see Theorems 9.6(b) and 9.11). If G_1 is abelian of type $(3^m, 3^n)$, then $|m - n| \leq 1$ since G has no normal cyclic subgroup of order 3^2 (indeed, G has a normal abelian subgroup of type $(3, 3)$ and it is a unique G-invariant subgroup of order 9 by Exercise 9,1; if $k = \min\{m, n\}$, then $\mho_k(G_1)$ is cyclic of order $p^{|m-n|}$ and characteristic in L so normal in G). Next, we obtain that $\mathrm{C}_G(\Omega_1(G_1)) = G_1$ so x does not centralize $\Omega_1(G_1)$. Now suppose that G_1 is nonabelian. Then $|G_1'| = 3$ since G_1' is G-invariant cyclic so G_1 is minimal nonabelian (Lemma 65.2(a)). In this case, by Lemma 65.1 (see also Exercise 1.8(a)), G_1 has the same defining relations as L in part (b) of our theorem. Since $\mho_{|m-n|}(G_1)$ is cyclic, we get again $|m - n| \leq 1$. As, by hypothesis, $G_1/\Omega_1(G_1)$ is noncyclic, we also have $\Omega_1(G_1) \leq \Phi(G_1) = \mathrm{Z}(G_1)$ since $\mathrm{d}(G_1) = 2$. Since again $\mathrm{C}_G(\Omega_1(G_1)) = G_1$, the element x does not centralize $\Omega_1(G_1)$.

Next we assume that G is not a 3-group of maximal class.

Now suppose that L and a are as in the statement of our theorem. We have to describe the structure of L. Put $G = \langle a, L \rangle$. Since L is regular, the subgroup $\Omega_1(L)$ is abelian of type (p, p); clearly, $\Omega_1(L) \lhd G$. As $|\Omega_1(G)| \geq p^3$, G is nonmetacyclic. Since L has no cyclic subgroup of index p, the quotient group $L/\Omega_1(L)$ is noncyclic.

Suppose that a does not centralize $\Omega_1(L)$. It follows that $H = \langle a, \Omega_1(L)\rangle$ is nonabelian of order p^3 and exponent p since $p > 2$. We have $G = LH$ since $H \not\leq L$ and $L \in \Gamma_1$.

Assume that G is regular. Then $\exp(\Omega_1(G)) = p$ (Theorem 7.2(b)) so, considering the intersection $L \cap \Omega_1(G)$, we conclude that $|\Omega_1(G)| = p|\Omega_1(L)| = p^3 = |H|$ whence $\Omega_1(G) = H$ (H is defined in the previous paragraph). It follows that G has no elementary abelian subgroups of order p^3. Since G is neither metacyclic nor a 3-group of maximal class (Theorems 9.5 and 9.6), we can conclude from Theorem 13.7 that $G/\Omega_1(G)$ is cyclic, a contradiction since

$$G/\Omega_1(G) \cong L\Omega_1(G)/\Omega_1(G) \cong L(L \cap \Omega_1(G)) = L/\Omega_1(L),$$

and the last quotient group, as we have noticed, is noncyclic.

Now let G be irregular (by assumption in the first paragraph of the proof, G is not a 3-group of maximal class). It follows from Theorems 9.5 and 9.6 that G is not of maximal class for $p > 3$ as well. Therefore, by Theorem 12.1(b), $G = L\Omega_1(G)$, where $\Omega_1(G)$ is of order p^p and exponent p. Since $L \cap \Omega_1(G) = \Omega_1(L)$ is elementary abelian of order p^2, we get $p = 3$. It follows that $\Omega_1(G) = H = \langle a, \Omega_1(L)\rangle$ is nonabelian of order 3^3 and exponent 3 so G has no elementary abelian subgroups of order 3^3. In this case, since G/H is noncyclic, the group G is of maximal class (Theorem 13.7), a final contradiction. □

As we have noticed, the regular maximal subgroup of a 3-group of maximal class and order $> 3^4$ is such as in conclusion of Theorem 109.1.

Corollary 109.2. *Suppose that $p > 2$ and L is an abelian group of type (p^m, p^n), $m > 1$, $n > 1$. An element $a \in \mathrm{Aut}(G)$ of order p does not centralize $\Omega_1(L)$ if and only if $p = 3$, $G = \langle a, L\rangle$ is a 3-group of maximal class and $|m - n| \leq 1$.*

Remark. Now we consider a similar but more complicated situation for $p = 2$. Suppose that a metacyclic 2-group L without cyclic subgroup of index 2 is maximal in a 2-group G and $\Omega_1(L) \leq \mathrm{Z}(L)$; then $\Omega_1(L)$ is a four-subgroup. In this case, G is not of maximal class. Suppose that there is an involution $a \in G - L$ which does not centralize $\Omega_1(L)$. We claim that G is not metacyclic. Assume that this is false. Then the nonabelian subgroup $\langle x, \Omega_1(L) \cong \mathrm{D}_8$ so G is of maximal class (Proposition 10.19), contrary to what has just been said. By hypothesis, $\mathrm{C}_G(\Omega_1(L)) = L$. Now we use Theorem 66.1 classifying minimal nonmetacyclic 2-groups. Let H be a minimal nonmetacyclic subgroup of G. If $H \cong \mathrm{E}_8$, then $L \cap H = \Omega_1(L)$ so $\mathrm{C}_G(\Omega_1(L)) \geq HL = G$, a contradiction. In case $H \cong \mathrm{Q}_8 \times \mathrm{C}_2$, we have $\mathrm{Z}(H) = \Omega_1(H) = \Omega_1(L) < H \cap L$ so we get $\mathrm{C}_G(\Omega_1(L)) \geq HL = G$, a contradiction. Now assume that $|H| = 2^5$ (this H is special with center of order 4). As $\exp(H) = 4$, it follows that $\Omega_1(L) = \Omega_1(H)$, and since $\Omega_1(H) = \mathrm{Z}(H)$, we get $\mathrm{C}_G(\Omega_1(L)) \geq HL = G$, a contradiction. Thus $H \cong \mathrm{D}_8 * \mathrm{C}_4$ is of order 16. Similarly, if $F < G$ is minimal nonabelian, then either $|F| = 8$ or $F \cong \mathrm{M}_{2^n}$ (Lemma 65.1). As we know (see Theorem 10.28), it is possible to choose F so that $F \not\leq L$.

If a noncyclic p-group L which contains a cyclic subgroup Z of index p is not a 2-group of maximal class (then $\Omega_1(L)$ is abelian of type (p, p)), is maximal in a p-group $G = \langle a, L\rangle$ and an element $a \in G - L$ of order p does not centralize $\Omega_1(L)$, then $H = \langle a, \Omega_1(L)\rangle$ is nonabelian of order p^3 and $G = HZ$ with $H \cap Z = \mathrm{Z}(H)$ and $\Omega_1(H) = H$. If, in addition, $p = 2$, then all minimal nonmetacyclic subgroups of G have order 2^4 and are isomorphic to $\mathrm{D}_8 * \mathrm{C}_4$ (Theorem 66.1).

Let L be a maximal subgroup of a p-group $G = \langle x, L\rangle$, where $p > 2$ and $\Omega_1(L)$ is abelian of type (p, p) (then L is either metacyclic or an irregular 3-group of maximal class by Theorem 13.7) and $o(x) = p$. Suppose that x does not centralize $\Omega_1(L)$. Then $H = \langle x, \Omega_1(L)\rangle$ is nonabelian of order p^3 and exponent p. Clearly, G has no subgroup of order p^4 and exponent p (if such a subgroup, say F, exists, then we get $|\Omega_1(F \cap L) = p^3 > p^2 = |\Omega_1(L)|$, a contradiction). Then either $G = HC$, where $H = \Omega_1(G)$ and C is cyclic, or G is a 3-group of maximal class (Theorem 12.1(a)). In the first case, $|L/\mho_1(L)| = |\Omega_1(L)| = p^2$ (Theorem 7.2(d)) so L is metacyclic (Theorem 9.11), and this case we have already considered. Now assume that G and L are 3-groups of maximal class and $|G| > 3^4$. Then $\mathrm{C}_G(\Omega_1(L)) = G_1$ is metacyclic and x does not centralize $\Omega_1(G_1)$. Such a G_1, by Theorem 109.1, is either abelian or minimal nonabelian so $G_1 \neq L$; we see that $L \cap G_1 = \Phi(G)$ is abelian of index 3 in L.

Exercise 1. Let G be a p-group, $p > 2$, and suppose that a noncyclic $M \in \Gamma_1$ is metacyclic. If $\mathrm{C}_G(\Omega_1(M)) = M$, then either M contains a cyclic subgroup of index p or G is a 3-group of maximal class. (Here we do not assume that G splits over M.)

Exercise 2. Let G be a 2-group and suppose that $M \in \Gamma_1$ is metacyclic but neither cyclic nor of maximal class. Suppose that $\mathrm{C}_G(\Omega_1(M)) = M$. Classify the minimal nonabelian subgroups of G which are not contained in M.

Answer. Q_8, D_8 and M_{2^n}.

§110

Equilibrated p-groups

We begin with the following

Definition (compare with [BDM]). A p-group G is said to be *weakly equilibrated* (in short WE-*group*) if it follows from $G = AB$ with $A, B < G$ that one of the factors A, B is G-invariant. A group G is said to be *equilibrated* (briefly: E-*group*) if every of its subgroup is weakly equilibrated. If, in addition, G is a p-group, then it is called a WE_p-*group* and an E_p-*group*, respectively.

Obviously, the properties WE, E, WE_p and E_p are inherited by quotient groups. It is not true that the property WE_p is inherited by subgroups (for example, if the fundamental subgroup G_1 of a 3-group G of maximal class and order 3^5 is nonabelian, then G_1 is not an E_3-group which follows from Exercise 5 below). However, as Lemma 110.1 shows, this group G is a WE_3-group. A minimal nonabelian WE_p-group is an E_p-group since abelian p-groups are E_p-groups.

Next, we follow [BDM]. We consider p-groups only. Note that in [BDM] the non-nilpotent groups are also studied.

In what follows G is a non-Dedekindian WE_p-group of order p^m (Dedekindian p-groups are E_p-groups). Since groups of order p^3 are E_p-groups, one may assume that $m > 3$. As all subgroups of M_{p^m} of order $> p$ are normal, M_{p^m} is an E_p-group. Moreover, all groups from Theorem 1.25 are E_p-groups.

Exercise 1. (a) A nonmetacyclic minimal nonabelian p-group G of order $p^m > p^3$ is not a WE_p-group.

(b) All two-generator WE_2-groups are metacyclic.

(c) If G is a nonmetacyclic two-generator WE_p-group, $p > 2$, then $|G : G'| = p^2$.

(d) If a metacyclic p-group G is a non-WE_p-group with $|G'| = p$ and $G = AB$, where A, B are not G-invariant, then A and B are cyclic.

Solution. (a) We first assume that $m = 4$. In this case, by Lemma 65.1,

$$G = \langle a, b \mid a^{p^2} = b^p = 1,\ c = [a, b],\ c^p = [a, c] = [b, c] = 1 \rangle.$$

Set $A = \langle a \rangle$ and $B = \langle a^p c, b \rangle$. Then $|A| = |B| = p^2$ and $A \cap B = \{1\}$ so we have $G = AB$ by the product formula. Since $G' = \langle c \rangle \not\leq A$ and $G' \not\leq B$, neither A nor B

are G-invariant, and our claim follows. Now let $m > 4$. In this case,

$$G = \langle a, b \mid a^{p^r} = b^{p^s} = 1,\ c = [a, b],\ c^p = 1,\ [a, c] = [b, c] = 1\rangle.$$

We also assume that $r \geq s$; then $r > 1$. Set $T = \langle a^{p^2}, b^p\rangle$. Then the quotient group G/T is a nonmetacyclic minimal nonabelian p-group of order p^4 so, by the above, it is not a WE_p-group. In this case, G is also not a WE_p-group since the property WE_p is inherited by epimorphic images.

(b) Suppose that a two-generator WE_2-group G is nonmetacyclic; then it is nonabelian and $|G : G'| > 4$ (Taussky's theorem). By Theorem 36.1, if $R < G'$ is G-invariant of index 2, then G/R is nonmetacyclic and minimal nonabelian. Therefore, by part (a), G/R is not a WE_2-group since $|G/R| > 2^3$, and our claim follows.

(c) Assume, by way of contradiction, that $|G : G'| > p^2$. If $R < G'$ of G-invariant of index p, then G/R is nonmetacyclic and minimal nonabelian (Theorem 36.1) so it is not a WE_p-group by (a) since $|G/R| > p^3$; then G is not a WE_p-group as well.

(d) A noncyclic subgroup of G contains $\Omega_1(G) > G'$ and a subgroup containing $\Omega_1(G)$ is normal. If $C < G$ is cyclic such that G/C is cyclic, then $A \cap C = \{1\} = B \cap C$, and the claim follows. (In the case under consideration, G is minimal nonabelian by Lemma 65.2(a).)

Exercise 1. A 2-group G of maximal class is an E_2-group.

Solution. Assume that $G = AB$, where $A, B < G$, and $|A| \geq |B|$, A and B are not normal in G; then $|A| \geq 4$, $|B| \geq 4$. Let $C < G$ be cyclic of index 2. Then, since $|B \cap C| \leq |A \cap C|$, we get $B \cap C \leq A \cap B$. As $B \cap C \lhd G$, one may assume that $B \cap C = \{1\}$. In this case, $|G : A| \leq |B| = 2$ so $A \lhd G$, contrary to the assumption. It follows that G is also an E_2-group since all its proper subgroups are either cyclic or of maximal class.

Exercise 2. Suppose that G is a two-generator nonmetacyclic p-group of order p^4, $p > 2$. Then G is a WE_p-group if and only if G is of maximal class and has no subgroup isomorphic to E_{p^3}.

Solution. Let G be a WE_p-group. We have to prove that G has no subgroup $\cong \mathrm{E}_{p^3}$. By Exercise 1(a), G is not minimal nonabelian. Let $B < G$ be minimal nonabelian. Since $\mathrm{d}(G) = 2$, we get $\mathrm{C}_G(B) < B$ so G is of maximal class (Proposition 10.17). Assume that G has a subgroup $U \cong \mathrm{E}_{p^3}$. Then $U = \mathrm{Z}(G) \times A$, where $A \cong \mathrm{E}_{p^2}$, so $A_G = \{1\}$, i.e., A is not G-invariant. Let $V < G$ be of order p^2 such that $V \not\leq U$; then V is not normal in G (otherwise, $V = \Phi(G) < U$).[1] In this case, $\mathrm{C}_G(V \cap U) = UV = G$ so $U \cap V = \mathrm{Z}(G)$, and we get $V \cap A = \{1\}$. Then $G = AB$ by the product formula, and we conclude that G is not a WE_p-group, contrary to the assumption. Now suppose that G has no subgroup $\cong \mathrm{E}_{p^3}$. We have to prove that then G is a WE_p-group. Assume that $G = AB$, where A and B are not normal in G; then $|A| = p^2 = |B|$. If A

[1] If V does not exist, then U is generated by all subgroups of G of order p^2 so G has a cyclic subgroup of index p, a contradiction (Theorem 1.2).

is noncyclic, then $\mathrm{Z}(G) < A$ (otherwise, $\mathrm{Z}(G)A \cong \mathrm{E}_{p^3}$, contrary to the assumption). If A is cyclic, then $\mathrm{Z}(G) = \mho_1(G) < A$ since $G/\mho_1(G)$ is of order p^3 (Theorem 9.11) and exponent p. Thus, in any case, $\mathrm{Z}(G)$ is contained in A and B so, by the product formula, $|AB| < p^4 = |G|$, a contradiction. Now it is clear that G is an E_p-group if it has no subgroup $\cong \mathrm{E}_{p^3}$.

Exercise 3. Suppose that G is a p-group of maximal class and order $> p^4$, $p > 3$. Then G is not a WE_p-group.

Solution. By Theorems 9.5 and 9.6, $|G/\mho_1(G)| \geq p^4$. Let $\mho_1(G) \leq N \lhd G$ be such that $|G/N| = p^4$; then $N < \Phi(G)$, $\exp(G/N) = p$ and G/N (of maximal class and exponent p) has a subgroup $\cong \mathrm{E}_{p^3}$. By Exercise 3, G/N is not a WE_p-group so is G.

Exercise 4. If $p > 2$ and $G = \langle a, b \mid a^{p^2} = b^{p^2} = 1, a^b = a^{1+p} \rangle$ is nonabelian metacyclic of order p^4 and exponent p^2, then G is not a WE_p-group.

Solution. We have $\mathrm{Z}(G) = \langle a^p \rangle \times \langle b^p \rangle = \Omega_1(G) = \mho_1(G)$ and $G' = \langle a^p \rangle$. Set $B = \langle b \rangle$; then B is not G-invariant. The quotient group $G/\langle a^p b^p \rangle$ is nonabelian so it has a nonnormal subgroup $A/\langle a^p b^p \rangle$ of order p. It follows that A is cyclic (indeed, all noncyclic subgroups of G are normal). In this case, $A \cap B = \{1\}$, and so we get $G = AB$ by the product formula. Thus G is not a WE_p-group.

Remark. Moreover, if $p > 2$, then $G = \langle a, b \mid a^{p^n} = b^{p^n} = 1, a^b = a^{1+p^{n-1}} \rangle$ is not a WE_p-group. The group G is metacyclic minimal nonabelian (Lemma 65.2(a)). We have $\mho_{n-1}(G) = \Omega_1(G) \leq \mathrm{Z}(G)$. If L is of order p and $L \notin \{\Omega_1(\langle b \rangle), G'\}$, then there is $x \in G$ such that $L = \langle x^{p^{n-1}} \rangle$ (Theorem 7.2(c)). Then, by the product formula, $G = UV$, where $U = \langle b \rangle$, $V = \langle x \rangle$ are not G-invariant. Indeed, $V \cap G' = \{1\}$, and if $V \lhd G$, then $G = \langle a \rangle \times V$ is abelian, a contradiction. From this it also follows that $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{n-1}} \rangle$, where $m < n$, is not a WE_p-group (consider the quotient group $G/\langle b^{p^{n-m}} \rangle$).

It is easy to show that a nonabelian metacyclic group G of order 2^4 and exponent 4 is a WE_2-group. To prove this, it suffices to notice that all subgroups of order 2 of G are characteristic and exactly one of them is maximal cyclic. Indeed, let $G = AB$, where $A, B < G$ are not G-invariant. We have

$$G \cong \mathscr{H}_2 = \langle x, y \mid x^4 = y^4 = 1, x^y = x^3 \rangle.$$

Since $G/\langle x^2 y^2 \rangle \cong \mathrm{Q}_8$, we get $A_G \neq \langle x^2 y^2 \rangle \neq B_G$. Then one of subgroups A_G, B_G contains $G' = \langle a^2 \rangle$ so is G-invariant.

Exercise 5. If G is a two-generator WE_p-group, $p > 2$, of order $> p^3$ that satisfies $|G/G'| > p^2$, then G is metacyclic. (*Hint.* Use Exercise 1(c). This also follows from Exercise 1(a) (take in G' a G-invariant subgroup of index p).)

Note that if G is a 3-group of maximal class not isomorphic to $\Sigma_{3^2} \in \mathrm{Syl}_3(\mathrm{S}_{3^2})$, then all subgroups of G are two-generator (see Exercise 9.13).

Lemma 110.1 (compare with [BDM, §4, Example 4]). *A 3-group G of maximal class and order $> 3^4$ is a* WE_3*-group.*

Proof. We use induction on $|G|$. Write $Z = \mathrm{Z}(G)$. Assume that $G = HK$, where $H, K < G$ are not G-invariant. By the paragraph preceding the lemma, Exercises 9.13, 3 and induction, in the factorization $G/Z = (HZ/Z)(KZ/Z)$ one of the factors, say HZ/Z, is G-invariant; then $HZ \triangleleft G$. By assumption, $Z \not\leq H$ so that $HZ = H \times Z$. Since $H \not\leq \Phi(G)$, we get $H \times Z \in \Gamma_1$ (every normal subgroup of index $> p$ in a p-group X of maximal class is contained in $\Phi(X)$). All members of the set Γ_1, apart from the fundamental subgroup G_1, are of maximal class. It follows that $H \times Z = G_1$. Since G_1 is metacyclic, the subgroup H is cyclic. Then $\Phi(H) = \Phi(G_1)$, a cyclic subgroup of order > 3, is G-invariant, a final contradiction (see Exercise 9.1(c)).[2] □

It follows that if G is a 3-group of maximal class and order $3^m > 3^4$, then G is an E_3-group provided its fundamental subgroup G_1 is either abelian or m is even (see the remark after Exercise 5).[3] Indeed, our group G is an E_3-group if and only if G_1 is a WE_3-group since if G_1 is a WE_3-group, then every proper subgroup of G is also a WE_3-group so G is an E_3-group (if $H \in \Gamma_1 - \{G_1\}$, then H is of maximal class and $H \cap G_1$ is abelian).

Now we are ready to prove the following

Theorem 110.2 ([BDM, Theorem 4.1]). *Suppose that G is a nonabelian two-generator E_p-group of order $> p^3$ and $p > 2$. Then one of the following holds:*

(a) *G is metacyclic (see Exercise 5).*

(b) *G is a 3-group of maximal class (all such groups are described in Lemma 110.3 below).*

(c) *G is of maximal class and order p^4 without subgroup $\cong \mathrm{E}_{p^3}$; see Exercise 3.*

Proof. Suppose that G is neither metacyclic nor of maximal class. Then $|G| > p^4$ (Exercise 3). Next, by Exercise 3 and Theorem 9.11, $|G/\mho_1(G)| = p^3$. By Exercise 6, $|G/G'| = p^2$. From Theorem 36.16 and Corollary 44.9 it follows that $G/\mho^2(G)$ is neither metacyclic nor of maximal class, where $\mho^2(G) = \mho_1(\mho_1(G))$. Therefore one may assume that $\mho^2(G) = \{1\}$; then $\exp(G) = p^2$.

Let $R \leq \mho_1(G)$ be G-invariant of order p. Then, by induction, either G/R is of maximal class and order p^4 or a 3-group of maximal class and order $\geq 3^5$. In both cases, $\bar{G} = G/R$ has no subgroup $\cong \mathrm{E}_{p^3}$ so all its maximal subgroups are two-generator.

(i) Let $\bar{G}$ be of maximal class and order p^4. Then $\bar{G}$ has an abelian subgroup T/R of type (p^2, p) (Exercise 3). By Lemma 65.2(a), Exercises 1(a) and 5, T is abelian of type (p^2, p^2) or (p^2, p, p) since $\exp(G) = p^2$. Since $|G/G'| = p^2$, we get $|\mathrm{Z}(G)| =$

[2] Thus, if a p-group of maximal class and order $> p^4$ is a WE_p-group, then $p \in \{2, 3\}$; see Exercises 2, 4 and Lemma 110.3(b), below.

[3] However, we do not assert that if m is even, then G is an E_3-group; see Lemma 110.3.

$\frac{1}{p}|G/G'| = p$ so that $\mathrm{Z}(G) = R$, and we conclude that G is of maximal class. In the case under consideration, since $|G/\mathfrak{V}_1(G)| = p^3$, we get $p = 3$ (Theorem 9.5).

(ii) Let $\bar{G}$ be a 3-group of maximal class and order $\geq 3^5$ (recall that $\exp(G_0) = 3^2$). By Theorem 13.7, there is in G a normal subgroup $E \cong \mathrm{E}_{27}$. As G/R is also of maximal class, we conclude that $E = \mathfrak{V}_1(D)$, where D/R is the fundamental subgroup of the quotient group G/R. Let $H/E = \mathrm{Z}(G/E)$; then $H \lhd G$ is of order 3^4. Since $|H| = 3^4 > 3^3 = |E| = |\Omega_1(D)|$, it follows that $\exp(H) = 9$ so that $K = \mathfrak{V}_1(H)$ is G-invariant of order 3. By induction, G/K is of maximal class and of order 3^5 with normal subgroup E/K of order 3^3 and exponent 3, contrary to Theorem 9.6(c). □

Lemma 110.3 (see [BDM, Example 4]). *A 3-group G of maximal class and order $3^m > 3^4$ is an E_3-group if and only if its fundamental subgroup G_1 is either abelian or*

$$G_1 = \langle a, b \mid a^{3^{s+1}} = b^{3^s} = 1,\ a^b = a^{1+3^s} \rangle.$$

Proof. All subgroups of G are two-generator (see Exercise 9.13). By Lemma 110.1, G is a WE_3-group. If the fundamental subgroup G_1 of G is abelian, it is a WE_3-group. Then all proper subgroups of G which have (metacyclic) abelian fundamental subgroups are WE_3-groups. Thus G is an E_3-group if G_1 is a WE_3-group.

Assume that G_1 is nonabelian. Then G_1, as we know, is minimal nonabelian (this follows from Exercise 9.1(b) and Lemma 65.2(a)). As we know, G is an E_3-group of and only if G_1 is a WE_3-group (so an E_3-group). Next, by Exercise 5 and the remark following it, G_1 is not a WE_3-group if $m - 1$ is even; then m is odd. Now let $m = 2k$.

By Lemma 65.1 and Theorems 9.5 and 9.6, we have

$$G_1 = \langle a, b \mid a^{3^r} = b^{3^s} = 1,\ a^b = a^{1+3^{r-1}} \rangle, \quad |r-s| = 1,\ r+s = m-1 = 2k-1.$$

Since $\mathrm{E}_9 \cong \Omega_1(G_1) < G_1$, all noncyclic subgroups of G_1 are G_1-invariant.

Let $s = r + 1$. Then $G_1/\mathfrak{V}_r(G_1)$ is not a WE_3-group (Exercise 5 and the remark following it) so G_1 and G are not E_3-groups.

Now let $r = s + 1$. We claim that then G is a WE_3-group. Assume that this is false. Then $G = AB$, where A and B are nonnormal in G so A and B do not contain G' hence they have trivial intersections with $\langle a \rangle$. It follows that $|A| \leq p^s$, $|B| \leq p^s$ so that $|G| = |AB| \leq p^{2s} < p^{r+s} = |G|$, a contradiction. Thus, in the case under consideration, G is a WE_3-group. □

Exercise 6. Let G be an extraspecial group of order p^{2m+1}, $m > 1$.

(a) Prove that G is a WE_p-group.

(b) If, in addition, $\exp(G) = p$, then G is not an E_p-group.

(c) If $m > 2$ and $p > 2$, then G is not an E_p-group.

Solution. (a) Assume that $G = AB$, where $A, B < G$ are not G-invariant. Then we have $G' \not\leq A, B$ so A, B are abelian of orders $\leq p^m$ (see §4). By the product formula, $|AB| < p^{2m+1} = |G|$, a contradiction.

(b) It suffices to assume that $m = 2$. We have $G = D * D_1$, where D and D_1 are nonabelian of order p^3. Let $L < D_1$ be of order p such that $L \neq G'$. Set $H = D \times L$. It suffices to show that H is not an E_3-group. Let $L_1 < D$ of order p be such that $L_1 \neq G'$ and set $A = L \times L_1$. Then $A \cong E_{p^2}$ is not normal in H since $D \cap A = L$ is not normal in D. Let $L_2 < Z(H)$ of order p be such that $L_2 \notin \{L, G'\}$ and let $L_3 < D$ of order p be such that $L_3 \notin \{L_1, G'\}$. Set $B = L_2 \times L_3$. Then B is not normal in H since $B \cap D = L_2$ is not normal in D. Since $A \cap B = \{1\}$, we get $H = AB$ is not a WE_p-group so G is not an E_p-group.

(c) Let $G = D_1 * \cdots * D_{m-1} * D_m$, where $D_1, \ldots, D_{m-1}$ are nonabelian of order p^3 and exponent p. Then $D_1 * D_2$ is not an E_p-group by (b) so that G is not an E_p-group.

Exercise 7. Prove that the metacyclic p-group $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}}, n \geq m \rangle$, $p > 2$, is not a WE_p-group. (*Hint.* See the last paragraph of the proof of Lemma 110.3.)

Exercise 8. Let $G = \langle a, b \mid a^{p^r} = b^{p^s} = 1, a^b = a^{1+p^{r-1}} \rangle$, $p > 2$, $r + s > 4$. Then G is a WE_p-group if and only if $s < r$.

Solution. Using the argument in the proof of Theorem 110.3, which is also applied to minimal nonabelian metacyclic p-groups with $p > 3$, we have to prove that if $s < r$, then G is a WE_p-group. Assume that this is false. Then $G = AB$, where A and B are not G-invariant. Since $G' < \Omega_1(G)$, we get $|\Omega_1(A)| = |\Omega_1(B)| = p$ so A and B are cyclic and $A \cap \langle a \rangle = \{1\} = B \cap \langle a \rangle$. It follows that $|A| \leq p^s$, $|B| \leq p^s$ so that $|G| \leq |A||B| \leq p^{2s} < p^{r+s} = |G|$, a contradiction. Thus G is a WE_p-group if and only if $s < r$.

Exercise 9. Let a WE-group G be nonnilpotent and solvable. Then we have $G = D \cdot P$, a semidirect product, where $P \in \mathrm{Syl}_p(G)$ for some prime p is G-invariant and D is Dedekindian.

Solution. Let $H < G$ be a maximal nonnormal subgroup of G; then $|G : H| = p^a$ for some prime p. Let $P \in \mathrm{Syl}_p(G)$. Since $G = HP$ and H is not G-invariant, we get $P \lhd G$. Let $F/P < G/P$. Since $G = HP \geq HF$, we obtain $G = HF$ so $F \lhd G$. It follows that G/P is Dedekindian. It remains to apply Hall's Theorem A.28.4 on solvable groups.

Exercise 10. Let a nonabelian WE_p-group $G = AB$ be such that $|G/G'| = p^2$ and $A \lhd G$, $B < G$. Prove that $|G : A| = p$.

Solution. If $|G : A| > p$, then $A \leq G' = \Phi(G)$ so $G = AB = B$, a contradiction.

Exercise 11. Let a nonabelian two-generator WE_p-group $G = AB$, where $A \lhd G$ and $B < G$. Prove that G/A is cyclic. (*Hint.* If G/A is noncyclic, then $A \leq \Phi(G)$.)

Exercise 12. Let a nonabelian two-generator non-WE_p-group $G = AB$, where A and B are maximal nonnormal subgroups of G. Then G/A^G and G/B^G are cyclic. (*Hint.* If G/A^G is noncyclic, then $A < A^G \leq \Phi(G)$.)

Exercise 13. Let G be a 2-group such that $G/\Omega_1(G) \cong \mathrm{Q}_8$. Is it true that G is not a WE_2-group? (*Hint.* See Lemma 42.1(c) about the structure of G. By that lemma, G is metacyclic.)

Exercise 14. Suppose that G is a metacyclic p-group. Then one of the following holds:

(a) $|G| = p^3$.

(b) G is a 2-group of maximal class.

(c) G has a subgroup isomorphic to M_{p^n}, $n > 3$.

(d) $\Omega_1(G) \le \mathrm{Z}(G)$.

Solution. Suppose that (a), (b) and (c) do not hold; then G is non-Dedekindian and $\Omega_1(G) \cong \mathrm{E}_{p^2}$. Let $A \le G$ be minimal nonabelian. If $|A| = p^3$, then either $p = 2$ and G is of maximal class or $G = A$ (Proposition 10.19), contrary to the assumption. It follows that $\Omega_1(A) \le \mathrm{Z}(A)$ (Lemma 65.1). Since all such A generate G (Theorem 10.28) and $\Omega_1(A) = \Omega_1(G)$, we conclude that $\Omega_1(G) \le \mathrm{Z}(G)$, i.e., (d) holds.

Lemma 110.4 ([BDM, Theorem 4.2]). *Let G be a metacyclic p-group, $p > 2$, let $\langle a\rangle = M \lhd G$ and $G/M = \langle bM\rangle$. Then $G = \langle b\rangle\langle ba\rangle$.*

Proof. One has $G = \langle a, b\rangle$. Suppose that $a^b = a^k$; then we get $k \equiv 1 \pmod p$ since $o(b)$ is a power of p and $p \mid (k^{o(b)} - 1)$. Let us show that $\langle b\rangle\langle ba\rangle = \langle ba\rangle\langle b\rangle$. We have

$$b^\alpha (ba)^\beta = b^{\alpha+\beta} a^{b^{\beta-1}} \dots a^b a = b^{\alpha+\beta} a^{1+k+\dots+k^{\beta-1}}.$$

Thus we must show that every integer can be expressed modulo $p^n = o(a)$ in the form $1 + k + \dots + k^{\beta-1}$. If this is not so, there exist integers β, γ with $0 \le \beta < \gamma < p^n$ such that

$$1 + k + \dots + k^{\beta-1} = 1 + k + \dots + k^{\gamma-1} \pmod{p^n}.$$

Hence, since p does not divide k, we get

$$1 + k + \dots + k^{\gamma-\beta-1} \equiv 0 \pmod{p^n}, \tag{1}$$

and $0 < \gamma - \beta < p^n$. It follows that $k \not\equiv 1 \pmod{p^n}$. But $k \equiv 1 \pmod p$; thus, if $k = 1 + p^m s$ with $\mathrm{GCD}(s, p) = 1$, then $1 \le m < n$. It follows from (1) that

$$\frac{k^{\gamma-\beta} - 1}{k - 1} = \frac{k^{\gamma-\beta} - 1}{sp^m} \equiv 0 \pmod{p^n}$$

so $k^{\gamma-\beta} \equiv 1 \pmod{p^{m+n}}$. We have

$$k^{\gamma-\beta} = (1 + sp^m)^{\gamma-\beta} = 1 + (\gamma - \beta)sp^m + Cp^{m+n}, \tag{2}$$

where C is a positive integer. By (2), we obtain that $p^n \mid (\gamma - \beta)$ so $\gamma - \beta \ge p^n$, a contradiction. □

Theorem 110.5 ([BDM, Theorem 4.2]). *Let G be a metacyclic* WE_p*-group, $p > 2$. Then* $\mathrm{cl}(G) \leq 2$.

Proof. We retain the same meaning for M, a and b as in the statement of Lemma 110.4. Since $G = \langle b\rangle\langle ba\rangle$ is a WE_p-group, either $\langle b\rangle \lhd G$ or $\langle ba\rangle \lhd G$; hence $[b, a]$, a generator of G', is contained either in $\langle b\rangle$ or $\langle ba\rangle$. But also $[b, a] \in M = \langle a\rangle$. It follows that $[b, a]$ commutes with b and a hence $[b, a]$ commutes with $\langle b, a\rangle = G$, and we conclude that $G' = \langle [b, a]\rangle \leq \mathrm{Z}(G)$. □

Exercise 15 ([BDM, Lemma 4.3(a)]). Suppose that a nonabelian E_p-group G has exponent p. Then $|G| = p^3$.

Solution. By hypothesis, $p > 2$. Assume that $|G| = p^4$. Then G contains an abelian subgroup A of index p so, by Exercise 3, $\mathrm{cl}(G) = 2$. By Lemma 65.1, G is not minimal nonabelian. Therefore it follows from Proposition 10.17 that $G = D \times L$, where $L \leq \mathrm{Z}(G)$ is of order p. As in the solution of Exercise 6(b), G is not a WE_p-group. Now let $|G| > p^4$. Since G is not minimal nonabelian (Lemma 65.1), it contains a nonabelian subgroup H of order p^4. By what has just been proved, the subgroup H is not a WE_p-group so G is not an E_p-group. Thus $|G| = p^3$.

Exercise 16. Let G be an E_p-group of order $> p^4$, $p > 2$, containing a nonabelian subgroup A of order p^3 and exponent p. Prove that one of the following holds:

(a) $\Omega_1(G) = A$ and $G = AC$, where C is cyclic.

(b) G is a 3-group of maximal class.

Solution. Assume that G has a normal subgroup $U \cong \mathrm{E}_{p^3}$. Let $U_1 < U$ be a G-invariant subgroup which is as small as possible and such that $U_1 \not\leq A$. Set $H = AU_1$. If $A \cap U_1 = \{1\}$, then $|U_1| = p$ and $H = A \times U_1$ is not a WE_p-group (see solution of Exercise 6(b)). Thus $A \cap U_1 > \{1\}$. Moreover, all minimal normal subgroups of G contained in U are contained in A. It follows that $|H| = p^4$. Assume that $U_1 = U$. Then H is not of maximal class (Exercise 3) so, by Proposition 10.17, $\mathrm{C}_H(A) \not\leq A$. Since $\Omega_1(H) = H$, we get $H = A \times C$ for some C of order p, and then H is not a WE_p-group. Thus $|U_1| = p^2$ and $U_1 \not\leq \mathrm{Z}(H)$ (otherwise, A is a direct factor of H). In this case, we have $\mathrm{C}_H(U_1) \cong \mathrm{E}_{p^3}$. Then, by Exercise 3, H is not of maximal class so $\mathrm{cl}(H) = 2$, and we conclude that $\exp(H) = p$ since $p > 2$. Then $H = A \times C$ again, a contradiction. Thus U does not exist and the result now follows from Theorem 13.7.

Theorem 110.6 ([BDM, Lemma 4.3(c)]). *If an* E_p*-group G contains a proper subgroup H of maximal class and order $> p^3$, $p > 2$, then $p = 3$ and G is of maximal class.*

Proof. Assume that G is not of maximal class. By Theorems 9.5 and 9.6, one may assume that $|H| = p^4$ (indeed, H contains a subgroup of maximal class and order p^4); then $\exp(H) = p^2$ and H has no subgroup $\cong \mathrm{E}_{p^3}$ (Exercise 3). Theorem 13.7 yields

that either H is a 3-group of maximal class or $H = C\Omega_1(H)$, where C is cyclic of order p^2 and $\Omega_1(H)$ is nonabelian of order p^3 and exponent p. By Exercise 16, the second case is impossible since a group from Exercise 16(a) has no such a subgroup as H (it is important that $|G| > p^4$). Thus H is of maximal class and order 3^4. Again H has no subgroups of order 3^3 and exponent 3. Indeed, if H has a nonabelian subgroup A of order 3^3 and exponent 3, then, by Exercise 16, $G = AC$, where $A = \Omega_1(G)$ and C is cyclic of order $> 3^2$. Such a G, however, has no subgroup of maximal class and order 3^4. By Exercise 13.10(a), we have $H < M \leq G$, where $|M : H| = p$ and M is not of maximal class. One may assume without loss of generality that $G = M$; then $G/G' \cong \mathrm{E}_{3^3}$ (Theorem 12.12(a)). By Theorem 12.12(b), $\bar{G} = G/\mathrm{K}_3(G)$ is of order 3^4 and exponent 3 since $|G| > 3^4$. As above, $\bar{G} = \bar{S} \times \bar{C}$, where $\bar{S}$ is nonabelian of order 3^3 and $|\bar{C}| = 3$. As we know, such a $\bar{G}$ is not an E_3-group, a contradiction. Thus G is a 3-group of maximal class. □

For further details on E_p-groups, see [BDM] and [Sil].

In view of Theorem 110.2, the classification of E_p-groups, $p > 2$, will follow from the solution of the following

Problem 1. Classify the p-groups all of whose nonabelian two-generator subgroups are either metacyclic or of maximal class.

Problem 2. Classify the metacyclic WE_p-groups.

§111

Characterization of abelian and minimal nonabelian groups

If G is abelian, then $G' = \Phi(G)'$ and it appears that this property characterizes abelian groups (Theorem 111.1). If G is either abelian or minimal nonabelian, then $H' = \Phi(G)'$ for all $H \in \Gamma_1$, where Γ_1 is the set of all maximal subgroups of G, and Theorem 111.3 shows that this property is characteristic for groups all of whose maximal subgroups are abelian.

In this section we consider also nonnilpotent groups. In Lemma J we collect some known results cited in what follows.

Lemma J. *Let G be a finite group.*

(a) (R. Baer [Bae6]) *If $P \in \mathrm{Syl}(G)$ is G-invariant, then $\Phi(P) = P \cap \Phi(G)$.*

(b) (Redei; see Exercise 1.8(a)) *If G is a nilpotent minimal nonabelian group, then G is a p-group, $|G'| = p$, $\mathrm{Z}(G) = \Phi(G)$ is of index p^2 in G and one of the following holds:*

  (i) *$p = 2$ and G is the ordinary quaternion group,*

  (ii) *$G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}}, m > 1\rangle$ is metacyclic of order p^{m+n},*

  (iii) *$G = \langle a, b \mid a^{p^m} = b^{p^n} = c^p = 1, c = [a, b], [a, c] = [b, c] = 1\rangle$ is nonmetacyclic of order p^{m+n+1}. In particular, if $\exp(G) = p$, then $p > 2$ and $|G| = p^3$.*

(c) (Miller–Moreno; see Lemma 10.8) *If G is a nonnilpotent minimal nonabelian group, then we have $|G| = p^a q^b$, $G = P \cdot Q$, where $P \in \mathrm{Syl}_p(G)$ is cyclic, $Q = G' \in \mathrm{Syl}_q(G)$ is a minimal normal subgroup of G, $\mathrm{Z}(G) = \Phi(G)$ has index p in P.*

(d) (Wielandt) *A group G is nilpotent if and only if $G' \leq \Phi(G)$ (or, what is the same, $G/\Phi(G)$ is nilpotent).*

(e) *If G is nilpotent and noncyclic, then G/G' is also noncyclic.*

(f) [Gas1] *If a Sylow p-subgroup is normal in $G/\Phi(G)$, then a Sylow p-subgroup is normal in G. If H is normal in G, then $\Phi(H) \leq \Phi(G)$.*

(g) *$\pi(G/\Phi(G)) = \pi(G)$, where $\pi(G)$ is the set of prime divisors of $|G|$.*

(h) [BG] *If* $\mathrm{N}_F(F \cap H) \neq F \cap H \neq \mathrm{N}_H(F \cap H)$ *for any two distinct* $F, H \in \Gamma_1$, *then either* G *is nilpotent or* $G/\Phi(G)$ *is (nonnilpotent) minimal nonabelian. The converse assertion is also true.*

(i) *If* G *is a nonabelian* p*-group such that* $G' \leq \mathrm{Z}(G)$ *has exponent* p, *then we have* $\Phi(G) \leq \mathrm{Z}(G)$.

(j) (Fitting; see Corollary 6.5) *Let* Q *be a normal abelian Sylow* q*-subgroup of a group* G. *Then* $Q \cap \mathrm{Z}(G)$ *is a direct factor of* G.

Let us prove Lemma J(a). Since $\Phi(P) \leq D = \Phi(G) \cap P$ (Lemma J(f)), it suffices to prove the reverse containment. To this end, one may assume that $\Phi(P) = \{1\}$; then P is elementary abelian. We have to show that $p \notin \pi(\Phi(G))$. Let H be a p'-Hall subgroup of G. Then $P = D \times L$, where L is H-admissible (Maschke). In this case, $G = HP = (HL) \cdot D$, a semidirect product with kernel D, so $D = \{1\}$ since $D \leq \Phi(G)$. Thus, in general case, $\Phi(P) = D$.

Let us prove Lemma J(i). Take $x, y \in G$. Since $\mathrm{cl}(G) = 2$, we have $1 = [x, y]^p = [x, y^p]$ so that $\mathfrak{V}_1(G) \leq \mathrm{Z}(G)$, and we obtain $\Phi(G) = G'\mathfrak{V}_1(G) \leq \mathrm{Z}(G)$.

Let Γ_1 (Γ_1^n) be the set of maximal (nonnormal maximal) subgroups of a group G. If G is not nilpotent, then the set Γ_1^n is not empty (Lemma J(d)).

Theorem 111.1. *The following conditions for a group* G *are equivalent:*

(a) $G' = \Phi(G)'$.

(b) G *is abelian.*

Proof. As we have noticed, (b) $\Rightarrow$ (a) so it remains to prove the reverse implication. We have $G' = \Phi(G)' \leq \Phi(G)$ so G is nilpotent (Lemma J(d)); then $G = P_1 \times \cdots \times P_k$, where $P_1, \ldots, P_k$ are Sylow subgroups of G. We have

$$\Phi(G) = \Phi(P_1) \times \cdots \times \Phi(P_k), \tag{1}$$

$$G' = P_1' \times \cdots \times P_k', \tag{2}$$

$$\Phi(G)' = \Phi(P_1)' \times \cdots \times \Phi(P_k)'. \tag{3}$$

Equality (1) follows from Lemma J(a), and (2), (3) are known properties of direct products. Since $\Phi(G)' = G'$, it follows from (2) and (3) that $\Phi(P_i)' = P_i'$ so P_i satisfies the hypothesis for $i = 1, \ldots, k$. To complete the proof, it suffices to show that P_i is abelian for $i = 1, \ldots, k$ so one may assume that $k = 1$, i.e., G is a p-group. Assume that G is nonabelian of the least possible order. We get $\Phi(G)' = G' > \{1\}$ so that $\Phi(G)$ is nonabelian. Let $R < \Phi(G)'$ be G-invariant of index p. Since $R < \Phi(G)' = G' < \Phi(G)$, we get

$$\Phi(G/R)' = (\Phi(G)/R)' = \Phi(G)'/R = G'/R = (G/R)'$$

whence the nonabelian group G/R satisfies the hypothesis so we must have $R = \{1\}$ by induction. In that case, we get $|\Phi(G)'| = |G'| = p$ so $G' \leq \mathrm{Z}(G)$. By Lemma J(i), $\Phi(G) \leq \mathrm{Z}(G)$ so that $\Phi(G)$ is abelian, contrary to what has been said above. □

Lemma 111.2. *Let G be a noncyclic p-group and $D = \langle \Phi(H) \mid H \in \Gamma_1 \rangle$. Then $D \leq \Phi(G)$ and $|\Phi(G) : D| \leq p$ with equality only for $p > 2$.*

Proof. Since all members of the set Γ_1 are G-invariant, we have $D \leq \Phi(G)$ (Lemma J(f)). As all maximal subgroups of the quotient group G/D are elementary abelian, G/D is either elementary abelian or nonabelian of order p^3 and exponent p (Lemma J(d)). In the first case, $D = \Phi(G)$; in the second case, $p > 2$ and $|\Phi(G) : D| = |\Phi(G/D)| = p$. Thus, in both cases, $|\Phi(G) : D| \leq p$, as desired. □

If $H \in \Gamma_1$, then $\Phi(G) < H$ so $\Phi(G)' \leq H'$. Below we consider the extreme case when $\Phi(G)' = H'$ for all $H \in \Gamma_1$.

Theorem 111.3. *The following assertions for a group G are equivalent:*

(a) $\Phi(G)' = H'$ *for all* $H \in \Gamma_1$.

(b) *G is either abelian or minimal nonabelian.*

Proof. Obviously, groups all of whose maximal subgroups are abelian satisfy condition (a) hence implication (b) $\Rightarrow$ (a) is true. Therefore it remains to prove the reverse implication. In what follows one may assume that G is nonabelian.

(i) Suppose that G is a nonabelian p-group satisfying condition (a). Note that $\Phi(G)$, $\Phi(G)'$ and H' are G-invariant for all $H \in \Gamma_1$. If $\Phi(G)$ is abelian, then all maximal subgroups of G are also abelian by hypothesis, and G is minimal nonabelian so (b) holds. Next we assume that $\Phi(G)' > \{1\}$. Let $R < \Phi(G)'$ be G-invariant of index p and set $\bar{G} = G/R$; then $\Phi(\bar{G})$ is nonabelian and $|\Phi(\bar{G})'| = p$. Take $H \in \Gamma_1$. We have

$$\Phi(\bar{G})' = \Phi(G/R)' = (\Phi(G)/R)' = \Phi(G)'/R = H'/R = \bar{H}' \tag{4}$$

is of order p so, by Lemma J(i), $\Phi(\bar{H}) \leq \mathrm{Z}(\bar{H})$ and hence $\Phi(\bar{H}) \leq \mathrm{Z}(\Phi(\bar{G}))$ since $\Phi(\bar{H}) \leq \Phi(\bar{G}) \leq \bar{H}$. Setting $\bar{D} = \langle \Phi(\bar{H}) \mid H \in \Gamma_1 \rangle$, we conclude $\bar{D} \leq \mathrm{Z}(\Phi(\bar{G}))$ so $\Phi(\bar{G})$ is abelian since $|\Phi(\bar{G}) : \bar{D}| \leq p$ by Lemma 111.2, contrary to what has already been said. Thus, if G is a p-group, then (a) $\Rightarrow$ (b).

In what follows we assume that G is not a prime-power group. Write $T = \Phi(G)'$; then $T = H'$ for all $H \in \Gamma_1$ by hypothesis. Therefore all maximal subgroups of G/T are abelian so the quotient group G/T is either abelian or minimal nonabelian. As in (i), one may assume that $\Phi(G)$ is nonabelian.

(ii) Suppose that G is nilpotent; then $G = P_1 \times \cdots \times P_k$, where $P_i \in \mathrm{Syl}_{p_i}(G)$, $i = 1, \ldots, k$, $k > 1$. It follows from (2) and (3) which are true for any nilpotent group that $\Phi(P_i)' = H_i'$ for all maximal subgroups H_i of P_i so P_i is either abelian or minimal nonabelian by (i). Then $\Phi(P_i)$ is abelian for all i so $\Phi(G)$ is abelian in view of (1), contrary to the assumption. Thus the theorem is true provided G is nilpotent.

Next we assume that G is not nilpotent. In this case, by Lemma J(d), G/T is nonnilpotent (and minimal nonabelian).

(iii) It remains to consider the case where G/T is minimal nonabelian and nonnilpotent. It follows from the structure of G/T (Lemma J(c)) that $\Phi(G/T) = \Phi(G)/T$ is

cyclic. Remembering that $\Phi(G)$ is nilpotent and $T = \Phi(G)'$, we conclude that $\Phi(G)$ is cyclic (Lemma J(e)) so abelian, a final contradiction. □

Corollary 111.4. *Suppose that a group G is neither abelian nor minimal nonabelian. Then there exists a nonabelian $H \in \Gamma_1$ such that $\Phi(G)' < H'$.*

Proof. We have $\Phi(G)' \leq H'$ for all $H \in \Gamma_1$. Assume that $\Phi(G)' = H'$ for all nonabelian $H \in \Gamma_1$; then $\Phi(G)$ is nonabelian (take a nonabelian $H \in \Gamma_1$) so the set Γ_1 has no abelian members. In that case, $\Phi(G)' = H'$ for *all* $H \in \Gamma_1$ by hypothesis, so that G is minimal nonabelian (Theorem 111.3), contrary to the hypothesis. □

We claim that the following conditions for a group G are equivalent:

(a) $H' \leq \Phi(G)$ for all $H \in \Gamma_1$,

(b) either G is nilpotent or $G/\Phi(G)$ is nonnilpotent minimal nonabelian,

(c) $\mathrm{N}_F(F \cap H) \neq F \cap H \neq \mathrm{N}_H(H \cap F)$ for all distinct $F, H \in \Gamma_1$.

Obviously, (a) $\Leftrightarrow$ (b) and (b) $\Rightarrow$ (c). Next, (b) follows from (c) by Lemma J(h).

Below we use some known results on Frobenius groups (see [BZ, §10.2]). Recall that G is said to be a *Frobenius group* if there is a subgroup $H < G$, $H > \{1\}$, such that $H \cap H^x = \{1\}$ for all $x \in G - H$. In that case, $G = H \cdot N$ is a semidirect product with kernel N, Sylow subgroups of H are either cyclic or generalized quaternion.

Lemma 111.5. *The following conditions for a nonnilpotent group G are equivalent:*

(a) *All members of the set Γ_1^n are abelian.*

(b) *$G/\mathrm{Z}(G) = (U/\mathrm{Z}(G)) \cdot (Q_1/\mathrm{Z}(G))$ is a Frobenius group with elementary abelian kernel $Q_1/\mathrm{Z}(G) = (G/\mathrm{Z}(G))'$ and a cyclic complement $U/\mathrm{Z}(G)$, $U \in \Gamma_1$.*

Proof. If U, V are two distinct abelian maximal subgroups of a nonabelian group G, then $U \cap V = \mathrm{Z}(G)$. As we have noticed, the set Γ_1^n is nonempty.

Suppose that G satisfies condition (a). Given $H \in \Gamma_1^n$, set $H_G = \bigcap_{x \in G} H^x$; then $H_G = \mathrm{Z}(G)$ by the previous paragraph. Set $\bar{G} = G/\mathrm{Z}(G)$; then $\bar{G} = \bar{H} \cdot \bar{Q}_1$ is a Frobenius group with kernel $\bar{Q}_1$ and complement $\bar{H}$. Since $\bar{H}$ is abelian, it is cyclic. There is in $\bar{Q}_1$ an $\bar{H}$-invariant Sylow subgroup by Sylow's theorem. Therefore, since $\bar{H}$ is maximal in $\bar{G}$, the subgroup $\bar{Q}_1$ is a p-group; moreover, $\bar{Q}_1$ is a minimal normal subgroup of $\bar{G}$ so it is elementary abelian. All nonnormal maximal subgroups of $\bar{G}$ are conjugate with $\bar{H}$ (Schur–Zassenhaus) so all members of the set Γ_1^n are conjugate in G (indeed, all members of the set Γ_1^n, being abelian, contain $\mathrm{Z}(G)$). Thus (a) $\Rightarrow$ (b).

Conversely, every group as in (b) satisfies condition (a). In fact, if $H \in \Gamma_1^n$, then $\mathrm{Z}(G) < H$. By (b), $H/\mathrm{Z}(G)$ is cyclic so H is abelian. □

The proof of Lemma 111.5 shows that if the set Γ_1^n has at least one abelian member, then the group G has the same structure as in Lemma 111.5(b).

Corollary 111.6. *A nonnilpotent group G satisfies $\Phi(G)' = H'$ for all $H \in \Gamma_1^n$ if and only if $\bar{G} = G/\Phi(G)'$ is as in Lemma 111.5*(b).

Proof. Suppose $\bar{G} = G/\Phi(G)'$ is as in Lemma 111.5(b) and $\bar{H}$ is a nonnormal maximal subgroup of $\bar{G}$; then $\bar{H}$ is cyclic by hypothesis, so $H' \leq \Phi(G)'$. As $\Phi(G) < H$, we get $\Phi(G)' \leq H'$ so $H' = \Phi(G)'$ and whence G satisfies the hypothesis.

Now suppose that $\Phi(G)' = H'$ for all $H \in \Gamma_1^n$. Then all nonnormal maximal subgroups of $G/\Phi(G)'$ are abelian so $G/\Phi(G)'$ is as in Lemma 111.5(b). □

Proposition 111.7. *Suppose that a nonnilpotent group G is not minimal nonabelian and such that $M' = \Phi(G)$ for all nonabelian $M \in \Gamma_1$. Then*

(a) *$G = P \cdot Q$ is a semidirect product with kernel $Q = G' \in \mathrm{Syl}_q(G)$, $P \in \mathrm{Syl}_p(G)$ is of order p, $\Phi(G) = \Phi(Q) > \{1\}$. Set $H = P\Phi(G)$. The set Γ_1 consists of two conjugacy classes of subgroups with representatives H and Q.*

(b) *$P^G = G$, where P^G is the normal closure of P in G.*

(c) *$G/\Phi(G)$ is minimal nonabelian so that $Q/\Phi(G)$ is a minimal normal subgroup of $G/\Phi(G)$.*

(d) *$H' < \Phi(G)$ if and only if G is minimal nonnilpotent.*

(e) *If $\Phi(G)$ is abelian, then G is either minimal nonnilpotent or a Frobenius group.*

Proof. By hypothesis, all maximal subgroups of $G/\Phi(G)$ are abelian so it is nonnilpotent and minimal nonabelian by Lemma J(d,c). We obtain that $\Phi(G/\Phi(G)) = \{1\}$ so that $|G/\Phi(G)| = pq^b$, where a subgroup of order p is not normal in $G/\Phi(G)$ (Lemma J(b,c)). By hypothesis, the set Γ_1 has a nonabelian member so $\Phi(G) > \{1\}$. Lemma J(g) yields $\pi(G) = \pi(G/\Phi(G)) = \{p, q\}$. Due to Lemma J(f), $Q \in \mathrm{Syl}_q(G)$ is normal in G. We have $G = P \cdot Q$, where $P \in \mathrm{Syl}_p(G)$. From Lemma J(a) we deduce $\Phi(Q) = Q \cap \Phi(G)$. By the above, $\Phi(G) = P_1 \times \Phi(Q)$, where P_1 is a maximal subgroup of P. The subgroup $H = P\Phi(Q) \in \Gamma_1$ and all nonnormal maximal subgroups of G are conjugate with H. Since P_1Q/Q is the unique normal maximal subgroup of G/Q, it follows that $G/Q \cong P$ is cyclic.

Let, as above, $P_1 < P$ be maximal; then, as we have noticed, $P_1 \leq \Phi(G)$. The subgroup $P_1Q = P_1 \times Q = M \in \Gamma_1$. Assume that $P_1 > \{1\}$ and M is nonabelian. We have $P_1 \not\leq M' = \Phi(G)$, a contradiction. Thus, if $P_1 > \{1\}$, then M is abelian. Similarly, $P_1 \not\leq (P\Phi(G))' = H'$ so that H is also abelian. It follows that G is minimal nonabelian, contrary to the hypothesis. Thus we get $P_1 = \{1\}$ so that $|P| = p$ and $Q \in \Gamma_1$. This completes the proof of (a). By Lemma J(a), $\Phi(G) = \Phi(Q)$.

Assume that there is $L \lhd G$ of index q. Since $L \in \Gamma_1$, we get $\Phi(G) < L$, and this is a contradiction since $G/\Phi(G)$ has no normal subgroup of index q. It follows that $P^G = G$, and the proof of (b) is complete.

Suppose that $H' < \Phi(G)$. Then H is abelian by hypothesis. In this case, we have $\mathrm{C}_G(\Phi(G)) \geq H^G \geq P^G = G$ so that $\Phi(G) = \mathrm{Z}(G)$ since $\mathrm{Z}(G/\Phi(G)) = \{1\}$, and we conclude that G is minimal nonnilpotent since $G/\Phi(G)$ is minimal nonabelian. The proof of (d) is complete.

Assume that $\Phi(Q)(= \Phi(G))$ is abelian and G is not minimal nonnilpotent. Then, by (d), $H = P\Phi(Q)$ is nonabelian so $H' = \Phi(Q)$ by hypothesis. In this case, due to

Lemma J(j), $\mathrm{N}_H(P) = P$ so that H is a Frobenius group as $|P| = p$. Since $G/\Phi(Q)$ is a Frobenius group, it follows that G is also a Frobenius group (in the case under consideration, $p > 2$, by Burnside). This completes the proof of (e) and, thereby, of the proposition. □

Let a nonabelian group G be such that $H' = \Phi(H)$ for all nonabelian $H \leq G$. Then G has no minimal nonnilpotent subgroups by Lemma J(d). It follows that the group G is nilpotent. Let $A \leq G$ be minimal nonabelian. Then A is a p-subgroup for some prime p and $A' = \Phi(A)$ has order p and index p^2 in A (Lemma J(b)) so that $|A| = |A'|p^2 = p^3$. Thus all minimal nonabelian subgroups of G have order equal to the cube of a prime. Suppose that $P \in \mathrm{Syl}_2(G)$ is nonabelian. Then P is among 2-groups described in §90. Now suppose that $G = Q \times H$, where $Q \in \mathrm{Syl}_q(G)$ is nonabelian and $H > \{1\}$. Assume that $Z \leq H$ is cyclic of order p^2. Then $K = Q \times Z$ does not satisfy the hypothesis since $\Phi(K) \not\leq K'$. Thus either G is a prime power or $G = Q \times H$, where $Q \in \mathrm{Syl}_q(G)$ is nonabelian and $\exp(H) > 1$ is square free. It follows that if H is also nonabelian, then $\exp(Q) = q$ and we conclude that $q > 2$. □

Problems

Problem 1. Study the nonabelian p-groups G of exponent $> p$ all of whose subgroups $H \leq G$ satisfy $\mathfrak{V}_1(\Phi(H)) = \mathfrak{V}_1(H)$. (Obviously, we must have $p > 2$ since for any 2-group X we have $\Phi(X) = \mathfrak{V}_1(X)$.)

Problem 2. Classify the p-groups G satisfying $H' = \Phi(G)'$ for all those $H \leq G$ that are neither abelian nor minimal nonabelian.

Problem 3. Study the p-groups G which satisfy $H' = \Phi(G)'$ for all $H \in \Gamma_i$, where $i \in \{1, \ldots, \mathrm{d}(G) - 1\}$ is fixed. (For $i = 1$, see Theorem 111.3.)

§112

Non-Dedekindian p-groups all of whose nonnormal subgroups have the same order

In this section we classify the groups G with the title property. If a subgroup $H < G$ is nonnormal, it is cyclic since it is not generated by its (G-invariant) maximal subgroups. The p-groups all of whose nonnormal subgroups are cyclic are classified in Theorem 16.2. Therefore Theorems 112.3 and 112.4 are partial cases of Theorem 16.2. However, our proofs of the theorems are essentially shorter and not so involved. Moreover, our approach is entirely different. Therefore we decided to present the proofs of Theorems 112.3 and 112.4. We also classify the nonnilpotent groups with the title property.

Theorem 112.3 was proved by D. Passman [Pas], and Theorem 112.4 was also proved by G. Zappa [Zap] (his proof is essentially longer).

If G is a non-Dedekindian minimal nonabelian p-group, then (see Exercise 1.8(a) or Lemma 65.1) $G = \langle a, b\rangle$, where

(MA1) $a^{p^m} = b^{p^n} = c^p = 1$, $[a,b] = c$, $[a,c] = [b,c] = 1$, $|G| = p^{m+n+1}$, $G = \langle b\rangle \cdot (\langle a\rangle \times \langle c\rangle) = \langle a\rangle \cdot (\langle b\rangle \times \langle c\rangle)$ is nonmetacyclic.

(MA2) $a^{p^m} = b^{p^n} = 1$, $a^b = a^{1+p^{m-1}}$, $|G| = p^{m+n}$ and $G = \langle b\rangle \cdot \langle a\rangle$ is metacyclic.

If a minimal nonabelian p-group is Dedekindian, then it is isomorphic to Q_8.

If G is a nonnilpotent minimal nonabelian group, then (Miller–Moreno [MM])

(MNA) $G = P \cdot Q$, where $P \in \mathrm{Syl}_p(G)$ is cyclic, $G' = Q \in \mathrm{Syl}_q(G)$ is an elementary abelian minimal normal subgroups (p, q are distinct primes), $\mathrm{Z}(G) = \mho_1(P)$, $|Q| = q^b$, where b is a minimal positive integer such that $p \mid q^b - 1$ hence b is the order of q modulo p.

The group from (MNA) is said to be an $\mathrm{A}(p,q)$-*group*.

Below we freely use the following fact. The diagonal subgroup X of the direct product $G = A \times B$ of two isomorphic nonabelian groups A and B is not G-invariant. Indeed, assume that this is false; then $A \cap X = B \cap X = \{1\}$ so $\mathrm{C}_G(X) \geq AB = G$ and $X \in \mathrm{Z}(G)$ is abelian, a contradiction since $X \cong A$ and A is nonabelian.

The following lemma may be useful in proofs of such results as Theorems 112.2 and 112.4. For its proof, see Lemma 96.1.

Lemma 112.1 (= Lemma 96.1). *Let $G = \langle a, b\rangle$ be a minimal nonabelian p-group as in* (MA1) *or* (MA2).

(a) *All nonnormal cyclic subgroups of G have the same order if and only if one of the following holds:*
  (a1) *G is as in* (MA2) *with $m \geq n$.*
  (a2) *G is as in* (MA1) *with $m = n$.*

(b) *All nonnormal subgroups of G have the same order if and only if one of the following holds:*
  (b1) *$G \in \{\mathrm{D}_8, S(p^3)\}$.*
  (b2) *G is as in* (MA2) *with $m \geq n$.*

(c) *All nonnormal cyclic subgroups of G of same order are conjugate if and only if $G \cong M_{p^t}$.*

(d) *All nonnormal subgroups of G are conjugate if and only if $G \cong M_{p^t}$.*

Let $\mathrm{nc}(G)$ denote the number of conjugate classes of nonnormal subgroups of a group G.

If G is nilpotent and $\mathrm{nc}(G) = 1$, then G is primary. Therefore, in Theorem 112.2, we confine to p-groups.

Theorem 112.2 (O. Schmidt [Sch3]). *Let G be a p-group. If $\mathrm{nc}(G) = 1$, then we have $G \cong \mathrm{M}_{p^n+1}$.*

Proof. See Lemma 96.4. □

Theorem 112.3 (Passman [Pas, Proposition 2.4] = Theorem 1.25). *If all nonnormal subgroups of a non-Dedekindian p-group G of order $> p^3$ have the same order p, then one and only one of the following holds:*

(a) *$G \cong \mathrm{M}_{p^n}$.*

(b) *$G = \mathrm{Z}(G)\Omega_1(G)$, where $\mathrm{Z}(G)$ is cyclic and $\Omega_1(G)$ is nonabelian of order p^3 so $\Omega_1(G) \in \{S(p^3), \mathrm{D}_8\}$ (note, that $\mathrm{D}_8 * \mathrm{Z}(G) \cong \mathrm{Q}_8 * \mathrm{Z}(G)$).*

(c) *The group $G = Q * D$ is extraspecial of order 2^5, where $Q \cong \mathrm{Q}_8$ and $D \cong \mathrm{D}_8$.*

Proof. It is easy to check that the groups (a)–(c) satisfy the hypothesis.

By Proposition 1.23 (see also Lemma 96.2), $|G'| = p$ (otherwise, there is in G' a G-invariant subgroup R of index p such that G/R contains a nonnormal subgroup K/R; then K is not G-invariant of order $> p$, contrary to the hypothesis). If G is minimal nonabelian, then either $|G| = p^3$ or $G \cong \mathrm{M}_{p^n}$, $n > 3$, by Lemma 112.1(a). Next we assume that G is not minimal nonabelian.

Let $U < G$ be minimal nonabelian; then $U' = G'$ so $U \lhd G$. In view of Lemma 4.3, $G = U*C$, where $C = \mathrm{C}_G(U)$. Lemma 112.1(b) yields $U \in \{\mathrm{Q}_8, \mathrm{D}_8, \mathrm{M}_{p^n+1}, \mathrm{S}(p^3)\}$ since, if U is non-Dedekindian, it satisfies the hypothesis of that lemma. By assumption, $C \not\leq U$. Let $K < G$ be nonnormal of order p; then K is contained in exactly one subgroup of G of order p^2 (otherwise, $K \lhd G$). Considering $K\Omega_1(\mathrm{Z}(G))$, we con-

clude that $\mathrm{Z}(G)$ is cyclic and so G has no subgroup $\cong \mathrm{E}_{p^3}$ (indeed, if such a subgroup exists, it must lie in $\mathrm{Z}(G)$).

Next we consider all four possibilities for U.

(i) Let $U \cong \mathrm{D}_8$. Assume that C has a subgroup, say V, of order 2 that satisfies $V \neq \mathrm{Z}(U)$. If $A < U$ is nonnormal, then $A \times V \cong \mathrm{E}_4$ is not G-invariant (indeed, $(A \times V) \cap U = A$ is not U-invariant), a contradiction. Thus C is either cyclic or $\cong \mathrm{Q}_8$ (recall that $|G'| = 2$) so $G = U * C$ is a group from (b) or (c). In what follows we assume that G has no subgroups $\cong \mathrm{D}_8$.

(ii) Let $U \cong \mathrm{Q}_8$. Since G is not Dedekindian, we get $\exp(C) > 2$ by Theorem 1.20. Let $L \leq C$ be cyclic of order 4; write $H = U * L$. Assume that $U \cap L = \{1\}$; then $H = U \times L$. Since $\Omega_1(H) < \mathrm{Z}(H)$, $\exp(H) = 4$ and H is non-Dedekindian (Theorem 1.20), it has a nonnormal cyclic subgroup of order 4, a contradiction. Thus $|H| = 16$. Then $H = U * L$ has a subgroup $\cong \mathrm{D}_8$ (see Appendix 16), contrary to the assumption. Next we assume that G has no subgroups $\cong \mathrm{Q}_8$.

(iii) Let $U \cong \mathrm{S}(p^3)$, $p > 2$. As in (i), C is cyclic (of order $> p$ with $U \cap C = \mathrm{Z}(U)$ since $|G| > p^3$), and we get a group from (b) since then $U = \Omega_1(G)$ by the regularity of G. In what follows we assume that G has no subgroups $\cong \mathrm{S}(p^3)$.

(iv) Suppose that $U \cong \mathrm{M}_{p^{n+1}}$. Assume that there is $K < G$ of order p such that $K \not\leq U$. Put $H = \Omega_1(U)K$; then H of order p^3 is generated by elements of order p. It follows from (i) and (iii) that $H \cong \mathrm{E}_{p^3}$. In this case, H has a non-G-invariant subgroup of order p^2 (otherwise, $H \leq \mathrm{Z}(G)$, which is a contradiction). Thus we obtain $\Omega_1(G) = \Omega_1(U) \cong \mathrm{E}_{p^2}$ and C is cyclic by (ii). There is $S \leq C$ such that $S \not\leq U$ but $\mho_1(S) < U$. Let $T < U$ be cyclic of index p. Then $U \cap S \leq \mathrm{Z}(U) = \Phi(U) < T$, $|T| \geq |S|$ so (the abelian group) $TS = T \times L$, where L of order p, and L is not contained in U (otherwise, $S < U$), a final contradiction. □

Let G be a non-Dedekindian p-group such that $|H/H_G| \leq p$ for all $H < G$. If a subgroup $H < G$ is nonnormal of maximal order, then G/H_G is one of groups of Theorem 112.3.

Let us show how to prove Theorem 112.2 making use of Theorem 112.3. Suppose that $H < G$ is nonnormal; then H is cyclic. Set $|H| = p^s$. If $s = 1$, then $G \cong \mathrm{M}_{p^{n+1}}$ (Theorem 112.3). If $s > 1$, then $G/\Omega_1(H) \cong \mathrm{M}_{p^m}$ by induction, and the proof is finished as in Theorem 96.4.

D. Passman [Pas, Theorem 2.9] considered the p-groups without nonnormal subgroups $U < V$ such that $|V : U| = p$.

Suppose that, as in [Pas, Theorem 2.9], a non-Dedekindian p-group G has no two nonnormal subgroups $U < V$ with $|V : U| = p$. Let $H < G$ be nonnormal of maximal order. Then H is cyclic since all its maximal subgroups are G-invariant, and G/H_G is as in Theorem 112.2.[1]

[1] As Passman [Pas] has noticed, the converse is also true, i.e., if all nonnormal subgroups of G are cyclic, then it has no chain $U < V$ with nonnormal U, V such that $|V : U| = p$. Therefore Theorem 2.9

We consider an important partial case of [Pas, Theorem 2.9]. Note that the statement of Theorem 112.4 is neither stated in [Pas] nor follows from [Pas, Theorem 2.9] (since in the last theorem groups of order $< 2^8$ were not considered). For a complete classification of groups from [Pas, Theorem 2.9], see Theorem 16.2.

Now we are ready to prove the main result of this section.

Theorem 112.4. *Suppose that all nonnormal subgroups of a p-group G have the same order $p^v > p$; then $\Omega_1(G) = \Omega_1(\mathrm{Z}(G))$, $|\Omega_1(G)| \le p^2$. If $|\Omega_1(G)| = p$, then $G \cong \mathrm{Q}_{16}$, $v = 2$. Now we let $\Omega_1(G) \cong \mathrm{E}_{p^2}$; then $G/\Omega_1(G)$ is abelian. Let $H < G$ be nonnormal; then H is cyclic, G/H_G is as in Theorem 112.3 and one and only one of the hollowing holds:*

(a) $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}} \rangle$ *is metacyclic minimal nonabelian,* $m \ge n = v > 1$.

(b) $G = Q \times L$, *where* $Q \cong \mathrm{Q}_8$, $L \cong \mathrm{C}_4$, *and* $v = 2$.

(c) G *is minimal nonmetacyclic and special of order* 2^5, $v = 2$.[2]

(d) G *is special of order* 2^6 *with* $\mathrm{Z}(G) = G' = \Phi(G) = \Omega_1(G) \cong \mathrm{E}_4$, $v = 2$.[3]

Proof. By hypothesis, $|G| > p^3$. The hypothesis is inherited by non-Dedekindian subgroups. Note that all nonnormal subgroups of any proper non-Dedekindian epimorphic image of G are also of same order (which, however, is $< p^v$). We have $\Omega_1(G) \le \mathrm{Z}(G)$ since $v > 1$. Let $H < G$ be nonnormal; then all maximal subgroups of H are G-invariant so they do not generate H, and we infer that H is cyclic. If $U/H_G < G/H_G$ is not normal, then we have $|U| = |H|$ so $|U/H_G| = p$, and hence G/H_G is as in Theorem 112.3. Next, H is contained in exactly one (G-invariant) subgroup of G of order p^{v+1} so $\mathrm{N}_G(H)/H$ has exactly one subgroup of order p. We assume that $|\Omega_1(G)| > p$ (if $|\Omega_1(G)| = p$, then $G \cong \mathrm{Q}_{16}$). It follows that $H\Omega_1(\mathrm{Z}(G))/H$ is cyclic so $|\Omega_1(\mathrm{Z}(G))| = p^2$ since H is cyclic and $|\Omega_1(G)| > p$. If G is minimal nonabelian, it is metacyclic as in Lemma 112.3(b2) with $m \ge n > 1$. Next we assume that G is not minimal nonabelian. If G is of maximal class, then $|\Omega_1(G)| = p$ since $\Omega_1(G) \le \mathrm{Z}(G)$; then, as we know, $G \cong \mathrm{Q}_{16}$. Next we assume that G is not of maximal class; then $\Omega_1(G) = \Omega_1(\mathrm{Z}(G)) \cong \mathrm{E}_{p^2}$ and so $G/\Omega_1(G)$ is Dedekindian since all subgroups of G containing $\Omega_1(G)$ are noncyclic so G-invariant.

---

from [Pas] yields an almost full classification of p-groups all of whose nonnormal subgroups are cyclic. See §16.

[2] Defining relations of G, namely,

$$G = \langle a, b, c \mid a^4 = b^4 = [a, b] = 1,\ c^2 = a^2,\ a^c = ab^2,\ b^c = ba^2 \rangle,$$

are given in Theorem 66.1.

[3] Defining relations of G, namely,

$$G = \langle a, b, c, d \mid a^4 = b^4 = [a, b] = 1,\ c^2 = a^2b^2,\ a^c = a^{-1},$$
$$b^c = a^2b^{-1},\ d^2 = a^2,\ a^d = a^{-1}b^2,\ b^d = b^{-1},\ [c, d] = 1 \rangle,$$

are given in Theorem 16.2(ix).

Assume that $G/\Omega_1(G)$ is nonabelian. By the previous paragraph, there exists $\mathrm{Q}_8 \cong Q/\Omega_1(G) \leq G/\Omega_1(G)$ for some $Q \leq G$ and all maximal subgroups of Q containing $\Omega_1(G)$ are abelian since $\Omega_1(G) \leq \mathrm{Z}(G)$; then $|\mathrm{Z}(Q)| = 8$ and $|Q'| = 2$ (Lemma 1.4). In this case, $Q' < \Omega_1(G)$, a contradiction since $Q/\Omega_1(G) \cong \mathrm{Q}_8$ is nonabelian. Thus $G/\Omega_1(G)$ is abelian so $G' \leq \Omega_1(G)$. We conclude that G' is of order $\leq p^2$ and exponent p.

(a) By the previous paragraph, $G' \leq \Omega_1(G) \cong \mathrm{E}_{p^2}$, and since $\Omega_1(G) \leq \mathrm{Z}(G)$, we get $\mathrm{cl}(G) = 2$. If $\mathrm{d}(G) = 2$, then G is minimal nonabelian (Lemma 65.2(a)), contrary to the assumption. Thus we have $\mathrm{d}(G) > 2$ so G is not metacyclic. If $p > 2$, then, since $(\mathrm{E}_{p^2} \cong)\Omega_1(G) \leq \mathrm{Z}(G)$, G has no minimal nonmetacyclic subgroups (Lemma 69.1(a,b)) so it is metacyclic, $\mathrm{d}(G) = 2$, contrary to what has just been said. Next we assume that $p = 2$ and $\mathrm{d}(G) > 2$.

(b) Suppose that $Q < G$ is nonabelian of order 8; then $Q \cong \mathrm{Q}_8$ as $\Omega_1(Q) \leq \mathrm{Z}(G)$, and $Q \lhd G$ since Q is noncyclic. Write $C = \mathrm{C}_G(Q)$; then G/C is isomorphic to a noncyclic subgroup of D_8, a Sylow 2-subgroup of $\mathrm{Aut}(Q) \cong \mathrm{S}_4$, the symmetric group of degree 4. As $G' \leq \mathrm{Z}(G) \leq C$, we get $G/C \cong \mathrm{E}_4$ so $G = Q * C$ is a central product by the product formula since $Q \cap C = \mathrm{Z}(Q)$ has index 4 in Q. Since G is not Dedekindian, there is a cyclic $L \leq C$ of order > 2. If $Q \cap L > \{1\}$, then $Q * L$ has a nonnormal subgroup of order $2 < 2^v$, a contradiction. Thus $Q \cap L = \{1\}$. Let elements $u, v \in Q$ generate different cyclic subgroups of order 4 and let x be a generator of L. If $o(x) > 4$, then $\langle ux \rangle$ and $\langle ux^2 \rangle$ of different orders are not v-invariant, a contradiction. Thus $\exp(C) = 4$ and so $v = 2$.

Suppose that C contains a minimal nonabelian subgroup, say D; then we obtain $|\Omega_1(D)| \leq |\Omega_1(G)| = 4$ so D is metacyclic by Lemma 65.1; then $|D| \leq 16$ since $\exp(D) \leq \exp(C) = 4$.

If $|D| = 8$, then $D \cong \mathrm{Q}_8$ and $QD = Q \times D$ since $Q \cap L = \{1\}$ for a cyclic $L < C$ of order 4. Then the diagonal subgroup of $Q \times D$ (of order $8 > 4$) is not normal in $Q \times D$, a contradiction.

Thus $D \cong \mathscr{H}_{2,2} = \langle a, b \mid a^4 = b^4,\ a^b = a^3 \rangle$, the unique nonabelian metacyclic group of order 16 and exponent 4. Then $Q \cap D = \mathrm{Z}(Q) = \langle z \rangle$ is a maximal cyclic subgroup of D of order 2 since $|\Omega_1(G)| = 4$; we have $z = a^2b^2$. To obtain a contradiction, one may assume that $G = Q * D$. Let u and v be generators of distinct cyclic subgroups of Q of order 4. Put $H = \langle ub, a \rangle$. We have

$$(ub)^2 = u^2b^2 = zb^2 = a^2b^2b^2 = a^2, \quad [ub, a] = [b, a] = a^2$$

so $H \cong \mathrm{Q}_8$. Since $[ub, v] = [u, v] = z \neq a^2$ (indeed, $Q \cap \langle a \rangle = \{1\}$), we get $z \notin H$, so $H \cap Q = \{1\}$. As $Q, H \lhd G$, we get $F = QH = Q \times H$. Then the diagonal subgroup X of F is not normal in F, a contradiction since $|X| = 8$.

Thus D does not exist so C is abelian and $\mathrm{d}(C) \leq 2$ as $\Omega_1(C) \leq \Omega_1(\mathrm{Z}(G)) \cong \mathrm{E}_4$. If C is abelian of type $(4, 4)$, there is in C a cyclic subgroup L of order 4 containing $Q \cap C = \mathrm{Z}(Q)$, contrary to what has already been proved. Thus C must be abelian

of type $(4,2)$ so, if $\mathrm{C}_4 \cong L_1 < C$, then $L_1 \cap Q = \{1\}$ and $G = Q \times L_1$ (indeed, by the product formula, $|G| = 2^5 = |Q \times L_1|$).

In what follows we assume that G has no nonabelian subgroups of order 8.

Let us show that $\nu = 2$. Indeed, by (a), $\mathrm{d}(G) > 2$. Then G/G' contains a subgroup $E/G' \cong \mathrm{E}_8$. Since $\mathrm{d}(E) > 2$, E is neither abelian (since $|\Omega_1(G)| = 4$) nor minimal nonabelian. Let $T < E$ be minimal nonabelian. We claim that T is metacyclic of order 16 and exponent 4. Indeed,

$$8 < |T| < |E| = |G'||E/G'| \le 2^5 \quad \text{and} \quad \Omega_1(T) \le \Omega_1(G) \cong \mathrm{E}_4$$

so T is metacyclic (see (MA1) and (MA2)) and $|T| = 16$ and hence $T \cong \mathcal{H}_{2,2}$ since $\exp(T) = 4$. Since T has a nonnormal (cyclic) subgroup of order 2^2, we get $\nu = 2$. Then $H \cong \mathrm{C}_4$, $|H_G| = 2$ and $\mathrm{C}_2 \cong H_G \le \Phi(G)$. By the above, $\bar{G} = G/H_G$ is a group from Theorem 112.3.

(c) Let $\bar{G} = G/H_G = \bar{Q} * \bar{C}$, where $\bar{Q} \cong \mathrm{Q}_8$, $\bar{Q} \cap \bar{C} = \Omega_1(\bar{C})$ and $\bar{C} \cong \mathrm{C}_{2^n}$, $n > 1$.

Suppose that $M < G$ is minimal nonmetacyclic. Since M has no nonabelian subgroup of order 8 and $\Omega_1(G) \cong \mathrm{E}_4$, we have $|M| = 2^5$ (Theorem 66.1). In this case, $\bar{L} = \Omega_2(\bar{G}) = \bar{Q} * \Omega_2(\bar{C})$ has order 16 so $\Omega_2(G) \le L$ and $|L| = |H_G||\bar{L}| = 2^5$. Since $\Omega_2(M) = M$ has order 2^5 (Theorem 66.1), we get $L = M$ so $\Omega_2(G) = M$.

Suppose that $(\Omega_2(G) =) M < G$. In this case, there is in G a cyclic subgroup V of order 8. Then $V \lhd G$ (since $\nu = 2$ by (b)) and $Z = V \cap M$ is cyclic of order 4 and G-invariant. It follows from the hypothesis and $G' = M' \cong \mathrm{E}_4$ that G/Z is nonabelian and Dedekindian since $\nu = 2$ and $\mathrm{E}_4 \cong G' \not\le Z$; next, by assumption, we have $|G/Z| > 8$ (indeed, $|G| > |M| = 2^5$). Therefore $M/Z \cong \mathrm{Q}_8$ so there are exactly four maximal subgroups of M that does not contain Z (indeed, M contains seven maximal subgroups and only three of them contain Z). Let K be one of such subgroups that is nonabelian (K exists since M has at most one abelian maximal subgroup in view of $|M'| = 4$). Then $K \cap V = \Omega_1(V)$ as $Z < V$. Since $M/\Omega_1(V)$ is nonabelian, it contains at most three abelian maximal subgroups by Exercise 1.6(a). Therefore one may assume that K is chosen so that $K/\Omega_1(V)$ is nonabelian. We have $KV/\Omega_1(V) = (K/\Omega_1(V)) \times (V/\Omega_1(V))$, and this group is non-Dedekindian by Theorem 1.20 since $|V/\Omega_1(V)| = 4$. Therefore since $K/\Omega_1(V) \in \{\mathrm{D}_8, \mathrm{Q}_8\}$, the group $KV/\Omega_1(V)$ (of exponent 4) possesses a nonnormal subgroup, say $T/\Omega_1(V)$, of order 4.[4] Since $|T| = 8 > 4$, we get a contradiction. Thus $G = M$ is minimal nonmetacyclic as in part (c) of the theorem.

(d) Suppose that $G/H_G = \bar{G} = \bar{D} * \bar{Q}$ is extraspecial of order 2^5, where $\bar{D} \cong \mathrm{D}_8$ and $\bar{Q} \cong \mathrm{Q}_8$. Since $H_G < \mathrm{Z}(G)$ and $\bar{G}$ is a monolith, we get $G/\mathrm{Z}(G) \cong \mathrm{E}_{16}$ so $|\Phi(G)| \le 4$ and $\exp(G) = 4$. Suppose that $M < G$ is minimal nonmetacyclic. As in

[4]This is clear if $K/\Omega_1(V) \cong \mathrm{Q}_8$ (in that case, all subgroups of order 2 are normal there). In case $K/\Omega_1(V) \cong \mathrm{D}_8$ and $R/\Omega_1(V) < K/\Omega_1(V)$ is noncentral so of order 2, $R/\Omega_1(V) \times \Omega_1(V/\Omega_1(V))$ of order 4 is not normal in $K/\Omega_1(V)$.

part (c), we obtain $|M| = 2^5$ and M is special. Then $\mathrm{Z}(M) = M' = \Phi(M) \cong \mathrm{E}_4$. It follows that $\Phi(G) = \Phi(M)$ so $\mathrm{Z}(G) = \Phi(G) = G' = M'$ and hence G is special of order 2^6.

If G is as in (c) or (d), then every subgroup of G of order > 4 contains $\Omega_1(G) = G'$ so is G-invariant. This means that this G satisfies the hypothesis.[5] □

Note that the central product $G = U * C$, where

$$U = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^3 \rangle \cong \mathcal{H}_{2,2} \quad \text{and} \quad C = \langle c \rangle$$

such that $a^2 = c^2$, has nonnormal subgroups of order 4 and 2 (for example, $\langle b \rangle$ and $\langle ac \rangle$), however $G/\langle a^2 b^2 \rangle \cong \mathrm{D}_8 * \mathrm{C}_4$.

For completeness, we prove the following

Proposition 112.5. *Let G be a nonnilpotent group and a positive integer n be fixed. Suppose that $\lambda(H) = n$ for all nonnormal $H < G$.[6] Then $G = PQ$ is minimal nonabelian as in* (MNA)*, where $P \in \mathrm{Syl}_p(G)$ is cyclic, $G' = Q \in \mathrm{Syl}_q(G)$, and one of the following holds:*

(a) $|P| = p^n$, $|Q| = q$.

(b) $n = 1$, $|P| = p$, $Q \cong \mathrm{E}_{q^2}$.

Proof. Groups (a) and (b) satisfy the hypothesis.

Now let $M \leq G$ be minimal nonnilpotent. Then $M = P \cdot Q$, where $P \in \mathrm{Syl}_p(M)$ is cyclic and $Q = G' \in \mathrm{Syl}_q(M)$ (see Lemma 10.8). Since P is not normal in M so neither in G and $\lambda(M) \neq \lambda(P)$, we get $|P| = p^n$ and so $M \lhd G$. Then $Q \lhd G$ since Q is characteristic in M. Since a maximal subgroup of M containing P is not normal in M, it follows that P is maximal in M so Q is a minimal normal subgroup of M and M is minimal nonabelian. By Frattini's lemma, $G = \mathrm{N}_G(P)M = \mathrm{N}_G(P) \cdot Q$ is a semidirect product with kernel Q. As $\mathrm{N}_G(P)$ is not normal in G, we get $\mathrm{N}_G(P) = P$ so $G = \mathrm{N}_G(P)Q = PQ = M$. Thus G is a minimal nonabelian group.

Let $n > 1$. Then $|Q| = q$ (otherwise, G also has a nonnormal subgroup of order q and $\lambda(q) = 1 < n$) so $|G| = p^n q$.

Let $n = 1$ and $|Q| > q$. Then Q has no proper subgroup of order q^2 so $|Q| = q^2$. Also, G of order pq^2 satisfies the hypothesis (this group is as in (b)). □

Proposition 112.5 is a generalization of the nonnilpotent part of the following.

Corollary 112.6 (O. Schmidt [Sch3]). *If G is a nonnilpotent group with* $\mathrm{nc}(G) = 1$*, then G is minimal nonabelian as in Proposition 112.5*(a).

[5] It is noticed in Theorem 16.2(ix) that all maximal subgroups of the group G from part (d) are minimal nonmetacyclic. Let us prove this. If $S \in \Gamma_1$, then S (of order 2^5) is nonmetacyclic since $\exp(G) = 4$. If $M \leq S$ is minimal nonmetacyclic, then, as in the first paragraph of (d), we get $|M| = 2^5 = |S|$ so $M = S$.

[6] Recall that $\lambda(H)$ is the number of prime factors of n, i.e., $\Lambda(H) = a_1 + \cdots + a_k$ provided that $|H| = \prod_{i=1}^{k} p^{a_i}$ is the standard decomposition.

The following proposition is also a particular case of Theorem 16.2.

Proposition 112.7. *Let G be a non-Dedekindian two-generator p-group of order $> p^3$ with cyclic derived subgroup G'. If all nonnormal subgroups of G are cyclic, then one of the following holds:*

(a) *G is minimal nonabelian and metacyclic as in* (MA2).

(b) *$p = 2$ and either $G \cong \mathrm{Q}_{16}$ or $G = \langle a, b \mid a^8 = 1, a^4 = b^4, a^b = a^3 \rangle$ is of order 2^5.*

Conversely, all nonnormal subgroups of groups from (a) *and* (b) *are cyclic.*

Proof. First we check the last assertion. Let G be minimal nonabelian metacyclic as in (MA2). Then $G' < \Omega_1(G) \cong \mathrm{E}_{p^2}$ so all nonnormal subgroups of G do not contain $\Omega_1(G)$. If $H < G$ is nonnormal, then $|\Omega_1(H)| = p$ hence H, being abelian, is cyclic (Proposition 1.3) so the groups from (a) satisfy the hypothesis. Now assume that G is as in (b). Clearly, Q_{16} satisfies the hypothesis. Now let G be the second group in (b). If $H < G$ is nonnormal and noncyclic, $H \not\leq \Omega_2(G)$ as $\Omega_1(G) = R \lhd G$ is the unique proper noncyclic subgroup of $\Omega_2(G) \cong \mathrm{C}_4 \times \mathrm{C}_2$. Thus $\exp(H) = 8 (= \exp(G))$ so $H \in \Gamma_1$, a contradiction. Next we find the groups satisfying the hypothesis.

Suppose that G is not a 2-group of maximal class (otherwise, $G \cong \mathrm{Q}_{16}$). In this case, there is in G a normal subgroup $R \cong \mathrm{E}_{p^2}$; then all subgroups of G/R are normal so G/R is Dedekindian.

If $p > 2$, then G/R is abelian. Since $G' \leq R$ and G' is cyclic, we get $|G'| = p$ so G is minimal nonabelian (Lemma 65.2(a)). In this case, G is metacyclic (otherwise, G has a nonnormal abelian subgroup of type (p, p) which is noncyclic).

Next we assume that $p = 2$ and G is not minimal nonabelian (see the first paragraph); then we have $|G'| > 2$ (Lemma 65.2(a)). It remains to show that then G is as the second group in (b). We have $G' \not\leq R$ so G/R is nonabelian Dedekindian, and since $\mathrm{d}(G/R) = 2$, we get $G/R \cong \mathrm{Q}_8$, $|G| = 2^5$ and $R < \Phi(G)$. Assume that G has a subgroup $E \cong \mathrm{E}_8$; then $E \leq \mathrm{Z}(G)$ since all subgroups of E of order 4 are G-invariant. In this case, G is minimal nonabelian, a contradiction. Thus G has no subgroup $\cong \mathrm{E}_8$ so $|\Omega_2(G)| = 8$ and G (of order 2^5) is as in Lemma 42.1(c) and hence has defining relations given in (b). □

Remark. Let $p > 2$ and let G be a nonabelian p-group all of whose nonnormal subgroups are cyclic. As in the proofs of Theorems 112.3 and 112.4, G has no subgroup $\cong \mathrm{E}_{p^3}$ so G is a group from Theorem 13.7. If $R \lhd G$ is abelian of type (p, p), then G/R is abelian by Theorem 1.20. If G is metacyclic, then, being cyclic, $|G'| = p$ and G is minimal nonabelian by Lemma 65.2(a). If G is a 3-group of maximal class and $|G| > 3^3$, then $|G| = 3^4$, $\Omega_1(G) \cong \mathrm{E}_9$. If $G = EC$, where $E = \Omega_1(G) \cong \mathrm{S}(p^3)$ and C is cyclic, then all subgroups of G of type (p, p) are normal so $|G'| = p$. Then, by Lemma 4.3, $G = E * \mathrm{C}_G(E)$, where $\mathrm{C}_G(E)$ is cyclic.

Problem. Classify the p-groups that have no three nonnormal subgroups of pairwise distinct orders.

§113

The class of 2-groups in §70 is not bounded

Suppose that all maximal subgroups of a nonabelian p-group G are generated by two elements but $\mathrm{d}(G) = 3$. By Theorem 70.2, if such a group G is of class > 2, then $p = 2$, $|G| \geq 2^7$, and $G/\mathrm{K}_3(G)$ is isomorphic to the Suzuki group of order 2^6 given in Theorem 70.1(d). If G is of class ≤ 3, then these groups are completely determined in §70, where in particular for $p > 2$, $|G| \leq p^5$ and G is of class 2 and for $p = 2$, $|G| \leq 2^8$.

Theorem 113.1 (E. Crestani). *Let G be a 2-group all of whose maximal subgroups are generated by two elements but $\mathrm{d}(G) = 3$. Then the nilpotence class of G is not bounded.*

Proof. Eleonora Crestani from University of Padova has invented the following ingenious construction of a 2-group G_n of order 2^{4n+4} for each fixed $n \geq 2$ such that $\mathrm{d}(G_n) = 3$, each maximal subgroup of G_n is generated by two elements and the class of G_n is at least n. Therefore the nilpotence class of such groups is not bounded. In fact, E. Crestani has also proved that the nilpotence class of G_n is exactly $2n$, but that would require further tedious computations.

In order to construct our 2-group G_n for each fixed $n \geq 2$, we start with the homocyclic group

$$H = \langle g_4, g_5, g_6, g_7 \rangle \cong \mathrm{C}_{2^n} \times \mathrm{C}_{2^n} \times \mathrm{C}_{2^n} \times \mathrm{C}_{2^n}$$

of order 2^{4n}. Let K be the splitting extension of H by the cyclic group $\langle g_3 \rangle \cong \mathrm{C}_4$ of order 4, where g_3 induces the automorphism of order 4 on H given by

$$(1)\quad g_3^4 = 1, \quad g_4^{g_3} = g_4^{-1} g_6^2, \quad g_5^{g_3} = g_5^{-1} g_7^2, \quad g_6^{g_3} = g_6 g_4^{-1}, \quad g_7^{g_3} = g_7 g_5^{-1}.$$

We compute $g_i^{g_3^2} = g_i^{-1}$ for $i = 4, 5, 6, 7$ and so g_3^2 inverts H which implies that all elements in Hg_3^2 are involutions.

Let $L = K\langle g_2 \rangle$ be the cyclic extension of order 2 of K, where

$$(2)\qquad \begin{aligned} &g_2^2 = g_6 g_7^2, && g_4^{g_2} = g_4^{-1} g_6^{-2} g_7^{-4}, && g_5^{g_2} = g_5^{-1} g_6^2 g_7^4, \\ &g_6^{g_2} = g_6 g_4^{-2} g_5^{-2}, && g_7^{g_2} = g_7 g_4 g_5, && g_3^{g_2} = g_3^{-1} g_7. \end{aligned}$$

Here we have to show that g_2 induces an automorphism on $K = \langle g_3, g_4, g_5, g_6, g_7 \rangle$. It is enough to see that $g_i^{g_2}$, $i = 3, 4, \ldots, 7$, generate K (which is obvious) and then

we have to show that the relations (1) for K remain invariant when we replace g_i with $g_i^{g_2}$, $i = 3, \dots, 7$. For example, $(g_3^{g_2})^2 = (g_3^{-1}g_7)^2 \in Hg_3^2$ (since $K/H \cong \mathrm{C}_4$) and we know that all elements in Hg_3^2 are involutions and so $\mathrm{o}(g_3^{-1}g_7) = 4$. Then we verify $(g_4^{g_2})^{g_3^{g_2}} = (g_4^{g_2})^{-1}(g_6^{g_2})^2$. Indeed,

$$\begin{aligned}(g_4^{g_2})^{g_3^{g_2}} &= (g_4^{-1}g_6^{-2}g_7^{-4})^{g_3^{-1}g_7} = (g_4^{-1}g_6^{-2}g_7^{-4})^{(g_3^2g_3g_7)}\\ &= (g_4g_6^2g_7^4)^{g_3g_7} = g_4^{-1}g_6^2 \cdot g_6^2g_4^{-2} \cdot g_7^4g_5^{-4} = g_4^{-3}g_5^{-4}g_6^4g_7^4,\end{aligned}$$

and for the right-hand side we get the same result:

$$(g_4^{g_2})^{-1}(g_6^{g_2})^2 = g_4g_6^2g_7^4 \cdot g_6^2g_4^{-4}g_5^{-4} = g_4^{-3}g_5^{-4}g_6^4g_7^4.$$

In the same way we show that the last three relations in (1) remain invariant under the above replacement. Then we have to show that g_2^2 acts the same way on K as the inner automorphism of K induced by $g_6g_7^2$ (since $g_2^2 = g_6g_7^2$). First we compute that g_2^2 fixes each of the elements g_4, g_5, g_6, g_7 in H and then we show that

$$g_3^{g_2^2} = g_3^{g_6g_7^2}.$$

Finally, $G_n = L\langle g_1\rangle$, where

$$\begin{aligned}&g_1^2 = g_3^2g_6^{-1}g_7^{-3}, \quad g_4^{g_1} = g_4^{-1}g_6^{-2}g_7^{-6}, \quad g_5^{g_1} = g_5^{-1}g_6^2g_7^4,\\ &g_6^{g_1} = g_6g_4^{-2}g_5^{-3}, \quad g_7^{g_1} = g_7g_4g_5, \qquad g_2^{g_1} = g_2g_3^2, \qquad g_3^{g_1} = g_3^{-1}g_6.\end{aligned} \tag{3}$$

We proceed in exactly the same way as in the previous paragraph. First we show that g_1 induces an automorphism on $L = \langle g_2, g_3, g_4, g_5, g_6, g_7\rangle$, where obviously $g_i^{g_1}$, $i = 2, \dots, 7$, generate L. We only check that the relations (1) and (2) for L remain invariant when we replace all g_i with $g_i^{g_1}$, $i = 2, 3, \dots, 7$. Then we check that g_1^2 acts the same way on the generators $g_2, g_3, \dots, g_7$ of L as the inner automorphism of L induced by $g_3^2g_6^{-1}g_7^{-3}$ (since $g_1^2 = g_3^2g_6^{-1}g_7^{-3}$). The group G_n is constructed.

Our group G_n exists because it is obtained with three consecutive cyclic extensions (of orders 4, 2, 2) of the homocyclic group $H \cong \mathrm{C}_{2^n} \times \mathrm{C}_{2^n} \times \mathrm{C}_{2^n} \times \mathrm{C}_{2^n}$, $n \geq 2$. From our relations (1), (2) and (3) we see that the subgroups H, K, L are normal in G_n. It is easy to see that the nilpotence class of G_n is at least n. Indeed, the involution g_3^2 inverts the cyclic subgroup $\langle g_4\rangle$ of order 2^n and so $\langle g_4, g_3^2\rangle \cong \mathrm{D}_{2^{n+1}}$ is a dihedral group of order 2^{n+1} and class n. Hence G_n is of class at least n.

We show that $G_n' = \langle g_3^2, g_4, g_5, g_6, g_7\rangle = H\langle g_3^2\rangle$ and since $G/G_n' \cong \mathrm{E}_8$, we also have $\Phi(G_n) = G_n'$, $\mathrm{d}(G_n) = 3$ and $G_n = \langle g_1, g_2, g_3\rangle$. Indeed, $H = \langle g_4, g_5, g_6, g_7\rangle$ and $K = H\langle g_3\rangle$ are normal in G_n and so $H\langle g_3^2\rangle$ is also normal in G as $K/H \cong \mathrm{C}_4$. From our relations (1), (2), (3) we get $g_1^2, g_2^2, g_3^2 \in H\langle g_3^2\rangle$ and

$$[g_2, g_1] = g_3^2, \ [g_3, g_1] = g_3^2g_6, \ [g_3, g_2] = g_3^2g_7, \ [g_3, g_6] = g_4, \ [g_3, g_7] = g_5,$$

which shows that $G_n/(H\langle g_3^2\rangle) \cong \mathrm{E}_8$ and $G_n' = H\langle g_3^2\rangle = \Phi(G)$. Thus $\mathrm{d}(G_n) = 3$ and $G_n = \langle g_1, g_2, g_3\rangle$.

It remains to prove that each maximal subgroup of G_n is generated by two elements. Our seven maximal subgroups of G_n are $H_i = T_i G_n'$, where T_i $(i = 1, 2, \ldots, 7)$ is one of the subgroups:

$$\langle g_1, g_2\rangle,\ \langle g_1, g_3\rangle,\ \langle g_2, g_3\rangle,\ \langle g_1 g_2, g_3\rangle,\ \langle g_1, g_2 g_3\rangle,\ \langle g_2, g_1 g_3\rangle,\ \langle g_1 g_2, g_1 g_3\rangle.$$

Here we shall freely use the relations (1), (2), (3) (without quoting).

(i) $H_1 = \langle g_1, g_2\rangle G_n' = \langle g_1, g_2\rangle$ since $\langle g_1, g_2\rangle \geq G_n'$. Indeed, we have

$$[g_1, g_2] = g_3^2, \quad g_1^2 = g_3^2 g_6^{-1} g_7^{-3}, \quad g_2^2 = g_6 g_7^2$$

and so $[g_1, g_2] g_1^2 g_2^2 = g_7^{-1}$ which shows that $g_3^2, g_6, g_7 \in \langle g_1, g_2\rangle$. Furthermore, we have $g_6^{g_1} (g_7^2)^{g_1} = g_6 g_7^2 g_5^{-1}$ and so $g_5 \in \langle g_1, g_2\rangle$. Finally, $g_7^{g_1} = g_7 g_5 g_4$ and so $g_4 \in \langle g_1, g_2\rangle$ and we are done.

(ii) $H_2 = \langle g_1, g_3\rangle G_n' = \langle g_1, g_3\rangle$ since $\langle g_1, g_3\rangle \geq G_n'$ which shows the following relations (in this order):

$$[g_3, g_1] = g_3^2 g_6, \quad g_1^2 = g_3^2 g_6^{-1} g_7^{-3}, \quad g_6^{g_1} (g_7^2)^{g_1} = g_6 g_7^2 g_5^{-1}, \quad g_7^{g_1} = g_7 g_5 g_4.$$

(iii) $H_3 = \langle g_2, g_3\rangle G_n' = \langle g_2, g_3\rangle$ since $\langle g_2, g_3\rangle \geq G_n'$ which show the relations

$$[g_3, g_2] = g_3^2 g_7, \quad g_7^{g_3} = g_7 g_5^{-1}, \quad g_7^{g_2} = g_7 g_4 g_5, \quad g_2^2 = g_6 g_7^2.$$

(iv) $H_4 = \langle g_1 g_2, g_3\rangle G_n' = \langle g_1 g_2, g_3\rangle$ since $\langle g_1 g_2, g_3\rangle \geq G_n'$. Indeed, we have $(g_1 g_2)^2 = g_5 g_7$, $(g_5 g_7)^{g_3} = g_5^{-2} g_7^3$ and so $g_3^2, g_5, g_7 \in \langle g_1 g_2, g_3\rangle$. Further, we get $[g_3, g_1 g_2] = g_4^{-2} g_6 (g_5^{-1} g_7^{-1})$ and so $g_4^{-2} g_6 \in \langle g_1 g_2, g_3\rangle$. Finally, we conclude $(g_4^{-2} g_6)^{g_3} = g_4 g_6^{-3} \in \langle g_1 g_2, g_3\rangle$ and so $g_4, g_6 \in \langle g_1 g_2, g_3\rangle$.

(v) $H_5 = \langle g_1, g_2 g_3\rangle G_n' = \langle g_1, g_2 g_3\rangle = T_5$ as $T_5 \geq G_n'$. Indeed, $[g_2 g_3, g_1] = g_6$ which implies that $g_6 \in T_5$. Further, $g_1^2 = g_3^2 g_6^{-1} g_7^{-3}$ implies that $g_3^2 g_7^{-3} \in T_5$, $(g_2 g_3)^2 = g_7^3 g_5^{-1} g_6$ gives $g_7^3 g_5^{-1} \in T_5$ and then also $g_3^2 g_5^{-1} \in T_5$. From the relations $g_6^{g_1} = g_6 g_4^{-2} g_5^{-3}$ and $g_6^{g_2 g_3} = g_4 g_5^2 g_7^{-4} g_6^{-3}$ it follows $g_4^{-2} g_5^{-3} \in T_5$, $g_4 g_5^2 g_7^{-4} \in T_5$ and then also $g_4^{-1} g_5^{-1} g_7^{-4} \in T_5$. In view of $(g_4 g_5 g_7^4)^{g_1} = g_4^3 g_5^3 g_7^2 \in T_5$, we obtain that $(g_4^{-1} g_5^{-1} g_7^{-4})^3 (g_4^3 g_5^3 g_7^2) = g_7^{-10}$ and so $g_7^2 \in T_5$ which also forces $g_4 g_5 \in T_5$. Then by the above, the relation $(g_4 g_5)^2 (g_4^{-2} g_5^{-3}) = g_5^{-1}$ gives that $g_5 \in T_5$. But from the above facts it also follows that $g_4, g_3^2, g_7 \in T_5$ and we are done.

(vi) $H_6 = \langle g_2, g_1 g_3\rangle G_n' = \langle g_2, g_1 g_3\rangle = T_6$ as $T_6 \geq G_n'$. Indeed, $[g_2, g_1 g_3] = g_7^{-1}$ and so $g_7 \in T_6$. From $g_2^2 = g_6 g_7^2$ it follows that $g_6 \in T_6$ and $(g_1 g_3)^2 = g_3^2 g_4^{-1} g_7^{-3}$ yields $g_3^2 g_4^{-1} \in T_6$. Further, the relation $g_7^{g_2} = g_7 g_4 g_5$ implies $g_4 g_5 \in T_6$. From $g_6^{g_1 g_3} = (g_4 g_5^3) g_6^{-3} g_7^{-6}$ it follows $g_4 g_5^3 \in T_6$ which together with a previous result gives $g_5^2 \in T_6$. Finally, $g_7^{g_1 g_3} = g_4^{-1} g_5^{-2} g_6^2 g_7^3$ implies with the previous results that $g_4, g_5, g_3^2 \in T_6$ and we are done.

(vii) $H_7 = \langle g_1 g_2, g_1 g_3\rangle G_n' = \langle g_1 g_2, g_1 g_3\rangle = T_7$ since $T_7 \geq G_n'$. Indeed, from $(g_1 g_2)^2 = g_5 g_7$ and $(g_1 g_3)^2 = g_3^2 g_4^{-1} g_7^{-3}$ we conclude that $t_1 = g_5 g_7 \in T_7$ and

$t_2 = g_3^2 g_4^{-1} g_7^{-3} \in T_7$. We compute

$$[g_1 g_2, g_1 g_3] = g_3^2 g_4^{-2} g_5^{-1} g_6 g_7^{-1}$$

and this gives $t_3 = g_3^2 g_4^{-2} g_5^{-1} g_6 g_7^{-1} \in T_7$. Further,

$$(g_5 g_7)^{g_1 g_3} = g_4^{-3} g_5^{-5} g_6^4 g_7^5$$

and so $t_4 = g_4^{-3} g_5^{-5} g_6^4 g_7^5 \in T_7$. Finally, we obtain $(g_3^2 g_4^{-1} g_7^{-3})^{g_1 g_2} = g_3^2 g_5^3 g_6^{-2} g_7^{-5}$ which implies that $t_5 = g_3^2 g_5^3 g_6^{-2} g_7^{-5} \in T_7$.

Now, the five elements t_1, t_2, t_3, t_4, t_5 also lie in G_n' and note that we have $\Phi(G_n') = \langle g_4^2, g_5^2, g_6^2, g_7^2 \rangle$ so that $G_n'/\Phi(G_n') \cong \mathrm{E}_{2^5}$. We claim that $\langle t_1, t_2, t_3, t_4, t_5 \rangle = G_n'$ and so $G_n' \leq T_7$, as required. Indeed, considering the cosets $t_i \Phi(G_n')$ $(i = 1, \ldots, 5)$, we see that $t_1 \Phi(G_n')$ contains $g_5 g_7$, $t_2 \Phi(G_n')$ contains $g_3^2 g_4 g_7$, $t_3 \Phi(G_n')$ contains $g_3^2 g_5 g_6 g_7$, $t_4 \Phi(G_n')$ contains $g_4 g_5 g_7$ and $t_5 \Phi(G_n')$ contains $g_3^2 g_5 g_7$ and these new five elements are obviously linearly independent mod $\Phi(G_n')$. □

§114

Further counting theorems

In what follows let $e(X)$ be the number of solutions of $x^p = 1$ in a p-group X and let $\Gamma_1(X)$ be the set of all maximal subgroups of a p-group X. In this section we closely follow [HupB, §VIII.5].

Theorem 114.1 ([Bla10] = [HupB, Theorem VIII.5.1]). *Let G be a p-group and let $\{1\} < N \leq \Omega_1(\mathrm{Z}(G))$. Then*

$$\sum_{M \in \Gamma_1(N)} e(G/M) = (|\Gamma_1(N)| - 1)e(G/N) + e(G).$$

Proof. Let $k = |\Gamma_1(N)|$; then $|N| = (p-1)k + 1$ since N is elementary abelian. If $Z \leq N$ is of order p, then

$$|\Gamma_1(N/Z)| = \frac{|N : Z| - 1}{p-1} = \frac{|N| - p}{p(p-1)} = \frac{(p-1)k + 1 - p}{p(p-1)} = \frac{k-1}{p}.$$

Let

$$\mathcal{Y} = \{(x, M) \mid x \in G - N,\ M \in \Gamma_1(N),\ x^p \in M\}.$$

For $x \in G - N$ and $x^p \in N$, let

$$\mathcal{Y}_x = \{M \in \Gamma_1(N) \mid x^p \in M\}.$$

Clearly, $|\mathcal{Y}_x|$ is the number of maximal subgroups of the quotient group $N/\langle x^p \rangle$. Thus $|\mathcal{Y}_x| = k$ if $x^p = 1$ and $|\mathcal{Y}_x| = \frac{k-1}{p}$ if $x^p \neq 1$ (see the first displayed formula in the proof). Hence

$$|\mathcal{Y}| = \sum_x |\mathcal{Y}_x| = \sum_{x^p=1} k + \sum_{x^p \neq 1} \frac{k-1}{p} = \sum_{x^p=1} \left(k - \frac{k-1}{p}\right) + \sum_x \frac{k-1}{p},$$

where x runs through the set of all elements of $G - N$ for which $x^p \in N$, i.e., all x with $(xN)^p = N$. Thus the number of $x \in G - N$ for which $x^p \in N$ is equal to $(e(G/N) - 1)|N|$. Hence

$$\begin{aligned} |\mathcal{Y}| &= (e(G) - |N|)\left(k - \frac{k-1}{p}\right) + (e(G/N) - 1)|N|\frac{k-1}{p} \\ &= e(G)\left(k - \frac{k-1}{p}\right) + e(G/N)|N|\frac{k-1}{p} - k|N|. \end{aligned} \tag{1}$$

On the other hand, suppose that $M \in \Gamma_1(N)$. The number of elements $x \in G - N$ for which $x^p \in M$ is $(e(G/M) - p)|M|$, so

$$|\mathcal{Y}| = \sum_{M \in \Gamma_1(N)} (e(G/M) - p)\frac{|N|}{p}. \tag{2}$$

Comparing the two expressions for $|\mathcal{Y}|$ in (1) and (2), we obtain

$$e(G)\frac{(p-1)k+1}{p} + e(G/N)|N|\frac{k-1}{p} - k|N| = \sum_{M \in \Gamma_1(N)} (e(G/M) - p)\frac{|N|}{p},$$

or, since $|N| = (p-1)k + 1$, $k = |\Gamma_1(N)|$, we get

$$e(G)\frac{|N|}{p} + e(G/N)|N|\frac{k-1}{p} - k|N| = \sum_{M \in \Gamma_1(N)} e(G/M) - k|N|,$$

and we conclude that

$$e(G) + e(G/N)(|\Gamma_1(N)| - 1) = \sum_{M \in \Gamma_1(N)} e(G/M),$$

as was to be shown. □

Thus

$$e(G) = \sum_{M \in \Gamma_1(N)} e(G/M) - (|\Gamma_1(N)| - 1)e(G/N).$$

Lemma 114.2 ([HupB, Lemma VIII.5.2]). *Suppose that a p-group $G = A * B$ (central product). Let $D = A \cap B$, $|D| = p$ and $\exp(A/D) = \exp(B/D) = p$. Then*

$$e(G) = \frac{1}{p}\left(e(A)e(B) + \frac{(|A| - e(A))(|B| - e(B))}{p-1}\right).$$

Proof. We have $G \cong (A \times B)/\langle (x, x^{-1})\rangle$ for a generator x of D. Thus

$$pe(G) = |\{(a,b) \in A \times B \mid a^p = x^i, b^p = x^{-i} \text{ for some } i \in \{0.1, \ldots, p-1\}\}|.$$

If $i = 0$, the number of solutions of $a^p = x^i (= 1)$ is $e(A)$; otherwise, it is equal to $\frac{|A| - e(A)}{p-1}$ since $\exp(A/D) = p$. Similar statements hold for B. Hence

$$\begin{aligned} pe(G) &= e(A)e(B) + (p-1)\frac{|A| - e(A)}{p-1} \cdot \frac{|B| - e(B)}{p-1} \\ &= e(A)e(B) + \frac{(|A| - e(A))(|B| - e(B))}{p-1}, \end{aligned}$$

completing the proof. □

We have, by Lemma 114.2,

$$e(\mathrm{Q}_8 * \mathrm{Q}_8) = \frac{1}{2}(2 \cdot 2 + (8-2)^2) = 20,$$
$$e(\mathrm{D}_8 * \mathrm{D}_8) = \frac{1}{2}(6^2 + (8-6)^2) = 20,$$
$$e(\mathrm{Q}_8 * \mathrm{D}_8) = \frac{1}{2}(2 \cdot 6 + 6 \cdot 2) = 12.$$

Theorem 114.3 ([HupB, Lemma VIII.5.3]). *Suppose that G is a 2-group, $\mathrm{d}(G) = d$ and $|\Phi(G)| = 2$. Then $e(G) \in \{2^d, 2^d \pm 2^{d-r}\}$, where r is a positive integer satisfying $2r \le d$. Further, if $e(G) = 2^d \pm 2^{d-\frac{1}{2}d}$, then G is extraspecial.*

Proof. Clearly, $\exp(G) = 4$. If G is abelian, then $e(G) = 2^d$.

Now let G be nonabelian. Then, by Lemma 4.2, $G = E\mathrm{Z}(G)$, where E is extraspecial. Let $E = \mathrm{ES}(m, 2)$ and $\mathrm{d}(\mathrm{Z}(G)) = s$; then $d = 2m + s - \epsilon$, where $\epsilon = 0$ if $\exp(\mathrm{Z}(G)) = 4$ and $\epsilon = 1$ if $\exp(\mathrm{Z}(G)) = 2$. We have

$$\mathrm{cd}(E) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\} = \{1, 2^m\}.$$

By the Frobenius–Schur formula (see [BZ, §4.6]), we get $e(E) = 2^{2m} \pm 2^m$ (indeed, $\mathrm{Irr}_1(E) = \{\chi\}$, where $\chi(1) = 2^m$).

Suppose that $\exp(\mathrm{Z}(G)) = 2$. Then $G = E \times T$, where $T \cong \mathrm{E}_{2^{s-1}}$, and so

$$e(G) = e(E)e(T) = (2^{2m} \pm 2^m)2^{s-1} = 2^{2m+s-1} \pm 2^{m+s-1}. \tag{3}$$

In this case,

$$d = 2m + s - 1, \quad m + s - 1 = (2m + s - 1) - m = d - m, \quad 2m \le d.$$

Now suppose that $\exp(\mathrm{Z}(G)) = 4$. Then $\mathrm{Z}(G) = \mathrm{C}_4 \times \mathrm{E}_{2^{s-1}}$, $\mathrm{d}(\mathrm{Z}(G)) = s$ and $e(\mathrm{Z}(G)) = 2^s$. Let us apply Lemma 114.2 with $A = E$ and $B = \mathrm{Z}(G)$. We have

$$2e(G) = 2^s[2^{2m} \pm 2^m + 2^{2m+1} - (2^{2m} \pm 2^m)] = 2^{2m+s+1} \tag{4}$$

so $e(G) = 2^{2m+s} = 2^d$, and we obtain again the desired result.

Now assume that $e(G) = 2^d \pm 2^{d-\frac{1}{2}d}$. Then, by (3) and (4), $\exp(\mathrm{Z}(G)) = 2$ and

$$d = 2m + s - 1, \quad \frac{1}{2}d = m + s - 1 \quad \text{(by (3))}$$

so that $2m + s - 1 = 2(m + s - 1)$. It follows that $s = 1$ so $G = E\mathrm{Z}(G) = E$ is extraspecial, completing the proof. □

Theorem 114.4 ([HupB, Theorem VIII.5.4]). *Suppose that G is a 2-group of class at most 2 and exponent at most 4. Suppose that $\{x \in G \mid x^2 = 1\} = N$ is a subgroup of G. Then $|G| \le |N|^3$; indeed, $|G| < |N|^3$ if G is not special.*

Proof. Since the theorem obviously holds if G is abelian (in this case, $|G| \leq |N|^2|$), we will assume, in what follows, that G is nonabelian. We prove the theorem by induction on $|N|$. If $|N| = 2$, then G is isomorphic to Q_8 (Proposition 1.3), and the assertion is clear. Suppose then that $|N| > 2$. Clearly, $\Phi(G) \leq N$ as $\exp(G/N) < \exp(G) = 4$.

First suppose that $G' < N$. We have $N \leq L$ where $L/G' = \Omega_1(G/G')$. Since L/G' is elementary abelian, we get $L/G' = (N/G') \times (K/G')$ for some $K \leq L$. As $G' < N$, we get $K < L$ so induction may be applied to K. Thus $|K| \leq |\Omega_1(K)|^3 = |N \cap K|^3 = |G'|^3$ so $|L| = |N||K|/|G'| \leq |N||G'|^2$. But

$$|L : G'| = |\Omega_1(G/G')| = |G/G' : \mho_1(G/G')| = |G : \Phi(G)|$$

so $|G : L| = |\Phi(G) : G'|$. Hence

$$\begin{aligned} |G| &= |G : L||L| = |\Phi(G) : G'||L| \leq |\Phi(G) : G'||N||G'|^2 = |\Phi(G)||N||G'| \\ &\leq |N||N||G'| = |N|^2|G'| < |N|^3 \end{aligned}$$

since $G' < N$ by assumption.

Suppose that $G' = N$; then $\Phi(G) = N$ also in view of $G' \leq \Phi(G) \leq N = G'$. Since G is of class 2, we obtain that $N \leq Z(G)$. Suppose next that $N < Z(G)$. Choose $z \in Z(G) - N$. Let M be a maximal subgroup of G not containing z (M exists since $z \notin \Phi(G)$). Thus

$$G = M\langle z\rangle, \quad M \cap \langle z\rangle = Z,$$

where $Z = \langle z^2\rangle \neq \{1\}$ (indeed, $\Omega_1(G) = N < Z(G)$ so $o(z) > 2$). We apply induction to M/Z. If $x \in M$ and $x^2 \in Z$, we have $x^2 = (z^2)^m = z^{2m}$ for some m and $xz^{-m} \in N$ since $(xz^{-m})^2 = x^2z^{-2m} = x^2x^{-2} = 1$). Hence $z^m \in M \cap \langle z\rangle = Z$ and $xZ \in N/Z$. Thus $|M/Z| \leq |N/Z|^3$, and this implies $|M| \leq \frac{|N|^3}{|Z|^2}$; then

$$|G| = 2|M| \leq \frac{2|N|^3}{|Z|^2} = \frac{1}{2}|N|^3 < |N|^3$$

since $|Z| = 2$ (recall that $\exp(G) = 4$).

Thus one may assume that $G' = \Phi(G) = Z(G) = N$; then G is special. We have $e(G) = |N| = 2^n$, and $e(G/N) = 2^d$, say. Next, $|\Gamma_1(N)| = 2^n - 1$. Hence, by Theorem 114.1,

$$\sum_{M \in \Gamma_1(N)} e(G/M) = (|\Gamma_1(N) - 1)e(G/N) + e(G) = (2^n - 2)2^d + 2^n. \tag{5}$$

By Theorem 114.3, $e(G/M) \in \{2^d, 2^d \pm 2^{d-r}\}$, where the positive integer r is such that $2r \leq d$. Substituting in (5), we obtain an equation of the form

$$2^{n+d} - 2^{d+1} + 2^n = \sum_i (\pm 2^{s_i}),$$

where $s_i \geq \frac{1}{2}d$. Suppose that $n < \frac{1}{2}d$. Then $s_i > n$ for all i, so the right-hand side is divisible by 2^{n+1}, which is a contradiction since $2^{n+1} \mid (2^{n+d} - 2^{d+1})$, but 2^{n+1} does not divide 2^n. Hence $n \geq \frac{1}{2}d$ and $|G| = 2^{d+n} \leq 2^{3n} = |N|^3$. □

Theorem 114.5 ([HupB, Theorem VIII.5.5]). *Let G be a nonidentity 2-group and suppose that* $\mathrm{Aut}(G)$ *permutes the set* $\mathrm{Inv}(G)$ *of involutions of G transitively. Further, let* $|\Omega_1(\mathrm{Z}(G))| = q$. *Then*

(a) $\Omega_1(\mathrm{Z}(G)) = \Omega_1(G)$.

(b) (Gross [Gro]) $|G| = q^m$ *for some positive integer m.*

(c) (Shaw) *If G is nonabelian and of exponent* 4, *then G is special and* $|G| \in \{q^2, q^3\}$.

Proof. Statement (a) is obvious.

(b) Given an involution $t \in G$, write $m_k = |\{y \in G \mid y^{2^{k-1}} = t\}|$ $(k \geq 1)$. Since $\mathrm{Aut}(G)$ permutes the set of involutions of G transitively, m_k is independent of t, and the number of elements of order 2^k in G is $(q-1)m_k$ $(k \geq 1)$. Hence

$$|G| - 1 = (q-1)(m_1 + m_2 + \cdots)$$

and so $q-1$ divides $|G|-1$. Let $|G| = q^m \cdot 2^s$, where $2^s < q$. Since

$$\frac{|G|-1}{q-1} = \frac{2^s \cdot q^m - 1}{q-1} = \frac{2^s(q^m-1)}{q-1} + \frac{2^s - 1}{q-1}$$

is an integer, we get $s = 0$ so $|G| = q^m$, proving (b).

(c) Since $\exp(G) = 4$, we get $\exp(G/\Omega_1(\mathrm{Z}(G))) = 2$ hence $G/\mathrm{Z}(G)$ is elementary abelian. Thus $G' \leq \Omega_1(\mathrm{Z}(G))$. As G is nonabelian, we have $G' > \{1\}$. By hypothesis, $\Omega_1(\mathrm{Z}(G))$ is a minimal characteristic subgroup of G so $G' = \Omega_1(\mathrm{Z}(G))$. Therefore G/G' is elementary abelian so $G' = \Phi(G)$. If $G' < \mathrm{Z}(G)$, then $\mathrm{Z}(G)$ contains an element z of order 4. Now, if $y \in G - \mathrm{Z}(G)$, y^2 is an involution. Since z^2 is also an involution, we obtain $y^2 = (z^2)^\alpha$ for some $\alpha \in \mathrm{Aut}(G)$. But then $y^2 = (z^\alpha)^2$ and $y(z^\alpha)^{-1} \in \mathrm{Z}(G)$ so $y \in \mathrm{Z}(G)$, which is a contradiction. Hence $G' = \mathrm{Z}(G) = \Omega_1(G)$.

By (b), $|G| = q^m$ for some positive integer m, and by Theorem 114.4, $m \leq 3$. Since G is nonabelian, $m > 1$ so $m = 2$ or 3.[1] □

[1] Both values of m are possible.

§115

Finite p-groups all of whose maximal subgroups except one are extraspecial

In a letter Z. Janko reported that he proved that if all maximal subgroups of a 2-group G except one are extraspecial, then G is of maximal class and order 2^4. Below we consider the similar problem for all p.

Recall that all maximal abelian subgroups of any extraspecial group of order p^{2m+1} have the same order p^{m+1}. In particular, if this group possesses an abelian subgroup of index p, then $m = 1$.

Theorem 115.1. *All nonabelian maximal subgroups of a nonabelian p-group G except one are extraspecial if and only if G is either minimal nonabelian or of order p^4.*

Proof. All nonabelian maximal subgroups of a nonabelian group G of order p^4 are extraspecial unless G is minimal nonabelian. In what follows we assume that G is not minimal nonabelian and $|G| > p^4$ (clearly, $|G| = p^{2m}$ for some $m > 2$ by Theorem 4.7(a)). Then there is a nonabelian $E \in \Gamma_1$. Since, by Exercise 1.6(a), the number of nonabelian members of the set Γ_1 is at least $p > 1$, one may assume that E is extraspecial.

Assume that there is an abelian $A \in \Gamma_1$. Since $A \cap E$ is an abelian maximal subgroup of the extraspecial group E, we get $|E| = p^3$ (Theorem 4.7(d)); then

$$|G| = p|E| = p^4,$$

contrary to the assumption. Thus the set Γ_1 has no abelian members.

Since $|\Gamma_1| \geq p + 1 \geq 3$, there is an extraspecial $F \in \Gamma_1 - \{E\}$. Note that $E' \lhd G$ and $E' = \Phi(E) \leq \Phi(G) < F$ so $E' = F'$ since F' is a unique normal subgroup of order p in F. Thus all extraspecial members of the set Γ_1 have the same derived subgroup E'. By what has been said in the previous paragraph, all members of the set Γ_1 except one are extraspecial. Since G has a maximal subgroup whose center is of order $> p$ and this subgroup is neither abelian nor extraspecial, it follows that the number of extraspecial members in the set Γ_1 is divisible by p (indeed, we have $|\Gamma_1| = 1 + p + \cdots + p^{\mathrm{d}(G)-1}$). Set $\bar{G} = G/E'$.

We consider the following two cases.

(i) Suppose that $\bar{G}$ is nonabelian. Since $\bar{G}$ has at most one nonabelian member and the number of abelian maximal subgroups of $\bar{G}$ is at least p, we conclude that G/E'

is minimal nonabelian (see the previous paragraph and Exercise 1.6(a)). As $\bar{E}$ and $\bar{F}$ are elementary abelian, we get $\Omega_1(\bar{G}) = \bar{G}$ so $\bar{G} \in \{\mathrm{D}_8, S(p^3)\}$, where $S(p^3)$ is nonabelian of order p^3 and exponent p. In this case, $|G| = |E'||\bar{G}| = p^4$, contrary to the assumption.

(ii) Thus $\bar{G}$ is abelian. As $\bar{G} = \bar{E}\bar{F}$, it follows that $\bar{G}$ is elementary abelian. Since $|\bar{E}| = p^{2m}$ for some $m > 1$, we get $|\bar{G}| = p^{2m+1}$ so $\bar{G} \cong \mathrm{E}_{p^{2m+1}}$ and $|G| = 2^{2m+2}$ with $G' = E'$. Therefore G is not extraspecial, and we conclude that $|\mathrm{Z}(G)| > p$. Since $G/\mathrm{Z}(G)$ is noncyclic, it contains two distinct maximal subgroups $M/\mathrm{Z}(G)$ and $N/\mathrm{Z}(G)$. As, by assumption, M and N are nonabelian and, obviously, M and N are not extraspecial (indeed, $|\mathrm{Z}(G)| > p$ and $\mathrm{Z}(G) \leq M \cap N$), we get a contradiction. □

Exercise 1. Classify the p-groups all of whose maximal subgroups except one are elementary abelian.

Answer. The dihedral group D_8 is the unique group with that property.

Corollary 115.2. *If all maximal subgroups of a nonabelian p-group G except one are extraspecial, then G is of maximal class and order p^4.*

A p-group G is said to be a CZ-*group* if G' is its unique minimal normal subgroup. In this case, $\mathrm{Z}(G)$ is cyclic. If $x, y \in G$, then we infer that $1 = [x, y]^p = [x, y^p]$ so $\mho_1(G) \leq \mathrm{Z}(G)$ and hence $\Phi(G) = G'\mho_1(G) \leq \mathrm{Z}(G)$, and we conclude that $\Phi(G)$ is also cyclic (see §4 on such G). A minimal nonabelian p-group X is a CZ-group if and only if its center is cyclic (in this case, X is either of order p^3 or $X \cong \mathrm{M}_{p^n}$). Obviously, extraspecial p-groups are CZ-groups.

Let G be a CZ-group. By Lemma 4.2, $G = (A_1 * \cdots * A_n)\mathrm{Z}(G)$, where $A_1, \ldots, A_n$ are minimal nonabelian. In our case, $\mathrm{Z}(G)$ is cyclic so $\mathrm{Z}(A_i)$ is cyclic for all i. Then it follows that $A_i \in \{\mathrm{D}_8, \mathrm{Q}_8, S(p^3), \mathrm{M}_{p^k}\}$. At least one member of the set Γ_1 is not a CZ-group.

Theorem 115.3. *Suppose that all maximal subgroups of a nonabelian p-group G of order $p^m > p^4$ except one are* CZ*-groups and let $F \in \Gamma_1$ be an arbitrary* CZ*-subgroup. Then $\mathrm{Z}(G)$ is cyclic.*

(a) *If G/F' is abelian, then G is a* CZ*-group.*[1]

Next we assume that G/M' is nonabelian for all CZ*-members $M \in \Gamma_1$. Then we have $F' = M'$ for all such M since $\mathrm{Z}(G)$ is cyclic.*

(b) *If the quotient group G/F' is minimal nonabelian, then $\mathrm{d}(G) = 2$ and $|G'| = p^2$. Also, $G/\mathrm{Z}(F)$ is abelian of type (p^2, p) and $\mathrm{Z}(F) < \Phi(G)$.*

(c) *Suppose that $G/\mathrm{Z}(F)$ is abelian (or, what is the same, $G' \leq \mathrm{Z}(F)$). Then $G/\mathrm{Z}(F)$ is abelian of type (p^2, p) and $\mathrm{d}(F) \leq 3$. If $M \in \Gamma_1 - \{F\}$ is a* CZ*-subgroup, then $\mathrm{Z}(M) \neq \mathrm{Z}(F)$ and $M/\mathrm{Z}(F)$ is cyclic; moreover, $M \cong \mathrm{M}_{p^{m-1}}$.*

[1] But we do not assert that all CZ-groups satisfy the hypothesis.

Proof. Assume that $\mathrm{Z}(G)$ is noncyclic. Then all members of the set Γ_1 that contain $\mathrm{Z}(G)$ are not CZ-groups. Since $G/\mathrm{Z}(G)$ is noncyclic, the set Γ_1 has at least $p+1 > 1$ members which are not CZ-groups, and this is a contradiction. Thus

(i) $\mathrm{Z}(G)$ is cyclic.

By hypothesis, the set Γ_1 has two distinct members F and H that are CZ-groups. By (i), $F' = H'$ since $F', H' \leq \mathrm{Z}(G)$. Then, by Exercise 1.6(a), the set $\Gamma_1(G/F')$ contains at least $p+1$ abelian members. Assume that the set $\Gamma_1(G/F')$ has a nonabelian member M/F'. Then M is not a CZ-group (otherwise, $M' = F'$ so M/F' is abelian), and we conclude that $\mathrm{d}(G) \geq 3$. Therefore, by Exercise 1.6(a), the set $\Gamma_1(G/F')$ has at least p^2 nonabelian members so the set Γ_1 has at least p^2 members that are not CZ-groups, and this is a contradiction. Thus

(ii) G/F' is either abelian or minimal nonabelian for any CZ-subgroup $F \in \Gamma_1$, $H' = F'$ for all CZ-subgroups $H \in \Gamma_1 - \{F\}$.

We consider two cases, mentioned in (ii), separately.

A. Suppose that G/F' is abelian; then $G' = F'$. Since $\mathrm{Z}(G)$ is cyclic by (i), G' is a unique minimal normal subgroup of G so G is a CZ-group.

B. Suppose that G/F' is minimal nonabelian. Since $F' \leq \Phi(F) \leq \Phi(G)$, we get $\mathrm{d}(G) = \mathrm{d}(G/F') = 2$. By Lemma 65.1, $\mathrm{d}(F) = \mathrm{d}(F/F') \leq 3$, and this is true for any CZ-member of the set Γ_1. Due to Lemma 4.2 (or Lemma 4.3), F is a product of minimal nonabelian subgroup and $\mathrm{Z}(F)$ so $F/\mathrm{Z}(F) \cong \mathrm{E}_{p^2}$ hence $|G/\mathrm{Z}(F)| = p^3$. Since $G/\mathrm{Z}(F)$ is noncyclic and $\mathrm{d}(G) = 2$, we obtain $\mathrm{Z}(F) < \Phi(G)$.

Suppose that the quotient group $G/\mathrm{Z}(F)$ is abelian; then $G/\mathrm{Z}(F)$ (of order p^3) is abelian of type (p^2, p) since $\mathrm{d}(G) = 2$. Let $H \in \Gamma_1 - \{F\}$ be a CZ-subgroup. We have $\mathrm{Z}(H) \neq \mathrm{Z}(F)$ (otherwise, $\mathrm{Z}(F) = \mathrm{Z}(G)$ and so G is minimal nonabelian, a contradiction). Then the quotient group $H/\mathrm{Z}(F)$ (recall that $\mathrm{Z}(F) \leq \Phi(G) < H$) is cyclic of order p^2 (indeed, $F/\mathrm{Z}(F)$ is the unique noncyclic maximal subgroup of $G/\mathrm{Z}(F)$ which is abelian of type (p^2, p)) so H is metacyclic since $\mathrm{Z}(F)$ is cyclic (indeed, F is a CZ-group). In this case, H is minimal nonabelian (Lemma 65.2(a)). Since $\mathrm{Z}(H)$ is cyclic and $|H| > p^3$, we get $H \cong \mathrm{M}_{p^{m-1}}$. □

Remark 1. Suppose that a p-group G is neither abelian nor minimal nonabelian. Let Γ_1' be the set of nonabelian members of the set Γ_1. It follows from Exercise 1.6(a) that $|\Gamma_1'| \geq p$. We suppose that the set Γ_1' contains $\leq p-1$ non-extraspecial members. One may assume that $|G| = p^m > p^4$ (groups of order p^4 satisfy the hypothesis). Then there is an extraspecial $E \in \Gamma_1$. Since $|E| \geq 2^5$, it follows that E has no abelian subgroup of index p, and we conclude, as above, that $\Gamma_1' = \Gamma_1$ so the set Γ_1 contains $\leq p-1$ non-extraspecial members. Because of $|\Gamma_1| \geq p+1$, there is an extraspecial $F \in \Gamma_1 - \{E\}$. As in the proof of Theorem 115.1, $\mathrm{Z}(G)$ is cyclic. Since $E', F' \leq \mathrm{Z}(G)$, we get $E' = F'$. Set $\bar{G} = G/E'$. Then the set $\Gamma_1(\bar{G})$ of maximal subgroups of $\bar{G}$ contains two distinct (elementary) abelian members, therefore, by Exercise 1.6(a), it contains at least $p+1$ abelian members. Next, $\Omega_1(\bar{G}) = \bar{E}\bar{F} = \bar{G}$ hence, if $\bar{G}$ is abelian,

it has exponent p. Assume that $\bar{G}$ is neither abelian nor minimal nonabelian. Then the set $\Gamma_1(\bar{G})$ contains at least p nonabelian members whose inverse images in G are not extraspecial, contrary to the hypothesis. Thus, if $\bar{G}$ is nonabelian, it is minimal nonabelian and so $|\bar{G}| = p^3$ (Lemma 65.1). (i) Assume that $\bar{G}$ is elementary abelian; then G is not extraspecial since $|G| = p|E| = p^{2(k+1)}$, where $|E| = p^{2k+1}$. It follows that $|\mathrm{Z}(G)| > p$. Since $G/\mathrm{Z}(G)$ is noncyclic, all $\geq p+1$ members of the set Γ_1 containing $\mathrm{Z}(G)$, are not extraspecial, contrary to the hypothesis (recall that the set Γ_1 has no abelian members). (ii) Now let $\bar{G}$ is minimal nonabelian of order p^3. Then we get $|G| = |\bar{G}||E'| = p^4$, contrary to the assumption.

Recall that a p-group G is said to be an *$\mathcal{A}_n$-group* if it has a nonabelian subgroup of index p^{n-1} but all its subgroups of index p^n are abelian. The p-groups which are $\mathcal{A}_2$-groups are classified in §71.

Remark 2. Let a p-group G be neither abelian nor minimal nonabelian. Suppose that all nonabelian members of the set Γ_1 are either extraspecial or minimal nonabelian. Then G is an $\mathcal{A}_2$-group. Indeed, by hypothesis, $|G| > p^3$. If $|G| = p^4$, it satisfies the hypothesis. In what follows we assume that $|G| > p^4$. If all nonabelian maximal subgroups are minimal nonabelian, then G is an $\mathcal{A}_2$-group. In the following we assume that there is an extraspecial $E \in \Gamma_1$. If $A \in \Gamma_1$ is either abelian or minimal nonabelian, then $E \cap A$ is abelian of index p in E so $|E| = p^3$. Then $|G| = p^4$, contrary to the assumption. Thus all maximal subgroups of G are extraspecial. This is impossible since there is in G a maximal subgroup with center of order $> p$.

Theorem 115.4. *Let a p-group G be neither abelian nor minimal nonabelian. Suppose that all nonabelian members of the set Γ_1 are either minimal nonabelian or of maximal class. Then one and only of the following holds:*

(a) *G is an $\mathcal{A}_2$-group.*

(b) *G is a p-group of maximal class with abelian subgroup of index p.*

(c) *G is a 3-group of maximal class with nonabelian fundamental subgroup G_1 (in this case, G_1 is minimal nonabelian).*

Proof. Suppose that G is not an $\mathcal{A}_2$-group; then $|G| > p^4$. In this case, there is in the set Γ_1 a member M of maximal class. Then, by Theorem 12.12(a), G is either of maximal class or $\mathrm{d}(G) = 3$; so, in the second case, the set Γ_1 contains exactly $p+1$ members that are either abelian or minimal nonabelian (Theorem 13.6).

(i) Suppose that G is of maximal class. One may assume that $p > 3$ as all p-groups of maximal class and order $> p^4$, $p \leq 3$, satisfy the hypothesis (see §9). If the set Γ_1 has an abelian member, then all nonabelian members of the set Γ_1 are of maximal class (Fitting's lemma) so G satisfies the hypothesis. Next we assume that Γ_1 has no abelian members. If $|G| > p^{p+1}$, then the fundamental subgroup G_1 of G must be minimal nonabelian since it is not of maximal class. In this case, as $p^{p-1} = |\Omega_1(G_1)| \leq p^3$ (Lemma 65.1), we get $p = 3$, contrary to the assumption.

Now let $|G| = p^m \leq p^{p+1}$; then $p > 3$ since $m > 4$. In this case, the set Γ_1 has at most two distinct members that are not of maximal class. Let $A \in \Gamma_1$ be not of maximal class. Then A is minimal nonabelian. We have $A' = \mathrm{Z}(G)$. Since $\mathrm{cl}(G) > 3$, we conclude that A is a unique member of the set Γ_1 which is not of maximal class (otherwise, $\mathrm{cl}(G/\mathrm{Z}(G)) = 2$). As $|\Omega_1(A)| \leq p^3$, it follows that G has no subgroup of order p^5 and exponent p. Since $m > 4$, we get $\exp(A) > p$. Next, the metacyclic abelian subgroup A/A' is the fundamental subgroup of G/A' (recall that $A' = \mathrm{Z}(G)$). It follows that $|G/A'| = p^4$ so $|G| = p^5$ and A/A' is abelian of type (p^2, p). Since $\exp(G/A') = p$, we get a contradiction.

(ii) Suppose that Γ_1 contains exactly $p + 1$ members, say $A_1, \ldots, A_{p+1}$, that are either abelian or minimal nonabelian. Then all intersections $M \cap A_i$ $(i = 1, \ldots, p+1)$ are abelian and have index p in M (here $M \in \Gamma_1$ is of maximal class). Since $m > 4$, M contains at most one abelian subgroup of index p. It follows that $M \cap A_1 = \cdots = M \cap A_{p+1}$ so $G/(M \cap A_1)$ contains $p + 2$ distinct subgroups

$$M/(M \cap A_1),\ A_1/(M \cap A_1),\ \ldots\ ,\ A_{p+1}/(M \cap A_{p+1})$$

of order p, a contradiction since the abelian group $G/(M \cap A_1)$ of type (p, p) contains exactly $p + 1$ subgroups of order p. □

Exercise 2. Classify the p-groups all of whose nonabelian maximal subgroups are either of maximal class or have derived subgroup of order p. (*Hint*. Use §137.)

Exercise 3. Classify the p-groups all of whose nonabelian maximal subgroups are either absolutely regular or of maximal class. (*Hint*. Use Theorem 12.1(b).)

Exercise 4. Classify the p-groups all of whose nonabelian maximal subgroups are either metacyclic or of maximal class.

Exercise 5. Classify the p-groups all of whose nonabelian members of the set Γ_2 are either minimal nonabelian or of maximal class.

Exercise 6. Classify the p-groups containing $\geq p$ extraspecial maximal subgroups.

§116

Groups covered by few proper subgroups

1^o *Introduction.* We say that a group G is covered by proper subgroups $A_1, \ldots, A_n$ if

$$G = A_1 \cup \cdots \cup A_n. \tag{1}$$

We have, in (1), $G > \{1\}$ and $n > 1$. A group is covered by its proper subgroups if and only if it is noncyclic (check!). Every noncyclic group is covered by (proper) cyclic subgroups. A group is not covered by two proper subgroups. Covering (1) is said to be *irredundant* if every proper subset of the set $\{A_1, \ldots, A_n\}$ does not cover G. In what follows we assume that (1) is an irredundant covering of G by proper subgroups.

Remark 1. If, in (1), $|A_1| \geq \cdots \geq |A_n|$, then $|G| \leq |A_1|n - (n-1) < n|A_1|$ and hence $|G : A_1| < n$.

Let $\mathcal{M}$ be a maximal subset (with respect to inclusion) of pairwise noncommuting elements of a nonabelian group G. We denote the set of all such subsets by $\Lambda(G)$. Write

$$\gamma(G) = \max\{|\mathcal{M}| \mid \mathcal{M} \in \Lambda(G)\}.$$

For any abelian group G we set $\gamma(G) = 1$. If H is a subgroup of G, then we have $\gamma(H) \leq \gamma(G)$.

Recall that two groups G and G_1 are lattice isomorphic if there is a bijective mapping ϕ of the set of subgroups of G onto the set of subgroups of G_1 such that, provided $F, H \leq G$, we have $(F \cap H)^\phi = F^\phi \cap H^\phi$ and $\langle F, H\rangle^\phi = \langle F^\phi, H^\phi\rangle$. If groups G and G_1 are lattice isomorphic, then the inequality $\gamma(G) \neq \gamma(G_1)$ is possible owing to the fact that some nonabelian groups are lattice isomorphic to abelian groups (indeed, the group $\mathrm{M}_{p^{n+1}}$ is lattice isomorphic to the abelian group of type (p^n, p)).

As Lemma 116.2(a) shows, if $\mathcal{M} \in \Lambda(G)$, then $G = \bigcup_{x \in \mathcal{M}} \mathrm{C}_G(x)$ and this covering is irredundant.

Every nonabelian group contains two noncommuting elements. If $a, b \in G$ satisfy $ab \neq ba$, then the elements a, b, ab are pairwise noncommuting, i.e., $\gamma(G) \geq 3$. For p-groups one can prove a stronger result.

Lemma 116.1. *Let G be a nonabelian p-group. Then*

(a) *If G is minimal nonabelian, then $\gamma(G) = p + 1$.*

(b) $\gamma(G) \geq p + 1$.

Proof. (a) Since all maximal subgroups of G are abelian, any two noncommuting elements of G are contained in distinct maximal subgroups of G. Thus $\gamma(G) \leq p+1$. If $M_1, \ldots, M_{p+1}$ are all the maximal subgroups of G and $x_i \in M_i - \Phi(G)$ for all i, then, for $i \neq j$, $\langle x_i, x_j \rangle = G$ is nonabelian, so $x_i x_j \neq x_j x_i$. Hence $x_1, \ldots, x_{p+1}$ are pairwise noncommuting elements so $\gamma(G) \geq p+1$, completing the proof.

(b) Let H be a minimal nonabelian subgroup of G. Then $\gamma(H) = p+1$ by (a), and so $\gamma(G) \geq \gamma(H) = p+1$. □

The following lemma establishes a connection between members of the set $\Lambda(G)$ with some irredundant coverings of a nonabelian group G. Part (b) of this lemma also shows that the members of $\Lambda(G)$ of cardinality $\gamma(G)$ have a special property.

If G is a minimal nonabelian p-group of order p^n, then

$$|\Lambda(G)| = (p^{n-1} - p^{n-2})^{p+1},$$

but G has only one irredundant covering (see Lemma 116.3(b) and Theorem 116.5).

Lemma 116.2. *Let G be a nonabelian group and $\mathcal{M} \in \Lambda(G)$. Then*

(a) *We have*

$$\bigcup_{x \in \mathcal{M}} \mathrm{C}_G(x) = G. \tag{2}$$

If $\mathcal{N} \subseteq \mathcal{M}_1 \in \Lambda(G)$ and $\bigcup_{x \in \mathcal{N}} \mathrm{C}_G(x) = G$, then $\mathcal{N} = \mathcal{M}_1$; in particular, (2) *is an irredundant covering.*

(b) *Suppose, in addition, that $|\mathcal{M}| = \gamma(G)$. If $x \in \mathcal{M}$, then $\langle G - \bigcup_{y \in \mathcal{M} - \{x\}} \mathrm{C}_G(y) \rangle$ is abelian.*

Proof. (a) Assume that there is $g \in G - \bigcup_{x \in \mathcal{M}} \mathrm{C}_G(x)$. Since $\mathcal{M} \subset \mathcal{M} \cup \{g\}$, it follows from the maximality of $\mathcal{M}$ that $gx = xg$ for some $x \in \mathcal{M}$; then $g \in \mathrm{C}_G(x)$, contrary to the choice of g. Thus $\bigcup_{x \in \mathcal{M}} \mathrm{C}_G(x) = G$.

Now assume that there is $u \in \mathcal{M}$ such that $\bigcup_{x \in \mathcal{M} - \{u\}} \mathrm{C}_G(x) = G$. Then there exists $v \in \mathcal{M} - \{u\}$ such that $u \in \mathrm{C}_G(v)$, so that u, v are distinct commuting members of the set $\mathcal{M}$, a contradiction. Thus the covering $\bigcup_{x \in \mathcal{M}} \mathrm{C}_G(x) = G$ is irredundant.

(b) Given $x \in \mathcal{M}$, set $D = G - \bigcup_{y \in \mathcal{M} - \{x\}} \mathrm{C}_G(y)$. The set D is nonempty. Assume that there are noncommuting $u, v \in D$. By the choice, every element of the set $\mathcal{M} - \{x\}$ does not commute with u and v. It follows that $(\mathcal{M} - \{x\}) \cup \{u, v\} \subseteq M_2 \in \Lambda(G)$, a contradiction since $|\mathcal{M}_2| > |\mathcal{M}| = \gamma(G)$. Thus all elements of the set D commute so the subgroup $\langle D \rangle$ is abelian. □

It follows from Lemma 116.2(a) that if $H < G$ is such that $\gamma(H) = \gamma(G)$ and if we have $\mathcal{M} = \{x_1, \ldots, x_{\gamma(G)}\} \in \Lambda(H)$, then there are $i \neq j$ with $\mathrm{C}_G(x_i) \not\leq H$ and $\mathrm{C}_G(x_j) \not\leq H$. Indeed, there is an index i such that $\mathrm{C}_G(x_i) \not\leq H$ since

$$\bigcup_{k=1}^{\gamma(G)} \mathrm{C}_G((x_k) = G > H \quad \text{(Lemma 116.2(a))}.$$

If for all $j \neq i$ we have $C_G(x_j) \leq H$, then $H \cup C_G(x_i) = G$, which is impossible since H and $C_G(x_j)$ are nonincident.

2^o *p-groups.* In this section we study the p-groups containing a maximal subset (with respect to inclusion) of pairwise noncommuting elements of cardinality $p+1$. Some related results are also established and discussed. Next, we study the p-groups which are covered by $\leq 2p$ proper subgroups. It is proved that if a p-group G admits an irredundant covering by $p+2$ subgroups, then $p = 2$.

A noncyclic p-group G admits an irredundant covering by $p+1$ maximal subgroups (indeed, if $T \lhd G$ is such that G/T is abelian of type (p, p), then $p+1$ maximal subgroups of G containing T cover G). Moreover, Lemma 2.1 shows that if a p-group G is covered by $p+1$ proper subgroups $A_1, \ldots, A_{p+1}$, then $|G : \bigcap_{i=1}^{p+1} A_i| = p^2$, i.e., all A_i are maximal in G.

Lemma 116.3 is known; however, we prove it to make our exposition self-contained.

Lemma 116.3. *Suppose that a noncyclic p-group G of order p^m is covered by n proper subgroups $A_1, \ldots, A_n$ as in* (1). *Then*

(a) $n \geq p+1$.

(b) *If $n = p+1$, then the covering* (1) *is irredundant and $|G : \bigcap_{i=1}^{p+1} A_i| = p^2$. In particular, the A_i are maximal in G.*

Proof. (a) If $n \leq p$, then

$$\left| \sum_{i=1}^{n} A_i^{\#} \right| \leq p(p^{m-1} - 1) = p^m - p < |G^{\#}|,$$

a contradiction.

(b) Now let $n = p+1$. Then the covering (1) is irredundant by (a). First assume that $A_1, \ldots, A_{p+1}$ are maximal in G; then $|A_i \cap A_j| = p^{m-2}$ for $i \neq j$. We have

$$G = A_{p+1} \cup \left(\bigcup_{i=1}^{p} (A_i - A_{p+1}) \right). \tag{3}$$

Since $A_i - A_j = A_i - (A_i \cap A_j)$ for $i \neq j$, the right-hand side of (3) contains at most

$$p^{m-1} + p(p^{m-1} - p^{m-2}) = p^m = |G|$$

elements so (3) is a partition of G. Then it follows that $A_i \cap A_{p+1} = A_j \cap A_{p+1}$ and $(A_i - A_{p+1}) \cap (A_j - A_{p+1}) = \varnothing$ for all distinct $i, j < p+1$ (indeed, one can take in (3) A_k instead of A_{p+1}). We conclude that $\bigcap_{i=1}^{p+1} A_i = A_1 \cap A_{p+1}$ has index p^2 in G.

It follows from the above computation (see the displayed formula after (3)) that, in fact, all subgroups $A_1, \ldots, A_{p+1}$ must be maximal in G (otherwise, we obtain that $|\bigcup_{i=1}^{p+1} A_i| < |G|$). □

It follows from Lemmas 116.2 and 116.3 that if G is a nonabelian p-group, then we have $\gamma(G) \geq p+1$. In Theorem 116.5(b), the p-groups G which satisfy $\gamma(G) = p+1$ are classified.

Lemma 116.4. *Let H be a minimal nonabelian subgroup of a p-group G. Then the intersection $\Lambda(H) \cap \Lambda(G)$ is not empty if and only if $G = H * \mathrm{C}_G(H)$ (central product); in this case, $\Lambda(H) \subseteq \Lambda(G)$.*

Proof. (i) Let $\mathcal{M} \in \Lambda(H) \cap \Lambda(G)$; then we have $|\mathcal{M}| = p+1$ (Lemma 116.1(a)). By hypothesis and Lemma 116.2(a), we get $G = \bigcup_{x \in \mathcal{M}} \mathrm{C}_G(x)$ so, by Lemma 116.3(b), $|G : \bigcap_{x \in \mathcal{M}} \mathrm{C}_G(x)| = p^2$. Since $\bigcap_{x \in \mathcal{M}} \mathrm{C}_G(x) = \mathrm{C}_G(\mathcal{M})$ and $\langle \mathcal{M} \rangle = H$, we get $\mathrm{C}_G(H) = \mathrm{C}_G(\mathcal{M})$. As $\mathrm{C}_G(H) \cap H = \mathrm{Z}(H)$ has index $p^2 = |G : \mathrm{C}_G(\mathcal{M})|$ in H, we obtain $G = H * \mathrm{C}_G(H)$ by the product formula.

(ii) Now suppose that we are given an (arbitrary) p-group $G = H * \mathrm{C}_G(H)$, where H is minimal nonabelian, and let $\mathcal{M} = \{x_1, \ldots, x_{p+1}\} \in \Lambda(H)$. Then we conclude $G = H * \mathrm{C}_G(H) \subseteq \bigcup_{x \in \mathcal{M}} \mathrm{C}_G(x)$, so $\mathcal{M} \in \Lambda(G)$ by Lemmas 116.2(a) and 116.3(a). Thus $\Lambda(H) \subseteq \Lambda(G)$ since $\mathcal{M}$ is arbitrary.[1] □

Theorem 116.5. *Let G be a nonabelian p-group.*

(a) *If $\mathcal{M} \in \Lambda(G)$ has cardinality $p+1$, then $|G : \mathrm{C}_G(x)| = p$ for all $x \in \mathcal{M}$ and $|G : \mathrm{C}_G(\mathcal{M})| = p^2$.*

(b) *$\gamma(G) = p+1$ if and only if $G = H\mathrm{Z}(G)$, where H is an arbitrary minimal nonabelian subgroup of G, $H \cap \mathrm{Z}(G) = \mathrm{Z}(H)$. If, in addition, G is of exponent p, then $G = H \times E$, where H is nonabelian of order p^3 and E is abelian.*

Proof. Statement (a) follows from Lemma 116.3(b).

(b) Suppose that $\gamma(G) = p+1$. Let $H \leq G$ be minimal nonabelian. Then we see that $\mathcal{M} \in \Lambda(H)$ has cardinality $p+1$ (Lemma 116.1(a)) so that $\mathcal{M} \in \Lambda(G)$ by hypothesis. By Lemma 116.4, $G = H * \mathrm{C}_G(H)$.

We claim that $\mathrm{C}_G(H) = \mathrm{Z}(G)$. It suffices to show that $\mathrm{C}_G(H)$ is abelian (indeed, then $\mathrm{C}_G(\mathrm{C}_G(H)) \geq H\mathrm{C}_G(H) = G$). Assume that this is false. Then $\mathrm{C}_G(H)$ contains two noncommuting elements b, b_1. Let $\mathcal{M} = \{a_1, \ldots, a_{p+1}\} \in \Lambda(H)$. Take $a \in L - \{\mathrm{Z}(H) \cup \{a_1\}\}$, where L is an (abelian) maximal subgroup of H containing a_1 (such an a exists since $|L - \mathrm{Z}(H)| > 1$). Then, as $[ab, a_i] = [a, a_i] \neq 1$ for $i > 1$ (indeed, for $i > 1$ the subgroup $\langle a, a_i \rangle = H$ is nonabelian), we see that the $p+1$ elements $ab, a_2, \ldots, a_{p+1}$ are pairwise noncommuting. Note that $[ab, ab_1] = [b, b_1] \neq 1$ and for $i > 1$ we have $[ab_1, a_i] = [a, a_i] \neq 1$. It follows that the $p+2 (> \gamma(G))$ elements $ab, ab_1, a_2, \ldots, a_{p+1}$ are pairwise noncommuting, which is a contradiction. Thus $\mathrm{C}_G(H)$ is abelian so coincides with $\mathrm{Z}(G)$.

Let us show that for our group $G = H\mathrm{Z}(G)$ we have $\gamma(G) < p+2$ (we have $\Lambda(H) \subseteq \Lambda(G)$, but our assertion is stronger). Indeed, assume that $g_1, \ldots, g_{p+2} \in G$

[1] We do not assert that, in the case under consideration, $\gamma(G) = \gamma(H)$ (however, this equality holds by Theorem 116.5).

are pairwise noncommuting. Then we have $g_i = h_i z_i$, where $h_i \in H$ and $z_i \in \mathrm{Z}(G)$ $(i = 1, 2, \ldots, p+2)$. Let $i \neq j$. Then

$$[h_i, h_j] = [h_i z_i, h_j z_j] = [g_i, g_j] \neq 1$$

so the minimal nonabelian p-group H contains the $p+2$ pairwise noncommuting elements $h_1, \ldots, h_{p+2}$, contrary to Lemma 116.1(a).

Now suppose that $G = H\mathrm{Z}(G)$ is of exponent p (here H is of order p^3 as minimal nonabelian group of exponent p by Lemma 65.1, and $\mathrm{Z}(G)$ is elementary abelian). In this case, $H \cap \mathrm{Z}(G) = \mathrm{Z}(H)$ is of order p so $\mathrm{Z}(G) = \mathrm{Z}(H) \times E$, where E is elementary abelian. Then $G = H \times E$, and this completes the proof of (b). □

Theorem 116.5(b), in particular, classifies the nonabelian p-groups possessing exactly $p+1$ distinct centralizers of noncentral elements.[2]

Proposition 116.6. *The following assertions for a nonabelian p-group G are equivalent:*

(a) *If $H \leq G$ is minimal nonabelian, then $\Lambda(H) \subseteq \Lambda(G)$.*

(b) *$G = (B_1 * \cdots * B_k)\mathrm{Z}(G)$, where $B_1, \ldots, B_k$ are minimal nonabelian.*

Proof. (a) $\Rightarrow$ (b). We proceed by induction on $|G|$. Let $B_1 \leq G$ be minimal nonabelian. Then $G = B_1 * \mathrm{C}_G(B_1)$ by Lemma 116.4. If $\mathrm{C}_G(B_1)$ is abelian, we are done. If $\mathrm{C}_G(B_1)$ is nonabelian, the result follows by induction applied to $\mathrm{C}_G(B_1)$.

(b) $\Rightarrow$ (a). Let G be as in (b) and $H \leq G$ be minimal nonabelian. Since $|G'| = p$, then, by [B1, Lemma 4.3(a)], we obtain $G = H * \mathrm{C}_G(H)$ so $\Lambda(H) \subseteq \Lambda(G)$ by Lemma 116.4. □

Remark 2. The argument in part (ii) of the proof of Lemma 116.4 shows that if H is a nonabelian subgroup of an arbitrary group $G = H * \mathrm{C}_G(H)$, then $\Lambda(H) \subseteq \Lambda(G)$.

3^o *Nonnilpotent groups.* In this subsection G is a nonnilpotent group. We consider coverings of nonnilpotent groups by a few proper subgroups. Minimal nonabelian and minimal nonnilpotent groups play a crucial role in what follows.

Let p be a prime divisor of $|G|$ such that G has no normal p-complement. Then there is in G a minimal nonnilpotent subgroup $H = Q \cdot P$, where $P = H' \in \mathrm{Syl}_p(H)$ and $Q \in \mathrm{Syl}_q(H)$ is cyclic (this follows from Frobenius' normal p-complement theorem; see, for example, [Isa5, Theorem 9.18]). We have $|P| = p^{b+c}$, where b is the order of p modulo q and $p^c = |P \cap \mathrm{Z}(H)|$ (see [BZ, Lemma 11.2]). In this case, there are in H exactly p^b Sylow q-subgroups, say

$$Q_1 = \langle x_1 \rangle, \ \ldots, \ Q_{p^b} = \langle x_{p^b} \rangle.$$

Then $x_1, \ldots, x_{p^b}$ are pairwise noncommuting elements (indeed, if $i \neq j$, then $\langle x_i, x_j \rangle$ is nonnilpotent since it has two distinct Sylow q-subgroups Q_i and Q_j so this two-generator subgroup coincides with H). If $\{y_1, \ldots, y_s\}$ is a maximal subset of pairwise

[2] Note that [P] yields an estimate of the index $|G : \mathrm{Z}(G)|$ in terms of $\gamma(G)$.

noncommuting elements of P, then

$$\{y_1, \dots, y_s, x_1, \dots, x_{p^b}\}$$

is a maximal subset (with respect to inclusion) of pairwise noncommuting elements of H of cardinality $p^b + s \geq p^b + 1$ (note that $s = 1$ if and only if P is abelian). If P is nonabelian, then $s \geq p+1$ (Lemma 116.1(b)). Thus $\gamma(G) \geq \gamma(H) = p^b + s \geq p^b + 1$.

Theorem 116.7. *Let G be a nonabelian group and p be a prime divisor of $|G|$.*

(a) *If G has no normal p-complement, then $\gamma(G) \geq p + 1$. If, in addition, p is the minimal prime divisor of $|G|$, then $\gamma(G) \geq p^2 + 1$.*

(b) *Suppose that G has a normal p-complement however a Sylow p-subgroup is not a direct factor of G. Then $\gamma(G) \geq p + 2$. If, in addition, $\gamma(G) = p + 2$, then either $p = 2$ and $q = 3$ or p is a Mersenne prime.*

(c) *If $G = P \times A$, where P is nonabelian, A is abelian and $\gamma(G) < p + 2$, then P is such as in Theorem 116.5*(b) *and A is abelian.*

Proof. Statement (a) was proved in the paragraph preceding the theorem.[3]

(b) Now assume that G has a normal p-complement H but $P \in \mathrm{Syl}_p(G)$ is not a direct factor of G. In this case, the p-solvable group G contains a nonnilpotent subgroup PQ, where $Q \in \mathrm{Syl}_q(H)$; then we get $Q = PQ \cap H \lhd PQ$. Therefore PQ contains a minimal nonnilpotent subgroup $F = P_1 Q_1$, where $P_1 \in \mathrm{Syl}_p(F)$ is cyclic and $Q_1 = F' \in \mathrm{Syl}_q(F)$. Then $|Q_1| = q^{b+c}$, where b is the order of q modulo p and $q^c = |Q_1 \cap \mathrm{Z}(F)|$. As above, there is $\mathcal{M} \in \Lambda(F)$ of cardinality $\geq q^b + 1$. Since $q^b \geq p + 1$, we get $|\mathcal{M}| \geq p + 2$. Now assume that $|\mathcal{M}| = p + 2$; then $q^b = p + 1$ so either $p = 2$ and $q = 3$ or $q = 2$ and p is a Mersenne prime.[4]

Statement (c) now follows from Remark 2 and Theorem 116.5(b). □

Proposition 116.8. *Let p be a minimal prime divisor of the order of a group G and let $G = \bigcup_{i=1}^{p+1} A_i$ be an irredundant covering. Then $|G : \bigcap_{i=1}^{p+1} A_i| = p^2$. In particular, $|G : A_i| = p$ for $i = 1, \dots, p + 1$.*

Proof. It follows from Remark 1 that if p is the minimal prime divisor of $|G|$, then it is not covered by p proper subgroups (otherwise, there is in G a proper subgroup of index $< p$, contrary to Lagrange's theorem). One may assume that $|A_1| \geq \cdots \geq |A_{p+1}|$. Then, by Remark 1, $|G : A_1| < p + 1$ so that $|G : A_1| = p$ and hence $A_1 \lhd G$.

First assume that all A_i are maximal in G. Set $|G| = g$ and $|G : A_i| = k_i$, where $i = 2, \dots, p + 1$. Note that $k_i \geq p$ for all i. We have

$$G = A_1 \cup \left(\bigcup_{i=2}^{p+1} (A_i - A_1) \right). \tag{4}$$

[3] If $G \cong \mathrm{A}_4$, the alternating group of degree 4, $p = 2$, then $\gamma(G) = 2^2 + 1$.

[4] If $G \cong \mathrm{A}_4$ and $p = 3$, then $\gamma(G) = 5 = 3 + 2$.

Further, $G = A_1 A_i$ for $i > 1$. Since $A_i - A_1 = A_i - (A_i \cap A_1)$ and $|A_i : (A_i \cap A_1)| = |G : A_1| = p$ so that

$$|G : (A_i \cap A_1)| = |G : A_i||A_i : (A_i \cap A_1)| = pk_i \quad \text{for } i > 1,$$

we obtain

$$|A_i - A_1| = |A_i - (A_i \cap A_1)| = \frac{g}{k_i} - \frac{g}{pk_i} = \frac{g}{k_i}\left(1 - \frac{1}{p}\right).$$

The right-hand side of formula (4) contains v elements, where

$$v \leq \frac{g}{p} + \left(1 - \frac{1}{p}\right)\sum_{i=2}^{p+1} \frac{g}{k_i} \leq \frac{g}{p} + \left(1 - \frac{1}{p}\right)\sum_{i=2}^{p+1} \frac{g}{p} = \frac{g}{p} + \frac{g}{p}\left(1 - \frac{1}{p}\right)p = g.$$

Since $v = g$, it follows that (4) is a partition of G and $k_i = p$ for all i. In this case, $|G : \bigcap_{i=1}^{p+1} A_i| = p^2$.

Now let $A_i \leq B_i < G$, where B_i are maximal in G for all i. Then $G = \bigcup_{i=1}^{p+1} B_i$ is an irredundant covering of G by the first sentence of the proof, and so $|G : B_i| = p$ for all i by the previous paragraph. If $A_i < B_i$ for some i, then, taking in the above displayed formula $A_j = B_j$ for $j \neq i$, we get a contradiction. Thus $B_i = A_i$ for all i and so $|G : \bigcup_{i=1}^{p+1} A_i| = p^2$ by the previous paragraph. □

Lemma 116.3(b) is a partial case of Proposition 116.8.

Let G be a non-p-nilpotent group. Then, using Theorem 116.7, one can show the following results:

(a) If $p = 2$, then $\gamma(G) \geq 5$.

(b) If $p > 2$, then $\gamma(G) \geq p + 1$.

(c) If $p > 2$ is a minimal prime divisor of $|G|$, then $\gamma(G) \geq p^2 + 1$.

4^o On the number of maximal subgroups appearing in some coverings of p-groups. In this subsection we consider irredundant coverings of a p-group by k proper subgroups, where $p + 1 < k \leq 2p$.

It is impossible to avoid some repetition in computations (otherwise, the proofs would be unreadable).

Remark 3. We claim that if a p-group G of order $\geq p^3$ is neither cyclic nor Q_8, it admits an irredundant covering by $2p$ subgroups. Indeed, let $T \lhd G$ be such that G/T is abelian of type (p, p). Let $A_1/T, \ldots, A_{p+1}/T$ be all subgroups of order p in G/T. Then $G = \bigcup_{i=1}^{p+1} A_i$ is an irredundant covering. Since G is neither cyclic nor isomorphic to Q_8, one may assume that A_1 is noncyclic (here we use Theorem 1.2 which implies that if a p-group contains $> p$ cyclic subgroups of index p, it is isomorphic to Q_8). In this case, there exists in T an A_1-invariant subgroup T_0 such that A_1/T_0

is abelian of type (p, p). Let $T = T_1, T_2, \ldots, T_{p+1}$ be all maximal subgroups of A_1 containing T_0. Then G is covered by $2p$ subgroups $A_2, \ldots, A_{p+1}, T_2, \ldots, T_{p+1}$ since $A_1 \le A_2 \cup (\bigcup_{i=2}^{p+1} T_i)$, and this covering is irredundant.

Lemma 116.9. *If a p-group G admits an irredundant covering by $p+2$ subgroups $A_1, \ldots, A_{p+2}$, then*

(a) *If $p > 2$, then at least $p+1$ of the A_i's are maximal in G.*

(b) *If $p = 2$, then at least two of the A_i's are maximal in G.*

Proof. Let $|A_1| \ge \cdots \ge |A_{p+2}|$ and $|G| = p^n$. By Remark 1.1, we get $|G : A_1| = p$. Assume that $|G : A_{p+1}| > p$. Then

$$\begin{aligned} p^n &= \left|\bigcup_{i=1}^{p+2} A_i\right| \le |A_1| + \sum_{i=2}^{p} |A_i - A_1| + \sum_{i=p+1}^{p+2} |A_i - A_1| \\ &= p^{n-1} + (p-1)(p^{n-1} - p^{n-2}) + 2(p^{n-2} - p^{n-3}) \\ &= p^n - p^{n-3}(p^2 - 3p + 2) \\ &= p^n - p^{n-3}(p-1)(p-2). \end{aligned}$$

If $p > 2$, then $p^n \le p^n - p^{n-3}(p-1)(p-2) < p^n$, which is a contradiction. Thus, if $p > 2$, then at least $p+1$ subgroups A_i are maximal in G, completing this case.

Now let $p = 2$ and assume that $|A_2| < 2^{n-1}$. Then

$$\begin{aligned} 2^n &= \left|\sum_{i=1}^{4} A_i\right| \le |A_1| + \sum_{i=2}^{4} |A_i - A_1| = 2^{n-1} + 3(2^{n-2} - 2^{n-3}) \\ &= 2^{n-1} + 3 \cdot 2^{n-3} = 7 \cdot 2^{n-3} < 2^n, \end{aligned}$$

a contradiction. Thus, if $p = 2$, then at least two A_i are maximal in G. □

Let $G = \bigcup_{i=1}^{4} A_i$ be an irredundant covering of a 2-group G of order $2^n > 2^3$, $|A_1| \ge |A_2| \ge |A_3| \ge |A_4|$. We claim that if $|G : A_3| = 2$, then $|G : A_4| = 2$ so all A_i are maximal in G. Then we have

$$G = A_1 \cup (A_2 - A_1) \cup (A_3 - A_1 - A_2) \cup (A_4 - A_1 - A_2 - A_3). \tag{5}$$

Assume that $|G : A_4| > 2$. We have $|G : (A_1 \cap A_2 \cap A_3)| = 2^3$ (Lemma 116.3) hence $|A_3 - A_1 - A_2| = 2^{n-3}$. Further,

$$\begin{aligned} A_3 - A_1 - A_2 &= (A_3 - A_1) - \big((A_3 - A_1) \cap A_2\big) \\ &= A_3 - (A_3 - A_1) - \big((A_3 \cap A_2) - (A_1 \cap A_2)\big) \\ &= A_3 - (A_3 - A_1) - \big((A_3 \cap A_3) - (A_3 \cap A_1 \cap A_2)\big). \end{aligned}$$

It follows that

$$|A_3 - A_1 - A_2| = 2^{n-1} - 2^{n-2} - (2^{n-2} - 2^{n-3}) = 2^{n-3}.$$

Now it is clear that $|A_4 - A_1 - A_2 - A_3| < 2^{n-3}$. Therefore the right-hand side of formula (5) contains v elements, where

$$v < 2^{n-1} + 2^{n-2} + 2^{n-3} + 2^{n-3} = 2^n,$$

which is a contradiction. Thus, in the case under consideration, either exactly two or four of the A_i's are maximal in G.

Let G be a 2-group which is not generated by two elements. We claim that then G admits an irredundant covering $G = \bigcup_{i=1}^{4} A_i$, where $A_i \in \Gamma_1$ for all i. Without loss of generality one may assume that $\Phi(G) = \{1\}$. Let $A_1, A_2 \in \Gamma_1$ be distinct, and set $T = A_1 \cap A_2$. Let $T < A_3 \in \Gamma_1 - \{A_1, A_2\}$ and let $S < T$ be of index 2; then $A_3/S \cong \mathrm{E}_4$. Let $T/S, T_1/S, T_2/S < A_3/S$ be of index 2. As $G/T_i \cong \mathrm{E}_4$, there are distinct $B_1, B_2 \in \Gamma_1 - \{A_3\}$ such that $B_i \cap A_3 = T_i$, $i = 1, 2$. Since A_3 is a subset of the set $A_1 \cup B_1 \cup B_2$ (indeed, $A_3 = T \cup T_1 \cup T_2$ is a subset of $A_1 \cup B_1 \cup B_2$), it follows that $G = A_1 \cup A_2 \cup B_1 \cup B_2$ is a covering (indeed, by the above, $G = A_1 \cup A_2 \cup A_3$ is a subset of $A_1 \cup A_2 \cup B_1 \cup B_2$). Due to the fact the intersection of any three distinct elements of the set $\{A_1, A_2, B_1, B_2\}$ has index p^3 in G, our covering is irredundant (Lemma 116.3(b)).

Similarly, if $p > 2$ and a p-group G is not generated by two elements, then it admits an irredundant covering by $2p$ maximal subgroups.

Lemma 116.10. *Suppose that A, B, C, D are pairwise distinct maximal subgroups of a p-group G of order p^n such that $|G : (A \cap B \cap C)| = p^3$. Then*

$$|A \cup B \cup C| = 3p^{n-1} - 3p^{n-2} + p^{n-3}, \tag{6}$$

$$|D - (A \cup B \cup C)| \leq p^{n-1} - 3p^{n-2} + 3p^{n-3} - p^{n-4}. \tag{7}$$

Proof. Note that if distinct $U, V < G$ are maximal, then $|G : (U \cap V)| = p^2$. By the inclusion-exclusion identity,

$$\begin{aligned} |A \cup B \cup C| &= (|A| + |B| + C|) - (|A \cap B| + |B \cap C| + |C \cap A|) + |A \cap B \cap C| \\ &= 3p^{n-1} - 3p^{n-2} + p^{n-3}, \end{aligned}$$

proving (6).

By hypothesis, $A \cap B \neq B \cap C \neq C \cap A$ (if, for example, $A \cap B = A \cap C$, then $A \cap B = (A \cap B) \cap (A \cap C) = A \cap B \cap C$, a contradiction since $|A \cap B| = p^{n-2} > p^{n-3} = |A \cap B \cap C|$). We have

$$D - (A \cup B \cup C) = D - (D \cap (A \cup B \cup C)), \tag{8}$$

and so

$$D - (A \cup B \cup C) = D - \big((D \cap A) \cup (D \cap B) \cup (D \cap C)\big).$$

By the inclusion-exclusion identity,

$$\begin{aligned}|(D \cap A) \cup (D \cap B) \cup (D \cap C)| &= \big(|D \cap A| + |D \cap B| + |D \cap C|\big) \\ &\quad - \big(|D \cap A \cap B| + |D \cap A \cap C| + |D \cap B \cap C|\big) \\ &\quad + |D \cap A \cap B \cap C|.\end{aligned}$$

If $A \cap B \subset D$, then $D \cap A \cap B \cap C = D \cap C$ has order p^{n-2}, a contradiction since $A \cap B \cap C \supseteq D \cap A \cap B \cap C$ has order p^{n-3} by hypothesis. Thus $A \cap B \not\subseteq D$, and the same is true for $A \cap C$ and $B \cap C$. Then, by the product formula and the previous displayed formula, we have

$$\begin{aligned}|D \cap A \cap B| = |D \cap A \cap C| = |D \cap B \cap C| &= p^{n-3}, \\ |D \cap (A \cup B \cup C)| = |(D \cap A) \cup (D \cap B) \cup (D \cap C)| &\\ = 3p^{n-2} - 3p^{n-3} + |D \cap A \cap B \cap C|.&\end{aligned}$$

Since $|D \cap A \cap B \cap C| \in \{p^{n-3}, p^{n-4}\}$, we obtain

$$|D \cap (A \cup B \cup C)| \geq 3p^{n-2} - 3p^{n-3} + p^{n-4}.$$

Now (7) follows from (8). □

Theorem 116.11. *If a group of order p^n admits an irredundant covering by $p+2$ subgroups, then $p = 2$.*

Proof. Assume that a group G of order p^n admits an irredundant covering by $p + 2$ proper subgroups $A_1, \ldots, A_{p+2}$ and $p > 2$. By Lemma 116.9(a), one may assume that $A_1, \ldots, A_{p+1}$ are maximal in G. Since $G \neq \bigcup_{i=1}^{p+1} A_i$, we have $|G : \bigcap_{i=1}^{p+1} A_i| \geq p^3$. One may assume, without loss of generality, that $|G : (A_1 \cap A_2 \cap A_3)| = p^3$. We may also assume that $|G : A_{p+2}| = p$. Then, by (6), we have

$$|A_1 \cup A_2 \cup A_3| = 3p^{n-1} - 3p^{n-2} + p^{n-3} \tag{9}$$

and, for $i > 3$,

$$|A_i - (A_1 \cup A_2 \cup A_3)| < p^{n-1} - 3p^{n-2} + 3p^{n-3} = p^{n-3}(p^2 - 3p + 3) \tag{10}$$

by (7).

Set $A_1 \cup A_2 \cup A_3 = U$. We have

$$G = U \cup \left(\bigcup_{i=4}^{p+2} (A_i - U)\right). \tag{11}$$

Therefore, taking into account (9) and (10), we obtain

$$\begin{aligned} |G| = p^n &\le (3p^{n-1} - 3p^{n-2} + p^{n-3}) + (p-1)p^{n-3}(p^2 - 3p + 3) \\ &= p^n - p^{n-3}(p^2 - 3p + 2) \\ &= p^n - p^{n-3}(p-1)(p-2) < p^n \end{aligned}$$

since $p > 2$, a final contradiction. Thus we must have $p = 2$. □

Proposition 116.12. *If a p-group G is covered by at most $k \le 2p$ proper subgroups $A_1, \dots, A_k$ (we do not assume that this covering is irredundant), then at least p of these subgroups are maximal in G. If $p > 3$ and $p + 2 < k < 2p$, then at least $p + 1$ summands in our covering are maximal in G.*

Proof. (i) In view of Lemma 116.9, one may assume that $p > 2$. Let $|A_1| \ge \cdots \ge |A_k|$. Then $|G : A_1| = p$ as $p > 2$ (Remark 1). Since we do not assume that our covering is irredundant, one can add new summands to obtain $k = 2p$. We also may assume, by way of contradiction, that $A_1, \dots, A_{p-1}$ are maximal in G and $A_p, \dots, A_{2p}$ have index p^2 in G. Indeed, if, for example, $|G : A_i| > p^2$ $(i > p-1)$, one can replace A_i by a subgroup that contains A_i and has index p^2 in G. If, for example, $|G : A_i| > p$ $(i < p)$, one can replace A_i by a maximal subgroup of G that contains A_i. We have

$$G = A_{p-1} \cup \left(\bigcup_{i=1}^{p-2} (A_i - A_{p-1}) \right) \cup \left(\bigcup_{i=p}^{2p} (A_i - A_{p-1}) \right). \tag{12}$$

The right-hand side of formula (12) contains v elements, where

$$\begin{aligned} v &\le p^{n-1} + (p-2)(p^{n-1} - p^{n-2}) + (p+1)(p^{n-2} - p^{n-3}) \\ &= p^n - p^{n-3}(p-1)^2 < p^n = |G|, \end{aligned}$$

a contradiction since $v = |G| = p^n$. Thus at least p subgroups A_i $(i \le 2p)$ are maximal in G.

(ii) To prove the last assertion, one may assume, by way of contradiction, that $A_1, \dots, A_p$ are maximal in G and $|G : A_i| = p^2$ for $i > p$ (see (i)). (Here $p > 3$ since $3 + 2 = 2 \cdot 3 - 1$.) We may also assume that $k = 2p - 1$ (if $k < 2p - 1$, one can add to our union $2p - 1 - k$ new summands of order p^{n-2}). Then, as above, we obtain

$$\begin{aligned} |G| = p^n &\le p^{n-1} + (p-1)(p^{n-1} - p^{n-2}) + (p-1)(p^{n-2} - p^{n-3}) \\ &= p^{n-1} + (p-1)(p^{n-1} - p^{n-3}) \\ &= p^n - p^{n-3}(p-1) < p^n, \end{aligned}$$

a contradiction. □

Proposition 116.13. *Suppose that a p-group G of order $p^n \geq p^4$, $p > 2$, is covered by k proper subgroups, say $A_1, \ldots, A_k$, where $p + 2 < k \leq 2p$. Let, in addition, any $p + 2$ subgroups A_i do not cover G, $|G : A_i| = p$ for $i \leq p$ and $|G : A_i| > p$ for $i > p$. Then*

(a) $k = 2p$ *and our covering is irredundant.*

(b) $|\bigcap_{i=1}^{p} A_i| = p^{n-2}$.

(c) $|A_i| = p^{n-2}$ *for* $i > p$.

(d) $|\bigcap_{i=p+1}^{2p} A_i| = p^{n-3}$.

Proof. By the second assertion of Proposition 116.12, we get $k = 2p$ so (a) is true.

We have

$$G = A_p \cup \left(\bigcup_{i=1}^{p-1} (A_i - A_p) \right) \cup \left(\bigcup_{i=p+1}^{2p} (A_i - A_p) \right). \tag{13}$$

(c) Assume that $|A_{p+1}| \geq \cdots \geq |A_{2p}|$ and $|A_{2p}| < p^{n-2}$. Then the right-hand side of (13) contains v elements, where

$$\begin{aligned} v &\leq p^{n-1} + (p-1)(p^{n-1} - p^{n-2}) + (p-1)(p^{n-2} - p^{n-3}) + (p^{n-3} - p^{n-4}) \\ &= p^{n-1} + (p-1)(p^{n-1} - p^{n-3}) + (p^{n-3} - p^{n-4}) \\ &= p^n - p^{n-4}(p-1)^2 < p^n = |G|, \end{aligned}$$

which is a contradiction. This proves (c).

(b, d) We have $|G : A_i| = p^2$ for $i > p$ by (c). In this case, the right-hand side of (13) contains v elements, where

$$v \leq p^{n-1} + (p-1)(p^{n-1} - p^{n-2}) + p(p^{n-2} - p^{n-3}) = p^n = |G|,$$

so (13) is a partition. This implies (b) and (d). □

A similar argument shows that if a p-group G is covered by p^2 proper subgroups, then at least two of these subgroups are maximal in G. Indeed, if only one summand of our covering is maximal in G (see Remark 1), we obtain

$$p^n \leq p^{n-1} + (p^2 - 1)(p^{n-2} - p^{n-3}) = p^n - p^{n-3}(p-1) < p^n,$$

a contradiction.

Corollary 116.14. *If a nonabelian p-group G has at most $2p$ pairwise noncommuting elements, then the centralizers of at least p of these elements are maximal in G.*

Remark 4. Let G be a group of maximal class and order p^{n+2}, $n \geq 2$, with abelian subgroup A of index p. In this case, every $x \in G - A$ satisfies $|\mathrm{C}_G(x)| = p^2$ (indeed,

$C_A(y) = Z(G)$ is of order p and $y^p \in Z(G)$ for all $y \in G - A$), and the number of maximal abelian subgroups of order p^2 not contained in A is equal to

$$\frac{|G - A|}{p(p-1)} = p^n$$

(indeed, if B is such a subgroup, then $|B - A| = p(p-1)$). These p^n subgroups together with A cover G and this covering is irredundant. The so-obtained set of cardinality $p^n + 1$ is contained in $\Lambda(G)$. It is easy to see that $\gamma(G) = p^n + 1$.

Remark 5. Let G be a nonabelian p-group. If $x \in G$ and A_x is a maximal abelian subgroup of $C_G(x)$, then A_x is also a maximal abelian subgroup of G. Let $\mathcal{M} \in \Lambda(G)$. Take in $C_G(x)$ a maximal abelian subgroup A_x for every $x \in \mathcal{M}$ (indeed, if $B > A_x$ is abelian, then, by choice, $B \not\leq C_G(x)$, a contradiction). Then $|\{A_x \mid x \in \mathcal{M}\}| = |\mathcal{M}|$. It follows that G has at least $\gamma(G)$ maximal abelian subgroups. If the group G has exactly $p + 1$ maximal abelian subgroups, say $A_1, \ldots, A_{p+1}$, they cover G. In this case, $A_1, \ldots, A_{p+1}$ are maximal in G (Lemma 116.2(b)) and G has the structure described in Theorem 116.6(b).

Remark 6. Let $B_1, \ldots, B_n$ be all maximal abelian subgroups of a nonabelian group G. Then $\gamma(G) \leq n$ since $G = \bigcup_{i=1}^n B_i$ (it is possible that this covering may be redundant). If $B_i \cap B_j = Z(G)$ for all $i \neq j$ (in this case, the considered covering is irredundant), then $\gamma(G) = n$. Indeed, take $x_i \in B_i - Z(G)$ for all i. We claim that $\{x_1, \ldots, x_n\} \in \Lambda(G)$ (indeed, if $\{x, x_1, \ldots, x_n\} \subset G$, then $x \in B_i$ for some i so $xx_i = x_i x$). For example, let G be a Sylow 2-subgroup of the simple Suzuki group $Sz(q)$, where $q = 2^{2m+1}$. Then $Z(G) = \Phi(G)$ has index 2^{2m+1} in G. If $A < G$ is maximal abelian, then $|A : Z(G)| = 2$. It follows that there is $\mathcal{M} \in \Lambda(G)$ of cardinality $2^{2m+1} - 1$; moreover, all members of the set $\Lambda(G)$ have the same cardinality.

Remark 7. Let $G = A * B$ be a central product of nonabelian groups A and B. Further, let $\mathcal{M} = \{a_1, \ldots, a_m\} \in \Lambda(A)$ and $\mathcal{N} = \{b_1, \ldots, b_n\} \in \Lambda(B)$. Then $m - 1 + n$ elements of the set

$$\mathcal{M}_1 = \{a_2, \ldots, a_m, a_1b_1, a_1b_2, \ldots, a_1b_n\}$$

are pairwise noncommuting. We claim that $\mathcal{M}_1 \in \Lambda(G)$. Assume that there exists $x \in G - \mathcal{M}_1$ such that all elements of the set $\mathcal{M}_1 \cup \{x\}$ are pairwise noncommuting. We have $x = ab$, where $a \in A$ and $b \in B$. For $i > 1$ we have $1 \neq [ab, a_i] = [a, a_i]$ so that $a \in D = A - \bigcup_{i=2}^n C_A(a_i)$. By Lemma 116.1(b), the subgroup $\langle D \rangle$ is abelian so $[a, a_1] = 1$ since $a_1 \in D$. For $i = 1, \ldots, n$ we have $1 \neq [ab, a_1b_i] = [ab, b_i] = [b, b_i]$. We conclude that $n + 1 > \gamma(B)$ elements $b, b_1, \ldots, b_n \in B$ are pairwise noncommuting, which is a contradiction. It is easy to deduce from this by induction that if G is an extraspecial group of order p^{2m+1}, then $\gamma(G) \geq mp + 1$.

It follows from Remark 7 and Lemma 116.1(a) that if G is a nonabelian p-group such that $\gamma(G) \leq 2p$, then $C_G(H)$ is abelian for all minimal nonabelian $H < G$.

Problems

Below we state some related problems.

Problem 1. Classify the 2-groups which do not contain five pairwise noncommuting elements. (See Lemma 1.3 and Theorem 116.11.)

Problem 2. Does there exist a p-group G admitting an irredundant covering by n subgroups, where $p+1 < n < 2p$? If 'yes', classify such the groups.

Problem 3. Describe the set of positive integers n such that there is an elementary abelian p-group admitting an irredundant covering by n maximal subgroups.

Problem 4. Let M, N be groups and $\gamma(M) = m$, $\gamma(N) = n$. Then $\gamma(M \times N) = mn$. (i) Estimate $\gamma(M * N)$ in terms of M, N and $M \cap N$. Consider the case where M, N are p-groups of maximal class. (ii) Find $\gamma(G)$, where G is an extraspecial group of order p^{2m+1}.

Problem 5. Classify the pairs of groups $N \lhd G$ such that $\gamma(G/N) = \gamma(G)$. (The set of such pairs is infinite: let G be a minimal nonabelian p-group with noncyclic center and $N < G$ with $G' \not\leq N$.)

Problem 6. Find $\gamma(\Sigma_{p^n})$, where Σ_{p^n} is a Sylow p-subgroup of the symmetric group S_{p^n} of degree p^n. Deal with the same problem for $\mathrm{UT}(m, p^n)$, a Sylow p-subgroup of the general linear group $\mathrm{GL}(m, p^n)$.

Problem 7. Study the nonabelian p-groups G such that $\mathrm{C}_G(H)$ is abelian for all minimal nonabelian $H \leq G$. (See the paragraph following Remark 7.)

Problem 8. Study the nonnilpotent groups G such that $\Lambda(H) \subseteq \Lambda(G)$ for all minimal nonnilpotent $H \leq G$. (Compare this with Lemma 2.2(b).)

Problem 9. Study the groups that are covered by (i) minimal nonnilpotent subgroups, (ii) minimal nonabelian subgroups, (iii) Frobenius subgroups.

Problem 10. Classify the p-groups that are covered by subgroups of maximal class.

Problem 11. Let H be a proper subgroup of maximal class of a p-group G such that $\Lambda(H) \subset \Lambda(G)$. Study the structure of G.

Problem 12. Find $\gamma(G)$, where $G \in \{\mathrm{A}_n, \mathrm{S}_n\}$ (for example, $\gamma(\mathrm{A}_5) = 21$; see also [Br].)

§117

2-groups all of whose nonnormal subgroups are either cyclic or of maximal class

The 2-groups all of whose nonnormal subgroups are cyclic are completely determined in §16. The first step in classifying the title groups was done by the first author in Theorem A.40.25. We finish the classification of the title groups by proving the following result which solves Problem 1978.

Theorem 117.1. *Let G be a 2-group all of whose nonnormal subgroups are either cyclic or of maximal class. Assume, in addition, that G has a nonnormal subgroup of maximal class. Then we have one of the following possibilities:*

(a) *G is generalized quaternion Q_{2^n}, $n \geq 5$.*

(b) *$G = \langle y, b \mid y^8 = b^4 = 1, b^y = bu, y^2 = ua, u^y = uz, a^y = a^{-1}, a^2 = b^2 = [a,b] = z, [u,a] = [u,b] = 1\rangle$, where G is of order 2^5 and class 3 with $\Omega_2(G) = \langle u\rangle \times \langle a,b\rangle \cong \mathrm{C}_2 \times \mathrm{Q}_8$, $\mathrm{Z}(G) = \langle z\rangle \cong \mathrm{C}_2$, $G' = \langle u,z\rangle \cong \mathrm{E}_4$ and $\Phi(G) = \langle u,a\rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$.*

(c) *G is any 2-group of class 2 with $\Omega_1(G) = G' \cong \mathrm{E}_4$ having a nonnormal quaternion subgroup.*

Conversely, each group in (a), (b) *and* (c) *satisfies the assumptions of our theorem.*

Proof. Let H be any nonnormal subgroup of maximal class. Suppose that H is not generalized quaternion. Let V be a four-subgroup in H. Then $V \trianglelefteq G$ and so $H \cong \mathrm{D}_8$. But H has another four-subgroup $W \neq V$ and W is normal in G. It then follows that $H = \langle V, W\rangle \trianglelefteq G$, a contradiction. Therefore H is generalized quaternion.

If G is of maximal class, then $G \cong \mathrm{Q}_{2^n}$, $n \geq 5$ (part (a) of our theorem), and so we assume in the sequel that G is not of maximal class. This implies that G possesses a normal four-subgroup U and G/U is Dedekindian.

Let Q be a nonnormal subgroup of maximal possible order in G such that $Q \cong \mathrm{Q}_{2^m}$, $m \geq 3$. Set $N = \mathrm{N}_G(Q)$ and $\langle z\rangle = \mathrm{Z}(Q)$ so that $Q < N < G$, $N \trianglelefteq G$ and $z \in \mathrm{Z}(N)$. Then each subgroup X of N with $X > Q$ is normal in G and so N/Q is Dedekindian. If X_1/Q and X_2/Q are two distinct subgroups of order 2 in N/Q, then $X_1 \trianglelefteq G$, $X_2 \trianglelefteq G$ and $X_1 \cap X_2 = Q$, a contradiction. We have proved that $N/Q \neq \{1\}$ is either cyclic or $N/Q \cong \mathrm{Q}_8$.

Let t be any involution in $G - Q$. Since $U = \langle z,t\rangle \trianglelefteq G$ and $U \cap Q = \langle z\rangle$, we have $|(UQ) : Q| = 2$ which implies $t \in N$. On the other hand, $Q/\langle z\rangle \cong \mathrm{D}_{2^{m-1}}$ (if $m \geq 4$)

or $Q/\langle z\rangle \cong \mathrm{E}_4$ (if $m = 3$) and G/U is Dedekindian. Hence $m = 3$ and $Q \cong \mathrm{Q}_8$. Set $L = QU$ so that $L \trianglelefteq G$ and $L/Q = \Omega_1(N/Q)$. Each involution in G is contained in N and so each involution in G is also contained in L. If $\mathrm{C}_L(Q) \leq Q$, then L would be of maximal class (and order 2^4), contrary to the fact that U is a normal four-subgroup in G. Hence $L = V * Q$ with $V \cap Q = \langle z\rangle$. If $V \cong \mathrm{C}_4$, then Q is a unique quaternion subgroup in L. In that case, $Q \trianglelefteq G$, a contradiction. Hence $V \cong \mathrm{E}_4$, $L = \langle t\rangle \times Q$ and $\Omega_1(G) = U = \langle z, t\rangle$.

Set $C = \mathrm{C}_G(Q)$ so that $C \cap L = \langle t, z\rangle$ and $C \trianglelefteq G$. If C does not cover N/Q, then $N/C \cong \mathrm{D}_8$ (since $\mathrm{Aut}(\mathrm{Q}_8) \cong \mathrm{S}_4$), contrary to the fact that G/U is Dedekindian. Thus we get $N = Q * C$ with $Q \cap C = \langle z\rangle$ and $C/\langle z\rangle \cong N/Q$ is either cyclic or quaternion.

Set $Q = \langle v, w\rangle$, where $\langle v\rangle$, $\langle w\rangle$, $\langle vw\rangle$ are three cyclic subgroups of index 2 in Q. Now, $\langle v, t\rangle$, $\langle w, t\rangle$ and $\langle vw, t\rangle$ are normal in G and so $\langle z\rangle \leq \mathrm{Z}(G)$, $|G : \mathrm{N}_G(\langle v\rangle)| \leq 2$, $|G : \mathrm{N}_G(\langle w\rangle)| \leq 2$ and $\mathrm{N}_G(\langle v\rangle) \cap \mathrm{N}_G(\langle w\rangle) = N$. Hence either $|G : N| = 2$ or $|G : N| = 4$ and in the second case $G/N \cong \mathrm{E}_4$, where $\mathrm{N}_G(\langle v\rangle)/N$, $\mathrm{N}_G(\langle w\rangle)/N$ and $\mathrm{N}_G(\langle vw\rangle)/N$ are three distinct subgroups of order 2 in G/N. In any case, there is an element v of order 4 in Q and an element $x \in G - N$ with $x^2 \in N$ so that $v^x = v^\epsilon t$, where $\epsilon \in \{1, -1\}$. Hence $[v, x] = t$ or zt and so, in particular, $\langle z, t\rangle \leq G'$. Clearly, z is not a square in C. Indeed, if there is $y \in C$ with $y^2 = z$, then $o(vy) = 2$, where $v \in Q - \langle z\rangle$ and $y \in C - L$ and so $vy \in N - L$, contrary to $\Omega_1(G) = \langle t, z\rangle$.

(i) First assume $C > \langle t, z\rangle$. Then $C/\langle z\rangle$ is either cyclic of order ≥ 4 or $C/\langle z\rangle \cong \mathrm{Q}_8$. In the first case, there is $c \in C$ such that $\langle c\rangle$ covers $C/\langle z\rangle$ and then (since z is not a square in C) $C = \langle c\rangle \times \langle z\rangle$, $\mathrm{Z}(N) = C$ and $\Omega_1(\langle c\rangle)$ is characteristic in C. It follows that $\Omega_1(\langle c\rangle) \leq \mathrm{Z}(G)$ and $U = \langle t, z\rangle \leq \mathrm{Z}(G)$. Suppose that $C/\langle z\rangle \cong \mathrm{Q}_8$. Then we get $\{1\} \neq C' \leq U = \langle t, z\rangle$. If $C' = U$, then, by a result of O. Taussky (Lemma 1.6), C is of maximal class and order 2^4, a contradiction. Hence $|C'| = 2$ and since C' covers $U/\langle z\rangle$, we have $U = C' \times \langle z\rangle$. Then it follows that $C' \leq \mathrm{Z}(G)$ and so again $U = \langle t, z\rangle \leq \mathrm{Z}(G)$.

We know that G/U is Dedekindian. Assume that G/U is nonabelian, i.e., G/U is Hamiltonian. In that case, G/U has a quaternion subgroup $V/U \cong \mathrm{Q}_8$. Set $W/U = \mathrm{Z}(V/U) = (V/U)'$ so that W is abelian of type $(4, 2)$ and therefore all elements in $W - U$ are of order 4. Let S_1, S_2, S_3 be three maximal subgroups of V which contain U. Then $S_i/U \cong \mathrm{C}_4$ and since $U \leq \mathrm{Z}(G)$, each S_i is an abelian maximal subgroup of V, $i = 1, 2, 3$. By Exercise P1, $|V'| = 2$. On the other hand, V' covers W/U and so there are involutions in $W - U$, a contradiction. Hence G/U is abelian and so $G' = U = \Omega_1(G) \leq \mathrm{Z}(G)$. We have obtained the groups from part (c) of our theorem.

(ii) Now assume $C = \langle t, z\rangle = U$ so that $N = L = \langle t\rangle \times Q \cong \mathrm{C}_2 \times \mathrm{Q}_8$ and $|G| = 2^5$ or 2^6. Suppose, in addition, that $\Omega_2(G) = N$. In that case, Theorem 52.1(d) implies that G is a unique group of order 2^5 with $\mathrm{Z}(G) = \langle z\rangle$, $G' = \langle t, z\rangle$ and $\Phi(G) \cong \mathrm{C}_4 \times \mathrm{C}_2$ which appears in part (b) of our theorem. From now on we may assume that there is an element $x \in G - N$ of order 4 and so $1 \neq x^2 \in U$. In this case,

we obtain $|(G/U) : \Omega_1(G/U)| \leq 2$ which implies that the Dedekindian group G/U cannot be Hamiltonian and so G/U is abelian which gives $G' = U$. We have also $\langle z \rangle \leq \mathrm{Z}(G) \leq U$. Since $\Omega_1(G) = U$, the case $U\langle x \rangle \cong \mathrm{D}_8$ is not possible and so x centralizes U. Because x normalizes $N = L$ and does not normalize Q, there is an element v of order 4 in Q with $v^2 = z$ such that x does not normalize $\langle v \rangle$. On the other hand, $\langle v, t \rangle \trianglelefteq G$ and so we may set $v^x = vt$ for a suitable element $t \in U - \langle z \rangle$ which gives $[v, x] = t$. But $U = \langle z, t \rangle \leq \mathrm{Z}(N\langle x \rangle)$ and so $\langle v, x \rangle$ is minimal nonabelian with $(\langle v, x \rangle)' = \langle [v, x] \rangle = \langle t \rangle$. Also, $\langle v, x \rangle \geq \langle t, z \rangle = U$ and so $\langle v, x \rangle \trianglelefteq G$. This implies that $(\langle v, x \rangle)' = \langle t \rangle \leq \mathrm{Z}(G)$ and so $\mathrm{Z}(G) = \langle t, z \rangle$. We have again obtained some groups from part (c) of our theorem. □

§118

Review of characterizations of p-groups with various minimal nonabelian subgroups

Recall that a group G is said to be *minimal nonabelian* if it is nonabelian but all its maximal subgroups are abelian.

A p-group H is *minimal nonabelian* if and only if $H = \langle a, b\rangle$ is two-generated and $|H'| = p$, i.e., $[a, b]^p = [a, b, a] = [a, b, b] = 1$. In that case, $\Phi(H) = \mathrm{Z}(H)$ so that $|H : \mathrm{Z}(H)| = p^2$.

Exercise 1.8(a) ([Red] and Lemma 65.1). Let G be a minimal nonabelian p-group. Then $|G'| = p$ and G/G' is abelian of rank two and G is one of the following groups:

(a) $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1,\ a^b = a^{1+p^{m-1}}\rangle$, $m \geq 2$, $n \geq 1$, $|G| = p^{m+n}$ (G is metacyclic).

(b) $G = \langle a, b \mid a^{p^m} = b^{p^n} = c^p = 1,\ [a, b] = c,\ [a, c] = [b, c] = 1\rangle$ is nonmetacyclic of order p^{m+n+1} and if $p = 2$, then $m + n > 2$. Next, G' is a maximal cyclic subgroup of G.

(c) $G \cong \mathrm{Q}_{2^3}$.

Our group G is nonmetacyclic if and only if G' is a maximal cyclic subgroup of G.

Proposition 10.19. *Let G be a metacyclic p-group containing a nonabelian subgroup B of order p^3. Then* (a) *if $p = 2$, then G is of maximal class,* (b) *if $p > 2$, then $|G| = p^3$, i.e., $G = B$.*

Proposition 10.28. *A nonabelian p-group is generated by its minimal nonabelian subgroups.*

Theorem 10.33. *All minimal nonabelian subgroups of a 2-group are dihedral if and only if $G = \langle x\rangle \cdot A$, where $a^x = a^{-1}$ for all $a \in A$.*

Theorem 10.34(a). *A p-group G, $p > 2$, is generated by minimal nonabelian subgroups of exponent p unless it contains a subgroup $\cong \Sigma_{p^2} \in \mathrm{Syl}_p(\mathrm{S}_{p^2})$.*

The following result generalizes Theorem 10.28 and plays an important role in what follows.

Lemma 57.1. *Let G be a nonabelian p-group and let A be any maximal abelian normal subgroup of G. Then for each $x \in G - A$ there is $a \in A$ such that $\langle a, x\rangle$ is minimal nonabelian.*

It follows that minimal nonabelian subgroups of G cover the set $G - A$ and so they generate G (see also Theorem 10.28). We have the following open problem. *Classify finite p-groups which are covered by its minimal nonabelian subgroups.* We have solved only the following two special cases of this problem.

Lemma 65.2(a). *Let G be a nonabelian p-group such that $G' \leq \Omega_1(\mathrm{Z}(G))$ and $\mathrm{d}(G) = 2$. Then G is minimal nonabelian.*

Theorem 76.A. *If G is a nonabelian p-group containing $\leq p^2 + p + 1$ minimal nonabelian subgroups, then all its subgroups of index p^3 are abelian.*

Theorem 92.1. *Let G be a nonabelian p-group such that for each minimal nonabelian subgroup H of G and each $x \in H - \mathrm{Z}(G)$ we have $\mathrm{C}_G(x) \leq H$. Then G is one of the following groups:*

(a) *G is minimal nonabelian.*

(b) *$p = 2$, $\mathrm{d}(G) = 3$ and*

$$G = \langle a, b, c \mid a^4 = b^4 = c^4 = 1,\ [a,b] = c^2,\ [a,c] = b^2c^2,\ [b,c] = a^2b^2,$$
$$[a^2,b] = [a^2,c] = [b^2,a] = [b^2,c] = [c^2,a] = [c^2,b] = 1\rangle,$$

where G is a special 2-group of order 2^6 with

$$\langle a^2, b^2, c^2\rangle = G' = \mathrm{Z}(G) = \Phi(G) = \Omega_1(G) \cong \mathrm{E}_8$$

and G is isomorphic to an S_2-subgroup of the simple group $\mathrm{Sz}(8)$.

(c) *$p > 2$, $\mathrm{d}(G) = 2$, G is of order p^5 and*

$$G = \langle a, x \mid a^{p^2} = x^{p^2} = 1,\ [a,x] = b,\ [a,b] = y_1,\ [x,b] = y_2,$$
$$b^p = y_1^p = y_2^p = [a,y_1] = [x,y_1] = [a,y_2] = [x,y_2] = 1,$$
$$a^p = y_1^\alpha y_2^\beta,\ x^p = y_1^\gamma y_2^\delta\rangle,$$

*where in case $p > 3$, $4\beta\gamma + (\delta - \alpha)^2$ is a quadratic non-residue (*mod p*). Here*

$$\Phi(G) = G' = \langle b, y_1, y_2\rangle = \Omega_1(G) \cong \mathrm{E}_{p^3},$$
$$\mathrm{Z}(G) = \mathrm{K}_3(G) = \mathfrak{V}_1(G) = \langle y_1, y_2\rangle \cong \mathrm{E}_{p^2}.$$

Conversely, all the above groups satisfy the assumptions of the theorem.

Theorem 92.2. *Let G be a nonabelian p-group such that whenever A is a maximal subgroup of any minimal nonabelian subgroup H in G, then A is also a maximal abelian subgroup of G. Then each abelian subgroup of G is contained in a minimal nonabelian subgroup and one of the following holds:*

(a) *G is minimal nonabelian.*

(b) *G is metacyclic.*

(c) *G is isomorphic to the group of order 2^6 defined in Theorem 92.1*(b).

(d) *G is isomorphic to a group of order p^5 defined in Theorem 92.1*(c).

Theorem 92.2 is in fact a proper generalization of Theorem 92.1 since the assumption of Theorem 92.1 implies the assumption of Theorem 92.2 but not vice versa. The assumptions of both Theorems 92.1 and 92.2 imply that each abelian subgroup of G is contained in a minimal nonabelian subgroup and so in both cases G is indeed covered by its minimal nonabelian subgroups.

If we know something about the structure of minimal nonabelian subgroups of a 2-group G, then we are able in some cases to determine the structure of G. In studying 2-groups all of whose minimal nonabelian subgroups are of exponent 4 (which, in general, is still an unsolved problem) the following lemma is crucial.

Lemma 57.2. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are of exponent 4 and let A be a maximal normal abelian subgroup of G. Then all elements in $G-A$ are of order ≤ 4 and so either $\exp(A) = 2$ or $\exp(A) = \exp(G)$. If $x \in G - A$ with $x^2 \in A$, then x inverts each element in $\mho_1(A)$ and in $A/\Omega_1(A)$. If $\exp(G) > 4$, then either G/A is cyclic of order ≤ 4 or $G/A \cong \mathrm{Q}_8$.*

Theorem 90.1. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to D_8 or Q_8. Then G is one of the following groups:*

(a) *G is generalized dihedral (i.e., $|G : \mathrm{H}_2(G)| = 2$).*

(b) *$G = H\mathrm{Z}(G)$, where H is of maximal class and $\mho_1(\mathrm{Z}(G)) \leq \mathrm{Z}(H)$.*

(c) *$G = H\mathrm{Z}(G)$, where H is extraspecial and $\mho_1(\mathrm{Z}(G)) \leq \mathrm{Z}(H)$.*

Theorem 57.3. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to $\mathscr{H}_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1}\rangle$. Then the following holds:*

(a) *If G is of exponent ≥ 8, then G has a unique abelian maximal subgroup A. We have $\exp(A) \geq 8$ and $E = \Omega_1(A) = \Omega_1(G) = \mathrm{Z}(G)$ is of order ≥ 4. All elements in $G - A$ are of order 4 and if v is one of them, then $\mathrm{C}_A(v) = E$ and v inverts $\Phi(A)$ and on A/E.*

(b) *If G is of exponent 4, then $G = K \times V$, where $\exp(V) \leq 2$ and for the group K we have one of the following possibilities:*

  (b1) *$K \cong \mathrm{H}_2$ is of order 2^4.*

  (b2) *K is the minimal nonmetacyclic group of order 2^5 (see Theorem 66.1(d)).*

  (b3) *K is a unique special group of order 2^6 with $\mathrm{Z}(K) \cong \mathrm{E}_4$ in which every maximal subgroup is minimal nonmetacyclic of order 2^5 (from (b2)):*

$$K = \langle a, b, c, d \mid a^4 = b^4 = 1,\ c^2 = a^2b^2,\ [a, b] = 1,\ a^c = a^{-1},\ b^c = a^2b^{-1},\ d^2 = a^2,\ a^d = a^{-1}b^2,\ b^d = b^{-1},\ [c, d] = 1\rangle.$$

  (b4) *K is a splitting extension of $B = B_1 \times \cdots \times B_m$, $m \geq 2$, with a cyclic group $\langle b\rangle$ of order 4, where $B_i \cong \mathrm{C}_4$, $i = 1, 2, \ldots, m$, and b inverts each element of B (and b^2 centralizes B).*

Theorem 57.4. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to* $\mathrm{H}_{16} = \langle a, t \mid a^4 = t^2 = 1, [a,t] = z, z^2 = [a,z] = [t,z] = 1\rangle$. *Then $\Omega_1(G)$ is a self-centralizing elementary abelian subgroup and G is of exponent* 4. *Moreover, the centralizer of any element of order* 4 *is abelian of type* $(4, 2, \ldots, 2)$.

Theorem 57.5. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to* $\mathrm{H}_{32} = \langle a, b \mid a^4 = b^4 = 1, [a,b] = z, z^2 = [a,z] = [b,z] = 1\rangle$. *Then $\Omega_1(G) \leq \mathrm{Z}(G)$ and G is of exponent* 4 *and class* 2.

Theorem 57.6. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to* $\mathrm{M}_{16} = \langle a, t \mid a^8 = t^2 = 1, a^t = a^5\rangle$. *Then $E = \Omega_1(G)$ is elementary abelian and if A is a maximal normal abelian subgroup of G containing E, then A is of type $(2^s, 2, \ldots, 2)$, $s \geq 2$, $|G : A| \leq 4$, each element x in $G - A$ is of order* 8, $|E : \mathrm{C}_E(x)| = 2$, *$x$ inverts each element in A/E and in $\mho_1(A)$ and we have the following possibilities:*

(a) *$s > 2$ in which case $|G : A| = 2$ and $G/E \cong \mathrm{Q}_{2^s}$ is generalized quaternion of order 2^s.*

(b) *$s = 2$ in which case either $G \cong \mathrm{M}_{16} \times V$ with $\exp(V) \leq 2$ or $G/E \cong \mathrm{Q}_8$ and $|G : A| = 4$.*

In Theorem 92.6 we classify nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic to Q_8 or $\mathrm{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1}\rangle$. This theorem generalizes a result of N. Blackburn concerning p-groups G which possess nonnormal subgroups and such that the intersection of all nonnormal subgroups is nontrivial (Corollary 92.7). Namely, it is easy to see that in such p-groups G we must have $p = 2$ and each minimal nonabelian subgroup of G is isomorphic to Q_8 or H_2.

Theorem 92.6. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to* Q_8 *or* $\mathrm{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1}\rangle$. *Then the following holds:*

(a) *If G is of exponent > 4, then G has a unique abelian maximal subgroup A, $|G'| > 2$ and all elements in $G - A$ are of order* 4. *We have $\Omega_1(A) = \Omega_1(G) \leq \mathrm{Z}(G)$ and if $x \in G - A$, then x inverts each element of $A/\Omega_1(A)$.*

(b) *If G is of exponent* 4, *then $G = K \times V$, where $\exp(V) \leq 2$ and for the group K we have one of the following possibilities:*

  (b1) *$K \cong \mathrm{Q}_8$ or $K \cong \mathrm{H}_2$.*

  (b2) *$K = \langle a, b, c \mid a^4 = b^4 = c^4 = [a,b] = 1, c^2 = a^2, [a,c] = b^2, [b,c] = a^2\rangle$ is the minimal nonmetacyclic group of order 2^5.*

  (b3) *K is a unique special group of order 2^6 with $\mathrm{Z}(K) \cong \mathrm{E}_4$ given in Theorem 57.3*(b3) *in which every maximal subgroup is isomorphic to the minimal nonmetacyclic group of order 2^5 (from* (b2)*).*

  (b4) *$K \cong \mathrm{Q}_8 \times \mathrm{C}_4$.*

(b5) $K \cong \mathrm{Q}_8 \times \mathrm{Q}_8$.

(b6) $G = K \times V$ *has an abelian maximal subgroup* B *of exponent* 4 *and an element* $v \in G - B$ *of order* 4 *which inverts each element of* B.

(b7) $K = Q * C$ *is a central product of* $Q = \langle a, b\rangle \cong \mathrm{Q}_8$ *and* $C = \langle c, d \mid c^4 = d^4 = 1,\ c^d = c^{-1}\rangle \cong \mathrm{H}_2$ *with* $Q \cap C = \langle c^2 d^2\rangle = \mathrm{Z}(Q)$, *where* K *is special of order* 2^6 *and* $\mathrm{Z}(K) = \Omega_1(K) \cong \mathrm{E}_4$.

Conversely, in each of the above groups in part (b) *every minimal nonabelian subgroup is isomorphic to* Q_8 *or* H_2.

Corollary 92.7 ([Bla7]). *Let* G *be a finite* p*-group which possesses nonnormal subgroups and let* $\mathrm{R}(G)$ *be the intersection of all nonnormal subgroups. If* $\mathrm{R}(G) > \{1\}$, *then* $p = 2$, $|\mathrm{R}(G)| = 2$ *and* G *is one of the following groups:*

(a) $G \cong \mathrm{Q}_8 \times \mathrm{C}_4 \times \mathrm{E}_{2^s}$, $s \geq 0$.

(b) $G \cong \mathrm{Q}_8 \times \mathrm{Q}_8 \times \mathrm{E}_{2^s}$, $s \geq 0$.

(c) G *has an abelian maximal subgroup* A *of exponent* > 2 *and an element* $x \in G - A$ *of order* 4 *which inverts each element in* A.

Theorem 93.1. *Let* G *be a nonabelian* 2*-group all of whose minimal nonabelian subgroups are metacyclic and have exponent* 4 *and assume that* D_8 *and* $\mathrm{H}_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1}\rangle$ *(and possibly* Q_8*) actually appear as subgroups of* G. *Then* G *has a unique abelian maximal subgroup* A *of exponent* > 4 *and an involution* $t \in G - A$ *such that* t *inverts each element in* $A/\Omega_1(A)$ *and in* $\Omega_2(A)$ *and there is an element* $a \in A$ *of order* > 4 *such that* $a^t = a^{-1}\zeta$ *with* $1 \neq \zeta \in \Omega_1(A)$, *where in case that* $\mathfrak{V}_1(A)$ *is cyclic we have* $\zeta \notin \mathfrak{V}_1(A)$.

Conversely, all these 2*-groups satisfy the assumptions of the theorem.*

Theorem 94.1. *Let* G *be a nonabelian* 2*-group all of whose minimal nonabelian subgroups are nonmetacyclic and have exponent* 4. *Then* $\exp(G) = 4$, $\Omega_1(G)$ *is elementary abelian and if* A *is a maximal normal abelian subgroup of* G *containing* $\Omega_1(G)$, *then* $\Phi(G) \leq \Omega_1(A)$ *is elementary abelian and* $\mathfrak{V}_1(A) \leq \mathrm{Z}(G)$.

Theorem 98.1. *Let* G *be a nonabelian* 2*-group all of whose minimal nonabelian subgroups are isomorphic to* $\mathrm{M}_{2^{n+1}}$, $n \geq 3$ *fixed. Then* $E = \Omega_1(G)$ *is elementary abelian. Let* A *be a maximal normal abelian subgroup of* G *containing* E. *Then* $A = \mathrm{C}_G(E)$, *all elements in* $G - A$ *are of order* 2^n, G/A *is elementary abelian of order* ≤ 4, *and if* $x \in G - A$, *then* $|E : \mathrm{C}_E(x)| = 2$, $A_0 = \mathrm{C}_A(x) = \mathrm{C}_E(x)\langle x^2\rangle$, A/A_0 *is cyclic,* $\langle A, x\rangle'$ *is cyclic of order* $|A/A_0|$, $\langle A, x\rangle' \cap A_0 = \Omega_1(\langle x\rangle)$, x *inverts* A/A_0 *and* $\mathfrak{V}_{n-2}(A)$. *We have two possibilities:*

(a) $\exp(A) = 2^m \geq 2^n$ *in which case* $|G : A| = 2$ *and* A *is of type* $(2^m, 2^{n-2}, 2, \ldots, 2)$.

(b) $\exp(A) \leq 2^{n-1}$ *in which case* A *is of type* $(2^{n-1}, 2^r, 2, \ldots, 2)$ *with* $1 \leq r \leq n-2$ *and either* $|G : A| = 2$ *or* $|G : A| = 4$, *where in the last case* $G/\Omega_{n-2}(A) \cong \mathrm{Q}_8$.

Conversely, if G *is a* 2*-group of type* (a) *or* (b), *then each minimal nonabelian subgroup of* G *is isomorphic to* $\mathrm{M}_{2^{n+1}}$, $n \geq 3$ *fixed.*

Finally, we consider the following general problem.

Theorem 95.1. *Let G be a nonabelian 2-group of exponent 2^e ($e \geq 3$) which does not possess a minimal nonabelian subgroup of exponent 2^e. Then G has a unique maximal normal abelian subgroup A. The factor group G/A is either cyclic or generalized quaternion and each element in $G - A$ is of order $< 2^e$. Also, G possesses at least one metacyclic minimal nonabelian subgroup and $|\mathrm{C}_G(\Omega_1(A)) : A| \leq 2$.*

Proposition (see commentary of Mann to Problem 115). *If $p > 2$ and all minimal nonabelian subgroups of a p-group G are of exponent p and $\exp(G) > p$, then we have $|G : \mathrm{H}_p(G)| = p$.*

Exercise A40.79. Given a positive integer n and a p-group G of order $\geq p^n$, put $\mathrm{D}_n(G) = \langle H' \mid H < G, |G : H| = p^n \rangle$. Obviously, $\mathrm{D}_n(G)$ is a characteristic subgroup of G. If G is nonabelian, then $\mathrm{D}_1(G) < G$ if and only if $G/\mathrm{D}_1(G)$ is minimal nonabelian.

Exercise 124.7. Let A be a proper minimal nonabelian subgroup of a p-group G. Suppose that all A-containing subgroups of G of order $p|A|$ are two-generator. Then A/A' is a maximal abelian subgroup of $\mathrm{N}_G(A)/A'$.

Theorem 111.3. *The following assertions for a group G are equivalent:*

(a) $\Phi(G)' = H'$ *for all* $H \in \Gamma_1$.

(b) *G is either abelian or minimal nonabelian.*

Theorem 124.30. *Let $H \cong \mathcal{H}_{2,p}$ be a proper subgroup of a metacyclic p-group G. Here $\mathcal{H}_{2,p}$ is the unique nonabelian metacyclic group of order p^4 and exponent p^2. Then one of the following holds:*

(a) *If $p > 2$, then $|G : H| = p$, $|G'| = p^2$ and either*

$$G = \langle z, u \mid z^{p^3} = u^{p^2} = 1,\ z^u = z^{1+p^2} \rangle$$

or

$$G = \langle z, u \mid z^{p^3} = u^{p^2} = 1,\ z^u = z^{1+p} \rangle.$$

(b) *If $p = 2$, $H \lhd G$, then $|G : H| = 2$.*

(c) *If $p = 2$ and H is not normal in G, then $\Omega_1(G) = \Omega_1(H)$ and $G/\Omega_1(G)$ is either dihedral or semidihedral.*

Proposition 124.31. *Suppose that $H \cong \mathrm{M}_{p^n}$, $n > 3$, is a proper subgroup of a metacyclic p-group G. Then $\mathrm{N}_G(H)/H$ is cyclic. Next assume that $n = 4$.*

(a) *If $p > 2$, then $|\mathrm{N}_G(H)/H| = p$.*

(b) *If $p = 2$, then $|\mathrm{N}_G(H)/H| \leq 4$.*

§119

Review of characterizations of p-groups of maximal class

In this section we review characterizations of p-groups of maximal class obtained in the book. We hope that this section will help the readers.

Recall that a group G of order p^m is called a *p-group of maximal class* if $m > 2$ and $\mathrm{cl}(G) = m - 1$. Thus p-groups G of maximal class are nonabelian.

Proposition 1.3. *Suppose that a p-group G of order p^m has only one subgroup of order p^n, $0 < n < m$. Then either G is cyclic or $p = 2$, $n = 1$ and $G \cong \mathrm{Q}_{2^m}$.*

Lemma 1.4. *Let N be a normal subgroup of a p-group G. If N has no G-invariant abelian subgroup of type (p, p), then N is either cyclic or a 2-group of maximal class.*

In particular, if N and G are as in Lemma 1.4 and $\mathrm{Z}_2(G) \cap N$ is cyclic, then N is either cyclic or a 2-group of maximal class. For $N = G$ we get a known result of P. Roquette [Roq]: A p-group without normal abelian subgroup of type (p, p) is either cyclic or 2-group of maximal class.

Proposition 1.6 (O. Taussky). *If G is a nonabelian 2-group such that $|G : G'| = 4$, then $G \in \{\mathrm{D}_{2^m}, \mathrm{Q}_{2^m}, \mathrm{SD}_{2^m}\}$.*

It follows from Proposition 1.6 that the groups D_{2^m}, Q_{2^m} and SD_{2^m} exhaust all groups of maximal class and order 2^m ($m > 2$). Therefore some results stated below are trivial for $p = 2$.

Proposition 1.8 (Suzuki). *Let G be a nonabelian p-group and let $A < G$ be of order p^2. If $\mathrm{C}_G(A) = A$, then G is of maximal class. In particular, if $x \in G^{\#}$ is such that $|\mathrm{C}_G(x)| = p^2$, then G is of maximal class.*

By Theorem 9.6(f), if G is a p-group of maximal class, there is $x \in G$ such that $|\mathrm{C}_G(x)| = p^2$.

Exercise 9.1. Let G be a p-group of maximal class and order p^m. Then

(a) $|G : G'| = p^2$, $|\mathrm{Z}(G)| = p$, nonabelian epimorphic images of G are of maximal class.

(b) If $1 \leq i < m - 1$, then G has only one normal subgroup of order p^i.

(c) If $p > 2$ and $m > 3$, then G has no cyclic normal subgroups of order p^2.

Note that Exercise 9.1(b) and Lemma 1.4 imply Exercise 9.1(c).

Lemma 9.1. *Let G be a noncyclic subgroup of order p^m, $m > 2$. If G contains, for any $i = 1, \dots, m-2$, only one normal subgroup of order p^i, then G is of maximal class. The converse is trivial.*

A number of most important properties of p-groups of maximal class is listed in the following two theorems.

Theorem 9.5. *Let G be a group of maximal class and order p^m, $m \le p+1$. Then $\Phi(G)$ and $G/\mathrm{Z}(G)$ have exponent p. If $m = p+1$, then the group G is irregular and $|\mathfrak{V}_1(G)| = p$.*

It follows from Theorem 9.5 that a p-group of maximal class and order $> p^{p+1}$ is irregular.

Theorem 9.6. *Let G be a group of maximal class and order p^m, $p > 2$, $m > p+1$. Then*

(a) $|G : \mathfrak{V}_1(G)| = p^p$. *In particular,* $\mathfrak{V}_1(G) = \mathrm{K}_p(G)$.

(b) *There is $G_1 \in \Gamma_1$ such that $|G_1 : \mathfrak{V}_1(G_1)| = p^{p-1}$. This subgroup G_1 is absolutely regular.*

(c) *G has no normal subgroups of order p^p and exponent p (this follows from (b) and Exercise 9.1*(b)*; here the condition $m > p+1$ is essential). Moreover, if $N \lhd G$ and $|G : N| > p$, then N is absolutely regular since $N < G_1$. Next, if $N \lhd G$ of order p^{p-1}, then* $\exp(N) = p$, $N = \Omega_1(G_1) = \Omega_1(G')$. *In particular, G has no normal cyclic subgroups of order p^2 (see Exercise 9.1*(c)*).*

(d) *Let $Z_2 = \mathrm{Z}_2(G)$ be a normal subgroup of order p^2 in G, $G_0 = \mathrm{C}_G(Z_2)$. Then G_0 is regular such that $|\Omega_1(G_0)| = p^{p-1}$ (see* (b)*).*

(e) *Let $\Gamma_1 = \{M_1 = G_0, M_2, \dots, M_{p+1}\}$, where G_0 is defined in* (d)*. Then the subgroups $M_2, \dots, M_{p+1}$ are of maximal class (and so irregular; see Theorem 9.5). Thus the subgroups G_1 from* (b) *and G_0 from* (d) *coincide. The subgroup G_1 is called the* fundamental *subgroup of G (in general, G_1 is defined for all $m \ge 4$).*

(f) *In this part, $m \ge 3$ (i.e., we do not assume as in other parts that $m > p+1$). The group G has an element a such that $|\mathrm{C}_G(a)| = p^2$, i.e., $\mathrm{C}_G(a) = \langle a, \mathrm{Z}(G)\rangle$ (this is trivial for $m \in \{3, 4\}$).*

(g) $[\mathrm{K}_i(G), \mathrm{K}_j(G)] \le \mathrm{K}_{i+j+1}(G)$ *for all $i, j \in \{1, \dots, m-1\}$. Here* $\mathrm{K}_1(G) = G_1$.[1]

By Exercise 9.1(b) for $|G| > p^3$,

$$G > G_1 = \mathrm{K}_1(G) > \mathrm{K}_2(G) = G' > \cdots > \mathrm{K}_{m-1}(G) = \mathrm{Z}(G) > \mathrm{K}_m(G) = \{1\}$$

is a chain of characteristic subgroups; all indices of this chain are equal to p.

[1] In what follows we do not use this property.

Let G_1 be the fundamental subgroup of a p-group G of maximal class, $|G| > p^{p+1}$, and $\exp(G_1) = p^{n+1}$. If $k \le n$, then $|\Omega_k(G)| = p^{k(p-1)}$. If $p = 3$, then G_1 is metacyclic: G_1 is either abelian or minimal nonabelian (this follows from Theorem 9.11, Exercise 9.1(c) and Lemma 65.2(a)).

Let G be a p-group of maximal class and order $p^m > p^{p+1}$ and $p + 1 \le n < m$. Then the number of subgroups of maximal class and order p^n in G is equal to p^{m-n}. This follows from Theorem 9.6(e). Indeed, by that theorem, our claim follows in case $n = m - 1$. To prove this for remaining values n, one should apply induction.

Theorem 9.7. *If a p-group G is such that $G/\mathrm{K}_{p+1}(G)$ is of maximal class, then G is also of maximal class.*[2]

Theorem 9.8. *Let G be a p-group, $p > 2$.*

(a) (1st Hall regularity criterion) *If G is absolutely regular, it is regular.*[3]

(b) (Hall) *If G has no normal subgroups of order p^{p-1} and exponent p, it is regular.*[4]

(c) (2nd Hall regularity criterion) *If $|G' : \mathfrak{V}_1(G')| < p^{p-1}$, then G is regular. In particular, if G' is cyclic, then G is regular.*

(d) *If G is irregular, then G' has a characteristic subgroup of exponent p and order $\ge p^{p-1}$.*

Theorem 9.11 ([Bla2, Theorem 2.6(i)]; Huppert; see also Corollary 36.7). *If $p > 2$, then G is metacyclic if and only if $|G : \mathfrak{V}_1(G)| \le p^2$.*

Exercise 9.13. If a p-group of maximal class, $p > 2$, possesses a subgroup H such that $\mathrm{d}(H) > p - 1$, then $G \cong \Sigma_{p^2}$, a Sylow p-subgroup of the symmetric group of degree p^2.[5] In particular, $\mathrm{d}(H) \le p$ for all $H \le G$ (this is also true for $p = 2$).

Remark 10.5. If A is a subgroup of a p-group G such that $\mathrm{N}_G(A)$ is of maximal class, so is G.

Proposition 10.17. *Let B be a nonabelian subgroup of order p^3 of a p-group G. If B satisfies $\mathrm{C}_G(B) < B$, then G is of maximal class.*

It follows that if a 2-group G has at most two proper subgroups isomorphic to D_8, then

$$G \in \{\mathrm{SD}_{16}, \mathrm{D}_{16}, \mathrm{SD}_{32}\}.$$

Note that we do not know all 2-groups which contain only one subgroup isomorphic to Q_8.

[2] For a more general result, see Theorem 12.9.

[3] This is also true for $p = 2$ since absolutely regular 2-groups are cyclic.

[4] This is a partial case of Theorem 12.1(a).

[5] This is not true for $p = 2$ as the dihedral group D_{16} shows.

Proposition 10.19. *If a metacyclic p-group G contains a nonabelian subgroup of order p^3, then either $|G| = p^3$ or G is a 2-group of maximal class.*[6]

Proposition 10.24. *Let R be a subgroup of order p of a nonabelian p-group G. If there is only one maximal chain connecting R with G, then either $\mathrm{C}_G(R) \cong \mathrm{E}_{p^2}$ (in this case, G is of maximal class by Proposition 1.8) or $G \cong \mathrm{M}_{p^n}$.*

Two very important characterizations of p-groups of maximal class are contained in the following theorem which is due to Blackburn. These results are most frequently cited in our book.

Theorem 12.1. (a) *If a p-group G has no normal subgroup of order p^p and exponent p, it is either absolutely regular or irregular of maximal class.*

(b) *Suppose that a p-group G is not absolutely regular. If G contains an absolutely regular subgroup H of index p, then either G is of maximal class or $G = H\Omega_1(G)$, where $\Omega_1(G)$ is of order p^p and exponent p.*

In particular, if all regular subgroups of an irregular p-group G are absolutely regular, then G is of maximal class and $|\Omega_1(G)| = p^{p-1}$. The most important assertion of Lemma 1.4 follows from Theorem 12.1(a). Theorem 1.2 follows from Theorem 12.1(b) and Proposition 1.6. It follows from Theorem 12.1(a) that if N is a normal subgroup of a p-group G and $N \cap \mathrm{Z}_p(G)$ is absolutely regular, then N is either absolutely regular or of maximal class.

Recall that $\mathrm{c}_k(G)$ is the number of cyclic subgroup of order p^k of a p-group G.

Lemma 12.3. *Let a p-group G be of maximal class and order $p^m > p^{p+1}$, $p > 2$. Then*

(a) $\mathrm{c}_1(G) \equiv 1 + p + \cdots + p^{p-2} \pmod{p^p}$.

(b) $\mathrm{c}_2(G) \equiv p^{p-2} \pmod{p^{p-1}}$.

(c) *If $n > 2$, then $p^{p-1} \mid \mathrm{c}_n(G) = \mathrm{c}_n(G_1)$.*

(d) *The number of subgroups of order p^{p-1} and exponent p in G is $\equiv 1 \pmod{p^{m-p}}$.*

Condition $m > p + 1$ is important in Theorem 12.1. Note that the classification of groups of order p^{p+1} is one of the most important problems in p-group theory.

Proposition 12.6. *Suppose that a group G of order p^m is not of maximal class and $m > n > p + 1$. Let $\mathcal{N}$ be the set of normal subgroups D of G such that G/D is of maximal class and order p^n. Then $|\mathcal{N}| \equiv 0 \pmod{p}$.*

The following theorem generalizes Theorem 9.7.

Theorem 12.9. *Suppose that a p-group G has only one normal subgroup L of index p^{p+1}. If G/L is of maximal class, then G is also of maximal class.*[7]

[6] This follows from Proposition 10.17.

[7] It is easily seen that this theorem follows from Proposition 12.6 (this was not noticed in §12 so that theorem was proved independently).

Theorem 12.12. (a) *If a two-generator p-group G contains a subgroup of maximal class and index p, then G itself is of maximal class. If $\mathrm{d}(G) = 3$, then $G' = \Phi(G)$, i.e., $G/G' \cong \mathrm{E}_{p^3}$.*

(b) *Suppose that a group G of order p^m, $m > 3$, contains a subgroup H of maximal class and index p. If G is not of maximal class, then exactly p^2 maximal subgroups of G are of maximal class. If, in addition, $p > 2$ and $m > 4$, then the remaining $p + 1$ maximal subgroups of G have no two generators and their intersection $\eta(G)$ has index p^2 in G. If, in addition, H is irregular, then $G/\mathrm{K}_{p+1}(G)$ is of order p^{p+1} and exponent p.*

Proposition 12.13. *Let G be a p-group. If $A \in \Gamma_1$ is absolutely regular and $M < G$ is irregular of maximal class, then G is also of maximal class.*

Theorem 13.2. *If G is a group of order p^m which is neither absolutely regular nor of maximal class, then*

(a) $\mathrm{c}_1(G) \equiv 1 + p + \cdots + p^{p-1} \pmod{p^p}$. *In particular, the number of solutions of $x^p = 1$ in G is divisible by p^p.*

(b) *If $k > 1$, then p^{p-1} divides $\mathrm{c}_k(G)$.*

Theorem 13.2 implies Theorem 10.17.

Recall that $e_k(G)$ is the number of subgroups of order p^k and exponent p in a p-group G.

The following theorem is the most important counting result.

Theorem 13.5 and 13.6. *If a p-group G is neither absolutely regular nor of maximal class, then*

(a) $e_p(G) \equiv 1 \pmod{p}$.

(b) *Let $|G| = p^m > p^n \geq p^{p+1}$. Then the number of subgroups of maximal class and order p^n in G is divisible by p^2.*

It follows that if N is a normal subgroup of a p-group G and N has no G-invariant subgroup of order p^p and exponent p, then it is either absolutely regular or of maximal class. Next, if $\mathrm{Z}_p(G) \cap N$ is absolutely regular, then N is either absolutely regular or of maximal class.

Proposition 13.14. (a) *If $\Omega_1(G)$ is either absolutely regular or irregular of maximal class, so is the p-group G.*

(b) *A p-group G is of maximal class if and only if $\Omega_2(G)$ is of maximal class.*

If an irregular p-group G is of maximal class, then one of the following holds:

(i) $|\Omega_1(G)| = p^{p-1}$,

(ii) $|G : \Omega_1(G)| \leq p$.

If G is of maximal class, then $\Omega_2(G) = G$.

Proposition 13.16. *Suppose that a nonabelian p-group G has a cyclic subgroup U of order p^2 such that $\mathrm{C}_G(U)$ is cyclic. Then G is of maximal class.*

It is important in the hypothesis of Proposition 13.16 that $|U| = p^2$; for $|U| > p^2$ the assertion does not hold. For a proof, see Appendix 40.

Remark 13.4. Let G be of order $p^m > p^k \geq p^{p+1}$, and $M \in \Gamma_1$. If $H < G$ is of maximal class and order p^k such that $H \not\leq M$ and all such H are of maximal class, then G is also of maximal class.

Remark 13.6. Let a p-group G satisfy the following conditions: (i) G contains a proper abelian subgroup A of order $\geq p^3$. (ii) Whenever $A < H \leq G$ and $|H : A| = p$, then $|\mathrm{Z}(H)| = p$. Then: (a) G is of maximal class, (b) $|G : A| = p$. To justify (b), it suffices to take A in $\mathrm{C}_G(R)$, where $R \lhd G$ is of order p^2.

Exercise 13.10. (a) Let $H < G$, where G is a p-group. If every subgroup of G of order $p|H|$ containing H is of maximal class, then G is also of maximal class.

(b) Let A be a proper absolutely regular subgroup of a p-group G, $p > 2$, $\exp(A) > p$, such that whenever $A < B \leq G$ with $|B : A| = p$, then $\Omega_1(B) = B$. Then G is of maximal class. If, in addition, $|A| > p^p$, then $|G : A| = p$.

Proposition 13.18. *Let $M < G$ be of maximal class, G is a p-group.*

(a) *Set $D = \Phi(M)$, $N = \mathrm{N}_G(M)$ and $C = \mathrm{C}_N(M/D)$. Let t be the number of subgroups $K \leq G$ of maximal class such that $M < K$ and $|K : M| = p$. Then $t = \mathrm{c}_1(N/M) - \mathrm{c}_1(C/M)$. If G is not of maximal class, then $t \equiv 0 \pmod{p}$.*

(b) *Suppose, in addition, that M is irregular and G is not of maximal class and a positive integer k is fixed. Then the number t of subgroups $L < G$ of maximal class and order $p^k|M|$ such that $M < L$ is a multiple of p.*

Theorem 13.19. *Let G be a group of maximal class of order p^m and exponent p^e, $m > p + 1$. Then*

(a) *If $3 \leq k \leq e$, then $\Omega_k^*(G) \leq G_1$, where $\Omega_k^*(G) = \langle x \in G \mid o(x) = p^k \rangle$, i.e., every element in $G - G_1$ has order $\leq p^2$. If $m > p + 1$, then $\exp(G_1) = p^e$.*

(b) *If $x \in G - G_1$, then $x^p \in \mathrm{Z}(G)$ so $\mathrm{H}_p(G/\mathrm{Z}(G)) = G_1/\mathrm{Z}(G)$. Here $\mathrm{H}_p(G) = \langle x \in G \mid o(x) > p \rangle$ is the Hughes subgroup of G.*

(c) *If $H < G$, $H \not\leq G_1$ and $|H| > p^p$, then H is of maximal class.*

(d) *If $H < G$ is irregular, then $\Omega_1(G_1) < H$.*

(e) *If $H < G$ is of order p^p and $H \not\leq G_1$, then $\Omega_1(G_1) < H$.*

(f) *If $p > 2$ and $L < G$ is of order p^{p-1}, then either $L < G_1$ or $\mathrm{Z}(G) < L$.*

(g) *If $L < G$ is of order p^{p-1} and $L \not\leq G_1$, then $\Omega_1(G)$ normalizes L.*

It follows from Theorems 9.5 and 13.19(b) that if G is of maximal class, then we have $\Omega_2^*(G) = G$.

Theorem 36.12. *Let G be a p-group of exponent $p^e > p^2$ and $1 < k < e$. Let U be a maximal member of the set of subgroups of G with exponent p^k.*

(a) *If U is absolutely regular, then G is also absolutely regular, $U = \Omega_k(G)$ and the subgroup U is not of maximal class.*

(b) *If U is irregular of maximal class, then G is also of maximal class.*

Lemma 36.13. *Let G be a p-group of order $> p^{p+1}$ with $|\Omega_2(G)| = p^{p+1}$. Then one of the following holds:*

(a) *G is absolutely regular.*

(b) *G is an L_p-group.*

(c) *$p = 2$ and $G = \langle a, b \mid a^{2^n} = 1, a^{2^{n-1}} = b^4, a^b = a^{-1+2^{n-2}} \rangle$.*

Theorem 36.14. *Let G be a p-group and suppose that $H < G$ is a maximal member of the set of subgroups of G of exponent p^2. Suppose, in addition, that $|H| = p^{p+1}$. Then one of the following holds:*

(a) *$H = \Omega_2(G)$ so G is as in Lemma 36.13.*

(b) *G is a 2-group of maximal class (in this case, H is also of maximal class).*

Recall that $\mho^2(G) = \mho_1(\mho_1(G))$. We have $\mho^2(G) \geq \mho_2(G)$ (strict inequality is possible).

Theorem 36.16. *Suppose that a p-group G is such that $G/\mho^2(G)$ is of maximal class. Then G is also of maximal class.*

Proposition 25.8(c). *If G is an irregular p-group of maximal class and $\phi : G \to G_0$ is a lattice isomorphism, then G^ϕ is also of maximal class.*

§120

Nonabelian 2-groups such that any two distinct minimal nonabelian subgroups have cyclic intersection

Our technique with minimal nonabelian subgroups of p-groups gives also the following rather deep result. This solves a problem stated by the first author for $p = 2$.

Theorem 120.1. *Let G be a nonabelian 2-group such that any two distinct minimal nonabelian subgroups of G have cyclic intersection. Then we have one of the following possibilities:*

(a) *G is minimal nonabelian.*

(b) *G is a 2-group of maximal class.*

(c) *$G = Q \times V$, where $Q \cong Q_{2^n}$, $n \geq 3$, is generalized quaternion and $V \neq \{1\}$ is elementary abelian.*

(d) *$G = \langle a, h \mid a^8 = h^4 = 1,\ [a,h] = v,\ v^4 = 1,\ [v,h] = v^2,\ a^2 = vh^2 \rangle$, where*

$$|G| = 2^5, \quad G' = \langle v \rangle \cong \mathrm{C}_4, \quad \mathrm{Z}(G) = \Omega_1(G) = \langle h^2, v^2 \rangle \cong \mathrm{E}_4,$$
$$\Phi(G) = \langle h^2, v \rangle \cong \mathrm{C}_2 \times \mathrm{C}_4, \quad \mathrm{cl}(G) = 3,$$

and maximal subgroups of G are $\langle h, v \rangle \cong \mathrm{H}_2$ (minimal nonabelian), $\langle a \rangle \times \langle h^2 \rangle$ (abelian of type $(8,2)$) and $\langle ah, v \rangle \times \langle h^2 \rangle \cong \mathrm{Q}_8 \times \mathrm{C}_2$.

Conversely, each of the above groups satisfies the assumption of our theorem.

Proof. Since minimal nonabelian 2-groups and 2-groups of maximal class satisfy the assumption of our theorem, we may assume that G is neither minimal nonabelian nor a 2-group of maximal class.

Suppose that G possesses noncommuting involutions. Since any two noncommuting involutions generate a dihedral subgroup, it follows that

$$D = \langle z, u, t \mid z^2 = u^2 = t^2 = 1,\ [u,z] = [t,z] = 1,\ [u,t] = z \rangle \cong \mathrm{D}_8$$

is a subgroup of G, where $\mathrm{Z}(D) = D' = \langle z \rangle$ and $\langle u, z \rangle$ and $\langle t, z \rangle$ are two four-subgroups of D. If $\mathrm{C}_G(D) \leq D$, then G is of maximal class (Proposition 10.17), a contradiction. Hence $\mathrm{C}_G(D) \not\leq D$ and let $v \in \mathrm{C}_G(D) - D$ be such that $v^2 \in \langle z \rangle$. Then

we get $D_1 = \langle z, u, vt\rangle \cong \mathrm{D}_8$ with $D \cap D_1 = \langle z, u\rangle \cong \mathrm{E}_4$, contrary to our assumption. We have proved that $\Omega_1(G)$ is elementary abelian of order ≥ 4 (since G is not generalized quaternion).

Assume that $E = \Omega_1(G) \not\leq \mathrm{Z}(G)$. Let $t \in E$ be a noncentral involution and set $H = \mathrm{C}_G(t)$ so that $E \leq H$ and $H < G$. Let S be a subgroup of G such that $S > H$ and $|S : H| = 2$ and take an element $x \in S - H$. Then $t' = t^x \neq t$ and $(t')^x = t^{x^2} = t$ which gives $W = \langle t, t'\rangle \cong \mathrm{E}_4$, $\mathrm{C}_G(W) = H$ and $S = \mathrm{N}_G(W)$. Set $z = tt'$ so that $z^x = z$, $[x, t] = z$ and so $M = \langle x, t\rangle = W\langle x\rangle$ is minimal nonabelian with $M' = \langle z\rangle$. We have either $\Omega_1(\langle x\rangle) = \langle z\rangle$ (in which case $M \cong \mathrm{M}_{2^n}$, $n \geq 4$, since $M \cong \mathrm{D}_8$ is not possible because there are no noncommuting involutions) or $\Omega_1(\langle x\rangle) = \langle u\rangle$ with $u \in E - W$ (in which case M is nonmetacyclic minimal nonabelian with $\Omega_1(M) = \langle u\rangle \times W \cong \mathrm{E}_8$). Suppose that $M = \langle x, t\rangle \neq S$. In this case, $M \cap H < H$ and take an element $h \in H - M$ so that $y = hx \in S - H$ and $y \notin M$. We get

$$t^y = t^{hx} = t^x = t', \quad (t')^y = t^{y^2} = t \quad \text{and} \quad z^y = (tt')^y = z.$$

Thus $M_1 = \langle y, t\rangle$ is minimal nonabelian with $M \cap M_1 \geq \langle t, t'\rangle \cong \mathrm{E}_4$, contrary to our assumption. We have proved that $S = M = \langle x, t\rangle = W\langle x\rangle$ is minimal nonabelian. If, in addition, $\Omega_1(\langle x\rangle) = \langle z\rangle$, then $E = W \trianglelefteq G$. But we know that $\mathrm{N}_G(W) = S$ and so $S = G$ is minimal nonabelian, a contradiction. Hence

$$E = \Omega_1(\langle x\rangle) \times W = \Omega_1(G) \cong \mathrm{E}_8$$

and $\mathrm{C}_G(E) = H$ so that G/H is isomorphic to a subgroup of D_8 and $S < G$. Since H is a maximal normal abelian subgroup of G, we may use Lemma 57.1. For any element $g \in G - S$, there is $h \in H$ such that $\langle g, h\rangle$ is minimal nonabelian. By our assumption, $\langle g, h\rangle \cap \Omega_1(S)$ is cyclic and so $\Omega_1(\langle g, h\rangle) \cong \mathrm{C}_2$ which forces $\langle g, h\rangle \cong \mathrm{Q}_8$. In particular, $o(g) = 4$ and $g^2 \in E$ so that g induces an involutory automorphism on E (noting that $\mathrm{C}_G(E) = H < S$). Let $e \in E$ be such that $e' = e^g \neq e$ which together with $(e')^g = e^{g^2} = e$ shows that $(ee')^g = ee' \neq 1$. Hence $\langle g, e\rangle$ is minimal nonabelian with $\langle g, e\rangle' = \langle ee'\rangle$. But

$$\langle g, e\rangle \cap S \geq \langle e, e'\rangle \cong \mathrm{E}_4,$$

contrary to our assumption. We have proved that $E = \Omega_1(G) \leq \mathrm{Z}(G)$.

Suppose that all minimal nonabelian subgroups of G are quaternion. In that case, Theorem 90.1 implies that $G = Q \times V$, where $Q \cong Q_{2^n}$, $n \geq 3$, is generalized quaternion and $V \neq \{1\}$ is elementary abelian, and so we have obtained the groups stated in part (c) of our theorem.

In what follows we assume that the group G possesses a minimal nonabelian subgroup $H = \langle a, b\rangle$ which is not quaternion. Then $|\Omega_1(H)| \geq 4$ and so $\Omega_1(H) \cong \mathrm{E}_4$ or $\Omega_1(H) \cong \mathrm{E}_8$. Since $\Omega_1(H) \leq \mathrm{Z}(G)$, it follows by the assumption of our theorem that $H \trianglelefteq G$ and $\Omega_1(H) \leq \mathrm{Z}(H) = \Phi(H)$. Also (Exercise P9), $\Phi(H) = \langle a^2, b^2, [a, b]\rangle$. Suppose that there is an involution $t \in G - H$. As $t \in \mathrm{Z}(G)$, we get $[at, b] = [a, b]$ and $H_1 = \langle at, b\rangle$ is minimal nonabelian with $\Phi(H_1) = \langle (at)^2 = a^2, b^2, [a, b]\rangle = \Phi(H)$

so that $H \cap H_1 \geq \Omega_1(H)$ is noncyclic, a contradiction. Hence we have proved that $\Omega_1(H) = \Omega_1(G) = E$ and so $4 \leq |E| \leq 8$.

Let K be any minimal nonabelian subgroup of G which is distinct from H. If K is not quaternion, then $|\Omega_1(K)| \geq 4$ and $\Omega_1(K) \leq \Omega_1(H) = \Omega_1(G)$ so that $H \cap K$ is noncyclic, a contradiction. We have proved that each minimal nonabelian subgroup of G which is distinct from H is quaternion.

Suppose that G/H is not elementary abelian. Then there is a subgroup $L > H$ such that $L/H \cong \mathrm{C}_4$. Let L_0 be a unique subgroup of index 2 in L which contains H. If $x \in L - L_0$, then $\langle x \rangle$ covers L/H and so $o(x) \geq 8$ since there are no involutions in $L_0 - H$ (noting that $\Omega_1(H) = \Omega_1(G)$). On the other hand, Lemma 57.1 implies that L is generated by its minimal nonabelian subgroups which are equal to H and quaternion subgroups of L. This shows that L possesses a quaternion subgroup which is not contained in L_0. But this contradicts the above fact that all elements in $L - L_0$ are of order ≥ 8. We have proved that $G/H \neq \{1\}$ is elementary abelian. In what follows we shall determine the structure of any subgroup $T > H$ with $|T/H| = 2$.

(i) First we show that T possesses at least one abelian maximal subgroup A.

Assume that this is false. Let $\{X, Y, Z\}$ be the set of maximal subgroups of H so that X, Y and Z are abelian and at least one of them, say X, is normal in T. In that case, X is a maximal normal abelian subgroup of T. For each $x \in T - H$, there is $a \in X$ such that $\langle x, a \rangle$ is minimal nonabelian (Lemma 57.1) and so $\langle x, a \rangle \cong \mathrm{Q}_8$. In particular, we obtain $o(x) = 4$ and $1 \neq x^2 \in \Omega_1(H) \leq \Phi(H)$ and $x^2 \in \mathrm{Z}(T)$. It follows that $\Phi(T) = \Phi(H)$ which implies that Y and Z are also maximal normal abelian subgroups of T. Let x_0 be a fixed element in $T - H$ so that $X\langle x_0 \rangle$ is nonabelian and each minimal nonabelian subgroup of $X\langle x_0 \rangle$ is isomorphic to Q_8. By Theorem 90.1, $X\langle x_0 \rangle = R \times V$, where $R \cong \mathrm{Q}_{2^n}$, $n \geq 3$, and $\exp(V) \leq 2$. Since $x_0 \notin \Phi(X\langle x_0 \rangle)$ and $o(x_0) = 4$ with $x_0^2 \in \mathrm{Z}(T)$, it follows that x_0 inverts X. Considering in the same way the nonabelian subgroups $Y\langle x_0 \rangle$ and $Z\langle x_0 \rangle$, we conclude that x_0 also inverts Y and Z. But $X \cup Y \cup Z = H$ and so x_0 inverts on H. This implies that H is abelian, a contradiction. Hence we have proved that T possesses at least one abelian maximal subgroup A.

(ii) We have $\Omega_1(H) = \Phi(H) = \mathrm{Z}(T)$ so that $\exp(H) = 4$ and either $|H| = 2^4$ if $\Omega_1(H) \cong \mathrm{E}_4$ or $|H| = 2^5$ if $\Omega_1(H) \cong \mathrm{E}_8$.

Indeed, let $x \in T - (A \cup H)$. By Lemma 57.1, there is $a \in A$ such that $\langle x, a \rangle$ is minimal nonabelian. Since $\langle x, a \rangle \neq H$, we have $\langle x, a \rangle \cong \mathrm{Q}_8$. In particular, we obtain $o(x) = o(a) = 4$, $x^2 = a^2 = z \in \mathrm{Z}(T)$ and x inverts a. Suppose that x centralizes an element b of order 4 in A. If $b^2 = z$, then ab is an involution and $(ab)^x = a^{-1}b = (ab)z$, contrary to the fact that $\Omega_1(G) \leq \mathrm{Z}(G)$. Hence $b^2 \neq z$ and we consider the subgroup $\langle ab, x \rangle$. We have

$$[ab, x] = [a, x]^b[b, x] = z^b = z \quad \text{and so} \quad \langle ab, x \rangle' = \langle z \rangle$$

which implies that $\langle ab, x \rangle$ is minimal nonabelian. But $(ab)^2 = a^2b^2 = zb^2 \neq z$ and $x^2 = z$ so that $\langle ab, x \rangle \ncong \mathrm{Q}_8$, contrary to the fact that $\langle ab, x \rangle \neq H$ (since, by choice,

$x \in T - (A \cup H)$). We have proved that x does not centralize any element of order 4 in A and so $C_A(x) = \Omega_1(H) = \Omega_1(T)$ which implies that $\Omega_1(H) = Z(T)$. On the other hand, we conclude that $\Phi(H) = Z(H)$ and $\Phi(H) \leq A$ so that $\Phi(H) \leq Z(T)$. This forces $\Phi(H) = \Omega_1(H)$, $\exp(H) = 4$, $|H| = 2^4$ if $\Omega_1(H) \cong E_4$ and $|H| = 2^5$ if $\Omega_1(H) \cong E_8$.

(iii) We have $|T'| = 4$ and so A is the unique abelian maximal subgroup of T. Each maximal subgroup X of T which is distinct from the subgroups A and H is of the form $X = R\Omega_1(H)$ with $R \cong Q_8$ and $R \cap \Omega_1(H) = Z(R)$.

We have $|H| = 4|\Omega_1(H)|$ and so $|T| = 8|\Omega_1(H)|$ as $\Omega_1(H) = \Phi(H)$. In view of Lemma 1.1, we get $|T| = 2|Z(T)||T'|$, where $Z(T) = \Omega_1(H)$ so that $|T'| = 4$. By Exercise P1, T has exactly one abelian maximal subgroup. Let X be any maximal subgroup of T distinct from A and H. Then X is nonabelian and each minimal nonabelian subgroup of X is isomorphic to Q_8. By Theorem 90.1, we have $X = R \times V$, where $R \cong Q_{2^n}$, $n \geq 3$, and $\exp(V) \leq 2$. On the other hand, $\Omega_1(H) = Z(T) = \Phi(H) \leq \Phi(T)$ and so $\Omega_1(H) \leq X$ which gives

$$Z(R) \times V = \Omega_1(X) = \Omega_1(H).$$

Since $|X| = |H| = 4|\Omega_1(H)|$, it follows that $R \cong Q_8$.

(iv) We have $d(T) = 2$.

Suppose that $d(T) > 2$ in which case we have $\Phi(T) = \Phi(H) = \Omega_1(H) = Z(T)$, $\exp(T) = 4$, $T' \leq Z(T)$ and $d(T) = 3$.

(iv1) Assume, in addition, that $\Omega_1(H) \cong E_4$ so that

$$H = \langle a, b \mid a^4 = b^4 = 1,\ [a,b] = z,\ z \in \{a^2, b^2\}\rangle \cong H_2,$$

where $a \in A$ and $A \cong C_4 \times C_4$. Let $c \in A - H$, where $1 \neq c^2 \in \Omega_1(H) = \langle a^2, b^2\rangle$, $c^2 \neq a^2$ and $T = \langle a, b, c\rangle$. If $[c,b] = 1$, then $T/\langle z\rangle$ is abelian, contrary to $|T'| = 4$. Hence $[c,b] \neq 1$ and $\langle c, b\rangle$ is minimal nonabelian so that $\langle c, b\rangle \cong Q_8$ (as $\langle c, b\rangle \neq H$). It follows $[c,b] = b^2$ and $c^2 = b^2$. Consider the subgroup $\langle cb, a\rangle$ with $[cb, a] = z$ so that $\langle cb, a\rangle \cong Q_8$ since $\langle cb, a\rangle \neq H$. We get

$$z = a^2 \quad \text{and} \quad (cb)^2 = c^2b^2[b,c] = c^2b^2b^2 = c^2 = b^2 \neq a^2,$$

a contradiction.

(iv2) It remains to consider the case $\Omega_1(H) \cong E_8$ so that

$$H = \langle a, b \mid a^4 = b^4 = 1,\ [a,b] = d,\ d^2 = [d,a] = [d,b] = 1\rangle,$$

where $a \in A$ and $\Omega_1(H) = \langle a^2, b^2, d\rangle \cong E_8$. Let $c \in A - H$, where $1 \neq c^2 \in \Omega_1(H)$ and $T = \langle a, b, c\rangle$. If $[c,b] = 1$, then $T/\langle d\rangle$ is abelian, contrary to $|T'| = 4$. Hence we get $[c,b] \neq 1$ and $\langle c, b\rangle$ is minimal nonabelian so that $\langle c, b\rangle \cong Q_8$ (since $\langle c, b\rangle \neq H$). It follows that $c^2 = b^2 = [c,b]$. We have $[c, ab] = [c,b] = b^2$ so that $\langle c, ab\rangle \cong Q_8$ since $\langle c, ab\rangle$ is minimal nonabelian distinct from H. But $(ab)^2 = a^2b^2d \neq c^2 = b^2$, a contradiction.

(v) Now we determine the structure of T. As $\mathrm{d}(T) = 2$, we have

$$A \cap H = \Phi(T), \quad \Phi(H) = \Omega_1(H) = \mathrm{Z}(T) < \Phi(T), \quad \Omega_1(H) = \Omega_1(T).$$

Since $|\Phi(T) : \Omega_1(H)| = 2$, it follows that $\Phi(T)$ is abelian of type $(4,2)$ or $(4,2,2)$ (depending on the possibilities $\Omega_1(H) \cong \mathrm{E}_4$ or $\Omega_1(H) \cong \mathrm{E}_8$). Take some elements $h \in H - A$ and $a \in A - H$ so that $\langle a, h\rangle = T$. If $[a,h] \in \Omega_1(H) = \mathrm{Z}(T)$, then $T/\langle [a,h]\rangle$ is abelian and so $T' = \langle [a,h]\rangle$, contrary to $|T'| = 4$. Hence we obtain that $[a,h] = v \in \Phi(T) - \Omega_1(H)$ which implies $o(v) = 4$, $T' = \langle v\rangle \cong \mathrm{C}_4$ and T is of class 3. Set $v^2 = z$ so that $H' = \langle z\rangle$. Since H' is not a maximal cyclic subgroup in H, it follows that H is metacyclic, $\Omega_1(H) \cong \mathrm{E}_4$ and so $|T| = 2^5$. We have

$$H = \langle h, v \mid h^4 = v^4 = 1,\ [h,v] = v^2 = z\rangle \cong \mathrm{H}_2,$$

where $\Omega_1(H) = \langle h^2, z\rangle \cong \mathrm{E}_4$. For any element $x \in T - (A \cup H)$ there is an element $k \in A$ such that $\langle x, k\rangle$ is minimal nonabelian (Lemma 57.1) and so $\langle x, k\rangle \cong \mathrm{Q}_8$ which implies that $o(x) = 4$ and $x^2 \in \Omega_1(H)$. Also, $\Phi(H) = \Omega_1(H)$ and so all elements in $T - A$ are of order 4. If any element in $A - H$ is of order 4, then $\mathfrak{V}_1(T) = \Omega_1(H)$, contrary to $A \cap H = \Phi(T)$. Hence $o(a) = 8$ and $a^2 \in (A \cap H) - \Omega_1(H)$. All elements in $A - H$ are of order 8 and so $\exp(T) = 8$. By (iii), we get $\langle ah\rangle \Phi(T) \cong \mathrm{Q}_8 \times \mathrm{C}_2$. Since $[ah, v] = [a,v]^h[h,v] = [h,v] = z$, we must have $\langle ah, v\rangle \cong \mathrm{Q}_8$ and therefore

$$v^2 = z = (ah)^2 = ahah = a^2a^{-1}h^{-1}h^2ah = a^2h^2[a,h] = a^2h^2v$$

and so $a^2 = vh^2$. The structure of T is uniquely determined:

$$T = \langle a, h \mid a^8 = h^4 = 1,\ [a,h] = v,\ v^4 = 1,\ [v,h] = v^2,\ a^2 = vh^2\rangle,$$

where all elements in $A - H$ are of order 8 and $A = \langle a\rangle \times \langle h^2\rangle$ is abelian of type $(8,2)$.

It is now easy to determine the structure of G. We know that $G/H \neq \{1\}$ is elementary abelian. Also, all minimal nonabelian subgroups of G are equal to $H \cong \mathrm{H}_2$ and some quaternion subgroups. Suppose that $|G/H| > 2$. Then there exists a subgroup $G_0 > H$ such that $G_0/H \cong \mathrm{E}_4$. If T/H is a subgroup of order 2 in G_0/H, then the structure of T is uniquely determined in (v) and for any other subgroup L/H of order 2 in G_0/H, we have $L \cong T$. In particular, $\exp(G_0) = \exp(T) = 8$. By Theorem 92.6, G_0 has a unique abelian maximal subgroup A_0 and $A_0 \cap T = A$ is the unique abelian maximal subgroup of T and is of type $(8,2)$. All elements in $A_0 - H$ are of order 8 and $\Omega_2(A_0) = A_0 \cap H = A \cap H$ which is abelian of type $(4,2)$. There is no such abelian group A_0 of order 2^5. We have proved that $G = T$ and so we have obtained the group of order 2^5 stated in part (d) of our theorem. □

§121

p-groups of breadth 2

In this section we prove a result of Parmeggiani and Stellmacher [PS1] on p-groups of breadth 2. We recall that the breadth $\mathrm{b}_G(x)$ of an element x in a p-group G is defined as $p^{\mathrm{b}_G(x)} = |G : \mathrm{C}_G(x)|$ and the breadth $\mathrm{b} = \mathrm{b}(G)$ is $\max\{\mathrm{b}_G(x) \mid x \in G\}$. We know that for a p-group G we have $\mathrm{b}(G) = 1$ if and only if $|G'| = p$ (see Exercise 2.7 and Proposition 121.9). This result is also proved in [Kno], where we additionally find the result that $|G'| \leq p^3$ for p-groups with $\mathrm{b}(G) = 2$.

Theorem 121.1. *Let G be a p-group. Then $\mathrm{b}(G) = 2$ if and only if one of the following holds:*

(a) $|G'| = p^2$, *or*

(b) $|G'| = p^3$ *and* $|G : \mathrm{Z}(G)| = p^3$.

Moreover, if $\mathrm{b}(G) = 2$ and $|G'| = p^3$, then $|A/\mathrm{Z}(G)| = p$ for every maximal normal abelian subgroup A of G.

We shall prove Theorem 121.1 in a series of lemmas. For that purpose we need the following definitions. Let A be a normal abelian subgroup in a p-group G and $x \in G$. Then

$$p^{\mathrm{b}_A(x)} = |A : \mathrm{C}_A(x)|, \quad \mathrm{b}_A = \mathrm{b}_A(G) = \max\{\mathrm{b}_A(x) \mid x \in G\},$$
$$\mathrm{B}_A = \{x \in G \mid \mathrm{b}_A(x) = \mathrm{b}_A(G)\}, \quad \mathrm{T}_A = \{x \in G \mid \mathrm{b}_A(x) = 1\},$$
$$\mathrm{M}_x = A\mathrm{C}_G(x), \quad \mathrm{G}_x = \langle \mathrm{M}_{ax} \mid a \in A\rangle, \quad \mathrm{D}_x = \bigcap_{a\in A} \mathrm{M}_{ax}.$$

Lemma 121.2. *For every $x \in G$, $[A, x] = [A, \langle x\rangle] = \{[a, x] \mid a \in A\}$. In particular, $|[A, x]| = p^{\mathrm{b}_A(x)} = |A : \mathrm{C}_A(x)|$.*

Proof. The map $a \to [a, x] \in A$ ($a \in A$) is a homomorphism from A into A since for any $a, a' \in A$ we have $[aa', x] = [a, x]^{a'}[a', x] = [a, x][a', x]$. The kernel of this homomorphism is $\mathrm{C}_A(x)$ and so $A/\mathrm{C}_A(x) \cong \{[a, x] \mid a \in A\} = A_0$, which is a subgroup of A.

Suppose that $[a, x^i] \in A_0$ for some $i \geq 1$. Then

$$[a, x^{i+1}] = [a, x^i x] = [a, x][a, x^i]^x = [a, x][a, x^i][[a, x^i], x] \in A_0$$

and so $[A, x] = [A, \langle x\rangle]$ which gives $|[A, \langle x\rangle]| = p^{\mathrm{b}_A(x)}$. □

Lemma 121.3. *Let $u, v \in G$ be such that $[A,u] \cap [A,v] = \{1\}$. Then $\mathrm{C}_A(u) \leq \mathrm{C}_A(v)$ or $\mathrm{b}_A(u) < \mathrm{b}_A(uv)$.*

Proof. Suppose that $\mathrm{C}_A(u) \not\leq \mathrm{C}_A(v)$. Then there is $a \in \mathrm{C}_A(u) - \mathrm{C}_A(v)$. Thus we get $a^{uv} = a^v \neq a$ and $1 \neq [a,uv] = [a,v][a,u]^v = [a,v]$ so that $[A,uv] \cap [A,v] \neq 1$. We have

$$(*) \qquad [A,u] \times [A,v] = [A,uv][A,v].$$

Indeed, for any $a \in A$, we obtain

$$[a,uv] = [a,v][a,u]^v = [a,v][a,u][[a,u],v] \in [A,u] \times [A,v],$$

and

$$\begin{aligned}[a,u] &= [a,(uv)v^{-1}] = [a,v^{-1}][a,(uv)]^{v^{-1}} \\ &= [a,v^{-1}][a,(uv)][[a,(uv)],v^{-1}] \in [A,uv][A,v],\end{aligned}$$

which proves $(*)$. From $(*)$ and $[A,uv] \cap [A,v] \neq \{1\}$ it then follows (using also Lemma 121.2) that $p^{\mathrm{b}_A(u)+\mathrm{b}_A(v)} < p^{\mathrm{b}_A(uv)+\mathrm{b}_A(v)}$ which gives $\mathrm{b}_A(u) < \mathrm{b}_A(uv)$ and we are done. □

Lemma 121.4. *Let $x, y \in \mathrm{T}_A$, $T = \langle x, y\rangle$ and $\bar{T} = (T\mathrm{C}_G(A))/\mathrm{C}_G(A)$. Then one of the following holds:*

(a) *$T - \mathrm{C}_G(A) \subseteq \mathrm{T}_A$ and $[A,x] = [A,T]$; moreover, $\mathrm{C}_A(x) \neq \mathrm{C}_A(y)$ if $\bar{T}$ is not cyclic.*

(b) *$T - \mathrm{C}_G(A) \subseteq \mathrm{T}_A$ and $\mathrm{C}_A(x) = \mathrm{C}_A(T)$; moreover, $[A,x] \neq [A,y]$ if $\bar{T}$ is not cyclic and in this case $[A,T] = [A,x] \times [A,y]$.*

(c) *$\mathrm{C}_A(T) = \mathrm{C}_A(x) \cap \mathrm{C}_A(y)$ and $[A,T] = [A,xy] = [A,x] \times [A,y]$.*

Proof. If $\bar{T}$ is cyclic, then $|T/\mathrm{T}_G(A)| = p$ and so $\mathrm{C}_A(x) = \mathrm{C}_A(y) = \mathrm{C}_A(T)$, and (b) holds. Indeed, we conclude that $|(A\langle x\rangle) : (\mathrm{C}_A(x)\langle x\rangle)| = p$ so that if $a \in A - \mathrm{C}_A(x)$, then $[a,x] \in A \cap (\mathrm{C}_A(x)\langle x\rangle) = \mathrm{C}_A(x)$. Hence $1 \neq [a,x] \in \mathrm{Z}(\langle a,x\rangle)$ and therefore $\langle a,x\rangle' = \langle [a,x]\rangle$ is of order p. This implies that $\langle a,x\rangle$ is minimal nonabelian and so $[a,x^p] = 1$ and $x^p \in \mathrm{C}_G(A)$. Similarly, we get $y^p \in \mathrm{C}_G(A)$ and therefore if $\bar{T}$ is cyclic, then $|T/\mathrm{C}_T(A)| = p$.

In what follows we may assume that the quotient group $\bar{T}$ is not cyclic. Assume that $[A,x] = [A,y] = \langle s\rangle$ (where $o(s) = p$) and $\mathrm{C}_A(x) = \mathrm{C}_A(y)$. If $a \in A - \mathrm{C}_A(x)$, then we may set $a^x = as$ and $a^y = as^j$ with $j \not\equiv 0 \pmod{p}$. We have seen in the previous paragraph that $s \in \mathrm{Z}(A\langle x\rangle)$ and $s \in \mathrm{Z}(A\langle y\rangle)$. Hence we have $a^{x^{-j}} = as^{-j}$ and so $a^{x^{-j}y} = as^{-j+j} = a$ and $x^{-j}y \in \mathrm{C}_G(A)$, contrary to our assumption that $\bar{T}$ is not cyclic. We have proved that both $[A,x] = [A,y]$ and $\mathrm{C}_A(x) = \mathrm{C}_A(y)$ cannot hold.

Assume first that $xy \in \mathrm{T}_A$. If, in addition, $[A,x] = [A,y] = [A,T]$, then by the above $\mathrm{C}_A(x) \neq \mathrm{C}_A(y)$ and (a) holds since for each $v \in T - \mathrm{C}_G(A)$, $[A,v] = [A,T]$

is of order p and so $v \in \mathrm{T}_A$. If $[A, x] \neq [A, y]$, then we obtain $[A, x] \cap [A, y] = \{1\}$ and Lemma 121.3 implies that $\mathrm{C}_A(x) = \mathrm{C}_A(y) = \mathrm{C}_A(T)$ and (b) holds since for each $v \in T - \mathrm{C}_G(A)$ we conclude that $\mathrm{C}_A(v) = \mathrm{C}_A(T)$ is of index p in A and so $v \in \mathrm{T}_A$. We have $|A : \mathrm{C}_A(T)| = p$, $\mathrm{C}_A(T) \leq \mathrm{Z}(AT)$ and $A_0 = [A, x] \times [A, y] \leq \mathrm{C}_A(T)$. Considering $(AT)/A_0$, we see that both x and y centralize A/A_0 and so $T = \langle x, y\rangle$ centralizes A/A_0 which gives $[A, T] \leq A_0$ and $[A, T] = [A, x] \times [A, y]$.

Assume now that $xy \notin \mathrm{T}_A$. Since $xy \notin \mathrm{C}_G(A)$ (since $\bar{T}$ is noncyclic), we have $\mathrm{C}_A(xy) = \mathrm{C}_A(x) \cap \mathrm{C}_A(y)$ and so $\mathrm{b}_A(xy) = 2$ and $|[A, xy]| = p^2$. On the other hand, for each $a \in A$

$$[a, xy] = [a, y][a, x]^y = [a, y][a, x][[a, x], y] \in [A, x][A, y].$$

Thus $[A, xy] = [A, x] \times [A, y] = [A, T]$ and (c) holds. □

Lemma 121.5. *Let $x, u, v \in G$ be such that $uv^{-1} \notin \mathrm{C}_G(A)$ and $\mathrm{b}_A(x) > 1$. Then at least one of the elements u, v, uv, ux, vx, uvx is not in T_A.*

Proof. Assume that

$$\Omega = \{u, v, uv, ux, vx, uvx\} \subseteq \mathrm{T}_A.$$

Consider

$$T_1 = \langle uv^{-1}, u\rangle, \quad T_2 = \langle uv^{-1}, vx\rangle, \quad T_3 = \langle u, vx\rangle.$$

Then case (a) or (b) of Lemma 121.4 applies to each of the subgroups T_1, T_2, T_3. Indeed, considering $T_3 = \langle u, vx\rangle$, we have $u, vx, u(vx) \in \mathrm{T}_A$ and so (a) or (b) of Lemma 121.4 holds. Consider $T_1 = \langle uv^{-1}, u\rangle$, where $uv^{-1} \notin \mathrm{C}_G(A)$. We have $v \in T_1$ and so $T_1 = \langle uv^{-1}, u\rangle = \langle u, v\rangle$, where $u, v, uv \in \mathrm{T}_A$ and so (a) or (b) of Lemma 121.4 holds for T_1. In particular, $T_1 - \mathrm{C}_G(A) \subseteq \mathrm{T}_A$ and so $uv^{-1} \in \mathrm{T}_A$. Finally, consider $T_2 = \langle uv^{-1}, vx\rangle$. Since $uv^{-1}, vx, uv^{-1}vx = ux \in \mathrm{T}_A$, again (a) or (b) of Lemma 121.4 holds for T_3.

By Lemma 121.4, we have $|[A, T_i]| = p$ or p^2 for each $i \in \{1, 2, 3\}$. Then fix $i, j \in \{1, 2, 3\}$ such that $i \neq j$ and $|[A, T_i]| = |[A, T_j]|$. Since $i \neq j$, we have

$$\langle T_i, T_j\rangle = \langle \Omega\rangle \quad \text{and} \quad T_i \cap T_j \not\leq \mathrm{C}_G(A).$$

Indeed, each $T_k \leq \langle \Omega\rangle$, $k = 1, 2, 3$. Also,

$$\langle T_1, T_2\rangle = \langle uv^{-1}, u, vx\rangle = \langle u, v, x\rangle = \langle \Omega\rangle,$$

$$\langle T_1, T_3\rangle = \langle uv^{-1}, u, vx\rangle = \langle T_1, T_2\rangle = \langle \Omega\rangle,$$

$$\langle T_2, T_3\rangle = \langle uv^{-1}, u, vx\rangle = \langle T_1, T_2\rangle = \langle \Omega\rangle.$$

Finally,

$$uv^{-1} \in T_1 \cap T_2 \quad \text{and} \quad uv^{-1} \notin \mathrm{C}_G(A),$$

$$u \in T_1 \cap T_3 \quad \text{and} \quad u \in \mathrm{T}_A,$$

$$vx \in T_2 \cap T_3 \quad \text{and} \quad vx \in \mathrm{T}_A.$$

Hence $T_i \cap T_j \not\leq \mathrm{C}_G(A)$.

Assume that $|[A, T_i]| = |[A, T_j]| = p^2$. Then case (b) of Lemma 121.4 applies to T_i and T_j, and every element in $\langle\Omega\rangle - \mathrm{C}_G(A)$ has the same centralizer on A. Since $x \in \langle\Omega\rangle$, it follows that $x \in \mathrm{T}_A$, a contradiction.

Assume now that $|[A, T_i]| = |[A, T_j]| = p$. Then, due to Lemma 121.4(a) and (b), every element in $\langle\Omega\rangle - \mathrm{C}_G(A)$ has the same commutator with A. But $x \in \langle\Omega\rangle - \mathrm{C}_G(A)$ and so $|[A, x]| = p$ and $x \in \mathrm{T}_A$, a contradiction. □

Lemma 121.6. *Let $x \in G$ and $a \in A$. Then the following hold:*

(a) $[a, \mathrm{M}_{ax} \cap \mathrm{M}_x] \le [A, x]$.

(b) $[A, \mathrm{D}_x] \le [A, x] = [\mathrm{D}_x, x]$.

(c) $[\mathrm{G}_x, x] \le [A, G]$.

Proof. Let $y \in \mathrm{M}_{ax} = \mathrm{C}_G(ax)A$ so that $y = cb$ for some $c \in \mathrm{C}_G(ax)$ and $b \in A$. It follows

$$a^y x^y = (ax)^y = (ax)^{cb} = (ax)^b = ax^b$$

and this gives

$$\begin{aligned}[a, y] = a^{-1}a^y = a^{-1} \cdot ax^b(x^{-1})^y = x^b(x^{-1})^y = (x^b x^{-1})(x(x^{-1})^y)\\ = [b, x^{-1}][x^{-1}, y].\end{aligned}$$

In particular, $[x^{-1}, y] \in [A, G]$ and so (noting that $[A, G] \trianglelefteq G$) $[y, x] \in [A, G]$ which gives $[\mathrm{G}_x, x] \le [A, G]$, and this is (c).

Assume that $y \in \mathrm{M}_x$ and so $y = a'd$, where $a' \in A$ and $d \in \mathrm{C}_G(x)$. We get

$$[x^{-1}, y] = [x^{-1}, a'd] = [x^{-1}, d][x^{-1}, a']^d = [x^{-1}, (a')^d] \in [A, x^{-1}] = [A, x].$$

If, in addition, $y \in \mathrm{M}_{ax}$, then we know from the previous paragraph that $[a, y]$ can be written as $[a, y] = [b, x^{-1}][x^{-1}, y]$, where $b \in A$ and so $[a, y] \in [A, x]$, which is (a).

We note that $[\mathrm{M}_x, x] = [A, x]$. Indeed, if $y \in \mathrm{M}_x$, then $y = a'd$ with $a' \in A$, $d \in \mathrm{C}_G(x)$ and so

$$[a'd, x] = [a', x]^d[d, x] = [(a')^d, x] \in [A, x].$$

This result together with (a) yields

$$[a, \mathrm{D}_x] \le [a, \mathrm{M}_{ax} \cap \mathrm{M}_x] \le [A, x] \le [\mathrm{D}_x, x] \le [\mathrm{M}_x, x] = [A, x]$$

and thus $[A, \mathrm{D}_x] \le [A, x] = [\mathrm{D}_x, x]$ and this is (b). □

Lemma 121.7. *Let $\mathrm{b}_A > 1$. Suppose that $[G, z] \le [A, G]$ for all $z \in G$ satisfying*

$$(**) \qquad \mathrm{b}_A(z) > 1 \quad \textit{and} \quad 2\mathrm{b}_A(z) \ge \mathrm{b}_A.$$

Then $G' = [\mathrm{C}_G(A), G]$.

Proof. Let $x \in \mathrm{B}_A$ and $y \in G$. Then we have $[A, x] \leq [A, y][A, yx]$. Indeed, we obtain that $[A, y] = \{[a, y] \mid a \in A\}$ and for each $a \in A$,

$$\begin{aligned}[a, yx] &= [a, x][a, y]^x = [a, x][a, y][[a, y], x] \\ &= [a, y][a[a, y], x] = [a, y][a^y, x]\end{aligned}$$

which gives $[A, yx] = \{[a, y][a^y, x] \mid a \in A\}$. Thus, $[a^y, x] \in [A, y][A, yx]$ for all $a \in A$ and $\{[a^y, x] \mid a \in A\} = [A, x]$ which proves our assertion.

It follows that we have one of the following two cases (considering the subgroup $[A, y][A, yx]$ which contains $[A, x]$, where $|[A, x]| = p^{\mathrm{b}_A}$):

(1) y or yx satisfy $(**)$ for all $y \in G$, or

(2) y and $yx \in \mathrm{T}_A$ for some $y \in G$, and $\mathrm{b}_A = 2$.

Assume that we are in case (1). Then we have $[G, y] \leq [A, G]$ or $[G, yx] \leq [A, G]$ for all $y \in G$. Since x satisfies $(**)$, we also obtain $[G, x] \leq [A, G]$. Thus, if for an element $y \in G$, $[G, yx] \leq [A, G]$, we have for all $g \in G$, $[g, yx] = [g, x][g, y]^x$ and so $[g, y]^x \in [A, G]$ which implies $[g, y] \in [A, G]$ since $[A, G] \trianglelefteq G$ and therefore $[G, y] \leq [A, G]$ for all $g \in G$. Thus $G' = [A, G] = [\mathrm{C}_G(A), G]$.

Suppose that we are in case (2). Then $[G, z] \leq [A, G]$ for all $z \in G - (\mathrm{T}_A \cup \mathrm{C}_G(A))$ and thus $[G, z] \leq [\mathrm{C}_G(A), G]$ for every $z \in G - \mathrm{T}_A$. Assume that there exist $u, v \in G$ such that $[u, v] \notin [\mathrm{C}_G(A), G]$, i.e., $[G, u] \not\leq [\mathrm{C}_G(A), G]$ and $[G, v] \not\leq [\mathrm{C}_G(A), G]$. Then also $[uv, v], [ux, v], [vx, u], [uvx, v] \notin [\mathrm{C}_G(A), G]$. Indeed,

$$\begin{aligned}[uv, v] &= [u, v]^v \notin [\mathrm{C}_G(A), G], \\ [ux, v] &= [u, v]^x[x, v] \notin [\mathrm{C}_G(A), G]\end{aligned}$$

since $[x, v] \in [x, G] \leq [A, G]$, $[u, v] \notin [\mathrm{C}_G(A), G]$, and

$$\begin{aligned}[vx, u] &= [v, u]^x[x, u] \notin [\mathrm{C}_G(A), G], \\ [uvx, v] &= [uv, v]^x[x, v] \notin [\mathrm{C}_G(A), G]\end{aligned}$$

since $[x, v] \in [A, G]$ and $[uv, v]^x \notin [\mathrm{C}_G(A), G]$. Hence $u, v, uv, ux, vx, uvx \in \mathrm{T}_A$. Moreover,

$$[u, v]^{v^{-1}} = [u^{v^{-1}}, v] = [v(uv^{-1}), v)] = [uv^{-1}, v] \notin [\mathrm{C}_G(A), G]$$

and so $uv^{-1} \notin \mathrm{C}_G(A)$. But then Lemma 121.5 gives a contradiction. □

Lemma 121.8. *Suppose* $\mathrm{b}_A = 1$. *Then either*

(i) $|A : (A \cap \mathrm{Z}(G))| = p$ *and* $\mathrm{C}_A(x) = \mathrm{C}_A(y)$ *for every* $x, y \in G - \mathrm{C}_G(A)$, *or*

(ii) $|[A, G]| = p$. *If, in addition, A is a maximal normal abelian subgroup of G, then in case* (i) $|G : \mathrm{Z}(G))| \leq p^{1+b}$ *and in case* (ii) $\mathrm{b}(G/[A, G]) < \mathrm{b}(G)$.

Proof. If $G/\mathrm{C}_G(A)$ is cyclic, then there is $g \in G$ such that $G = \mathrm{C}_G(A)\langle g\rangle$. It follows that $|A/\mathrm{C}_A(g)| = p$, $\mathrm{C}_A(g) = \mathrm{Z}(G) \cap A$ and $[A, g] = [A, G]$ is of order p so (i) and (ii) hold.

Hence we may assume that there exist $x, y \in G$ such that for $T = \langle x, y\rangle$ the quotient group $T\mathrm{C}_G(A)/\mathrm{C}_G(A)$ is not cyclic. Then cases (a) or (b) of Lemma 121.4 hold for T.

Assume that (b) holds for T, i.e., $\mathrm{C}_A(x) = \mathrm{C}_A(y)$ and $[A, x] \neq [A, y]$. Then for every $z \in G - \mathrm{C}_G(A)$ either $[A, z] \neq [A, x]$ or $[A, z] \neq [A, y]$. Hence Lemma 121.4 applied to $\langle z, x\rangle$ or $\langle z, y\rangle$ gives $\mathrm{C}_A(x) = \mathrm{C}_A(y) = \mathrm{C}_A(z)$ and thus $\mathrm{C}_A(x) = A \cap \mathrm{Z}(G)$. This is (i).

Assume that (a) holds for T, i.e., $\mathrm{C}_A(x) \neq \mathrm{C}_A(y)$ and $[A, x] = [A, y]$. Thus for every $z \in G - \mathrm{C}_G(A)$ either $\mathrm{C}_A(z) \neq \mathrm{C}_A(x)$ or $\mathrm{C}_A(z) \neq \mathrm{C}_A(y)$. Hence another application of Lemma 121.4 gives $[A, x] = [A, y] = [A, z]$ and thus $[A, G] = [A, x]$ is of order p. This is (ii).

Let A be a maximal normal abelian subgroup of G. Suppose that (i) holds and let $a \in A - \mathrm{Z}(G)$. Then

$$\mathrm{C}_G(a) = A \quad \text{and} \quad |G : \mathrm{Z}(G)| = |G : A||A : \mathrm{Z}(G)| = |G : \mathrm{C}_G(a)|p \leq p^{\mathrm{b}+1}.$$

Assume that (ii) holds. Then $D = [A, G]$ is a normal subgroup of G of order p such that $\mathrm{b}(G/D) < \mathrm{b} = \mathrm{b}(G)$. □

Proposition 121.9 (Knoche). *Suppose that* $\mathrm{b} = \mathrm{b}(G) = 1$. *Then* $|G'| = p$.

Proof. We suppose, in addition, that A is a maximal normal abelian subgroup of G so that $\mathrm{C}_G(A) = A$. For every $x \in G - A$ we have $G = \mathrm{C}_G(x)A = \mathrm{D}_x = \mathrm{G}_x$. Hence Lemma 121.6(b) gives $|[G, A]| = p$ and Lemma 121.6(c) yields $[G, x] \leq [G, A]$ and so $G' = [G, A]$ is of order p. □

Proof of Theorem 121.1. Let A be a maximal normal abelian subgroup of G and suppose that $\mathrm{b} = \mathrm{b}(G) = 2$. If $\mathrm{b}_A = 2$ for some maximal normal abelian subgroup A of G, then for each $x \in G$ such that $\mathrm{b}_A(x) = 2$ we have $\mathrm{M}_x = \mathrm{C}_G(x)A = G$ so that $\mathrm{G}_x = G$ and Lemma 121.6(c) gives $[G, x] \leq [A, G]$. Hence the condition $(**)$ of Lemma 121.7 is satisfied and so $G' = [A, G]$. Since $G = \mathrm{M}_{ax} = \mathrm{C}_G(ax)A$ for every $a \in A$, we have $G = \mathrm{D}_x$ and so Lemma 121.6(b) gives $[A, G] \leq [A, x]$. Thus $[A, G] = [A, x]$ is of order p^2 and so $|G'| = |[A, x]| = p^2$. Hence we may assume that $\mathrm{b}_A = 1$ for every maximal normal abelian subgroup A of G. We discuss the two cases of Lemma 121.8.

Assume that case (i) of Lemma 121.8 holds. For $a \in A - \mathrm{Z}(G)$ we get $\mathrm{C}_G(a) = A$ and thus $|G/\mathrm{Z}(G)| \leq p^3$. Now, $\mathrm{b} = 2$ gives $|G/\mathrm{Z}(G)| = p^3$ and $|[A, G]| = p^2$ since a has exactly p^2 conjugates in G. Consider $\bar{G} = G/[A, G]$ so that $\bar{G}$ is either abelian or $\bar{A} = \mathrm{Z}(\bar{G})$, $\bar{G}/\bar{A} \cong \mathrm{E}_{p^2}$ and so $\bar{G}$ has more than one abelian maximal subgroup which implies $|\bar{G}'| = p$. Thus $|G'/[A, G]| \leq p$ and so we get (a) or (b) of our theorem.

Assume that case (ii) of Lemma 121.8 holds, i.e., $|[A, G]| = p$. Set $\bar{G} = G/[A, G]$. Then $\bar{A} \leq \mathrm{Z}(\bar{G})$ and $\mathrm{b}(\bar{G}) \leq 1$. Hence by Proposition 121.9, $|\bar{G}'| \leq p$. As $|[A, G]| = p$ and $\mathrm{b} = 2$, we conclude (by Proposition 121.9) that $|G'| = p^2$ and we get case (a) of our theorem.

Suppose that G satisfies (a) or (b) of our theorem. Then clearly $\mathrm{b} \leq 2$ and Proposition 121.9 gives $\mathrm{b} = 2$ since $|G'| > p$. Theorem 121.1 is proved. □

§122

p-groups all of whose subgroups have normalizers of index at most p

This section is written by the second author.

Here we give a proof of the following result which was proved for $p > 2$ and predicted for $p = 2$ by J. P. Bohanon in [Boh].

Theorem 122.1. *Let G be a p-group such that for each subgroup H of G we have $|G : \mathrm{N}_G(H)| \leq p$. Then the following holds:*

(a) *If $p = 2$, then $|G : \mathrm{Z}(G)| \leq 2^4$.*

(b) *If $p > 2$, then $|G : \mathrm{Z}(G)| \leq p^3$.*

Our proof is elementary but very involved. In particular, we do not use any computer results for 2-groups of orders $\leq 2^8$ which have the title property and also we do not use the representation theory for such groups in case $p > 2$.

We recall that the breadth $\mathrm{b}_G(x)$ of an element x in a p-group G is defined as

$$p^{\mathrm{b}_G(x)} = |G : \mathrm{C}_G(x)|,$$

and the (element) breadth $\mathrm{b}(G)$ of G is

$$\max\{\mathrm{b}_G(x) \mid x \in G\}.$$

Also, for an abelian normal subgroup A in a p-group G and an element $x \in G$ we set

$$p^{\mathrm{b}_A(x)} = |A : \mathrm{C}_A(x)|$$

and define

$$\begin{aligned} \mathrm{b}_A &= \mathrm{b}_A(G) = \max\{\mathrm{b}_A(x) \mid x \in G\}, \\ \mathrm{B}_A &= \{x \in G \mid \mathrm{b}_A(x) = \mathrm{b}_A(G)\}, \\ \mathrm{T}_A &= \{x \in G \mid \mathrm{b}_A(x) = 1\}. \end{aligned}$$

We define the subgroup breadth $\mathrm{sb}(G)$ of a p-group G by

$$p^{\mathrm{sb}(G)} = \max\{|G : \mathrm{N}_G(H)| \mid H \leq G\}.$$

Note that the title groups are either Dedekindian or have the subgroup breadth 1.

We shall first prove some preliminary results (Propositions 122.2 to 122.18) about p-groups with the subgroup breadth 1. Some of these results are of independent interest since they give additional information about such groups which is not contained in Theorem 122.1. In particular, Propositions 122.2, 122.7, 122.8, 122.13 and 122.16 give important properties of p-groups with the subgroup breadth 1.

Proposition 122.2. *Let G be a p-group with* $\mathrm{sb}(G) = 1$. *Then $\Phi(G)$ is abelian.*

Proof. Obviously, $\Phi(G)$ is Dedekindian and so either $\Phi(G)$ is abelian or $p = 2$ and $\Phi(G)$ is Hamiltonian, i.e., $\Phi(G) = Q \times V$, where $Q \cong \mathrm{Q}_8$ and $\exp(V) \leq 1$. Suppose that we are in the second case, where $V \neq \{1\}$ (by a classical result of Burnside). Set $U = \mathrm{Z}(Q) \times V$ so that $U = \mathrm{Z}(\Phi(G))$ is normal in G and $|U : V| = 2$. If $V \trianglelefteq G$, then $\Phi(G/V) = \Phi(G)/V \cong \mathrm{Q}_8$, contrary to a classical result of Burnside. Thus V is not normal in G and set $T = \mathrm{N}_G(V)$ so that $\Phi(G) < T$ and $|G : T| = 2$.

Take an element $g \in G - T$. We have $V^g \neq V$ and $V^g < U$. It follows that $V_0 = V \cap V^g$ is normal in G and $|V : V_0| = 2$. Hence $\Phi(G/V_0) = \Phi(G)/V_0 \cong \mathrm{Q}_8 \times \mathrm{C}_2$ and such groups G/V_0 are classified in Theorem 85.1. In particular, G/V_0 contains a subgroup H of order 2^6 given by

$$\begin{aligned} H = \langle x, y \mid\ & x^8 = y^8 = 1,\ x^4 = y^4 = z,\ x^2 = a,\ y^2 = b, \\ & [a,b] = z,\ a^y = at,\ t^2 = [t,a] = [t,b] = 1, \\ & t^x = t^y = tz,\ b^x = btz,\ (xy)^2 = tz^\epsilon,\ \epsilon = 0, 1\rangle, \end{aligned}$$

where

$$\langle a, b\rangle \cong \mathrm{Q}_8, \quad \Phi(H) = \langle a, b\rangle \times \langle t\rangle \cong \mathrm{Q}_8 \times \mathrm{C}_2, \quad \mathrm{Z}(H) = \mathrm{Z}(\langle a, b\rangle) = \langle z\rangle.$$

We have

$$a^y = at, \quad b^x = btz = b^{-1}t, \quad a^{yx} = (at)^x = at^x = atz = a^{-1}t$$

and so $\mathrm{N}_H(\langle a, b\rangle) = \Phi(H)$ is of index 4 in H, a contradiction. □

Proposition 122.3. *Let G be a p-group with* $\mathrm{sb}(G) = 1$. *If $A \leq G$ is a maximal normal abelian containing $\Phi(G)$ (noting that $\Phi(G)$ is abelian by Proposition 122.2), then $1 \leq \mathrm{b}_A(G) \leq 2$, i.e., for each $x \in G - A$ we have $p \leq |A : \mathrm{C}_A(x)| \leq p^2$.*

Proof. We infer that that $G/A \neq \{1\}$ is elementary abelian. Let $x \in G - A$ so that $x^p \in A$ and $|(A\langle x\rangle) : A| = p$. Set

$$M = \mathrm{N}_{A\langle x\rangle}(\langle x\rangle) \quad \text{and} \quad A_0 = M \cap A$$

so that $|(A\langle x\rangle) : M| \leq p$ and $|A : A_0| \leq p$. We have

$$M' \leq A_0 \cap \langle x\rangle = \langle x^p\rangle \leq \mathrm{Z}(A\langle x\rangle),$$

and so M is of class ≤ 2. Suppose that M is of class 2. For any $a \in A_0$ we have

$[a, x] \in \langle x^p \rangle \neq \{1\}$ since $M' \leq \langle x^p \rangle$ and $M' \neq \{1\}$. We get $[a, x]^p = [a, x^p] = 1$ and so $[A_0, \langle x \rangle] = \Omega_1(\langle x \rangle) = M'$ is of order p (see Lemma 121.2) which implies $|A_0 : \mathrm{C}_{A_0}(x)| = p$. Since $\mathrm{C}_G(A) = A$, we obtain $p \leq |A : \mathrm{C}_A(x)| \leq p^2$, and we are done. □

Proposition 122.4. *If $G = Q_1 Q_2$, where $[Q_1, Q_2] = \{1\}$ and $Q_1 \cong Q_2 \cong \mathrm{Q}_8$, then we have* $\mathrm{sb}(G) > 1$.

Proof. First suppose that

$$Q_1 \cap Q_2 = \mathrm{Z}(Q_1) = \mathrm{Z}(Q_2) = G' = \langle z \rangle$$

so that G is extraspecial of order 2^5 and "type +". In this case, G possesses a four-subgroup S such that $S \cap \langle z \rangle = \{1\}$. We have $[\mathrm{N}_G(S), S] \leq S \cap \langle z \rangle = \{1\}$ and so $\mathrm{N}_G(S) = \mathrm{C}_G(S) = S \times \langle z \rangle$ which gives $|G : \mathrm{N}_G(S)| = 4$.

Assume now that $G = Q_1 \times Q_2$, and set $Q_1 = \langle a_1, b_1 \rangle$ with $Q_1' = \langle z_1 \rangle$ and $Q_2 = \langle a_2, b_2 \rangle$ with $Q_2' = \langle z_2 \rangle$. Considering the subgroup $U = \langle a_1 a_2, b_1 b_2 \rangle$ with $U' = \langle z_1 z_2 \rangle$, we have $G = Q_1 U$ with $Q_1 \cap U = \{1\}$ and so $\mathrm{N}_G(U) = U \mathrm{N}_{Q_1}(U)$, where $\mathrm{N}_{Q_1}(U) = \mathrm{C}_{Q_1}(U)$. But

$$(b_1 b_2)^{a_1} = b_1 b_2 z_1, \quad (a_1 a_2)^{b_1} = a_1 a_2 z_1, \quad (b_1 b_2)^{b_1 a_1} = b_1 b_2 z_1$$

and so $\mathrm{C}_{Q_1}(U) = \langle z_1 \rangle$ which gives $\mathrm{N}_G(U) = U \times \langle z_1 \rangle$ and we are done. □

Proposition 122.5 (J. Shareshian). *Let G be a 2-group with* $\mathrm{sb}(G) = 1$ *and we assume that G possesses two involutions which do not commute. Then $|G : \mathrm{Z}(G)| \leq 2^4$ and $|G'| \leq 4$ so that* $\mathrm{b}(G) \leq 2$.

Proof. Let s, t be involutions in G which do not commute. Then $\langle s, t \rangle \cong \mathrm{D}_{2^n}$ is a dihedral subgroup of order 2^n, $n \geq 3$. If $n > 3$, then $\mathrm{sb}(\mathrm{D}_{2^n}) > 1$ and so $D = \langle s, t \rangle \cong \mathrm{D}_8$. Set $\mathrm{Z}(D) = \langle z \rangle$ and note that $\{s, sz\}$ and $\{t, tz\}$ are already complete conjugate classes in G of s and t, respectively. This implies $\langle s, z \rangle \trianglelefteq G$, $\langle t, z \rangle \trianglelefteq G$, $D \trianglelefteq G$, $G = D * C$, where $C = \mathrm{C}_G(D)$ and $D \cap C = \langle z \rangle$. If C is Dedekindian, then the fact that $\mathrm{Z}(C) = \mathrm{Z}(G)$ implies $|G : \mathrm{Z}(G)| \leq 2^4$ and $|G'| \leq 4$. Suppose that C has a nonnormal subgroup H such that $\langle z \rangle \not\leq H$ and let $K \neq H$ be a conjugate of H in C. Then the four subgroups

$$\langle t, H \rangle = \langle t \rangle \times \langle H \rangle, \quad \langle t, K \rangle, \quad \langle tz, H \rangle, \quad \langle tz, K \rangle$$

are pairwise distinct and conjugate subgroups in G, a contradiction. Hence, assuming that C is not Dedekindian, each nonnormal subgroup of C contains $\langle z \rangle$. Such groups C are completely determined by N. Blackburn (see Corollary 92.7) and so we have one of the following three possibilities:

(1) $C \cong \mathrm{Q}_8 \times \mathrm{C}_4 \times \mathrm{E}_{2^s}$;

(2) $C \cong \mathrm{Q}_8 \times \mathrm{Q}_8 \times \mathrm{E}_{2^s}$ $(s \geq 0)$;

(3) C has an abelian normal subgroup A of exponent > 2 with $|C : A| = 2$ and an element g of order 4 in $C - A$ such that $g^2 = z$ and g inverts each element in A.

In case (1), $|G : \mathrm{Z}(G)| = 2^4$ and $|G'| \leq 4$. In case (2), $\mathrm{sb}(\mathrm{Q}_8 \times \mathrm{Q}_8) > 1$ (by Proposition 122.4), a contradiction. Assume that we are in case (3). Note that $(st)^2 = z$ so that stg is an involution that inverts on A. As $\mathrm{sb}(\mathrm{D}_{16}) > 1$, we must have $\exp(A) = 4$. Suppose that there exists $b \in A$ such that $o(b) = 4$ and $b^2 \neq z = g^2$. We obtain that $\langle stg, b\rangle \cong \mathrm{D}_8$ so that $(stg)^b = stgb^2$. Also, $(stg)^s = stgz$ and $(stgb^2)^s = stgzb^2$. It follows that the four involutions stg, $stgz$, $stgb^2$, $stgzb^2$ are pairwise distinct and conjugate, a contradiction. Therefore we have an element $h \in A$ such that $h^2 = z$, $h^g = h^{-1}$, $\langle h, g\rangle \cong \mathrm{Q}_8$ and $C \cong \mathrm{Q}_8 \times \mathrm{E}_{2^s}$. But then C is Dedekindian, contrary to our assumption. □

Proposition 122.6 (J. Shareshian). *Let G be a 2-group with $\mathrm{sb}(G) = 1$, $\mathrm{Z}(G)$ is cyclic and all involutions of G commute with each other. Then G contains at most three involutions.*

Proof. Suppose that our proposition is false. Since $\Omega_1(G)$ is elementary abelian of order ≥ 8, G possesses a normal elementary abelian subgroup E of order 8. Let z be the unique involution in E which lies in $\mathrm{Z}(G)$, and let t be any involution in $E - \langle z\rangle$. Since $|G : \mathrm{C}_G(t)| = 2$, there are exactly two conjugates $\{t, t'\}$ of t in G and so the four-subgroup $\langle t, t'\rangle$ is normal in G which implies $z \in \langle t, t'\rangle$ and so $t' = tz$. This gives $[G, E] = \langle z\rangle$. Set $E = \langle z, s, t\rangle$ and consider the four-subgroup $S = \langle s, t\rangle$. We have $[\mathrm{N}_G(S), S] \leq S \cap \langle z\rangle = \{1\}$ and so $\mathrm{N}_G(S) = \mathrm{C}_G(S) = \mathrm{C}_G(s) \cap \mathrm{C}_G(t)$, where $\mathrm{C}_G(s)$ and $\mathrm{C}_G(t)$ are subgroups of index 2 in G. Since $|G : \mathrm{N}_G(S)| = 2$, we get $\mathrm{C}_G(s) = \mathrm{C}_G(t) = \mathrm{C}_G(E)$ with $|G : \mathrm{C}_G(E)| = 2$. Let $g \in G - \mathrm{C}_G(E)$ so that $s^g = sz$ and $t^g = tz$. But then $(st)^g = st$ and so $st \in \mathrm{Z}(G)$, a contradiction. □

Proposition 122.7. *Let G be a metacyclic p-group with $|G'| = p^2$. If $\mathrm{sb}(G) = 1$, then $p = 2$ and either $G \cong \mathrm{Q}_{16}$ or*

$$G = \langle a, b \mid a^8 = 1,\ b^{2^n} = a^4,\ a^b = a^{-1+4\eta}\rangle,$$

where $n \geq 2$ and $\eta = 0, 1$.

Proof. First suppose $|G| = p^4$. Then G has a cyclic subgroup H of index p. If $p > 2$, then $G \cong \mathrm{M}_{p^4}$ and $|G'| = p$, a contradiction. We have $p = 2$ and G is of maximal class. If G is dihedral or semidihedral, then there exists an involution $i \in G - H$ and $|G : \mathrm{C}_G(i)| = 4$, a contradiction. Hence we obtain in this case that $G \cong \mathrm{Q}_{16}$.

Now suppose that $|G| > p^4$. In view of Corollary 65.3, a metacyclic p-group G is an A_2-group if and only if $|G'| = p^2$. According to Proposition 71.2, we have two possibilities for the structure of G:

(a) $$G = \langle a, b \mid a^{p^m} = 1,\ b^{p^n} = a^{\epsilon p^{m-1}},\ a^b = a^{1+p^{m-2}}\rangle,$$

where $m \geq 3$, $n \geq 2$, $\epsilon = 0, 1$, and in case $p = 2$, $m \geq 4$;

(b) $$p = 2, \quad G = \langle a, b \mid a^8 = 1, , b^{2^n} = a^{4\epsilon},\ a^b = a^{-1+4\eta}\rangle,$$

where $n \geq 2$, $\epsilon, \eta = 0, 1$.

Suppose that G is a 2-group in (b). If $\epsilon = 0$, then $|G : \mathrm{N}_G(\langle b\rangle)| = 2$ implies that b centralizes $\langle a^2\rangle$, a contradiction. Hence $\epsilon = 1$ and we have obtained all 2-groups stated in our proposition. It remains to be shown that all groups in (a) are not of subgroup breadth 1.

Suppose that G is a p-group from (a). If $\epsilon = 0$, then $|G : \mathrm{N}_G(\langle b\rangle)| = p$ gives that b centralizes a^p, a contradiction. Hence $\epsilon = 1$ and so we may set

$$G = \langle a, b \mid a^{p^m} = b^{-p^n} = z,\ z^p = 1,\ a^{p^{m-1}} = v,\ a^b = av\rangle,$$

where $m \geq 2, n \geq 2$, and if $p = 2$, then $m \geq 3$. We have $|G| = p^{m+n+1}$, $[a, b] = v$, $[a^p, b] = z$, $[a^{p^2}, b] = 1$, $G' = \langle v\rangle$ and G is of class 2 if and only if $m \geq 3$ since in that case $\langle v\rangle \leq \langle a^{p^2}\rangle \leq \mathrm{Z}(G)$.

(i) First assume $m \geq 3$ so that G is of class 2. In that case, we also have $[a, b^p] = z$, $[a, b^{p^2}] = 1$.

(i1) Suppose $m = n$. Since $\langle ba\rangle$ covers $G/\langle a\rangle \cong \mathrm{C}_{p^n}$, it follows that $o(ba) \geq p^n$. On the other hand,

$$(ba)^{p^n} = b^{p^n} a^{p^n} [a, b]^{\binom{p^n}{2}} = z^{-1} z = 1$$

and so $G = \langle a\rangle\langle ba\rangle$ with $\langle a\rangle \cap \langle ba\rangle$. But a^p normalizes $\langle ba\rangle$ and so we conclude that $\langle a^p\rangle\langle ba\rangle = \langle a^p\rangle \times \langle ba\rangle$ which gives $\mathrm{C}_G(a^p) = G$, a contradiction.

(i2) Suppose $m > n$. Then there is $a' \in \langle a\rangle$ such that $\langle a'\rangle < \langle a\rangle$ and $(a')^{p^n} = z$. Here again $\langle ba'\rangle$ covers $G/\langle a\rangle \cong \mathrm{C}_{p^n}$ and so $o(ba') \geq p^n$. On the other hand,

$$(ba')^{p^n} = b^{p^n} (a')^{p^n} [a', b]^{\binom{p^n}{2}} = z^{-1} z = 1$$

since $a' \in \langle a^p\rangle$ and so $[a', b] \in \langle z\rangle$. Thus G is a splitting extension of $\langle a\rangle$ by $\langle ba'\rangle$. It follows that a^p normalizes $\langle ba'\rangle$ and so a^p centralizes $\langle ba'\rangle$, $a^p \in \mathrm{Z}(G)$, a contradiction.

(i3) Suppose $n > m$. Then there is $b' \in \langle b\rangle$ such that $\langle b'\rangle < \langle b\rangle$ and $(b')^{p^m} = z^{-1}$. Since $b' \in \langle b^p\rangle$, it follows that $[a, b'] \in \langle z\rangle$. We get

$$(b'a)^{p^m} = (b')^{p^m} a^{p^m} [a, b']^{\binom{p^m}{2}} = z^{-1} z = 1$$

and

$$(b'a)^{p^{m-1}} = (b')^{p^{m-1}} a^{p^{m-1}} [a, b']^{\binom{p^{m-1}}{2}} = (b')^{p^{m-1}} v \neq 1,$$

and so $o(b'a) = p^m$ and $\langle b\rangle \cap \langle b'a\rangle = \{1\}$ since $(b')^{p^{m-1}} v$ is an element of order p which is not contained in $\langle z\rangle$ (noting that $v \in \langle a\rangle$ and $(b')^{p^{m-1}} \notin \langle a\rangle$). Now, we get $G = \langle b, b'a\rangle = \langle b\rangle\langle b'a\rangle$ since $o(b) = p^{n+1}$, $o(b'a) = p^m$, $\langle b\rangle \cap \langle b'a\rangle = \{1\}$, and $|G| = p^{m+n+1}$. But b^p normalizes $\langle b'a\rangle$ and so $[b'a, b^p] \in \langle v\rangle \cap \langle b'a\rangle = \{1\}$ which gives $b^p \in \mathrm{Z}(G)$, contrary to $[a, b^p] = z$.

(ii) Assume that $m = 2$ so that G is of class 3, $G' = \langle v\rangle$, $[G, G'] = \langle z\rangle$ and $p > 2$.

(ii1) Suppose, in addition, that $m = n = 2$ so that $|G| = p^5$. Since $\langle ba\rangle$ covers $G/\langle a\rangle \cong \mathrm{C}_{p^2}$, we have $o(ba) \geq p^2$. By the Hall–Petrescu formula (Appendix A.1),

$$(ba)^{p^2} = b^{p^2} a^{p^2} c_2^{\binom{p^2}{2}} c_3^{\binom{p^2}{3}},$$

where $c_2 \in \langle v\rangle$, $c_3 \in \langle z\rangle$ and so $(ba)^{p^2} = z^{-1}z = 1$ which gives $o(ba) = p^2$. Hence $G = \langle a\rangle\langle ba\rangle$ with $\langle a\rangle \cap \langle ba\rangle = \{1\}$. On the other hand, $a^p = v$ normalizes $\langle ba\rangle$ and so v centralizes ba. We get $\mathrm{C}_G(v) \geq \langle a, ba\rangle = G$, contrary to $v^b = vz$.

(ii2) Suppose $n > 2$. Then there is $b' \in \langle b\rangle$ such that $\langle b'\rangle < \langle b\rangle$ and $(b')^{p^2} = z^{-1}$. Note that $\langle a, b'\rangle$ is a proper subgroup of the A_2-group G and so $\langle a, b'\rangle$ is abelian or minimal nonabelian which gives $[a, b'] \in \langle z\rangle$. We get

$$(b'a)^{p^2} = (b')^{p^2} a^{p^2} [a, b']^{\binom{p^2}{2}} = z^{-1}z = 1$$

and so $o(b'a) \leq p^2$. Also, we obtain

$$(b'a)^p = (b')^p a^p [a, b']^{\binom{p}{2}} = (b')^p v \neq 1$$

since $(b')^p v$ is an element of order p which is not contained in $\langle z\rangle$ (indeed, $\langle v\rangle \leq \langle a\rangle$ and $(b')^p \notin \langle a\rangle$, and so $(b')^p v \notin \langle a\rangle$). Hence $G = \langle b\rangle\langle b'a\rangle$ with $\langle b\rangle \cap \langle b'a\rangle = \{1\}$. Then b^p normalizes $\langle b'a\rangle$ and so $[b^p, \langle b'a\rangle] \leq \langle b'a\rangle \cap \langle v\rangle = \{1\}$. Thus we obtain that $\mathrm{C}_G(b^p) \geq \langle b, b'a\rangle = G$ and so $b^p \in \mathrm{Z}(G)$. But then $\langle b\rangle$ induces on $\langle a\rangle$ an automorphism of order p which implies that $|G'| = p$, a contradiction. Our proposition is proved. □

Proposition 122.8. *Let G be a p-group with* $\mathrm{sb}(G) = 1$. *Then* $\mathrm{b}(G) \leq 2$ *if* $p > 2$ *and* $\mathrm{b}(G) \leq 3$ *if* $p = 2$.

Proof. Let A be a maximal normal abelian subgroup of G which contains $\Phi(G)$ (noting that $\Phi(G)$ is abelian by Proposition 122.2). By Proposition 122.3, $1 \leq \mathrm{b}_A(G) \leq 2$.

Let $x \in A$ so that $\mathrm{N}_G(\langle x\rangle) \geq A$ and $|G : \mathrm{N}_G(\langle x\rangle)| \leq p$. We have $\mathrm{C}_G(x) \geq A$ and $\mathrm{N}_G(\langle x\rangle)/\mathrm{C}_G(x)$ is elementary abelian acting faithfully on $\langle x\rangle$. Hence, if $p > 2$, then $|\mathrm{N}_G(\langle x\rangle)/\mathrm{C}_G(x)| \leq p$ and if $p = 2$, then $|\mathrm{N}_G(\langle x\rangle)/\mathrm{C}_G(x)| \leq 4$. In the first case $\mathrm{b}_G(x) \leq 2$ and in the second case $\mathrm{b}_G(x) \leq 3$.

Let $x \in G - A$ and assume that $|A : \mathrm{C}_A(x)| = p$. First suppose, in addition, that the subgroup A does not normalize $\langle x\rangle$ in which case $\mathrm{N}_G(\langle x\rangle)$ covers G/A and we have $\mathrm{N}_G(\langle x\rangle) \cap A = \mathrm{C}_A(x)$. Since $\mathrm{N}_G(\langle x\rangle)/\mathrm{C}_G(x)$ is elementary abelian of order $\leq p$ in case $p > 2$ and elementary abelian of order ≤ 4 if $p = 2$, we get again $\mathrm{b}_G(x) \leq 2$ for $p > 2$ and $\mathrm{b}_G(x) \leq 3$ for $p = 2$. Now suppose that A normalizes $\langle x\rangle$ so that $\mathrm{N}_G(\langle x\rangle) \geq A$ and $|G : \mathrm{N}_G(\langle x\rangle)| \leq p$. Assume that $p > 2$ and that $\mathrm{C}_G(x)$ does not cover $\mathrm{N}_G(\langle x\rangle)/A$. Then $|\mathrm{N}_G(\langle x\rangle)/(A\mathrm{C}_G(x))| = p$ and $\mathrm{N}_G(\langle x\rangle)/\mathrm{C}_G(x) \cong \mathrm{C}_{p^2}$. Let $y \in \mathrm{N}_G(\langle x\rangle) - \mathrm{C}_G(x)$ be such that $\langle y\rangle$ covers $\mathrm{N}_G(\langle x\rangle)/\mathrm{C}_G(x)$ so that $y^p \in A - \mathrm{C}_A(x)$ and $y^{p^2} \in \mathrm{C}_A(x)$. In that case, we have $o(x) \geq p^3$ and $x^y = xv$, where $v \in \langle x^p\rangle$ and $o(v) = p^2$. Consider the metacyclic subgroup $H = \langle x\rangle\langle y\rangle$ with $H' = \langle v\rangle \cong \mathrm{C}_{p^2}$.

Since $\mathrm{sb}(H) = 1$, Proposition 122.7 gives a contradiction. Hence if $p > 2$, $\mathrm{C}_G(x)$ must cover $\mathrm{N}_G(\langle x\rangle)/A$ and so in this case $\mathrm{b}_G(x) \leq 2$. Now assume that $p = 2$ and also $\mathrm{N}_G(\langle x\rangle)/(A\mathrm{C}_G(x)) \cong \mathrm{E}_4$ which implies that $\mathrm{N}_G(\langle x\rangle)/\mathrm{C}_G(x) \cong \mathrm{C}_4 \times \mathrm{C}_2$. Then there exists again an element $y \in \mathrm{N}_G(\langle x\rangle)$ such that $y^2 \in A - \mathrm{C}_A(x)$ and $x^y = xv$, $v \in \langle x^2\rangle$, $o(v) = 4$ and $o(x) \geq 2^4$. Considering the metacyclic subgroup $K = \langle x\rangle\langle y\rangle$ with $K' = \langle v\rangle \cong \mathrm{C}_4$, Proposition 122,7 gives again a contradiction. Hence we obtain that $|\mathrm{N}_G(\langle x\rangle)/(A\mathrm{C}_G(x))| \leq 2$ which implies in this case $\mathrm{b}_G(x) \leq 3$.

We consider now an element $g \in G-A$ such that $|A : \mathrm{C}_A(g)| = p^2$. Set $P = A\langle g\rangle$, where $g^p \in \mathrm{C}_A(g)$. By Lemma 121.2, $|[A, g]| = p^2$. If $\langle g\rangle \trianglelefteq P$, then

$$P' \leq A \cap \langle g\rangle = \langle g^p\rangle \leq \mathrm{Z}(P), \quad [A, g] \leq \langle g^p\rangle,$$

and so P is of class 2 and for each $a \in A$, $[a, g]^p = [a, g^p] = 1$ and this implies $[A, g] = \Omega_1(\langle g\rangle)$, contrary to $|[A, g]| = p^2$. Hence $|P : \mathrm{N}_P(\langle g\rangle)| = p$ which yields that $\mathrm{N}_G(\langle g\rangle)$ covers G/A. Set $A_1 = \mathrm{N}_A(\langle g\rangle)$ so that $A_1 \trianglelefteq G$. Suppose that in case $p > 2$, $|\mathrm{N}_G(\langle g\rangle) : (A_1\mathrm{C}_G(g))| = p$ and in case $p = 2$, $|\mathrm{N}_G(\langle g\rangle) : (A_1\mathrm{C}_G(g))| = 4$. Then in both cases there is $y \in \mathrm{N}_G(\langle g\rangle) - (A_1\mathrm{C}_G(g))$ such that $y^p \in A_1 - \mathrm{C}_A(g)$ and $g^y = gv$, where $v \in \langle g^p\rangle$, $o(v) = p^2$, $o(g) \geq p^3$ and in case $p = 2$, $o(g) \geq 2^4$. Considering the metacyclic subgroup $L = \langle g\rangle\langle y\rangle$ with $L' = \langle v\rangle \cong \mathrm{C}_{p^2}$, Proposition 122.7 gives a contradiction. Hence in case $p > 2$, $\mathrm{C}_G(g)$ covers $\mathrm{N}_G(\langle g\rangle)/A_1$ and so $\mathrm{b}_G(g) = 2$, and in case $p = 2$, $|\mathrm{N}_G(\langle g\rangle)/(A_1\mathrm{C}_G(g))| \leq 2$ so that in this case $\mathrm{b}_G(g) \leq 3$ and we are done. □

Proposition 122.9. *Let G be a p-group with* $\mathrm{sb}(G) = 1$. *If G is a minimal counterexample to Theorem 122.1, then* $\Omega_1(\mathrm{Z}(G)) \leq G'$.

Proof. Let G be a minimal counterexample to Theorem 122.1 and suppose that there is $i \in \Omega_1(\mathrm{Z}(G))$ with $i \notin G'$. Set $Z/\langle i\rangle = \mathrm{Z}(G/\langle i\rangle)$ so that for $p > 2$, $|G/Z| \leq p^3$ and for $p = 2$, $|G/Z| \leq 2^4$. Since $[G, Z] \leq \langle i\rangle$ and $i \notin G'$, we get $[G, Z] = \{1\}$ and so $Z = \mathrm{Z}(G)$, contrary to the fact that G was a minimal counterexample to Theorem 122.1. □

Proposition 122.10. *Let G be a p-group with* $\mathrm{sb}(G) = 1$. *Let A be a maximal normal abelian subgroup of G containing $\Phi(G)$ such that* $\mathrm{b}_A(G) = 1$ *(i.e., for each $x \in G-A$, $|A : \mathrm{C}_A(x)| = p$). Then Theorem 122.1 holds.*

Proof. Let G be a minimal counterexample to this proposition. Using Lemma 121.8, we have either $|A : \mathrm{Z}(G)| = p$ or $|[G, A]| = p$.

(i) First assume $|A : \mathrm{Z}(G)| = p$. Let $a \in A - \mathrm{Z}(G)$ so that $\mathrm{C}_G(a) = A$. In case $|G/A| \leq p^2$, we get $|G/\mathrm{Z}(G)| \leq p^3$, which contradicts the fact that G is a minimal counterexample. Hence $|G/A| \geq p^3$ and then Proposition 122.8 forces $p = 2$ and $\mathrm{b}_G(a) = 3$ so that $|G/A| = 2^3$. But then $|G/\mathrm{Z}(G)| = 2^4$, a contradiction.

(ii) Now assume $[G, A] = \langle z\rangle$ is of order p. We may also assume $|A/\mathrm{Z}(G)| > p$ which forces $|G/A| > p$. For any $x, y \in G - A$ such that $\langle x, y\rangle A/A \cong \mathrm{E}_{p^2}$ we have, by Lemma 121.4, $\mathrm{C}_A(x) \neq \mathrm{C}_A(y)$. We show that $\Phi(A) \leq \mathrm{Z}(G)$. Indeed, if $a \in A$

and $g \in G$ are such that $[a, g] \neq 1$, then $[a, g] \in \langle z \rangle \leq \mathrm{Z}(G)$ so that $\langle a, g \rangle' = \langle z \rangle$ and therefore $\langle a, g \rangle$ is minimal nonabelian. Then $a^p \in \Phi(\langle a, g \rangle) = \mathrm{Z}(\langle a, g \rangle)$ and so $[a^p, g] = 1$ which gives $a^p \in \mathrm{Z}(G)$.

Due to Proposition 73.8, A possesses a basis $\{a_1, a_2, \ldots, a_n\}$, $n \geq 2$, (noting that $\mho_1(A) \leq \mathrm{Z}(G)$) such that $z \in \langle a_n \rangle$. Set $A_0 = \langle a_1, \ldots, a_{n-1} \rangle$ and $G_0 = \mathrm{N}_G(A_0)$ so that $|G : G_0| \leq p$. We get $[G_0, A_0] \leq A_0 \cap \langle z \rangle = 1$ so that $A^* = A_0 \times \langle a_n^p \rangle = \mathrm{Z}(G_0)$, where $|A : A^*| = p$. If $|G_0 : A| > p$, then there are elements $x, y \in G_0 - A$ such that $\langle x, y \rangle A/A \cong \mathrm{E}_{p^2}$ and $\mathrm{C}_A(x) = \mathrm{C}_A(y) = A^*$, contrary to the above remark. Hence $|G_0/A| \leq p$ which together with $|G/A| > p$ gives $G/A \cong \mathrm{E}_{p^2}$ and $|G : G_0| = p$. Let $g_1, g_2 \in G - A$ so that $\langle g_1, g_2 \rangle$ covers G/A. Then $\mathrm{C}_A(g_1) \neq \mathrm{C}_A(g_2)$ (by the above remark) yields $\mathrm{C}_A(g_1) \cap \mathrm{C}_A(g_2) = \mathrm{Z}(G)$, $A/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ and for each $x \in A - \mathrm{Z}(G)$, $|G : \mathrm{C}_G(x)| = p$. If $p = 2$, then $|G/\mathrm{Z}(G)| = 2^4$, a contradiction. We must have $p > 2$ and then Proposition 122.8 implies $\mathrm{b}(G) \leq 2$.

By Proposition 73.8, $\mathrm{Z}(G)$ has a basis $\{z_1, z_2, \ldots, z_r\}$, $r \geq 1$, such that $z \in \langle z_1 \rangle$. In case $r > 1$, we consider the subgroup $S = \langle z_2, \ldots, z_r \rangle \neq \{1\}$ and the factor group G/S. Let $g \in G - A$ and assume that $[g, A] \leq S$. But then $[g, A] \leq S \cap \langle z \rangle = 1$ and so g centralizes A, a contradiction. Hence A/S is a maximal normal abelian subgroup of G/S. Let $a \in A - \mathrm{Z}(G)$ and assume $[G, a] \leq S$. Then $[G, a] \leq S \cap \langle z \rangle = 1$ and so $a \in \mathrm{Z}(G)$, a contradiction. Hence $\mathrm{Z}(G)/S = \mathrm{Z}(G/S)$ and so $|G/S : \mathrm{Z}(G/S)| = p^4$. This contradicts the fact that G was a minimal counterexample to our proposition. It follows that $S = \{1\}$ and so $\mathrm{Z}(G) = \langle z_1 \rangle$ is cyclic.

Suppose that z_1 is not a p-th power of any element in the subgroup A. Then for each $x \in A - \mathrm{Z}(G)$ we have $x^p \in \langle z_1^p \rangle$ and so $\langle z_1 \rangle$ is a cyclic subgroup of the maximal possible order in A. Then there is a complement $U \cong \mathrm{E}_{p^2}$ of $\langle z_1 \rangle$ in A. We obtain that $|\mathrm{N}_G(U) : A| \geq p$ and $[\mathrm{N}_G(U), U] \leq U \cap \langle z \rangle = \{1\}$ and so $\mathrm{N}_G(U)$ centralizes A, a contradiction. Hence we may set $A = \langle a \rangle \times \langle b \rangle$, where $a^p = z_1$, $\langle a^p \rangle = \mathrm{Z}(G)$, $z \in \langle a^p \rangle$, and $o(b) = p$.

We shall prove that there are no elements of order p in $G - A$. Assume that there is an element c of order p in $G - A$. First suppose $[b, c] \neq 1$ so that $\langle [b, c] \rangle = \langle z \rangle$ and $T = \langle b, c \rangle \cong \mathrm{S}(p^3)$ is the nonabelian group of order p^3 and exponent p with $\mathrm{Z}(T) = \langle z \rangle$. All p conjugates of b in G are contained in $\langle b, z \rangle$ and all p conjugates of c in G are contained in $\langle c, z \rangle$ which implies $\langle b, z \rangle \trianglelefteq G$, $\langle c, z \rangle \trianglelefteq G$, $\langle T \rangle \trianglelefteq G$, and $G = T * H$, where $H = \mathrm{C}_G(T)$ with $T \cap H = \langle z \rangle$. We have $\mathrm{Z}(H) = \mathrm{Z}(G) = \langle z_1 \rangle$ and $H/\mathrm{Z}(H) \cong \mathrm{E}_{p^2}$. Since all $p + 1$ maximal subgroups of H containing $\langle z_1 \rangle$ are abelian, we obtain that $|H'| = p$, $H' \leq \langle z_1 \rangle$ and so $H' = \langle z \rangle$ and $G' = \langle z \rangle$. Due to the fact that $\Phi(G) = \Phi(T)\Phi(H) \leq \langle z_1 \rangle$ and $\Phi(A) = \langle z_1 \rangle$, we get $\Phi(H) = \langle z_1 \rangle$ and so H is minimal nonabelian. It follows that either $H \cong \mathrm{S}(p^3)$ or $H \cong \mathrm{M}_{p^n}$, $n \geq 3$. In any case, there is an element d of order p in $H - \mathrm{Z}(H)$. We have

$$[\mathrm{N}_G(\langle b, d \rangle), \langle b, d \rangle] \leq \langle b, d \rangle \cap \langle z \rangle = \{1\},$$

and so

$$\mathrm{N}_G(\langle b, d \rangle) = \mathrm{C}_G(\langle b, d \rangle) = \mathrm{C}_G(b) \cap \mathrm{C}_G(d) = (H\langle b \rangle) \cap (T\langle z_1, d \rangle) = \langle z_1 \rangle \langle b, d \rangle$$

which is of index p^2 in G, a contradiction. Thus we have proved that $[b, c] = 1$. Since $(A\langle c\rangle)' = \langle z\rangle$, we get

$$\mathrm{N}_{A\langle c\rangle}(\langle b, c\rangle) = \mathrm{C}_{A\langle c\rangle}(\langle b, c\rangle) = \mathrm{C}_{A\langle c\rangle}(c)$$

which is of index p in $A\langle c\rangle$. Due to $|G : \mathrm{N}_G(\langle b, c\rangle)| = p$, it follows that $\mathrm{N}_G(\langle b, c\rangle)$ covers G/A. But $A \trianglelefteq G$ and $\langle b, c\rangle \cap A = \langle b\rangle$ and so $\mathrm{N}_G(\langle b\rangle) = \mathrm{C}_G(\langle b\rangle)$ also covers G/A and so $b \in \mathrm{Z}(G)$, a contradiction. We have proved

$$\Omega_1(G) = \Omega_1(A) = \langle b, z\rangle \cong \mathrm{E}_{p^2}.$$

Since $|G/\mathrm{Z}(G)| = p^4$, we have $|G| \geq p^5$. If $\mathrm{b}(G) = 1$, then Proposition 121.9 (Knoche) implies $|G'| = p$. In case $\mathrm{b}(G) = 2$, Theorem 121.1 yields that $|G'| = p^2$. By Theorem 13.7, G is metacyclic (since G cannot be a 3-group of maximal class because $|G'| \leq p^2$ and $|G| \geq p^5$). If $|G'| = p$, then G is minimal nonabelian in which case $|G/\mathrm{Z}(G)| = p^2$, a contradiction. Finally, if $|G'| = p^2$, then Proposition 122.7 gives a contradiction. □

Proposition 122.11. *Let G be a 2-group with $|G'| = 2$ such that $G/\mathrm{Z}(G) \cong \mathrm{E}_{16}$. Suppose that G possesses an abelian subgroup S which satisfies $G' \cap S = \{1\}$ and $S/(S \cap \mathrm{Z}(G)) \cong \mathrm{E}_4$. Then $|G : \mathrm{N}_G(S)| = 4$ and so* $\mathrm{sb}(G) > 1$.

Proof. We have $[\mathrm{N}_G(S), S] \leq S \cap G' = \{1\}$ and so $\mathrm{N}_G(S) = \mathrm{C}_G(S) \geq \mathrm{Z}(G)S$, where $|G : (\mathrm{Z}(G)S)| = 4$. If $\mathrm{C}_G(S) > \mathrm{Z}(G)S$, then G has an abelian maximal subgroup which implies (Lemma 1.1) $|G| = 2|\mathrm{Z}(G)||G'|$ and so $|G/\mathrm{Z}(G)| = 4$, a contradiction. Hence $\mathrm{C}_G(S) = \mathrm{Z}(G)S$ and we are done. □

Proposition 122.12. *Let G be a 2-group of order 2^5 possessing a maximal subgroup $M \cong \mathrm{E}_{16}$. If there is an element $x \in G - M$ such that $\mathrm{C}_M(x) \cong \mathrm{E}_4$, then* $\mathrm{sb}(G) > 1$.

Proof. By Lemma 99.2, there is an involution $i \in G - M$ so that $\mathrm{C}_M(i) = \mathrm{C}_M(x)$. But then $|G : \mathrm{C}_G(i)| = 4$ and we are done. □

Proposition 122.13. *Let G be a p-group with* $\mathrm{sb}(G) = 1$. *If $|G'| = p$, then we have $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ unless $p = 2$, $G/\mathrm{Z}(G) \cong \mathrm{E}_{16}$ and $G \cong (\mathrm{Q}_8 * D) \times \mathrm{E}_{2^n}$, $n \geq 0$, $\mathrm{Q}_8 \cap D = \mathrm{Z}(\mathrm{Q}_8) = D'$, where $D \cong \mathrm{D}_8$ or $D \cong \mathrm{P}$ is the nonmetacyclic minimal nonabelian group of order 2^4.*

Proof. Since $|G'| = p$, Lemma 4.2 gives $G = A_1 * A_2 * \cdots * A_k\mathrm{Z}(G)$ with $k \geq 1$, where $A_1, \ldots, A_k$ are minimal nonabelian and $A_1' = A_2' = \cdots = A_k' = G' = \langle z\rangle$ being of order p. If $k = 1$, then $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ and we are done. We may assume $k > 1$ and we set $G = (A_1 * A_2)C$, where $C = \mathrm{C}_G(A_1 * A_2)$ and $(A_1 * A_2) \cap C = \mathrm{Z}(A_1 * A_2) = \mathrm{Z}(A_1)\mathrm{Z}(A_2)$ so that $|G/C| = p^4$ and $\mathrm{Z}(G) \leq C$. Note that $|G'| = p$ implies $\mathrm{b}(G) = 1$ so that we may use Proposition 122.10. It follows that $C = \mathrm{Z}(G)$ must be abelian and $p = 2$. Thus it remains to study a 2-group $G = (A_1 * A_2)\mathrm{Z}(G)$, where A_1 and A_2 are minimal nonabelian with $A_1' = A_2' = G' = \langle z\rangle$. We have

$$G' = \langle z\rangle \leq A_1 \cap A_2 \leq \mathrm{Z}(A_1 * A_2) = \mathrm{Z}(A_1)\mathrm{Z}(A_2) \quad \text{and} \quad G/\mathrm{Z}(G) \cong \mathrm{E}_{16}.$$

(i) First assume that there is an involution $t \in G - \mathrm{Z}(G)$. Let $b \in G - \mathrm{Z}(G)$ be such that $[b,t] = z$ and then $B_1 = \langle b, t\rangle$ is minimal nonabelian. Set $C = \mathrm{C}_G(B_1)$ so that $G = B_1 * C$ with $B_1 \cap C = \mathrm{Z}(B_1)$. Since $G/\mathrm{Z}(G) \cong \mathrm{E}_{16}$, C is nonabelian. Let B_2 be a minimal nonabelian subgroup of C and then $C = B_2\mathrm{Z}(G)$. We set $G_1 = B_1 * B_2$ so that $G = G_1\mathrm{Z}(G)$. Suppose that B_2 possesses a nonnormal cyclic subgroup $\langle b'\rangle$. Set $\langle u\rangle = \Omega_1(\langle b'\rangle)$ and $S = \langle t\rangle \times \langle b'\rangle$ so that $u \neq z$, where $\langle z\rangle = G' = B_2' = B_1'$. Then $\Omega_1(S) = \langle t, u\rangle$ does not contain z. But then Proposition 122.11 gives a contradiction. Hence B_2 is Dedekindian which implies that $B_2 \cong \mathrm{Q}_8$, $B_1 \cap B_2 = \langle z\rangle$ and $\mathrm{Z}(B_1) = \mathrm{Z}(G_1)$. Set $B_2 = \langle r, s\rangle$.

(i1) Suppose that B_1 is metacyclic. Then either $B_1 \cong \mathrm{D}_8$ or $B_1 \cong \mathrm{M}_{2^m}$, $m \geq 4$. In the second case, $\mathrm{Z}(B_1)$ is cyclic of order ≥ 4 so that there is $v \in \mathrm{Z}(B_1)$ such that $v^2 = z$ and then $i = vr$ is a noncentral involution in $G_1 - (B_1 \cup B_2)$. We obtain $S = \langle i, t\rangle \cong \mathrm{E}_4$, $S \cap \mathrm{Z}(G) = \{1\}$ and $z \notin S$ so that Proposition 122.11 gives a contradiction. Hence in this case we must have $G = (\mathrm{Q}_8 * \mathrm{D}_8)\mathrm{Z}(G)$.

(i2) Now assume that B_1 is nonmetacyclic so that we may set

$$B_1 = \langle t, b \mid t^2 = b^{2^m} = 1,\ [t,b] = z,\ z^2 = [z,t] = [z,b] = 1\rangle,$$

where $m \geq 2$ and $\mathrm{Z}(B_1) = \langle b^2\rangle \times \langle z\rangle$. Assume that $m \geq 3$ in which case there is an element w of order 4 in $\langle b^2\rangle \leq \mathrm{Z}(B_1)$ so that $w^2 \neq z$ and $(wr)^2 = w^2 z$. Considering the abelian subgroup $S = \langle t\rangle \times \langle wr\rangle$, we have $\Omega_1(S) = \langle t, w^2 z\rangle \not\geq \langle z\rangle$, and again Proposition 122.11 gives a contradiction. Hence in this case we have $m = 2$ and so $G = (\mathrm{Q}_8 * \mathrm{P})\mathrm{Z}(G)$, where P is the nonmetacyclic minimal nonabelian group of order 2^4.

(ii) Assume that there exist no involutions in $G - \mathrm{Z}(G)$. We have seen above that $G = (A_1 * A_2)\mathrm{Z}(G)$, where we may assume that $A_1 \ncong \mathrm{Q}_8$ (noting that $\mathrm{Q}_8 * \mathrm{Q}_8$ possesses noncentral involutions). There is an element $d \in A_1 - \mathrm{Z}(A_1)$ such that $z \notin \langle d\rangle$ and $1 \neq d^2 \in \mathrm{Z}(G)$, where $\langle z\rangle = G'$. Let $b \in G$ be given such that $[d,b] = z$ and $B_1 = \langle d, b\rangle$ is minimal nonabelian, where $b, d \in B_1 - \mathrm{Z}(B_1)$. Note that $\langle d\rangle/\langle d^2\rangle$ is a noncentral subgroup of order 2 in $G/\langle d^2\rangle$. We have $G = B_1 * C$, where $C = \mathrm{C}_G(B_1)$ and $B_1 \cap C = \mathrm{Z}(B_1)$. If $C/\langle d^2\rangle$ is abelian, then we obtain that $C' \leq \langle d^2\rangle \cap \langle z\rangle = \{1\}$ and $C = \mathrm{Z}(G)$ is abelian, contrary to $G/\mathrm{Z}(G) \cong \mathrm{E}_{16}$. Let $B_2/\langle d^2\rangle$ be a minimal nonabelian subgroup of $C/\langle d^2\rangle$, where $B_2 \geq \langle d^2\rangle \times \langle z\rangle$ and $B_2' = \langle z\rangle$. If $B_2/\langle d^2\rangle \ncong \mathrm{Q}_8$, then there is $b' \in B_2 - \mathrm{Z}(B_2)$ such that $\langle b'\rangle \cap \langle d^2, z\rangle \leq \langle d^2\rangle$. Working in the factor group $(B_1 * B_2)/\langle d^2\rangle$, we get (as in (i)) that $\mathrm{sb}((B_1 * B_2)/\langle d^2\rangle) > 1$, a contradiction. Hence $B_2/\langle d^2\rangle \cong \mathrm{Q}_8$ so that $B_1 \cap B_2 = \langle d^2\rangle \times \langle z\rangle$. By our results in (i) (applied to $(B_1 * B_2)/\langle d^2\rangle$), we get $B_1/\langle d^2\rangle \cong \mathrm{D}_8$ or P.

Set $\Omega_1(\langle d^2\rangle) = \langle u\rangle$ and since $B_2/\langle d^2\rangle \cong \mathrm{Q}_8$, we have $\Omega_1(B_2) = \langle u, z\rangle \cong \mathrm{E}_4$. Since $\mathrm{Z}(B_2) = \langle d^2, z\rangle$, any minimal nonabelian subgroup X of B_2 covers $B_2/\langle d^2, z\rangle$ and $z \in X$. As $|\Omega_1(X)| \leq 4$, X is metacyclic and z is a square in X so that there is an element $x \in X - \langle d^2, z\rangle$ such that $x^2 = z$, $\langle z\rangle = X'$, $\langle x\rangle \trianglelefteq G$ and $\langle x\rangle$ is a maximal cyclic subgroup of G. If there is $y \in B_1$ such that $y^2 = z$, then xy is a noncentral in-

volution in G, a contradiction. Hence z is not a square in B_1 and therefore B_1 is nonmetacyclic minimal nonabelian.

If $B_1/\langle d^2\rangle \cong \mathrm{D}_8$, then we have $\mathrm{Z}(B_1) = \langle d^2\rangle \times \langle z\rangle$ and there are no involutions in $B_1 - \langle d^2, z\rangle$ so that $\Omega_1(B_1) = \langle u, z\rangle$, contrary to the fact that B_1 is nonmetacyclic. We have proved that $B_1/\langle d^2\rangle \cong \mathrm{P}$. Set $E = \Omega_1(B_1)$ so that $E \cong \mathrm{E}_8$, $\mathrm{Z}(B_1) = \langle d^2\rangle E$ and $E \cap \langle d^2, z\rangle = \langle u, z\rangle$. By the structure of B_1 (being nonmetacyclic minimal nonabelian), there exists $e \in B_1 - \mathrm{Z}(B_1)$ such that $e^2 = l$ is an involution in E, where $E = \langle u, z, l\rangle$ and $B_1 = \langle d, e\rangle$. Let $y \in B_2 - \langle d^2, z\rangle$ be such that $\langle x, y\rangle$ covers the factor group $B_2/\langle d^2, z\rangle$. Then $\langle x, y\rangle$ is minimal nonabelian with $y^2 \in \langle d^2, z\rangle - \langle d^2\rangle$.

Assume that $o(d^2) \geq 4$ and let $d' \in \langle d^2\rangle$ be an element of order 4 so that $(d')^2 = u$. Consider the subgroup $S = \langle e, xd'\rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$ with $\Omega_1(S) = \langle l, uz\rangle \cong \mathrm{E}_4$ and $z \notin S$. By Proposition 122.11, we get a contradiction (noting that $S \cap \mathrm{Z}(G) = \Omega_1(S)$). Hence $o(d^2) = 2$ and so $d^2 = u$. If $y^2 = z$, then $\langle x, y\rangle \cong \mathrm{Q}_8$ and $B_2 = \langle u\rangle \times \langle x, y\rangle$. In case $y^2 = uz$, we conclude that $B_2 = \langle x, y\rangle \cong \mathrm{H}_2$ is minimal nonabelian, where $\mathrm{H}_2 = \langle x, y \mid x^4 = y^4 = 1,\ x^y = x^{-1}\rangle$, $x^2 = z$, $y^2 = uz$ and u is not a square in H_2.

We have proved that

$$B_1 = \langle d, e \mid d^4 = e^4 = 1,\ [d, e] = z,\ z^2 = [z, d] = [z, e] = 1\rangle,$$

where $d^2 = u$, $e^2 = l$, $\Omega_1(B_1) = \langle u, l, z\rangle$, and $B_1 * B_2 \cong B_1 * \mathrm{Q}_8$ or $B_1 * B_2 \cong B_1 * \mathrm{H}_2$.

If $B_1 * B_2 \cong B_1 * \mathrm{Q}_8$ with $B_1 \cap \mathrm{Q}_8 = \langle z\rangle$, then consider $B_1/\langle uz, lz\rangle \cong \mathrm{Q}_8$ so that $(B_1 * \mathrm{Q}_8)/\langle uz, lz\rangle \cong \mathrm{Q}_8 * \mathrm{Q}_8$, which is a contradiction by Proposition 122.4. Hence we must have

$$B_2 \cong \mathrm{H}_2 = \langle x, y \mid x^4 = y^4 = 1,\ x^y = x^{-1}\rangle,$$

where $x^2 = z$, $y^2 = uz$ and u is not a square in B_2. In this case, we consider the subgroup $S^* = \langle y, de\rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$. Since

$$S^* \cap \mathrm{Z}(G) = \Omega_1(S^*) = \langle uz, ulz\rangle \not\supseteq \langle z\rangle,$$

Proposition 122.11 gives a contradiction.

(iii) We have proved that $G = (\mathrm{D}_8 * \mathrm{Q}_8)\mathrm{Z}(G)$ or $G = (\mathrm{P} * \mathrm{Q}_8)\mathrm{Z}(G)$. It remains to be proved that $\mathrm{Z}(G)$ is elementary abelian. We may set $G = (A_1 * A_2)\mathrm{Z}(G)$, where

(a) $$A_1 = \langle b, t \mid b^4 = t^2 = 1,\ b^2 = z,\ b^t = bz\rangle \cong \mathrm{D}_8$$

or

(b) $$A_1 = \langle b, t \mid b^4 = t^2 = 1,\ b^2 = u,\ [b, t] = z,\ z^2 = [z, b] = [z, t] = 1\rangle \cong \mathrm{P}$$

and

$$A_2 = \langle x, y \mid x^2 = y^2 = z,\ z^2 = 1,\ [x, y] = z\rangle \cong \mathrm{Q}_8 \quad \text{with } A_1 \cap A_2 = \langle z\rangle.$$

First assume that $\mathrm{Z}(G)$ has an element v of order 4 such that $v^2 = s \notin A_1 * A_2$. In both cases (a) and (b), we consider the abelian subgroup $S = \langle vx, t\rangle$ of G which satisfies $\Omega_1(S) = \langle t, sz\rangle \not\geq \langle z\rangle$ so that Proposition 122.11 gives a contradiction.

Now assume that $\mathrm{Z}(G)$ has an element v of order 4 such that $v^2 \in \mathrm{Z}(A_1 * A_2)$. In case (a), we must have $v^2 = z$ and then we consider the subgroup $S = \langle vx, t\rangle \cong \mathrm{E}_4$, where vx is an involution in $G - (A_1 * A_2)$ commuting with t and so $z \notin S$ and Proposition 122.11 gives a contradiction. In case (b), we have either $v^2 = z$ or $v^2 = u$ since there is an outer automorphism α of A_1 induced by $t^\alpha = t$ and $b^\alpha = bt$, where $(bt)^2 = uz$ and so $u^\alpha = uz$. If $v^2 = z$, we consider the subgroup $S = \langle vx, t\rangle \cong \mathrm{E}_4$ with $z \notin S$. In case $v^2 = u$, we consider the subgroup

$$S = \langle vx, t\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2 \quad \text{with } \Omega_1(S) = \langle t, uz\rangle \not\geq \langle z\rangle.$$

In both cases, we get a contradiction with the help of Proposition 122.11. Our proposition is proved. □

Proposition 122.14. *Let G be a 2-group with* $\mathrm{sb}(G) = 1$. *Then* $\mathrm{b}(G) \leq 3$ *and let a be an element in G with eight conjugates. Then we have $o(a) = 8$, $|G : \mathrm{N}_G(\langle a\rangle)| = 2$ and* $\mathrm{N}_G(\langle a\rangle)/\mathrm{C}_G(a) \cong \mathrm{E}_4$.

Proof. We have $\mathrm{b}(G) \leq 3$ by Proposition 122.8. Let a be an element in G with eight conjugates. Set $C = \mathrm{C}_G(a)$ so that $|G : C| = 8$. Also set $H = \mathrm{N}_G(\langle a\rangle)$ so that $|G : H| \leq 2$. Since $|H/C| \geq 4$, we have $o(a) \geq 8$. Suppose that $o(a) = 2^n$ with $n \geq 4$. Assume that there is an element $x \in H - C$ such that $a^x = a^{-1}z^\epsilon$, where $z = a^{2^{n-1}}$ and $\epsilon = 0, 1$. This implies $\langle x\rangle \cap \langle a\rangle \leq \langle z\rangle$. On the other hand, a^2 normalizes $\langle x\rangle$ and so $[a^2, x] \leq \langle x\rangle \cap \langle a\rangle \leq \langle z\rangle$. But $(a^2)^x = (a^{-1}z^\epsilon)^2 = a^{-2}$ and so $[a^2, x] = a^{-4}$ with $o(a^{-4}) \geq 4$, a contradiction. It follows that H/C contains only the involutory automorphism induced by $a \to az$. Hence H/C is cyclic. Assume that $H - C$ contains an element y which induces on $\langle a\rangle$ an automorphism of order 4 given by $a^y = av$, where $v = a^{2^{n-2}}$. Then $\langle a, y\rangle$ is metacyclic with $\langle a, y\rangle' = \langle v\rangle \cong \mathrm{C}_4$. But then Proposition 122.7 gives a contradiction. We get $H/C \cong \mathrm{C}_4$, $|G : H| = 2$, and if $y \in H - C$ is such that $\langle y\rangle$ covers H/C, then $a^y = a^{-1}v$, where v is an element of order 4 in $\langle a\rangle$ and $v^2 = z$ with $\Omega_1(\langle a\rangle) = \langle z\rangle$. Note that $(a^4)^y = (a^{-1}v)^4 = a^{-4}$ and so $v^y = v^{-1}$ and

$$a^{y^2} = (a^{-1}v)^y = (a^{-1}v)^{-1}v^y = az$$

which implies $\langle y\rangle \cap \langle a\rangle \leq \langle z\rangle$. On the other hand, a^2 normalizes $\langle y\rangle$ and so $[a^2, y] \leq \langle y\rangle \cap \langle a\rangle \leq \langle z\rangle$. But $(a^2)^y = (a^{-1}v)^2 = a^{-2}z$ and so $[a^2, y] = a^{-4}z$ which is of order ≥ 4, a contradiction. We have proved that $o(a) = 8$ and then $|G : H| = 2$ and $H/C \cong \mathrm{E}_4$. □

Proposition 122.15. *Let G be a 2-group with* $\mathrm{sb}(G) = 1$. *Let a be an element in G with eight conjugates. By Proposition 122.14, we have $o(a) = 8$, $|G : \mathrm{N}_G(\langle a\rangle)| = 2$, and* $\mathrm{N}_G(\langle a\rangle)/\mathrm{C}_G(a) \cong \mathrm{E}_4$. *If $b, c \in \mathrm{N}_G(\langle a\rangle) - \mathrm{C}_G(a)$ are such that $a^b = a^{-1}$ and*

$a^c = a^{-1}z$ *with* $z = a^4$, *then* $o(b) = o(c) = 8$ *and*

$$\Omega_1(\langle b\rangle) = \Omega_1(\langle c\rangle) = \langle b\rangle \cap \langle a\rangle = \langle c\rangle \cap \langle a\rangle = \langle z\rangle.$$

We have

- $L = \langle b, a^2\rangle \cong \mathrm{M}_{16}$, *where* $b^4 = a^4 = z$, $z^2 = 1$, $[a^2, b] = z$, $L \trianglelefteq G$, $t = a^2b^2$ *is an involution and* $\Omega_1(L) = \langle t, z\rangle$.
- $b^a = ba^2$, $(a^2)^a = a^2$ *and so* a *induces on* L *an outer automorphism of order* 4 *as* $b^{a^2} = ba^4 = bz$, *where* a^2 *induces on* L *an inner automorphism of order* 2.
- $\mathrm{Aut}(L) = D \times \langle\alpha\rangle$, *where* $D \cong \mathrm{D}_8$ *and* α *is an outer involutory automorphism of* L *induced by* $b^\alpha = b^{-1}$ *and* $(a^2)^\alpha = a^2$.

Proof. Let a be an element in G with eight conjugates so that $o(a) = 8$ and then set $C = \mathrm{C}_G(a)$, $H = \mathrm{N}_G(\langle a\rangle)$, where $|G : H| = 2$ and $H/C \cong \mathrm{E}_4$. Let $b, c \in H - C$ be such that $\langle b, c\rangle$ covers H/C and $a^b = a^{-1}$, $a^c = a^{-1}z$ with $z = a^4$. This implies that $\langle b\rangle \cap \langle a\rangle \leq \langle z\rangle$ and $\langle c\rangle \cap \langle a\rangle \leq \langle z\rangle$. On the other hand, a^2 normalizes $\langle b\rangle$ and $\langle c\rangle$. If $\langle b\rangle \cap \langle a\rangle = \{1\}$, then a^2 centralizes $\langle b\rangle$, a contradiction. In case $\langle c\rangle \cap \langle a\rangle = \{1\}$, a^2 centralizes $\langle c\rangle$, a contradiction. Hence we have

$$\langle b\rangle \cap \langle a\rangle = \langle c\rangle \cap \langle a\rangle = \langle z\rangle,$$

and so we may set $b^{2^m} = z$ and $c^{2^l} = z$, where $m \geq 1$ and $l \geq 2$. Indeed, if $c^2 = z$, then $\langle a, c\rangle \cong \mathrm{SD}_{16}$, and so $\langle a, c\rangle$ possesses a noncentral involution i with $\mathrm{C}_{\langle a,c\rangle}(i) = \langle i, z\rangle \cong \mathrm{E}_4$, a contradiction.

We shall study the structure of the subgroup $M = \langle a, b, c\rangle$, where $M' \geq \langle a^2\rangle$ since $[a, b] = a^{-2}$, $[a, c] = a^2$. If b has only four conjugates in M, then $b^c = ba^{2i}$ (for some integer i) since b has already four conjugates in $\langle b, a\rangle$ with $\langle b, a\rangle' = \langle a^2\rangle$ and this gives $[b, c] \in \langle a^2\rangle$ and $M' = \langle a^2\rangle$ so that $\mathrm{b}(M) = 2$. Similarly, if c has only four conjugates in M, then $c^b = ca^{2j}$ (for some integer j) and this gives $[c, b] \in \langle a^2\rangle$ and $M' = \langle a^2\rangle$ so that $\mathrm{b}(M) = 2$. Hence b has only four conjugates in M if and only if c has only four conjugates in M and in that case $M' = \langle a^2\rangle$ and $\mathrm{b}(M) = 2$. Conversely, if $M' = \langle a^2\rangle$, then $\mathrm{b}(M) = 2$ and so both b and c have exactly four conjugates in M.

We aim to show that $o(b) = o(c) = 8$.

First assume that b or c has eight conjugates in M. By the previous paragraph, both b and c have exactly eight conjugates in M. From Proposition 122.14 we then conclude that $o(b) = o(c) = 8$.

In the sequel we assume that both b and c have exactly four conjugates in M and so $M' = \langle a^2\rangle$. Set $[b, c] = a^{2i}$ (i integer) and compute

$$[b^2, c] = [b, c]^b[b, c] = (a^{2i})^b a^{2i} = a^{-2i}a^{2i} = 1,$$
$$[b, c^2] = [b, c][b, c]^c = a^{2i}(a^{2i})^c = a^{2i}a^{-2i} = 1,$$

and so $\langle b^2, c^2\rangle \leq \mathrm{Z}(M)$.

Assume $m \geq 3$, where $b^{2^m} = z$ and set $b' = b^{2^{m-2}}$ so that $o(b') = 8$, $(b')^4 = z$ and $b' \in \mathrm{Z}(M)$. It follows that $\langle b', a\rangle = \langle b'\rangle * \langle a\rangle$ with $\langle b'\rangle \cap \langle a\rangle = \langle z\rangle$. Because of $(b'a)^2 = (b')^2a^2 \neq 1$ and $(b'a)^4 = (b')^4a^4 = zz = 1$, we obtain that $o(b'a) = 4$. Set $S = \langle b'a\rangle$ and we claim that S has more than two conjugates in M. Indeed, we have $S^b = \langle b'a^{-1}\rangle$ and $S^c = \langle b'a^{-1}z\rangle$. If $S = S^b$, then either $b'a = b'a^{-1}$ (and then $a^2 = 1$) or $b'a = (b'a^{-1})^{-1} = (b')^{-1}a$ (and then $(b')^2 = 1$), a contradiction. In case $S = S^c$, either $b'a = b'a^{-1}z$ (and then $a^2 = z$) or $b'a = (b')^{-1}az$ (and then $(b')^2 = z$), a contradiction. If $S^b = S^c$, then either $b'a^{-1} = b'a^{-1}z$ (and then $z = 1$) or $b'a^{-1} = (b')^{-1}az$ (and then $(b')^2 = a^2z$), a contradiction. Thus $m \leq 2$.

Assume $l \geq 3$, where $c^{2^l} = z$ and set $c' = c^{2^{l-2}}$ so that $o(c') = 8$, $(c')^4 = z$ and $c' \in \mathrm{Z}(M)$. It follows that $\langle c', a\rangle = \langle c'\rangle * \langle a\rangle$ with $\langle c'\rangle \cap \langle a\rangle = \langle z\rangle$. Then we have $T = \langle c'a\rangle \cong \mathrm{C}_4$ and we claim that T has more than two conjugates in M. Indeed, we obtain $T^b = \langle c'a^{-1}\rangle$ and $T^c = \langle c'a^{-1}z\rangle$. If $T = T^b$, then either $c'a = c'a^{-1}$ or $c'a = (c')^{-1}a$, a contradiction. In case $T = T^c$, we conclude either $c'a = c'a^{-1}z$ or $c'a = (c')^{-1}az$, a contradiction. Finally, if $T^b = T^c$, then either $c'a^{-1} = c'a^{-1}z$ or $c'a^{-1} = (c')^{-1}az$, a contradiction. Thus $l \leq 2$ and so $l = 2$ and $o(c) = 8$.

Suppose $o(b) = 4$ so that $b^2 = z$, $\langle a, b\rangle \cong \mathrm{Q}_{16}$ since $a^b = a^{-1}$. Then

$$Q = \langle a^2, b\rangle \cong \mathrm{Q}_8, \quad c^2 \in \mathrm{Z}(M), \quad o(c^2) = 4,$$

and so $c^2 \notin Q$. But we have $c^4 = z$, where $\langle z\rangle = \mathrm{Z}(Q)$ and so $\langle Q, c^2\rangle = Q * \langle c^2\rangle$ with $Q \cap \langle c^2\rangle = \langle z\rangle$ and therefore $\langle Q, c^2\rangle$ contains a subgroup isomorphic to D_8. By Proposition 122.5, $|G'| \leq 4$ and so $\mathrm{b}(G) \leq 2$, contrary to the fact that a has eight conjugates in G. Hence $o(b) = 8$. We have proved that in any case $o(b) = o(c) = 8$, as required.

We have

$$L = \langle b, a^2\rangle = \langle b, a^2b^2 = t \mid b^8 = t^2 = 1,\ b^t = bz,\ z = b^4 = a^4\rangle \cong \mathrm{M}_{16}.$$

Since $b^a = ba^2$, it follows that the only two distinct cyclic subgroups $\langle b\rangle$ and $\langle ba^2\rangle$ of order 8 in L are conjugate under a and so $\langle b, b^a = ba^2\rangle = L$ is normal in G. From the fact that $\langle b^2\rangle = \mathrm{Z}(L)$ is normal in G and $\Omega_2(L) = \langle b^2, a^2\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$, we infer that $\langle a^2\rangle$ is also normal in G (noting that $\langle a^2\rangle$ and $\langle b^2\rangle$ are the only two cyclic subgroups of order 4 in $\Omega_2(L)$).

Each automorphism $\alpha \in \mathrm{Aut}(L)$ sends b onto one of the eight elements of order 8 in the set $(\langle b\rangle - \langle b^2\rangle) \cup (\langle ba^2\rangle - \langle b^2\rangle)$ and α sends a^2 onto one of the two elements in $\{a^2, a^{-2} = a^2z\}$ and so $|\mathrm{Aut}(L)| = 8 \cdot 2 = 16$. Since $\mathrm{Inn}(L) \cong L/\mathrm{Z}(L) \cong \mathrm{E}_4$, we have $|\mathrm{Aut}(L)/\mathrm{Inn}(L)| = 4$. Also, $\mathrm{Inn}(L) = \langle i_{a^2}, i_b\rangle$, where i_x is the inner automorphism of L induced by conjugation with the element $x \in L - \mathrm{Z}(L)$. We define the outer automorphisms β_a (induced by conjugation with the element $a \in G$) and α by

$$b^{\beta_a} = b^a = ba^2, \quad (a^2)^{\beta_a} = (a^2)^a = a^2 \quad \text{and} \quad b^\alpha = b^{-1}, \quad (a^2)^\alpha = a^2,$$

where $(\beta_a)^2 = i_{a^2}$ and $\alpha^2 = 1$. We check that $\mathrm{Inn}(L)\langle\beta_a\rangle \cong \mathrm{D}_8$ and that α com-

mutes with β_a and i_b and so

$$\mathrm{Aut}(L) = (\mathrm{Inn}(L)\langle\beta_a\rangle) \times \langle\alpha\rangle \cong \mathrm{D}_8 \times \mathrm{C}_2.$$

Our proposition is completely proved. □

The following proposition is the key result of the whole section.

Proposition 122.16. *Let G be a 2-group with $\mathrm{sb}(G) = 1$. Then $\mathrm{b}(G) \leq 2$, i.e., the element breadth of G is at most 2.*

Proof. Let G be a minimal counterexample to this proposition. Note that in this case Proposition 122.8 implies that $\mathrm{b}(G) \leq 3$. Then G possesses an element a which has exactly eight conjugates in G. We use Proposition 122.15 together with the notation and all details stated in that proposition.

Set $C = \mathrm{C}_G(L)$ so that $L \cap C = \mathrm{Z}(L) = \langle b^2\rangle$, $a \in G - (LC)$ and $\{1\} \neq G/(LC)$ is elementary abelian of order at most 4. We aim to show that C is abelian. Suppose that C is nonabelian. Note that C cannot be Hamiltonian since C has a central subgroup $\langle b^2\rangle \cong \mathrm{C}_4$. Let $\langle x\rangle$ be a nonnormal cyclic subgroup of C such that $z \notin \langle x\rangle$ and let $c' \in C$ be such that $\langle x^{c'}\rangle \neq \langle x\rangle$ and then $z \notin \langle x^{c'}\rangle$. Now, $t = a^2b^2$ is a noncentral involution in L and $t \neq t^b = tz$. Set $S = \langle x, t\rangle = \langle x\rangle \times \langle t\rangle$ and we claim that

$$S = \langle x, t\rangle, \quad S_1 = \langle x^{c'}, t\rangle, \quad S_2 = \langle x, tz\rangle \quad \text{and} \quad S_3 = \langle x^{c'}, tz\rangle$$

are pairwise distinct conjugates of S. If $S = S_1$, then

$$S \cap C = \langle x\rangle = S_1 \cap C = \langle x^{c'}\rangle,$$

a contradiction. In case $S = S_2$, we get

$$S \cap L = \langle t\rangle = S_2 \cap L = \langle tz\rangle,$$

a contradiction. If $S_1 = S_2$, then

$$S_1 \cap C = \langle x^{c'}\rangle = S_2 \cap C = \langle x\rangle,$$

a contradiction. Thus we have proved that each nonnormal subgroup of C contains $\langle z\rangle$. By a result of N. Blackburn (see Corollary 92.7), we have three possibilities for the structure of C.

(1) $C \cong \mathrm{Q}_8 \times \mathrm{Q}_8 \times \mathrm{E}_{2^s}$ ($s \geq 0$) which is not possible since C has a central subgroup $\langle b^2\rangle$ which is cyclic of order 4.

(2) $C \cong \mathrm{Q}_8 \times \mathrm{C}_4 \times \mathrm{E}_{2^s}$ ($s \geq 0$) and let $Q \cong \mathrm{Q}_8$ be a quaternion subgroup of C. If $z \in Q$, then the subgroup $\langle b^2, Q\rangle$ contains a subgroup isomorphic to D_8. In that case, Proposition 122.5 implies $|G'| \leq 4$ which gives $\mathrm{b}(G) \leq 2$, a contradiction. Hence $Q = \langle x, y\rangle$ with $\mathrm{Z}(Q) = \langle z'\rangle \neq \langle z\rangle$. But then $\langle b^2x\rangle$ is nonnormal in C and $z \notin \langle b^2x\rangle$, a contradiction.

(3) C possesses an abelian maximal subgroup A with $\exp(A) > 2$ and an element $v \in C - A$ of order 4 such that $x^v = x^{-1}$ for all $x \in A$. But C has a central subgroup $\langle b^2 \rangle \cong \mathrm{C}_4$, a contradiction. We have proved that C is abelian.

(i) First assume that $\mathrm{b}_G(b) = 3$, i.e., b has exactly eight conjugates in G. By Proposition 122.14, G possesses an element d such that $b^d = b^{-1}$ and so, by Proposition 122.15, our group G induces on $L \cong \mathrm{M}_{16}$ the full automorphism group of L (which is isomorphic to the group $\mathrm{D}_8 \times \mathrm{C}_2$) and so we may choose our element d so that $b^d = b^{-1}$, $(a^2)^d = a^2$, $d^2 \in C$, $o(d) = 8$, $d^4 = z$ and $G = (LC)\langle a, d \rangle$. Also, the automorphism of L induced by d commutes with all automorphisms of L and so $f = [d, a] \in C$.

Consider the subgroup

$$H = \langle b, d \mid b^8 = d^8 = 1,\ b^4 = d^4 = z,\ b^d = b^{-1} \rangle,$$

where $\mathrm{Z}(H) = \langle d^2 \rangle$. Since

$$(bd)^2 = bdbd = bd^2b^d = bd^2b^{-1} = d^2, \quad [b, bd] = [b, d] = b^{-2},$$

it follows that the cyclic subgroup $S = \langle bd \rangle$ of order 8 is not normal in H. Thus two conjugates of S in G are already contained in H. On the other hand,

$$(bd)^a = b^a d^a = ba^2 \cdot df = (bd)a^2 f,$$

which forces $a^2 f \in H$. Since $a^2 f \in LC$ and $H \cap (LC) = \langle b, d^2 \rangle$, we deduce that $a^2 f$ must be contained in the abelian subgroup $\langle b, d^2 \rangle$. But $b^{a^2 f} = (bz)^f = bz \neq b$, a contradiction.

(ii) Now assume that $\mathrm{b}_G(b) = 2$, i.e., there is no element in G which inverts $\langle b \rangle$. We get $G = (LC)\langle a \rangle$, where $C = \mathrm{C}_G(L)$ is abelian and $|G : (LC)| = 2$. Since b inverts $\langle a \rangle$, b^2 centralizes $\langle a \rangle$ and so $\mathrm{C}_G(\langle b^2 \rangle) \geq \langle L, C, a \rangle = G$ so that $b^2 \in \mathrm{Z}(G)$. We have

$$\mathrm{N}_G(\langle a \rangle) = \langle a \rangle \mathrm{N}_{LC}(\langle a \rangle)$$

and noting that $L = \langle a^2, b \rangle$ normalizes $\langle a \rangle$, we obtain that $\mathrm{N}_{LC}(\langle a \rangle) = LC_0$, where $C_0 = \mathrm{N}_C(\langle a \rangle)$, $C_0 \geq \langle b^2 \rangle$ and $|C : C_0| = 2$ (Proposition 122.14). Let $x \in C - C_0$ so that $C \trianglelefteq G$ implies $[a, x] = f_0 \in C$ and $a^x = af_0$. Hence we have $f_0 \notin \langle a \rangle$ and so $f_0 \in C - \langle z \rangle$ since $\langle a \rangle \cap C = \langle z \rangle$.

Consider the subgroup

$$K = \langle a, b \mid a^8 = b^8 = 1,\ a^4 = b^4 = z,\ a^b = a^{-1} \rangle,$$

where $\mathrm{Z}(K) = \langle b^2 \rangle$. Since

$$(ab)^2 = abab = ab^2a^b = ab^2a^{-1} = b^2 \quad \text{and} \quad [ab, a] = [b, a] = a^2,$$

the cyclic subgroup $\langle ab \rangle$ of order 8 is not normal in K and so two conjugates of $\langle ab \rangle$ in G are already contained in K. On the other hand, $(ab)^x = af_0b = (ab)f_0$ which

implies $f_0 \in K$. But $K \cap (LC) = \langle a^2, b\rangle = L$ and so $f_0 \in (L \cap C) - \langle z\rangle$. Thus $f_0 = (b^2)^{\pm 1}$ and therefore replacing b with b^{-1} (if necessary), we may set $f_0 = b^2$ and so $a^x = ab^2$. Then we get

$$a^{x^2} = (ab^2)^x = (ab^2)b^2 = ab^4 = az$$

and so $x^2 \in C_0$ but $x^2 \notin C_1$, where $C_1 = \mathrm{C}_C(a) \geq \langle b^2\rangle$. On the other hand, C centralizes $\langle a^2\rangle$ and so in $C_0 - C_1$ we cannot have elements which invert $\langle a\rangle$. This gives

$$|C_0 : C_1| = 2, \quad x^2 \in C_0 - C_1, \quad C_1 = \mathrm{Z}(G).$$

For any $y \in C_0 - C_1$ we have $a^y = az$ and $a^{yb} = a^{-1}z$. By Proposition 122.15, we have $o(yb) = 8$ and $(yb)^4 = z$. Then we get $y^4b^4 = z$ and $y^4 = 1$ so that C_0 is of exponent 4. Suppose that $\mathrm{Z}(G) = C_1 = \langle b^2\rangle$ is cyclic. If, in addition, G possesses noncommuting involutions, then Proposition 122.5 implies that $|G'| \leq 4$ which gives $\mathrm{b}(G) \leq 2$, a contradiction. By Proposition 122.6, G has at most three involutions and so

$$\Omega_1(G) = \Omega_1(L) = \langle z, t\rangle \cong \mathrm{E}_4.$$

But $\exp(C_0) = 4$ and $|C_0 : \langle b^2\rangle| = 2$ and so there exist involutions in $C_0 - \langle b^2\rangle$, a contradiction. Hence we get $C_1 = \mathrm{Z}(G) > \langle b^2\rangle$ so that there is a central involution $u \in C_1 - \langle b^2\rangle$. Considering the factor group $\bar{G} = G/\langle u\rangle$, then the fact that G was a minimal counterexample to our proposition gives $\mathrm{b}(\bar{G}) \leq 2$. On the other hand, from $a^b = a^{-1}$, $a^x = ab^2$, $a^{x^2} = az$ we deduce that $\bar{a}$ has in $\bar{G}$ eight conjugates, a final contradiction. Our proposition is proved. □

Proposition 122.17. *Let G be a 2-group with* $\mathrm{sb}(G) = 1$ *which is a minimal counterexample to Theorem 122.1. Then $|G'| = 4$, and let $z \in G'$ be a central involution in G. If $R/\langle z\rangle = \mathrm{Z}(G/\langle z\rangle)$, then $G/R \cong \mathrm{E}_{16}$.*

Proof. Let G be a 2-group with $\mathrm{sb}(G) = 1$ which is a minimal counterexample to Theorem 122.1. If $|G'| = 2$, then Proposition 122.13 implies $|G/\mathrm{Z}(G)| \leq 2^4$, a contradiction. Hence $|G'| > 2$ and so $\mathrm{b}(G) > 1$ by Proposition 121.9 (Knoche). On the other hand, Proposition 122.16 gives $\mathrm{b}(G) \leq 2$ and so $\mathrm{b}(G) = 2$. Since $|G/\mathrm{Z}(G)| \geq 2^5$, Theorem 121.1 implies $|G'| = 4$.

Let $z \in G'$ be a central involution in G and set $\bar{G} = G/\langle z\rangle$ so that $\mathrm{sb}(\bar{G}) \leq 1$ and $|\bar{G}'| = 2$. By Proposition 122.13, $\bar{G}/\mathrm{Z}(\bar{G}) \cong \mathrm{E}_4$ or $\bar{G}/\mathrm{Z}(\bar{G}) \cong \mathrm{E}_{16}$. Assume that $\bar{G}/\mathrm{Z}(\bar{G}) \cong \mathrm{E}_4$ and so we have only to rule out this case. Set $\mathrm{Z}(\bar{G}) = R/\langle z\rangle$, where $G/R \cong \mathrm{E}_4$ and $r \in R$ if and only if $[G, r] \leq \langle z\rangle$. We have $[G, R] = \langle z\rangle$. Indeed, if $[G, R] = \{1\}$, then we get $R = \mathrm{Z}(G)$, a contradiction. Also, $[G, r] \leq \langle z\rangle$ implies that $|G : \mathrm{C}_G(r)| \leq 2$.

Let A be a maximal normal abelian subgroup of G which contains $\Phi(G)$ so that $\{1\} \neq G/A$ is elementary abelian. In view of Propositions 122.3 and 122.10, there is $g \in G - A$ such that $|A : \mathrm{C}_A(g)| = 4$ and then Lemma 121.2 implies $|[A, g]| = 4$ so

that $[A, G] = G'$. If $|G : A| = 2$, then we have $|G/\mathrm{Z}(G)| = 8$, a contradiction. Hence $|G : A| \geq 4$. Since $[G, G'] \leq \langle z\rangle$, we have $G' \leq R$. As $[A, g] \not\leq \langle z\rangle$, it follows that $A \not\leq R$. For each $x \in (AR) - A$, $x \in \mathrm{T}_A$, i.e., $|A : \mathrm{C}_A(x)| = 2$. Therefore R does not cover G/A because $g \notin \mathrm{T}_A$. Hence $|A : (A\cap R)| = 2$ and $|G : (AR)| = 2$ which gives $G = (AR)\langle g\rangle$. We have $R' \leq \langle z\rangle$ and $[A, R] = \langle z\rangle$ (noting that $|R : (A \cap R)| \geq 2$) and so $(AR)' = \langle z\rangle$. Since $|A : \mathrm{C}_A(g)| = 4$, g does not centralize $A \cap R$ and so we get $[A \cap R, g] = \langle z\rangle$ which gives $|A \cap R : \mathrm{C}_{A\cap R}(g)| = 2$ and therefore $\mathrm{C}_A(g)$ is a subgroup of index 2 in $A \cap R$ and so $g^2 \in \mathrm{C}_{A\cap R}(g)$. Also, $R' \leq \langle z\rangle$ and $[R, g] = \langle z\rangle$ imply $(R\langle g\rangle)' = \langle z\rangle$.

Since G is a minimal counterexample to Theorem 122.1, we have $|G/\mathrm{Z}(G)| \geq 2^5$ and so Propositions 122.5 and 122.9 imply that $\Omega_1(G)$ is elementary abelian and $\Omega_1(\mathrm{Z}(G)) \leq G'$. In particular, D_8 is not a subgroup of G.

First suppose $|G/A| = 4$. If R is abelian, then $\mathrm{C}_G(\mathrm{C}_A(g)) \geq \langle R, g, A\rangle = G$, $\mathrm{C}_A(g) \leq \mathrm{Z}(G)$ and $|G : \mathrm{C}_A(g)| = 2^4$, a contradiction. Hence R is nonabelian with $R' = \langle z\rangle$ and $A \cap R$ is an abelian maximal subgroup of R. Then Lemma 1.1 gives $|R| = 2|\mathrm{Z}(R)||R'|$ and so $Z = \mathrm{Z}(R)$ is a subgroup of index 2 in $A\cap R$. If $\mathrm{C}_A(g) = Z$, we get $\mathrm{C}_G(Z) \geq \langle R, g, A\rangle = G$ and $|G : Z| = 2^4$, a contradiction. It follows that $Z_0 = \mathrm{C}_A(g) \cap Z$ is of index 4 in $A \cap R$ and $Z_0 = \mathrm{Z}(R\langle g\rangle)$ with $|(R\langle g\rangle)/Z_0| = 2^4$. Since $(R\langle g\rangle)' = \langle z\rangle$ and $\mathrm{sb}(R\langle g\rangle) = 1$, we may apply Proposition 122.13 and get (noting that D_8 is not a subgroup of G) $R\langle g\rangle \cong (\mathrm{P} * \mathrm{Q}_8) \times \mathrm{E}_{2^s}$, $s \geq 0$, where P is the nonmetacyclic minimal nonabelian subgroup of order 2^4 and $\mathrm{P} \cap \mathrm{Q}_8 = \langle z\rangle$.

Now assume $|G/A| > 4$ so that $|(AR)/A| \geq 4$. Note that we have $(AR)' = \langle z\rangle$ and $\mathrm{Z}(AR) < A$ which gives $|(AR)/\mathrm{Z}(AR)| \geq 2^3$. Applying Proposition 122.13, we get $AR \cong (\mathrm{P} * \mathrm{Q}_8) \times \mathrm{E}_{2^s}$, $s \geq 0$.

We have shown that in any case G possesses a maximal subgroup $M = (P * Q)\times S$, where

$$P = \langle b, t \mid b^4 = t^2 = 1,\ [b, t] = z,\ z^2 = [b, z] = [t, z] = 1\rangle,$$
$$Q = \langle r, s\rangle \cong \mathrm{Q}_8, \quad P \cap Q = \langle z\rangle \quad \text{and} \quad S \cong \mathrm{E}_{2^s},\ s \geq 0.$$

Set $b^2 = u$ so that

$$\mathrm{Z}(P) = \langle u, z\rangle \cong \mathrm{E}_4 \quad \text{and} \quad \Omega_1(P) = \langle u, z, t\rangle \cong \mathrm{E}_8.$$

Since $\langle b\rangle$ and $\langle bz\rangle$ are two distinct conjugates in G of the cyclic subgroup $\langle b\rangle \cong \mathrm{C}_4$, it follows that $\langle b, bz\rangle = \langle b\rangle \times \langle z\rangle$ is normal in G and so $\mho_1(\langle b, bz\rangle) = \langle u\rangle$ is also normal in G. Thus $u \in \mathrm{Z}(G)$ and since $\Omega_1(\mathrm{Z}(G)) \leq G'$, we get $G' = \mathrm{Z}(P) \leq \mathrm{Z}(G)$ which shows that G is of class 2. Suppose that $S \neq \{1\}$ and let x be an involution in S. We have $\langle t, x\rangle \cong \mathrm{E}_4$ and $\langle t, x\rangle \cap G' = \{1\}$. Then

$$[\mathrm{N}_G(\langle t, x\rangle), \langle t, x\rangle] \leq \langle t, x\rangle \cap G' = \{1\},$$

and so

$$\mathrm{N}_G(\langle t, x\rangle) = \mathrm{C}_G(\langle t, x\rangle) = \mathrm{C}_G(x) \cap \mathrm{C}_G(t).$$

But $\Omega_1(\mathrm{Z}(G)) = G' = \langle u, z\rangle$ whence $x \notin \mathrm{Z}(G)$ and so $\mathrm{C}_G(x) = M$. Because of $|M : \mathrm{C}_M(t)| = 2$, we have $|G : (\mathrm{C}_G(x) \cap \mathrm{C}_G(t))| = 4$, a contradiction. Hence we get $S = \{1\}$ and so $M = P * Q$, $\mathrm{Z}(M) = \mathrm{Z}(P) = G' \leq \mathrm{Z}(G)$. Since $|G/\mathrm{Z}(G)| \geq 2^5$, we have $\mathrm{Z}(P) = G' = \mathrm{Z}(G)$.

We shall show that there are no involutions in $G - M$. Indeed, let i be an involution in $G - M$ and note that $\langle t, i\rangle \cong \mathrm{E}_4$ and $\langle t, i\rangle \cap \mathrm{Z}(G) = \{1\}$ so that $E = \langle z, u, t, i\rangle$ is isomorphic to E_{16}. Also, $b^2 = u$ and $E \trianglelefteq G$ and therefore $|E\langle b\rangle| = 2^5$. We have

$$[\mathrm{N}_G(\langle t, i\rangle), \langle t, i\rangle] \leq \langle t, i\rangle \cap G' = \{1\} \quad \text{and so} \quad \mathrm{N}_G(\langle t, i\rangle) = \mathrm{C}_G(\langle t, i\rangle)$$

which together with $|G : \mathrm{N}_G(\langle t, i\rangle)| = 2$ gives $\mathrm{C}_G(t) = \mathrm{C}_G(i) = \mathrm{C}_G(ti) = EQ$, where $b \notin EQ$ and $|G : (EQ)| = 2$. In particular, $\mathrm{C}_E(b) = \langle u, z\rangle \cong \mathrm{E}_4$ and so Proposition 122.12 implies $\mathrm{sb}(E\langle b\rangle) > 1$, a contradiction. We have proved that there are no involutions in $G - M$ and so

$$\Omega_1(G) = \Omega_1(M) = \Omega_1(P) = \langle z, u, t\rangle \cong \mathrm{E}_8.$$

Note that $P/\langle u\rangle \cong \mathrm{D}_8$ and so $M/\langle u\rangle \cong \mathrm{D}_8 * \mathrm{Q}_8$ and therefore, applying Proposition 122.13 on the factor group $G/\langle u\rangle$, we see that there is an element $v \in G - M$ such that $v^2 = u$ and $[v, M] \leq \langle u\rangle$. If $b^v = b$, then $v^2 = b^2 = u$ gives that vb is an involution in $G - M$, a contradiction. Hence $b^v = bu = b^{-1}$ and so $\langle b, v\rangle \cong \mathrm{Q}_8$. Since t and $t^b = tz$ are the only conjugates of t in G, we cannot have $t^v = tu$ and so $[t, v] = 1$. If v centralizes $Q = \langle r, s\rangle$, then

$$\langle\langle b, v\rangle, Q\rangle = \langle b, v\rangle \times Q \cong \mathrm{Q}_8 \times \mathrm{Q}_8,$$

and then Proposition 122.4 gives a contradiction. In case $r^v = ru$ and $s^v = su$, we have $(rs)^v = rs$. Hence we may choose generators r, s of Q so that $[r, v] = 1$ and $[s, v] = u$. The structure of G (of order 2^7) is uniquely determined.

We compute

$$(bts)^2 = (bt)^2 s^2 = uz \cdot z = u \quad \text{and} \quad [v, bts] = u \cdot u = 1$$

and so $v \cdot bts$ is an involution in $G - M$, a final contradiction. Our proposition is proved. □

Proposition 122.18. *Let G be a 2-group with $\mathrm{sb}(G) = 1$ which is a minimal counterexample to Theorem 122.1. Then $|G'| = 4$ and let $z \in G'$ be a central involution in G. We have $G = AB$, where A and B are normal subgroups of G,*

$$A \cap B = \langle z\rangle, \quad A \cong \mathrm{Q}_8, \mathrm{C}_4, \mathrm{E}_4 \text{ or } \mathrm{C}_2$$

and if $A \cong \mathrm{Q}_8$, then $[A, B] = 1$, and $G' = B'$, $B/\langle z\rangle \cong \mathrm{Q}_8 * \mathrm{D}_8$ with $\mathrm{Q}_8 \cap \mathrm{D}_8 = \mathrm{Z}(\mathrm{Q}_8)$ or $B/\langle z\rangle \cong \mathrm{Q}_8 * \mathrm{P}$ with $\mathrm{Q}_8 \cap \mathrm{P} = \mathrm{Z}(\mathrm{Q}_8) = \mathrm{P}'$, where P is the nonmetacyclic minimal nonabelian group of order 2^4.

Proof. By Proposition 122.17, we have $|G'| = 4$ and if $z \in G'$ is a central involution in G, then $G/\langle z\rangle$ is isomorphic to one of the groups stated in the second half of Proposition 122.13. More precisely, we have $G = AB$, where A and B are normal subgroups of G, $A \cap B = \langle z\rangle$, $A/\langle z\rangle \cong \mathrm{E}_{2^n}$, $n \geq 0$, $B/\langle z\rangle \cong \mathrm{Q}_8 * D$ with $\mathrm{Q}_8 \cap D = \mathrm{Z}(\mathrm{Q}_8) = D'$, $D \cong \mathrm{D}_8$ or P, where P is the nonmetacyclic minimal nonabelian group of order 2^4. Further, $G' \leq B$ and set $T/\langle z\rangle = \mathrm{Z}(B/\langle z\rangle)$ so that $T = G'$ (in case $B/\langle z\rangle \cong \mathrm{Q}_8 * \mathrm{D}_8$) or $T/\langle z\rangle \cong \mathrm{E}_4$ (in case $B/\langle z\rangle \cong \mathrm{Q}_8 * P$) and in both cases $B/T \cong \mathrm{E}_{16}$ and $\mathrm{Z}(B) \leq T$. If $B < G$, then the fact that G is a minimal counterexample to Theorem 122.1 gives $|B/\mathrm{Z}(B)| \leq 2^4$ and so in this case $\mathrm{Z}(B) = T$.

Suppose that A is nonabelian so that in this case $A' = \langle z\rangle$ and A/A' is elementary abelian. We may also assume that A is not Hamiltonian and so $\mathrm{sb}(A) = 1$. By Proposition 122.5, D_8 is not a subgroup of A. Also, P cannot be a subgroup of A since P/P' is not elementary abelian. Then, by Proposition 122.13, we get $A/\mathrm{Z}(A) \cong E_4$. Let A_0 be a minimal nonabelian subgroup of A so that $A = A_0\mathrm{Z}(A)$. But we have $A_0' = \langle z\rangle = \Phi(A_0) = \Phi(A)$ and so $A_0 \cong \mathrm{Q}_8$ and $A_0 \cap \mathrm{Z}(A) = \langle z\rangle$ with $\mathrm{Z}(A)/\langle z\rangle$ being elementary abelian. If there is $v \in \mathrm{Z}(A)$ such that $v^2 = z$, then $A_0 * \langle v\rangle$ contains a subgroup isomorphic to D_8, a contradiction (Proposition 122.5). It follows that $\mathrm{Z}(A)$ is elementary abelian and so A is Hamiltonian after all. We have proved that A is either abelian with $\mathfrak{V}_1(A) \leq \langle z\rangle$ or A is Hamiltonian with $A' = \langle z\rangle$.

Suppose that A possesses a central involution t satisfying $t \neq z$ and $A > \langle t, z\rangle$. Set $G_0 = B\langle t\rangle$ so that $G_0 < G$. As $B < G$, we get $T = \mathrm{Z}(B)$ and $T/\langle z\rangle = \mathrm{Z}(B/\langle z\rangle)$. We have $[B, t] \leq \langle z\rangle$ and

$$G_0/\langle z\rangle = (\langle t, z\rangle/\langle z\rangle) \times (B/\langle z\rangle) \cong \mathrm{C}_2 \times (B/\langle z\rangle).$$

Hence $\mathrm{Z}(G_0/\langle z\rangle) = (\langle t\rangle T)/\langle z\rangle$ and so $\mathrm{Z}(G_0) \leq \langle t\rangle T$. On the other hand, we have $G_0 < G$ and so (by the minimality of G) $\mathrm{Z}(G_0) = \langle t\rangle T$. In particular, t centralizes B and so $\mathrm{C}_G(t) \geq \langle A, B\rangle = G$. Hence t is a central involution in G which is not contained in G' (since $G' \leq B$), contrary to Proposition 122.9. We have proved that $A \cong \mathrm{Q}_8, \mathrm{C}_4, \mathrm{E}_4$ or C_2.

Assume that $A \cong \mathrm{Q}_8$ and let $\langle v\rangle$ be any cyclic subgroup of order 4 in A. As $v^2 = z$ and $[v, B] \leq \langle z\rangle$, we have $\langle v\rangle \trianglelefteq G$. Set again $G_0 = \langle v\rangle B$ so that $G_0 < G$ which gives $T = \mathrm{Z}(B)$ and $T/\langle z\rangle = \mathrm{Z}(B/\langle z\rangle)$. Due to the fact that $G_0/\langle z\rangle \cong \mathrm{C}_2 \times (B/\langle z\rangle)$, we have $\mathrm{Z}(G_0/\langle z\rangle) = (\langle v\rangle T)/\langle z\rangle$ and so $\mathrm{Z}(G_0) \leq \langle v\rangle T$. But $|G_0/(\langle v\rangle T)| = 2^4$ and $G_0 < G$ and so $\mathrm{Z}(G_0) = \langle v\rangle T$. In particular, v centralizes B. But $\langle v\rangle$ was any cyclic subgroup of order 4 in $A \cong \mathrm{Q}_8$ and so $[A, B] = 1$.

It remains to prove that $G' = B'$. Assume $|B'| = 2$ so that $G' = \langle z\rangle \times B' \leq \mathrm{Z}(G)$ and therefore G is of class 2. Also, $B < G$ and so $A > \langle z\rangle$ which gives (because of the minimality of G) $T = \mathrm{Z}(B)$ and $B/\mathrm{Z}(B) \cong \mathrm{E}_{16}$. By Proposition 122.13, we obtain that $B = (\mathrm{Q}_8 * \mathrm{P}) \times \mathrm{E}_{2^s}$, $s \geq 0$, with

$$B' = \mathrm{Z}(\mathrm{Q}_8) = \langle z'\rangle = \mathrm{P}' = \mathrm{Q}_8 \cap \mathrm{P}$$

since D_8 is not a subgroup of G. If $z \in Q_8 * P$, then $z \in Z(P) - \langle z' \rangle$ and

$$B/\langle z \rangle \cong (Q_8 * D_8) \times E_{2^s}$$

and so $s = 0$. In case $z \notin Q_8 * P$, we get

$$B/\langle z \rangle \cong (Q_8 * P) \times E_{2^{s-1}}$$

and so $s = 1$. Thus it follows that we have either $B = \langle z \rangle \times (Q_8 * P)$ or $B = Q_8 * P$. If $A \cong Q_8$, then $[A, B] = 1$ and so $\langle A, Q_8 \rangle = A \times Q_8$, which is a contradiction (by Proposition 122.4). Hence $A \cong E_4$ or $A \cong C_4$ and $[A, B] = \langle z \rangle$ since $G' = \langle z, z' \rangle$.

First assume $B = \langle z \rangle \times (Q_8 * P)$, where we set

$$P = \langle b, t \mid b^4 = t^2 = 1,\ b^2 = u,\ [b, t] = z',\ (z')^2 = [b, z'] = [t, z'] = 1 \rangle$$

and $Q_8 = \langle r, s \mid r^2 = s^2 = z',\ [r, s] = z' \rangle$. Since $\{t, tz'\}$ are the only two conjugates of t in G and $\{\langle b \rangle, \langle bz' \rangle\}$ are the only two conjugates of $\langle b \rangle \cong C_4$ in G, we have $\langle t, tz' \rangle \trianglelefteq G$ and $\langle b, bz' \rangle \trianglelefteq G$ and so $P \trianglelefteq G$. This gives $[A, P] \leq A \cap P = \{1\}$ and so A centralizes P. Since $A \trianglelefteq G$ and $[A, B] = \langle z \rangle$, we have $|G : C_G(A)| = 2$ and so we may set $[A, r] = 1$ and $[A, s] = z$. Consider the cyclic subgroup $\langle sb \rangle \cong C_4$ with $(sb)^2 = z'u$ and $(sb)^t = (sb)z'$ so that $\{\langle sb \rangle, \langle sbz' \rangle\}$ are the only two conjugates of $\langle sb \rangle$ in G (and they are contained in $Q_8 * P$). For $a \in A - \langle z \rangle$, $(sb)^a = szb = (sb)z$ and $(sb)z \notin Q_8 * P$, a contradiction.

Finally, suppose that $B = Q_8 * P$, where we may set

$$P = \langle b, t \mid b^4 = t^2 = 1,\ b^2 = z,\ [b, t] = z',\ (z')^2 = [b, z'] = [t, z'] = 1 \rangle$$

(noting that both z and zz' are squares in P) and $Q_8 = \langle r, s \mid r^2 = s^2 = z',\ [r, s] = z' \rangle$. Also, $[A, B] = \langle z \rangle$ and since $\{t, tz'\}$ are the only two conjugates of t in G, we have $[A, t] = 1$ (as $[A, t] = z$ is not possible) and so A centralizes t. Assume that $A \cong E_4$ and let i be an involution in $A - \langle z \rangle$. We have $[N_G(\langle i, t \rangle), \langle i, t \rangle] \leq \langle i, t \rangle \cap G' = \{1\}$ since $G' = \langle z, z' \rangle$. Hence $N_G(\langle i, t \rangle) = C_G(\langle i, t \rangle)$ and since $|G : N_G(\langle i, t \rangle)| = 2$ and $\langle i, t \rangle \cap Z(G) = \{1\}$ (because $\Omega_1(Z(G)) \leq G'$ by Proposition 122.9), we obtain

$$C_G(t) = C_G(i) = C_G(it) = \langle i, t, z \rangle \times Q_8.$$

As $[A, B] = \langle z \rangle$, we have $[i, b] = z$ and so $b^i = bz = b^{-1}$ which gives $\langle b, i \rangle \cong D_8$, a contradiction.

We have proved that $A = \langle v \rangle$ with $v^2 = z$ and $[v, t] = 1$ (because A centralizes t). Since $A \trianglelefteq G$, we get $|G : C_G(v)| = 2$ and so $|B : C_B(v)| = 2$. If v centralizes Q_8, then $[v, b] = z$ and so $\langle v, b \rangle \cong Q_8$ centralizes $Q_8 = \langle r, s \rangle$, which is a contradiction (by Proposition 122,4). Hence we may assume $[v, r] = 1$ and $[v, s] = z$. Suppose that v centralizes b. Then $i' = vb$ is an involution and so $[i', t] = 1$ by Proposition 122.5. But v centralizes t and so also b centralizes t, a contradiction. Hence $[v, b] = z$ and the structure of G is uniquely determined.

We see that $vtbrs$ is an involution in $G - B$. Indeed,

$$(vt \cdot brs)^2 = (vt)^2(brs)^2[brs, vt] = 1$$

and then we must have $[t, vtbrs] = 1$. On the other hand, computing in G we get

$$[t, vtbrs] = [t, v][t, t][t, b][t, r][t, s] = z'$$

which is a final contradiction. Our proposition is proved. □

Proof of Theorem 122.1 for $p = 2$. Let G be a 2-group with $\mathrm{sb}(G) = 1$ (i.e., the subgroup breadth of G is equal to 1) and assume that G is a minimal counterexample to Theorem 122.1, i.e., $|G/\mathrm{Z}(G)| \geq 2^5$ but for each proper subgroup or factor group X of G, we have $|X/\mathrm{Z}(X)| \leq 2^4$. Then Proposition 122.5 gives that $\Omega_1(G)$ is elementary abelian and Proposition 122.9 yields $\Omega_1(\mathrm{Z}(G)) \leq G'$.

The starting point in our proof is Proposition 122.18 which gives the following facts. We have $|G'| = 4$, and let z be fixed involution in $G' \cap \mathrm{Z}(G)$. Then $G = AB$, where A and B are normal subgroups of G with $A \cap B = \langle z \rangle$, $A \cong \mathrm{Q}_8, \mathrm{C}_4, \mathrm{E}_4$ or C_2 and if $A \cong \mathrm{Q}_8$, then $[A, B] = \{1\}$. Further, $B = CD$ with

$$C \cap D = G' = B', \quad [C, D] \leq \langle z \rangle, \quad C/\langle z \rangle \cong \mathrm{Q}_8 \quad \text{and} \quad D/\langle z \rangle \cong \mathrm{D}_8 \text{ or P},$$

where P is the nonmetacyclic minimal nonabelian subgroup of order 2^4. Hence C and D are also normal subgroups of G.

At this point it is possible to determine the structure of C. For each $x \in C - G'$, $x^2 \in G' - \langle z \rangle$ and so $\langle z, x \rangle = G'\langle x \rangle$ is abelian. It follows that all three maximal subgroups of C which contain G' are abelian and so $|C'| = 2$ (Exercise P1). But C' covers $G'/\langle z \rangle$ and so $G' = \langle z \rangle \times C' \cong \mathrm{E}_4$ and since $C' \leq \mathrm{Z}(G)$, we get $G' \leq \mathrm{Z}(G)$ and so G is of class 2 whose commutator subgroup is a four-subgroup. We have $\Omega_1(C) = G'$ and z is not a square in C. Set $\langle c' \rangle = C'$ so that $G' = B' = \langle z, c' \rangle$. If $\Phi(C) = \langle c' \rangle$, then there is a maximal subgroup Q of C which does not contain $\langle z \rangle$ in which case $C = \langle z \rangle \times Q$ with $Q \cong \mathrm{Q}_8$ and $Q' = \langle c' \rangle$. In case $\Phi(C) = G'$, we infer that C is minimal nonabelian of order 2^4 and exponent 4. Since $\Omega_1(C) = G' \cong \mathrm{E}_4$, it follows that C is metacyclic and so c' is a square in C. There are $r, s \in C - G'$ such that $r^2 = c'$, $s^2 = c'z$ and $[r, s] = c'$. In this case,

$$C = \langle r, s \mid r^4 = s^4 = 1,\ r^2 = c',\ s^2 = zc',\ [r, s] = c' \rangle \cong \mathcal{H}_2,$$

where $\mathcal{H}_2$ is defined by $\mathcal{H}_2 = \langle x, y \mid x^4 = y^4 = 1,\ x^y = x^{-1} \rangle$.

In any case, there are elements $r, s \in C - G'$ of order 4 such that $r^2 = c'$, $s^2 = c'z^\epsilon$, $\epsilon = 0, 1$ and $[r, s] = c'$. We see that $(rs)^2 = r^2s^2[s, r] = c' \cdot c'z^\epsilon \cdot c' = c'z^\epsilon$. Fix this notation in the rest of the proof which we split into two parts: Part 1, where $D/\langle z \rangle \cong \mathrm{D}_8$, and Part 2, where $D/\langle z \rangle \cong \mathrm{P}$ with P being the nonmetacyclic minimal nonabelian group of order 2^4. It is interesting to note that Part 1 will be more difficult than Part 2.

Part 1, where $D/\langle z\rangle \cong \mathrm{D}_8$. Each of the three maximal subgroups of D containing G' are abelian and so $D' = \langle d'\rangle$ is of order 2 and $d' \in G' - \langle z\rangle$ and so we may set $d' = c'z^\eta$, $\eta = 0, 1$. If $\Phi(D) < G'$, then $\Phi(D) = D' = \langle d'\rangle$ and $D = \langle z\rangle \times D_0$, where $D_0 \cong \mathrm{D}_8$, a contradiction (since dihedral groups cannot be subgroups in G). Hence we have $\Phi(D) = G'$ and so D is minimal nonabelian of order 2^4 and exponent 4. If $\Omega_1(D) = G'$, then $D \cong \mathcal{H}_2$ and if $\Omega_1(D) \cong \mathrm{E}_8$, then $D \cong \mathrm{P}$. In case $D \cong \mathrm{H}_2$, the fact that $D/\langle z\rangle \cong \mathrm{D}_8$ shows that z is a square in D. If $D \cong \mathrm{P}$, then d' is the only involution in $\mathrm{Z}(D)$ which is not a square in D. In any case, there is $y \in D$ such that $y^2 = z$. Also, $G' = B' = \mathrm{Z}(B) \leq \mathrm{Z}(G)$ and $|B/\mathrm{Z}(B)| = 2^4$ so that we must have $G > B$ which implies $A > \langle z\rangle$. If $A \cong \mathrm{Q}_8$, then we know that $[A, B] = \{1\}$ and so $A * \langle y\rangle$ (with $A \cap \langle y\rangle = \langle z\rangle$) contains a subgroup isomorphic to D_8, a contradiction. It follows that $A \cong \mathrm{E}_4$, or C_4. In view of $|G/\mathrm{Z}(G)| \geq 2^5$, we have $A \not\leq \mathrm{Z}(G)$ and so $[A, B] = \langle z\rangle$ and $G' = B' = \mathrm{Z}(B) = \mathrm{Z}(G) = \Phi(G)$.

(i) First assume

$$D = \langle b, t \mid b^4 = 1,\ b^2 = z,\ t^2 = 1,\ [b, t] = d',\ (d')^2 = [d', b] = [d', t] = 1\rangle \cong \mathrm{P},$$

where $\{t, t^b = td'\}$ are the only two conjugates of t in G. On the other hand, we obtain $[C, t] \leq [C, D] \leq \langle z\rangle$ and so we must have $[C, t] = \{1\}$ which gives $\mathrm{C}_B(t) = \langle t\rangle \times C$. Since $[C, D] \leq \langle z\rangle$, we may set $[b, r] = z^{\epsilon_1}$ and $[b, s] = z^{\epsilon_2}$, where $\epsilon_1, \epsilon_2 \in \{0, 1\}$.

We compute $[t, tbr] = d'$, $[t, tbs] = d'$ and $[t, tbrs] = d'$, which shows that no one of the elements $\{tbr, tbs, tbrs\}$ could be an involution (since $\Omega_1(G)$ is elementary abelian). On the other hand,

$$((tb)r)^2 = (tb)^2r^2[r, tb] = zd' \cdot c' \cdot z^{\epsilon_1} = zz^\eta z^{\epsilon_1} = z^{1+\eta+\epsilon_1}$$

which gives $\eta + \epsilon_1 \equiv 0 \pmod 2$,

$$((tb)s)^2 = zd' \cdot c'z^\epsilon \cdot z^{\epsilon_2} = zz^\eta z^\epsilon z^{\epsilon_2} = z^{1+\eta+\epsilon+\epsilon_2}$$

which gives $\eta + \epsilon + \epsilon_2 \equiv 0 \pmod 2$,

$$((tb)(rs))^2 = zd' \cdot c'z^\epsilon \cdot z^{\epsilon_1+\epsilon_2} = z^{1+\eta+\epsilon+\epsilon_1+\epsilon_2}$$

which gives $\eta + \epsilon + \epsilon_1 + \epsilon_2 \equiv 0 \pmod 2$.

From the above relations we get $\epsilon_1 = 0$ and $\eta = 0$. But then we have $d' = c'$ and so $D' = C'$ which gives $[C, D] = \langle z\rangle$ since $B' = G'$. This implies $\epsilon_2 = 1$ and then the above relations also give $\epsilon = 1$ so that $C \cong \mathrm{H}_2$. The structure of B is uniquely determined.

Consider the abelian subgroup $S = \langle t, s\rangle = \langle t\rangle \times \langle s\rangle$, where $s^2 = zc'$. Due to the fact that $[\mathrm{N}_B(S), S] \leq S \cap G' = \langle zc'\rangle$, an element $x \in B$ lies in $\mathrm{N}_B(S)$ if and only if $[t, x] \in \langle zc'\rangle$ and $[s, x] \in \langle zc'\rangle$. We have $\mathrm{C}_B(t) = \langle t\rangle \times C$ and $t^b = tc'$ (where $c' \neq zc'$) and so $\mathrm{N}_B(S) \leq \langle t\rangle \times C$. Also, $r \in \mathrm{C}_B(t)$ but $[s, r] = c' \neq zc'$ and so $\mathrm{N}_B(S)$ is a proper subgroup of $\mathrm{C}_B(t)$ which shows $|B : \mathrm{N}_B(S)| \geq 4$, a contradiction.

(ii) Now assume

$$D = \langle b, f \mid b^4 = 1,\ f^4 = 1,\ b^2 = z,\ f^2 = d',\ [b, f] = d'\rangle \cong \mathrm{H}_2,$$

where

$$\Omega_1(D) = \Omega_1(C) = G' = B' = \langle z, c' \rangle = \langle z, d' \rangle = \mathrm{Z}(B) = \mathrm{Z}(G) = \Phi(G).$$

Here we have two possibilities for $c'd' = z^\eta$, namely, $\eta = 0$ or 1.

(ii1) First assume $\eta = 0$, i.e., $d' = c'$ which implies $[C, D] = \langle z \rangle$ since $B' = G'$. We set

$$[b, r] = z^{\epsilon_1}, \quad [b, s] = z^{\epsilon_2}, \quad [f, r] = z^{\epsilon_3}, \quad [f, s] = z^{\epsilon_4},$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 \in \{0, 1\}$, and compute

$$(fr)^2 = c' \cdot c' \cdot z^{\epsilon_3} = z^{\epsilon_3},$$
$$(fs)^2 = c' \cdot c' z^{\epsilon} \cdot z^{\epsilon_4} = z^{\epsilon + \epsilon_4},$$
$$(f(rs))^2 = c' \cdot c' z^{\epsilon} \cdot z^{\epsilon_3 + \epsilon_4} = z^{\epsilon + \epsilon_3 + \epsilon_4}.$$

Assume $\epsilon_3 = 0$ so that $[f, r] = 1$ and $i = fr$ is an involution. Then

$$i^b = f^b r^b = fc' \cdot rz^{\epsilon_1} = ic' z^{\epsilon_1} \quad \text{and} \quad i^s = f^s r^s = fz^{\epsilon_4} rc' = ic' z^{\epsilon_4}$$

so that we have

$$\epsilon_4 = \epsilon_1, \quad i^{bs} = i \quad \text{and} \quad \mathrm{C}_B(i) = G' \langle f, r, bs \rangle.$$

Suppose, in addition, that $\epsilon_1 = 1$ and consider the abelian subgroup $S = \langle i \rangle \times \langle f \rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$ with $f^2 = c'$. Since $[\mathrm{N}_B(S), S] \leq S \cap G' = \langle c' \rangle$, an element $x \in B$ lies in $\mathrm{N}_B(S)$ if and only if $[i, x] \in \langle c' \rangle$ and $[f, x] \in \langle c' \rangle$. As $i^b = i(c'z)$, we conclude that $\mathrm{N}_B(S) \leq \mathrm{C}_B(i)$. But $bs \in \mathrm{C}_B(i)$ and $f^{bs} = (fc')^s = fz^{\epsilon_4} c' = f(zc')$ and so $\mathrm{N}_B(S)$ is a proper subgroup of $\mathrm{C}_B(i)$ and so $|B : \mathrm{N}_B(S)| \geq 4$, a contradiction. Thus we have proved that $\epsilon_1 = \epsilon_4 = 0$ and so $[b, r] = [f, s] = 1$. But $[C, D] = \langle z \rangle$ and so we must have $\epsilon_2 = 1$ and $[b, s] = z$. If $\epsilon = 0$, then $\langle r, s \rangle \cong \mathrm{Q}_8$ and $\langle r, s \rangle * \langle f \rangle$ (with $\langle r, s \rangle \cap \langle f \rangle = \langle c' \rangle$) contains a subgroup isomorphic to D_8, a contradiction. Hence $\epsilon = 1$ and so $s^2 = (rs)^2 = c'z$ and therefore $C \cong \mathrm{H}_2$ so that the structure of B is in this case uniquely determined.

Let us consider the abelian subgroup $S^* = \langle i \rangle \times \langle bs \rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$ with $(bs)^2 = c'z$. Since $[\mathrm{N}_B(S^*), S^*] \leq S^* \cap G' = \langle c'z \rangle$, an element $x \in B$ lies in $\mathrm{N}_B(S^*)$ if and only if $[i, x] \in \langle c'z \rangle$ and $[bs, x] \in \langle c'z \rangle$. As $i^b = ic'$, we have $\mathrm{N}_B(S^*) \leq \mathrm{C}_B(i)$. But $r \in \mathrm{C}_B(i)$ and $[bs, r] = c' \neq c'z$ and so $\mathrm{N}_B(S^*)$ is a proper subgroup of $\mathrm{C}_B(i)$ and therefore $|B : \mathrm{N}_B(S^*)| \geq 4$, a contradiction.

We have proved that $\epsilon_3 = 1$ and so $[f, r] = z$. If $[f, s] = z$, then $[f, rs] = 1$ and so interchanging s and rs (if necessary) and noting that $s^2 = (rs)^2 = c'z^\epsilon$, we may assume from the start that $[f, s] = 1$ and so $\epsilon_4 = 0$. Assume that $\epsilon = 1$. Then $j = frs$ is an involution in $B - G'$, $j^r = fz \cdot r \cdot sc' = jzc'$, $j^s = jc'$ and $\{j, jzc', jc'\}$ are three pairwise distinct conjugate involutions in B, a contradiction. Hence we obtain $\epsilon = 0$ so that $r^2 = s^2 = (rs)^2 = c'$, $\langle r, s \rangle \cong \mathrm{Q}_8$ and $u = fs$ is an involution in

$B-G'$. We have $u^r = fz\cdot sc' = uzc'$ and so $\{u, uzc'\}$ are the only two conjugates of u in G. Also, $u^b = fc'\cdot sz^{\epsilon_2} = uc'z^{\epsilon_2}$ which gives $\epsilon_2 = 1$, $[b,s] = z$ and $u^{br} = u$ so that $\mathrm{C}_B(u) = G'\langle f, s, br\rangle$.

Let us consider the abelian subgroup $S_0 = \langle u\rangle \times \langle f\rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$ with $f^2 = c'$. Since $[\mathrm{N}_B(S_0), S_0] \leq S_0 \cap G' = \langle c'\rangle$, an element $x \in B$ lies in $\mathrm{N}_B(S_0)$ if and only if $[u,x] \in \langle c'\rangle$ and $[f,x] \in \langle c'\rangle$. As $u^b = uc'z$, we infer that $\mathrm{N}_B(S_0) \leq \mathrm{C}_B(u)$. But $br \in \mathrm{C}_B(u)$ and $[f, br] = c'z \neq c'$ and so $\mathrm{N}_B(S_0)$ is a proper subgroup of $\mathrm{C}_B(u)$ and so $|B : \mathrm{N}_B(S_0)| \geq 4$, a contradiction.

(ii2) We have proved that $\eta = 1$, i.e., $d' = c'z$. Since $[D, C] \leq \langle z\rangle$, we may set again

$$[b,r] = z^{\epsilon_1}, \quad [b,s] = z^{\epsilon_2}, \quad [f,r] = z^{\epsilon_3}, \quad [f,s] = z^{\epsilon_4},$$

where $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4 \in \{0,1\}$, and we look for involutions in $B-(C\cup D)$. We compute

$$(fr)^2 = c'z\cdot c'\cdot z^{\epsilon_3} = z^{1+\epsilon_3},$$
$$(fs)^2 = c'z\cdot c'z^{\epsilon}\cdot z^{\epsilon_4} = z^{1+\epsilon+\epsilon_4},$$
$$(f(rs))^2 = c'z\cdot c'z^{\epsilon}\cdot z^{\epsilon_3+\epsilon_4} = z^{1+\epsilon+\epsilon_3+\epsilon_4}.$$

If $\epsilon_3 = 1$, then $(fr)^2 = 1$, $(fs)^2 = z^{1+(\epsilon+\epsilon_4)}$, $(f(rs))^2 = z^{\epsilon+\epsilon_4}$ and so fr is an involution and either fs or frs is an involution. But in that case, we conclude that $[fr, fs] = c'z^{1+\epsilon_4} \neq 1$ and $[fr, frs] = c'z^{\epsilon_4} \neq 1$, contrary to the fact that $\Omega_1(G)$ must be elementary abelian. Hence $\epsilon_3 = 0$ and then

$$(fr)^2 = z, \quad (fs)^2 = z^{1+(\epsilon+\epsilon_4)}, \quad (frs)^2 = z^{1+(\epsilon+\epsilon_4)}.$$

If $\epsilon + \epsilon_4 \equiv 1 \pmod 2$, then both fs and frs are involutions which is not possible since $[fs, frs] = c' \neq 1$. Hence $\epsilon+\epsilon_4 \equiv 0 \pmod 2$ and so $\epsilon_4 = \epsilon$. We have proved that $[f,r] = 1$ and $[f,s] = z^{\epsilon}$ which gives $(fr)^2 = (fs)^2 = (frs)^2 = z$. Also note that $b^2 = (bf)^2 = z$ and so if there is an involution $i \in A - \langle z\rangle$, then i commutes with b (otherwise, $[i,b] = z$ and then $\langle i, b\rangle \cong \mathrm{D}_8$), bf, fr, fs, frs. But we have $\langle b, bf, fr, fs, frs\rangle = B$ and so $[A, B] = 1$, contrary to the fact that we know that $[A, B] = \langle z\rangle$. Hence $A = \langle a\rangle \cong \mathrm{C}_4$ with $a^2 = z$.

Suppose that there are no involutions in $G - B$. Then

$$[a,b] = [a,bf] = [a,fr] = [a,fs] = [a,frs] = z.$$

From $[a,b] = [a,bf] = z$ follows $[a,f] = 1$. But then $[a,r] = [a,s] = [a,rs] = z$, a contradiction. Hence it follows that a commutes with at least one element x in the set $L = \{b, bf, fr, fs, frs\}$ in which case ax is an involution in $G - B$. We check that no two distinct elements in the set L commute. If a would commute with two distinct elements $x, y \in L$, then ax and ay are involutions and then $1 = [ax, ay] = [x, y]$, a contradiction. We have proved that a must commute with exactly one of the five elements in L. But we may interchange s and rs and so it is enough to consider the following four cases:

(a) $[a,b] = 1$, (b) $[a,bf] = 1$, (c) $[a,fr] = 1$, (d) $[a,fs] = 1$.

(ii2a) We assume $[a,b]=1$ so that $i=ab$ is an involution in $G-B$ and

$$[a,bf]=[a,fr]=[a,fs]=[a,frs]=z.$$

This implies $[a,f]=z$, $[a,r]=[a,s]=1$. Since $i^f=(ab)^f=az\cdot bc'z=ic'$, $\{i,ic'\}$ are the only two conjugates of i in G. Then $i^r=(ab)^r=a\cdot bz^{\epsilon_1}=iz^{\epsilon_1}$ gives $\epsilon_1=0$ and $i^s=(ab)^s=a\cdot bz^{\epsilon_2}=iz^{\epsilon_2}$ gives $\epsilon_2=0$.

We have $\mathrm{C}_B(i)=\langle b\rangle\langle r,s\rangle=\langle b\rangle C$ and $i^f=ic'$. Consider the abelian subgroup $S=\langle i\rangle\times\langle br\rangle\cong\mathrm{C}_2\times\mathrm{C}_4$ with $(br)^2=zc'$. Since $[\mathrm{N}_G(S),S]\le S\cap G'=\langle zc'\rangle$, an element $x\in G$ lies in $\mathrm{N}_G(S)$ if and only if $[i,x]\in\langle zc'\rangle$ and $[br,x]\in\langle zc'\rangle$. As $i^f=ic'$, we have $\mathrm{N}_G(S)\le\mathrm{C}_G(i)$. But $s\in\mathrm{C}_G(i)$ and $(br)^s=br^s=(br)c'$ and so $\mathrm{N}_G(S)$ is a proper subgroup of $\mathrm{C}_G(i)$ and therefore $|G:\mathrm{N}_G(S)|\ge 4$, a contradiction.

(ii2b) We assume that $[a,bf]=1$ so that $i=abf$ is an involution in $G-B$ and $[a,b]=[a,fr]=[a,fs]=[a,frs]=z$. This gives $[a,f]=z$, $[a,r]=[a,s]=1$. Since

$$\begin{aligned}i^f&=(abf)^f=az\cdot bc'z\cdot f=ic',\\ i^r&=(abf)^r=a\cdot bz^{\epsilon_1}\cdot f=iz^{\epsilon_1},\\ i^s&=(abf)^s=a\cdot bz^{\epsilon_2}\cdot fz^{\epsilon}=iz^{\epsilon+\epsilon_2},\end{aligned}$$

we get $\epsilon_1=0$ and $\epsilon_2=\epsilon$.

If $\epsilon=0$, then we consider the abelian subgroup $S_1=\langle i\rangle\times\langle as\rangle\cong\mathrm{C}_2\times\mathrm{C}_4$ with $(as)^2=zc'$. As $[\mathrm{N}_G(S_1),S_1]\le S_1\cap G'=\langle zc'\rangle$, an element $x\in G$ lies in $\mathrm{N}_G(S_1)$ if and only if $[i,x]\in\langle zc'\rangle$ and $[as,x]\in\langle zc'\rangle$. Since $i^f=ic'$ and $|G:\mathrm{C}_G(i)|=2$ (noting that $\Omega_1(\mathrm{Z}(G))\le G'$), we obtain $\mathrm{N}_G(S_1)\le\mathrm{C}_G(i)$. But we have $r\in\mathrm{C}_G(i)$ and $(as)^r=(as)c'$ and so $\mathrm{N}_G(S_1)$ is a proper subgroup of $\mathrm{C}_G(i)$ and therefore we get $|G:\mathrm{N}_G(S_1)|\ge 4$, a contradiction.

If $\epsilon=1$, then we consider the abelian subgroup $S_2=\langle i\rangle\times\langle s\rangle\cong\mathrm{C}_2\times\mathrm{C}_4$ with $s^2=zc'$. Since $[\mathrm{N}_G(S_2),S_2]\le S_2\cap G'=\langle zc'\rangle$, an element $x\in G$ lies in $\mathrm{N}_G(S_2)$ if and only if $[i,x]\in\langle zc'\rangle$ and $[s,x]\in\langle zc'\rangle$. Because $i^f=ic'$ and $|G:\mathrm{C}_G(i)|=2$, we have $\mathrm{N}_G(S_2)\le\mathrm{C}_G(i)$. But $r\in\mathrm{C}_G(i)$ and $s^r=sc'$ and so $\mathrm{N}_G(S_2)$ is a proper subgroup of $\mathrm{C}_G(i)$ and therefore $|G:\mathrm{N}_G(S_2)|\ge 4$, a contradiction.

(ii2c) We assume $[a,fr]=1$ so that $i=afr$ is an involution in $G-B$ and

$$[a,b]=[a,bf]=[a,fs]=[a,frs]=z.$$

This gives $[a,f]=1$, $[a,r]=1$, $[a,s]=z$. We have

$$\begin{aligned}i^b&=(afr)^b=az\cdot fc'z\cdot rz^{\epsilon_1}=ic'z^{\epsilon_1},\\ i^s&=(afr)^s=az\cdot fz^{\epsilon}\cdot rc'=ic'z^{\epsilon+1},\end{aligned}$$

and so $\epsilon_1=\epsilon+1$. As $i^r=(afr)^r=i$ and $[i,sb]=1$, we have $\mathrm{C}_G(i)=\langle a,f,r,sb\rangle$.

If $\epsilon = 0$, then we consider the abelian subgroup $S_1 = \langle i \rangle \times \langle r \rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$ with $r^2 = c'$. Since $[\mathrm{N}_G(S_1), S_1] \leq S_1 \cap G' = \langle c' \rangle$, an element $x \in G$ lies in $\mathrm{N}_G(S_1)$ if and only if $[i, x] \in \langle c' \rangle$ and $[r, x] \in \langle c' \rangle$. Because $i^b = ic'z$ and $|G : \mathrm{C}_G(i)| = 2$, we have $\mathrm{N}_G(S_1) \leq \mathrm{C}_G(i) < G$. But $sb \in \mathrm{C}_G(i)$ and $[r, sb] = zc'$ and so $\mathrm{N}_G(S_1)$ is a proper subgroup of $\mathrm{C}_G(i)$ and therefore $|G : \mathrm{N}_G(S_1)| \geq 4$, a contradiction.

If $\epsilon = 1$, then we consider the abelian subgroup $S_2 = \langle i \rangle \times \langle ar \rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$ with $(ar)^2 = zc'$. Since $[\mathrm{N}_G(S_2), S_2] \leq S_2 \cap G' = \langle zc' \rangle$, an element $x \in G$ lies in $\mathrm{N}_G(S_2)$ if and only if $[i, x] \in \langle zc' \rangle$ and $[ar, x] \in \langle zc' \rangle$. Because $i^b = (afr)^b = ic'$ and $|G : \mathrm{C}_G(i)| = 2$, we get $\mathrm{N}_G(S_2) \leq \mathrm{C}_G(i) < G$. But $sb \in \mathrm{C}_G(i)$ and $[ar, sb] = c'$ and so $\mathrm{N}_G(S_2)$ is a proper subgroup of $\mathrm{C}_G(i)$ and therefore $|G : \mathrm{N}_G(S_2)| \geq 4$, a contradiction.

(ii2d) We assume $[a, fs] = 1$ so that $i = afs$ is an involution in $G - B$ and

$$[a, b] = [a, bf] = [a, fr] = [a, frs] = z.$$

This gives $[a, f] = 1$, $[a, r] = z$, $[a, s] = 1$. We have

$$i^b = (afs)^b = az \cdot fc'z \cdot sz^{\epsilon_2} = ic'z^{\epsilon_2}, \quad i^s = (afs)^s = a \cdot fz^{\epsilon} \cdot s = iz^{\epsilon},$$

and so $\epsilon = 0$. Also,

$$i^r = (afs)^r = az \cdot f \cdot sc' = izc'$$

which gives $\epsilon_2 = 1$ and $i^f = i$, $i^{br} = i$ and therefore $\mathrm{C}_G(i) = \langle a, f, s, br \rangle$.

We consider the abelian subgroup $S = \langle i \rangle \times \langle s \rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$ with $s^2 = c'$. Since $[\mathrm{N}_G(S), S] \leq S \cap G' = \langle c' \rangle$, an element $x \in G$ lies in $\mathrm{N}_G(S)$ if and only if $[i, x] \in \langle c' \rangle$ and $[s, x] \in \langle c' \rangle$. As $i^b = ic'z$ and $|G : \mathrm{C}_G(i)| = 2$, we have $\mathrm{N}_G(S) \leq \mathrm{C}_G(i) < G$. But $br \in \mathrm{C}_G(i)$ and $[s, br] = zc'$ and so $\mathrm{N}_G(S)$ is a proper subgroup of $\mathrm{C}_G(i)$ and therefore $|G : \mathrm{N}_G(S)| \geq 4$, a contradiction.

Part 2, where $D/\langle z \rangle \cong \mathrm{P}$. Here P is the nonmetacyclic minimal nonabelian subgroup of order 2^4. We set

$$W/\langle z \rangle = \mathrm{Z}(D/\langle z \rangle) = \Phi(D/\langle z \rangle)$$

so that

$$W > G', \quad |W : G'| = 2, \quad W/\langle z \rangle \cong \mathrm{E}_4, \quad W/\langle z \rangle = \mathrm{Z}(B/\langle z \rangle)$$

and hence $\mathrm{Z}(B) \leq W$. There is $y \in D$ such that $y^2 \in W - G'$ (noting that $\Phi(D)$ covers $W/\langle z \rangle$). For each $g \in G$, $[y^2, g] = [y, g]^2 = 1$ and so $y^2 \in \mathrm{Z}(G)$ and therefore $W \leq \mathrm{Z}(G)$, $W = \mathrm{Z}(B)$, and $B/\mathrm{Z}(B) \cong \mathrm{E}_{2^4}$. Since $[A, B] \leq \langle z \rangle$ and $A/\langle z \rangle$ is elementary abelian, we get $W = \Phi(G)$. Each of three maximal subgroups of D containing W are abelian and so $D' = \langle d' \rangle$ is of order 2, where $d' \in G' - \langle z \rangle$.

First suppose that $z \notin \Phi(D)$ and then $D = \langle z \rangle \times P_0$, where $P_0 \cong \mathrm{P}$ so that we may set

$$P_0 = \langle b, t \mid b^4 = t^2 = 1,\ [b, t] = d',\ (d')^2 = [d', t] = [d', b] = 1 \rangle.$$

Since $\{t, t^b = td'\}$ are the only two conjugates of t in G and $[C, D] \leq \langle z\rangle$, we must have $[t, r] = [t, s] = 1$. Similarly, $\langle b\rangle$ and $\langle b^t\rangle = \langle bd'\rangle$ are the only two conjugates of $\langle b\rangle$ in G and so $[b, r] = [b, s] = 1$. We have proved that $[C, D] = \{1\}$. If $D' = C'$, then $B' = C' = D'$ is of order 2, contrary to $B' = G'$. Hence we have $d' \neq c'$ and so $d' = c'z$. We claim that $\langle br\rangle \cong \mathrm{C}_4$, $\langle (br)^t\rangle = \langle br \cdot c'z\rangle$ and $\langle (br)^s\rangle = \langle br \cdot c'\rangle$ are three distinct cyclic subgroups of order 4 and this gives a contradiction. Indeed, the elements of order 4 in $\langle br\rangle$ are br and $(br)(br)^2 = br \cdot b^2c'$, the elements of order 4 in $\langle br \cdot c'z\rangle$ are $br \cdot c'z$ and $br \cdot b^2z$, and the elements of order 4 in $\langle br \cdot c'\rangle$ are $br \cdot c'$ and $br \cdot b^2$. We see that the above six elements of order 4 are pairwise distinct and we are done.

We have proved that $z \in \Phi(D)$ and so $W = \Phi(D)$ with $D/W \cong \mathrm{E}_4$ which together with $|D'| = 2$ implies that D is minimal nonabelian of order 2^5. Since $D/\langle z\rangle \cong \mathrm{P}$ is nonmetacyclic of exponent 4, it follows that D is nonmetacyclic of exponent 4 or 8.

If D is of exponent 4, then

$$D = \langle b, f \mid b^4 = f^4 = 1,\ [b, f] = d',\ (d')^2 = [d', b] = [d', f] = 1\rangle,$$

where

$$\Omega_1(D) = W = \Phi(D) = \mathrm{Z}(D) = \langle b^2, f^2, d'\rangle \cong \mathrm{E}_8.$$

In case that z is not a square in D, we get $\Omega_1(D/\langle z\rangle) = W/\langle z\rangle \cong \mathrm{E}_4$ which implies that $D/\langle z\rangle$ is metacyclic minimal nonabelian, contrary to $D/\langle z\rangle \cong \mathrm{P}$. Hence z is a square in D so that we may choose the generators b and f of D so that $b^2 = z$.

If D is of exponent 8, then

$$D = \langle b, t \mid b^8 = t^2 = 1,\ [b, t] = d',\ (d')^2 = [d', b] = [d', t] = 1\rangle,$$

where $b^4 = z$ since $D/\langle z\rangle \cong \mathrm{P}$ is of exponent 4.

We have proved that in any case z is a square in D. Suppose that $A \cong \mathrm{Q}_8$. Then we know that $[A, B] = \{1\}$ and let $b' \in D$ be such that $(b')^2 = z$. But then the subgroup $A * \langle b'\rangle$ with $A \cap \langle b'\rangle = \langle z\rangle$ possesses a subgroup isomorphic to D_8, a contradiction. If $A \leq \mathrm{Z}(G)$, then $|G/\mathrm{Z}(G)| = 2^4$, a contradiction. Hence we have $A \cong \mathrm{C}_4$ or E_4 and $[A, B] = \langle z\rangle$.

(i) First suppose that D is of exponent 4, i.e.,

$$D = \langle b, f \mid b^4 = f^4 = 1,\ [b, f] = d',\ (d')^2 = [d', b] = [d', f] = 1\rangle,$$

where $b^2 = z$ and $d' \in G' - \langle z\rangle$. Now, $\langle f\rangle$ (where f and ff^2 are its elements of order 4) and $\langle f^b\rangle = \langle fd'\rangle$ (where fd' and ff^2d' are its elements of order 4) are the only conjugates of $\langle f\rangle$ in G. Hence if $[f, C] = \langle z\rangle$, then $\langle f\rangle$ is conjugate under C to $\langle fz\rangle$ (where fz and ff^2z are its elements of order 4) and so $\langle fz\rangle$ is distinct from $\langle f\rangle$ and $\langle fd'\rangle$, a contradiction. Similarly, $\langle fb\rangle$ (where fb and fbf^2zd' are its elements of order 4) and $\langle (fb)^b\rangle = \langle fbd'\rangle$ (where fbd' and fbf^2z are its elements of order 4) are the only conjugates of $\langle fb\rangle$ in G. Hence if $[fb, C] = \langle z\rangle$, then $\langle fb\rangle$

is conjugate under C to $\langle fbz\rangle$ (where fbz and fbf^2d' are its elements of order 4) and so $\langle fbz\rangle$ is distinct from $\langle fb\rangle$ and $\langle fbd'\rangle$, a contradiction. Since $D = \langle f, fb\rangle$, we get $[C, D] = \{1\}$ which implies $D' \neq C'$ (since $B' = G'$) and so $d' = c'z$.

We claim that $\langle fr\rangle \cong \mathrm{C}_4$ has more than two conjugates in G which gives a contradiction. Indeed, $\langle fr\rangle$ (where fr and frf^2c' are its elements of order 4), $\langle (fr)^b\rangle = \langle frc'z\rangle$ (where $frc'z$ and frf^2z are its elements of order 4), and $\langle (fr)^s\rangle = \langle frc'\rangle$ (where frc' and frf^2 are its elements of order 4) are three pairwise distinct conjugates of $\langle fr\rangle$.

(ii) Now assume that D is of exponent 8, i.e.,

$$D = \langle b, t \mid b^8 = t^2 = 1,\ [b,t] = d',\ (d')^2 = [d', b] = [d', t] = 1\rangle,$$

where $b^4 = z$ and $d' \in G' - \langle z\rangle$. We have here

$$W = \langle b^2\rangle \times \langle c'\rangle = \langle b^2\rangle \times \langle d'\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$$

and $W = \mathrm{Z}(B) = \mathrm{Z}(G) = \Phi(G)$. Since $\{t, t^b = td'\}$ is the complete conjugate class in G, $[C, t] = \langle z\rangle$ is not possible and so we get $[t, r] = [t, s] = 1$.

We have $r^2 = c'$ and $s^2 = (rs)^2 = c'z^\epsilon$, $\epsilon = 0, 1$. Assume at the moment that $\epsilon = 1$ so that $C \cong \mathrm{H}_2$. Then replace s with $s' = sb^2$, where $o(b^2) = 4$ and $b^2 \in \mathrm{Z}(B)$. We obtain $(s')^2 = (sb^2)^2 = s^2b^4 = c'z \cdot z = c'$ and $[s', r] = [s, r] = c'$ so that $\langle r, s'\rangle \cong \mathrm{Q}_8$. Replacing $C = \langle r, s\rangle$ with $C^* = \langle z\rangle \times \langle r, s'\rangle \cong \mathrm{C}_2 \times \mathrm{Q}_8$, we may assume (writing again s instead of s' and C instead of C^*) from the start that $\epsilon = 0$, i.e., $s^2 = (rs)^2 = c'$ and $C = \langle z\rangle \times \langle r, s\rangle$, where $\langle r, s\rangle \cong \mathrm{Q}_8$. Since $[b, \langle r, s\rangle] \leq \langle z\rangle$, we may choose the generators r, s of $\langle r, s\rangle$ so that $[b, r] = 1$.

Assume that $d' = c'$ in which case we must have $[b, s] = z$ since $B' = G'$. Consider the abelian subgroup $S = \langle t\rangle \times \langle b^2s\rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$, where $(b^2s)^2 = zc'$. Note that $[\mathrm{N}_B(S), S] \leq S \cap B' = \langle zc'\rangle$. We conclude that $|B : \mathrm{C}_B(t)| = 2$ and $t^b = tc'$ so that $\mathrm{N}_B(S) \leq \mathrm{C}_B(t)$. But r centralizes t and $(b^2s)^r = (b^2s)c'$ and so $r \notin \mathrm{N}_B(S)$ and therefore $|B : \mathrm{N}_B(S)| \geq 4$, a contradiction.

We have proved that $d' = c'z$ and so we have the following two possibilities: $[b, s] = 1$ or $[b, s] = z$. But we shall show that these two possibilities give isomorphic groups. Indeed, if $[b, s] = z$, then replace b with $b^* = br$ and replace s with $s^* = ts$. We have

$$(b^*)^4 = (br)^4 = z, \quad [b^*, t] = [br, t] = zc',$$

where $\langle c'\rangle = \langle s^*, r\rangle'$ and $Q^* = \langle s^*, r\rangle \cong \mathrm{Q}_8$ since $(s^*)^2 = s^2 = c'$, $r^2 = c'$, and $[s^*, r] = [ts, r] = c'$. In addition, $[\langle b^*, t\rangle, Q^*] = \{1\}$. Indeed, t commutes with Q^*, $[b^*, r] = [br, r] = [b, r] = 1$ and

$$[b^*, s^*] = [br, ts] = [b, t][b, s][r, t][r, s] = zc' \cdot z \cdot 1 \cdot c' = 1.$$

Thus we may assume from the start that $[b, s] = 1$. The structure of B is uniquely determined.

It is easy to see that there are involutions in $G - B$. Indeed, if $A \cong \mathrm{E}_4$, then there is an involution $i \in A - \langle z \rangle = A - B$. Suppose that $A = \langle v \rangle \cong \mathrm{C}_4$ with $v^2 = z$. Since $b^2 \in \mathrm{Z}(G)$ and $b^4 = z$, $i = vb^2$ is an involution in $G - B$.

Let i be an involution in $G - B$ from the previous paragraph. Then we deduce that $\langle i, t \rangle \cong \mathrm{E}_4$, $\langle i, t \rangle \cap G' = \{1\}$ and $\langle i, t \rangle \cap \mathrm{Z}(G) = \{1\}$. From

$$[\mathrm{N}_G(\langle i, t \rangle), \langle i, t \rangle] \leq \langle i, t \rangle \cap G' = \{1\}$$

it follows that

$$\mathrm{N}_G(\langle i, t \rangle) = \mathrm{C}_G(\langle i, t \rangle) = \mathrm{C}_G(i) \cap \mathrm{C}_G(t).$$

But $|G : \mathrm{N}_G(\langle i, t \rangle)| = 2$ and so we must have $\mathrm{C}_G(i) = \mathrm{C}_G(t) = \langle i, t \rangle \times \langle b^2, r, s \rangle$, which is a subgroup of index 2 in G. As $[t, b] = c'z \neq 1$, we have also $[i, b] \neq 1$. Note that $[A, b] \leq \langle z \rangle$ and so if $i \in A$, then $[i, b] = z$. If $i = vb^2$ (in case $A = \langle v \rangle \cong \mathrm{C}_4$), then $[i, b] = [vb^2, b] = [v, b] = z$. Hence in any case $[i, b] = z$. Consider the abelian subgroup $S = \langle it \rangle \times \langle b^2 s \rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$, where $(b^2 s)^2 = b^4 s^2 = zc'$. Note that $[\mathrm{N}_G(S), S] \leq S \cap G' = \langle zc' \rangle$. In view of $(it)^b = iz \cdot tc'z = it \cdot c'$, we must have $\mathrm{N}_G(S) \leq \mathrm{C}_G(it) = \mathrm{C}_G(t)$. On the other hand, r centralizes it but $(b^2 s)^r = b^2 s \cdot c'$ and so $r \notin \mathrm{N}_G(S)$. We obtain that $|G : \mathrm{N}_G(S)| \geq 4$, a contradiction. Theorem 122.1 is completely proved for $p = 2$. □

Proof of Theorem 122.1 for $p > 2$. Let G be a p-group, $p > 2$, with $\mathrm{sb}(G) = 1$ which is a minimal counterexample to Theorem 122.1 and so $|G/\mathrm{Z}(G)| > p^3$. By Proposition 122.9, $\Omega_1(\mathrm{Z}(G)) \leq G'$. Due to Proposition 122.8, $\mathrm{b}(G) \leq 2$, i.e., the element breadth of G is at most 2. If $\mathrm{b}(G) = 1$, then Proposition 121.9 implies that $|G'| = p$. But then Proposition 122.13 gives $|G/\mathrm{Z}(G)| = p^2$, a contradiction. Hence we obtain $\mathrm{b}(G) = 2$. In that case, Theorem 121.1 implies $|G'| = p^2$ (because $|G'| = p^3$ would imply $|G/\mathrm{Z}(G)| = p^3$). Also, we note that G cannot possess an abelian maximal subgroup because in that case Lemma 1.1 gives $|G| = p|\mathrm{Z}(G)||G'|$ and then we conclude $|G/\mathrm{Z}(G)| = p^3$, a contradiction.

Let $1 \neq z \in G' \cap \Omega_1(\mathrm{Z}(G))$ so that for $\bar{G} = G/\langle z \rangle$, $\mathrm{b}(\bar{G}) = 1$ and $\mathrm{sb}(\bar{G}) = 1$. Set $R/\langle z \rangle = \mathrm{Z}(\bar{G})$ and then Proposition 122.13 gives $G/R \cong \mathrm{E}_{p^2}$. We have $r \in R$ if and only if $[G, r] \leq \langle z \rangle$ in which case $|G : \mathrm{C}_G(r)| \leq p$. Also, $[G, R] = \langle z \rangle$ because if $[G, R] = 1$, then $|G/\mathrm{Z}(G)| = p^2$, a contradiction. As $[G, G'] \leq \langle z \rangle$, we have $G' \leq R$.

Let A be any maximal normal abelian subgroup in G which contains $\Phi(G)$, where $\Phi(G)$ is abelian (Proposition 122.2). By Proposition 122.10, we have $\mathrm{sb}_A(G) = 2$, and we fix an element $g \in G$ such that $|A : \mathrm{C}_A(g)| = p^2$ and then $|[A, g]| = p^2$ (Proposition 121.2) so that $[A, g] = G'$. This implies that $A \not\leq R$ and R does not cover G/A so that $|A : (A \cap R)| = p$ and $|G : (AR)| = p$, where $g \in G - (AR)$ so that $G = (AR)\langle g \rangle$. For each $x \in (AR) - A$, $x \in \mathrm{T}_A$, i.e., $|A : \mathrm{C}_A(x)| = p$ (noting that for each $r \in R$ we have $|G : \mathrm{C}_G(r)| \leq p$). Since $|A : \mathrm{C}_A(g)| = p^2$, g does not centralize $R \cap A$ and so $[R \cap A, g] = \langle z \rangle$ which implies $|(R \cap A) : \mathrm{C}_{R \cap A}(g)| = p$ and therefore $\mathrm{C}_{R \cap A}(g) = \mathrm{C}_A(g)$ so that $g^p \in \mathrm{C}_{R \cap A}(g)$. As $[R, R] \leq \langle z \rangle$ and $[g, R] = \langle z \rangle$, we have $(R\langle g \rangle)' = \langle z \rangle$. Also, $R' \leq \langle z \rangle$ and $[A, R] = \langle z \rangle$ (noting that $R \not\leq A$ since G has no abelian maximal subgroup) and so $(AR)' = \langle z \rangle$.

Assume that $|G/A| > p^2$ so that $|(AR)/A| \geq p^2$. We have $\mathrm{Z}(AR) < A$ and so $|(AR) : \mathrm{Z}(AR)| \geq p^3$, which contradicts Proposition 122.13 applied to AR. Hence we get $G/A \cong \mathrm{E}_{p^2}$ and then $|R : (R \cap A)| = p$. Since $(R\langle g\rangle)' = \langle z\rangle$, we may apply Proposition 122.3 to $R\langle g\rangle$ and we get $|(R\langle g\rangle) : \mathrm{Z}(R\langle g\rangle)| = p^2$.

Suppose that R is abelian. Then

$$\mathrm{C}_G(\mathrm{C}_A(g)) \geq \langle A, R, g\rangle = G$$

which gives $\mathrm{Z}(G) = \mathrm{C}_A(g)$ and $|G : \mathrm{Z}(G)| = p^4$.

Now assume that R is nonabelian so that $R' = \langle z\rangle$. In that case, $R \cap A$ is an abelian maximal subgroup of R and then we get from $|R| = p|\mathrm{Z}(R)||R'|$ (Lemma 1.1) that $|R : \mathrm{Z}(R)| = p^2$, where $Z = \mathrm{Z}(R)$ is a subgroup of index p in $R \cap A$. But we infer that $|(R\langle g\rangle) : \mathrm{Z}(R\langle g\rangle)| = p^2$, and so there is an element $h \in (R\langle g\rangle) - R$ such that $h \in \mathrm{Z}(R\langle g\rangle)$. We get $\mathrm{C}_G(Z) \geq \langle A, R, h\rangle = G$ and so again $Z = \mathrm{C}_A(g) = \mathrm{Z}(G)$ and $|G : \mathrm{Z}(G)| = p^4$.

Thus we have proved that for any maximal normal abelian subgroup A of G containing $\Phi(G)$, $G/A \cong \mathrm{E}_{p^2}$ and $\mathrm{C}_A(g) = \mathrm{Z}(G)$ is of index p^4 in G, where $g \in G - A$ is such that $|A : \mathrm{C}_A(g)| = p^2$. We shall fix this notation for A, R and g in the rest of the proof.

(i) We prove that $\Omega_1(G)$ is elementary abelian.

Suppose that x, y are some elements of order p in the group G such that $[x, y] \neq 1$. Then $C = \mathrm{C}_G(x) = \mathrm{N}_G(\langle x\rangle)$ implies that $|G : C| = p$ and $y \in G - C$ so that the set $\{x, x^y, \ldots, x^{y^{p-1}}\}$ contains p conjugates of x in G and they are all central elements in C which implies that $N = \langle x, x^y, \ldots, x^{y^{p-1}}\rangle$ is an elementary abelian normal subgroup in G, $N \leq C$, and $|N| \geq p^2$. Set $N_0 = \mathrm{C}_N(y)$ so that $|N : N_0| = p$ and $x \in N - N_0$ since $|G : \mathrm{C}_G(y)| = p$. We have $N_0 = \mathrm{Z}(\langle x, y\rangle)$ and $\langle x, y\rangle/N_0 \cong \mathrm{E}_{p^2}$ so that $1 \neq [x, y] = z' \in N_0$ and $\langle x, y\rangle' = \langle z'\rangle$ is of order p which implies that $\langle x, y\rangle$ is minimal nonabelian. Hence $S = \langle x, y\rangle \cong \mathrm{S}(p^3)$ which is the minimal nonabelian group of order p^3 and exponent p and so $N_0 = \langle z'\rangle$ and $N \cong \mathrm{E}_{p^2}$.

All p conjugates of x in S are contained in $\langle x, z'\rangle$ and they are all conjugates of x in G and so $\langle x, z'\rangle \trianglelefteq G$. Similarly, all p conjugates of y in S are contained in $\langle y, z'\rangle$ and they are all conjugates of y in G and so $\langle y, z'\rangle \trianglelefteq G$. This fact implies that $S = \langle x, y\rangle \trianglelefteq G$, $G = S * P$, where $P = \mathrm{C}_G(S)$ and $S \cap P = \langle z'\rangle = \mathrm{Z}(S)$. If P is abelian, then $G' = S' = \langle z'\rangle$ is of order p, a contradiction. Hence P is nonabelian and so P possesses nonnormal subgroups (Lemma 1.18). If all nonnormal subgroups of P contain $\langle z'\rangle$, then Corollary 92.7 (N. Blackburn) implies $p = 2$, a contradiction. Let P_1 be a nonnormal subgroup of P such that $z' \notin P_1$ and set $U = \langle P_1, x\rangle = P_1 \times \langle x\rangle$. We have $U \cap P = P_1$ and $U \cap S = \langle x\rangle$. If $h \in G$ normalizes U, then h normalizes $U \cap S = \langle x\rangle$ and so h centralizes x. But h also normalizes $U \cap P = P_1$ and so we get $\mathrm{N}_G(U) = \mathrm{C}_G(x) \cap \mathrm{N}_G(P_1)$. On the other hand, we have $\mathrm{C}_G(x) = P \times \langle x\rangle$ and $|G : \mathrm{C}_G(x)| = p$. But P_1 is not normal in $P \times \langle x\rangle$ (since P_1 is a nonnormal subgroup of P_1) and so $\mathrm{N}_G(U)$ is a proper subgroup of $P \times \langle x\rangle$ which gives $|G : \mathrm{N}_G(U)| \geq p^2$, a contradiction.

(ii) $\Omega_1(G)$ is elementary abelian of order p^3.

First suppose that G possesses a normal elementary abelian subgroup F of order p^4. Set $F_0 = F \cap G'$ so that $|F_0| \leq p^2$. Let x, y be any elements in $F - F_0$ such that $\langle x, y\rangle \cong \mathrm{E}_{p^2}$ and $\langle x, y\rangle \cap G' = \{1\}$. Then $[\mathrm{N}_G(\langle x, y\rangle), \langle x, y\rangle] \leq \langle x, y\rangle \cap G' = \{1\}$ and so

$$\mathrm{N}_G(\langle x, y\rangle) = \mathrm{C}_G(\langle x, y\rangle) = \mathrm{C}_G(x) \cap \mathrm{C}_G(y).$$

Note that for each $x \in F - F_0$ we have $|G : \mathrm{C}_G(x)| = p$ since $\Omega_1(\mathrm{Z}(G)) \leq G'$. As $|G : \mathrm{N}_G(\langle x, y\rangle)| = p$, we have $C = \mathrm{C}_G(x) = \mathrm{C}_G(y)$ and so $C = \mathrm{C}_G(F)$ is a subgroup of index p in G. In particular, $\Phi(G)$ centralizes F and so we may choose a maximal normal abelian subgroup A of G so that $A \geq F\Phi(G)$. Recalling our results about A and $g \in G - A$ with $|A : \mathrm{C}_A(g)| = p^2$ (from the beginning of our proof), we know that $G/A \cong \mathrm{E}_{p^2}$ and $\mathrm{C}_A(g) = \mathrm{Z}(G)$. Since $\mathrm{C}_F(g) \leq \Omega_1(\mathrm{Z}(G)) \leq G'$ and $|G'| = p^2$, we see that $|\mathrm{C}_F(g)| \leq p^2$ and so F covers $A/\mathrm{C}_A(g)$. But $C = \mathrm{C}_G(F)$ is a subgroup of index p in G and so $C > A$ and C centralizes $\langle \mathrm{Z}(G), F\rangle = A$, contrary to $\mathrm{C}_G(A) = A$.

Now assume that $\Omega_1(G) \cong \mathrm{E}_{p^2}$. In view of Theorem 13.7, G is either metacyclic (with $G' \cong \mathrm{C}_{p^2}$) or a 3-group of maximal class. In case that G is metacyclic, Proposition 122.7 implies that $\mathrm{sb}(G) > 1$, a contradiction. If G is a 3-group of maximal class, then $|G/G'| = 3^2$ and so $|G| = 3^4$. But then $|G : \mathrm{Z}(G)| \leq 3^3$, a contradiction. Thus we have proved that $\Omega_1(G) \cong \mathrm{E}_{p^3}$.

(iii) We have $\mathrm{E}_{p^3} \cong O = \Omega_1(G) \leq \Phi(G)$.

Suppose that this is false. Let N be a maximal subgroup of G which does not contain O so that $O \cap N = \Omega_1(N) \cong \mathrm{E}_{p^2}$. Also we know that N is nonabelian. By Theorem 13.7, N is either metacyclic or a 3-group of maximal class. Suppose that N is metacyclic. If $N' \cong \mathrm{C}_{p^2}$, then Proposition 122.7 implies that $\mathrm{sb}(N) > 1$, a contradiction. Hence we have $|N'| = p$ which gives that N is minimal nonabelian and then $\Phi(N) = \mathrm{Z}(N)$ and $|N : \mathrm{Z}(N)| = p^2$. Let $y \in O - N$ so that $|N : \mathrm{C}_N(y)| = p$ and thus y centralizes $\Phi(N) = \mathrm{Z}(N)$ which gives $\mathrm{Z}(N) = \mathrm{Z}(G)$ and $|G : \mathrm{Z}(G)| \leq p^3$, a contradiction.

We have proved that N is a 3-group of maximal class. In that case, $|N : N'| = 3^2$. If $|N'| = 3$, then $|N| = 3^3$, $|G| = 3^4$ and $|G : \mathrm{Z}(G)| \leq 3^3$, a contradiction. Hence $|N'| = 3^2$ and $|G| = 3^5$. We have $G' \leq N \cap O$ and so

$$G' = N' = N \cap O \cong \mathrm{E}_9.$$

Since $N/N' \cong \mathrm{E}_9$ and $O/N' \cong \mathrm{C}_3$, we get $\Phi(G) = \Phi(N) = N \cap O = G'$. As G has no abelian maximal subgroup, we have $\mathrm{C}_G(O) = O$ so that $O = A$ is a maximal normal abelian subgroup of G containing $\Phi(G)$. We recall our results about A, R and g from the beginning of the proof. Since $R \geq G'$, we obtain $R \cap A = G'$, $g^3 \in G'$, and $N^* = R\langle g\rangle$ is another maximal subgroup of G which does not contain O since $N^* \cap A = G' = \Omega_1(N^*) \cong \mathrm{E}_9$ and $|(N^*)'| = 3$. By Theorem 13.7, N^* is metacyclic and so N^* is minimal nonabelian with $\mathrm{Z}(N^*) = \Phi(N^*)$ and $|N^* : \mathrm{Z}(N^*)| = 3^2$.

Let $v \in A - G'$ so that v centralizes a maximal subgroup of N^* and so v centralizes $\Phi(N^*) = \mathrm{Z}(N^*)$ which forces $\mathrm{Z}(N^*) \leq \mathrm{Z}(G)$. But then $|G : \mathrm{Z}(G)| \leq 3^3$, a contradiction.

It is now easy to complete the proof of Theorem 122.1 for $p > 2$. To do this, we recall again our results about $A \geq \Phi(G)$, R, g and z from the beginning of the proof. We have $\Phi(G) \leq (R\langle g\rangle) \cap A = R \cap A$, where $G/A \cong \mathrm{E}_{p^2}$, $|A : (R \cap A)| = p$, $|(R \cap A) : \mathrm{C}_{R\cap A}(g)| = p$, and $\mathrm{C}_A(g) = \mathrm{C}_{R\cap A}(g) = \mathrm{Z}(G)$. By (iii), we conclude that $\mathrm{E}_{p^3} \cong O = \Omega_1(G) \leq \Phi(G)$ and so $O \leq R \cap A$. Since $\Omega_1(\mathrm{Z}(G)) \leq G'$, we have $O \not\leq \mathrm{Z}(G)$ and so $\mathrm{E}_{p^2} \cong G' = O \cap \mathrm{Z}(G)$ and O covers $(R \cap A)/\mathrm{Z}(G)$. In particular, the group G is of class 2 with an elementary abelian commutator subgroup of order p^2. For each $x, y \in G$ we have $[x^p, y] = [x, y]^p = 1$ and so $x^p \in \mathrm{Z}(G)$ which implies that $\Phi(G) = \mathfrak{V}_1(G)G' \leq \mathrm{Z}(G)$. But then $O \leq \Phi(G) \leq \mathrm{Z}(G)$, a final contradiction. Theorem 122.1 is completely proved. □

It follows from Theorem 122.1 that if G is a metacyclic group of order p^{2m+1}, where $m > 1$ if $p > 2$ and $n > 2$ if $p = 2$, then there is in G a subgroup H such that $|G : \mathrm{N}_G(H)| > p$.

§123

Subgroups of finite groups generated by all elements in two shortest conjugacy classes

Here we present some results of I. M. Isaacs (Subgroups generated by small classes in finite groups, *Proc. Amer. Math. Soc.* **136** (2008), 2299–2301) which generalize the results of A. Mann about subgroups of p-groups which are generated by all elements of the first two class sizes.

Let $\mathrm{M}(G)$ be the subgroup of a finite group G generated by all elements that lie in conjugacy classes of the two smallest sizes. The following simple result is the key for all following arguments.

Lemma 123.1. *Let A be an abelian normal subgroup of a group G. Let x be a noncentral element of G and $a \in A$. Then $|\mathrm{C}_G([a,x])| > |\mathrm{C}_G(x)|$, and so the G-class of $[a,x]$ is smaller than that of x.*

Proof. Consider the map $u \to [u,x]$ ($u \in A$) from A into A. Since for any $u, v \in A$ we have $[uv,x] = [u,x]^v[v,x] = [u,x][v,x]$, it follows that our map is a homomorphism onto $[A,x] = \{[u,x] \mid u \in A\}$ with kernel $\mathrm{C}_A(x)$. Thus $[A,x]$ is a subgroup of A and $|[A,x]| = |A/\mathrm{C}_A(x)|$.

Set $H = A\mathrm{C}_G(x)$ so that $|H| = (|A||\mathrm{C}_G(x)|)/|\mathrm{C}_A(x)|$ and

$$|A|/|\mathrm{C}_A(x)| = |H|/|\mathrm{C}_G(x)|.$$

Obviously, $[A,x] \trianglelefteq H$. Indeed, if $c \in \mathrm{C}_G(x)$ and $[u,x] \in [A,x]$ with $u \in A$, then $[u,c]^c = [u^c, x^c] = [u^c, x] \in [A,x]$.

We may assume that $[a,x] \neq 1$ because x is noncentral (and so in case $[a,x] = 1$, our result is trivial). Hence the conjugacy class of $[a,x]$ in H has $|H|/|\mathrm{C}_H([a,x])|$ elements so that

$$|H|/|\mathrm{C}_H([a,x])| < |[A,x]| = |A|/|\mathrm{C}_A(x)| = |H|/|\mathrm{C}_G(x)|$$

which gives $|\mathrm{C}_H([a,x])| > |\mathrm{C}_G(x)|$ and we are done. □

Lemma 123.2. *For an abelian normal subgroup A of a group G, $[A, \mathrm{M}(G)] \leq \mathrm{Z}(G)$.*

Proof. If $x \in \mathrm{M}(G)$ is contained in a conjugacy class of G of size m, where m is the smallest class size exceeding 1, then, by Lemma 123.1, we have $[a,x] \in \mathrm{Z}(G)$ for each $a \in A$. Hence all generators of $\mathrm{M}(G)$ centralize $A/(A \cap \mathrm{Z}(G))$. Thus $\mathrm{M}(G)$ centralizes $A/(A \cap \mathrm{Z}(G))$ and so $[A, \mathrm{M}(G)] \leq \mathrm{Z}(G)$. □

Theorem 123.3. *Let G be a group that contains a self-centralizing abelian normal subgroup A. Then* $\mathrm{M}(G)$ *is nilpotent of class at most* 3.

Proof. Set $M = \mathrm{M}(G)$ so that Lemma 123.2 yields $[A, M] \leq \mathrm{Z}(G)$ and therefore $[A, M, M] = \{1\}$. Since $[M, A, M] = \{1\}$, the three-subgroups lemma implies that $[M, M, A] = \{1\}$ and then $M' \leq \mathrm{C}_G(A) = A$. But in that case we get $[M', M, M] \leq [A, M, M] = \{1\}$, and so M is nilpotent of class at most 3. □

A maximal normal abelian subgroup in a supersolvable group G is self-centralizing and so we get the following result.

Corollary 123.4. *Let G be a supersolvable group. Then* $\mathrm{M}(G)$ *is nilpotent of class at most* 3. *In particular, if G is a p-group, then* $\mathrm{M}(G)$ *is of class at most* 3.

Theorem 123.5. *Let G be a group and assume that* $\mathrm{M}(G)$ *has a nonidentity solvable normal subgroup. Then* $\mathrm{Z}(\mathrm{M}(G))$ *is nontrivial.*

Proof. Write $M = \mathrm{M}(G)$. By our assumption, the Fitting subgroup $\mathrm{F}(M)$ of M is nontrivial. Let $Z = \mathrm{Z}(\mathrm{F}(M))$ so that Z is a nontrivial characteristic abelian subgroup of M, and therefore $Z \trianglelefteq G$. Due to Lemma 123.2, $[Z, M] \leq \mathrm{Z}(G)$. If $[Z, M] \neq \{1\}$, then $\mathrm{Z}(G)$ is nontrivial. By the definition of $M = \mathrm{M}(G)$, $\mathrm{Z}(G) \leq M$ and so $\mathrm{Z}(M)$ is nontrivial and we are done in this case. If $[Z, M] = \{1\}$, then $\{1\} \neq Z \leq \mathrm{Z}(M)$. In any case, $\mathrm{Z}(M)$ is nontrivial. □

Finally, we prove a result about arbitrary finite group G (without any assumptions).

Theorem 123.6. *Let G be any finite group. Then the Fitting subgroup of* $\mathrm{M}(G)$ *has the nilpotence class at most* 4.

Proof. Write again $M = \mathrm{M}(G)$ and set $F = \mathrm{F}(M)$. Let n be the nilpotence class of F so that $\mathrm{K}_n(F) \neq \{1\}$ and $\mathrm{K}_{n+1}(F) = \{1\}$. We want to show that $n \leq 4$ and so we may assume that $n \geq 3$ so that $\mathrm{K}_{n-2}(F)$ is defined. If this normal subgroup is abelian, Lemma 123.2 yields $[\mathrm{K}_{n-2}(F), M] \leq \mathrm{Z}(G)$ and then $\mathrm{K}_n(F) = [\mathrm{K}_{n-2}(F), M, M] = \{1\}$, a contradiction. Hence $\mathrm{K}_{n-2}(F)$ is nonabelian and then

$$\{1\} \neq [\mathrm{K}_{n-2}(F), \mathrm{K}_{n-2}(F)] \leq \mathrm{K}_{2n-4}(F).$$

Since $\mathrm{K}_{n+1}(F) = \{1\}$, we must have $2n - 4 < n + 1$ and so $n < 5$, as required. □

§124

The number of subgroups of given order in a metacyclic p-group

In this section we compute the number of subgroups of given order in a metacyclic p-group and also prove some structure results.

In the following lemma we gather some known results which we use in what follows.

Lemma J. *Let G be a nonabelian metacyclic p-group.*

(a) *Let G be of order p^4 and exponent p^2; then G is minimal nonabelian.*
   (i) *If $p = 2$, then $G \cong \mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^3 \rangle$, all subgroups of order 2 are characteristic in G, exactly one maximal cyclic subgroup of G has order 2.*
   (ii) *If $p > 2$, then $G = \langle a, b \mid a^{p^2} = b^{p^2} = 1,\ a^b = a^{1+p} \rangle$, all maximal cyclic subgroups of G have order p^2.*

(b) (Proposition 10.19) *If G has a nonabelian subgroup of order p^3, then it is of maximal class. In particular, if $p > 2$, then $|G| = p^3$.*

(c) *If $p = 2$ and $L \lhd G$ is such that G/L is nonabelian of order 8, then L is characteristic in G.*

(d) (Theorem 1.2 and Lemma 1.6) *There are four and only four series of nonabelian 2-groups with cyclic subgroup of index 2, namely D_{2^n}, Q_{2^n}, SD_{2^n}, M_{2^n}.*

(e) *$|\Omega_1(G)| \neq p^2$ if and only if G is a 2-group of maximal class.*

Let us prove Lemma J(a). There is in G a normal cyclic subgroup $A = \langle a \rangle$ such that G/A is cyclic; then we have $|A| = p^2$. If $B < G$ is cyclic and such that $AB = G$, then $|B| = p^2$; let $B = \langle b \rangle$. Since $|G : \mathrm{C}_G(A)| = p$ and the group of automorphisms of A is generated by the automorphism $a \to a^{1+p}$ of order p, one can write $a^b = a^{1+p}$ hence the group G has the same defining relations as in (a). Therefore, if $p > 2$, then G is regular, and (ii) follows easily.

Now let $p = 2$. The subgroup $G' = \langle a^2 \rangle$ is characteristic in G. Next, G has exactly three subgroups of order 2: $G' = \langle a^2 \rangle$, $U = \langle b^2 \rangle$ and $V = \langle a^2 b^2 \rangle$, and all these subgroups are central. Since $G/V \cong \mathrm{Q}_8$ and V is the unique subgroup of order 2 not contained in a cyclic subgroup of order 4, it follows that V is characteristic in G, and hence U is also characteristic in G.

Let us prove Lemma J(c). We have $\mho_2(G) \le L$. If $\mho_2(G) = L$, then it is nothing to prove. Now let $\mho_2(G) < L$. Then $|G : \mho_2(G)| = 2^4$, so $G/\mho_2(G)$ is nonabelian metacyclic of order 2^4 and exponent 4, and now the result follows from Lemma J(a).

In what follows we freely use the following fact: If G is a metacyclic p-group, then $\Omega_1(G) \cong \mathrm{E}_{p^2}$ unless G is either cyclic or a 2-group of maximal class.

1^o *Mann's theorem on the number of subgroups of given order in certain metacyclic p-groups.* Let G be a metacyclic group of order p^n and exponent p^e and let $f = n-e$; clearly, $f \le e$. We also write $e = e(G)$ and $f = f(G)$. This notation is applicable to subgroups and epimorphic images of G as well.

We begin with the following

Definition. A p-group G is said to be *quasi-regular* if it is metacyclic and

(QR1) if $p = 2$, then G has no nonabelian sections of order 8.

(QR2) if H is a section of G, then $\mho_1(H) = \{x^p \mid x \in H\}$, i.e., all elements of $\mho_1(H)$ are p-th powers.

A more general condition than (QR2) was considered by Mann (see §11) for all p-groups, where p is an arbitrary prime.

All metacyclic p-groups, $p > 2$, are quasi-regular (Theorem 7.2(c)). If G is a quasi-regular p-group, then $\exp(\Omega_m(G)) \le p^m$ for all positive integers m (this is proved by induction on $|G|$). The group $\mathcal{H}_2$ (see Lemma J(a)) is not quasi-regular since it has two nonabelian sections of order 8. The groups M_{2^n} are quasi-regular.

Exercise. Metacyclic quasi-regular p-groups G are powerful (see §26).

Solution. This is obvious for $p > 2$ (indeed, $G' \le \Phi(G) = \mho_1(G)$). Now let $p = 2$ and write $\bar{G} = G/\mho_2(G)$. We have to prove that $\bar{G}$ is abelian. Assume that this is false. We have $|\bar{G}| \in \{2^3, 2^4\}$. Then $|\bar{G}| \ne 2^3$ by (QR1). By Lemma J(a), there exists only one nonabelian metacyclic group of order 2^4 and exponent 4, namely $\mathcal{H}_2$. For this group we have $\bar{G}/\langle b^2\rangle \cong \mathrm{D}_8$ so $\bar{G}$ does not satisfy condition (QR1), which is a contradiction.

Let $\mathrm{s}_m(G)$ ($\mathrm{s}'_m(G)$, $\mathrm{c}_m(G)$) be the number of subgroups (noncyclic subgroups, cyclic subgroups) of order p^m in a p-group G. In what follows, c, e, f, m, n, t are positive integers.

The next theorem was inspired by Mann's letter to the first author at June 28, 2009.

Theorem 124.1 (Mann [M33] for $p > 2$; see also 5^o). *Let G be a quasi-regular metacyclic group of order p^n and exponent $p^e < p^n$, $m \le n$, and set $f(G) = f = n - e$. Then one of the following holds:*

(a) *If $m \le f$, then $\mathrm{s}_m(G) = \frac{p^{m+1}-1}{p-1}$.*

(b) *If $f < m \le e$, then $\mathrm{s}_m(G) = \frac{p^{f+1}-1}{p-1}$ so that $\mathrm{s}_m(G)$ is independent of m.*

(c) *If $m > e$, then $\mathrm{s}_m(G) = \frac{p^{n-m+1}-1}{p-1}$.*

As we know, this is the unique result presenting exact values for $s_m(G)$ for such a general class of p-groups.

Of course, Theorem 124.1 is not true for general metacyclic 2-groups as 2-groups of maximal class show.

We need the following

Lemma 124.2. *Suppose that G is a quasi-regular metacyclic group of order p^n and exponent p^e. Given a cyclic $A \le G$ of order p^e, there is a cyclic $B \le G$ such that $G = AB$ and $A \cap B = \{1\}$.*

Proof. We use induction on $|G|$. One may assume that the group G is nonabelian and $f = n - e > 1$ (otherwise, the result is either trivial for $n = e$ or follows from Introduction, Exercise 4, and Theorem 1.2). Then the subgroup $\mho_1(G)$ is noncyclic of exponent p^{e-1} by (QR2)). We have $|A \cap \mho_1(G)| = p^{e-1}$. Therefore, by induction, $\mho_1(G) = UV$, where $U = A \cap \mho_1(G)$, V is cyclic and $U \cap V = \{1\}$. It follows that $A \cap V = \{1\}$. Let $V = \langle v \rangle$. Then, by (QR2), there is $b \in G$ such that $v = b^p$. Set $B = \langle b \rangle$. Then $A \cap B = \{1\}$ and $G = AB$. (Clearly, $|B| = p^f$.) □

Note that for general abelian p-groups cyclic subgroups of maximal order are complemented (Introduction, Exercise 4). As Lemma 124.2 shows, this property also holds for quasi-regular metacyclic p-groups so for all metacyclic p-groups, $p > 2$. Generalized quaternion groups show that this is not true, in general, for $p = 2$. However, it is not true that if $p > 2$ and $A \lhd G$ is cyclic and such that G/A is cyclic, then A is complemented in G. Example: G is abelian of type (p, p^n), $n > 2$, and A is a cyclic subgroup of order p^2 not contained in $\Phi(G)$. Indeed, then G/A is cyclic, but A is not complemented in G (otherwise, we have $|\Omega_2(G)| = p^4$, a contradiction since, in fact, $|\Omega_2(G)| = p^3$).

Proof of Theorem 124.1. One may assume that $1 < m < n$.

If $f = 1$, then G is either abelian of type (p^e, p) or $G \cong M_{p^n}$ (see Theorem 1.2). In both these cases, we get $s_m(G) = p + 1$, and the same result is obtained from (a–c). In what follows we assume that $f > 1$; then G has no cyclic subgroup of index p.

By Lemma 124.2, $G = AB$, where $A, B < G$ are cyclic of orders p^e, p^f, respectively. Taking into account that G is quasi-regular and $f \le e$, we get

$$(*) \qquad |\Omega_k(G)| = p^{2k} (k \le f) \quad \text{and} \quad G/\Omega_f(G) \cong C_{p^{e-f}} = C_{p^{n-2f}}.$$

We have

$$s_m(G) = s'_m(G) + c_m(G). \tag{1}$$

If $H \le G$ is noncyclic, then $\Omega_1(G) \le H$ since $|\Omega_1(G)| = p^2 = |\Omega_1(H)|$ (Lemma J(e)), and so

$$s'_m(G) = s_{m-2}(G/\Omega_1(G)). \tag{2}$$

One can rewrite (1) as follows:

$$s_m(G) = s_{m-2}(G/\Omega_1(G)) + c_m(G). \tag{3}$$

(A) We first compute $c_m(G)$ for $m \le e$ (if $m > e$, then $c_m(G) = 0$). Since G is quasi-regular and $p^{m-1}(p-1) = \varphi(p^m)$ is the number of elements of order p^m in C_{p^m}, it follows that

$$c_m(G) = \frac{|\Omega_m(G) - \Omega_{m-1}(G)|}{p^{m-1}(p-1)}. \tag{4}$$

(i) Suppose that $m \le f$. Then we get $|\Omega_m(G)| = p^{2m}$, $|\Omega_{m-1}(G)| = p^{2m-2}$ so that, by (4),

$$c_m(G) = \frac{p^{2m} - p^{2m-2}}{p^{m-1}(p-1)} = p^{m-1}(p+1). \tag{5}$$

(ii) Suppose that $f < m \le e$. By $(*)$, we have

$$|\Omega_m(G)| = p^{2f+m-f} = p^{m+f} \quad \text{and} \quad |\Omega_{m-1}(G)| = p^{2f+m-1-f} = p^{m+f-1}.$$

Therefore, by (4),

$$c_m(G) = \frac{p^{m+f} - p^{m+f-1}}{p^{m-1}(p-1)} = p^f. \tag{6}$$

(B) In view of (3), it remains to compute $s_{m-2}(G/\Omega_1(G))$. Here we use induction on m. We have

$$\begin{aligned} p^{n_1} &= |G/\Omega_1(G)| = p^{n-2}, \\ e_1 &= e(G/\Omega_1(G)) = e-1, \\ f_1 &= f(G/\Omega_1(G)) = f-1 \end{aligned} \tag{7}$$

(for example, $f_1 = n_1 - e_1 = (n-2) - (e-1) = n - e - 1 = f - 1$).

(j) Let $m \le f$; then $m - 2 \le f - 2 < f - 1 = f_1 = f(G/\Omega_1(G))$. By induction (see part (a) of the statement),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{m-2+1} - 1}{p-1} = \frac{p^{m-1} - 1}{p-1}$$

so that, by (3) and (5), we get

$$s_m(G) = \frac{p^{m-1} - 1}{p-1} + p^{m-1}(p+1) = \frac{p^{m+1} - 1}{p-1},$$

completing this case.

(jj) Let $f < m \le e$; then

$$f_1 = f(G/\Omega_1(G)) = f - 1 \le m - 2 \le e - 2 < e - 1 = e(G/\Omega_1(G)) = e_1.$$

If $m - 2 = f - 1$ or, what is the same, $m - 1 = f$, then, by induction (see part (a)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{m-2+1} - 1}{p-1} = \frac{p^f - 1}{p-1}$$

so, by (3) and (6), we obtain

$$s_m(G) = p^f + \frac{p^f - 1}{p - 1} = \frac{p^{f+1} - 1}{p - 1},$$

as in (b), and we are done in this case.

Now let $m - 2 > f - 1$ or, what is the same, $m > f + 1$. Then, by induction (see part (b)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{f-1+1} - 1}{p - 1} = \frac{p^f - 1}{p - 1}$$

so, by (3) and (6), we have

$$s_m(G) = p^f + \frac{p^f - 1}{p - 1} = \frac{p^{f+1} - 1}{p - 1},$$

completing case (jj).

(jjj) Now let $m \geq e + 1$ or, what is the same, $m - 2 \geq e - 1 = e(G/\Omega_1(G)) = e_1$. Then $s_m(G) = s_{m-2}(G/\Omega_1(G))$ since all subgroups of G of order p^m are noncyclic hence contain $\Omega_1(G)$.

Let $m - 2 = e - 1 = e_1$, i.e., $e + 1 = m$; then, by induction (see part (b)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{(f-1)+1} - 1}{p - 1} = \frac{p^f - 1}{p - 1} = \frac{p^{n-e} - 1}{p - 1} = \frac{p^{n-m+1} - 1}{p - 1},$$

and this coincides with the formula in (c).

Now let $m - 2 > e - 1$, i.e., $m > e + 1$. Then, by induction (see part (c)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{(n-2)-(m-2)+1} - 1}{p - 1} = \frac{p^{n-m+1} - 1}{p - 1},$$

and this coincides with the formula in (c). Since all possibilities for m are considered, the proof is complete. □

Corollary 124.3 (Mann [M33] for $p > 2$). *If G and m, n, f, e are as in Theorem 124.1 (i.e., G is quasi-regular), then $s_m(G) = s_{n-m}(G)$.*

Proof. One may assume that G is noncyclic and $1 < m < n$.

(i) Let $m \leq f$; then $n - m \geq n - f = e$.

- If $n - m = e$, then $m = n - e = f$. We have, by Theorem 124.1(b,a),

$$s_{n-m}(G) = s_e(G) = \frac{p^{f+1} - 1}{p - 1} = \frac{p^{m+1} - 1}{p - 1} = s_m(G).$$

- If $n - m > e$, then $m < n - e = f$. We have, by Theorem 124.1(c,a),

$$s_{n-m}(G) = \frac{p^{n-(n-m)+1} - 1}{p - 1} = \frac{p^{m+1} - 1}{p - 1} = s_m(G).$$

(ii) Let $f < m \le e$; then $f = n - e \le n - m < n - f = e$.

- If $n - m = f$, then $m = n - f = e$. We have, by Theorem 124.1(a,b),

$$s_{n-m} = s_f(G) = \frac{p^{f+1} - 1}{p - 1} = s_e(G) = s_m(G).$$

- If $f < n - m < e$, then, by Theorem 124.1(b),

$$s_{n-m}(G) = \frac{p^{f+1} - 1}{p - 1} = s_m(G).$$

(iii) Let $m > e$, then $n - m < n - e = f$ so, by Theorem 124.1(a,c),

$$s_{n-m}(G) = \frac{p^{n-m+1} - 1}{p - 1} = s_m(G),$$

and the proof is complete. □

The group $G = \mathcal{H}_2$ with $n = 4$, $e = f = 2$ is not quasi-regular, however, $s_m(G)$ is such as in Theorem 124.1.

2° The number of cyclic subgroups of given order in a metacyclic 2-group. In this subsection we shall find the number of cyclic subgroups of given order in a metacyclic 2-group.

In this and the following subsections we suppose that G is a metacyclic group of order 2^n. Set

$$w = w(G) = \max\{i \mid |\Omega_i(G)| = 2^{2i}\} \quad \text{but} \quad |\Omega_{w+1}(G)| \ne 2^{2(w+2)}.$$

In this case, we write $R(G) = \Omega_w(G)$. Then we get $|R(G)| = 2^{2w}$ and $G/R(G)$ is either cyclic or a 2-group of maximal class (Lemma J(e)). We shall retain this notation in what follows.

If $w = 0$, then either G is cyclic or of maximal class (Lemma J(e)).

Part A of the following known theorem completes the case $w = 0$.

Theorem 124.4. *Suppose that G is a 2-group of maximal class and $n > 3$.*

A. *If $n > m > 2$, then $c_m(G) = 1$.*
   (a) *If $G \cong D_{2^n}$, then $c_1(G) = 2^{n-1} + 1$ and $c_2(G) = 1$.*
   (b) *If $G \cong Q_{2^n}$, then $c_1(G) = 1$, $c_2(G) = 2^{n-2} + 1$.*
   (c) *If $G \cong SD_{2^n}$, then $c_1(G) = 2^{n-2} + 1$ and $c_2(G) = 2^{n-3} + 1$.*

B. *We have $s_m(G) = 2^{n-m} + 1$ for $2 \le m < n$.*

If G is a group from Theorem 124.4, then its maximal subgroups are known (for example, if $G = SD_{2^{n+1}}$, then $\Gamma_1 = \{C, D, Q\}$, where C is cyclic, D is dihedral and Q is generalized quaternion). This allows us, using induction and Hall's enumeration principle, to prove that theorem.

In what follows $w = w(G)$ is a positive integer.

Theorem 124.5. *Suppose that G satisfies $R(G) = G$; then $|G| = 2^n = 2^{2w}$. In that case, we have $G = AB$, where $A \lhd G$ and B are cyclic of the same order 2^w and $\mathrm{c}_m(G) = 3 \cdot 2^{m-1}$ for all $m \in \{1, \dots, w\}$.*

Proof. Since G is metacyclic, there is a cyclic $A \lhd G$ such that G/A is cyclic. It follows from $\exp(G) = 2^w$ and $|A| \le 2^w$ that $|G : A| \le 2^w = \exp(G)$ whence $|A| = 2^w$. If $B < G$ is cyclic such that $AB = G$, then, since $\exp(G) = 2^w$, we get $|B| = 2^w$, $A \cap B = \{1\}$, and the first assertion of the theorem is proven.

Since $|\Omega_t(G)| = 2^{2t}$ for all nonnegative integers $t \le w$, we get

$$\mathrm{c}_m(G) = \frac{|\Omega_m(G) - \Omega_{m-1}(G)|}{2^{m-1}} = \frac{2^{2m} - 2^{2m-2}}{2^{m-1}} = 3 \cdot 2^{m-1},$$

completing the proof. □

In view of Theorem 124.5, we suppose in what follows that $(\Omega_w(G) =) R(G) < G$. By Theorem 124.5, if $m \le w$, then $\mathrm{c}_m(G) = 3 \cdot 2^{m-1}$. Therefore in the following two theorems we assume that $m > w$ and $R(G) < G$.

Theorem 124.6. *Suppose that $G/R(G)$ is nonidentity cyclic and $m > w$. Then we have $\mathrm{c}_m(G) = 2^w$.*

Proof. We obtain

$$|\Omega_m(G)| = 2^{2w+(m-w)} = 2^{w+m},$$
$$|\Omega_{m-1}(G)| = 2^{2w+(m-1-w)} = 2^{w+m-1}.$$

Therefore

$$\mathrm{c}_m(G) = \frac{|\Omega_m(G) - \Omega_{m-1}(G)|}{2^{m-1}} = \frac{2^{w+m} - 2^{w+m-1}}{2^{m-1}} = 2^w,$$

and the proof is complete. □

In what follows we assume that the quotient group $G/R(G)$ is of maximal class. If $L/R(G) < G/R(G)$ is cyclic of order 2^s, $s > 0$, then we infer that $\mathrm{c}_m(L) = 2^w$ by Theorem 124.6. In case that $L_1/R(G) < G/R(G)$ is another cyclic subgroup of order 2^s, we conclude that $L \cap L_1$ has no cyclic subgroups of order 2^{w+s}. If $L < G$ is cyclic of order $2^m > 2^w$, then, by the product formula, $LR(G)/R(G)$ is cyclic of order 2^{m-w} since $|L \cap R(G)| = 2^w$. Therefore we get

Theorem 124.7. *Suppose that $G/R(G)$ is a 2-group of maximal class and $m > w$. Then $\mathrm{c}_m(G) = 2^w \cdot \mathrm{c}_{m-w}(G/R(G))$.*

Since $\mathrm{c}_{m-w}(G/R(G))$ is known (Theorem 124.4.A), we have completed the computation of $\mathrm{c}_m(G)$ if $G/R(G)$ is of maximal class. Thus the number $\mathrm{c}_m(G)$ is computed for all metacyclic 2-groups.

3^o *The number of subgroups of given order in a metacyclic* 2*-group.* In this subsection we compute the number $s_m(G)$ of subgroups of order 2^m in G, where $G > \{1\}$ is a metacyclic 2-group. We first consider a metacyclic 2-group $G = R(G)(= \Omega_w(G))$ (see the second paragraph of 2^o) for which this problem is solved without difficulty (however, this is a key result as we shall see in the sequel). In what follows G is a metacyclic 2-group of order 2^n with $R(G) > \{1\}$ or, what is the same, $w \geq 1$ (see Theorem 124.4).

Theorem 124.8. *If G is a metacyclic 2-group such that $G = R(G)$, $w \geq 1$ (in this case, $|G| = 2^{2w}$) and $1 \leq m \leq 2w$, then one of the following holds:*

(a) *If $m \leq w$, then $s_m(G) = 2^{m+1} - 1$.*

(b) *If $1 \leq t \leq w$, then $s_{w+t}(G) = 2^{w-t+1} - 1$.*

Proof. It is easily checked that the theorem is true for $w = 1$ and $t = w$. Next we assume that $w > 1$ and $t < w$. As in the proof of Theorem 124.1, formulas (1), (2) and (3) hold. Therefore, in view of Theorem 124.5, it remains to find the number of noncyclic subgroups of order 2^m. If $H < G$ is noncyclic, then $\Omega_1(G) \leq H$ so the number of noncyclic subgroups of order 2^m in G is equal to $s_{m-2}(G/\Omega_1(G))$. We proceed by induction on w. Obviously, $R(G/\Omega_t(G)) = G/\Omega_t(G)$ for $t \leq w$.

(a) Suppose that $m \leq w$. In our case, we obtain that $w' = w(G/\Omega_1(G)) = w - 1$, $|G/\Omega_1(G)| = 2^{2w-2}$. We have $m - 2 < w - 1 = w'$. Let $H < G$ be of order 2^m. If H is noncyclic, then the number of such H is G is equal to

$$s_{m-2}(G/\Omega_1(G)) = 2^{(m-2)+1} - 1 = 2^{m-1} - 1$$

by induction (see the previous paragraph). If $H < G$ is cyclic, then the number of such H is equal to $c_m(\Omega_m(G)) = 3 \cdot 2^{2m-1}$ (Theorem 124.5) so, by (3), we obtain

$$s_m(G) = 3 \cdot 2^{m-1} + (2^{m-1} - 1) = 2^{m+1} - 1,$$

completing the proof of (a).

(b) In what follows we assume that $m = w+t$, where $1 \leq t < m$. As $\exp(G) = 2^w$, we obtain that $\exp(G/\Omega_t(G)) = 2^{w-t}$. If $H \leq G$ is of order 2^{w+t}, then $\Omega_t(G) < H$ and $|H/\Omega_t(G)| = 2^{w-t}$, and so $s_{w+t}(G) = s_{w-t}(G/\Omega_t(G))$. As we know, we have $R(G/\Omega_t(G)) = G/\Omega_t(G)$; therefore, using the formula from the previous sentence and (a) for $G/\Omega_t(G)$, we get

$$s_{w+t}(G) = s_{w-t}(G/\Omega_t(G)) = 2^{w-t+1} - 1$$

by induction, and the proof is complete. □

It is easy to show that the groups from Theorem 124.8 coincide with metacyclic 2-groups G of order 2^{2w} and exponent 2^w. Indeed, if G is such a group, then $\Omega_1(G)$ is abelian of type $(2, 2)$ by Lemma J(e), and now, by induction, $|\Omega_i(G/\Omega_1(G))| = 2^{2i}$ for all $i \leq m - 1$, and our claim follows.

It follows that the number $s_m(G)$ from Theorem 124.8 is computed by the same formulas as in Theorem 124.1. The group $\mathcal{H}_2$ is a group from Theorem 124.8 but not from Theorem 124.1.

Note that a group $G = AB$ from Theorem 124.8 has a noncyclic center. This is the case if one of the subgroups A, B, say A, is normal in G since $\Omega_1(A) \le Z(G)$ and, in view of $|\mathrm{Aut}(A)| = 2^{m-1}$, $\Omega_1(B)$ centralizes A so contained in $Z(G)$. Now suppose that A and B are not normal in G. Then there exists $x \in G - N_G(A)$ such that $A^x \ne A$. By Ore (see Lemma A.28.8), $AA^x \ne G$ so $A \cap A^x \ge \Omega_1(A) > \{1\}$ for all $x \in G$ by the product formula. It follows that $A_G = \bigcap_{x \in G} A^x > \{1\}$ so $Z(G) \ge \Omega_1(A) > \{1\}$. Similarly, $Z(G) \ge \Omega_1(B) > \{1\}$, and our claim follows since $\Omega_1(A) \times \Omega_1(B) \le Z(G)$ is noncyclic.

Suppose that a metacyclic 2-group G is such that $G/R(G)$ is nonidentity cyclic and $R(G) > \{1\}$. We claim that in this case $G = AB$, where $A, B < G$ are cyclic and $A \cap B = \{1\}$. Indeed, suppose that $\exp(G) = 2^e$ and, as above, $\exp(R(G)) = p^w$; then $w < e$. Let $A < G$ be cyclic of order 2^e; then $A \cap R(G)$ is cyclic of order 2^w. By Theorem 124.5, $R(G) = (A \cap R(G))B$, where $B < R(G)$ is cyclic of order 2^w and $(A \cap R(G)) \cap B = \{1\}$. It follows that $A \cap B = \{1\}$, so $AB = G$ by the product formula.

Let $\Gamma_1 = \{A, B, C\}$ be the set of all maximal subgroups of a noncyclic metacyclic 2-group G. Then, supposing $2^m < |G|$, we have, by Hall's enumeration principle,

$$s_m(G) = s_m(A) + s_m(B) + s_m(C) - 2s_m(\Phi(G)). \tag{8}$$

We may assume that G has no cyclic subgroup of index 2 (see Theorem 124.4). In case $2^{m+2} = |G| = 2^n$, we get

$$s_m(G) = s_{n-2}(G) = 3 \cdot 3 - 2 \cdot 1 = 7 = 2^2 + 3$$

by (8). We shall freely use this fact in what follows. Next we retain the notation introduced in this paragraph.

Now we compute $s_m(G)$ for the case where $G/R(G)$ is nonidentity cyclic. The following lemmas will help us to state the inductive hypothesis. If $m \le w$, then we have $s_m(G) = s_m(R(G))$, and this number is computed in Theorem 124.8(a). Therefore in what follows we consider case $m > w$ only.

Lemma 124.9. *Suppose that G is a metacyclic 2-group that satisfies $|G/R(G)| = 2$. If $1 \le t \le w + 1$, then $s_{w+t}(G) = 2^{w-t+2} - 1$.*

Proof. If $t = w + 1$, then $w + t = 2w + 1 = n$, where $2^n = |G|$; then

$$1 = s_{w+t}(G) = s_n(G) = 1 = 2^{w-(w+1)+2} - 1,$$

as in the statement.

Next we assume that $t < w + 1$. We have $\exp(G) = 2^{w+1}$. If $w = 1$, then $t = 1$, G is abelian of type $(4, 2)$, and so $s_{w+t}(G) = s_2(G) = 3 = 2^2 - 1 = 2^{1-1+2} - 1$, as in statement. Therefore one may also assume that $w > 1$.

In view of Theorem 124.8(b), $s_{w+t}(R(G)) = 2^{w-t+1} - 1$ so it suffices to find the number of subgroups $H < G$ of order 2^{w+t} such that $H \not\leq R(G)$. Let H be such a subgroup; then $\exp(H) = 2^{w+1} = \exp(G)$.

If H is cyclic, then $m = w + 1$ so $t = 1$, hence the number of such H is equal to $c_{w+1}(G) = 2^w$ (Theorem 124.6), and we get

$$\begin{aligned} s_{w+1}(G) &= s_{w+1}(R(G)) + c_{w+1}(G) \\ &= (2^{w-1+1} - 1) + 2^w = 2^{w+1} - 1, \end{aligned}$$

completing this case.

Next we assume that $|H| = 2^{(w+1)+t}$, where $0 < t < w$. In this case, H is non-cyclic and $\Omega_t(G) < H$. Suppose that $H \not\leq R(G)$. Since $\exp(H) = 2^{w+1} = \exp(G)$, it follows that $H/\Omega_t(G)$ is of order $2^{w+t+1-2t} = 2^{w-t+1}$ and exponent 2^{w-t+1}, and we conclude that $H/\Omega_t(G)$ is cyclic. We have $w(G/\Omega_t(G)) = w - t$. Therefore the number of such H is equal to $c_{w-t+1}(G/\Omega_t(G)) = 2^{w-t}$ (Theorem 124.6). Since $s_{w+1+t}(R(G)) = 2^{w-(t+1)+1} - 1 = 2^{w-t} - 1$ (Theorem 124.8), we obtain

$$s_{w+t+1}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing $t+1$ by t in the last equality, we get $s_{w+t}(G) = 2^{w-t+2} - 1$, as required. □

Lemma 124.10. *Suppose that a metacyclic 2-group G is such that $G/R(G)$ is cyclic of order 4.*

(a) *We have* $s_{w+1}(G) = 2^{w+1} - 1$.

(b) *If* $2 \leq t \leq m$, *then* $s_{w+t}(G) = 2^{w-t+3} - 1$.

Proof. (a) Since $|\Omega_{w+1}(G)/R(G)| = 2$, we have, by Lemma 124.9,

$$s_{w+1}(G) = s_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1,$$

and (a) is proven.

(b) If $t = w + 2$, then $2^{w+t} = |G|$ so

$$s_{w+(w+2)}(G) = 1 = 2^{w-(w+2)+3} - 1,$$

as in the statement.

In what follows we assume that $t < w + 2$. If $w = 1$, then $|G| = 2^4$ has a cyclic subgroup of index 2, $t = 2$ (by hypothesis),

$$s_{1+t}(G) = s_3(G) = 3 = 2^2 - 1 = 2^{1-2+3} - 1,$$

and this coincides with the required result. In the sequel we assume that $w > 1$.

Set $U = \Omega_{w+1}(G)$; then $|U : R(G)| = 2 = |G : U|$. As $s_{w+t}(U) = 2^{w-t+2} - 1$ (Lemma 124.9), it suffices to compute the number of $H < G$ of order 2^{w+t} such that $H \not\leq U$. Let H be such a subgroup. Then $\exp(H) = 2^{w+2} = \exp(G)$. If H is cyclic, then $|H| = 2^{w+2}$ (this holds if and only if $t = 2$), and so the number of such H in G

is equal to $c_{w+2}(G) = 2^w$ (Theorem 124.6), and we get

$$\begin{aligned} s_{w+2}(G) &= c_{w+2}(G) + s_{w+2}(U) \\ &= 2^w + (2^{w-2+2} - 1) = 2^{w+1} - 1 \\ &= 2^{w-2+3} - 1, \end{aligned}$$

and this coincides with the required result for $t = 2$. (Note that if $t = 2$ and $H \not\leq U$, then H is cyclic.)

Now we suppose that $|H| = 2^{(w+2)+t}$, where $0 < t < w$. In this case, H is noncyclic of exponent $2^{w+2} = \exp(G)$, $\Omega_t(G) < H$ and $H/\Omega_t(G)$ is cyclic of order $2^{w+t+2-2t} = 2^{w-t+2}$ (cyclic since $|H/\Omega_t(G)| = 2^{w-t+2} = \exp(H/\Omega_t(G))$. As $\exp(R(G/\Omega_t(G)) = 2^{w-t}$, the number of such H equals $c_{w-t+2}(G/\Omega_t(G)) = 2^{w-t}$ (Theorem 124.6). Since $s_{w+t+2}(U) = 2^{w-(t+2)+2} - 1 = 2^{w-t} - 1$ (Lemma 124.9), we get

$$s_{w+t+2}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing in the last equality $t + 2$ by t, we get $s_{w+t}(G) = 2^{w-t+3} - 1$, completing the proof. □

Lemma 124.11. *Suppose that G is a metacyclic 2-group such that $G/R(G)$ is cyclic of order 2^3, $w > 0$.*

(a) *If $t = 1$, then $s_{w+1}(G) = 2^{w+1} - 1$.*

(b) *If $t = 2$, then $s_{w+2}(G) = 2^{w+1} - 1$.*

(c) *If $3 \leq t < w + 3$, then $s_{w+t}(G) = 2^{w-t+4} - 1$.*

Proof. Statements (a) and (b) follow from Lemmas 124.9 and 124.10, respectively. Indeed, let $t = 1$. Then

$$s_{w+1}(G) = s_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1 \quad \text{(Lemma 124.9)}.$$

Now let $t = 2$. Then

$$s_{w+2}(G) = s_{w+2}(\Omega_{w+2}(G)) = 2^{w-2+3} - 1 = 2^{w+1} - 1 \quad \text{(Lemma 124.10)}.$$

(c) One may assume that $t < w + 3$. If $w = 1$, then $t = 3$, by hypothesis, G has a cyclic subgroup of index 2 so $s_{1+3}(G) = 3 = 2^{1-3+4}-1$. Next we assume that $w > 1$. Set $U = \Omega_{t+2}(G)$.

Let $H < G$ be of order 2^{w+3}. Since $s_{w+3}(U) = 2^{w-3+3} - 1 = 2^w - 1$ (Lemma 124.10), it suffices to count the number of those subgroups H that are not contained in U. In this case, we get $\exp(H) = 2^{w+3}$ so H is cyclic. Then the number of such H is equal to $c_{w+3}(G) = 2^w$ (Theorem 124.6). We get

$$s_{w+3}(G) = 2^w + (2^w - 1) = 2^{w+1} - 1 = 2^{w-3+4} - 1,$$

and this coincides with the required result for $t = 3$.

Suppose that $|H| = 2^{w+3+t}$, where $0 < t < w$, and $H < G$, $H \not\leq U$. Then we conclude that $\Omega_t(G) < H$, $H/\Omega_t(G)$ is cyclic of order 2^{w-t+3}. The number of such H is equal to $c_{w-t+3}(G/\Omega_t(G)) = 2^{w-t}$ since $\exp(R(G/\Omega_t(G))) = 2^{w-t}$ (Theorem 124.6). All such H are not contained in U as $\exp(H) = 2^{w+3} > 2^{w+2} = \exp(U)$. Since $s_{w+3+t}(U) = 2^{w-(t+3)+3} - 1 = 2^{w-t} - 1$ (Lemma 124.10), we get

$$s_{w+3+t}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing in the last equality $t + 3$ by t, we get $s_{w+t}(G) = 2^{w-t+4} - 1$, completing the proof. □

The proofs of the previous three lemmas are similar. Our goal there was to state inductive hypothesis and show as to attain this. In any case, Lemma 124.9 must be proved (it is the basis of induction). Now we are ready to prove the following

Theorem 124.12. *Suppose that G is a metacyclic 2-group of order 2^n such that $w > 1$ and $G/R(G)$ is cyclic of order 2^c (in this case, $n = 2w + c$).*[1]

(a) *If $1 \leq t < c$, then $s_{w+t}(G) = 2^{w+1} - 1$.*

(b) *If $c \leq t \leq w + c$, then $s_{w+t}(G) = 2^{w-t+c+1} - 1$.*

Proof. We proceed by induction on c. As in previous three lemmas, one may assume that $t < w + c$.

(i) First we consider case $t \geq c$.

Since $w > 0$, G is noncyclic. Set $U = \Omega_{w+c-1}(G)$; then $\exp(U) = 2^{w+c-1} = \frac{1}{2}\exp(G)$, $|G : U| = 2$ and $U/R(U) = UR(G)/R(G)$ is cyclic of order $2^{c-1} > 1$.

The theorem holds for $c = 1, 2, 3$ (Lemmas 124.9–124.11) so one may assume that $c > 3$. We have $\exp(G) = 2^{w+c}$. By induction,

$$s_{w+t}(U) = 2^{w-t+(c-1)+1} - 1 = 2^{w-t+c} - 1$$

since $t > c - 1 = \log_2(|UR(G)/R(G)|)$. Therefore it suffices to find the number of those $H < G$ of order 2^{w+t} that are not contained in U. All such subgroups have the same exponent $2^{w+c} = \exp(G)$. If such an H is cyclic, then $|H| = 2^{w+c}$ (this holds if and only if $t = c$), and the number of such H in G is equal to $c_{w+c}(G) = 2^w$ (Theorem 124.6). Therefore we obtain

$$s_{w+c}(G) = c_{w+c}(G) + s_{w+c}(U) = 2^w + (2^{w-c+c} - 1) = 2^{w+1} - 1,$$

and this coincides with the required result for $t = c$.

Next we assume that $|H| = 2^{w+c+t}$, where $0 < t < w$. Then $\Omega_t(G) < H$ and $H/\Omega_t(G)$ is of order $2^{w+c+t-2t} = 2^{w-t+c} = \exp(H/\Omega_t(G))$ whence $H/\Omega_t(G)$ is cyclic. We have $s_{w+c+t}(U) = 2^{w-(c+t)+(c-1)+1} - 1 = 2^{w-t} - 1$ by induction.

[1] If $w = 1$, then the number of proper subgroups of given order in G is equal to $2^2 - 1$ since G has a cyclic subgroup of index 2 and $\mathrm{cl}(G) \leq 2$.

Since $R(G/\Omega_t(G)) = R(G)/\Omega_t(G)$ and $\exp(R(G/\Omega_t(G))) = 2^{w-t}$, the number of such H equals $c_{w-t+c}(G/\Omega_t(G)) = 2^{w-t}$ (Theorem 124.6). Therefore

$$s_{w+c+t}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing in the displayed formula $t + c$ by t, we get $s_{w+t} = 2^{w-t+c+1} - 1$, and the proof of (b) is complete.

(ii) It remains to prove (a); then $t < c$. In this case, $H < V = \Omega_{w+t}(G)$.

The subgroup $V/R(G)$ is cyclic of order 2^t. By part (b), applied to V, we obtain that $s_{w+t}(V) = 2^{w-t+t+1} - 1 = 2^{w+1} - 1$. Since $s_{w+t}(G) = s_{w+t}(V)$, the proof of (a) is complete. □

To complete the computation of the value $s_m(G)$, it remains to consider the case where $G/R(G)$ is a 2-group of maximal class and order 2^c. Note that the factor group $G/R(G)$ contains a cyclic subgroup of index 2 (Theorem 1.2). In the notation of (8) (namely, $\Gamma_1 = \{A, B, C\}$ is the set of maximal subgroups of G) we assume in the sequel that $C/R(G)$ is cyclic. These three cases will be covered in Theorems 124.16, 124.18 and 124.19 and in the supplements to them. In those theorems we consider the case $w > 1, t \geq c-1$. In the supplements we consider the cases $w = 1$ and $t = 1$ separately. In the case under consideration, $R(G) < \Phi(G)$ as $d(G/R(G)) = 2 = d(G)$.

The following two lemmas are the bases of induction for Theorems 124.16 and 124.18, respectively.

Lemma 124.13. *Suppose that G is a metacyclic 2-group such that $G/R(G) \cong Q_8$ and $w + t > w > 1$, $t \leq w + 3$.*

(a) *If $t = 1$, then $s_{w+1}(G) = 2^{w+1} - 1$.*

(b) *If $2 \leq t \leq w + 3$, then $s_{w+t}(G) = 2^{w-t+4} - 1$.*

Proof. If $t = w + 3$, then we have $w + t = n$, where $2^n = |G|$, so we obtain that $s_{w+t}(G) = 1 = 2^{w-(w+3)+4} - 1$, as in (b). If $t = w + 2$, then $w + t = n - 1$ so

$$s_{w+t}(G) = 3 = 2^2 - 1 = 2^{w-(w+2)+4} - 1,$$

as in (b). In what follows we assume that $t < w + 2$.

We have $R(A) = R(B) = R(C) = R(\Phi(G)) = R(G)$ and the quotient groups $A/R(G)$, $B/R(G)$ and $C/R(G)$ are cyclic of order 4, $|\Phi(G)/R(\Phi(G)| = 2$.

If $t = 1$, then, by Lemma 124.9,

$$s_{w+1}(G) = s(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1,$$

and the proof of (a) is complete.

Now let $t > 1$. Then

$$s_{w+t}(A) = s_{w+t}(B) = s_{w+t}(C) = 2^{w-t+3} - 1 \quad \text{(Lemma 124.10)},$$

$$s_{w+t}(\Phi(G)) = 2^{w-t+2} - 1 \quad \text{(Lemma 124.9)}$$

so, by (8),

$$\mathrm{s}_{w+t}(G) = 3 \cdot (2^{w-t+3} - 1) - 2 \cdot (2^{w-t+2} - 1) = 2^{w-t+4} - 1,$$

and the proof is complete. □

Lemma 124.14. *Suppose that G is a metacyclic 2-group such that $G/R(G) \cong \mathrm{D}_8$ and $w + t > w > 1$, $1 \leq t \leq w + 3$.*

(a) *If $t = 1$, then $\mathrm{s}_{w+1}(G) = 2^{w+3} - 2^{w+1} - 1 = 3 \cdot 2^{w+1} - 1$.*

(b) *If $t > 1$, then $\mathrm{s}_{w+t}(G) = 2^{w-t+4} - 1$.*

Proof. In the notation of identity (8), we have $R(A) = A$, $R(B) = B$ so we obtain $w(A) = w(B) = w + 1$, $R(C) = R(\Phi(G)) = R(G)$ so $w(C) = w(\Phi(G)) = w$. In case $t = w + 3$, we get $w + t = n$, and, as in the previous lemma, we infer that $\mathrm{s}_{w+t}(G) = 1 = 2^{w-(w+3)+4} - 1$, as in (b). If $t = w + 2$, then

$$\mathrm{s}_{w+t}(G) = 3 = 2^2 - 1 = 2^{w-(w+2)+4} - 1,$$

as in (b). Next we assume that $t < w + 2$.

For $t = 1$, we have

$$\begin{aligned}
\mathrm{s}_{w+1}(A) = \mathrm{s}_{w+1}(B) &= 2^{(w+1)+1} - 1 = 2^{w+2} - 1 && \text{(Theorem 124.8(a)),}\\
\mathrm{s}_{w+1}(C) &= \mathrm{s}_{w+1}(\Omega_{w+1}(C)) = \mathrm{s}_{w+1}(\Phi(G))\\
&= 2^{w-1+2} - 1 = 2^{w+1} - 1 && \text{(Lemma 124.9)}
\end{aligned}$$

so that, by (8),

$$\begin{aligned}
\mathrm{s}_{w+1}(G) &= 2 \cdot (2^{w+2} - 1) + (2^{w+1} - 1) - 2(2^{w+1} - 1)\\
&= 2^{w+3} - 2^{w+1} - 1 = 3 \cdot 2^{w+1} - 1,
\end{aligned}$$

as in (a).

If $t > 1$, then $w + t = (w + 1) + (t - 1)$ so that

$$\begin{aligned}
\mathrm{s}_{w+t}(A) = \mathrm{s}_{w+t}(B) &= 2^{(w+1)-(t-1)+1} - 1\\
&= 2^{w-t+3} - 1 && \text{(Theorem 124.8(b)),}\\
\mathrm{s}_{w+t}(C) &= 2^{w-t+3} - 1 && \text{(Lemma 124.10),}\\
\mathrm{s}_{w+t}(\Phi(G)) &= 2^{w-t+2} - 1 && \text{(Lemma 124.9)}
\end{aligned}$$

so that, by (8),

$$\mathrm{s}_{w+t}(G) = 3(2^{w-t+3} - 1) - 2(2^{w-t+2} - 1) = 2^{w-t+4} - 1,$$

completing the proof. □

Lemma 124.15. *Let G be a metacyclic 2-group of order 2^n such that $G/R(G) \cong \mathrm{Q}_{2^4}$, $w > 1$ and $1 \le t \le w + 4$. Then*

(a) $\mathrm{s}_{w+1}(G) = 2^{w+1} - 1$.

(b) *If $2 \le t \le w + 4$, then* $\mathrm{s}_{w+t}(G) = 2^{w-t+5} - 1$.

Proof. If $t = w + 4$, then

$$\mathrm{s}_{w+(w+4)}(G) = \mathrm{s}_n(G) = 1 = 2^{w-(w+4)+5} - 1,$$

as in (b). In case $t = w + 3$, we get

$$\mathrm{s}_{w+(w+3)}(G) = 3 = 2^2 - 1 = 2^{w-(w+3)+5} - 1,$$

as in (b). If $t = 1$, then, by Lemma 124.9,

$$\mathrm{s}_{w+1}(G) = \mathrm{s}_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1,$$

as in (a).

We have $w(M) = w$ for $M \in \{A, B, C, \Phi(G)\}$.

Now let $t = 2$. Then

$$\begin{aligned} \mathrm{s}_{w+2}(A) = \mathrm{s}_{w+2}(B) &= 2^{w-2+4} - 1 = 2^{w+2} - 1 && \text{(Lemma 124.13)}, \\ \mathrm{s}_{w+2}(C) &= 2^{w-2+4} - 1 = 2^{w+2} - 1 && \text{(Lemma 124.11)}, \\ \mathrm{s}_{w+2}(\Phi(G)) &= 2^{w-2+3} - 1 = 2^{w+1} - 1 && \text{(Lemma 124.10)}. \end{aligned}$$

Therefore, by (8), we get

$$\mathrm{s}_{w+2}(G) = 3(2^{w+2} - 1) - 2(2^{w+1} - 1) = 2^{w+3} - 1 = 2^{w-2+5} - 1,$$

as in (b).

Next we assume that $2 < t < w + 3$. By Lemma 124.13, Theorem 124.12 and identity (8),

$$\begin{aligned} \mathrm{s}_{w+t}(G) &= 2(2^{w-t+4} - 1) + (2^{w-t+4} - 1) - 2(2^{w-t+3} - 1) \\ &= 2^{w-t+5} - 1, \end{aligned}$$

and the proof is complete. □

Now we are ready to prove the following

Theorem 124.16. *Suppose that G is a metacyclic 2-group such that $G/R(G) \cong \mathrm{Q}_{2^c}$ and $w + t > w > 1$, $c - 1 \le t \le w + c$. Then* $\mathrm{s}_{w+t}(G) = 2^{w-t+c+1} - 1$.

Proof. We proceed by induction on c. The statement of the theorem is true for $c = 3, 4$ (Lemmas 124.13, 124.15) and $t \in \{w + c - 1, w + c\}$ (direct checking; see Lemma 124.15). Next assume that $c > 4$ and $t < w + c - 1$. As in Lemma 124.15, we

have $w(M) = w$ for $M \in \{A, B, C, \Phi(G)\}$. We obtain

$$A/R(G) \cong \mathrm{Q}_{2^{c-1}} \cong B/R(G), \quad C/R(G) \cong \mathrm{C}_{2^{c-1}}, \quad \Phi(G)/R(G) \cong \mathrm{C}_{2^{c-2}}.$$

Then, by induction,

$$\mathrm{s}_{w+t}(A) = \mathrm{s}_{w+t}(B) = 2^{w-t+c} - 1.$$

By Theorem 124.12,

$$\mathrm{s}_{w+t}(C) = 2^{w-t+c} - 1, \quad \mathrm{s}_{w+t}(\Phi(G)) = 2^{w-t+c-1} - 1.$$

Therefore, by (8), we obtain

$$\mathrm{s}_{w+t}(G) = 3(2^{w-t+c} - 1) - 2(2^{w-t+c-1} - 1) = 2^{w-t+c+1} - 1,$$

and the proof is complete. □

There is no problem to compute $\mathrm{s}_{w+t}(G)$ for $t < c - 1$. Our method works also in this case.

Now suppose that $w = 1$ and $G/R(G)$ is of maximal class and order 2^c. Taking into account that C and $\Phi(G)$ have cyclic subgroups of index 2, $\mathrm{cl}(C) \leq 2$ and $\Phi(G)$ is abelian (indeed, $\mathrm{C}_G(R(G)) \geq \Phi(G)$), we obtain $\mathrm{s}_{1+t}(C) = \mathrm{s}_{1+t}(\Phi(G)) = 3$. Therefore, by (8), we get

$$\mathrm{s}_{1+t}(G) = \mathrm{s}_{1+t}(A) + \mathrm{s}_{1+t}(B) + 3 - 2 \cdot 3 = \mathrm{s}_{1+t}(A) + \mathrm{s}_{1+t}(B) - 3. \tag{9}$$

Supplement 1 to Theorem 124.16. *Let $G/R(G) \cong \mathrm{Q}_{2^c}$, $w = 1$, $|G| = 2^n = 2^{2+c}$, $1 \leq t < c$. Then*

(a) $\mathrm{s}_2(G) = 3$ *(in that case, $t = 1$).*

(b) *If $1 < t < c$, then $\mathrm{s}_{1+t}(G) = 2^{1-t+c} + 3$.*

Proof. One may assume that $1 + t < n - 2 (= c)$ (we have $\mathrm{s}_{n-2}(G) = 2^2 + 3 = 2^{1-t+c} + 3$, where $t = n - 3$ and $c = n - 2$; see the displayed formula following (8)). If $t = 1$, then $\mathrm{s}_{1+1}(G) = \mathrm{s}_2(\Omega_2(G)) = \mathrm{s}_2(\Phi(G)) = 3$ since $\Omega_2(G) (\leq \Phi(G))$ is abelian of type $(4, 2)$ and $\Phi(G)$ has a cyclic subgroup of index 2. Next we also assume that $t > 1$. By the same displayed formula following (8), if $c = 3$ and $t = 2$, then we get $\mathrm{s}_3(G) = 2^2 + 3 = 2^{1-2+3} + 3$.

If $c = 4$, then $t = 2$ (by assumption, $1 < t < n - 3 = c - 1$) so, by (9) and the previous paragraph,

$$\mathrm{s}_{1+2}(G) = 2(2^2 + 3) - 3 = 2^3 + 3 = 2^{1-2+4} + 3,$$

as in (b).

In case $c = 5$, we get $t \in \{2, 3\}$ so, by (9),

$$\mathrm{s}_{1+2}(G) = 2(2^3 + 3) - 3 = 2^4 + 3 = 2^{1-2+5} + 3 \quad \text{(by the previous paragraph)},$$

$$\mathrm{s}_{1+3}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-3+5} + 3 \quad \text{(by the first paragraph)}.$$

If $c = 6$, then $t \in \{2, 3, 4\}$. We have, by (9) and the previous paragraphs,

$$\mathrm{s}_{1+2}(G) = 2(2^4 + 3) - 3 = 2^5 + 3 = 2^{1-2+6} + 3,$$
$$\mathrm{s}_{1+3}(G) = 2(2^3 + 3) - 3 = 2^4 + 3 = 2^{1-3+6} + 3,$$
$$\mathrm{s}_{1+4}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-4+6} + 3.$$

Now let $|G/R(G)| = 2^c$, where $t \in \{2, \dots, c-1\}$, $c > 3$. We claim that $\mathrm{s}_{1+t}(G) = 2^{1-t+c}+3$. We prove this by induction on c. By the above, this is true for $c = 3, 4, 5, 6$ so one may assume that $c > 6$. Applying induction and (9), we obtain

$$\mathrm{s}_{1+t}(G) = 2(2^{1-t+c-1} + 3) - 3 = 2^{1-t+c} + 3,$$

and we are done. □

We see that the cases $w = 1$ and $w > 1$ are essentially different.

Supplement 2 to Theorem 124.16. *Let $G/R(G) \cong \mathrm{Q}_{2^c}$, $w > 1$ and $t = 1$. Then we have $\mathrm{s}_{w+1}(G) = 2^{w+1} - 1$.*

Proof. For arbitrary $c \geq 3$ we have, by Lemma 124.9,

$$\mathrm{s}_{w+1}(G) = \mathrm{s}_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1,$$

as required. □

Lemma 124.17. *Suppose that G is a metacyclic 2-group such that $G/R(G) \cong \mathrm{D}_{2^4}$, $w + t > w > 1$ and $1 < t < w + 3$. Then $\mathrm{s}_{w+t}(G) = 2^{w-t+5} - 1 = 2^{w-t+(4+1)} - 1$.*

Proof. It follows from the structure of the maximal subgroups of G that $w(M) = w$ for $M \in \{A, B, C, \Phi(G)\}$. By Lemmas 124.14, 124.12 and (8), we have

$$\mathrm{s}_{w+t}(G) = 2(2^{w-t+4} - 1) + (2^{w-t+4} - 1) - 2(2^{w-t+3} - 1) = 2^{w-t+5} - 1,$$

and we are done. □

Now we are ready to prove the following

Theorem 124.18. *Suppose that G is a metacyclic 2-group such that $G/R(G) \cong \mathrm{D}_{2^c}$, $w + t > w > 1$, $c - 1 \leq t < w + c - 1$. Then $\mathrm{s}_{w+t}(G) = 2^{w-t+c+1} - 1$.*

Proof. We proceed by induction on c. The theorem holds for $c = 3, 4$ (Lemmas 124.14 and 124.17) so one may assume that $c > 4$. As above, we have $w(M) = w$ for each $M \in \{A, B, C, \Phi(G)\}$. By induction, Theorem 124.12 and (8), we obtain

$$\begin{aligned}\mathrm{s}_{w+t}(G) &= 2(2^{w-t+c} - 1) + (2^{w-t+c} - 1) - 2(2^{w-t+c-1} - 1)\\ &= 2^{w-t+c+1} - 1,\end{aligned}$$

completing the proof. □

Now we consider the case $G/R(G) \cong \mathrm{D}_{2^c}$, $w = 1$. As above, $|G| = 2^n$.

Supplement 1 to Theorem 124.18. *Suppose that $G/R(G) \cong \mathrm{D}_{2^c}$, $w = 1$ (in this case, $n = c + 2$) and $1 \le t < c$. Then we have $\mathrm{s}_{1+t}(G) = 2^{1-t+c} + 3$. (If $t = c$, then $\mathrm{s}_{1+c}(G) = |\Gamma_1| = 3$.)*

Proof. By the paragraph containing (8), $\mathrm{s}_{n-2}(G) = 2^2 + 3 = 2^{1-(n-3)+n-2} + 3$ (here $t = n - 3$ and $c = n - 2$), as in the statement. Therefore one may assume in the sequel that $t < n - 3 = (c + 2) - 3 = c - 1$.

Let $t = 1$. If $H < G$ is of order 4 and $H \ne R(G)$, then $HR(G)$ of order 8 contains exactly two $\ne R(G)$ subgroups of order 4 since $HR(G)$ is abelian of type $(2^2, 2)$ by Lemma J(b). Since $\mathrm{s}_1(G/R(G)) = 2^{c-1} + 1$, we get

$$\mathrm{s}_{1+1}(G) = 1 + 2(2^{c-1} + 1) = 2^c + 3 = 2^{1-1+c} + 3,$$

as in the statement. In what follows we assume that $t > 1$; then $c > 3$.

Let $c = 4$. Then $t = 2$. Using (9), we obtain

$$\mathrm{s}_{1+2}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-2+4} + 3$$

by the displayed formula following (8).

Let $c = 5$. Then $t \in \{2, 3\}$ and

$$\mathrm{s}_{1+2}(G) = 2(2^3 + 3) - 3 = 2^4 + 3 = 2^{1-2+5} + 3,$$
$$\mathrm{s}_{1+3}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-3+5} + 3$$

(the first equality follows from the previous paragraph and the second one follows from the displayed formula following (8)).

Now we will prove by induction on c that $\mathrm{s}_{1+t}(G) = 2^{1-t+c} + 3$. This is true for $c = 3, 4, 5$ and $t = 1$. By induction, Theorem 124.12 and (9), we get

$$\mathrm{s}_{1+t}(G) = 2(2^{1-t+c-1} + 3) - 3 = 2^{1-t+c} + 3,$$

as required. □

Supplement 2 to Theorem 124.18. *Suppose that $G/R(G) \cong \mathrm{D}_{2^c}$, $w > 1$. Then we have $\mathrm{s}_{w+1}(G) = 2^{w+c-1} + 2^{w+1} - 1$.*

Proof. Let

$$X_1/R(G), \dots, X_{2^{c-1}}/R(G), X_{2^{c-1}+1}/R(G) = \mathrm{Z}(G/R(G))$$

be all subgroups of order 2 in $G/R(G)$. Then

$$R(X_i) = R(G), \quad \mathrm{s}_{w+1}(X_i) = 2^{w-1+2} - 1 = 2^{w+1} - 1 \quad \text{for all } i \quad \text{(Lemma 124.9)}$$

and

$$\mathrm{s}_{w+1}(R(G)) = 2^{w-1+1} - 1 = 2^w - 1 \quad \text{(Theorem 124.8(b))}.$$

We get $X_i \cap X_j = R(G)$ for $i \neq j$ and, given $H < G$ of order 2^{w+1} not contained in $R(G)$, there is exactly one $i \leq 2^{c-1}+1$ such that $H < X_i (= HR(G))$. Therefore

$$\begin{aligned} \mathrm{s}_{w+1}(G) &= \sum_{i=1}^{2^{c-1}+1} \mathrm{s}_{w+1}(X_i) - 2^{c-1}\mathrm{s}_{w+1}(R(G)) \\ &= (2^{c-1}+1)(2^{w+1}-1) - 2^{c-1}(2^w - 1) = 2^{w+c-1} + 2^{w+1} - 1, \end{aligned}$$

and the proof is complete. (It is easy to check that, for $t = 1$ and $c = 3$, the obtained result coincides with Lemma 124.14(a).) □

In the following supplement we consider the groups G such that $G/R(G) \cong \mathrm{D}_{2^c}$, $w > 1$ and $t = 2$. Note that the cases $t = 3, \ldots, c-2$ are more difficult and, to treat them, one has to use the enumeration principle and induction on c for each value of t.

Supplement 3 to Theorem 124.18. *Suppose that G is a metacyclic 2-group such that $G/R(G) \cong \mathrm{D}_{2^c}$, $w > 1$ and $t = 2$. Then $\mathrm{s}_{w+2}(G) = 2^{w+c-2} + 2^{w+1} - 1$.*

Proof. Suppose that $X_1/R(G), \ldots, X_{2^{c-2}}/R(G) < G/R(G)$ are abelian of type $(2,2)$ and $X_{2^{c-2}+1}/R(G) = Y/R(G) < G/R(G)$ cyclic of order 4. For $i \neq j$ we have $X_i \cap X_j = \Omega_{w+1}(Y)$. Given $H < G$ of order 2^{w+2}, there is $i \in \{1, \ldots, 2^{c-2}+1\}$ such that $H < X_i$ since $|H \cap R(G)| \geq 2^w$. Therefore

$$\mathrm{s}_{w+2}(G) = \sum_{i=1}^{2^{c-2}+1} \mathrm{s}_{w+2}(X_i) - 2^{c-2} \cdot \mathrm{s}_{w+2}(\Omega_{w+1}(Y)). \tag{10}$$

We have $R(X_i) = X_i$ for $i \leq 2^{c-2}$ and $R(Y) = R(G)$. By Theorem 124.8(b),

$$\mathrm{s}_{w+2}(X_i) = \mathrm{s}_{(w+1)+1}(X_i) = 2^{(w+1)-1+1} - 1 = 2^{w+1} - 1, \quad i \leq 2^{c-2},$$

and, by Lemmas 124.10, 124.9, respectively (recall that $Y = X_{2^{c-2}+1}$),

$$\mathrm{s}_{w+2}(Y) = 2^{w-2+3} - 1 = 2^{w+1} - 1, \quad \mathrm{s}_{w+2}(\Omega_{w+1}(Y)) = 2^{w-2+2} - 1 = 2^w - 1.$$

Therefore we get, by (10),

$$\begin{aligned} \mathrm{s}_{w+2}(G) &= 2^{c-2} \cdot (2^{w+1} - 1) + (2^{w+1} - 1) - 2^{c-2} \cdot (2^w - 1) \\ &= 2^{w+c-2} + 2^{w+1} - 1, \end{aligned}$$

and the proof is complete. □

The cases $G/R(G) \in \{\mathrm{Q}_{2^c}, \mathrm{SD}_{2^c}\}$, where $w > 1$ and $t = 2$, are considered similarly.

Theorem 124.19. *Suppose that G is a metacyclic 2-group such that $G/R(G) \cong \mathrm{SD}_{2^c}$ and $w + t > w > 1$, $c - 1 \leq t \leq w + c$. Then $\mathrm{s}_{w+t}(G) = 2^{w-t+c+1} - 1$.*

Proof. It is easily seen that the theorem holds for $t \in \{w+c-1, w+c\}$. Next we assume that $t < w+c-1$.

By Theorems 124.12, 124.16, 124.18 and (8), we have

$$\mathrm{s}_{w+t}(G) = 3(2^{w-t+c}-1) - 2(2^{w-t+c-1}-1) = 2^{w-t+c+1} - 1,$$

and the proof is complete. □

Supplement 1 to Theorem 124.19. *Let* $G/R(G) \cong \mathrm{SD}_{2^c}$, $w = 1$ *and* $t \geq 1$. *Then*

(a) *If* $t = 1$, *then* $\mathrm{s}_{1+1}(G) = \mathrm{s}_2(G) = 2^{c-1} + 3$.

(b) *If* $1 < t \leq c-1$, *then* $\mathrm{s}_{1+t}(G) = 2^{1-t+c} + 3$.

Proof. In case $t = c-1$, the result follows from the paragraph containing (8). Now let $t < c-1$.

By Supplements 1 to Theorems 124.16 and 124.18 and (9),

$$\mathrm{s}_{1+1}(G) = \mathrm{s}_2(G) = 3 + (2^{1-1+c-1} + 3) - 3 = 2^{c-1} + 3,$$

$$\mathrm{s}_{1+t}(G) = 2(2^{1-t+c-1} + 3) - 3 = 2^{1-t+c} + 3 \quad \text{for } 1 < t < c,$$

completing the proof. □

Supplement 2 to Theorem 124.19. *Suppose that* $G/R(G) \cong \mathrm{SD}_{2^c}$, $w > 1$. *Then we have* $\mathrm{s}_{w+1}(G) = 2^{w+c-2} + 2^{w+1} - 1$.

Proof. Let

$$X_1/R(G), \ldots, X_{2^{c-2}}/R(G), X_{2^{c-2}+1}/R(G) = \mathrm{Z}(G/R(G))$$

be all subgroups of order 2 in $G/R(G)$. Then $\mathrm{s}_{w+1}(X_i) = 2^{w-1+2} - 1 = 2^{w+1} - 1$ for all i (Lemma 124.9), $\mathrm{s}_{w+1}(R(G)) = 2^{w-1+1} - 1 = 2^w - 1$ (Theorem 124.8) and $X_i \cap X_j = R(G)$ for all $i \neq j$. We obtain (see Supplement 2 to Theorem 124.18)

$$\begin{aligned}\mathrm{s}_{w+1}(G) &= (2^{c-2}+1)(2^{w+1}-1) - 2^{c-2}(2^w - 1)\\ &= 2^{w+c-2} + 2^{w+1} - 1,\end{aligned}$$

and we are done. □

The lower restrictions for t in Theorems 124.16, 124.18 and 124.19 are made for technical reasons (otherwise, the statements of these theorems would be more complicated). However, if necessary, it is not difficult, using the above approach, consider the $c-3$ cases for which $t \in \{2, \ldots, c-2\}$.

If G is a noncyclic p-group of order p^n with $\mathrm{s}_k(G) = 1$ for some $k \in \{1, \ldots, n-1\}$, then we have $k = 1$, $p = 2$ and G is a generalized quaternion group (Proposition 1.3). By Sylow's theorem, $\mathrm{s}_k(G) \equiv 1 \pmod{p}$ for the same k. It follows that if G is neither cyclic nor generalized quaternion and $k < n$, then $\mathrm{s}_k(G) \geq 1 + p$. Therefore it is natural to classify the noncyclic p-groups G of order $p^n > p^3$ satisfying $\mathrm{s}_k(G) = 1 + p$ for some fixed $k \in \{2, \ldots, n-2\}$ ($\mathrm{s}_{n-1}(G) = 1 + p$ if and only if $\mathrm{d}(G) = 2$).

Proposition 124.20. *Let G be a group of order $p^n > p^3$ satisfying $s_k(G) = 1 + p$ for some fixed $k \in \{2, \dots, n-2\}$. Then one of the following holds:*

(a) *G is abelian of type (p^{n-1}, p).*

(b) *$G \cong M_{p^n}$.*

(c) *$p = 2$, $k = 2$ and $G = \langle a, b \mid a^{2^{n-2}} = 1, n > 4, a^{2^{n-3}} = b^2 = 1, a^b = a^{-1} \rangle$ is metacyclic as in Lemma 42.1*(c).

Proof. It is easy to see that G is not a 2-group of maximal class (otherwise, by Theorem 124.4, $s_k(G) \equiv 1 \pmod 4$ so $s_k(G) \neq 1 + 2$). In that case, G has a normal abelian subgroup R of type (p, p) (Lemma 1.4).

(i) Suppose that $k = 2$. Assume that G has a subgroup E of order p^3 and exponent p; then E is nonabelian (otherwise, we have $s_2(E) = 1 + p + p^2 > 1 + p$), $s_2(E) = 1 + p = s_2(G)$. It follows that all subgroups of G of order p^2 are contained in E so $\exp(G) = p$, $s_2(G) \equiv 1 + p + 2p^2 \pmod{p^3}$ (Theorem 5.9), a contradiction. Thus E does not exist.

Assume that G/R has two distinct subgroups X/R and Y/R of order p. Then X and Y contain together at least $s_2(X) + s_2(Y) - 1 = 2p + 1 > p + 1$ distinct subgroups of order p^2, a contradiction. Thus G/R is either cyclic or generalized quaternion. In the first case, G is one of groups (a, b). If G/R is generalized quaternion, then we obtain that $|\Omega_2(G)| = 2^3$ so G is as in (c) by Lemma 42.1(c).

(ii) Suppose that $k > 2$. Then, as in part (i), G/R contains exactly one (proper since $k < n - 1$) subgroup of order p^{k-1}. In that case, G/R is cyclic. The subgroup $C_G(R)$ is abelian with cyclic subgroup of index p and $|G : C_G(R)| \leq p$. Then $\Omega_1(G) = R$ so G is either as in (a) or in (b). □

Now let $s_1(G) = 1 + p$. If $p > 2$, then G is either metacyclic or a 3-group of maximal class (Theorem 13.7). Such G are also described very well for $p = 2$ in §82.

Proposition 124.21. *Let M be a metacyclic p-group and let G be a p-group of order $p^n > p^3$, $p > 2$. If $s_2(G) = s_2(M)$, then one of the following holds:*

(a) *G is metacyclic.*

(b) *$G = EC$, where $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent p and C is cyclic of order $> p$.*

(c) *G is of maximal class and order p^4, all maximal subgroups of G are two-generator.*

Proof. One may assume that the p-group M is noncyclic; then G is also noncyclic. We have $s_2(G) = s_2(M) = \{1 + p, 1 + p + p^2\}$ (Theorem 124.1).

Assume that G is nonmetacyclic. Then $s_2(G) = 1 + p + p^2$ by Theorem 124.20, and so $\Omega_2(G)$ is nonmetacyclic by Remark 41.2.

(i) Assume that G has a subgroup E of order p^4 and exponent p. Then we obtain that $s_2(E) = 1 + p + 2p^2 + sp^3$ for some nonnegative integer (Theorem 5.9) so $s_2(E) > 1 + p + p^2 = s_2(G)$, a contradiction.

(ii) Assume that G has an elementary abelian subgroup E of order p^3. Then we get $s_2(E) = 1 + p + p^2$, so, by the first paragraph, all subgroups of G of order p^2 are contained in E. It follows that $\exp(G) = p$, and so, by (i), $G = E$ is of order p^3, contrary to the hypothesis.

(iii) It follows from (ii) that either G is a 3-group of maximal class or $G = EC$, where $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent p and C is cyclic (Theorem 13.7). The group $G = EC$ satisfies the hypothesis (note that one of such groups is of maximal class; then its order is equal to p^4).

Suppose that G is a 3-group of maximal class and order $> 3^4$. Let G_1 be the fundamental subgroup of G (see §9); then G_1 is metacyclic without cyclic subgroup of index 3 (Theorems 9.6 and 9.11) so that

$$s_2(G_1) = 1 + 3 + 3^2 = s_2(M) = s_2(G).$$

It follows that all subgroups of G of order 3^2 are contained in G_1 so that $\Omega_2(G) \leq G_1$. However (see Proposition 13.14(b)), $\Omega_2(G) = G > G_1$, and this is a contradiction. Thus, if G is a 3-group of maximal class, then $n = 4$. By (ii), G has no subgroup of type $(3, 3, 3)$, and this holds if and only if G is not isomorphic to a Sylow 3-subgroup of the symmetric group of degree 9. □

4^o *A property of metacyclic 2-groups with nonabelian section of order* 8. In this subsection G is a metacyclic 2-group containing subgroups $L \lhd M$ such that M/L is nonabelian of order 8 (M/L is said to be a section of G).

In what follows we freely use the following known fact: There is only one nonabelian metacyclic group of order 16 and exponent 4. Before we denoted this group by $\mathcal{H}_2$.

If $G = R(G)$, then $R(\mho_1(G)) = \mho_1(G)$. We use this obvious fact in the proof of the following

Theorem 124.22. *Suppose that a metacyclic 2-group G has a nonabelian section of order* 8. *If G is not of maximal class, then the following hold:*

(a) *There is $R \lhd G$ such that $G/R \cong Q_8$ and $G/\mho_2(G) \cong \mathcal{H}_2$.*

(b) $\mho_1(G)$ *has no nonabelian section of order* 8.

Proof. (a) We use induction on $|G|$. Let $L \lhd M \leq G$ be such that M/L is nonabelian of order 8. One may assume that $M < G$ (otherwise, there is nothing to prove). Let $M \leq H \in \Gamma_1$. Then, by induction, there is $S \lhd H$ such that H/S is nonabelian of order 8. By Lemma J(c), S is characteristic in H so normal in G. Due to Lemma J(b), G/S is of maximal class. Let $R/S = Z(G/S)$; then G/R is nonabelian of order 8, as was to be shown.

(b) Assume that $\mho_1(G) = \Phi(G)$ has a nonabelian section of order 8. Then, by (a), there is $S \lhd \mho_1(G)$ such that $\mho_1(G)/S$ is nonabelian of order 8. Due to Lemma J(c), S is characteristic in $\mho_1(G)$ so normal in G. By Lemma J(b), the quotient group G/S is of maximal class (of order 2^5). Thus $\Phi(G/S) = \mho_1(G/S)$ is nonabelian of order 8, contrary to Lemma 1.4. □

5^o Mann's proof of Theorem 124.1 for $p > 2$. The content of this subsection is taken from [Man33] (only in one place we made a change using Lemma 124.2). We retain the notation introduced in 1^o.

Proof of Theorem 124.1. Below G is a metacyclic p-group, $p > 2$. We use the same notation as in 1^o.

By Lemma 124.2, G is the product of two cyclic subgroups with trivial intersection, say $G = \langle x\rangle\langle y\rangle = AB,\ A\cap B = \{1\}$. By regularity, p^e is the maximum of the orders of x and y, and thus we may assume that $|A| = p^e$, and then $|B| = p^f$. Hence $e \geq f$. Since $G' \leq \mho_1(G)$, we have $\mho_{e-1}(G') = \{1\}$. In a regular group, by Theorem 7.2(f), $[G, \mho_k(G)] = \mho_k(G')$. Taking $k = e-1$, we get $[G, \mho_{e-1}(G)] = \mho_{e-1}(G') = \{1\}$, and hence $\mho_{e-1}(G) \leq \mathrm{Z}(G)$, and in particular $N = \langle x^{p^{e-1}}\rangle$ is a central subgroup of order p.

Write $\mathrm{z}_m(G)$ for the number of subgroups of G of order p^m that do not contain N. It is clear that

$$\mathrm{s}_m(G) = \mathrm{s}_{m-1}(G/N) + \mathrm{z}_m(G). \tag{11}$$

Note that in the quotient group G/N the invariants corresponding to e and f are $e-1$ and f (arranged in order). We now evaluate $\mathrm{z}_m(G)$. Let H be any subgroup of order p^m not containing N. Since $\Omega_1(G) = N \times \mho_{f-1}(B)$ has order p^2, we see that $|\Omega_1(H)| = |H \cap \Omega_1(G)| = p$, and thus H is cyclic since $p > 2$. If $m > f$, then we have $|H| > |G : A|$, therefore $H \cap A \neq \{1\}$, and $H \geq N$ so that $\mathrm{z}_m(G) = 0$. Now let $m \leq f$. Then

$$|\Omega_m(G)| = |\Omega_m(A)\Omega_m(B)| = p^{2m}, \quad |\Omega_{m-1}(G)| = p^{2(m-1)},$$

and G contains $p^{2m} - p^{2(m-1)}$ elements of order p^m and so

$$\frac{p^{2m} - p^{2(m-1)}}{(p-1)p^{m-1}} = p^{m-1}(p+1)$$

cyclic subgroups of order p^m. Let z be a generator of N. If a cyclic subgroup H contains N, then H is generated by some element t such that $t^{p^{m-1}} = z$. Then the elements of G whose p^{m-1} powers are equal to z are the elements of the coset $t\,\Omega_{m-1}(G)$, their number is $p^{2(m-1)}$, and H contains p^{m-1} of them. It follows that there are p^{m-1} cyclic subgroups of order p^m containing N, and $\mathrm{z}_m(G) = p^m$. Now the first formula of the theorem follows by induction, noting that $m - 1 \leq f(G/N)$.

Next, let $f \leq m \leq e$. If $m = f$, then the result follows from the previous case, so we assume that $m > f$. Then we get $\mathrm{s}_m(G) = \mathrm{s}_{m-1}(G/N)$. Here $e > f$, implying $e(G/N) = e-1$ and $f(G/N) = f$, and thus $e(G/N) \geq m - 1 \geq f(G/N)$, and we apply induction.

Finally, assume that $m \geq e$. Again $\mathrm{s}_m(G) = \mathrm{s}_{m-1}(G/N)$, and once more the case of equality $m = e$ is covered by the previous case, therefore we may assume that $m > e$, implying $m - 1 \geq e(G/N)$, and we apply induction. □

6^o *The p-groups with the same number of subgroups of some order as in a metacyclic p-group.* Mann reported that, given a metacyclic p-group G, $p > 2$, he classified the p-groups H such that $\mathrm{s}_1(H) = \mathrm{s}_1(G)$ and $\mathrm{s}_2(H) = \mathrm{s}_2(G)$ (see also [Man33, Proposition 2] and Theorem 124.31). First we offer another proof of this result. Then we shall prove a related result.

Proposition 124.23. *Suppose that G and H are p-groups of exponent $> p$, $p > 2$, and G is metacyclic. Write $L_{p^k}(G) = \{x \in G \mid o(x) \leq p^k\}$. If $|L_{p^2}(H)| = |L_{p^2}(G)|$, then one of the following holds:*

(a) *H is metacyclic.*

(b) *$p = 3$ and H is of maximal class and order 3^4; moreover, H is minimal nonmetacyclic.*

(c) *$|\Omega_1(H)| = p^3$ and $H/\Omega_1(H) > \{1\}$ is cyclic.*

In particular (Mann), if $s_1(H) = \mathrm{s}_1(G)$ and $s_2(H) = \mathrm{s}_2(G)$, then H is as in parts (a–c) *with nonabelian $\Omega_1(H)$ of order p^3.*

Proof. One may assume that H is nonmetacyclic. Then

$$|L_{p^2}(H)| = |L_{p^2}(G)| \in \{p^3, p^4\}.$$

Write $R = \Omega_1(G)$; then R is abelian of type (p, p). Let $M/R = \Omega_1(G/R)$. Then we get $M = \Omega_2(G) = L_{p^2}$. If $|M/R| = p$, then $|\Omega_2(H)| = p^3$ and so H has a cyclic subgroup of index p so it is as in (a). Next we assume that $|M| = p^4$. Then we obtain $|\Omega_2(H)| = p^4$.

- If $|\Omega_1(H)| = p^2$, then H is a 3-group of maximal class. Since $\Omega_2(H) = H$, we get $|H| = 3^4$ so H is as in (b).
- If $|\Omega_1(H)| = p^3$, then H is as in (c).

Now let $\mathrm{s}_1(H) = \mathrm{s}_1(G)(= 1 + p)$ and $\mathrm{s}_2(H) = \mathrm{s}_2(G) \in \{1 + p, 1 + p + p^2\}$. In this case, $|L_{p^2}(H)| = |\Omega_2(H)| = p^4$ so that, by the above, H is as in (a–c) (with $\Omega_1(H)$ is nonabelian of order p^3 in (c)). □

The analogous problem for $p = 2$ is surprisingly complicated.

Denote by $\mathrm{s}^{[k]}(G)$ the number of subgroups of index p^k in a p-group G.

Proposition 124.24. *Suppose that G and H be p-groups of exponent $> p$ and assume that G is metacyclic. If $\mathrm{s}^{[1]}(H) = \mathrm{s}^{[1]}(G)$ and $\mathrm{s}^{[2]}(H) = \mathrm{s}^{[2]}(G)$, then one of the following holds:*

(a) *H is metacyclic.*

(b) *$p > 2$ and $\mathrm{K}_3(H) = \mathfrak{V}_1(H)$ has index p^3 in G.*

Proof. One may assume that the group G is noncyclic. Then we have $\mathrm{s}^{[1]}(G) = 1 + p$, i.e., $2 = \mathrm{d}(G) = \mathrm{d}(H)$. Using Hall's enumeration principle, we further conclude that $\mathrm{s}^{[2]}(G) \in \{1 + p, 1 + p + p^2\}$. If $\mathrm{s}^{[2]}(G) = 1 + p$, then G has a cyclic subgroup of

index p. Therefore, if $s^{[2]}(H) = p+1$, then, by what has just been said, H has a cyclic subgroup of index p so metacyclic. Now let $s^{[2]}(H) = p^2 + p + 1$. In this case, using Hall's enumeration principle, we conclude that the ranks of all maximal subgroups of H are equal to 2. Then, by Proposition 36.3, if $p > 2$, then we get case (b), if $p = 2$, then H is metacyclic. □

Corollary 124.25. *Suppose that G and H are p-groups and assume that G is metacyclic. If $s_k(H) = s_k(G)$ holds for all positive integers k, then H is either metacyclic or minimal nonmetacyclic of order 3^4.*

Proposition 124.26. *Let G be an absolutely regular p-group of exponent $> p$, $p > 2$. If H is such a p-group that $c_1(H) = c_1(G)$ and $c_2(H) = c_2(G)$, then one of the following holds:*

(a) *H is absolutely regular.*

(b) *H is irregular of maximal class and order $\le p^{2(p-1)}$ and $|\Omega_1(H)| = p^{p-1}$.*

Proof. Let $|\Omega_1(G)| = p^r$ and $|\Omega_2(G)| = p^{r+s}$; then, since G is absolutely regular, we have

$$r, s \le p-1, \quad c_1(G) = 1 + p + \cdots + p^{r-1} = c_1(H),$$

$$c_2(G) = \frac{p^{r+s} - p^r}{p(p-1)} = p^{r-1}(1 + p + \cdots + p^{s-1}) = c_2(H).$$

By Theorems 13.2(a) and 9.5, H is either absolutely regular or irregular of maximal class.

Assume that the group H is irregular of maximal class. Then we obtain $r = p-1$, $|\Omega_1(H)| = |\Omega_1(G)| = p^{p-1}$. Let $|H| = p^n$ and let F be an absolutely regular maximal subgroup of H; then $n \ge p+1$ (see Theorems 9.5 and 9.6). By Theorem 13.19, all elements of the set $H - F$ have the same order p^2. Therefore there are in H exactly

$$\frac{p^n - p^{n-1}}{p(p-1)} = p^{n-2}$$

cyclic subgroups of order p^2 not contained in F. Let $|\Omega_2(F)| = p^{p-1+t}$; then we get $t \le p-1$ since F is absolutely regular, and we have

$$c_2(F) = \frac{p^{p-1+t} - p^{p-1}}{p(p-1)} = p^{p-2}(1 + p + \cdots + p^{t-1})$$

so that

$$\begin{aligned} c_2(H) &= p^{p-2}(1 + p + \cdots + p^{t-1}) + p^{n-2} = p^{r-1}(1 + p + \cdots + p^{s-1}) \\ &= p^{p-2}(1 + p + \cdots + p^{s-1}). \end{aligned}$$

As $n \ge p+1$, we get

$$n = 2 + (r-1) + (s-1) = r + s \le (p-1) + (s-1) = 2(p-1). \qquad \square$$

7^o *On subgroups of metacyclic p-groups.* We begin with the following exercises.

Exercise 1. Let G be a nonabelian metacyclic p-group that is not generalized quaternion. Then the following conditions are equivalent:

(a) All minimal nonabelian subgroups of G have no cyclic subgroups of index p.

(b) $\Omega_1(G) \le \mathrm{Z}(G)$.

Solution. (a) $\Rightarrow$ (b). If a subgroup $H \le G$ is minimal nonabelian, then we obtain that $\Omega_1(G) = \Omega_1(H) \le \mathrm{Z}(H)$. Since G is generated by its minimal nonabelian subgroups (Theorem 10.28), we get $\Omega_1(G) \le \mathrm{Z}(G)$.

(b) $\Rightarrow$ (a). Assume that a minimal nonabelian $F \le G$ has a cyclic subgroup of index p. Then we obtain $\Omega_1(G) \not\le F$ (otherwise, F would be abelian). It follows that $p = 2$ so $F \cong \mathrm{Q}_8$ (see Exercise 1.8(a) or Lemma 65.1). In this case, G is of maximal class (Lemma J(b)) so G is generalized quaternion, contrary to the hypothesis.

Exercise 2. Let a metacyclic p-group G be neither abelian nor minimal nonabelian. If $\Omega_1(G) \not\le \mathrm{Z}(G)$, then G contains at least $k \ge p-1$ minimal nonabelian subgroups with a cyclic subgroup of index p. If $k = p-1$, then $|G'| = p^2$ so all subgroups of index p^2 in G are abelian.

Solution. One may assume that G has no cyclic subgroup of index p; then G has no nonabelian subgroup of order p^3. If $p = 2$, then $k \ge 1$ (Exercise 1). Now let $p > 2$. Then $\mathrm{C}_G(\Omega_1(G)) = C$ is maximal in G and the minimal nonabelian subgroups of C have no cyclic subgroups of index p. If $A < G$ is minimal nonabelian without cyclic subgroup of index p, then $A \not\le C$ and we obtain that $\Omega_1(G) = \Omega_1(A) \le \mathrm{Z}(A)$ so that $\mathrm{C}_G(\Omega_1(G)) \ge CA = G$, contrary to the hypothesis. Thus every minimal nonabelian subgroup of G not contained in C has a cyclic subgroup of index p. It follows from §76 that $k \ge p-1$ in all cases. Now suppose that $k = p-1$. Then, by Lemma 76.5(a), $\Gamma_1 = \{C, A_1, \dots, A_{p-1}, A\}$, where $A_1, \dots, A_{p-1}$ are minimal nonabelian and A is abelian. In view of Lemma 64.1(u), we get $|G'| \le p|A_1'A'| = p^2$. If $|G'| = p$, then G is minimal nonabelian (Lemma 65.2(a)), contrary to the hypothesis. Thus $|G'| = p^2$. In this case, all subgroups of G of index p^2 are abelian (Corollary 65.3), as asserted.

Exercise 3. Let G and k be such as in Exercise 2. Study the structure of G provided $k = p$. (*Hint.* See Lemma 76.13.)

Lemma 124.27. *Let $G > \{1\}$ be a metacyclic p-group, $A < B \le G$. Then $A' < B'$ unless B is abelian.*

Proof. Assume that B is nonabelian and $A' = B'$. Take in B' a subgroup L of index p. Then B/L is minimal nonabelian (Lemma 65.2(a)) so A/L is abelian. In this case, we get $A' \le L < B'$, as was to be shown. □

Theorem 124.28. *Suppose that G is a metacyclic p-group with derived subgroup of order $p^n > p$ and let t be the number of maximal subgroups of G having derived subgroup of order p^{n-1}. Then $t \in \{p, p+1\}$.*

Proof. By Lemma 64.1(u), there exists $H \in \Gamma_1$ such that $|H'| = p^{n-1}$ so that $t > 0$. Assume that there are distinct $A, B \in \Gamma_1$ such that $|A'| \leq |B'| < p^{n-1}$. Since G' is cyclic, we get $A' \leq B'$. Then, by Lemma 64.1(u), we have

$$|G'| \leq p|A'B'| = p|B'| < p \cdot p^{n-1} = p^n,$$

contrary to the hypothesis. Thus there is in Γ_1 at most one member whose derived subgroup has order $< p^{n-1}$. Since G is noncyclic so $|\Gamma_1| = p+1$ and G has no maximal subgroup whose derived subgroup has order p^n (Lemma 124.27), we conclude that $t \geq p$. We are done since $t \leq p+1$. □

Using induction and Hall's enumeration principle, one obtains

Corollary 124.29. *Suppose that G is a metacyclic p-group with derived subgroup of order $p^n > p^2$. If t denotes the number of subgroups H of G with $|H'| = p^{n-2}$ and $|G : H| = p^2$, then $p^2 - p \leq t \leq (p+1)^2$.*

Proof. Let $M_1, \ldots, M_s$ be all members of the set Γ_1 whose derived subgroups have order p^{n-1}; then $s \in \{p, p+1\}$ (Theorem 124.28). Let $t(M_i)$ be the number of those maximal subgroups of M_i whose derived subgroups have order p^{n-2} and let $\epsilon = 0$ if $|\Phi(G)'| < p^{n-2}$ and $\epsilon = 1$ if $|\Phi(G)'| = p^{n-2}$; then we have $t(M_i) \in \{p, p+1\}$ (Theorem 124.28). By Hall's enumeration principle,

$$t = \sum_{i=1}^{s} t(M_i) - p\epsilon.$$

It follows that $p^2 - p \leq t \leq (p+1)^2$. □

Exercise 4. Suppose that G is a metacyclic 2-group of order $> 2^{2k}$, $k > 1$. If all minimal nonabelian subgroups of G are isomorphic to

$$\mathcal{H}_k = \langle a, b \mid a^{2^k} = b^{2^k} = 1, a^b = a^{1+2^{k-1}} \rangle,$$

then $\Omega_{k-1}(G) = \mathrm{Z}(G)$ is abelian of type $(2^{k-1}, 2^{k-1})$ and $G/\mathrm{Z}(G)$ is dihedral.

Solution. By Proposition 10.28, the group G is generated by minimal nonabelian subgroups. It follows that all minimal nonabelian subgroups are not normal in G (otherwise, they would be coincide). If $A < G$ is minimal nonabelian, then we obtain that $\Omega_{k-1}(G) = \Omega_{k-1}(A) = \mathrm{Z}(A)$ and thus we get $\Omega_{k-1}(G) \leq \mathrm{Z}(G)$ since such subgroups A generate G (Theorem 10.28). Moreover, since $A \cap \mathrm{Z}(G) = \mathrm{Z}(A)$, we get $\Omega_{k-1}(G) = \mathrm{Z}(G)$. Therefore the nonabelian metacyclic quotient group $G/\Omega_{k-1}(G)$ is generated by abelian subgroups of type $(2,2)$, and we conclude that it is dihedral since $|G/\Omega_1(G)| \geq 8$ (see Theorem 1.2).

Exercise 5. If A metacyclic 2-group G contains two distinct minimal nonabelian subgroups A and B of order 2^{2k} and exponent 2^k, then $G/\Omega_{k-1}(G)$ is either dihedral or semidihedral. If $G/\Omega_{k-1}(G)$ is dihedral, then $\Omega_{k-1}(G) = \mathrm{Z}(G)$.

Solution. We have $\Omega_{k-1}(G) = \Omega_{k-1}(A) = \Omega_{k-1}(B)$. As $A/\Omega_{k-1}(G)$, $B/\Omega_{k-1}(G)$ are nonnormal four-subgroups of $G/\Omega_{k-1}(G)$, it follows that $G/\Omega_{k-1}(G)$ is of maximal class (Lemma J(e)); moreover, $G/\Omega_{k-1}(G)$ is either dihedral or semidihedral. Suppose that $G/\Omega_{k-1}(G)$ is dihedral. If $H/\Omega_{k-1}(G)$ is abelian of type $(2,2)$, then either H is abelian or $H \cong \langle a, b \mid a^{2^k} = b^{2^k} = 1,\ a^b = a^{1+2^{k-1}} \rangle$. In both cases, we obtain $\Omega_{k-1}(G) = \mathrm{Z}(H)$. As such subgroups H generate G, we get

$$\Omega_{k-1}(G) \leq \mathrm{Z}(G).$$

Now the equality of these two subgroups follows since $\mathrm{Z}(G) \cap H = \Omega_{k-1}(G)$.

Exercise 6. Suppose that G is a metacyclic p-group and $B < G$ minimal nonabelian. Then B/B' is a maximal abelian subgroup of G/B'.

Solution. Assume that $B/B' < A/B'$, where A/B' is abelian. Then $A' = B'$, contrary to Lemma 124.27.

Exercise 7. Let A be a proper minimal nonabelian subgroup of a p-group G. Suppose that all subgroups of G containing A of order $p|A|$ are two-generator. Then A/A' is a maximal abelian subgroup of $\mathrm{N}_G(A)/A'$.

Hint. Let $A < T \leq \mathrm{N}_G(A)$ be such that $|T : A| = p$ and T/A' is abelian. Since $\mathrm{d}(T) = 2$ and $T' = A'$ is of order p, it follows from Lemma 65.2(a) that T is minimal nonabelian, which is a contradiction.

Exercise 8 (= Proposition 10.17). Let B be a nonabelian subgroup of order p^3 of a p-group G. If $\mathrm{C}_G(B) < G$, then G is of maximal class.

Solution. Set $N = \mathrm{N}_G(B)$. Then, by N/C-Theorem, $|N| = p^4$ so N is a unique subgroup of order p^4 in G containing B. We claim that $\mathrm{d}(N) = 2$ (otherwise, N contains at least two distinct abelian subgroups of order p^3 so $|\mathrm{Z}(N)| = p^2$; then $\mathrm{C}_G(B) \not\leq B$, a contradiction). Clearly, $\mathrm{Z}(G) = \mathrm{Z}(B) = B'$. Then, by Exercise 7, B/B' is a maximal abelian subgroup of G/B' so G/B' is of maximal class (Proposition 1.8). Since $\mathrm{Z}(G) = B'$ is of order p, it follows that G is of maximal class as well.

Exercise 9. Let $H < G$, where G is a metacyclic p-group. If $H > R(H)$, then we have $R(H) \lhd G$. (*Hint.* We have $R(H) = \Omega_e(G)$, where $\exp(R(H)) = p^e$.)

Exercise 10. Let G be a metacyclic 2-group and let $h_n(G)$ be the number of subgroups $H < G$ such that $H = R(H)$ is of order 2^{2n}. Then one of the following holds:

(a) $h_n(G) = 1$.

(b) $h_n(G)$ is even. In that case, if $h_n(G) > 0$, then $G/\Omega_{n-1}(G)$ is either dihedral or semidihedral.

Solution. Let $H < G$ be such that $H = R(H)$ is of order 2^{2n}. If $H \lhd G$, then we have $H = \Omega_n(G)$ and $h_n(G) = 1$. Now let H be nonnormal in G; then all such H

are nonnormal in G. In this case, $h_n(G)$ is even. Then $\Omega_{n-1}(H) = \Omega_{n-1}(G)$ and $H/\Omega_{n-1}(H) \cong \mathrm{E}_4$ is non-G-invariant. By Lemma J(e), It follows that $G/\Omega_{n-1}(G)$ is either dihedral or semidihedral.

Exercise 11. Prove that there exists a metacyclic p-group G such that G contains a maximal normal abelian subgroup A with nonabelian G/A.

Solution (Mann). Let G be a semidirect product of a cyclic group A of order p^n by a cyclic group B whose generator induces on A the automorphism $x \to x^{1+p^k}$. The order of B is the order of the automorphism. Choose $n = 2k + 2$. Then G' is the subgroup $\mho_k(A)$ and $\mathrm{Z}(G) = \mho_{n-k}(A)$. Let L be the unique subgroup between G' and $\mathrm{Z}(G)$, and let $D = \mathrm{C}_B(L)$. Then LD is a maximal normal abelian subgroup with nonabelian factor group. Many more examples can be produced by choosing other values of n and k to make the distance between G' and $\mathrm{Z}(G)$ bigger.

Let $\mathscr{H}_{2,p} = \langle a, b \mid a^{p^2} = b^{p^2} = 1,\ a^b = a^{1+p} \rangle$. Then $\mathscr{H}_{2,p}$ is the unique nonabelian metacyclic group of order p^4 and exponent p^2. For $p = 2$ we have $\mathscr{H}_{2,2} = \mathscr{H}_2$.

Theorem 124.30. *Let $H \cong \mathscr{H}_{2,p}$ be a proper subgroup of a metacyclic p-group G. Then one of the following holds:*

(a) *If $p > 2$, then $|G : H| = p$, $|G'| = p^2$, G/G' is abelian of type (p^2, p) and G/Z is cyclic of order p^2 for some cyclic $Z \lhd G$.*

(b) *If $p = 2$ and $H \lhd G$, then $|G : H| = 2$, $|G'| = 4$, G/G' is abelian of type $(4, 2)$ and G/Z is cyclic of order 4 for some cyclic $Z \lhd G$.*

(c) *If $p = 2$ and the subgroup H is not normal in G, then we have $\Omega_1(G) = \Omega_1(H)$ and $|G : \mathrm{C}_G(\Omega_1(G))| \leq 2$. If, in addition, $|G| > 2^5$, then $G/\Omega_1(G)$ is either dihedral or semidihedral.*

Proof. Let G have a proper normal nonabelian subgroup H of order p^4 and exponent p^2. Then we have $R = \Omega_1(H) = \Omega_1(G) \lhd G$. Set $C = \mathrm{C}_G(R)$. Let $L < R$ be of order p, $L \neq H'$. Then $H/L \leq C/L$ is nonabelian of order p^3 so $H = C$ if $p > 2$ and C/L is of maximal class if $p = 2$ (Lemma J(b)). In the case under consideration, $|G : C| \leq p$. Let $p > 2$; then $H = C$. In this case, $G' < C$ so $|G'| = p^2$ since G' is cyclic and G is not minimal nonabelian (see Lemma 65.2(a). There is a cyclic $Z \lhd G$ such that G/Z is cyclic. Since $G' < Z$, it follows that G/G' is abelian of type (p^2, p). Now let $p = 2$ and $H \lhd G$; then L is characteristic in H (Lemma J(a)). Then $C = G$ since $L \lhd G$ so G/L is of maximal class (Lemma J(b)). Since $L \not\leq G'$, it follows that $|G : G'| = 8$ so G/G' is abelian of type $(4, 2)$. As above, there is a cyclic $Z \lhd G$ such that G/Z is cyclic of order 4.

Let H be not normal in G and C as above; then $p = 2$. Suppose that $|G| > 2^5$. Take $L < R(= \Omega_1(G))$ of order 2, $L \neq H'$. Then $H/L \leq C/L$ is nonabelian of order 8 so C/L is of maximal class. In this case, $C/\Omega_1(G) \leq G/\Omega_1(G)$ is of maximal class with nonnormal abelian subgroup $H/\Omega_1(G)$ of type $(2, 2)$, and we conclude that $G/\Omega_1(G)$ is either dihedral or semidihedral. □

Proposition 124.31. *Suppose that $H \cong \mathrm{M}_{p^n}$, $n > 3$, is a proper subgroup of a metacyclic p-group G. Then $\mathrm{N}_G(H)/H$ is cyclic. Next, assume that $n = 4$.*

(a) *If $p > 2$, then $|\mathrm{N}_G(H)/H| = p$.*

(b) *If $p = 2$, then $|\mathrm{N}_G(H)/H| \leq 4$.*

Proof. Assume that $\mathrm{N}_G(H)/H$ is noncyclic. Write $N = \mathrm{N}_G(H)$. In this case, we have $H \not\leq \Phi(N)$. Indeed, otherwise $\Omega_1(H) = \Omega_1(N) \leq \mathrm{Z}(N)$ (see the proof of Lemma 1.4). Then $\Omega_1(H) \leq \mathrm{Z}(H)$ so H is abelian, a contradiction. Thus $\mathrm{N}_G(H)/H$ is cyclic. Next we assume that $n = 4$. By Exercise 8, H/H' is a maximal abelian subgroup of N/H'.

If $p > 2$, then a Sylow p-subgroup of $\mathrm{Aut}(H/H')$ is nonabelian of order p^3 and exponent p so N/H, being cyclic, has order p.

Now let $p = 2$. Then $\mathrm{Aut}(H/H') \cong \mathrm{D}_8$ so N/H is a cyclic subgroup of D_8, and we conclude that N/H is cyclic of order ≤ 4. □

Problems

Below we state some related problems.

Problem 1. Study the metacyclic p-groups, $p > 2$, possessing a nonabelian section of order p^3. (See Theorem 124.22.)

Problem 2. Find the number of subgroups of given order in a nonmetacyclic minimal nonabelian p-group.

Problem 3. Let G be an abelian group of type $(p^{a_1}, \ldots, p^{a_k})$. Find the types of all maximal subgroups of G counting multiplicities.

Problem 4. Find the number of subgroups of given order in an abelian p-group of rank 3.

Problem 5. Let G be a homocyclic p-group of rank d.

(i) Find the number of subgroups of given order in G.

(ii) Find the number of subgroups of rank 2 and given order in G.

Problem 6. Given a positive integer $k > 1$, classify the p-groups G such that there exists a metacyclic p-group M satisfying $\mathrm{s}_k(G) = \mathrm{s}_k(M)$.

Problem 7. Study the p-groups G such that $\mathrm{s}_k(G) = \mathrm{s}_k(A)$ for all positive integers k and some abelian p-group A.

Problem 8. Given $p > 2$ and $n > p$, does there exist an absolutely regular p-group A (see §9) and an irregular p-group G of the same order p^n satisfying $\mathrm{s}_k(G) = \mathrm{s}_k(A)$ for all $k \in \{2, \ldots, n-1\}$?

§125

p-groups G containing a maximal subgroup H all of whose subgroups are G-invariant

Here we solve a problem stated by the first author.

Theorem 125.1. *Let G be a nonabelian p-group containing a maximal subgroup H such that all subgroups of H are G-invariant. Then there is an element $g \in G - H$ such that one of the following holds:*

(i) *$p = 2$, H is Hamiltonian, i.e., $H = Q \times V$, where $Q \cong \mathrm{Q}_8$, $\exp(V) \leq 1$, and $g \in \mathrm{Z}(G)$, $o(g) \leq 4$.*

(ii) *$p = 2$, H is abelian of exponent 2^e, $e \geq 2$, and either g inverts each element in H or $e \geq 3$ and g satisfies $h^g = h^{-1+2^{e-1}}$ for all $h \in H$. In both cases, $\mathrm{Z}(G) = \mathrm{C}_H(g) = \Omega_1(H)$ is elementary abelian and $o(g) \leq 4$.*

(iii) *$p = 2$, H is abelian of exponent 2^e, $e \geq 3$, and $h^g = h^{1+2^{e-1}}$ for all $h \in H$, where $\mathrm{Z}(G) = \mathrm{C}_H(g) = \Omega_{e-1}(H)$.*

(iv) *$p > 2$, H is abelian of exponent p^e, $e \geq 2$, and $h^g = h^{1+p^{e-1}}$ for all $h \in H$, where $\mathrm{Z}(G) = \mathrm{C}_H(g) = \Omega_{e-1}(H)$.*

Proof. (i) First assume that H is nonabelian. Then $p = 2$ and $H = Q \times V$, where $Q \cong \mathrm{Q}_8$ and $\exp(V) \leq 1$. Set $U = \mathrm{Z}(Q) \times V = \Omega_1(H)$ so that $U \leq \mathrm{Z}(G)$ since each subgroup of order 2 in U is normal (and so central) in G. But each subgroup of Q is also normal in G and so $G = Q * C$, where $C = \mathrm{C}_G(Q)$, $Q \cap C = \mathrm{Z}(Q)$ and $H \cap C = U$. Thus C is abelian and so $C = \mathrm{Z}(G)$. We take an element $g \in C - H$ so that $g \in \mathrm{Z}(G)$, $g^2 \in U$ and $o(g) \leq 4$.

(ii) Now assume that H is abelian, $p = 2$, and $\Omega_2(H) \not\leq \mathrm{Z}(G)$. Let g be an element in $G - H$. We have $\mathrm{C}_H(g) = \mathrm{Z}(G)$ and $g^2 \in \mathrm{Z}(G)$. Let v be an element of order 4 in $H - \mathrm{Z}(G)$. Then $v^g = v^{-1} = vz$, where $z = v^2 \in \mathrm{Z}(G)$. Suppose that $\mathrm{Z}(G)$ possesses an element w of order 4. If $w^2 = z$, then vw is an involution in $H - \mathrm{Z}(G)$ and vw is central in G, a contradiction. Hence we get $w^2 = u \neq z$ and $\langle v, w\rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$. But then we obtain $(vw)^g = (vz)w = (vw)z$ and $z \notin \langle vw\rangle$ as $(vw)^2 = zu$ which implies that $\langle vw\rangle$ is not normal in the group G, a contradiction. We have proved that $\mathrm{Z}(G) = \Omega_1(H) = \mathrm{C}_H(g)$ is elementary abelian. For any $x \in H - \mathrm{Z}(G)$ we obtain that $o(x) \geq 4$ and $\mathrm{C}_{\langle x\rangle}(g) = \Omega_1(\langle x\rangle)$ and so either $x^g = x^{-1}$ or $o(x) > 4$ and $x^g = x^{-1}x'$, where $\langle x'\rangle = \Omega_1(x)$. Also, $g^2 \in \mathrm{Z}(G)$ and so $o(g) \leq 4$.

Suppose that g does not invert each element in H. Then $\exp(H) = 2^e$ with $e \geq 3$. If g inverts each element of order 2^e in H, then g inverts each element in H since elements of order 2^e generate H, a contradiction. Hence there is an element $h_1 \in H$ of order 2^e such that g does not invert $\langle h_1 \rangle$ and so $h_1^g = h_1^{-1+2^{e-1}}$. There exists a basis $\{h_1, \ldots, h_r\}$, $r \geq 1$, of H which contains h_1 (since h_1 is of the maximal possible order in H). Assume that there is $h_i \in \{h_1, \ldots, h_r\}$ such that $i > 1$, $o(h_i) = 2^e$ and $h_i^g = h_i^{-1}$. But then

$$(h_1 h_i)^g = h_1^{-1+2^{e-1}} h_i^{-1} = (h_1 h_i)^{-1} h_1^{2^{e-1}}$$

and $\Omega_1(\langle h_1 h_i \rangle) = h_1^{2^{e-1}} h_i^{2^{e-1}} \neq h_1^{2^{e-1}}$ which shows that $\langle h_1 h_i \rangle$ is not normal in G, a contradiction. Hence we must have $h_i^g = h_i^{-1+2^{e-1}}$. Suppose that there is an element $h_j \in \{h_1, \ldots, h_r\}$ such that $j > 1$, $o(h_j) = 2^{e'}$, $e' < e$, but

$$h_j^g \neq h_j^{-1} \quad \text{and so} \quad e' \geq 3 \text{ and } h_j^g = h_j^{-1+2^{e'-1}}.$$

Let $h_1' \in \langle h_1 \rangle$ be such that $o(h_1') = 2^{e'}$ which implies that $(h_1')^g = (h_1')^{-1}$. But then

$$(h_1' h_j)^g = (h_1')^{-1} h_j^{-1+2^{e'-1}} \quad \text{and} \quad \Omega_1(\langle h_1' h_j \rangle) = (h_1')^{2^{e'-1}} h_j^{2^{e'-1}} \neq h_j^{2^{e'-1}}$$

which shows that $\langle h_1' h_j \rangle$ is not normal in G, a contradiction. Hence we must have

$$h_j^g = h_j^{-1} = h_j^{-1+2^{e-1}}$$

since $o(h_j) < 2^e$. We have proved that $h_i^g = h_i^{-1+2^{e-1}}$ for all $1 \leq i \leq r$ and so for all $h \in H$, $h^g = h^{-1+2^{e-1}}$ and we are done.

(iii) Assume that H is abelian, $p = 2$, and $\Omega_2(H) \leq \mathrm{Z}(G)$. Then H is of exponent 2^e, $e \geq 3$, and let $g \in G - H$ so that g centralizes $\Omega_2(H)$. If $x \in H - \mathrm{Z}(G)$, then $o(x) \geq 8$, $\mathrm{C}_{\langle x \rangle}(g) = \langle x^2 \rangle$ and so $x^g = xx'$, where $\langle x' \rangle = \Omega_1(\langle x \rangle)$. Since all elements of order 2^e generate H, there is $h_1 \in H$ of order 2^e such that $h_1^g = h_1^{1+2^{e-1}}$. Let $\{h_1, \ldots, h_r\}$, $r \geq 1$, be a basis of H containing h_1. Suppose that there is an element $h_i \in \{h_1, \ldots, h_r\}$ such that $i > 1$, $o(h_i) = 2^e$ and $h_i^g = h_i$. But then

$$(h_1 h_i)^g = (h_1 h_i) h_1^{2^{e-1}} \quad \text{and} \quad h_1^{2^{e-1}} \notin \langle h_1 h_i \rangle,$$

a contradiction. Hence $h_i^g = h_i^{1+2^{e-1}}$. Assume that there is $h_j \in \{h_1, \ldots, h_r\}$, $j > 1$, $o(h_j) = 2^{e'}$, $e' \geq 3$, $e' < e$, and

$$h_j^g = h_j^{1+2^{e'-1}}.$$

Let $h_1' \in \langle h_1 \rangle$ with $o(h_1') = 2^{e'}$ which gives $(h_1')^g = h_1'$. But then

$$(h_1' h_j)^g = (h_1' h_j) h_j^{2^{e'-1}}$$

so that $h_j^{2^{e'-1}} \notin \langle h_1' h_j \rangle$, a contradiction. Hence

$$h_j^g = h_j = h_j^{1+2^{e-1}}.$$

It follows that for each $h \in H$, $h^g = h^{1+2^{e-1}}$, $\mathrm{Z}(G) = \Omega_{e-1}(H)$, and we are done.

(iv) Finally, assume $p > 2$ so that H is abelian of exponent p^e, $e \geq 2$. We have $\mathrm{Z}(G) = \mathrm{C}_H(g)$, where g is an element in $G - H$ and g satisfies $g^p \in \mathrm{Z}(G)$. For each $x \in H - \mathrm{Z}(G)$, g induces on $\langle x \rangle$ an automorphism of order p and so $x^g = xx'$, where $1 \neq x' \in \Omega_1(\langle x \rangle)$. Since all elements of order p^e generate H, there is $h_1 \in H$ of order p^e such that, replacing g with g^l for some $l \not\equiv 0 \pmod{p}$ if necessary, we may set

$$h_1^g = h_1^{1+p^{e-1}}.$$

Let $\{h_1, \ldots, h_r\}$, $r \geq 1$, be a basis of H containing h_1. Let $h_i \in \{h_1, \ldots, h_r\}$ be such that $i > 1$, $o(h_i) = p^e$ but $h_i^g = h_i$. Then

$$(h_1 h_i)^g = (h_1 h_i) h_1^{p^{e-1}},$$

where $h_1^{p^{e-1}} \notin \langle h_1 h_i \rangle$, a contradiction. Hence we may set $h_i^g = h_i^{1+p^{e-1}} h_i'$, where $h_i' \in \Omega_1(\langle h_i \rangle)$. Then

$$(h_1 h_i)^g = h_1^{1+p^{e-1}} h_i^{1+p^{e-1}} h_i' = (h_1 h_i)^{1+p^{e-1}} h_i'$$

and

$$(h_1 h_i)^{p^{e-1}} h_i' = h_1^{p^{e-1}} (h_i^{p^{e-1}} h_i') \in \Omega_1(\langle h_1 h_i \rangle) = \langle h_1^{p^{e-1}} h_i^{p^{e-1}} \rangle$$

which gives $h_i' = 1$. Thus $h_i^g = h_i^{1+p^{e-1}}$. Let $h_j \in \{h_1, \ldots, h_r\}$ be such that $j > 1$, $o(h_j) = p^{e'}$, $e' \geq 2$, $e' < e$ but $h_j^g = h_j h_j'$, where $1 \neq h_j' \in \Omega_1(\langle h_j \rangle)$. Let $h_1' \in \langle h_1 \rangle$ be such that $o(h_1') = p^{e'}$ which gives that $(h_1')^g = h_1'$. But then

$$(h_1' h_j)^g = (h_1' h_j) h_j',$$

where $h_j' \notin \langle h_1' h_j \rangle$, a contradiction. Hence

$$h_j^g = h_j = h_j^{1+p^{e-1}}$$

and so for each $h \in H$, $h^g = h^{1+p^{e-1}}$, $\Omega_{e-1} = \mathrm{Z}(G)$, and we are done. □

§126

The existence of p-groups $G_1 < G$ such that $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G)$

Benjamin Sambale has constructed a 2-group G of order 32 which possesses a maximal subgroup G_1 such that $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G)$. We give here a simple proof of this fact which solves Problem 211 (for $p = 2$).

Theorem 126.1. *There exist* 2*-groups* $G_1 < G$ *with* $|G| = 32$ *and* $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G)$.

Proof. We construct our 2-group G as a splitting and faithful extension of its abelian normal subgroup $H = \langle a, b \mid a^4 = b^2 = [a, b] = 1\rangle$ of type $(4, 2)$ with a cyclic subgroup $\langle c\rangle \cong \mathrm{C}_4$ of order 4, where $a^c = a^{-1}b$ and $b^c = ba^2$. Then $\langle a^2\rangle = \mathrm{Z}(G)$ and c^2 inverts each element in H and so all elements in Hc^2 are involutions. Thus all elements in $G - (H\langle c^2\rangle) = Hc \cup Hc^{-1}$ are of order 4 and so $G_1 = H\langle c^2\rangle = \Omega_1(G)$ is a characteristic subgroup of G. Since

$$H = \Omega_2^*(G_1), \quad \langle a^2, b\rangle = \Omega_1(H), \quad \langle a^2\rangle = \mathfrak{V}_1(H) = \mathrm{Z}(G),$$

we conclude that H, $\langle a^2, b\rangle \cong \mathrm{E}_4$ and $\langle a^2\rangle$ are also characteristic subgroups of G. As $b = aa^c$, we have $G = \langle a, c\rangle$ and so G is given in terms of generators and relations as follows:

$$(*) \qquad G = \langle a, c \mid a^4 = c^4 = (aa^c)^2 = [a, aa^c] = 1,\ a^{c^2} = a^{-1}\rangle.$$

Note that $\langle a\rangle$ and $\langle ab\rangle$ are the only two cyclic subgroups of order 4 in H and since $\langle a\rangle^c = \langle a^c\rangle = \langle a^{-1}b\rangle = \langle ab\rangle$, we have $\mathrm{N}_G(\langle a\rangle) = G_1$. Hence for each $x \in G - G_1$ and $y \in H - \Omega_1(H)$, $\langle y\rangle$ and $\langle y^x\rangle$ are two distinct cyclic subgroups of order 4 in H, which gives that $\langle x, y\rangle = G$.

Each automorphism ψ of G sends a to one of $\{a, a^{-1}, ab, a^{-1}b\}$ and c is sent to one of 16 elements in $G - G_1$ which shows that $|\mathrm{Aut}(G)| \le 4 \cdot 16 = 64$. Conversely, take $a^\psi \in \{a, a^{-1}, ab, a^{-1}b\}$ (4 possibilities) and $c^\psi \in G - G_1 = Hc \cup Hc^{-1}$ (16 possibilities). We know from the previous paragraph that $\langle a^\psi, c^\psi\rangle = G$ and we verify that a^ψ and c^ψ satisfy all relations in $(*)$ (in place of a and c, respectively) and so $a \to a^\psi$, $c \to c^\psi$ induces an automorphism of G, hence $|\mathrm{Aut}(G)| = 4 \cdot 16 = 64$. Indeed, a^ψ and c^ψ are elements of order 4. Also, a^ψ and $(a^\psi)^{c^\psi}$ are two elements in $H - \Omega_1(H)$ so that $a^\psi(a^\psi)^{c^\psi} \in \Omega_1(H)$ and therefore $(a^\psi(a^\psi)^{c^\psi})^2 = 1$. Obviously, a^ψ and $(a^\psi)^{c^\psi}$ (lying in the abelian subgroup H) commute. Finally, $(c^\psi)^2 \in G_1 - H$

and so $(c^\psi)^2$ is an involution which inverts each element in H and therefore we obtain $(a^\psi)^{(c^\psi)^2} = (a^\psi)^{-1}$.

It is easy to show that $|\mathrm{Aut}(G_1)| = 64$. We have

$$(**) \qquad G_1 = \langle a, b, d = c^2 \mid a^4 = b^2 = [a, b] = d^2 = 1,\ a^d = a^{-1},\ b^d = b \rangle,$$

and for each $\phi \in \mathrm{Aut}(G_1)$ we conclude that $a^\phi \in \{a, a^{-1}, ab, a^{-1}b\}$ (4 possibilities), $b^\phi \in \{b, ba^2\}$ (2 possibilities) and $d^\phi \in G_1 - H$ (8 possibilities) which implies that $|\mathrm{Aut}(G_1)| \leq 4 \cdot 2 \cdot 8 = 64$. For the converse, if we consider $a^\phi \in \{a, a^{-1}, ab, a^{-1}b\}$, $b^\phi \in \{b, ba^2\}$ and $d^\phi \in G_1 - H$, then obviously $\langle a^\phi, b^\phi, d^\phi \rangle = G_1$ and a^ϕ, b^ϕ, d^ϕ satisfy all relations in $(**)$ since each element in $G_1 - H$ is an involution which inverts each element in H. We have proved that $|\mathrm{Aut}(G_1)| = 64$.

It remains to show $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G)$. First we determine the structure of $\mathrm{Aut}(G)$. The restriction of $\mathrm{Aut}(G)$ to H provides a homomorphism $f : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$. If $\psi \in \ker(f)$, then

$$a^\psi = a, \quad b = b^\psi = (ac^{-1}ac)^\psi = a(c^\psi)^{-1}ac^\psi$$

which gives $a^{c^\psi} = a^{-1}b = a^c$ and so $c^\psi \in Hc$. We may set $\psi = \psi_h$ with $a^{\psi_h} = a$ and $c^{\psi_h} = hc$ $(h \in H)$ so that $\ker(f) = \{\psi_h \mid h \in H\}$. The map $\psi_h \to h$ $(h \in H)$ is an isomorphism from $\ker(f)$ onto H and so $\ker(f) \cong \mathrm{C}_4 \times \mathrm{C}_2$ and $\mathrm{Aut}(G)/\ker(f) \cong \mathrm{Aut}(H) \cong \mathrm{D}_8$ and therefore f is a homomorphism from $\mathrm{Aut}(G)$ onto $\mathrm{Aut}(H)$. Now we construct a complement of $\ker(f)$ in $\mathrm{Aut}(G)$. Define

$$L = \langle \alpha, \beta \in \mathrm{Aut}(G), \text{ where } a^\alpha = ab,\ c^\alpha = c \text{ and } a^\beta = a,\ c^\beta = c^{-1} \rangle.$$

Then

$$\begin{aligned} a^{\alpha^2} &= (ab)^\alpha = (a \cdot ac^{-1}ac)^\alpha = (a^2c^{-1}ac)^\alpha \\ &= a^2(c^{-1} \cdot ab \cdot c) = a^2 \cdot a^{-1}b \cdot ba^2 = a^{-1} \end{aligned}$$

and $c^{\alpha^2} = c$ so that $o(\alpha) = 4$ and obviously $o(\beta) = 2$. Then we show that $(\alpha\beta)^2 = 1$. Indeed,

$$a^{\alpha\beta} = (ab)^\beta = ab^\beta = a(ac^{-1}ac)^\beta = a \cdot acac^{-1} = a^2cac^{-1}$$

and $c^{\alpha\beta} = c^{-1}$. This gives (noting that $a^2 \in \mathrm{Z}(G)$)

$$\begin{aligned} a^{(\alpha\beta)^2} &= (a^2cac^{-1})^{\alpha\beta} = (a^2cac^{-1})^2c^{-1}(a^2cac^{-1})c \\ &= a^2cac^{-1} \cdot a^2cac^{-1} \cdot c^{-1} \cdot a^2ca = a^2ca^2c^{-1}a = a \end{aligned}$$

and $c^{(\alpha\beta)^2} = c$ which shows $(\alpha\beta)^2 = 1$. We have proved that $L = \langle \alpha, \beta \mid \alpha^4 = \beta^2 = (\alpha\beta)^2 = 1 \rangle \cong \mathrm{D}_8$. Since $\mathrm{Z}(L) = \langle \alpha^2 \rangle$ and $\alpha^2 \notin \ker(f)$, we get $\ker(f) \cap L = \{1\}$. Thus we have shown so far that $\mathrm{Aut}(G)$ is a semidirect product of $\ker(f) \cong H$ and

$L \cong \mathrm{Aut}(H) \cong \mathrm{D}_8$. It is easy to justify that $\mathrm{C}_{\mathrm{Aut}(G)}(\ker(f)) = \ker(f)$. Indeed, if we have $\mathrm{C}_{\mathrm{Aut}(G)}(\ker(f)) > \ker(f)$, then α^2 centralizes $\ker(f)$. In particular, we obtain that $\alpha^2\psi_a = \psi_a\alpha^2$. But $c^{\alpha^2\psi_a} = c^{\psi_a} = ac$ and $c^{\psi_a\alpha^2} = (ac)^{\alpha^2} = a^{-1}c$, a contradiction. We have proved that $\mathrm{Aut}(G)$ is isomorphic to the holomorph of $H \cong \mathrm{C}_4 \times \mathrm{C}_2$.

Now we determine the structure of $\mathrm{Aut}(G_1)$, where G_1 is given in $(**)$. The restriction of $\mathrm{Aut}(G_1)$ to H gives rise to a homomorphism $f_0 : \mathrm{Aut}(G_1) \to \mathrm{Aut}(H)$ with

$$\ker(f_0) = \{\phi_h \mid h \in H\}, \text{ where } a^{\phi_h} = a,\ b^{\phi_h} = b,\ d^{\phi_h} = hd.$$

The map $\phi_h \to h$ $(h \in H)$ gives an isomorphism $\ker(f_0) \cong H$. Thus we conclude $\mathrm{Aut}(G_1)/\ker(f_0) \cong \mathrm{Aut}(H) \cong \mathrm{D}_8$. The automorphisms $\psi \in \mathrm{Aut}(G_1)$ with $d^\psi = d$ form a complement $L_0 \cong \mathrm{D}_8$ of $\ker(f_0)$ in $\mathrm{Aut}(G_1)$. Let $\psi \in L_0$ with $a^\psi = a^{-1}b$, $b^\psi = ba^2$ so that ψ^2 inverts each element in H and therefore $\langle\psi^2\rangle = \mathrm{Z}(L_0)$. In case $\mathrm{C}_{\mathrm{Aut}(G_1)}(\ker(f_0)) > \ker(f_0)$, we infer that ψ^2 centralizes $\ker(f_0)$. In particular, we have $\phi_a\psi^2 = \psi^2\phi_a$. But then $d^{\phi_a\psi^2} = (ad)^{\psi^2} = a^{-1}d$ and $d^{\psi^2\phi_a} = d^{\phi_a} = ad$, a contradiction. Hence $\mathrm{C}_{\mathrm{Aut}(G_1)}(\ker(f_0)) = \ker(f_0)$ and so $\mathrm{Aut}(G_1)$ is also isomorphic to the holomorph of $H \cong \mathrm{C}_4 \times \mathrm{C}_2$ and we are done. □

A similar example was presented in [Li4].

§127

On 2-groups containing a maximal elementary abelian subgroup of order 4

In the following theorem Problem 1591 is solved.

Theorem 127.1 (Janko). *Let G be a 2-group which contains a maximal elementary abelian subgroup A of order 4. If G contains also an elementary abelian subgroup E of order 16, then G is isomorphic to one of the groups of Theorem 49.3.*[1]

Proof. By Exercise 51 in Appendix 40, G has no normal elementary abelian subgroup of order 8. Due to Exercise 52 in Appendix 40, every subgroup of G is generated by four elements. In particular, G has no elementary abelian subgroup of order > 16. Obviously, G is neither abelian nor a 2-group of maximal class. Then G possesses a normal four-subgroup U. If $A \leq \mathrm{Z}(G)$, then AE is elementary abelian of order > 16, contrary to what has just been said. Therefore, since A is a maximal elementary abelian subgroup of G, it follows that $\Omega_1(\mathrm{Z}(G)) < A$ and so, in particular, $\mathrm{Z}(G)$ is cyclic. Set $\langle z\rangle = \Omega_1(\mathrm{Z}(G))$; then we have $\langle z\rangle \leq A \cap U$ and $|G : \mathrm{C}_G(U)| = 2$. Note that $|E \cap \mathrm{C}_G(U)| \geq 8$ and so $A \neq U$ which gives $A \cap U = \langle z\rangle$. But then $A \not\leq \mathrm{C}_G(U)$ and so $A \cap \mathrm{C}_G(U) = \langle z\rangle$. Let $t \in A - \mathrm{C}_G(U)$ so that

$$\mathrm{C}_G(t) = \langle t\rangle \times \mathrm{C}_{\mathrm{C}_G(U)}(t)$$

by the modular law, and therefore z is the only involution in $L = \mathrm{C}_{\mathrm{C}_G(U)}(t)$ (indeed, if $z \in F < \mathrm{C}_{\mathrm{C}_G(U)}(t)$, where F is abelian of type $(2, 2)$, then $A < \langle t, F\rangle \cong \mathrm{E}_8$, contrary to the hypothesis). Hence L is either cyclic of order 2^m, $m \geq 2$, or L is generalized quaternion. Indeed, if L is cyclic of order 2, then G would be of maximal class (Proposition 1.8), a contradiction.

Suppose that $L \cong \mathrm{C}_{2^m}$, $m \geq 2$. By Theorem 48.1, in that case G does not possess an elementary abelian subgroup of order 16.

Hence we have $L \cong \mathrm{Q}_{2^m}$, $m \geq 3$, and then G is isomorphic to one of the groups from Theorem 49.3 and we are done. □

Thus the groups from Theorem 127.1 are determined up to isomorphism.

[1] In Theorem 49.3 the 2-groups G containing an involution t such that $\mathrm{C}_G(t) = \langle t\rangle \times Q$, where Q is a generalized quaternion group, are classified if G also possesses an elementary abelian subgroup of order 16.

Remark. Let t be an element of order p of a p-group G such that $\mathrm{C}_G(t) = \langle t \rangle \times Q$, where $|\Omega_1(Q)| = p$ is a generalized quaternion group. Then $\Omega_1(\mathrm{C}_G(t)) \cong \mathrm{E}_{p^2}$ is a maximal elementary abelian subgroup of G. In that case, G has no normal subgroup of order p^{p+1} and exponent p (see Exercise 51 in Appendix 40). Now, if $p = 2$, by the proof of the theorem, G has no elementary abelian subgroup of order 2^5 by Exercise 52 in Appendix 40.

G. Glauberman and N. Mazza have proved that if $p > 2$ and a p-group G possesses a maximal elementary abelian subgroup of order p^2, then it has no elementary abelian subgroup of order p^{p+1}. As the symmetric group S_{p^2}, $p > 2$, shows, this estimate is best possible.

Exercise. Suppose that a p-group G, $p > 2$, possesses a maximal elementary abelian subgroup A of order p^2. If there is in G an elementary abelian subgroup E of order p^3, then there is $a \in A^{\#}$ such that $\mathrm{C}_G(a) = \langle a \rangle \times Q$, where Q has exactly one subgroup of order p. Next, G has no normal subgroup of order p^{p+1} and exponent p (compare with Glauberman–Mazza's result from the paragraph preceding the exercise). In view of Theorem 13.7, one may assume that $E \lhd G$. In that case, AE is of maximal class and order p^4. Assume, in addition, that $p > 3$; then $\exp(AE) = p$. Let $AE \leq H \leq G$, where H is as large as possible among all subgroups of exponent p. As $\mathrm{C}_H(A) = A$, it follows that H is of maximal class (Proposition 1.8), so $|H| \leq p^p$ (Theorem 9.5).

§128

The commutator subgroup of p-groups with the subgroup breadth 1

Recall that the subgroup breadth $\mathrm{sb}(G)$ of a p-group G is defined by

$$p^{\mathrm{sb}(G)} = \max\{|G : \mathrm{N}_G(H)| \mid H \leq G\}.$$

This section is a continuation of §122 and here we prove some results which are crucial on the way of classifying completely p-groups G with $\mathrm{sb}(G) = 1$.

Theorem 128.1. *If a p-group G has the subgroup breadth 1, then $|G'| \leq p^2$.*

Proof. By Propositions 122.8 and 122.16, the element breadth $\mathrm{b}(G)$ of G is at most 2. Recall that the element breadth $\mathrm{b}(G)$ of a p-group G is defined by

$$p^{\mathrm{b}(G)} = \max\{|G : \mathrm{C}_G(x)| \mid x \in G\}.$$

If $\mathrm{b}(G) = 1$, then by Proposition 121.9 (Knoche), $|G'| = p$. We may assume in the sequel that $\mathrm{b}(G) = 2$. Then we use Theorem 121.1 (Parmeggiani–Stellmacher) and conclude that we must be in part (b) of that theorem (otherwise, $|G'| = p^2$ and we are finished) which implies that $|G'| = p^3$ and $|G : \mathrm{Z}(G)| = p^3$.

By Proposition 122.2, $\Phi(G)$ is abelian. Let A be a maximal normal abelian subgroup of G containing $\Phi(G)$ so that $G/A \neq \{1\}$ is elementary abelian. If $|G/A| = p$, then Lemma 1.1 gives $|G| = p|\mathrm{Z}(G)||G'|$, which contradicts $|G'| = |G : \mathrm{Z}(G)| = p^3$. Hence $|G/A| \geq p^2$. But $\mathrm{Z}(G) < A$ and so $G/A \cong \mathrm{E}_{p^2}$ and $|A : \mathrm{Z}(G)| = p$. For each $x \in G - A$, $x^p \in \mathrm{Z}(G)$ and so $G/\mathrm{Z}(G)$ is of order p^3 and exponent p. Also, for each $x \in G - A$, $\mathrm{C}_A(x) = \mathrm{Z}(G)$ and so $|[A, x]| = p$ (Lemma 121.2) and $[A, x] \leq \mathrm{Z}(G)$ since $A/\mathrm{Z}(G) \leq \mathrm{Z}(G/\mathrm{Z}(G))$.

(i) First assume that $G/\mathrm{Z}(G)$ is nonabelian.

Then $p > 2$ and $G/\mathrm{Z}(G) \cong \mathrm{S}(p^3)$ (the nonabelian group of order p^3 and exponent p). Since G' covers $A/\mathrm{Z}(G)$, we get $|G' \cap \mathrm{Z}(G)| = p^2$. For any $x, y \in G - A$ such that $A\langle x, y\rangle = G$ we have $[A, x] \neq [A, y]$. Indeed, if $[A, x] = [A, y]$, then we obtain $A/[A, x] = \mathrm{Z}(G/[A, x])$ which implies that $G/[A, x]$ has (at least) two distinct abelian maximal subgroups. But then $|(G/[A, x])'| = p$ and then $|G'| = p^2$, a contradiction. Hence if G_i/A, $i = 1, 2, \ldots, p + 1$, are $p + 1$ pairwise distinct subgroups of order p in G/A, then $[A, G_i] = [G', G_i]$ $(i = 1, 2, \ldots, p + 1)$ are $p + 1$ pairwise distinct subgroups of order p in $G' \cap \mathrm{Z}(G)$ so that $G' \cap \mathrm{Z}(G) \cong \mathrm{E}_{p^2}$. On the other hand,

for each $x \in A - \mathrm{Z}(G)$ we have $\mathrm{C}_G(x) = A$ which shows that there are no elements of order p in $A - \mathrm{Z}(G)$. In particular, all elements in the set $G' - \mathrm{Z}(G)$ are of order p^2. Let $a \in G' - \mathrm{Z}(G)$ and then set $z = a^p$ so that $\mathfrak{V}_1(G') = \langle z \rangle$ and G' is abelian of type (p^2, p).

Let M be any maximal subgroup of G which contains $\mathrm{Z}(G)$. Since $G' \leq M$, we must have $M > A$. This simple remark will be used often in the following arguments.

Let $g \in G - A$ be such that $[a, g] = z$. Then $g^p \in \mathrm{Z}(G)$ and $\mathrm{C}_G(g) = \mathrm{Z}(G)\langle g \rangle$. Indeed, we have $\mathrm{C}_A(g) = \mathrm{Z}(G)$ and so if $\mathrm{C}_G(g) > \mathrm{Z}(G)\langle g \rangle$, then $\mathrm{C}_G(g)$ covers G/A and so $\mathrm{C}_G(g)$ would be a maximal subgroup of G containing $\mathrm{Z}(G)$ but not containing A, contrary to our simple remark from the previous paragraph. On the other hand, $|\mathrm{N}_G(\langle g \rangle) : \mathrm{C}_G(g)| = p$ and so $o(g) \geq p^2$ and $\mathrm{N}_G(\langle g \rangle) = A\langle g \rangle$. Indeed, if $\langle g \rangle \trianglelefteq G$, then $A/\mathrm{Z}(G)$ and $(\mathrm{Z}(G)\langle g \rangle)/\mathrm{Z}(G)$ are two distinct normal subgroups of order p in the factor group $G/\mathrm{Z}(G)$, contrary to $G/\mathrm{Z}(G) \cong \mathrm{S}(p^3)$. Also, if $\mathrm{N}_G(\langle g \rangle) \neq A\langle g \rangle$, then $\mathrm{N}_G(\langle g \rangle)$ is a maximal subgroup of G which contains $\mathrm{Z}(G)$ but does not contain A, contrary to our simple remark.

We have proved that $\langle a \rangle$ normalizes $\langle g \rangle$. Since $[a, g] = z$, we have $\Omega_1(\langle g \rangle) = \langle z \rangle$. If $o(g) \geq p^3$, then there is an element $h \in \langle g^p \rangle \leq \mathrm{Z}(G)$ such that $o(h) = p^2$ and $h^p = z^{-1}$. But then $ah \in A - \mathrm{Z}(G)$ and $(ah)^p = a^p h^p = zz^{-1} = 1$, a contradiction. Hence $o(g) = p^2$ and $1 \neq g^p \in \langle z \rangle$. We get $\langle a, g \rangle = U \cong \mathrm{M}_{p^3}$ with $U \cap A = \langle a \rangle$. Since $\Omega_1(U) \cong \mathrm{E}_{p^2}$, there is an element g' of order p in $U - A$. But then we must have $\mathrm{C}_A(g') = \mathrm{Z}(G)$ and $|G : \mathrm{C}_G(g')| = p$ which shows that $\mathrm{C}_G(g')$ covers G/A. Hence $\mathrm{C}_G(g')$ is a maximal subgroup of G containing $\mathrm{Z}(G)$ but not containing A, contrary to our simple remark.

(ii) Assume that $G/\mathrm{Z}(G)$ is abelian.

In that case, we get $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^3}$ and so $\Phi(G) \leq \mathrm{Z}(G)$. For any $x, y \in G$ we have $[x, y]^p = [x^p, y] = 1$ and so $G' \cong \mathrm{E}_{p^3}$. If there is an element $x \in G - \mathrm{Z}(G)$ of order p, then we infer that $|G : \mathrm{C}_G(x)| = p$ and so $\mathrm{C}_G(x)$ is an abelian maximal subgroup of G, a contradiction. Hence $\Omega_1(G) \leq \mathrm{Z}(G)$. If $x, y, z \in G - \mathrm{Z}(G)$ are such that $G = \mathrm{Z}(G)\langle x, y, z \rangle$, then $G' = \langle [x, y], [x, z], [y, z] \rangle$.

Let h be any element in $G - \mathrm{Z}(G)$. Then $o(h) \geq p^2$ and $[\langle h \rangle, G] \cong \mathrm{E}_{p^2}$. We have $\mathrm{C}_G(h) = \mathrm{Z}(G)\langle h \rangle$ with $|G : \mathrm{C}_G(h)| = p^2$ because G has no abelian maximal subgroup. If $\langle h \rangle \trianglelefteq G$, then $[\langle h \rangle, G] \leq \langle h \rangle$ and so $[\langle h \rangle, G]$ is cyclic of order p^2, a contradiction. It follows that $|G : \mathrm{N}_G(\langle h \rangle)| = p$. Then we get

$$[\langle h \rangle, \mathrm{N}_G(\langle h \rangle)] \leq \langle h \rangle \cap [\langle h \rangle, G]$$

and so

$$\Omega_1(\langle h \rangle) \leq [\langle h \rangle \cap G].$$

We have proved the following fact which will be used often in the following arguments:

(∗) For each $h \in G - \mathrm{Z}(G)$ we have $\Omega_1(\langle h \rangle) \leq [\langle h \rangle, G] \leq G'$.

(ii1) Suppose that $p > 2$.

Amongst all elements in $G - \mathrm{Z}(G)$ let a be one of smallest possible order p^m, $m \geq 2$. Then we set $t_1 = a^{p^{m-1}}$ so that (by $(*)$) $t_1 \in G'$. Further, let b be any element in $G - (\mathrm{Z}(G)\langle a\rangle)$ such that $[a, b] = t_1$. From $(*)$ we conclude that such an element b exists. Let $c \in G - (\mathrm{Z}(G)\langle a, b\rangle)$ so that setting $t_2 = [a, c]$ and $t_3 = [b, c]$, we obtain $\langle t_1, t_2, t_3\rangle = G'$, where $\mathrm{Z}(G)\langle a, b, c\rangle = G$. Since $[b, a] = t_1^{-1}$ and $[b, c] = t_3$, we get $[\langle b\rangle, G] = \langle t_1, t_3\rangle$. As $[ab, a] = t_1^{-1}$ and $[ab, c] = t_2 t_3$, we have

$$[\langle ab\rangle, G] = \langle t_1, t_2 t_3\rangle.$$

First suppose that $o(b) > o(a) = p^m$. Then, using $(*)$, we get

$$\Omega_1(\langle b\rangle) = \Omega_1(\langle ab\rangle) = \langle t_1^{\alpha} t_3^{\beta}\rangle = \langle t_1^{\gamma}(t_2 t_3)^{\delta}\rangle = \langle t_1^{\gamma} t_2^{\delta} t_3^{\delta}\rangle,$$

where not both α and β are $\equiv 0 \pmod{p}$ and also not both γ and δ are $\equiv 0 \pmod{p}$. We get $\delta \equiv 0 \pmod{p}$ and then

$$\beta \equiv 0 \pmod{p}, \quad \alpha \not\equiv 0 \pmod{p}, \quad \gamma \not\equiv 0 \pmod{p}.$$

But then

$$b^p \in \mathrm{Z}(G), \quad o(b^p) \geq p^m, \quad \langle b^p\rangle \geq \langle t_1\rangle$$

which implies that there is an element $y \in \langle b^p\rangle$ such that $y^{p^{m-1}} = t_1^{-1}$. We obtain

$$(ay)^{p^{m-1}} = a^{p^{m-1}} y^{p^{m-1}} = t_1 t_1^{-1} = 1$$

and so $o(ay) \leq p^{m-1}$ and $ay \in G - \mathrm{Z}(G)$, which is a contradiction.

We have proved that for each $b \in G - \mathrm{Z}(G)$ with $[a, b] = t_1$ we have $o(b) = p^m$. It follows that for each $x \in \mathrm{Z}(G)$, $o(xb) = p^m$ and so $o(x) \leq p^m$ which gives that $\exp(\mathrm{Z}(G)) \leq p^m$. Hence all elements in $(\mathrm{Z}(G)\langle a\rangle) - \mathrm{Z}(G)$ are also of order p^m.

Since $[\langle b\rangle, G] = \langle t_1, t_3\rangle$, the fact stated in $(*)$ implies $b^{p^{m-1}} = t_1^{\alpha} t_3^{\beta}$, where not both α and β are $\equiv 0 \pmod{p}$. Then

$$(ab)^{p^{m-1}} = a^{p^{m-1}} b^{p^{m-1}} = t_1 \cdot t_1^{\alpha} t_3^{\beta} = t_1^{\alpha+1} t_3^{\beta} \in G'$$

and so the minimality of $o(b) = p^m$ yields that $o(ab) = p^m$ and $t_1^{\alpha+1} t_3^{\beta} \neq 1$. On the other hand, the fact that $[\langle ab\rangle, G] = \langle t_1, t_2 t_3\rangle$ gives together with $(*)$ that

$$(ab)^{p^{m-1}} = t_1^{\alpha+1} t_3^{\beta} = t_1^{\gamma}(t_2 t_3)^{\delta} = t_1^{\gamma} t_2^{\delta} t_3^{\delta},$$

where not both γ and δ are $\equiv 0 \pmod{p}$. We conclude that $\delta \equiv 0 \pmod{p}$ and then $\beta \equiv 0 \pmod{p}$ and

$$\gamma \equiv \alpha + 1 \pmod{p} \quad \text{with} \quad \alpha \not\equiv 0 \pmod{p} \quad \text{and} \quad \alpha + 1 \not\equiv 0 \pmod{p}.$$

Hence $b^{p^{m-1}} = t_1^{\alpha}$ and so, replacing b with $b' = b^{\eta}$, where $\eta\alpha \equiv -1 \pmod{p}$, we compute

$$(ab')^{p^{m-1}} = a^{p^{m-1}}(b')^{p^{m-1}} = t_1(b^{p^{m-1}})^{\eta} = t_1 t_1^{\alpha\eta} = t_1 t_1^{-1} = 1.$$

Since $ab' \notin \mathrm{Z}(G)$ and $o(ab') \leq p^{m-1}$, we get a contradiction to the minimality of $o(b) = p^m$.

(ii2) Assume that $p = 2$.

Amongst all elements in $G - \mathrm{Z}(G)$ let a be one of maximal possible order 2^m, $m \geq 2$. Then set $t_1 = a^{2^{m-1}}$ so that $(*)$ implies $t_1 \in [a, G]$. Let b be any element in $G - (\mathrm{Z}(G)\langle a\rangle)$ such that $[a, b] = t_1$. Take an element $c \in G - (\mathrm{Z}(G)\langle a, b\rangle)$ and set $t_2 = [a, c]$ and $t_3 = [b, c]$, where $G' = \langle t_1, t_2, t_3\rangle$. Since $[b, c] = t_3$ and $[b, a] = t_1$, $(*)$ implies $\Omega_1(\langle b\rangle) \leq \langle t_1, t_3\rangle$ and therefore $\Omega_1(\langle b\rangle) = \langle t_1^{\alpha} t_3^{\beta}\rangle$, where $\alpha, \beta \in \{0, 1\}$ and not both α and β are equal to 0. As $[c, b] = t_3$ and $[c, a] = t_2$, it follows from $(*)$ that $\Omega_1(\langle c\rangle) \leq \langle t_2, t_3\rangle$ and therefore $\Omega_1(\langle c\rangle) = \langle t_2^{\epsilon} t_3^{\eta}\rangle$, where $\epsilon, \eta \in \{0, 1\}$ and not both ϵ and η are equal to 0.

First assume $m = 2$ so that all elements in $G - \mathrm{Z}(G)$ are of order 4. We have

$$(ab)^2 = a^2 b^2 [b, a] = t_1 \cdot t_1^{\alpha} t_3^{\beta} \cdot t_1 = t_1^{\alpha} t_3^{\beta}, \quad [ab, a] = t_1, \quad [ab, c] = t_2 t_3,$$

and so $[ab, G] = \langle t_1, t_2 t_3\rangle$. Using $(*)$, we get $t_1^{\alpha} t_3^{\beta} \in \langle t_1, t_2 t_3\rangle$ and so $\beta = 0$, $\alpha = 1$, $(ab)^2 = t_1$, and $b^2 = t_1$. We have

$$(ac)^2 = t_1 \cdot t_2^{\epsilon} t_3^{\eta} \cdot t_2 = t_1 t_2^{\epsilon+1} t_3^{\eta}, \quad [ac, a] = t_2, \quad [ac, b] = t_1 t_3,$$

and so $[ac, G] = \langle t_2, t_1 t_3\rangle$. Again using $(*)$, we get $t_1 t_2^{\epsilon+1} t_3^{\eta} \in \langle t_2, t_1 t_3\rangle$ and so $\eta = 1$. We have

$$(bc)^2 = t_1 \cdot t_2^{\epsilon} t_3 \cdot t_3 = t_1 t_2^{\epsilon}, \quad [bc, b] = t_3, \quad [bc, a] = t_1 t_2$$

and so $[bc, G] = \langle t_3, t_1 t_2\rangle$. Applying $(*)$, we obtain that $t_1 t_2^{\epsilon} \in \langle t_3, t_1 t_2\rangle$, and so $\epsilon = 1$, $c^2 = t_2 t_3$. Finally, we have

$$(ab \cdot c)^2 = (ab)^2 c^2 [c, ab] = t_1 \cdot t_2 t_3 \cdot t_2 t_3 = t_1, \quad [abc, a] = t_1 t_2, \quad [abc, b] = t_1 t_3$$

and so $[abc, G] = \langle t_1 t_2, t_1 t_3\rangle$. Using $(*)$, we get $t_1 \in \langle t_1 t_2, t_1 t_3\rangle$, a contradiction.

We have proved that $m \geq 3$, where a is an element of maximal possible order 2^m in $G - \mathrm{Z}(G)$. Now suppose that for each $b \in G - (\mathrm{Z}(G)\langle a\rangle)$ such that $[a, b] = t_1$ we have always $o(b) = 2^m$. We get $b^{2^{m-1}} = t_1^{\alpha} t_3^{\beta}$, where not both α and β are equal to 0. Since $[ab, a] = t_1$, $[ab, c] = t_2 t_3$, we obtain (using $(*)$) $(ab)^{2^{m-1}} = t_1^{\gamma}(t_2 t_3)^{\delta}$, where not both γ and δ are equal 0. We note that $[a, ab] = t_1$ and so, by our assumption, we have $o(ab) = 2^m$. On the other hand,

$$(ab)^{2^{m-1}} = t_1 \cdot t_1^{\alpha} t_3^{\beta} = t_1^{\alpha+1} t_3^{\beta}.$$

Hence $t_1^{\alpha+1}t_3^{\beta} = t_1^{\gamma}t_2^{\delta}t_3^{\delta}$ and this implies $\delta = 0$ and then $t_1^{\alpha+1}t_3^{\beta} = t_1^{\gamma}$ gives $\beta = 0$ and $\alpha + 1 \equiv \gamma \pmod 2$. Since $\delta = 0$, we must have $\gamma = 1$ and then $\alpha = 0$. But then both α and β are equal to 0, a contradiction.

By the previous paragraph, we may take an element b in $G - (\mathrm{Z}(G)\langle a\rangle)$ such that $[a, b] = t_1$ and $o(b) < 2^m$. In that case, we have $(ab)^{2^{m-1}} = a^{2^{m-1}} = t_1$. It is easy to see that $\exp(\mathrm{Z}(G)) = 2^{m-1}$. Indeed, in any case, $\exp(\mathrm{Z}(G)) \leq 2^m$ since all elements in $G - \mathrm{Z}(G)$ are of order at most 2^m. Suppose that there is $z \in \mathrm{Z}(G)$ with $o(z) = 2^m$. Then $b' = bz$ is of order 2^m and since $[b', G] = [b, G] = \langle t_1, t_3\rangle$, we have (by $(*)$) $\Omega_1(\langle b'\rangle) \in \langle t_1, t_3\rangle$ and so

$$(b')^{2^{m-1}} = (b)^{2^{m-1}} z^{2^{m-1}} = z^{2^{m-1}} \in \langle t_1, t_3\rangle.$$

If $z^{2^{m-1}} \in \{t_3, t_1t_3\}$, then $(az)^{2^{m-1}} \in \{t_3, t_1t_3\}$, a contradiction as $[az, G] = \langle t_1, t_2\rangle$. Therefore $z^{2^{m-1}} = t_1$. However, $[c, G] = [cz, G] = \langle t_2, t_3\rangle$ and so $\Omega_1(\langle c\rangle) = t_2^{\epsilon}t_3^{\eta}$, where $\epsilon, \eta \in \{0, 1\}$ and not both ϵ and η are equal to 0 and $\Omega_1(\langle cz\rangle \leq \langle t_2, t_3\rangle$. In case $o(c) < 2^m$, we get $(cz)^{2^{m-1}} = t_1$, a contradiction. If $o(c) = 2^m$, then

$$c^{2^{m-1}} = t_2^{\epsilon}t_3^{\eta} \quad \text{and} \quad (cz)^{2^{m-1}} = t_2^{\epsilon}t_3^{\eta} \cdot t_1,$$

a contradiction. Hence $\exp(\mathrm{Z}(G)) = 2^{m-1}$ and so all elements in $\mathrm{Z}(G)a$ and $\mathrm{Z}(G)ab$ are of order 2^m and all elements in $\mathrm{Z}(G)b$ are of order $< 2^m$.

Consider ac, where $[ac, b] = t_1t_3$, $[ac, a] = t_2$ so that $[ac, G] = \langle t_2, t_1t_3\rangle$ and therefore (by $(*)$)

$$\Omega_1(\langle ac\rangle) \leq \langle t_2, t_1t_3\rangle.$$

On the other hand,

$$(ac)^{2^{m-1}} = t_1c^{2^{m-1}}.$$

If $c^{2^{m-1}} = 1$, then $(ac)^{2^{m-1}} = t_1$, a contradiction. Hence we have $o(c) = 2^m$ and so $c^{2^{m-1}} = t_2^{\epsilon}t_3^{\eta}$, where not both ϵ and η are equal 0. Then $(ac)^{2^{m-1}} = t_1t_2^{\epsilon}t_3^{\eta} \in \langle t_2, t_1t_3\rangle$ and so $\eta = 1$ and $c^{2^{m-1}} = t_2^{\epsilon}t_3$.

Consider $(ab)c$, where $[abc, a] = t_1t_2$, $[abc, c] = t_2t_3$ so that, by $(*)$,

$$\Omega_1(\langle abc\rangle) \leq \langle t_1t_2, t_2t_3\rangle.$$

On the other hand,

$$((ab)c)^{2^{m-1}} = t_1 \cdot t_2^{\epsilon}t_3 \in \langle t_1t_2, t_2t_3\rangle,$$

and so $\epsilon = 0$ and we get $c^{2^{m-1}} = t_3$ and $(abc)^{2^{m-1}} = t_1t_3$.

Finally, we consider bc, where $[bc, b] = t_3$, $[bc, a] = t_1t_2$ so that (by $(*)$)

$$\Omega_1(\langle bc\rangle) \leq \langle t_1t_2, t_3\rangle.$$

On the other hand, $(bc)^{2^{m-1}} = t_3$.

We see that $\langle b\rangle$ normalizes the subgroups

$$\langle a\rangle, \quad \langle ab\rangle, \quad \langle c\rangle, \quad \langle ac\rangle, \quad \langle bc\rangle, \quad \langle abc\rangle,$$

and all elements in the cosets

$$\mathrm{Z}(G)a, \quad \mathrm{Z}(G)ab, \quad \mathrm{Z}(G)c, \quad \mathrm{Z}(G)ac, \quad \mathrm{Z}(G)bc, \quad \mathrm{Z}(G)abc$$

are of order 2^m and they are also normalized by $\langle b\rangle$.

Let b_0 be an element of smallest possible order 2^s in $\mathrm{Z}(G)b$, where $2 \le s \le m-1$, $m \ge 3$. Then $b_0^{2^{s-1}} = t_1^{\alpha} t_3^{\beta}$, where neither α nor β are equal to 0. Since

$$a^{2^{m-1}} = t_1, \quad c^{2^{m-1}} = t_3, \quad (ac)^{2^{m-1}} = t_1 t_3,$$

there is an element x of order 2^s in one of the subgroups

$$\langle a^2\rangle, \quad \langle c^2\rangle, \quad \langle (ac)^2\rangle$$

so that $x \in \mathrm{Z}(G)$ and $x^{2^{s-1}} = t_1^{\alpha} t_3^{\beta}$. Then we get

$$(xb_0)^{2^{s-1}} = t_1^{\alpha} t_3^{\beta} \cdot t_1^{\alpha} t_3^{\beta} = 1$$

and so $o(xb_0) \le 2^{s-1}$ and $xb_0 \in \mathrm{Z}(G)b$, a final contradiction. Thus our theorem is proved. □

Theorem 128.2. *Let G be a p-group with the subgroup breadth 1 and let $p > 2$. Then G possesses an abelian maximal subgroup and G' (of order $\le p^2$) is elementary abelian.*

Proof. By Theorem 122.1(b), $|G : \mathrm{Z}(G)| \le p^3$. Due to Theorem 128.1, $|G'| \le p^2$. If $|G : \mathrm{Z}(G)| = p^2$, then $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ and this implies $|G'| = p$. In case $|G'| = p$, Proposition 122.13 yields $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$.

In what follows we may assume that $|G/\mathrm{Z}(G)| = p^3$ and $|G'| = p^2$. Also, we assume that G does not possess any abelian maximal subgroup. Let A be a maximal normal abelian subgroup of G containing $\Phi(G)$ (which is abelian) so that G/A is elementary abelian of order $\ge p^2$. As $\mathrm{Z}(G) < A$ and $|G/\mathrm{Z}(G)| = p^3$, we have $G/A \cong \mathrm{E}_{p^2}$ and $|A : \mathrm{Z}(G)| = p$. For any $g \in G - A$, $g^p \in \mathrm{Z}(G)$ and so $G/\mathrm{Z}(G)$ is of order p^3 and exponent p.

(i) First assume that $G/\mathrm{Z}(G)$ is nonabelian and so $G/\mathrm{Z}(G) \cong \mathrm{S}(p^3)$ (the nonabelian group of order p^3 and exponent p).

Since G' covers $A/\mathrm{Z}(G)$, we infer that $G' \cap \mathrm{Z}(G) \cong \mathrm{C}_p$. For any $x \in A - \mathrm{Z}(G)$, $\mathrm{C}_G(x) = A$ which implies $o(x) \ge p^2$.

Suppose that there is an element $y \in G - A$ of order p. As $\mathrm{C}_A(y) = \mathrm{Z}(G)$, it follows that that $\mathrm{C}_G(y)$ must cover G/A, which contradicts the structure of $G/\mathrm{Z}(G) \cong \mathrm{S}(p^3)$. We have proved that $\Omega_1(G) \le \mathrm{Z}(G)$. In particular, $G' = \langle a\rangle \cong \mathrm{C}_{p^2}$ and set $a^p = z$. Let $g \in G - A$ so that $o(g) \ge p^2$ and $1 \ne g^p \in \mathrm{Z}(G)$. As $[g,a] \ne 1$ and $[g,a] \in \mathrm{Z}(G)$, we have $\langle [g,a]\rangle = \langle z\rangle$, $\langle g,a\rangle' = \langle z\rangle$ and $\langle g,a\rangle$ is minimal nonabelian. Then replacing g with g^i for some $i \not\equiv 0 \pmod p$ (if necessary), we may assume that $[g,a] = z$.

If $\langle g\rangle \trianglelefteq G$, then $A/\mathrm{Z}(G)$ and $(\langle g\rangle \mathrm{Z}(G))/\mathrm{Z}(G)$ would be two distinct normal subgroups of order p in $G/\mathrm{Z}(G) \cong \mathrm{S}(p^3)$, a contradiction. Hence $|G : \mathrm{N}_G(\langle g\rangle)| = p$. If $\mathrm{N}_A(\langle g\rangle) = \mathrm{Z}(G)$, then $\mathrm{N}_G(\langle g\rangle)$ must cover G/A and $\mathrm{N}_G(\langle g\rangle) \cap A = \mathrm{Z}(G)$, contrary to the structure of $G/\mathrm{Z}(G)$. It follows that $\mathrm{N}_G(\langle g\rangle) = A\langle g\rangle$ so that a normalizes $\langle g\rangle$ and so $[g, a] = z$ implies that $\Omega_1(\langle g\rangle) = \langle z\rangle$. If $o(g) \geq p^3$, then there is an element $l \in \langle g^p\rangle \leq \mathrm{Z}(G)$ such that $o(l) = p^2$ and $l^p = z^{-1}$. But then

$$(al)^p = a^p l^p = zz^{-1} = 1$$

and so $o(al) = p$ and $al \in A - \mathrm{Z}(G)$, a contradiction. Hence we have $o(g) = p^2$ and $\langle a, g\rangle \cong \mathrm{M}_{p^3}$ with $\langle a, g\rangle \cap A = \langle a\rangle$. On the other hand, $\Omega_1(\langle a, g\rangle) \cong \mathrm{E}_{p^2}$ and so there are elements of order p in $\langle a, g\rangle - A$, a contradiction.

(ii) Now assume that $G/\mathrm{Z}(G)$ is abelian and so $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^3}$.

Hence $\Phi(G) \leq \mathrm{Z}(G)$ and so for any $x, y \in G$ we have $[x, y]^p = [x^p, y] = 1$ which implies that $G' \cong \mathrm{E}_{p^2}$. If $x, y \in G - \mathrm{Z}$ are such that $(\langle x, y\rangle \mathrm{Z}(G))/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$, then $[x, y] \neq 1$ since G has no abelian maximal subgroups.

Let $a, b \in G - \mathrm{Z}(G)$ be such that $(\langle a, b\rangle \mathrm{Z}(G))/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ which implies that $[a, b] = t_1 \neq 1$. Let c be an element in $G - (\langle a, b\rangle \mathrm{Z}(G))$ so that $\langle a, b, c\rangle \mathrm{Z}(G) = G$. Set $[a, c] = t_2 \neq 1$ and we claim that $\langle t_1, t_2\rangle = G'$. Indeed, suppose $t_2 = [a, c] = t_1^i$ for some $i \not\equiv 0 \pmod{p}$. Then

$$[a, b^{-i}c] = [a, b]^{-i}[a, c] = t_1^{-i} t_1^i = 1$$

and $(\langle a, b^{-i}c\rangle \mathrm{Z}(G))/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$, a contradiction.

Assume that $[b, c] = t_1^j$ for some $j \not\equiv 0 \pmod{p}$. Then we get

$$[b, a^j c] = [b, a]^j [b, c] = t_1^{-j} t_1^j = 1$$

which together with $(\langle b, a^j c\rangle \mathrm{Z}(G))/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ gives a contradiction. Thus we have proved that $[b, c] = t_1^\alpha t_2^\beta$, where $\beta \not\equiv 0 \pmod{p}$. As $\langle a^{-\beta} b, b^{\alpha\beta^{-1}} c, b\rangle \mathrm{Z}(G) = G$, we have

$$(\langle a^{-\beta} b, b^{\alpha\beta^{-1}} c\rangle \mathrm{Z}(G))/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}.$$

On the other hand,

$$[a^{-\beta} b, b^{\alpha\beta^{-1}} c] = [a, b]^{-\beta\alpha\beta^{-1}} [a, c]^{-\beta} [b, c] = t_1^{-\alpha} t_2^{-\beta} \cdot t_1^\alpha t_2^\beta = 1,$$

a contradiction.

We have proved that G possesses an abelian maximal subgroup A. Then $\mathrm{Z}(G) < A$ and $|A/\mathrm{Z}(G)| = p^2$. For each $x \in G - A$, $\mathrm{C}_A(x) = \mathrm{Z}(G)$ and so $x^p \in \mathrm{Z}(G)$. Hence $G/\mathrm{Z}(G)$ is generated by its elements of order p and therefore $\exp(G/\mathrm{Z}(G)) = p$. In particular, $A/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$. For a fixed element $g \in G - A$ the map

$$a \to [a, g] \quad (a \in A)$$

is a homomorphism from A into A with the kernel $\mathrm{C}_A(g) = \mathrm{Z}(G)$ and so

$$A/\mathrm{Z}(G) \cong \{[a, g] \mid a \in A\} = G'$$

which implies that $G' \cong \mathrm{E}_{p^2}$. Our theorem is proved. □

Theorem 128.3. *Let G be a 2-group with the subgroup breadth 1. Then G possesses a normal abelian subgroup of index 4.*

Proof. Suppose that this result is false. Then we get $|G/\mathrm{Z}(G)| \geq 2^4$ and so, by Theorem 122.1(a), $|G/\mathrm{Z}(G)| = 2^4$. Let A be a maximal normal abelian subgroup of G so that G/A is of order $\geq 2^3$. Since $\mathrm{Z}(G) < A$ and $|G/\mathrm{Z}(G)| = 2^4$, we have $|G/A| = 2^3$ and $|A/\mathrm{Z}(G)| = 2$.

By Proposition 122.16, the element breadth of G is at most 2. But if $a \in A - \mathrm{Z}(G)$, then $\mathrm{C}_G(a) = A$ and so $|G : \mathrm{C}_G(a)| = 2^3$, a contradiction. □

§129

On two-generator 2-groups with exactly one maximal subgroup which is not two-generator

By Theorem 71.6, a nonmetacyclic two-generator 2-group G contains an even number of two-generator maximal subgroups. We begin a study of the structure of that G provided it contains exactly two two-generator maximal subgroups (Problem 1969).

Theorem 129.1 (Janko). *Let G be a two-generator 2-group with exactly one maximal subgroup which is not two-generator. Then the other two maximal subgroups are either both metacyclic (and such groups G are completely determined in §87) or both are nonmetacyclic.*

Proof. Set $\Gamma_1 = \{A, B, C\}$, where $\mathrm{d}(C) \geq 3$. By Schreier's inequality (Appendix 25), we have $\mathrm{d}(C) = 3$. Since G is nonmetacyclic, G is nonabelian and $\mathrm{d}(A) = \mathrm{d}(B) = 2$. If both A and B are metacyclic, then such groups G are completely determined in §87. Therefore we may assume that A is nonmetacyclic and so A is nonabelian. In what follows we assume (by way of contradiction) that B is metacyclic.

Let $H \in \{A, B, C\}$. Then we have $\Phi(H) = \mho_1(H) \geq \mho_2(G)$. On the other hand, we infer that $\mho_2(A) \leq \mho_2(G)$ and $\mho_2(A) \trianglelefteq G$ so that $A/\mho_2(A)$ is two-generator and nonmetacyclic (Corollary 44.9). Also, $B/\mho_2(A)$ is metacyclic (but noncyclic) and $\mathrm{d}(C/\mho_2(A)) = 3$. Finally, $G/\mho_2(G)$ is nonmetacyclic (Corollary 44.9) and therefore $G/\mho_2(A)$ is nonmetacyclic with $\mathrm{d}(G/\mho_2(A)) = 2$. It follows that we may assume that $\mho_2(A) = \{1\}$. Hence $\exp(A) = 4$ and so $\exp(G) \leq 8$.

Since B is metacyclic of exponent ≤ 8, we get $|B| \leq 2^6$. Suppose that $|B| = 2^6$. Then $B \cap A$ is a metacyclic subgroup of exponent 4 and order 2^5, a contradiction. Hence B is metacyclic of order $\leq 2^5$ and so $|G| \leq 2^6$.

If $|G| = 2^4$, then $|A| = 2^3$ which together with $\mathrm{d}(A) = 2$ implies that A is metacyclic, a contradiction. It follows that $|G| = 2^5$ or $|G| = 2^6$.

(i) First assume that $|G| = 2^5$. If $|A'| = 4$, then, by a result of O. Taussky (Lemma 1.6), A is of maximal class and so A is metacyclic, a contradiction. Hence $|A'| = 2$ which together with $\mathrm{d}(A) = 2$ implies that A is the nonmetacyclic minimal nonabelian group of order 2^4. Then we get $E = \Omega_1(A) \cong \mathrm{E}_8$ and $E \trianglelefteq G$. If $G/E \cong \mathrm{E}_4$, then $E = \Phi(G)$ (since $\mathrm{d}(G) = 2$) and so $E \leq B$, a contradiction (since B is metacyclic). Hence $G/E \cong \mathrm{C}_4$ and let $g \in G - A$ be such that $\langle g \rangle$ covers G/E. In that case, $g^2 \in A - E$ is of order 4 and so $o(g) = 8$ and $\langle g \rangle \cap E \cong \mathrm{C}_2$. Since $\mathrm{C}_A(E) = E$ and

$G/E \cong \mathrm{C}_4$, it follows that $\mathrm{C}_G(E) = E$ and $\Omega_1(G) = E$ so that G is a faithful and nonsplitting extension of $E \cong \mathrm{E}_8$ by C_4.

As $A = E\langle g^2\rangle$ is a unique maximal subgroup of G containing E, it follows that C does not contain E. Hence $C \cap E = U \cong \mathrm{E}_4$ and C covers G/E so that $C/U \cong \mathrm{C}_4$. But $\Omega_1(C) = U$ and so if $h \in C - U$ is such that $\langle h\rangle$ covers C/U, then $o(h) = 8$. It follows that C has a cyclic subgroup of index 2, contrary to $\mathrm{d}(C) = 3$.

(ii) It remains to consider the case $|G| = 2^6$. In this case, $|\Phi(G)| = 2^4$ and $\Phi(G)$ is a maximal subgroup of A. On the other hand, $\Phi(G) < B$ and B is metacyclic and so $\Phi(G)$ is a metacyclic group of exponent 4. Hence we have either $\Phi(G) \cong \mathrm{C}_4 \times \mathrm{C}_4$ or $\Phi(G) \cong \mathscr{H}_2 = \langle x, y \mid x^4 = y^4 = 1,\ x^y = x^{-1}\rangle$. In any case, $\Omega_1(\Phi(G)) \cong \mathrm{E}_4$ and $\mathfrak{V}_1(\Phi(G)) = \Omega_1(\Phi(G))$. Since A does not possess elements of order 8, we have for each $x \in A - \Phi(G)$, $x^2 \in \Omega_1(\Phi(G))$ which gives $\Phi(A) = \mathfrak{V}_1(A) = \Omega_1(\Phi(G))$, contrary to $\mathrm{d}(A) = 2$. Our theorem is proved. □

§130

Soft subgroups of p-groups

We present here some work of L. Hethelyi on soft subgroups of p-groups. A subgroup A of a nonabelian p-group G is called a *soft subgroup* if it satisfies $\mathrm{C}_G(A) = A$ and $|\mathrm{N}_G(A) : A| = p$. Note that a nonabelian p-group P is of maximal class if and only if P possesses a soft subgroup of order p^2.

Our induction arguments will be based on the following:

Lemma 130.1. *Let A be a soft subgroup in a nonabelian p-group G, $N = \mathrm{N}_G(A)$, and let K be the core of A in G, $\bar{G} = G/K$. Then $\bar{N}$ is soft in $\bar{G}$ and $\bar{N} = \bar{A} \times \mathrm{Z}(\bar{G})$. Moreover, $|N'| = p$ if $|G : A| > p$.*

Proof. We may assume that $G > N$. Obviously, $\bar{N} = \mathrm{N}_{\bar{G}}(\bar{A}) \geq \bar{A}\mathrm{Z}(\bar{G})$. Now we see that $\bar{A} \cap \mathrm{Z}(\bar{G})$ is normal in $\bar{G}$, hence trivial. Then $|\bar{N} : \bar{A}| = p$ implies the second assertion: $\bar{N} = \bar{A} \times \mathrm{Z}(\bar{G})$. We infer that $\mathrm{C}_{\bar{G}}(\bar{N}) \leq \mathrm{C}_{\bar{G}}(\bar{A}) \leq \mathrm{N}_{\bar{G}}(\bar{A}) = \bar{N}$, i.e., $\bar{N}$ is self-centralizing. Let us denote $N_2 = \mathrm{N}_G(N)$, so $\mathrm{N}_{\bar{G}}(\bar{N}) = \bar{N}_2$. For $x \in N_2 - N$, $A^x \neq A$ is a maximal subgroup in N, hence $A^x \cap A = \mathrm{Z}(N)$, $|N : \mathrm{Z}(N)| = p^2$, $|N'| = p$. Counting the conjugate subgroups A^x, $x \in N_2$, we obtain $|N_2 : N| = p$ (noting that N has at most $p + 1$ abelian maximal subgroups), thus $\bar{N}$ is soft in $\bar{G}$. □

Lemma 130.2. *Suppose that A is a soft subgroup in a nonabelian p-group G and set $|G : A| = p^n$, where $n \geq 1$. Then the subgroups of G containing A form a chain*

$$A = N_0 < N_1 < \cdots < N_{n-1} = M < N_n = G,$$

where $\mathrm{N}_G(N_{i-1}) = N_i$ and $|N_i : N_{i-1}| = p$, $i = 1, \ldots, n$.

Proof (see also Appendix 40, Exercise 72). By induction, Lemma 130.1 yields at once $|N_i : N_{i-1}| = p$. Now if $A \leq X \leq G$, then let N_j be the largest subgroup of our chain contained in X. Suppose $N_j < X$. Since $N_{j+1} = \mathrm{N}_G(N_j) = \mathrm{N}_X(N_j)$, we have $N_{j+1} \leq X$, a contradiction. Hence $N_j = X$. □

In what follows we shall use the notation introduced in Lemma 130.2. Moreover, for $X \leq Y$, $\mathrm{core}(X : Y)$ denotes the largest normal subgroup of Y contained in X and X^Y stands for the smallest normal subgroup of Y containing X.

Corollary 130.3. *For any $v \in G - M$ we have $\langle A, A^v \rangle = M$, where M is the unique maximal subgroup of G containing a soft subgroup A of G.*

Proof. By Lemma 130.2, we have $\langle A, A^v\rangle = N_j$ for some $j \le n-1$. Since $A \le N_j$ and $A \le N_j^{v^{-1}}$, it follows that v normalizes N_j. But from $\mathrm{N}_G(N_j) = N_{j+1}$ we infer $v \in N_{j+1}$ and so $N_j = M$. □

Corollary 130.4. *There exists $a \in A$ such that $\mathrm{C}_G(a) = A$, where A is a soft subgroup of G.*

Proof. As $A = \mathrm{C}_G(A) = \bigcap_{a\in A} \mathrm{C}_G(a)$, the assertion follows from Lemma 130.2. □

Proposition 130.5. *Let M be the unique maximal subgroup of a p-group G containing a soft subgroup A of G. For the upper central series of M we have:*

(i) $\mathrm{Z}_i(M) = \mathrm{core}(N_{i-1} : G) = N_{i-1} \cap N_{i-1}^v$ *for any* $v \in G - M$, $i = 1, \ldots, n$.

(ii) $\mathrm{Z}_{i+1}(M)/\mathrm{Z}_i(M)$ *is elementary abelian of order* $\le p^2$, $i = 1, \ldots, n-1$.

(iii) $\mathrm{Z}_i(G) \le \mathrm{Z}_i(M)$, $i = 1, \ldots, n$.

Proof. (i) For $i = 1$ we have $N_0 = A$ and let $v \in G - M$ be fixed. By Corollary 130.3, $\langle A, A^v\rangle = M$. Now, $\mathrm{Z}(M) = \mathrm{C}_M(A) \cap \mathrm{C}_M(A^v) = A \cap A^v$. Finally, Lemma 130.1 proves (i) by induction.

(ii) We have $\mathrm{Z}_i(M) = N_{i-1} \cap N_{i-1}^v \le N_{i-1} \cap N_i^v \le N_i \cap N_i^v = \mathrm{Z}_{i+1}(M)$. The index in both steps is 1 or p, so

$$|\mathrm{Z}_{i+1}(M)/\mathrm{Z}_i(M)| \le p^2.$$

If the index is p^2, inserting also $N_i \cap N_{i-1}^v$ in the middle, we see that the factor is elementary abelian. Indeed, $(N_{i-1} \cap N_i^v)/\mathrm{Z}_i(M)$ and $(N_i \cap N_{i-1}^v)/\mathrm{Z}_i(M)$ are two distinct subgroups of order p in $\mathrm{Z}_{i+1}(M)/\mathrm{Z}_i(M)$.

(iii) For $i = 1$ we have $\mathrm{Z}_1(G) \le \mathrm{core}(A : G) = \mathrm{Z}_1(M)$. Lemma 130.1 is again applicable and gives our result. □

Now, as a corollary to Proposition 130.5 (i) and (iii), we obtain:

Theorem 130.6. *Let A be a soft subgroup of a p-group G with $|G : A| = p^n$, where $n \ge 1$. Then there is a unique maximal subgroup M of G containing A. The nilpotence class of M is n and the nilpotence class of G is at least $n+1$. Since A is also soft in N_i, $i = 1, \ldots, n-1$, every above statement is also true for N_i.*

Corollary 130.7. *The nilpotence class of N_i is $i+1$ for $i = 0, \ldots, n-1$.*

Corollary 130.8. *We have $|A : \mathrm{core}(A : G)| \le p^{n-1}$.*

Proof. Making use of Proposition 130.5 (i) and (ii), we obtain

$$\begin{aligned} |A : \mathrm{core}(A : G)| &= p^{-n+1}|M : \mathrm{core}(A : G)| \\ &= p^{-n+1}|\mathrm{Z}_n(M) : \mathrm{Z}_1(M)| \\ &\le p^{-n+1}p^{2(n-1)} = p^{n-1}. \end{aligned}$$

□

Proposition 130.9. *Let M be the unique maximal subgroup of a p-group G containing a soft subgroup A of G. For the lower central series of M we have:*

(i) $\mathrm{K}_i(M) = \mathrm{n.cl.}(N'_{n+1-i} : G) = \langle N'_{n+1-i}, N'^{v}_{n+1-i} \rangle$ *for any $v \in G - M$, where $i = 2, \ldots, n$;*

(ii) $\mathrm{K}_i(M)/\mathrm{K}_{i+1}(M)$ *is elementary abelian of order $\leq p^2$, $i = 2, \ldots, n$.*

Proof. (i) Let $i = n$ and we may assume that $n > 1$. Since $\mathrm{K}_n(M)$ is normal in G, $\mathrm{K}_n(M) \leq \mathrm{Z}_1(M) \leq A$ and $\mathrm{cl}(M/\mathrm{K}_n(M)) = n-1$, Lemma 130.1 implies that the factor group $N_1/\mathrm{K}_n(M)$ is soft in $G/\mathrm{K}_n(M)$. Indeed, if $N_1/\mathrm{K}_n(M)$ is nonabelian, then $A\mathrm{K}_n(M)$ would be soft in $G/\mathrm{K}_n(M)$ and then $\mathrm{cl}(M/\mathrm{K}_n(M)) = n$. Hence we obtain that $N'_1 \leq \mathrm{K}_n(M)$. Conversely, for $T = \langle N'_1, N'^{v}_1 \rangle$ we have

$$\mathrm{Z}_2(M)/T = (N_1 \cap N_1^v)/T \leq \mathrm{Z}(\langle N_1, N_1^v \rangle/T) = \mathrm{Z}(M/T),$$

hence $\mathrm{cl}(M/T) < \mathrm{cl}(M)$, so $T \geq \mathrm{K}_n(M)$ also holds and therefore

$$\mathrm{K}_n(M) = \langle N'_1, N'^{v}_1 \rangle = \mathrm{n.cl.}(N'_1 : G).$$

Now, for $i < n$, (i) follows by backwards induction.

(ii) Suppose that $i = n$. Since we may assume that $n > 1$, Lemma 130.1 implies

$$|\mathrm{K}_n(M)| = |\langle N'_1, N'^{v}_1 \rangle| \leq |N'_1|^2 \leq p^2.$$

The result then follows by induction. □

Proposition 130.10. *Suppose that M is the unique maximal subgroup of a p-group G containing a soft subgroup A of G. For the series of commutator subgroups N'_i we have $N'_i A = N_{i-1}$, $i = 1, \ldots, n$ and so $N'_1 < N'_2 < \cdots < N'_n = G'$ and so, in particular, $G'A = M$.*

Proof. Clearly, we have $N'_i A \leq N_{i-1}$ and $N'_i A \trianglelefteq N_i$. Now Lemma 130.2 yields that $N'_i A = N_{i-1}$. □

Theorem 130.11. *Suppose that A and B are soft subgroups of a p-group G contained in the same maximal subgroup M of G. Then B is conjugate to A.*

Proof. Suppose that $|G : A| = p^2$. Then $|G/\mathrm{Z}(M)| = p^3$, $A/\mathrm{Z}(M) \not\leq \mathrm{Z}(G/\mathrm{Z}(M))$, $B/\mathrm{Z}(M) \not\leq \mathrm{Z}(G/\mathrm{Z}(M))$, and $|A/\mathrm{Z}(M)| = |B/\mathrm{Z}(M)| = p$. However, we obtain that $|M/\mathrm{Z}(M)| = p^2$ and so $A/\mathrm{Z}(M)$ is conjugate to $B/\mathrm{Z}(M)$. Thus, for $|G : A| = p^2$, A is conjugate to B.

Suppose that $|G : A| > p^2$. Set $N_1 = \mathrm{N}_G(A)$ and $\bar{G} = G/\mathrm{Z}(M)$ with bar convention. Then $\bar{N}_1$ and $\mathrm{N}_{\bar{G}}(\bar{B}) = \overline{\mathrm{N}_G(B)}$ are soft subgroups of $\bar{G}$ contained in $\bar{M}$ (by Proposition 130.5(i) and Lemma 130.1). By induction, $\mathrm{N}_{\bar{G}}(\bar{B})$ is conjugate to $\bar{N}_1$ and so $\mathrm{N}_G(B)$ is conjugate to N_1. Thus we can assume $B < N_1$. However, B is conjugate to A in $N_2 = \mathrm{N}_G(N_1)$ by the previous paragraph. □

Theorem 130.12. *Suppose that A is a maximal normal abelian subgroup of a nonabelian p-group G. Assume that G/A is cyclic and that G possesses a soft subgroup B distinct from A. Then $G = AB$.*

Proof. Suppose that this theorem is false. Since $A \neq B$, neither A nor B is of index p in G. As $AB < G$ and $AB \trianglelefteq G$, we get $|G : (AB)| = p$ and so $M = AB$ is the unique maximal subgroup of G containing B. We have $A \cap B = \mathrm{Z}(M) \trianglelefteq G$. Now set $N_1 = \mathrm{N}_G(B)$ so that $|N_1 : B| = p$ and $N_1 \leq M$. Let $x \in G - N_1$ be such that x normalizes N_1. Then $B \cap B^x = \mathrm{Z}(N_1) \geq \mathrm{Z}(M)$ and $|B : \mathrm{Z}(N_1)| = p$. Set $R = A\mathrm{Z}(N_1)$; then $R \trianglelefteq G$ and $G/R \cong \mathrm{C}_{p^2}$. Since $\mathrm{C}_G(B) = B$, we have for each $b \in B - \mathrm{Z}(N_1)$, $\mathrm{C}_G(b) = B$. Let $|B| = p^k$ and $|M| = p^n$ so that

$$|B - \mathrm{Z}(N_1)| = p^k - p^{k-1} = p^{k-1}(p-1)$$

and

$$|M - R| = p^n - p^{n-1} = p^{n-1}(p-1).$$

Note that all conjugates in G of the subset $B - \mathrm{Z}(N_1)$ lie in $M - R$ and there are exactly $|G : \mathrm{N}_G(B)| = |G : N_1| = p^{n+1}/p^{k+1} = p^{n-k}$ such distinct conjugates.

For any $g \in G - N_1$ we have $(B - \mathrm{Z}(N_1)) \cap (B - \mathrm{Z}(N_1))^g = \varnothing$ since for each $b \in B - \mathrm{Z}(N_1)$, $\mathrm{C}_G(b) = B$. Hence the number of elements contained in the union of all these conjugates is $p^{n-k} \cdot p^{k-1}(p-1) = p^{n-1}(p-1)$, which is the number of all elements contained in $M - R$. It follows that each element $y \in M - R$ is conjugate in G to an element $b \in B - \mathrm{Z}(N_1)$ and so $\mathrm{C}_G(y) \leq M$. On the other hand, $G/R \cong \mathrm{C}_{p^2}$ and so if $v \in G - M$, then $v^p \in M - R$ but $\mathrm{C}_G(v^p) \not\leq M$, a contradiction. Our theorem is proved. □

Theorem 130.13. *Suppose that A is a maximal normal abelian subgroup of a nonabelian p-group G. Assume that G/A is cyclic and that G possesses a soft subgroup B distinct from A. Then we have:*

(i) $\mathrm{d}(G/\mathrm{Z}(G)) = 2$, *and if* $|G : A| = p^\alpha$, *then* $G/(G'\mathrm{Z}(G))$ *is of type* (p^α, p).

(ii) *G is a CF-group, i.e., the index of any term of the lower central series of G beyond G' in its predecessor is at most p.*

Proof. (i) By Theorem 130.12, we have $G = AB$ and so $\mathrm{Z}(G) = A \cap B$. Let M be the unique maximal subgroup of G containing B. We have $G' \leq A \cap M$. On the other hand, $G'B$ is a normal subgroup of G containing B and so $G'B = M$ which implies $A \cap M = G'\mathrm{Z}(G)$. Since

$$G/(G'\mathrm{Z}(G)) = A/(G'\mathrm{Z}(G)) \times M/(G'\mathrm{Z}(G)),$$

we infer that $G/(G'\mathrm{Z}(G))$ is of type (p^α, p). Take an element $b \in B - \mathrm{Z}(G)$ so that $\langle b \rangle$ covers $B/\mathrm{Z}(G)$ and take an element $a \in A - M$. Then $\langle b \rangle$ covers G/A and

$$G = \langle a, b \rangle (A \cap M) = \langle a, b \rangle G'\mathrm{Z}(G) = \langle a, b \rangle \mathrm{Z}(G)$$

which implies $\mathrm{d}(G/\mathrm{Z}(G)) = 2$.

(ii) Since $a^p \in G'\mathrm{Z}(G)$, we have $[a^p, b] \in \mathrm{K}_3(G)$. Now

$$[a^p, b] = a^{-p}(b^{-1}a^p b) = a^{-p}(a^p)^b = (a^{-1}a^b)^p = [a, b]^p,$$

so $[a, b]^p \in \mathrm{K}_3(G)$. Since $G' = \langle [a, b], \mathrm{K}_3(G)\rangle$, $|G' : \mathrm{K}_3(G)| = p$. It follows by an easy induction that $|\mathrm{K}_i(G) : \mathrm{K}_{i+1}(G)| = p$ for $\mathrm{K}_i(G) \neq \{1\}$: in fact, if $i \geq 3$ and $\mathrm{K}_{i-1}(G) = \langle u, \mathrm{K}_i(G)\rangle$ with $u^p \in \mathrm{K}_i(G)$, then $\mathrm{K}_i(G) = \langle [a, u], [b, u], \mathrm{K}_{i+1}(G)\rangle$ and $[a, u] = 1$ as $u \in G' \leq A$ and $a \in A$. Also, we obtain that $[b, u]^p \in \mathrm{K}_{i+1}(G)$ since $[b, u]^p = (u^b)^{-p}u^p = [b, u^p] \in \mathrm{K}_{i+1}(G)$. Indeed,

$$[b, u^p] = (b^{-1}u^{-p}b)u^p = (b^{-1}u^{-1}b)^p u^p = ((u^{-1})^b u)^p = [b, u]^p$$

since $u \in G'$, $(u^{-1})^b \in G'$ and $G' \leq A$. Thus G is a CF-group. □

Theorem 130.14. *Suppose that G is a p-group of class greater than 2 and A is an abelian subgroup of G of index p. Then the following are equivalent:*

(a) *Every maximal abelian subgroup of G is soft.*

(b) *G has a soft subgroup distinct from A.*

(c) *$G/\mathrm{Z}(G)$ is a p-group of maximal class.*

(d) $|\mathrm{Z}_2(G) : \mathrm{Z}(G)| = p$.

Proof. The implication (a) ⇒ (b) is trivial.

(b) ⇒ (c). By Theorem 130.13, G is a CF-group and $G/(G'\mathrm{Z}(G))$ is of type (p, p). If $\bar{G} = G/\mathrm{Z}(G)$, then $\bar{G}/\bar{G}'$ is of type (p, p) and $\bar{G}$ is a CF-group, so $\bar{G}$ is of maximal class.

The implication (c) ⇒ (d) is trivial.

(d) ⇒ (a). Let $B \neq A$ be an abelian maximal subgroup of G so that $AB = G$ and $A \cap B = \mathrm{Z}(G)$. Set $N = \mathrm{N}_G(B)$ so that $N = (N \cap A)B$. We have $[N \cap A, B] \leq B \cap A = \mathrm{Z}(G)$ so $N \cap A \leq \mathrm{Z}_2(G)$. Hence $|N : B| = |(N \cap A) : \mathrm{Z}(G)| = p$ and B is soft. □

Theorem 130.15. *Suppose that G is a nonabelian p-group which possesses a maximal normal abelian subgroup A such that G/A is cyclic. If $|\mathrm{Z}(G) \cap G'| = p$, then G has a soft subgroup distinct from A.*

Proof. Note that $G = A\langle b\rangle$ for some element $b \in G - A$ so that $\mathrm{C}_A(b) = \mathrm{Z}(G)$ and $\mathrm{C}_G(b) = \mathrm{Z}(G)\langle b\rangle = B$. We prove that B is soft in G. First of all, B is abelian and self-centralizing and set $N = \mathrm{N}_G(B)$. Further, we have $|N : B| = |(N \cap A) : \mathrm{Z}(G)|$ and $|(N \cap A) : \mathrm{Z}(G)| = |[N \cap A, \langle b\rangle]| = p$ by Lemma 121.2. □

§131

p-groups with a 2-uniserial subgroup of order p

Let us say that a subgroup H of a p-group G is *n-uniserial* ($n \geq 1$) if for each index $i = 1, 2, \ldots, n$ there is a unique subgroup K_i such that $H \leq K_i$ and $|K_i : H| = p^i$. In case the subgroups of G containing H form a chain, we say that H is *uniserially embedded* in G. We shall classify here all p-groups G which possess a subgroup of order p which is 2-uniserial and so extend some results for $p > 2$ of N. Blackburn and L. Hethelyi to the case of 2-groups.

Theorem 131.1 (Janko). *Let G be a p-group and let L be a 2-uniserial subgroup of order p. Then L is uniserially embedded in G (and so G is one of the groups in Exercise A40.77 of Appendix 40) or $p = 2$ and*

$$G = \langle a, t, x \mid a^{2^m} = t^2 = [a, t] = 1,\ u = a^{2^{m-1}},$$
$$v = a^{2^{m-2}},\ x^2 = tv,\ a^x = a^{-1},\ t^x = tu \rangle,$$

where

$$m \geq 3, \quad |G| = 2^{m+2}, \quad \mathrm{Z}(G) = \langle tv \rangle \cong C_4,$$
$$\Phi(G) = \langle t \rangle \times \langle a^2 \rangle \cong \mathrm{C}_2 \times \mathrm{C}_{2^{m-1}}, \quad G' = \langle a^2 \rangle \cong C_{2^{m-1}}$$

and here $L = \langle t \rangle \cong C_2$ is 2-uniserial but not 3-uniserial in G (and so $\langle t \rangle$ is not uniserially embedded in G).

Proof. Let L be a 2-uniserial subgroup of order p in G.

(i) First assume $p > 2$. Set $N = \mathrm{N}_G(L) = \mathrm{C}_G(L)$. If $|N/L| = p$, then N is a self-centralizing abelian subgroup of order p^2 and $|\mathrm{N}_G(N) : N| = p$. This means that N is a soft subgroup in G and so Lemma 130.2 implies that all subgroups of G containing N form a chain. Hence in this case L is uniserially embedded in G. We may assume $|N/L| > p$. Since there is only one subgroup of order p in N/L, it follows that N/L is cyclic. If $N = G$, then L is uniserially embedded in G and we are done. Thus we may assume $N < G$. In this case, L is not characteristic in N and so N is not cyclic.

Set $R = \Omega_1(N) \cong \mathrm{E}_{p^2}$ and $N_1 = \mathrm{N}_G(R)$ so that $N < N_1$ since R is characteristic in N. As there is only one subgroup of order p in N_1/R, we see that N_1/R is cyclic. Since $R < N$, we infer that $R = \Omega_1(N_1)$ is characteristic in N_1, and we conclude

that $N_1 = G$. In that case, $\Omega_1(G) = R \cong \mathrm{E}_{p^2}$ and G possesses a cyclic subgroup of index p which does not contain L. Thus L is uniserially embedded in G and we are done in case $p > 2$.

(ii) Assume now $p = 2$ and set $L = \langle t \rangle$. Since the involution t is contained in exactly one subgroup of order 4 in G, Theorem A.14.1 implies that we have one of the following possibilities:

(a) G is cyclic.

(b) $\mathrm{C}_G(t) = \langle t \rangle \times \mathrm{C}_{2^m}$, $m \geq 1$.

(c) $\mathrm{C}_G(t) = \langle t \rangle \times \mathrm{Q}_{2^m}$, $m \geq 3$.

(d) $G = \langle a, b \rangle$ with defining relations

$$a^{2^m} = b^4 = 1, \quad m \geq 2, \quad u = a^{2^{m-1}}, \quad b^2 = ut,$$
$$t^2 = 1, \quad a^b = a^{-1}t^\epsilon, \quad \epsilon = 0, 1.$$

Here $\mathrm{Z}(G) = \langle t, u \rangle \cong \mathrm{E}_4$, $G/\langle t \rangle \cong \mathrm{Q}_{2^{m+1}}$, $G' = \langle a^2 t^\epsilon \rangle$, and G is metacyclic if and only if $\epsilon = 0$.

In case (a), $\langle t \rangle$ is uniserially embedded in G. In cases (c) and (d), $\mathrm{C}_G(t)/\langle t \rangle$ is a generalized quaternion group and so there are two distinct cyclic subgroups $S/\langle t \rangle$ and $T/\langle t \rangle$ of order 4 contained in $\mathrm{C}_G(t)/\langle t \rangle$. But then S and T are two distinct subgroups of order 8 which contain $\langle t \rangle$ and so $\langle t \rangle$ is not 2-uniserial in G, a contradiction.

It remains to consider the above case (b), where $\mathrm{C}_G(t) = \langle t \rangle \times C$ with $C = \langle a \rangle$ and $o(a) = 2^m$, $m \geq 1$. If $\mathrm{C}_G(t) = G$, then $\langle t \rangle$ is uniserially embedded in G. From now on we assume $\mathrm{C}_G(t) < G$ and so G is nonabelian. We may apply Theorem 48.1 in which such groups G are classified. In cases (a) and (b) of that theorem, G is either of maximal class or $G \cong \mathrm{M}_{2^n}$, $n \geq 4$, and in these cases $\langle t \rangle$ is uniserially embedded in G. In cases (d–h) of that theorem, we have $m \geq 2$ and t is contained in a subgroup $D \cong \mathrm{D}_8$. On the other hand, t is also contained in $\langle t \rangle \times \Omega_2(\langle a \rangle)$ which is an abelian subgroup of type $(2, 4)$. Hence in all these cases $\langle t \rangle$ is not 2-uniserial in G, a contradiction.

We have proved that we must be in case (c) of Theorem 48.1. From here we know that $T = \mathrm{C}_G(t) = \langle t \rangle \times \langle a \rangle$ is of index 2 in G, $o(a) = 2^m$ with $m \geq 3$ and $t \in \Phi(G)$ so that $\Phi(G) = \langle t \rangle \times \langle a^2 \rangle$, where $\langle a^2 \rangle = \Phi(T)$. Hence there is an element $x \in G - T$ such that $x^2 \in \langle t, a^2 \rangle - \langle a^2 \rangle$. Set $u = a^{2^{m-1}}$ and $\Omega_2(\langle a \rangle) = \langle v \rangle \cong \mathrm{C}_4$ so that $v^2 = u$, $u \in \mathrm{Z}(G)$ and $\Omega_1(T) = \langle t, u \rangle \cong \mathrm{E}_4$. Also, we have $t^x = tu$ and so $x^2 \notin \langle t, u \rangle$ and $\Phi(G) = \langle t \rangle \times \langle a^2 \rangle = \langle x^2, a^2 \rangle$. Obviously, x does not centralize a^2. Indeed, if $[x, a^2] = 1$, then x centralizes $\Phi(G) = \langle x^2, a^2 \rangle$ and so x would centralize t, a contradiction.

Thus we have proved that x induces on T an involutory automorphism such that $t^x = tu$ and x does not centralize $\langle a^2 \rangle$. In Theorem 34.8(d) the structure of $\mathrm{Aut}(T)$ is determined. In particular, we get $a^x = a^{-1}u^\epsilon$, where $\epsilon = 0, 1$. If $\epsilon = 1$, then we

replace a with $a' = at$ and obtain

$$(a')^x = (at)^x = a^x t^x = (a^{-1}u)\cdot(tu) = a^{-1}t = (at)^{-1} = (a')^{-1}.$$

Hence writing again a instead of a', we may assume from the start that $a^x = a^{-1}$. We see that $\mathrm{C}_T(x) = \langle tv\rangle = \mathrm{Z}(G) \cong \mathrm{C}_4$ since $(tv)^2 = u$. Also, $\langle a^2\rangle \leq \mathrm{Z}(G)$ and $o(x^2) \geq 4$ and so $x^2 = (tv)^{\pm 1} = tv^{\pm 1}$. Replacing v with v^{-1} if necessary, we may assume that $x^2 = tv$ and so the structure of G is uniquely determined.

Let $xt^r a^s$ (r, s are integers) be any element in $G - T$. Then we compute

$$\begin{aligned}(xt^r a^s)^2 &= xt^r a^s \cdot xt^r a^s = x^2 (t^r a^s)^x t^r a^s \\ &= tv\cdot(tu)^r \cdot a^{-s}\cdot t^r a^s = tvu^r = (tv)^{\pm 1},\end{aligned}$$

and see that all elements in $G-T$ are of order 8. It follows that $\langle t\rangle \times \langle v\rangle$ is the only subgroup of order 8 containing $\langle t\rangle$ which shows that $\langle t\rangle$ is 2-uniserial in G. But G is not 3-uniserial since $\langle t\rangle \times \langle a^{2^{m-3}}\rangle$ and $\langle t, x\rangle \cong \mathrm{M}_{2^4}$ are two distinct subgroups of order 2^4 containing $\langle t\rangle$, and the theorem is proved. □

§132

On centralizers of elements in p-groups

We present here some results of N. Blackburn [Bla12] about the centralizers of elements in p-groups. Suppose that K is a p-group and s is an element of order p in the center of K. We are concerned with the question: What are the p-groups G for which $K \leq G$ and $K = \mathrm{C}_G(s)$? In particular, is there a bound on the order or class of G? In fact, we show by Theorem 132.1 that these two last questions are the same.

Theorem 132.1. *Let G be a p-group of class k. Suppose that $s \in G$ and $|\mathrm{C}_G(s)| = p^r$. Then $|G| \leq p^{rk}$.*

Proof. Let

$$G = \mathrm{K}_1(G) > \mathrm{K}_2(G) > \cdots > \mathrm{K}_k(G) > \mathrm{K}_{k+1}(G) = \{1\}$$

be the lower central series of G. For $1 \leq i \leq k$, set $H = \langle s, \mathrm{K}_i(G)\rangle$. Every conjugate of s in H is of the form $s^h = s[s,h]$ ($h \in H$) so the number of conjugates of s in H is at most $|H'|$. Thus

$$|H'| \geq |H : \mathrm{C}_H(s)| \geq |H|/p^r \geq |\mathrm{K}_i(G)|/p^r.$$

But we see that $\mathrm{K}_i(G)/\mathrm{K}_{i+1}(G) \leq \mathrm{Z}(G/\mathrm{K}_{i+1}(G))$ and $H/\mathrm{K}_i(G)$ is cyclic and so $H/\mathrm{K}_{i+1}(G)$ is abelian. Then we get $H' \leq \mathrm{K}_{i+1}(G)$ and so, by the above inequality, $|\mathrm{K}_{i+1}(G)| \geq |\mathrm{K}_i(G)|/p^r$ which implies $|\mathrm{K}_i(G) : \mathrm{K}_{i+1}(G)| \leq p^r$ for $i = 1, \ldots, k$. Hence $|G| \leq p^{rk}$. □

If s is an element of order p in a p-group G, then set $C = \mathrm{C}_G(s)$. Then, as a rule, we have infinitely many p-groups G with such a fixed centralizer C. For example, if $C \cong \mathrm{E}_{p^2}$, then there are infinitely many p-groups of maximal class which all have such a small centralizer of s. However, there are examples for the structure of C which is small in a rather strong sense, where there exist only finitely many p-groups G with such a fixed centralizer C. This will be seen in the next two theorems.

Theorem 132.2. *Let s be an element of order p in a p-group G and set $C = \mathrm{C}_G(s)$. If there exists a positive integer m such that $s = x^{p^{m-1}}$ for some $x \in C$ and if C has no elementary abelian subgroup of order p^{m+1}, then $|G : C| < p^m$.*

Proof. If this theorem is false, then there is a subgroup H of G such that $H \geq C$ and $|H : C| = p^m$. Thus s has p^m conjugates $s_1, s_2, \ldots, s_{p^m}$ in H. If $s_i = s^{u_i}$ ($u_i \in H$),

put $x_i = x^{u_i}$; thus $x_1, \ldots, x_{p^m}$ are distinct conjugates of x in H since $x_i^{p^{m-1}} = s_i$. If M is a maximal subgroup of H containing C, then $x_i \in M$ as $x \in M$ and M is normal in H. Since $|M : C| = p^{m-1}$, it follows that

$$s_i = x_i^{p^{m-1}} \in C, \quad i = 1, \ldots, p^m.$$

Indeed, if $s_i \notin C$, then $C \cap \langle x_i \rangle = \{1\}$ and so, by the product formula, we obtain $|M| \geq |C||\langle x_i \rangle| = |C|p^m$, a contradiction (because $|H : M| = p$ and $|H| = |C|p^m$). But then s_i, s_j commute for any $i, j \in \{1, 2, \ldots, p^m\}$. Hence $\langle s_1, \ldots, s_{p^m} \rangle$ is elementary abelian of order $\geq p^{m+1}$, a contradiction. □

Theorem 132.3. *Let s be an element of order p in a p-group G and set $C = \mathrm{C}_G(s)$. Suppose that s is the p-th power of some element $x \in C$ and $|C| = p^l$, where $l \geq 3$ and $2l \leq p + 4$. Then $|G : C| < p^{l-2}$.*

Proof. If $l = 3$, then, by the structure of groups of order p^3, $\langle s \rangle = \Omega_1(\Phi(C))$ and so $\langle s \rangle$ is characteristic in C. But then $\mathrm{N}_G(C)$ centralizes $\langle s \rangle$ which implies $G = C$ and we are done. Now we assume $l > 3$ so that p is odd and $2l \leq p + 3$. If our assertion is false, there exists a subgroup H of G such that $H \geq C$ and $|H : C| = p^{l-2}$. Let M be a maximal subgroup of H such that $M \geq C$. Thus $|M| = p^{2l-3} \leq p^p$ and so M is regular (Theorem 7.1(b)). It follows that the elements of M of order at most p form a characteristic subgroup E of M (Theorem 7.2(b)). We have $M \trianglelefteq H$ and $s \in E$.

As $|H : C| = p^{l-2}$, s has p^{l-2} conjugates $s_1, \ldots, s_{p^{l-2}}$ in H. If $s_i = s^{u_i}$ $(u_i \in H)$, put $x_i = x^{u_i}$. Since $x \in C$, we have $x_i \in M$. If $i \neq j$, we get $x_i^p \neq x_j^p$. By Theorem 7.2(a), we infer that $x_i x_j^{-1} \notin E$. Thus $|M : E| > p^{l-2}$ and so $|M : E| \geq p^{l-1}$. Similarly, $|E| > p^{l-2}$ since $s_i \in E$. Hence $|E| \geq p^{l-1}$ which implies $|M| \geq p^{2l-2}$, a contradiction. Our theorem is proved. □

In his paper [Bla12], N. Blackburn has studied 2-groups G which possess an involution s such that $\mathrm{C}_G(s)$ is the nonmetacyclic minimal nonabelian group of order 16. We shall describe these groups G more closely by using the results from §51 and §130.

Theorem 132.4. *Suppose that G is a 2-group of order 2^5 which possesses an involution s such that $C = \mathrm{C}_G(s)$ is the nonmetacyclic minimal nonabelian group of order 2^4. Then $E = \Omega_1(C)$ is a self-centralizing elementary abelian group of order 8. Also, $E = \Phi(G)$ and so G is isomorphic to a unique group of order 2^5 given in Theorem 51.3.*

Proof. We may set

$$C = \mathrm{C}_G(s) = \langle r, t \mid r^4 = t^2 = 1,\ [r, t] = z,\ z^2 = [z, r] = [z, t] = 1 \rangle,$$

where

$$\langle z \rangle = C', \quad \mathrm{Z}(C) = \Phi(C) = \langle r^2, z \rangle$$

and

$$E = \Omega_1(C) = \langle r^2, z, t \rangle \cong \mathrm{E}_8 \quad \text{with } \mathrm{C}_G(E) = E.$$

Since G centralizes $\langle z\rangle = C'$, it follows that $s \in \{r^2, r^2z\}$ and G (normalizing $\mathrm{Z}(C)$) fuses r^2 and r^2z. We may set $s = r^2$ and for any $v \in G - C$, $s^v = sz$. Note that for any $t' \in E - \mathrm{Z}(C)$ we have $(rt')^2 = r^2(t')^2[t', r] = sz$ and so we may put $r^v = rt'$ with some $t' \in E - \mathrm{Z}(C)$. It follows that $t' \in G'$ and so $E \le \Phi(G)$ gives $E = \Phi(G)$. Then Theorem 51.3 applies and such a group G is uniquely determined. □

Theorem 132.5. *Let G be a 2-group of order $> 2^5$ which possesses an involution s such that $C = \mathrm{C}_G(s)$ is the nonmetacyclic minimal nonabelian group of order 2^4. Then we have $|G| = 2^{n+3}$, $n \ge 3$, $|G'| = 2^n$, $\mathrm{Z}(G) = \langle z\rangle = C'$ is of order 2, G is of class $n + 1$ (coclass 2) and G is a CF-group (i.e., the index of any term of the lower central series of G beyond $G' = \mathrm{K}_2(G)$ in its predecessor is at most 2). Moreover, $\mathrm{Z}(C) = \langle z, s\rangle \cong \mathrm{E}_4$, $G' \cap C = W \ne \mathrm{Z}(C)$ is a normal four-subgroup of G, $\mathrm{K}_3(G)$ is abelian of order 2^{n-1} and rank 2, s inverts $\mathrm{K}_3(G)$, $L = \langle s\rangle \mathrm{K}_3(G)$ is normal in G, $G/L \cong \mathrm{D}_8$, $s \notin G'$, $\Phi(G) = \langle s\rangle G'$, and so $\mathrm{d}(G) = 2$. Finally, $E = \Omega_1(C)$ is a self-centralizing elementary abelian subgroup of order 8, $E < \Phi(G)$, and we have one of the following possibilities:*

(a) *$n = 3$, E is normal in G and G is isomorphic to one of the four distinct groups of order 2^6 given in Theorem 51.4.*

(b) *$n > 3$, E is not normal in G, G has no normal elementary abelian subgroup of order 8, W is the unique normal four-subgroup in G, and G is one of the groups described in* (c) *and* (d) *of Theorem 51.6.*

Proof. We may set

$$C = \mathrm{C}_G(s) = \langle r, t \mid r^4 = t^2 = 1,\ [r, t] = z,\ z^2 = [z, r] = [z, t] = 1\rangle,$$

where

$$\langle z\rangle = C', \quad \mathrm{Z}(C) = \Phi(C) = \langle r^2, z\rangle$$

and

$$E = \Omega_1(C) = \langle r^2, z, t\rangle \cong \mathrm{E}_8 \quad \text{with } \mathrm{C}_G(E) = E.$$

Since $\mathrm{N}_G(C) > C$ centralizes $\langle z\rangle = C'$, it follows that $s \in \{r^2, r^2z\}$ and $\mathrm{N}_G(C)$ (normalizing $\mathrm{Z}(C)$) fuses r^2 and r^2z. This gives $|\mathrm{N}_G(C) : C| = 2$ and we may assume $s = r^2$ (noting that $(rt)^2 = r^2t^2[t, r] = r^2z$). Also, $\mathrm{Z}(G) \le \mathrm{Z}(C)$ and so $\mathrm{Z}(G) = \langle z\rangle$ is of order 2.

Set $A = \langle r, z\rangle = \langle r\rangle \times \langle z\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$ so that $\mathrm{C}_G(r) \le C$ and therefore $\mathrm{C}_G(r) = A$, which implies that A is a self-centralizing abelian subgroup of type $(4, 2)$. As $\mathrm{N}_G(A)$ centralizes $\langle s\rangle = \mho_1(A)$, it follows that $\mathrm{N}_G(A) = C$ which together with $|C : A| = 2$ gives that A is a soft subgroup in G. We may apply all results from §130 about soft subgroups.

Set $|G : A| = 2^n$ so that $|G| = 2^{n+3}$ with $n \ge 3$. By Lemma 130.2, all subgroups of G containing A form a chain. As $\mathrm{C}_G(r) = A$, the conjugacy class of r has 2^n elements and so $|G'| \ge 2^n$. However, if $|G'| > 2^n$, then $|G'| = 2^{n+1}$ and so $|G/G'| = 4$.

By a result of O. Taussky (Lemma 1.6), G would be of maximal class, a contradiction (since G has an abelian subgroup A of type $(4, 2)$). We have proved that $|G'| = 2^n$.

Let M be a unique maximal subgroup of G containing the soft subgroup A. By Theorem 130.6, the nilpotence class of M is equal to n and the class of G is at least $n + 1$. However, if the class of G is greater than $n + 1$, then the class of G is $n + 2$ and so G would be of maximal class, a contradiction. We have proved that G is of class $n + 1$. But $|G/G'| = 2^3$ and so the index of any term of the lower central series of G beyond G' in its predecessor is at most 2 which implies that G is a CF-group.

By Proposition 130.10, we have $G'A = M$. On the other hand, we have $\langle z\rangle = C'$ and so $\langle z\rangle \leq G' \cap A$. But $|M| = 2^{n+2}$ and so, by the product formula, $G' \cap A = \langle z\rangle$. In particular, $s = r^2 \notin G'$ and so $\langle s\rangle G' = \Phi(G)$, $|G : \Phi(G)| = 4$, and $\mathrm{d}(G) = 2$.

The subgroup A is also a soft subgroup in M and let K $(\geq C)$ be a unique maximal subgroup of M containing A. By Proposition 130.10 (applied to M), $K = AM'$ with $A \cap M' = \langle z\rangle$, M' is normal in G, and $|G' : M'| = 2$. On the other hand, we have $\mathrm{K}_3(G) = [G, G'] \leq M'$ and so the fact that G is a CF-group gives $\mathrm{K}_3(G) = M'$. Since $s = r^2 \in \Phi(M)$ and $M' \leq \Phi(M)$, we get

$$\Phi(M) = \langle s\rangle M', \quad \text{where } |\Phi(M) : M'| = 2.$$

Note that $\Phi(M)$ is normal in G and so $\Phi(M) - M'$ is a normal subset of G with exactly $|M'| = 2^{n-1}$ elements. Hence the involution s and all its $2^{n-1} = |G : C|$ conjugates must be contained in $\Phi(M) - M'$. It follows that all elements in $sM' = s\mathrm{K}_3(G)$ are involutions. This implies that $\mathrm{K}_3(G)$ is abelian. Also, $L = \langle s\rangle \mathrm{K}_3(G) = \Phi(M)$ and so L is normal in the group G. We have $|L| = 2^n$ so that G/L is nonabelian of order 8 since $G' \not\leq K > L$. But $M/\Phi(M) = M/L \cong \mathrm{E}_4$ and so $G/L \cong \mathrm{D}_8$.

As $AM' = K$ with $A \cap M' = \langle z\rangle$ and $A < C \leq K$ with $|C : A| = 2$, it follows that $C \cap M' = W$ is of order 4. We know that s inverts W. If $W \cong \mathrm{C}_4$, then $W\langle s\rangle \cong \mathrm{D}_8$, contrary to the fact that C is minimal nonabelian. Hence we infer that $W \cong \mathrm{E}_4$ and so $E = \langle s\rangle \times W = \Omega_1(C) \cong \mathrm{E}_8$. Since $\mathrm{C}_{M'}(s) = W$ and s inverts M', we obtain $W = \Omega_1(M')$. It follows that M' is abelian of rank 2 and W is a normal four-subgroup in G with $W \neq \mathrm{Z}(C) = \langle z, s\rangle$ since $s \notin G'$. Also, $s \in \Phi(G)$ and $W \leq M' \leq \Phi(G)$ gives $E = \langle s\rangle \times W = \Omega_1(C) \leq \Phi(G)$. But $G' > M'$ and so $G' \not\leq E$ and therefore $E < \Phi(G)$. Also, E is self-centralizing in G and so we are in a position to apply the results from §51.

If $n = 3$, then $M' = \mathrm{K}_3(G)$ is of order 4 and so $\mathrm{K}_3(G) = W$. All four conjugates of s in G lie in sW and so $E = \langle s\rangle \times W$ is normal in G. Theorem 51.4 is applicable and we get exactly four groups of order 64.

If $n > 3$, then $M' = \mathrm{K}_3(G)$ is of order > 4 and so all 2^{n-1} conjugates of s in G (forming the set $s\mathrm{K}_3(G)$) do not lie in E. This gives that E is not normal in G. In this case, Theorem 51.6 is applicable. Our group G has no normal elementary abelian subgroup of order 8 and W is the unique normal four-subgroup in G. The group G is then described in parts (c) and (d) of Theorem 51.6. □

Exercise. Suppose that x is a noncentral element of a p-group G, $o(x) = p$, such that $C = \mathrm{C}_G(x)$ is minimal nonabelian such that $C/\Omega_1(G)$ is nonidentity cyclic. Prove that

(a) $\Omega_1(C) \cong \mathrm{E}_{p^3}$.

(b) $|\mathrm{Z}(G)| = p$.

(c) If $x \in R < \Omega_1(C)$ is of order p^2, then we have $|\mathrm{N}_G(R) : C| = p$. In particular, $|\mathrm{N}_G(C) : C| = p$ so that $\mathrm{N}_G(C) = \mathrm{N}_G(R)$.

Study the structure of $\mathrm{N}_G(C)$ in detail.

§133

Class and breadth of a p-group

Let G be a p-group and let x be an element of G. We recall that the breadth of x is the nonnegative integer $\mathrm{b}(x)$ such that

$$p^{\mathrm{b}(x)} = |G : \mathrm{C}_G(x)|.$$

The breadth of the group G, denoted by $\mathrm{b}(G)$ or just b, is the maximum of the breadths of its elements. Thus p^b is the size of the largest of the conjugacy classes of G.

It was shown by C. R. Leedham-Green, P. M. Neumann, and J. Wiegold in [LGNW] that there is a close relationship between the breadth b of a p-group G and its nilpotence class $c = \mathrm{cl}(G)$. In particular, we present here a (technically somewhat simpler) proof of their result:

Theorem 133.1. *Let G be a p-group of the breadth b and class c. Then*

$$c < \frac{p}{p-1}b + 1.$$

Since $p/(p-1) = 1 + 1/(p-1) \leq 2$, we get a bound $c < 2b + 1$ or $c \leq 2b$ which is independent of p.

A slightly stronger result was proved by M. Cartwright (*Bull. London Math. Soc.* **19** (1987), 425–430) in case of 2-groups, where he has shown that $c \leq \frac{5}{3}b + 1$.

The Class-Breadth Conjecture. For any p-group G we have $c \leq b + 1$.

This bound is attained by any group G of order p^n ($n \geq 3$) and maximal class $n-1$ since such a group always possesses an element x such that $|\mathrm{C}_G(x)| = p^2$ and so we have $b = \mathrm{b}(G) = \mathrm{b}(x) = n - 2$. However, the class-breadth conjecture was shown in [ENOB] to be false at least for $p = 2$. But the conjecture remains open for p-groups of odd order.

The class-breadth conjecture has been established under various conditions. For example, if $b < p$, then $c \leq b+1$ (Theorem 133.5) and if G is metabelian, then $c \leq b+1$ (Theorem 133.6).

In order to prove Theorem 133.1, we have to prove first the following two technical lemmas. If

$$G = \mathrm{K}_1(G) > \mathrm{K}_2(G) > \cdots > \mathrm{K}_c(G) > \mathrm{K}_{c+1}(G) = \{1\}$$

is the lower central series of a p-group G of class c, then we define the *two-step centralizer* C_i $(i = 1, 2, \ldots, c-1)$ by

$$C_i = \mathrm{C}_G(\mathrm{K}_i(G)/\mathrm{K}_{i+2}(G)) = \{g \in G \mid [g, x] \in \mathrm{K}_{i+2}(G) \text{ for all } x \in \mathrm{K}_i(G)\}.$$

It is clear that C_i is normal in G, $C_i \geq \mathrm{K}_{i+2}(G)$ and C_i is a proper subgroup of G for all $i = 1, 2, \ldots, c-1$.

Lemma 133.2. *Let G be a p-group and $x \in G$. Then $b(x) \geq s(x)$, where $s(x)$ denotes the number of indices i $(i = 1, 2, \ldots, c-1)$ for which $x \notin C_i$.*

Proof. We use induction on the length c of the lower central series of G. The lemma is certainly correct for p-groups with the lower central series of length 1 (in that case, G is abelian), for then $b(x)$ and $s(x)$ are both 0 whatever x may be. Let us suppose that the lemma is known to be right for p-groups with the lower central series of length $c-1$. We set

$$S(x) = \{i \mid 1 \leq i \leq c-1 \text{ and } x \notin C_i\}$$

so that $s(x) = |S(x)|$. Put $\bar{G} = G/\mathrm{K}_c(G)$ and embellish other symbols with a bar to denote images under canonic epimorphism of G onto $\bar{G}$, or simply to denote the corresponding notion in $\bar{G}$. Notice that if $1 \leq i \leq c-2$, then

$$\overline{C_i} = \mathrm{C}_{\bar{G}}(\overline{\mathrm{K}_i(G)}/(\overline{\mathrm{K}_{i+2}(G)}) = C_i/\mathrm{K}_c(G)$$

so that our convention is unambiguous; and if $1 \leq i \leq c-2$, then $\bar{x} \in \overline{C_i}$ if and only if $x \in C_i$. An instance for our inductive hypothesis is that $\bar{b}(\bar{x}) \geq \bar{s}(\bar{x})$. There are two cases to consider.

Suppose first that $x \in C_{c-1}$ which means that x centralizes $\mathrm{K}_{c-1}(G)$. Then we have $S(x) = \bar{S}(\bar{x})$ so that $s(x) = \bar{s}(\bar{x})$; and since certainly $b(x) \geq \bar{b}(\bar{x})$, the inductive hypothesis gives

$$b(x) \geq \bar{b}(\bar{x}) \geq \bar{s}(\bar{x}) = s(x),$$

as required.

The other possibility is $x \notin C_{c-1}$, i.e., x does not centralize $\mathrm{K}_{c-1}(G)$. In this case, $S(x) = \bar{S}(\bar{x}) \cup \{c-1\}$, and so $s(x) = \bar{s}(\bar{x}) + 1$. On the other hand, as $\overline{\mathrm{K}_{c-1}(G)} \leq \mathrm{Z}(\bar{G})$ and therefore $\overline{\mathrm{K}_{c-1}(G)}$ is centralized by $\bar{x}$, we have (noting that $\overline{\mathrm{K}_{c-1}(G)} \leq \mathrm{C}_{\bar{G}}(\bar{x})$ and $\overline{\mathrm{C}_G(x)} \leq \mathrm{C}_{\bar{G}}(\bar{x})$)

$$|\bar{G} : \mathrm{C}_{\bar{G}}(\bar{x})| \leq |\bar{G} : (\overline{\mathrm{C}_G(x)\mathrm{K}_{c-1}(G)})| = |G : (\mathrm{C}_G(x)\mathrm{K}_{c-1}(G))| < |G : \mathrm{C}_G(x)|,$$

the last inequality is strict because $\mathrm{K}_{c-1}(G) \not\leq \mathrm{C}_G(x)$ (by our assumption). This gives $\bar{b}(\bar{x}) < b(x)$ and so $\bar{b}(\bar{x}) \leq b(x) - 1$, and therefore by the above,

$$b(x) \geq \bar{b}(\bar{x}) + 1 \geq \bar{s}(\bar{x}) + 1 = s(x).$$

This case also yields the desired inequality and induction completes the proof. □

Lemma 133.3. *Let G be a p-group of class $c \geq 2$. Then there exists an element $g \in G$ which lies in $t(g)$ two-step centralizers C_i $(1 \leq i \leq c-1)$ and $t(g) < \frac{1}{p}(c-1)$.*

Proof. For $x \in G$, let $t_i(x) = 1$ if $x \in C_i$ and $t_i(x) = 0$ if $x \notin C_i$, $1 \leq i \leq c-1$. Thus $\sum_{i=1}^{c-1} t_i(x) = t(x)$ is the number of two-step centralizers C_i in which x lies.

We estimate the average of $t_i(x)$ over G:

$$\frac{1}{|G|}\sum_{x\in G} t_i(x) = \frac{1}{|G|}|C_i| \leq \frac{1}{p},$$

the latter inequality arises from the fact that C_i is a proper subgroup of G and hence has index at least p. It follows that

$$\frac{1}{|G|}\sum_{i=1}^{c-1}\sum_{x\in G} t_i(x) = \frac{1}{|G|}\sum_{x\in G} t(x) \leq \frac{c-1}{p}.$$

In this inequality the summands $t(x)$ are nonnegative, and one of them, $t(1) = c-1$, exceeds $\frac{c-1}{p}$. Therefore at least one summand $t(g)$ for some $g \in G$ is less than $\frac{c-1}{p}$, and this is what the lemma states. □

Proof of Theorem 133.1. We combine both Lemmas 133.2 and 133.3 together with the notation introduced there. Since $s(g) + t(g) = c-1$, we get

$$\begin{aligned} b \geq b(g) \geq s(g) &= (c-1) - t(g) > (c-1) - \frac{1}{p}(c-1) \\ &= (c-1)\Big(1 - \frac{1}{p}\Big) = (c-1)\frac{p-1}{p}. \end{aligned}$$

This gives $c < \frac{p}{p-1}b + 1$ and we are done. □

Lemma 133.4. *If C_i, $i = 1, 2, \ldots, c-1$, are the two-step centralizers in a p-group G of class $c \geq 2$ and if $\bigcup_{i=1}^{c-1} C_i \neq G$, then $c \leq \mathrm{b}+1$ and so the class-breadth conjecture holds.*

Proof. If $x \in G$, $x \notin \bigcup C_i$, then we have $s(x) = c-1$ and, using Lemma 133.2, we get $c - 1 \leq b(x) \leq b$ and $c \leq b + 1$. □

Theorem 133.5. *Let G be a p-group with $b = \mathrm{b}(G) < p$. Then $c = \mathrm{cl}(G) \leq b + 1$ and so the class-breadth conjecture holds.*

Proof. From Theorem 133.1 follows

$$\begin{aligned} c &< \frac{p}{p-1}b + 1 = \Big(1 + \frac{1}{p-1}\Big)b + 1 = b + 1 + \frac{b}{p-1} \\ &\leq b + 1 + \frac{p-1}{p-1} = b + 2, \end{aligned}$$

and since both c and b are integers, we get $c \leq b + 1$. □

Theorem 133.6. *Let G be a p-group such that $\mathrm{K}_p(G)$ is contained in $\mathrm{Z}(G')$. Then the class-breadth conjecture holds. In particular, if G is metabelian, then the class-breadth conjecture holds.*

Proof. Let C_i, $1 \leq i \leq c-1$, be the two-step centralizers of the lower central series of length c of G. That is, $C_i = \mathrm{C}_G(\mathrm{K}_i(G)/\mathrm{K}_{i+2}(G))$.

We note that G cannot be covered by less than $p+1$ proper subgroups. Indeed, considering a normal subgroup G_0 of G such that $G/G_0 \cong \mathrm{E}_{p^2}$, we see that E_{p^2} is partitioned by exactly $p+1$ subgroups of order p.

We may assume that $c \geq p+2$. Indeed, if $c \leq p+1$, then the two-step centralizers $C_1, C_2, \ldots, C_{c-1}$ contain at most p proper subgroups of G and so they cannot cover G. But then, by Lemma 133.4, the class-breadth conjecture holds.

We first use the fact that $\mathrm{K}_p(G) \leq \mathrm{Z}(\mathrm{K}_2(G))$ to show $C_i \leq C_{i+1}$ whenever we have $p \leq i < c-1$. To do this, suppose that $g \in C_i$. Now $\mathrm{K}_{i+1}(G)$ is generated by the set of commutators $\{[x,a] \mid x \in \mathrm{K}_i(G),\ a \in G\}$, and so we need only to prove that $[[x,a],g] \in \mathrm{K}_{i+3}(G)$ whenever $x \in \mathrm{K}_i(G)$ and $a \in G$. From the Hall–Witt identity (Introduction, Exercise 13)

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$$

we get by setting $y = a^{-1}$ and $z = g$

$$[x, a, g]^{a^{-1}} [a^{-1}, g^{-1}, x]^g [g, x^{-1}, a^{-1}]^x = 1.$$

As $x \in \mathrm{K}_i(G) \leq \mathrm{K}_p(G)$ while $[a^{-1}, g^{-1}] \in \mathrm{K}_2(G)$, we have $[a^{-1}, g^{-1}, x] = 1$ by our assumption. Hence

$$[x, a, g]^{a^{-1}} [g, x^{-1}, a^{-1}]^x = 1.$$

Since $g \in C_i$ and $x^{-1} \in \mathrm{K}_i(G)$, it follows that $[g, x^{-1}] \in \mathrm{K}_{i+2}(G)$ and so we obtain $[g, x^{-1}, a^{-1}] \in \mathrm{K}_{i+3}(G)$ which implies that $[g, x^{-1}, a^{-1}]^x \in \mathrm{K}_{i+3}(G)$. Thus we get $[x, a, g]^{a^{-1}} \in \mathrm{K}_{i+3}(G)$ and so $[x, a, g] \in \mathrm{K}_{i+3}(G)$ and $g \in C_{i+1}$. We have shown that

$$C_p \leq C_{p+1} \leq \cdots \leq C_{c-1}.$$

Therefore

$$\bigcup_{i=1}^{c-1} C_i = C_{c-1} \cup \bigcup_{i=1}^{p-1} C_i.$$

This exhibits $\bigcup_{i=1}^{c-1} C_i$ as a union of p subgroups of index at most p in G; it therefore cannot be the whole of G (see §116). Lemma 133.4 then completes the proof. □

§134

On p-groups with maximal elementary abelian subgroup of order p^2

1^o. Glauberman and Mazza [GM] have proved that if a p-group G, $p > 2$, possesses a maximal elementary abelian subgroup R of order p^2 (i.e., R is not contained in an elementary abelian subgroup of G of order p^3; in general, E is a maximal elementary abelian subgroup of a p-group G provided $\Omega_1(\mathrm{C}_G(E)) = E$), then G has no elementary abelian subgroup of order p^{p+1}. The proof of this deep result is not elementary. The result above is not true for $p = 2$ (see §127). Some information on the structure of the groups with title property is contained in Theorem 134.6. In particular, if we have $\exp(R^G) = p$, then G has no elementary abelian subgroup of order p^{p+1}. The proof of this result is fairly involved. However, we cannot present an elementary proof of the theorem of Glauberman–Mazza.

In this section we continue to study the structure of groups from [GM] clearing the structure of $\mathrm{C}_G(R)$ also in case $p = 2$. In that case, there is G containing an elementary abelian subgroup of order 2^4, and all such G are determined in Theorem 127.1.

If a 2-group G has a maximal elementary abelian subgroup R of order 4, then every subgroup of G is generated by four elements so G has no elementary abelian subgroup of order 2^5. Indeed, in view of a theorem of MacWilliams (see §50), it suffices to show that G has no normal elementary abelian subgroup of order 8. Assume that $E \cong \mathrm{E}_8$ is a normal subgroup of G. Then, since RE is not of maximal class, we get $\mathrm{C}_{RE}(R) > R$ (Proposition 1.8), and $\mathrm{C}_{RE}(R)$ is elementary abelian by the modular law, and this is a contradiction. The same MacWilliams' result shows that every subgroup of G is generated by four elements. Note that the wreath product $G = \mathrm{Q}_{2^n} \operatorname{wr} \mathrm{C}_2$ has a maximal elementary abelian subgroup of order 4 and a maximal subgroup B (the base of this wreath product) with $\mathrm{d}(B) = 4$.

We begin with the following auxiliary result.

Proposition 134.1. *Suppose that a p-group G contains a maximal elementary abelian subgroup R of order p^2 and assume that R is not normal in G. If $x \in R - \mathrm{Z}(G)$, then $C_G(x) = \mathrm{C}_G(R)$ has no metacyclic subgroup of order p^4 and exponent p^2.*

Proof. By hypothesis, G is nonabelian and $\Omega_1(\mathrm{Z}(G)) < R$. Write $C = \mathrm{C}_G(R)$ and $N = \mathrm{N}_G(R)$; then $|N : C| = p$ by N/C-Theorem (see Proposition 12 in Introduction). Obviously, $\Omega_1(C) = R$. Assume, by way of contradiction, that $L \leq C$ is meta-

cyclic of order p^4 and exponent p^2. Clearly, $\mathrm{Z}(G) \cap R = U$ has order p so $\mathrm{Z}(G)$ is cyclic. If $y \in R-U$, then $\mathrm{C}_G(y) = C(= \mathrm{C}_G(R))$ since $R = \langle y\rangle \times U$ and $U \leq \mathrm{Z}(G)$. Since $\exp(L) = p^2$ and L is metacyclic, we have $L = AB$, where A and B are cyclic of order p^2 such that $A \cap B = \{1\}$. At least one of the subgroups $\Omega_1(A)$, $\Omega_1(B)$ is different from $U(= \Omega_1(\mathrm{Z}(G))$; denote that subgroup by $\langle x\rangle$; then, as we have noticed, $\mathrm{C}_G(x) = C$. Let, for definiteness, $x \in A$. We have $\langle x\rangle \times U = R$.

If G has no normal abelian subgroup of type (p, p), it is a 2-group of maximal class (Lemma 1.4), and such a group G has no subgroup isomorphic to L, a contradiction. Let $E \lhd G$ be abelian of type (p, p); then we have $R \neq E$ by hypothesis, and $U < E$. Write $F = \langle x, E\rangle$, where x is chosen in the previous paragraph. Clearly, we get $x \notin E$ (otherwise, $E = \langle x\rangle \times U = R$). Since $R < F$ and $\Omega_1(F) = F$, it follows that F is nonabelian of order p^3. Recall that $A < L$ is the cyclic subgroup of order p^2 containing x. Write $W = A \cdot E$ (the natural semidirect product with kernel E); then $F < W$ and F/E is a unique subgroup of order p in the cyclic group W/E of order p^2. Since the centralizer $\mathrm{C}_W(E)$ has index $\leq p$ in W, it contains F so F is abelian, contrary to what has just been proved. Thus L does not exist. □

Theorem 134.2. *Suppose that a nonabelian p-group G, $p > 2$, possesses a maximal elementary abelian subgroup R of order p^2. Set $C = \mathrm{C}_G(R)$. Then one of the following holds:*

(a) *G is metacyclic; then $R = \Omega_1(G)$.*

(b) *G is a p-group of maximal class. If, in addition, $R \lhd G$, then $p = 3$.*[1]

(c) *C has a cyclic subgroup of index p so it is abelian of type (p^n, p), $n > 1$.*

Proof. If $R \leq \mathrm{Z}(G)$, then $C = G$ has no elementary abelian subgroup of order p^3 so it is metacyclic (Theorem 13.7). In what follows we assume that $R \not\leq \mathrm{Z}(G)$; then $\mathrm{Z}(G)$ is cyclic. It follows that, in any case, C is metacyclic.

Suppose that $R \lhd G$. If G contains an elementary abelian subgroup A of order p^3, then $\mathrm{C}_{RA}(R) > R$ is elementary abelian, contrary to the hypothesis. Then, by Theorem 13.7, one of the following holds: (i) G is metacyclic. (ii) $G = \Omega_1(G)Z$, where $\Omega_1(G)$ is nonabelian of order p^3 and exponent p and Z is cyclic. (iii) G is a 3-group of maximal class. In case (i), there exist no further restrictions on the structure of G. In case (ii), $\mathrm{C}_G(R)$ has a cyclic subgroup of index p. Finally, in case (iii), if $|G| > 3^4$, we have $R = \Omega_1(\Phi(G))$ and $\mathrm{C}_G(R) = C$ has no cyclic subgroups of index 3 by Exercise 9.1(c); in this case, C is either abelian or minimal nonabelian. In what follows we assume that R is not G-invariant; then G is not metacyclic. We also assume that G is not of maximal class. Then $|C| > p^2$ (Proposition 1.8).

Then, by Proposition 134.1, the (metacyclic) centralizer C has no metacyclic subgroup of order p^4 and exponent p^2. We claim that in the case under consideration C

[1] If a 3-group G of maximal class is not isomorphic to a Sylow 3-subgroup of the symmetric group of degree 3^2, then all maximal elementary abelian subgroups of G have order 3^2 (Exercise 9.13). If $p > 3$, then there is a p-group G of maximal class and order $> p^4$ that has no such subgroup as R (this is the case if $\Omega_1(G) \leq \Phi(G)$).

has a cyclic subgroup of index p. One may assume that $|C| > p^4$. Since C is regular (Theorem 7.1(c)), we get $|\Omega_2(C)| \le p^4$ and $\exp(\Omega_2(C)) = p^2$ so that $|\Omega_2(C)| = p^3$ by what has just been said. It follows that C/R has only one subgroup of order p, and hence it is cyclic. If $Z < C$ is maximal such that $R \not\le Z$ (Z exists since $R \not\le \Phi(C)$), then Z is cyclic of index p in C. Since $R \le \mathrm{Z}(C)$, the subgroup C is abelian of type (p^n, p) as in (c). □

Note that the p-groups G, $p > 2$, such that $\mathrm{C}_G(x)$ is abelian of type (p^n, p) for some $x \in G$ of order p were studied in great detail in the rarely cited important Blackburn's result (see Theorem A.38.10); that paper yields essential additional information on groups in part (c) of Theorem 134.2.

A subgroup A of a p-group G is said to be *soft* in G, if it satisfies $\mathrm{C}_G(A) = A$ and $|\mathrm{N}_G(A) : A| = p$ (see §130). Thus soft subgroups are abelian. A subgroup C from Theorem 134.2(c) is soft. Moreover, if a nonnormal $R < G$ is of order p^2, then we get $|\mathrm{N}_G(R) : \mathrm{C}_G(R)| = p$, and if, in addition, $\mathrm{C}_G(R)$ is abelian, then it is soft in G. Soft subgroups have a number of remarkable properties (see [Het4] and further papers of L. Hethelyi listed in MathSciNet; see also §130). One of such properties is proved in the following remark (note that this proof is distinct from the original one due to L. Hethelyi [Het4]).

Remark 1 (the result of this remark coincides with Lemma 130.2). Let A be a nonnormal maximal abelian subgroup of a p-group G, $|\mathrm{N}_G(A) : A| = p$. Let us prove that if $A < H < G$, then $|\mathrm{N}_G(H) : H| = p$ (it follows that there is only one maximal chain connecting A with G). Set $N_0 = \mathrm{N}_G(A)$; then $|N_0 : A| = p$ and N_0 is nonabelian. Set $N_1 = \mathrm{N}_G(N_0)$. Then N_0 contains $|N_1 : N_0| > 1$ conjugates of A under N_1. Since N_0 is nonabelian, the number of abelian subgroups of index p in N_0 is equal to $p + 1$ (see Exercise 1.6(a)), therefore we get $|N_1 : N_0| = p$. The intersection of all abelian subgroups of index p in N_0 coincides with $\mathrm{Z}(N_0) = Z \lhd N_1$. The quotient group N_1/Z is nonabelian since its subgroup A/Z (of index p^2) is not normal. Since $\mathrm{C}_G(A) = A$, we obtain $\mathrm{Z}(G) \le Z < A$. Let $R \le \mathrm{Z}(G)$ be of order p. Then either A/R or N_0/R is a maximal abelian subgroup of G/R since N_1/R, having a nonabelian epimorphic image of $N_1/\mathrm{Z}(G)$, is nonabelian.[2] Clearly, the pair $K/R < G/R$, where K/R is the above chosen maximal abelian subgroup of G/R containing A/R, satisfies the identity $|\mathrm{N}_{G/R}(K/R) : K/R| = p$ by the above as $K \in \{A, N_0\}$. Thus K/R is soft in G/R. By induction, there is only one maximal chain connecting K/R and G/R so there is only one maximal chain connection A and G. Indeed, there is nothing to prove in case $K = A$. If $K > A$, then $K = N_0$ so the result also holds since N_0 is a unique subgroup of G of order $p|A|$ containing A. Similarly, by induction, we obtain the second assertion on indices.

Remark 2. If R and G are as in Theorem 134.2, then every subgroup $H \le G$ such that $R < H$ and $\exp(H) = p$ has order $\le p^p$. Indeed, we have $|\mathrm{C}_H(R)| = p^2$ so H is

[2] In fact (see Lemma 130.1), N_0/R is abelian, but we do not use this fact.

of maximal class (Proposition 1.8), and now the claim follows from Blackburn's theory of p-groups of maximal class (see Theorems 9.5, 9.6). Assume that there is in G a normal subgroup L of order p^{p+1} and exponent p. Then $\mathrm{C}_{RL}(R) = R$ by the modular law, so RL is of maximal class (Proposition 1.8). This is a contradiction since a p-group of maximal class cannot contain such a subgroup as L (Theorem 9.6).

The case $p = 2$ is considered in the following theorem.

If a 2-group G contains a maximal elementary abelian subgroup $R \lhd G$ of order 4, then G has no normal elementary abelian subgroup of order 2^3; the structure of such G is in some detail described in §50. Note that a minimal nonmetacyclic group X of order 2^5 satisfies $|\Omega_1(X)| = 4$ and $\mathrm{d}(X) = 3$ (the group X is special).

Theorem 134.3. *Suppose that a nonabelian 2-group G contains a maximal elementary abelian subgroup R of order 4 and assume that R is not normal in G. Then one of the following holds:*

(a) *The centralizer $\mathrm{C}_G(R)$ has a cyclic subgroup of index 2 (so it is abelian).*

(b) *The centralizer $\mathrm{C}_G(R) = Q \times Z$, where Q is a generalized quaternion group and $|Z| = 2$.*[3]

Proof. Set $C = \mathrm{C}_G(R)$; then $\Omega_1(C) = R$. As R is not normal in G, the subgroup C has no metacyclic subgroup of order 16 and exponent 4 by Proposition 134.1, and this allows us to describe the structure of C.

If C is abelian, we get case (a) since C has no abelian subgroup of type $(4, 4)$ and so $|\Omega_2(C)| \leq 2^3$ (see the proof of Theorem 134.2).

Suppose that C is nonabelian. Then C contains a minimal nonabelian subgroup A. As $\Omega_1(A) \leq \Omega_1(C) = R$, it follows that A is metacyclic (Lemma 65.1). Assume that $|A| > 8$. Then $R < A$ since $\Omega_1(A) \cong \mathrm{E}_4 \cong R = \Omega_1(C)$, so $R = \Omega_1(A) \leq \mathrm{Z}(A)$, and we infer that A has no cyclic subgroup of index 2 (otherwise, A will be abelian). Since, by Proposition 134.1, A has no metacyclic subgroup of order 16 and exponent 4, we get a contradiction. Therefore $|A| = 8$. As $A \ncong \mathrm{D}_8$, we obtain $A \cong \mathrm{Q}_8$. Thus all minimal nonabelian subgroups of C are isomorphic to Q_8. It follows that $C = Q \times Z$, where Q is a generalized quaternion group and $|Z| = 2$ (see Corollary A.17.3), and the proof is complete. □

Proposition 134.4 ([GM, Lemma 2.5] for $p > 2$). *Suppose that a p-group G that is not a 2-group of maximal class contains a non-G-invariant maximal elementary abelian subgroup R of order p^2. Then G has only one normal elementary abelian subgroup of order p^2 unless $p = 2$, and G contains a proper subgroup of order 2^4 that is isomorphic to the group $\mathrm{D}_8 * \mathrm{C}_4$ of order 16.*

[3] In this case, $\mathrm{Z}(G) = \Omega_1(Q)$ has order 2 since this subgroup is characteristic in C and $\mathrm{Z}(G)$ is cyclic. It follows that $\mathrm{C}_G(Z) = C$. The 2-groups G containing an involution x such that $\mathrm{C}_G(x) = Q \times \langle x \rangle$, where Q is either cyclic or a generalized quaternion group, are described in §§48, 49.

Proof. Assume that E and F are distinct G-invariant abelian subgroups of type (p, p) in G. Since $\mathrm{Z}(G)$ is cyclic, we get $E \cap F = U$, where $U = \Omega_1(\mathrm{Z}(G))$ so $|E \cap F| = p$ and the subgroup $H = EF$ has order p^3 by the product formula. For the subgroups E/U and F/U we get $E/U, F/U \leq \mathrm{Z}(G/U)$. If H is abelian, it is elementary, and so $R \not\leq H$. In case that H is nonabelian, it is either of exponent $p > 2$ or isomorphic to D_8 (this follows from the description of groups of order p^3). In that case, all noncyclic subgroups of index p in H are normal in G since $H/U \leq \mathrm{Z}(G)$ and $U = \Phi(H)$. It follows that $R \not\leq H$, again. Write $D = HR$; then $\Omega_1(D) = D$ and, as $U = H \cap R$ has order p, we get $|D| = p^4$ by the product formula. Since E/U and F/U are central subgroups of G/U, it follows that $D/U \cong \mathrm{E}_{p^3}$ so that $\mathrm{d}(D) = 3$ and $\mathrm{cl}(D) = 2$.

Suppose that H is abelian. Then $\mathrm{C}_D(R)$ is of exponent p so it coincides with R by hypothesis, and it follows from Proposition 1.8 that $\mathrm{cl}(D) = 3 > 2$, contrary to the last sentence of the previous paragraph.

Now let H be nonabelian. By Proposition 10.17, we have $\mathrm{C}_D(H) \not\leq H$ since D is not of maximal class, and so $\mathrm{Z}(D)$ has order p^2. It follows that $\mathrm{Z}(D)$ is cyclic (otherwise, we obtain $R < R\mathrm{Z}(D) \cong \mathrm{E}_{p^3}$, contrary to the hypothesis). In that case, we have $p = 2$ (if $p > 2$, then $D = \Omega_1(D)$ is of exponent p, a contradiction). It follows that $D \cong \mathrm{D}_8 * \mathrm{C}_4$ has order 2^4 (note that $\mathrm{D}_8 * \mathrm{C}_4 \cong \mathrm{Q}_8 * \mathrm{C}_4$). □

In particular, if, in Proposition 134.4, $p > 2$, then G has only one normal abelian subgroup of type (p, p), as asserted in [GM, Lemma 2.5].

Definition. A proper subgroup A of a p-group G is said to be *generalized soft* if, whenever $A \leq H < G$, then $|\mathrm{N}_G(H) : H| = p$. (In that case, there is only one maximal chain connecting A and G, but the converse is not true.)

In the following proposition we consider the p-groups containing a subgroup of order p that is, as a rule, generalized soft.

Proposition 134.5. *Suppose that a p-group G contains a subgroup L of order p such that there is only one maximal chain connecting L and G. Then one of the following holds:*

(a) *G is abelian with cyclic subgroup of index p.*

(b) $G = \langle a, b \mid a^{p^n} = b^p = 1,\ b^a = a^{1+p^{n-1}} \rangle \cong \mathrm{M}_{p^{n+1}}$.

(c) *G is a p-group of maximal class.*[4]

Proof. Write $N = \mathrm{N}_G(L)$; then N/L is cyclic. If $N = G$, we have case (a). Next we assume that $N < G$. If $|N/L| = p$, then G is of maximal class by Proposition 1.8. Now assume that $|N/L| > p$. Since L is not G-invariant, it is not characteristic in N so N is not cyclic. Let $R = \Omega_1(N)$ and $N_1 = \mathrm{N}_G(R)$. Since R is characteristic in N, we get $N < N_1$. By hypothesis, N_1/R is cyclic. Since $R < N < N_1$, it follows that

[4]Not all p-groups of maximal class contain such a subgroup as L (for example, a p-group G of maximal class, $p > 3$, such that $|\Omega_1(G)| = p^{p-1}$ has no such subgroup).

$R = \Omega_1(N_1)$ is characteristic in N_1, and we conclude that $N_1 = G$. In that case, G/R is cyclic so G possesses a cyclic subgroup of index p hence $G \cong \mathrm{M}_{p^{n+1}}$ by Theorem 1.2. □

Remark 3. Below we describe the pairs $L < G$ of 2-groups such that $L \cong \mathrm{E}_4$, L is not G-invariant and there is only one maximal chain connecting L with G. We write $C = \mathrm{C}_G(L)$; then $C < G$. One may assume that $L < C$ (otherwise, G is of maximal class by Proposition 1.8). In that case, $C/L > \{1\}$ is cyclic so C is a maximal abelian subgroup of G of rank 2 or 3. If $|C/L| = 2$, then we obtain that $C \in \{\mathrm{E}_8, \mathrm{C}_4 \times \mathrm{C}_2\}$. Such G are described in §§50, 77. Next assume that $|C/L| > 2$. Let $\mathrm{d}(C) = 3$. Then $T = \Omega_1(C) \cong \mathrm{E}_8$ is a proper characteristic subgroup in C. In that case, we see that $\mathrm{N}_G(T)/T > C/T > \{1\}$ is cyclic by hypothesis, and so $T = \Omega_1(\mathrm{N}_G(T))$ is characteristic in $\mathrm{N}_G(T)$, and we conclude that $\mathrm{N}_G(T) = G$ hence $\Omega_1(G) = T$. It follows that $G/\Omega_1(G)$ is cyclic and $\Omega_1(G) \cong \mathrm{E}_8$. Then G has a cyclic subgroup of index 4 (such G are described in §74). Now let C be abelian of rank 2; then $L = \Omega_1(C)$ so C has a cyclic subgroup of index 2 by Proposition 134.1. In that case, $\mathrm{N}_G(L)/L$ is cyclic by hypothesis. Therefore it follows from $L < C < \mathrm{N}_G(L)$ that $L = \Omega_1(\mathrm{N}_G(L))$ is characteristic in $\mathrm{N}_G(L)$ so $\mathrm{N}_G(L) = G$, i.e., $L \lhd G$, contrary to the hypothesis.

2^o. In this subsection we prove two theorems. We suppose that the p-groups R, E and G appearing in these theorems satisfy the following

Hypothesis. (1) $p > 2$, R is a nonnormal maximal elementary abelian subgroup of order p^2 of a p-group G.

(2) E is a maximal elementary abelian subgroup of G, $E \neq R$.

(3) G is not of maximal class.

Let us prove that if R and G satisfy the Hypothesis, then $\mathrm{Z}(G)$ is cyclic. Indeed, $\mathrm{Z}(G) < \mathrm{C}_G(R)$ and $\Omega_1(\mathrm{C}_G(R)) = R$ so that $\Omega_1(\mathrm{Z}(G)) < R$, and our claim follows.

Theorem 134.6. *Let p, G, R, E be as in the Hypothesis. Suppose that* $\exp(R^G) = p$ *and let $R^G \leq M \lhd G$, where M is as large as possible subjecting* $\exp(M) = p$. *Then one of the following holds:*

(a) *The subgroups R^G and M are of maximal class, $|M| \leq p^p$.*

(b) *If G is irregular, then $|M| = p^p$.*

(c) *If $|\Omega_1(G)| = p^p$, then $G/\Omega_1(G)$ is cyclic.*

(d) *If $|M| = p^p$, then ME is of maximal class and order p^{p+1} so that $|E| \leq p^p$.*

Theorem 134.7. *Let p, G, R, E be as in the Hypothesis. Suppose that* $\exp(R^G) > p$. *Then the following hold:*

(a) *There is $M \lhd G$ of order p^p and exponent p. Write $H = MR$ and $F = MC$, where $C = \mathrm{C}_G(R)$; then H is of maximal class and order p^{p+1}, $H < F$.*

(b) *Let $H < T \leq G$, where $|T : H| = p$; then the subgroup T is not of maximal class and $T = M\Omega_2(C)$ is the unique subgroup of G of order $p|H|$ containing H so that $\mathrm{N}_G(H)/H$ is cyclic.*

(c) *F/M is abelian of type (p^{n-1}, p), $H \lhd F$ and F/H is cyclic of order p^{n-1}.*

(d) *If $R < B < H$ with $|B : R| = p$, then B is nonabelian and $\mathrm{C}_G(B)$ is cyclic.*

(e) *The subgroup H is not normal in G.*

(f) $\Omega_1(\mathrm{Z}(G)) \leq \mho_1(C)$.

(g) *If $|ME : M| > p$, then $R \not\leq ME$.*

(h) *If $A \lhd G$ is of order $p^k < p^p$ and exponent p, then $A < M$.*

Our proofs of Theorems 134.6 and 134.7 are essentially based on Blackburn's theory of p-groups of maximal class (see §9) and Hall's results on regular p-groups (see §7). In both theorems G is nonabelian.

Remark 4. If R is as in the Hypothesis, then it is not contained in $\Phi(G)$. Assume, by way of contradiction, that $R \leq \Phi(G)$; then $\Phi(G)$ is noncyclic. In this case, there is in $\Phi(G)$ a G-invariant abelian subgroup L of type (p, p) (Lemma 1.4). As $L \leq \mathrm{Z}(\Phi(G))$ (consider $\mathrm{C}_G(L)$!), the subgroup RL is elementary abelian properly containing R, a contradiction. It follows from $\mathrm{Z}(G) < \mathrm{C}_G(R)$ that $\mathrm{Z}(G)$ is cyclic (see the paragraph following the Hypothesis.

Note that if G satisfies the Hypothesis, it has no normal subgroup of order p^{p+1} and exponent p. Indeed, assume that $B \lhd G$ is of order p^{p+1} and exponent p. Write $H = BR$. By Theorem 9.6(c), H is not of maximal class as $B \leq H$ so that $\mathrm{C}_H(R) > R$ (Proposition 1.8), and we conclude that $\mathrm{C}_B(R) \not\leq R$. If $L < \mathrm{C}_B(R)$ is of order p is such that $L \not\leq R$, then $RL = R \times L$ is an elementary abelian p-group properly containing R, which is a contradiction. Thus B does not exist.

Proof of Theorem 134.6. By Proposition 1.8, if $R < K \leq G$ and $\exp(K) = p$, then K is of maximal class and order $\leq p^p$. Therefore, by assumption, $\exp(G) > p$. Obviously, G is nonmetacyclic.

In this theorem $\exp(R^G) = p$. Since R is not normal in G, we get $R < R^G$. Let M be a maximal G-invariant subgroup of exponent p containing R^G. Then, by Proposition 1.8, the subgroups R^G and M are of maximal class as $\mathrm{C}_M(R) = R = \mathrm{C}_{R^G}(R)$ (see part (1) of the Hypothesis). By Proposition 1.8 and Theorem 9.5, we obtain that $|M| \leq p^p$. Set $Q = MC$, where $C = \mathrm{C}_G(R)$. Since, by Theorem 134.2(c), C is abelian of type (p^n, p), $n > 1$, and $R = M \cap C$, then $Q/M \cong C/(C \cap M) = C/R$ is cyclic of order p^{n-1}.

(i) By Theorem 7.2(b), if G is regular, then $M = \Omega_1(G)$. There is no further restriction on the structure of G in this case.

We claim that if G is irregular, then $|M| = p^p$. Indeed, by Theorem 12.1(a), there is $N \lhd G$ of order p^p and exponent p since, by assumption, G is not of maximal class.

As we know, $M \le p^p$. One may assume that $M \not\le N$ (otherwise, there is nothing to prove). Let N_1 be a G-invariant subgroup of N satisfying $N_1 \not\le M$ and such that N_1 is as small as possible. Then $|MN_1| = p|M| \le p^{p+1}$ hence $\exp(MN_1) = p^2$ by the choice of M. Therefore MN_1 is irregular hence $|MN_1| \ge p^{p+1}$ (Theorem 7.1(b)), and we conclude that MN_1 is of maximal class and order p^{p+1} (Theorem 7.2(b)). Since $M \not\le \Phi(MN_1)$ (otherwise, we have $MN_1 = N_1$, contrary to the proved equality $|MN_1| = p^{p+1}$), we infer that $|MN_1 : M| = p$ (Exercise 9.1(b)); then $|M| = p^p$, as asserted. It is important in what follows that $R < M$.

(ii) Let $T/M \le G/M$ be of order p such that $T \not\le Q(= MC)$ (see the second paragraph of the proof; such a T exists if and only if G/M is noncyclic). Since

$$\mathrm{C}_T(R) = T \cap C = R,$$

the subgroup T is of maximal class (Proposition 1.8).

(iii) In what follows we suppose that $|M| = p^p$ (this is the case provided G is irregular by (i), however, we do not assume here that G is irregular). Set $W = ME$, where $E < G$ is as in part (2) of the Hypothesis. We claim that W is of maximal class. This is the case if $E < M$. Now let $E \not\le M$; then $M < W$. To prove our claim, take $M < U \le ME$ such that $|U : M| = p$. By the modular law, we get $U = M(U \cap E)$ so that $\Omega_1(U) = U$. Assume that $\exp(U) = p$. Then U is not of maximal class since $|U| = p^{p+1}$ (Theorem 9.5) so that $\mathrm{C}_U(R) > R$ (Proposition 1.8), which is a contradiction. Thus $\exp(U) > p$ so that U is irregular (Theorem 7.2(b)). As $|U| = p^{p+1}$, we conclude that U is of maximal class (Theorem 7.1(b)). Thus all subgroups of order p^{p+1} lying between M and $W = ME$ are of maximal class. It follows from Exercise 10.10 that W is also of maximal class. By Exercise 9.1(b),

$$|W| = p|M| = p^{p+1}$$

since $M \not\le \Phi(W)$, and we conclude that $|E| < |W| = p^{p+1}$.

(iv) Suppose that $|\Omega_1(G)| = p^p$; then $M = \Omega_1(G)$ (see the definition of M in the second paragraph of the proof). Assume that G/M is noncyclic. Assume, in addition, that $p = 3$. Then G has no elementary abelian subgroup of order p^3. In this case, however, G/M is cyclic by Theorem 13.7, contrary to the assumption. Thus $p > 3$. Since $Q/M = MC/M$ is cyclic, there is $T/M < G/M$ of order p such that $T/M \not\le Q/M$ (Proposition 1.3); then $T \not\le Q$. It follows that $T \cap Q = M$ so that $\mathrm{C}_T(R) = R$, and Proposition 1.8 implies that T is of maximal class. Since $|T| = p^{p+1}$, we infer that T is irregular (Theorem 9.5). Let $T < L \le G$ be such that $|L : T| = p$. The subgroup L is not of maximal class since $M \lhd L$, $|L| > p^{p+1}$ and M is of order p^p and exponent p (see Theorem 9.6(c)). Therefore, by Theorem 12.12(b), $L/\mathrm{K}_p(L)$ is of order p^{p+1} and exponent p. It follows that L has no absolutely regular subgroup of index p (otherwise, $|L/\mathfrak{V}_1(L) \le p^p$). Let $D < M$ be G-invariant of order p^2 and set $V = \mathrm{C}_G(D)$; then V is maximal in G as $D \not\le \mathrm{Z}(M)$ in view of $|\mathrm{Z}(M)| = p < |D|$. The intersection $M \cap V = \Omega_1(V)$ has order p^{p-1} hence V is absolutely regular since it is not of maximal class in view of $D \le \mathrm{Z}(V)$ (Theorem 12.1(b)). Then $L \cap V$, as

a subgroup of the absolutely regular group V, is absolutely regular of index p in L, contrary to what has been said above. Thus G/M is cyclic, as was to be shown. The proof of our theorem is completed. □

Proof of Theorem 134.7. By hypothesis, in this case $\exp(R^G) > p$ hence R^G is irregular in view of $\Omega_1(R^G) = R^G$ (Theorem 7.2(b)). Since G is not of maximal class, there is $M \lhd G$ of order p^p and exponent p (Theorem 12.1(a)). We have $R \not\leq M$ since $\exp(R^G) > p = \exp(M)$.

(i) We claim that $H = MR$ is of maximal class and order p^{p+1}. Indeed, we have $|M \cap R| = p$ since $\mathrm{Z}(G)$ is cyclic, and so $|MR| = p^{p+1}$ by the product formula. Next, $\mathrm{C}_H(R) = H \cap \mathrm{C}_G(R) = R$ since $\mathrm{C}_H(R) = R * \mathrm{C}_M(R) = R$ by the modular law, and our claim follows from Proposition 1.8 (in the case under consideration, $\exp(\mathrm{C}_H(R)) = p$ by Theorems 7.1(b) and 7.2(b) since $\mathrm{cl}(\mathrm{C}_H(R)) < p$).

(ii) Let $R < S < H$, where $|H : S| = p$; then we get $S = R(S \cap M)$ by the modular law, so $\exp(S) = p$ since $\Omega_1(S) = S$ and $|S| = p^p$ (Theorems 7.1(b) and 7.2(b)). If $H \lhd G$, then, considering the action of G on maximal subgroups of H via conjugation, we obtain $S \lhd G$ (indeed, since $\exp(H) = p^2$ and $\mathrm{d}(H) = 2$, H has at most p maximal subgroups of exponent p and one of them, namely M, is normal in G), and this is a contradiction since $R^G \leq S$ and $\exp(R^G) > \exp(S)$. Thus H is not normal in G.

(iii) Write $F = MC$; then we obtain $MR = H < F$ since $|F| \geq p^2|M| > |H|$ (recall that $R \not\leq M$ and $\exp(C) > p$; see Theorem 134.2(c)). Let $H < T \leq G$, where $|T : H| = p$; then T is not of maximal class since $M \lhd T$ (Theorem 9.6(c)). Then we have $\mathrm{C}_T(R) > R$ (Proposition 1.8) so that $\Omega_2(C) < T$. By the product formula, we obtain $T = M\Omega_2(C) \leq MC = F$ so that T is the unique subgroup of $\mathrm{N}_G(H)$ of order $p|H|$ containing H, and we infer that $\mathrm{N}_G(H)/H$ is cyclic since $p > 2$ (Proposition 1.3). By Theorem 12.12(b), $T/\mathrm{K}_p(T)$ is of order p^{p+1} and exponent p so that

$$\begin{aligned}\mho_1(T) = \mathrm{K}_p(T) = \mathrm{K}_p(H) = \mathrm{Z}(M) = \mho_1(H) = \mho_1(\Omega_2(C))\\ = R \cap \mathrm{Z}(G) = \Omega_1(\mathrm{Z}(G)).\end{aligned}$$

It follows that F/M is abelian of type (p^{n-1}, p) so that $H \lhd F$ and hence F/H is cyclic of order p^{n-1}. If $R < B < H$ with $|B : R| = p$, then B is nonabelian of order p^3 and exponent p, and $\mathrm{C}_T(B) = \Omega_2(C)$; moreover, $\mathrm{C}_G(B)$ is cyclic since $R < B$.

(iv) Let $|M| = p^p$ and $|ME : M| > p$. We have to prove that $R \not\leq ME$. Assume that this is false. Since $R \cap M = \mathrm{Z}(M)$ is of order p, we have $|MR| = p^{p+1}$ by the product formula. Next, $\mathrm{C}_{MR}(R)$, being of exponent p, coincides with R, and we conclude that MR is of maximal class (Proposition 1.8). Let $M < U < ME$ be such that $|U : M| = p$ and $U \neq MR$. As $U = M(U \cap E)$ by the modular law, we obtain that $\Omega_1(U) = U$. Assume that $\exp(U) = p$. Write $H = UR$ (note that $U \lhd ME$). Since H is not of maximal class (Theorem 9.6(c)), we get $\mathrm{C}_H(R) > R$. Again by the modular law, we conclude that $\mathrm{C}_H(R) = M(U \cap \mathrm{C}_H(R))$ so that $\exp(\mathrm{C}_H(R)) = p$,

contrary to Theorem 134.2(c) since H is neither metacyclic nor of maximal class (note that MR is also of maximal class). Hence we obtain that $\exp(U) > p$ so U is irregular (Theorem 7.2(b)). Since $|U| = p|M| = p^{p+1}$, it follows that U is of maximal class (Theorem 7.1(b)). Thus all subgroups of G of order $p|M|$ lying between M and ME are of maximal class. Therefore ME is also of maximal class (Exercise 10.10). Since $M \not\leq \Phi(ME)$, we get $|ME : M| = p$ (Exercise 9.1(b)), contrary to the assumption.

(v) Now let $A \lhd G$ be of order $p^k < p^p$ and exponent p. We have to prove that A satisfies $A < M$, where M is as in part (a) of the statement of our theorem. This is true for $k = 1$ since $\mathrm{Z}(G)$ is cyclic. Now assume that we have proved that any normal subgroup of G of order $< p^k$ and exponent p is contained in M. Set $J = AM$. Then, by assumption, $|A \cap M| = p^{k-1}$. By the product formula, we infer that $|J| = p^{p+1}$. Due to Exercise 9.1(b), J is not of maximal class since it has two nonincident proper normal subgroups of different orders. It follows that $\mathrm{cl}(J) < p$, and we conclude that J is regular (Theorem 7.1(b)). Since $\Omega_1(J) = J$, it follows from Theorem 7.2(b) that $\exp(J) = p$. This is a contradiction since, as we have noticed (see the paragraph preceding the proof of Theorem 134.6), G has no normal subgroup of order p^{p+1} and exponent p. Thus we get $A < M$. □

Exercise 1. Theorem 134.7(h) also holds under the condition of Theorem 134.6. (*Hint*. Argue as in part (v) of the proof of Theorem 134.7.)

Exercise 2. Suppose that a pair of p-groups $R < G$ satisfy the Hypothesis. If M and N are two distinct G-invariant subgroups of order p^p and exponent p, then MN is of maximal class and order p^{p+1}.

Solution. Let $A < M$ be a G invariant subgroup of index p. By Theorem 134.7(h) and Exercise 1, we get $A < N$ so that MN is of order p^{p+1}. As we know, $\exp(MN) = p^2$ so MN is irregular. It follows that MN is of maximal class.

Exercise 3. Suppose that R is a nonnormal maximal elementary abelian subgroup of a p-group G, $p > 2$. Then $C = \mathrm{C}_G(R)$ is abelian with cyclic subgroup of index p unless $\mathrm{N}_G(R)$ is either metacyclic or a 3-group of maximal class.

Solution. By Theorem 13.7, C is metacyclic. Set $N = \mathrm{N}_G(R)$; then $|N : C| = p$. Since N has no normal elementary abelian subgroup of order p^3, the result follows from Theorem 13.7.

Remark 5. Suppose that G is a p-group and $M \lhd G$ is of order p^p and exponent p such that every subgroup of order p^{p+1} between M and G has an exponent p^2. Then G has no elementary abelian subgroup of order p^{p+1}. Indeed, let $E \leq G$ be elementary abelian and let $E \not\leq M$ (otherwise, there is nothing to prove). Write $H = ME$ and let $H < U \leq G$, where $|U : H| = p$. Then, by hypothesis, $\exp(U) = p^2$. By the modular law, $U = M(U \cap E)$ so that $\Omega_1(U) = U$, and hence U is of maximal class (Theorems 7.1(b) and 7.2(b)) and order p^{p+1}. Since U is arbitrary, we conclude as

above that the group G is of maximal class and order p^{p+1} (Exercise 10.10). It follows that $|E| \leq p^p$, as asserted. (This argument is the same as in part (iv) of the proof of Theorem 134.7.)

Problems

Problem 1. Suppose that G, $p > 2$, possesses a maximal elementary abelian subgroup of order p^2 and $H \leq G$. (i) Is it true that $\mathrm{d}(H) \leq p$? (ii) Is it true that $|H| < p^{p+1}$ provided $\exp(H) = p$?

Problem 2. Suppose that G, $p > 2$, possesses a maximal elementary abelian subgroup of order p^n. Is it true that G has no elementary abelian subgroup of order $p^{1+p^{n-1}}$?

Problem 3. Study the p-groups all of whose minimal nonabelian (so all nonabelian) subgroups are generalized soft.

Problem 4. Study the p-groups containing a cyclic generalized soft subgroup of order p^n. (The problem is nontrivial even for $n = 2$.)

In the following three problems R is a nonnormal maximal elementary abelian subgroup of order p^2 in a p-group G.

Problem 5. Study the structure of R^G, where $\exp(R) > p$. Consider in detail the case when R^G is of maximal class.

Problem 6. Study the structure of G provided R^G is of maximal class.

Problem 7. Study the structure of G provided $\mathrm{C}_G(R)$ is metacyclic.

Problem 8. Study the p-groups G containing a nonabelian subgroup B of order p^3 such that $\mathrm{C}_G(B)$ is cyclic. (See the statement of Theorem 134.7.)

§135

Finite p-groups generated by certain minimal nonabelian subgroups

Recall that a group is said to be minimal nonabelian if it is nonabelian but all its proper subgroups are abelian. A nonabelian group contains a minimal nonabelian subgroup. Therefore it is natural to believe that minimal nonabelian groups essentially impact on the structure of a nonabelian group.

As many places of our book show, knowledge of all minimal nonabelian subgroups of a nonabelian p-group G allows us to do strong conclusions on its structure. This is analogous to impact of minimal nonnilpotent subgroups on the structure of a nonnilpotent group (this is true in view of Frobenius' normal p-complement theorem). To justify our thought, we present the following two examples (other examples are given after the proof of Lemma 135.5):

(i) If a p-group G possesses at most $p^2 + p + 1$ minimal nonabelian subgroups, then all its subgroups of index p^3 are abelian (see §76).

(ii) If all minimal nonabelian subgroups of a 2-group G have the same order 8, then either the Hughes subgroup has index 2 in G or $G = H\mathrm{Z}(G)$, where H is either of maximal class or extraspecial and $\mho_1(\mathrm{Z}(G)) \leq \mathrm{Z}(H)$ (see Theorem 90.1).

In what follows all considered groups have prime power order.

Let $\mathcal{MA}(G)$ be the set of all minimal nonabelian subgroups of a p-group G. If G is nonabelian, we have, by Lemma 135.7 below, $G = \langle \mathcal{MA}(G) \rangle$, i.e., G is generated by all members of the set $\mathcal{MA}(G)$ (this result is important in the proof of assertion (i) above). Since minimal nonabelian subgroups are small, that result shows that in a complicated p-group G the set $\mathcal{MA}(G)$ is large. However, in some cases, certain well-described subsets of that set also generate G, and in what follows we present some of such subsets.

There is, for $p > 2$, only one, up to isomorphism, minimal nonabelian p-group generated by elements of order p and its order is p^3 (Exercise 1.8(a)). We denote this group by $S(p^3)$. The dihedral group D_8 of order 8 is the only minimal nonabelian 2-group generated by involutions.

Let k be a positive integer and let $\mathcal{MA}_k(G)$ be the set of minimal nonabelian subgroups A of a p-group G such that $A = \Omega_k(A)$. Since for any p-group $X > \{1\}$ we

have $\exp(X/\Omega_1(X)) < \exp(X)$, it follows that if $A \ncong \mathrm{D}_8$ is as above and $k > 1$, then

$$(*) \qquad \exp(A) \le \exp(\Omega_1(A)) \cdot \exp(A/\Omega_1(A)) \le p \cdot p^{k-1} = p^k,$$

since, in view of $|A'| = p$, the quotient group $A/\Omega_1(A)$ is abelian of exponent $\le p^{k-1}$ and $\exp(\Omega_1(A)) = p$.

In the following paragraph we shall use the following fact. Let G be a nonabelian p-group. Further, assume that all containing $\Phi(G)$ subgroups of G of order $p|\Phi(G)|$ are abelian. Then $\mathrm{C}_G(\Phi(G))$ possesses all subgroups T of G of order $p|\Phi(G)|$ such that $\Phi(G) < T$. Since all such T generate G, it follows that $\Phi(G) \le \mathrm{Z}(G)$.

Let G be a nonabelian p-group. Suppose that $\Phi(G) \not\le \mathrm{Z}(G)$. In this case, there is a sequence $\Phi(G) = T_0 < T_1 < \cdots < T_{\mathrm{d}(G)} = G$ of subgroups and $A_1, \ldots, A_{\mathrm{d}(G)}$ of minimal nonabelian subgroups such that T_1 is nonabelian and, for $i = 1, \ldots, \mathrm{d}(G)$, one has $A_i \le T_i$ but $A_i \not\le T_{i-1}$ (Lemma 135.7 below); then $|T_i : T_{i-1}| = p$ and $A_i T_{i-1} = T_i$. It follows that

$$G = T_{\mathrm{d}(G)} = \langle A_1\Phi(G), A_2, \ldots, A_{\mathrm{d}(G)}\rangle = \langle A_1, A_2, \ldots, A_{\mathrm{d}(G)}\rangle.$$

Thus, in the case under consideration, G is generated by $\mathrm{d}(G)$ minimal nonabelian subgroups. If, however, $\Phi(G) \le \mathrm{Z}(G)$, the same argument shows that G is generated by $\mathrm{d}(G) - 1$ minimal nonabelian subgroups (note that there is a containing $\Phi(G)$ subgroup of G of order $p|\Phi(G)|$ that is not contained in $\mathrm{Z}(G)$). The obtained estimate is not best possible (for example, an extraspecial group G of order p^{1+2m} is generated by $m < 2m = \mathrm{d}(G)$ minimal nonabelian subgroups since it is a central product of m nonabelian subgroups of order p^3).

Let $k = \delta(G)$ denote the minimal number of minimal nonabelian subgroups, say $A_1, \ldots, A_k$, generating a nonabelian p-group G. Set

$$T_0 = \Phi(G), \quad T_1 = \Phi(G)A_1, \quad T_2 = T_1A_2, \quad \ldots, \quad T_k = T_{k-1}A_k = G.$$

Since, for all i, $\Phi(A_i) \le \Phi(G)$ has index p^2 in A_i, we get $|T_i : T_{i-1}| \le p^2$. It follows that

$$p^{\mathrm{d}(G)} = |G : \Phi(G)| = |T_k : T_{k-1}| \ldots |T_1 : T_0| \le p^{2k} = p^{2\delta(G)},$$

and we obtain

$$\delta(G) \le \mathrm{d}(G) \le 2\delta(G).$$

As we have noticed, the lower estimate is attained for extraspecial p-groups. This estimate can be slightly improved in the case $\Phi(G) \le \mathrm{Z}(G)$.

In this section, however, we study the generation of a nonabelian p-group G by minimal nonabelian subgroups satisfying certain additional properties.

Write

$$\mathrm{D}_k(G) = \langle \mathcal{MA}_k(G)\rangle, \quad \mathrm{D}_k^*(G) = \langle A \mid A \in \mathcal{MA}_k(G), \exp(A) = p^k\rangle.$$

Obviously, $\mathrm{D}_k(G), \mathrm{D}_k^*(G) \le \Omega_k(G)$.

In what follows we establish criteria guaranteeing the equality $\mathrm{D}_k(G) = G$ and also study the p-groups G satisfying $\mathrm{D}_k(G) < G$ for a positive integer k (see Theorem 135.1(b) and Remark 2).

Let us prove that if G is a nonabelian regular group of exponent p^e, then we have $G = \mathrm{D}_e^*(G)$. Assume that G is a counterexample of minimal order. Then we conclude that $e > 1$ (Lemma 135.7) and G is not minimal nonabelian. Setting $H = \Omega_{e-1}(G)$, we have $\exp(H) = p^{e-1}$ (Theorem 7.2(b)). By Lemma 135.7, there exists a minimal nonabelian subgroup $A < G$ such that $A \not\leq H$; then $\exp(A) = p^e$. If $M \in \Gamma_1$ is nonabelian of exponent p^e, then we get $\mathrm{D}_e^*(M) = M$ by induction (such M exist: take M containing A). By Theorem 7.2(b), there exists in G at most one maximal subgroup of exponent p^{e-1} (otherwise, $H = G$). Therefore all other members of the set Γ_1 have exponent p^e. Since the number of abelian maximal subgroups in G is 0, 1 or $p+1$ and $|\Gamma_1| \equiv 1 \pmod p$, there are at least p nonabelian members of the set Γ_1. It follows that there are in Γ_1 at least $p-1$ nonabelian members of exponent p^e. Since G is nonabelian regular, we have $p > 2$ so $p - 1 > 1$. It follows that there is a nonabelian $N \in \Gamma_1 - \{M\}$ of exponent p^e. By induction, we see that $\mathrm{D}_e^*(N) = N$. Therefore $\mathrm{D}_e^*(G) \geq \mathrm{D}_e^*(M)\mathrm{D}_e^*(N) = MN = G$, contrary to the assumption.

It is proved in Lemma 30.3 that if a nonabelian 2-group $G = \Omega_1(G)$, then we have $G = \mathrm{D}_1(G)$. To clear up our path, we offer another proof of this equality. Since G is nonabelian, it contains two noncommuting involutions a and b. Then $\langle a, b\rangle$ is dihedral so it contains a subgroup $A \cong \mathrm{D}_8$. Set $H = \mathrm{D}_1(G)$. Let $x \in G - A$ be an involution. If $x \in \mathrm{C}_G(A)$, we get $U = A\langle x\rangle = A \times \langle x\rangle$. There are in U exactly four maximal subgroups not containing x, and these subgroups generate U and are isomorphic to D_8, and we conclude that $x \in U \leq H$. Now assume that x does not centralize A. In this case, there is in $A = \Omega_1(A)$ an involution y such that $xy \neq yx$. Then $\langle x, y\rangle$ is dihedral so it is generated by subgroups isomorphic to D_8, and again $x \in \langle x, y\rangle \leq H$. Thus all involutions are contained in H so $H \geq \Omega_1(G) = G$.

Considering the group $S(p^3)$ as an analog of D_8, we note that a result similar to the result of the previous paragraph does not hold for $p > 2$ as a Sylow p-subgroup Σ_{p^2} of the symmetric group of degree p^2 shows. Indeed, Σ_{p^2} has exactly two maximal subgroups, say E and M, both of exponent p, E is abelian and M is nonabelian,[1] and so $\mathrm{D}_1(G) = M < G$ (Lemma 135.7) since M is nonabelian in view of $\mathrm{cl}(\Sigma_{p^2}) = p > 2$, and any $L \in \Gamma_1 - \{M.E\}$ satisfies $\mathrm{D}_1(L) = L \cap E$ hence $\mathcal{MA}_1(L) = \varnothing$.

As Theorem 30.1(d) shows, if a nonabelian p-group $G = \Omega_1(G)$, $p > 2$, has no subgroup $\cong \Sigma_{p^2}$, then G is generated by subgroups isomorphic to $S(p^3)$. However, the proof of this result was omitted there. Here (see Theorem 135.1(a)) we offer its

[1]The group $G = \Sigma_{p^2}$ is the wreath product of two groups of order p. Let E be the base of G; then E is elementary abelian of order p^p and $G = \langle x\rangle \cdot E$ is a semidirect product, $o(x) = p$. Next, we have $\mathrm{C}_G(x) = \langle x\rangle \times \mathrm{Z}(G)$, where $|\mathrm{Z}(G)| = p$, so $|\mathrm{C}_G(x)| = p^2$, and hence G is of maximal class (Proposition 1.8). Set $M = \langle x\rangle \cdot \Phi(G)$; then $M = \Omega_1(M)$ is regular so $\exp(M) = p$. The set $E \cup M$ contains exactly $2p^p - p^{p-1} - 1$ elements of order p, and this number coincides with the number of elements of order p in G. Thus G has exactly two maximal subgroups E and M of exponent p.

proof independent of Theorem 30.1. Next, we study in Theorem 135.1(b) the p-groups $G = \Omega_1(G)$, $p > 2$, such that $\mathrm{D}_1(G) < G$.

Remark 1. Let $G = \Omega_1(G)$, $p > 2$, be a nonabelian p-group. Suppose that whenever $x, y \in G$ are noncommuting elements of order p, then $\mathrm{D}_1(\langle x, y\rangle) = \langle x, y\rangle$. We claim that then $G = \mathrm{D}_1(G)$. By hypothesis, G, being nonabelian, contains a subgroup $L \cong S(p^3)$. Let $H = \mathrm{D}_1(G)$; then $H > \{1\}$. Assume that $H < G$. Then there is $x \in G - H$ of order p. If $x \in \mathrm{C}_G(L)$, then $U = \langle x, L\rangle = \langle x\rangle \times L$. Since U is generated by p^2 its maximal subgroups not containing x, and all these subgroups are isomorphic to $L \cong S(p^3)$, we get $x \in H$, a contradiction. Now assume that $x \notin \mathrm{C}_G(L)$. Then there is $y \in L^{\#}$ (of order p) such that $xy \neq yx$. In this case, by hypothesis, the nonabelian subgroup $\langle x, y\rangle = \mathrm{D}_1(\langle x, y\rangle)$ hence $x \in H$, a contradiction. Thus we have $H = G$.

Theorem 135.1. *Let $G = \Omega_1(G)$ be a nonabelian p-group, $p > 2$. Then*

(a) (Theorem 30.1(d)) *If G has no subgroup isomorphic to Σ_{p^2}, then $G = \mathrm{D}_1(G)$.*

(b) (Locating of elements of order p) *Suppose that $H = D_1(G) < G$ and E is a maximal by inclusion normal elementary abelian subgroup of G. Then the set $H \cup E$ contains all elements of G of order p. Next, E is a unique maximal normal elementary abelian subgroup of G, $|E| \geq p^p$ and $G = HE$; in particular, $\Phi(H) \leq H$.*

Corollary 135.2. *The result of Remark 1 follows from Theorem 135.1*(a).

Proof. Our group G has no subgroup isomorphic to Σ_{p^2} since Σ_{p^2} is generated by two noncommuting elements of order p and, as we have noticed, $\mathrm{D}_1(G) < G$. Therefore the result follows from Theorem 135.1(a). □

The next lemma is useful in proofs by induction (see the proofs of Lemma 135.8 and Theorem 135.1).

Lemma 135.3 (= Lemma 30.2). *Let k be a positive integer and A a proper subgroup of a p-group $G = \Omega_k(G)$ such that $\Omega_k(A) = A$. Then we have $A \leq M \in \Gamma_1$, where $M = \Omega_k(M)$. In particular, there are two distinct $U, V \in \Gamma_1$ such that $\Omega_k(U) = U$ and $\Omega_k(V) = V$.*

Lemma 135.4. *Suppose that a nonabelian p-group G has an abelian subgroup A of index p. If $|G : G'| = p^2$, then G is of maximal class.*

Proof. We proceed by induction on $|G|$. One may assume that $|G| > p^3$. By Lemma 1.1, $|\mathrm{Z}(G)| = \frac{1}{p}|G : G'| = p$ so $\mathrm{Z}(G)$ is a unique minimal normal subgroup of G. Since $\mathrm{Z}(G) < G'$ and

$$|G/\mathrm{Z}(G) : G'/\mathrm{Z}(G)| = |G : G'| = p^2,$$

the quotient group $G/\mathrm{Z}(G)$ is of maximal class by induction, and the result follows since $|\mathrm{Z}(G)| = p$. □

Lemma 135.5. *Suppose that $A < G$ is a normal abelian subgroup of a p-group G such that $A \not\leq \mathrm{Z}(G)$. Then for every $x \in G - \mathrm{C}_G(A)$ there is $a \in A$ such that $\langle x, a\rangle$ is a minimal nonabelian subgroup.*[2]

Proof. Let $x \in G - \mathrm{C}_G(A)$. Bringing to mind our aim, one may assume, without loss of generality, that $G = A\langle x\rangle$; then $\mathrm{C}_A(x) = U =: A \cap \mathrm{Z}(G)$. One may also assume that $|A : U| = p$ (if not, let us consider instead of A an x-invariant subgroup $A_1 \leq A$ of order $p|U|$ such that $U < A_1$). Since G is nonabelian, the quotient group G/U is noncyclic. It follows that $G/U = (\langle x, U\rangle/U) \times (A/U)$ is abelian of type (p^k, p), where p^k is the order of x modulo U. In this case, G/U contains two distinct cyclic subgroups M/U and N/U of order p^k so maximal in G/U. Then M, N are abelian maximal subgroups of G, and we see that $\mathrm{Z}(G) = M \cap N$ has index p^2 in G. By Lemma 1.1, $|G'| = \frac{1}{p}|G : \mathrm{Z}(G)| = p$. Let $a \in A - U (= A - \mathrm{C}_G(x))$ and set $H = \langle x, a\rangle$; then H is nonabelian, $|H'| = |G'| = p$ and $\mathrm{d}(H) = 2$. From Lemma 65.2(a) it follows that H is minimal nonabelian. □

Below we offer some applications of Lemma 135.5.

Suppose that all minimal nonabelian subgroups of a nonabelian 2-group G have the same order 8. Let A be a maximal abelian normal subgroup of G. By Lemma 135.5, all elements of the set $G - A$ have order 2 or 4. Assume that there is $x \in G - A$ of order 4. Then there is $a \in A$ such that $H = \langle a, x\rangle$ has order 8. Since $\Phi(G) \leq H \cap A$, it follows that $x^2 \in A$, and we conclude that $\Phi(G) \leq A$. Such groups are classified in Theorem 90.1.

Let $p > 2$ and A be a maximal abelian normal subgroup of a nonabelian p-group G of exponent $> p$. If all minimal nonabelian subgroups of G are isomorphic to $\mathrm{S}(p^3)$, then A is equal to the Hughes subgroup $\mathrm{H}_p(G)$ of G. Indeed, by Lemma 135.5, all elements of the set $G - A$ have order p, and we conclude that $\mathrm{H}_p(G) \leq A$ as $\exp(A) > p$. Since A is generated by elements of maximal order, we get, in fact, $\mathrm{H}_p(G) = A$.[3]

Suppose that all minimal nonabelian subgroups M of a nonabelian p-group G satisfy $\Omega_k(M) \leq \mathrm{Z}(M)$, where k is a fixed positive integer. We claim that if A is a normal abelian subgroup of G such that $\exp(A) \leq p^k$ and $|A|$ is as large as possible, then $\Omega_k(G) \leq A$. Assume that there is an element $x \in G - A$ of order $\leq p^k$. Then $\langle x, A\rangle$ is nonabelian (Corollary 10.2) so $A \not\leq \mathrm{Z}(G)$. In this case, there is in A an element a such that $H = \langle a, x\rangle$ is minimal nonabelian. By hypothesis, $x, y \in \mathrm{Z}(H)$ so H is abelian, a contradiction. Thus x does not exist, and we conclude that $\Omega_k(G) \leq A$; moreover, $\Omega_k(G) = A$.

Lemma 135.6. *Suppose that $G = \Omega_k(G)$ is a nonabelian p-group, $p^k > 2$. Then the set $\mathcal{MA}_k(G)$ is not empty.*

[2] In particular, if $A < G$ is a maximal normal abelian, then for each $x \in G - A$ there is $a \in A$ such that the subgroup $\langle x, a\rangle$ is minimal nonabelian. This important result, which is due to Z. Janko, coincides with Lemma 57.1.

[3] According to Mann's commentary to item 115 in Research problems and themes I, one has the equality $|G : A| = p$.

Proof (compare with the proof of Lemma 30.4(a)). Let $E < G$ be a G-invariant abelian subgroup of exponent $\leq p^k$ of maximal order. Take $x \in G - E$ of order $\leq p^k$. Then $H = \langle x, E\rangle$ is nonabelian by Corollary 10.2. By Lemma 135.5, there is $a \in E$ such that the subgroup $B = \langle x, a\rangle$ is minimal nonabelian. Since $o(x) = o(a) \leq p^k$, we get $\Omega_k(B) = B$. By (∗), $\exp(B) \leq p^k$ so that $B \in \mathcal{MA}_k(G)$. □

Lemma 135.7 (= Theorem 10.28). *A nonabelian p-group is generated by minimal nonabelian subgroups.*

We present an application of Lemma 135.7. Let $G = D \times C$, where $D \cong \mathrm{D}_8$ and $C \cong \mathrm{C}_{2^n}$ $(n > 2)$. At first sight, the set $\mathcal{MA}(G)$ has no member of exponent 2^n. But this is false. Indeed, we have $\Omega_{n-1}(G) = D \times \Omega_{n-1}(C) < G$. By Lemma 135.7, there is $M \in \mathcal{MA}(G)$ such that $M \not\leq \Omega_{n-1}(G)$ hence $\exp(M) = 2^n$.

Note that Lemma 135.7 follows from Lemma 135.5. Indeed, if, in Lemma 135.5, A is a maximal normal abelian subgroup of G, then $x \in G - A$ is contained in some minimal nonabelian subgroup of G. Since $\langle G - A\rangle = G$, our claim follows.

The following lemma covers a partial case of Theorem 135.1(a) (but it does not follow from that theorem).

Lemma 135.8. *Suppose that a nonabelian p-group $G = \Omega_1(G)$ has no subgroup isomorphic to Σ_{p^2}. If G possesses an elementary abelian subgroup V of index p, then we have* $\exp(G) = p$.

Proof. Since G is nonabelian, we get $p > 2$. By hypothesis, there is $x \in G - V$ of order p; then $G = \langle x\rangle \cdot V$ is a semidirect product with kernel V. Let $x \in F \in \Gamma_1$; then $F = \langle x\rangle \cdot (F \cap V)$ by the modular law, so $\Omega_1(F) = F$. By induction, $\exp(F) = p$. Thus every maximal subgroup of G containing x has exponent p. If $|G| \leq p^p$, it is regular so of exponent p (Theorems 7.1(b), 7.2(b)). Next we assume that $|G| \geq p^{p+1}$. If $|G : G'| = p^2$, then G is of maximal class (Lemma 135.4) so we get $G \cong \Sigma_{p^2}$ by Exercise 9.13, a contradiction. Thus $|G : G'| > p^2$. Since $\Omega_1(G) = G$, it follows that G/G' is elementary abelian. Set $H = \langle x\rangle \cdot G'$; then G/H is elementary abelian of order $> p$. Let $T_1/H, \ldots, T_n/H$ be all maximal subgroups of G/H; then $n \geq p + 1$. By the above, $\exp(T_i) = p$ for all $i \leq n$. Therefore it follows from $G = \bigcup_{i=1}^{n} T_i$ that $\exp(G) = p$. □

Proof of Theorem 135.1. (a) Let G be a counterexample of minimal order; then we get $|G| > p^3$ and $\exp(G) > p$ by Exercise 1.8(a) and Lemma 135.7 so G is irregular and $|G| \geq p^{p+1}$. All proper nonabelian subgroups $H = \Omega_1(H)$ of G satisfy $\mathrm{D}_1(H) = H$ by induction. Due to Lemmas 135.6 and 135.3, there is a nonabelian $U \in \Gamma_1$ such that $\Omega_1(U) = U$; then $\mathrm{D}_1(U) = U$ by induction. By the last assertion of Lemma 135.3, there exists $V \in \Gamma_1 - \{U\}$ such that $\Omega_1(V) = V$. One may assume that $V \neq \mathrm{D}_1(V)$ (otherwise, $\mathrm{D}_1(G) = \mathrm{D}_1(UV) \geq \mathrm{D}_1(U)\mathrm{D}_1(V) = UV = G$). Then V is elementary abelian by induction. If $x \in G - V$ is of order p, then $G = \langle x\rangle \cdot V$, a semidirect product with kernel V, and now the result follows from Lemmas 135.8 and 135.7 since G has no subgroup isomorphic to Σ_{p^2}.

(b) By hypothesis, we get $H = \mathrm{D}_1(G) < G$. Let E be a normal elementary abelian subgroup of G such that $|E|$ is as large as possible. Assume that there is an element $x \in G - (H \cup E)$ of order p. Set $L = \langle x, E\rangle$. By Corollary 10.2, L is nonabelian. If L is regular, then it follows from $\Omega_1(L) = L$ that $\exp(L) = p$ by Theorem 7.2(b), and so $L = \mathrm{D}_1(L)$ by Exercise 1.8(a) and Lemma 135.7, a contradiction since $L \not\leq H$ by the choice of x. Thus L is irregular so $|E| \geq p^p$ (Theorem 7.1(b)). Assume that $|\mathrm{Z}(L)| = p$. It follows from Lemma 135.4 that L is of maximal class (indeed, we have $|G : G'| = p|\mathrm{Z}(G)| = p^2$ by Lemma 1.1) so $L \cong \Sigma_{p^2}$ by Exercise 9.13). In that case, $U = \langle x, \Phi(L)\rangle$ is nonabelian (by Fitting's lemma) of exponent p (Theorem 7.2(b)) so $U = \mathrm{D}_1(U)$; then $x \in U \leq H$, contrary to the choice of x. Thus $|\mathrm{Z}(L)| > p$. Note that $\mathrm{Z}(L) = \mathrm{C}_E(x)$. Let $T/\mathrm{Z}(L)$ be an L-invariant subgroup of order p in $E/\mathrm{Z}(L)$ so T is elementary abelian. Then $V = \langle x, T\rangle$ is nonabelian since x does not centralize T, and $\Omega_1(V) = V$. We have $\mathrm{cl}(V) = 2$ since $|V/\mathrm{Z}(L)| = p^2$. It follows from this and $p > 2$ that $\exp(V) = p$ (Theorems 7.1(b) and 7.2(b)). Then, by Lemma 135.7 and Exercise 1.8(a), we have $V = \mathrm{D}_1(V)$, and we obtain $x \in V \leq H$, a contradiction. Thus the set $G-(H\cup E)$ has no elements of order p, as was to be shown. Since $G = \Omega_1(G)$ and the subgroup HE ($\supset H \cup E$) contains all elements of G ($= \Omega_1(G)$) of order p, we conclude that $G = HE$. Because $G/H \cong E/(E \cap H)$ is elementary abelian, we get $\Phi(G) \leq H$. In particular, $E \not\leq H$ since, by assumption, $H < G$.

Assume that $E_1 < G$ is another maximal G-invariant elementary abelian subgroup. Then EE_1 is nonabelian, by Corollary 10.2, so it is of class 2 (Fitting's lemma). It follows that $\exp(EE_1) = p$ (Theorems 7.1(b) and 7.2(b)) so $\mathrm{D}_1(EE_1) = EE_1$ by Exercise 1.8(a) and Lemma 135.7, and we conclude that $E < EE_1 \leq H$, contrary to the last sentence of the previous paragraph. □

The subgroup E from Theorem 135.1(b) has the following property: If $x \in G - E$ is of order p, then the subgroup $H_x = \langle x, E\rangle$ contains a subgroup isomorphic to Σ_{p^2}. Indeed, since $E \not\leq \mathrm{D}_1(G)$, it follows that $\mathrm{D}_1(H_x) < H_x$, and the claim follows from Theorem 135.1(a).

Theorem 135.1(a) can be restated as follows:

If $p > 2$, then for a nonabelian p-group G one of the following holds:

(i) $\Omega_1(G)$ is elementary abelian.

(ii) G contains a subgroup isomorphic to Σ_{p^2}.

(iii) $\mathrm{D}_1(G) = \Omega_1(G)$.

Assume that $p > 2$. The group Σ_{p^2} satisfies the hypothesis of Theorem 135.1(b). Let $G = \Sigma_{p^2} \times L$, where $L > \{1\}$ is elementary abelian p-group. Let $M, E < \Sigma_{p^2}$ be maximal of exponent p, M be nonabelian and E be abelian. Write $W = \mathrm{D}_1(G)$. We claim that $W = M \times L$. By Lemma 135.7 and Exercise 1.8(a), we get $M \times L \leq W$. It remains to prove the reverse inclusion $W \leq M \times L$. Let $S(p^3) \cong A < G$ and set $F = LA$; then $\exp(F) = p$, F is nonabelian so $\mathrm{D}_1(F) = F$. We have to prove that $A < M \times L$. By the modular law, $F = L \times (F \cap \Sigma_{p^2})$ so that $T = F \cap \Sigma_{p^2}$ is nonabel-

ian of exponent p since $\exp(F) = p$ and $L \leq \mathrm{Z}(F)$. We get $T \cong S(p^3)$ as $|T| = p^3$. It follows that $T \leq \mathrm{D}_1(\Sigma_{p^2}) = M$. Thus $A < LT \leq LM$ so that $W = LM$. Therefore the set of p-groups satisfying the hypothesis of Theorem 135.1(b) is infinite.

Remark 2. Let $k > 1$ and $G = \Omega_k(G)$ be a nonabelian p-group. Suppose that G is such that $\mathrm{D}_k(G) < G$. Then G possesses only one maximal G-invariant abelian subgroup A of exponent $\leq p^k$. The set $A \cup \mathrm{D}_k(G)$ contains all elements of orders $\leq p^k$ so that $G = A\mathrm{D}_k(G)$. In particular, $A \not\leq \mathrm{D}_k(G)$ and $G' \leq \mathrm{D}_k(G)$. Indeed, we have $\mathcal{MA}_k(G) \neq \varnothing$ (Lemma 135.6) so $\mathrm{D}_k(G) = H > \{1\}$. By hypothesis, $H < G$. Let A be a G-invariant abelian subgroup of exponent $\leq p^k$ such that $|A|$ is as large as possible. We claim that the set $H \cup A$ contains all elements of orders $\leq p^k$. Assume that this is false. Then there exists an element $x \in G - (H \cup A)$ of order $\leq p^k$. Set $F = \langle x, A\rangle$; then F is nonabelian by Corollary 10.2 since $p^k > 2$. By Lemma 135.5, there is an element $a \in A$ such that $L = \langle x, a\rangle$ is minimal nonabelian. As $o(x), o(a) \leq p^k$, it follows that $\Omega_k(L) = L$, and we conclude that $x \in L \in \mathcal{MA}_k(G) = H$ by $(*)$, contrary to the choice of x. Thus x does not exist. Since $HA\ (\supset H \cup A)$ is normal in G and the set $H \cup A$ contains all elements of G of orders $\leq p^k$, we get $G = \Omega_k(G) \leq HA$ so that $G = HA$. In particular, $A \not\leq H$ and $G' \leq H$ since $G/H \cong A/(H \cap A)$ is abelian. Assume that there is another maximal G-invariant abelian subgroup A_1 of exponent $\leq p^k$. By the above, $A_1 \not\leq H$. Therefore, since $A_1 \subset H \cup A$, it follows that $A_1 = (A_1 \cap H) \cup (A_1 \cap A)$ is a union of two nonincident subgroups, which is impossible.

The groups from Theorem 135.1(b) and Remark 2 deserve further investigation. In particular, we do not even know if a group G from Remark 2 satisfying $\mathrm{D}_k(G) > G$ does exist.

Write $\mu_k(G) = |\mathcal{MA}_k(G)|$. Clearly, $\mu_k(G) = \mu_k(\mathrm{D}_k(G))$.

Proposition 135.9. *Let G be a 2-group with nonabelian $\Omega_1(G)$. Then*

(a) $\mu_1(G) = 1$ *if and only if* $G \in \{\mathrm{D}_8, \mathrm{SD}_{16}\}$.

(b) $\mu_1(G) = 2$ *if and only if* $G \in \{\mathrm{D}_{16}, \mathrm{SD}_{32}\}$.

(c) $\mu_1(G) = 3$ *if and only if* $\Omega_1(G) = D * C$, *the central product, where* $D \cong \mathrm{D}_8$, *C is cyclic of order 4 and* $D \cap C = \mathrm{Z}(D)$. *Next,* $\bar{G} = G/\mathrm{C}_G(D) \in \{\mathrm{E}_4, \mathrm{D}_8\}$. *If* $\bar{G} \cong \mathrm{E}_4$, *then* $G = D * \mathrm{C}_G(D)$, *where* $\mathrm{C}_G(D)$ *is cyclic. If* $\bar{G} \cong \mathrm{D}_8$, *then we have $G = DQ$, where $D \cap Q = \mathrm{Z}(D)$ and Q is either cyclic or a generalized quaternion group, Q is not G-invariant,* $|Q : \mathrm{C}_G(D)| = 2$. *In the second case, G is as in Theorem 43.9 (in this case, G contains exactly seven involutions).*

Proof. Note that $\mu_1(G) = \mu_1(\Omega_1(G))$. Since $\Omega_1(G)$ is nonabelian, we conclude that $\mu_1(G) \geq 1$. As we know, all members of the set $\mathcal{MA}_1(G)$ are isomorphic to D_8.

Let $D \in \mathcal{MA}_1(G)$. If $\mathrm{C}_G(D) < D$, then we see that G is of maximal class by Proposition 10.17. In this case, if $|G| = 2^n$, then we get $\mu_1(G) = 2^{n-3}$ if $G \cong \mathrm{D}_{2^n}$ and $\mu_1(G) = 2^{n-4}$ if $G \cong \mathrm{SD}_{2^n}$ (clearly, $\mu_1(\mathrm{Q}_{2^n}) = 0$). Therefore, if $\mu_1(G) = 1$, then

$G \in \{\mathrm{D}_8, \mathrm{SD}_{16}\}$, and if $\mu_1(G) = 2$, then we have $G \in \{\mathrm{D}_{16}, \mathrm{SD}_{32}\}$. If $\mathrm{C}_G(D) \not\leq D$, let $L \leq \mathrm{C}_G(D)$ be cyclic of minimal order such that $L \not\leq D$; then we get $|L| \leq 4$. In case $|L| = 2$, we obtain that $\mu_1(DL) = \mu_1(D \times L) = 4 > 3$, a contradiction. If $|L| = 4$, then $DL = D*L$ is the central product of order 16, and then $\mu_1(DL) = 3$. The cases (a), (b) are completed.

Now let $\mu_1(G) = 3$; then G is not of maximal class. One may assume from the start that $D \lhd G$. If $L_1 \neq L$ is another cyclic subgroup of order 4 in $\mathrm{C}_G(D)$ (see the previous paragraph), then $\mu_1(DL_1) = 3$ and then $\mu_1(G) \geq 5$, a contradiction. Thus L is the unique cyclic subgroup of order 4 in $\mathrm{C}_G(D)$. Then we have $\mu_1(\mathrm{C}_G(D)) = 0$. Indeed, if $D_1 \in \mathcal{MA}_1(\mathrm{C}_G(D))$, then, since $\mu_1(\mathrm{C}_G(D)) \leq 2$, $\mathrm{C}_G(D)$ is of maximal class by (a) and (b), so $DD_1 = D * D_1$ is extraspecial of order 2^5. If $L_0 < D_1$ is cyclic of order 4, then $\mu_1(D*L_0) = 3$ by the above. As $D_1 \not\leq D*L_0$, we get $\mu_1(D*D_1) > 3$, a contradiction. It follows that $\mathrm{C}_G(D)$ is cyclic by Theorem 1.17(b). In this case, we have $\Omega_1(G) = D * L$, where L is cyclic of order 4 since $\Omega_1(G) = \mathrm{D}_1(G)$.

The quotient group $G/\mathrm{C}_G(D) \in \{\mathrm{E}_4, \mathrm{D}_8\}$ is a subgroup of a Sylow 2-subgroup of $\mathrm{Aut}(D) \cong \mathrm{S}_4$ containing $D/\mathrm{Z}(D) \cong \mathrm{E}_4$.

If $G/\mathrm{C}_G(D) \cong \mathrm{E}_4$, then $G = D * \mathrm{C}_G(D)$, where $\mathrm{C}_G(D)$ is cyclic.

Let $\bar{G} = G/\mathrm{C}_G(D) \cong \mathrm{D}_8$. Let $\bar{x} \in \bar{G} - \bar{D}$ be an involution and $Q = \langle x, \mathrm{C}_G(D)\rangle$. Then Q has only one subgroup of order 2 coinciding with $\mathrm{Z}(D)$ so Q is either cyclic or a generalized quaternion group. In that case, G is as in Theorem 43.9(b, c). □

Let G be a 2-group with $\mu_1(G) = 4$. Take $\mathrm{D}_8 \cong D < G$. If $\mathrm{C}_G(D) < D$, then G is of maximal class so $G \in \{\mathrm{D}_{32}, \mathrm{SD}_{64}\}$. Next we assume that $\mathrm{C}_G(D) \not\leq D$. Assume that $\mathrm{C}_G(D) = C > \{1\}$ is cyclic. Then $\mu_1(DC) = 3$. Let $\mathrm{D}_8 \cong D_1 \not\leq CD$. Since G is not of maximal class, $\mathrm{C}_G(D_1) \not\leq D_1$. In this case, we obtain $\mu_1(D_1\mathrm{C}_G(D_1)) \geq 3$ so $\mu_1(G) \geq 5 > 4$, a contradiction. Thus $\mathrm{C}_G(D)$ is noncyclic. If $G = D \times R$, where $R > \{1\}$ is either cyclic or generalized quaternion, then $\mu_1(G) = 4$.

It is easy to show that if a 2-group G contains exactly one subgroup $\cong \mathrm{Q}_8$, then we have $G \in \{\mathrm{Q}_8, \mathrm{SD}_{16}, \mathrm{Q}_8 * \mathrm{C}_{2^n}\}$ (the last group has order $2^{n+2} \geq 2^4$). It is not easy to classify the 2-groups with exactly two or three subgroups isomorphic to Q_8.

Proposition 135.10. *Suppose that $p > 2$ and G is a p-group with nonabelian $\Omega_1(G)$. If $\mu_1(G) = 1$, then one of the following holds:*

(a) *$G = C\Omega_1(G)$, where C is cyclic and $\Omega_1(G) \cong S(p^3)$, $|G| = p^2|C|$.*

(b) *G is a group of maximal class and order 3^4. If, in addition, $G = \Omega_1(G)$, then we have $G \cong \Sigma_{3^2}$.*

Proof. By hypothesis, we have $\mathrm{D}_1(G) \cong S(p^3)$. One may assume that $\mathrm{D}_1(G) < G$.

If $\mathrm{D}_1(G) = \Omega_1(G)$, then G has no normal elementary abelian subgroup of order p^3 so G is as in (a) or a 3-group of maximal class. In the second case, $|G| = 3^4$ so G is as in (b).[4]

[4] According to a report of Mann, the set of groups X of maximal class and order p^{p+1}, $p > 2$, satisfying $|\Omega_1(G)| = p^p$ is nonempty.

Now let $\mathrm{D}_1(G) < \Omega_1(G)$. Take $x \in \Omega_1(G) - \mathrm{D}_1(G)$ and write $H = \langle x, \mathrm{D}_1(G)\rangle$; then $\Omega_1(H) = H$. If $\exp(H) = p$, then we get $\mu_1(G) \geq p > 1$ by Theorem 5.8(b), a contradiction. Thus $\exp(H) > p$ so H is irregular, and we obtain $p = 3$ by Theorem 12.1(a). If $H = \Omega_1(G)$, then G is of maximal class by Theorem 13.5 since H has at most two subgroups of order 3^3 and exponent 3. In this case, in view of $\mathrm{D}_1(G) \triangleleft G$, we get $|G| = 3^4$ (Theorem 9.6(c)) so $G = H$. Thus we conclude that (the irregular 3-group) $G = \Omega_1(G) > \mathrm{D}_1(G)$ has only one nonabelian subgroup $\mathrm{D}_1(G)$ of order 3^3 and exponent 3 so $G \cong \Sigma_{3^2}$ by Theorem 30.6. □

Set $\alpha_1(G) = |\mathcal{MA}(G)|$. It is known (see §76) that $\alpha_1(G) \geq p$ unless G is either abelian or minimal nonabelian. Recall that a p-group is said to be an *$\mathcal{A}_2$-group* if all its subgroups of index p^2 are abelian but G has a nonabelian maximal subgroup (see §76).

Given a noncyclic p-group G, set $\Gamma_2 = \{H < G \mid \Phi(G) < H, |G : H| = p^2\}$.

Proposition 135.11. *If a p-group G possesses a proper $\mathcal{A}_2$-subgroup, then there exist $\alpha_1(G) - (2p - 3)$ pairwise distinct minimal nonabelian subgroups generating G.*

Proof. Let $H \in \Gamma_1$ be neither abelian nor minimal nonabelian (such an H exists by hypothesis). Then $\alpha_1(H) \geq p$ by Remark 76.1. The subgroup H contains a member T of the set Γ_2; then $T \neq \mathrm{Z}(G)$. Let $H_1/T = H/T, H_2/T, \ldots, H_{p+1}/T$ be all subgroups of order p in G/T; then we have $H_1 = H, H_2, \ldots, H_{p+1} \in \Gamma_1$. One may assume that $H = H_1, \ldots, H_p$ are nonabelian. By Remark 76.1, H contains $p - 1$ pairwise distinct minimal nonabelian subgroups, say $S_1, \ldots, S_{p-1}$, that are not contained in T. For $i \in \{2, \ldots, p\}$, let M_i be a minimal nonabelian subgroup of H_i that is not contained in T (if H_i is minimal nonabelian, then $M_i = H_i$). By Lemma 135.7, we have $G = \langle H_p, S_1\rangle = \langle \mathcal{MA}(H_p) \cup \{S_1\}\rangle$. Therefore

$$\begin{aligned} G &= \langle \mathcal{MA}(G) - \{S_2, \ldots, S_p, M_2, \ldots, M_{p-1}\}\rangle && \text{if } p > 2, \\ G &= \langle \mathcal{MA}(G) - \{S_2\}\rangle && \text{if } p = 2. \end{aligned}$$

The proof is complete. □

Given a subgroup N of a nonabelian p-group X, denote by $\Delta_N(X)$ the subgroup generated by all those minimal nonabelian subgroups of X which are not contained in N. If N is abelian, then $\Delta_N(X) = X$ (Lemma 135.7), and $\Delta_N(X) = \{1\}$ if and only if $N = X$ is minimal nonabelian.

Proposition 135.12. *Suppose that N is a proper subgroup of a nonabelian p-group G. If $\Delta_N(G) < G$, then $p = 2$.*

Proof. By the paragraph preceding the proposition, N is neither abelian nor minimal nonabelian. Assume, by way of contradiction, that $p > 2$. We proceed by induction on $|G|$.

First suppose that $N \in \Gamma_1$. Since $|\Gamma_1| \equiv 1 + p \pmod{p^2}$ and, by Exercise 1.6(a), the set Γ_1 contains 0, 1 or $p + 1$ abelian members, it follows that the set Γ_1 contains

at least p nonabelian members, say $N = M_1, M_2 \ldots, M_p$. Let $i > 1$. If $A \leq M_i$ is minimal nonabelian and such that $A \not\leq N \cap M_i$, then $A \not\leq N$ so that $A \leq \Delta_N(G)$. By induction, $\Delta_{N\cap M_i}(M_i) = M_i$ for $i > 1$. Therefore $M_i \leq \Delta_N(G)$ for $i > 1$. Since $p \geq 3$, we get $\Delta_N(G) \geq M_2M_3 = G$, contrary to the hypothesis.

Now suppose that a nonabelian $N \notin \Gamma_1$. Then we have $N < M_1 \in \Gamma_1$, and M_1 is nonabelian as well. By the previous paragraph, we see that $\Delta_{M_1}(G) = G$. However, $G = \Delta_{M_1}(G) \leq \Delta_N(G)$. Since, by hypothesis, $\Delta_N(G) < G$, this is a final contradiction.

Thus, if G is not minimal nonabelian, then $p = 2$. □

Let a nonabelian 2-group G be such that $\Gamma_1 = \{N, M, A\}$, where N, M are nonabelian and A is abelian. Then $\Delta_N(G) \leq M < G$. Thus the set of nonabelian 2-groups satisfying the hypothesis of Proposition 135.12 is infinite. However, some useful information on the pairs of 2-groups $N < G$ satisfying $\Delta_N(G) < G$ is contained in the following

Proposition 135.13. *Suppose that N is a proper subgroup of a nonabelian 2-group G. If $\Delta_N(G) < G$, then the following hold:*

(a) $N \in \Gamma_1$.

(b) $\Delta_N(G) \in \Gamma_1$.

(c) *If $N \cap \Delta_N(G) = T$, then there is an abelian $A \in \Gamma_1$ such that $T < A$.*

(d) *A is the unique abelian member of the set Γ_1.*

In what follows we assume that $\mathrm{d}(G) > 2$.

(e) *The set Γ_1 has no minimal nonabelian members.*

(f) *If a nonabelian $K < G$ is such that $K \not\leq \Delta_N(G)$ and $K \not\leq N$, then $K \cap N$ is nonabelian and $\Delta_{N\cap K}(K) = K \cap \Delta_N(G)$.*

(g) *If a nonabelian $L < G$ is such that $L \not\leq N$, $L \not\leq \Delta_N(G)$ and L is minimal by inclusion subjecting the above conditions, then* $\mathrm{d}(L) = 2$ *and*

$$\Delta_{L\cap\Delta_N(G)}(L) = L \cap N.$$

Proof. As we have noticed, N is nonabelian.

(i) First suppose that $N \in \Gamma_1$.

Assume that the set Γ_1 has no abelian members. Let $M \in \Gamma_1 - \{N\}$ be arbitrary and let $K \in \Gamma_1 - \{N, M\}$ be such that $N \cap M < K$. Let $S \leq K$ be minimal nonabelian such that $S \not\leq N \cap K (= N \cap M)$. Then $S \not\leq M$. As $S \leq \Delta_N(G)$, we get $\Delta_N(G) \not\leq M$. Since M is arbitrary, it follows that $\Delta_N(G)$ is not contained in any maximal subgroup of G, and we conclude that $\Delta_N(G) = G$, contrary to the hypothesis. Thus there is an abelian $A \in \Gamma_1$.

Let $\Delta_N(G) \leq M \in \Gamma_1$ and let $N \cap M < L \in \Gamma_1 - \{M, N\}$. We claim that L is abelian. Assume that this is false. Take $S \leq L$ such that $S \not\leq N \cap L (= N \cap M)$. Then

$S \not\leq M$ so that $S \not\leq \Delta_N(G)$. Since $S \not\leq N$, we get a contradiction. Thus L is abelian, and so one may assume that $L = A$.

(ii) Now we show that $N, \Delta_N(G) \in \Gamma_1$. Assume that $N \cup \Delta_N(G) \cup A \neq G$. Take $x \in G - (N \cup M \cup A)$, where $\Delta_N(G) \leq M \in \Gamma_1$. Then, by Lemma 135.5, there exists $a \in A$ such that the subgroup $U = \langle a, x \rangle$ is minimal nonabelian. By the choice of x, the subgroup U is not contained in N and $\Delta_N(G)$, which is a contradiction. Thus we get $G = N \cup \Delta_N(G) \cup A$. Then it follows from Lemma 116.3 that $N, \Delta_N(G) \in \Gamma_1$, completing the proof of (a) and (b).

(iii) Assume that there exists an abelian $A_1 \in \Gamma_1 - \{A\}$. Set $T = N \cap A_1$ and let H, N, A_1 be all maximal subgroups of G containing T. Clearly, $T \neq N \cap A$. Take $x \in H - T$. Then there is $a_1 \in A_1$ such that $M = \langle a_1, x \rangle$ is minimal nonabelian. By the choice of x, we have $M \not\leq N$ whence $M \leq \Delta_N(G)$. Such M cover the set $H - T$. Since $\langle H - T \rangle = H$, it follows that $H \leq \Delta_N(G)$. Because H and $\Delta_N(G)$ are distinct maximal subgroups of G, we get a contradiction. Thus A_1 does not exist, completing the proof of (d).

(iv) Supposing that $\mathrm{d}(G) > 2$, we will prove that the set Γ_1 has no minimal nonabelian members. Assume that this is false and let $H \in \Gamma_1$ be minimal nonabelian. Then, by hypothesis, either $H = N$ or $H = \Delta_N(G)$.

(iv1) Assume that $H = \Delta_N(G)$. Then H is the unique minimal nonabelian subgroup of G not contained in N, i.e., in the notation of §76, $\beta_1(G, N) = 1$. Then, by Lemma 76.5, $\mathrm{d}(G) = 2$, contrary to the hypothesis.

(iv2) Assume that $H = N$. Then N is the unique minimal nonabelian subgroup of G not contained in $\Delta_N(G)$, and again, as in (iv1), $\beta_1(G, \Delta_N(G)) = 1$ and $\mathrm{d}(G) = 2$, a contradiction.

Thus H does not exist, so (e) is true.

In what follows we assume that $\mathrm{d}(G) > 2$.

(v) Let a nonabelian $K < G$ be as in (f) (K exists since $\mathrm{d}(G) > 2$, for example, $K \in \Gamma_1 - \{N, \Delta_N(G), A\}$). By hypothesis, K is not minimal nonabelian. Due to Lemma 135.7, $K \cap \Delta_N(G)$ is nonabelian (otherwise, all minimal nonabelian subgroups of K are contained in $K \cap N$ so $K \leq N$ by Lemma 135.7). Let $S < K$ be minimal nonabelian such that $S \not\leq K \cap \Delta_N(G)$; then $S \not\leq \Delta_N(G)$. By hypothesis, $S < N$ so $S \leq K \cap N$. It follows that $\Delta_{K \cap \Delta_N(G)}(K) = K \cap N$. Since one of the proper subgroups $K \cap N$ and $\delta_{K \cap N}(K)$ of K is nonabelian, we infer from Lemma 135.7 that the second is also nonabelian. This completes the proof of (f).

(vi) Let L be such as in (g). Write $T = \Delta_N(G) \cap N \cap A$. Take $x \in \Delta_N(G) - T$, $y \in N - T$ such that $xy \neq yx$ (since $\langle N - T \rangle = N$, such x, y exist). Let $H = \langle x, y \rangle$; then H is nonabelian and $H \not\leq \Delta_N(G)$, $H \not\leq N$ and $H < G$ as $\mathrm{d}(H) = 2 < \mathrm{d}(G)$. Then we have $\Delta_{H \cap \Delta_N(G)}(H) = H \cap N$ by (f). If a nonabelian $L \leq H$ is minimal by inclusion such $L \not\leq \Delta_N(G)$ and $L \not\leq N$, then the above argument shows that L is the desired subgroup. □

Remark 3. Suppose that $p > 2$ and G is a p-group such that $1 < \mu_1(G) < p$ (see Proposition 11), say $\mathcal{MA}_1(G) = \{S_1, \ldots, S_k\}$, $1 < k < p$. Then all subgroups S_i are normal in G. Set $H = S_1S_2$. If $\exp(H) = p$, then, by Lemma 30.5(a), we have $\mu_1(H) \geq p > \mu_1(G)$, a contradiction. Thus we get $\exp(H) > p$ so H is irregular (Theorem 7.2(b)), and we infer that $|H| = p^4$, $p = 3$ by Fitting's lemma and Theorem 7.1(b). By Theorems 30.7 and 9.6, the group G is of maximal class and order 3^4. (In this case, $G \ncong \Sigma_{3^2}$.)

Problems

Problem 1. Study the p-groups $G = \Omega_k(G)$ containing exactly two distinct maximal subgroups U, V such that $\Omega_k(U) = U$ and $\Omega_k(V) = V$.

Problem 2. Study the nonabelian p-groups $G = \Omega_k^*(G)(= \langle x \in G \mid o(x) = p^k \rangle)$, $k > 1$, that are not generated by minimal nonabelian subgroups of exponent p^k. (See Remark 2 and Theorem 135.9.)

Problem 3. Let $k > 1$. Study the p-groups $G > \Omega_k^*(G)$ such that $H = \Omega_k^*(H)$ for all $H < G$ with $\exp(H) \geq p^k$.

Problem 4. Study the p-groups G such that

$$\Omega_1(\Phi(G)) < \Phi(G) \text{ however } \Omega_1(\Phi(H)) = \Phi(H)$$
$$(\Omega_1(G') < G' \text{ however } \Omega_1(H') = H')$$

for all $H < G$ (two problems).

Problem 5. Given $k > 1$, classify the nonabelian p-groups $G = \Omega_k(G)$ containing exactly one minimal nonabelian subgroup of exponent $\leq p^k$. (Compare this with Proposition 135.10.)

Problem 6. Classify the p-groups G, $p > 2$, with $\mu_1(G) \leq p$ (see Remark 3).

Problem 7. Classify the 2-groups G such that $\Omega_1(G) \cong \mathrm{D}_8 \times \mathrm{C}_2$.

§136

p-groups in which certain proper nonabelian subgroups are two-generator

We study the p-groups all of whose nonabelian subgroups of a fixed order are two-generator. A number of important results of this kind for abelian subgroups were proved by Blackburn and are used essentially in the Odd Order paper [FT].

Blackburn has classified the p-groups, $p > 2$, all of whose normal abelian subgroups are two-generator (see Theorem 13.7 and Theorem 69.4); for $p = 2$ this was done by the second author in §50. In contrast, in this section we study the p-groups, $p > 2$, in which certain nonabelian subgroups are two-generator. All our proofs are fairly short but involved.

It is known a comparatively small number of structure results for groups of exponent p. One of such results is Theorem 136.1.

Theorem 136.1. *Suppose that G is a nonabelian group of order p^m and exponent p and n is a fixed integer such that $3 < n < m$. Then the following assertions are equivalent:*

(a) *All nonabelian subgroups of G of order p^n are two-generator.*

(b) *G is of maximal class with abelian subgroup of index p. In particular, $m \leq p$.*

Since all nonabelian groups of order p^3 are two-generator, the hypothesis of Theorem 136.1 is fulfilled in case $n = 3$ for all nonabelian groups of exponent p. Therefore we assume there that $n > 3$. Note that $p > 3$ in this theorem (indeed, groups of exponent 3 are of class at most 2).

It is impossible to state an analog of Theorem 136.1 for nonabelian p-groups of exponent $> p$ since many such groups need not necessarily contain a nonabelian subgroup of order p^n for a fixed $n > 2$. For groups of exponent p the existence of such subgroups is due to the fact that minimal nonabelian subgroups of exponent p have order p^3 (see Lemma 136.2(ii)).

We collect in Lemma 136.2 most results used in what follows. Some results are not stated in full generality.

Lemma 136.2. *Suppose that G is a nonabelian group of order p^m.*

(i) (Theorem 5.8(b)) *If G is of exponent p and $n \in \{3, \ldots, m-1\}$, then the number of two-generator subgroups of order p^n in G is divisible by p.*

(ii) (Redei; see Lemma 65.1) *Suppose that G is minimal nonabelian. Then*

$$\mathrm{d}(G) = 2, \quad |G'| = p, \quad |G : \mathrm{Z}(G)| = p^2.$$

If $\exp(G) = p$, *then* $|G| = p^3$ *(in this case* $p > 2$*).*[1] *Next,* $|\Omega_1(G)| \leq p^3$ *and* $|G/\mathfrak{V}_1(G)| \leq p^3$.

(iii) (Exercise 13.10(a)) *Let $H < G$. If all subgroups of G of order $p|H|$ containing H are of maximal class, then G is also of maximal class.*

(iv) (Tuan; Lemma 1.1) *If $A < G$ is abelian of index p, then $|G| = p|G'||\mathrm{Z}(G)|$.*

(v) (Proposition 10.17) *If $B \leq G$ is nonabelian of order p^3 such that $\mathrm{C}_G(B) < B$, then G is of maximal class.*

(vi) (Exercise 1.6(a)) *The number of abelian subgroups of index p in G is equal to one of the numbers* 0, 1 *or* $p + 1$.

(vii) (Theorem 12.12(a)) *Suppose that G contains a subgroup H of maximal class and index p. If* $\mathrm{d}(G) = 2$, *then G is also of maximal class (otherwise, we have* $\mathrm{d}(G) = 3$*).*

(viii) (Blackburn; see Theorem 9.5) *If G of maximal class is regular (in particular, of exponent p), then $|G| \leq p^p$.*

(ix) (Hall's regularity criterion; see Theorem 9.8(a)) *If G is irregular, then we have $|G/\mathfrak{V}_1(G)| \geq p^p$. In particular, absolutely regular p-groups are regular.*

(x) (Theorem 44.12) *Suppose that N is a two-generator normal subgroup of G. If $N \leq \Phi(G)$, then N is metacyclic.*

(xi) (Lemma 30.3(a, b)) *Suppose that a p-group $G = \Omega_k(G)$ contains a subgroup $E = \Omega_k(E)$. Then we have $E \leq U \in \Gamma_k$ with $\Omega_k(U) = U$. There is also $V \in \Gamma_1 - \{U\}$ with $\Omega_k(V) = V$.*

(xii) (Blackburn; see Theorem 12.1(a)) *If a group G is neither absolutely regular nor of maximal class, it has a normal subgroup of order p^p and exponent p.*

(xiii) (Feit–Thompson [FT, Lemma 8.3]; see also Corollary 10.2) *If $E < G$ is a maximal normal elementary abelian subgroup of G, $p > 2$, then E satisfies $\Omega_1(\mathrm{C}_G(E)) = E$.*

(xiv) (Lemma 57.1) *Let $A < G$ be a maximal normal abelian subgroup. Then for any $x \in G - A$ there is $a \in A$ such that the subgroup $\langle x, a\rangle$ is minimal nonabelian.*

(xv) (Theorem 10.28) *Any nonabelian p-group G is generated by minimal nonabelian subgroups.*

(xvi) *If G contains an abelian subgroup of index p and $|G : G'| = p^2$, then G is of maximal class.*

[1] It follows from this the fact important in what follows: a nonabelian group of exponent p contains a nonabelian subgroup of order p^3.

(xvii) *If G is of order p^4 and exponent p and $\mathrm{d}(G) = 2$, then G is of maximal class.*

(xviii) *If G is a p-group of maximal class with abelian subgroup of index p, then all nonabelian subgroups of G are of maximal class so two-generator.*

Proof of Lemma 136.2(xvi). We proceed by induction on $|G|$. By Lemma 136.2(iv), $|\mathrm{Z}(G)| = \frac{1}{p}|G : G'| = p$. Write $\bar{G} = G/Z(G)$. Then

$$|\bar{G} : \bar{G}'| \leq p^2 = |G : G'|$$

so that $|\bar{G} : \bar{G}'| = p^2$. Therefore, if $|G| = p^3$, we are done. If $|G| > p^3$, then $\bar{G}$ is of maximal class by induction. Then G is also of maximal class since $|\mathrm{Z}(G)| = p$. □

Proof of Lemma 136.2(xvii). Obviously, the group G has an abelian subgroup of index p. Since $G' = \Phi(G)$ and, by hypothesis, $|G : G'| = p^2$, the result follows from Lemma 136.2(xvi). □

Proof of Lemma 136.2(xviii). One may assume that $|G| > p^3$. We proceed by induction on $|G|$. Let $H \in \Gamma_1$ be nonabelian and $A \in \Gamma_1$ be abelian. As $G = AH$, we conclude that $\mathrm{cl}(H) = \mathrm{cl}(G) - 1$ (Fitting's lemma) hence H is of maximal class. Now let $U < G$ be nonabelian. Let $U \leq H \in \Gamma_1$. By the above, H is of maximal class, and $A \cap H$ is abelian of index p in H. Therefore, by induction, U is of maximal class. □

Proof of Theorem 136.1. We first have to prove that (a) $\Rightarrow$ (b). Assume that G is a counterexample of minimal order; then G is not of maximal class. Since $\exp(G) = p$, we have $G' = \Phi(G)$.

(i) Suppose that $n = m - 1$. Since $|\Gamma_1| \equiv 1 \pmod{p}$, there is in G a non-two-generator subgroup, say A, of order p^n (Lemma 136.2(i)). By hypothesis, A is abelian. Due to Lemma 136.2(ii), G is not minimal nonabelian since $m > 4$. Therefore there is a nonabelian $M \in \Gamma_1$. We have

$$\mathrm{d}(G) \leq \mathrm{d}(M) + 1 = 3$$

since, by hypothesis, $\mathrm{d}(M) = 2$. Next, $M \cap A$ is an abelian subgroup of index p in M. As $|M : M'| = |M : \Phi(M)| = p^2$, the subgroup M is of maximal class (Lemma 136.2(xvi)). Then, by Lemma 136.2(vii), $\mathrm{d}(G) = 3$ since, by assumption, G is not of maximal class.

Assume that $m = 5$ so $n = 4$. Let $B < G$ be minimal nonabelian; then $|B| = p^3$ (Lemma 136.2(ii)). If $\mathrm{C}_G(B) < B$, then G is of maximal class (Lemma 136.2(v)), contrary to the assumption. Thus there exists $x \in \mathrm{C}_G(B) - B$. Then $K = B \times \langle x \rangle$ is nonabelian of order $p^4 = p^n$ and $\mathrm{d}(K) = 3$, contrary to the hypothesis. Thus $m > 5$.

Now we are ready to complete the proof of our implication in case $n = m - 1$. Take $N \lhd G$ such that $N < G'$ and $|G/N| = p^5$ (recall that $|G : G'| = p^3$); then $N > \{1\}$, and G/N is neither abelian nor of maximal class. Therefore there is in G/N a nonabelian maximal subgroup M/N (Lemma 136.2(ii)); then $M \in \Gamma_1$ is nonabelian. By hypothesis, $\mathrm{d}(M) = 2$ hence $\mathrm{d}(M/N) = 2$. Thus all nonabelian maximal sub-

groups of G/N are two-generator. By induction, G/N is of maximal class, which is a contradiction since $\mathrm{d}(G/N) = 3 > 2$. Thus, if $n = m - 1$, then G is of maximal class with and abelian subgroup of index p.

(ii) Now let $3 < n < m - 1$. Let $B < G$ be nonabelian of order p^n (B exists by Lemma 136.2(ii)), and let $B < H < G$, where $|H| = p^{n+1}$. By hypothesis, all nonabelian maximal subgroups of H are two-generator so H is of maximal class by (i). Thus all B-containing subgroups of G of order $p|B| = p^{n+1}$ are of maximal class. By Lemma 136.2(iii), the group G is of maximal class as well.

Take $L \in \Gamma_1$ such that $\mathrm{d}(L) > 2$ (L exists by Lemma 136.2(i)). Then either by hypothesis (provided $m = 5$) or by induction (provided $m > 5$), we conclude that the subgroup L is abelian.

The implication (b) $\Rightarrow$ (a) follows from Lemma 136.2(xviii). Finally, the inequality $m \le p$ follows from Lemma 136.2(viii). □

Remark 1. Suppose that a p-group G of order $p^m > p^4$ is neither abelian nor minimal nonabelian. We claim that all proper nonabelian subgroups of G have centers of order p if and only if G is of maximal class with abelian subgroup of index p. Indeed, all minimal nonabelian subgroups have the same order p^3 (Lemma 136.2(ii)). If $B < G$ is minimal nonabelian, then $\mathrm{C}_G(B) = \mathrm{Z}(B) < B$ is of order p. Therefore G is of maximal class (Lemma 136.2(v)). If $R \lhd G$ is of order p^2, then $\mathrm{C}_G(R)$ has no minimal nonabelian subgroups by the above, so $\mathrm{C}_G(R)$ is abelian and maximal in G. Conversely, if G is of maximal class with abelian subgroup of index p, then all proper nonabelian subgroups of G have the same center of order p (Lemma 136.2(xviii)). The simple argument above was the starting point of some subsequent considerations.

Theorem 136.3. *Suppose that G is a nonabelian group of order $p^m > p^4$ and assume that $n \in \{4, \dots, m-1\}$ is fixed. If a p-group G has a nonabelian subgroup of order p^n and all nonabelian subgroups of order p^n have centers of the same order p, then G is of maximal class.*

Proof. By hypothesis, G is neither abelian nor minimal nonabelian.

(i) Suppose that $n = m - 1$. Let $R \lhd G$ be of order p^2. Then $|G : \mathrm{C}_G(R)| \le p$. In this case, there is a maximal subgroup M of G such that $R < M \le \mathrm{C}_G(R)$. Since $R \le \mathrm{Z}(M)$ is of order $p^2 > p$, the subgroup M is abelian by hypothesis. Let $H \in \Gamma_1$ be nonabelian; then $|\mathrm{Z}(H)| = p$. In this case, H has an abelian subgroup $H \cap M$ of index p. By Lemma 136.2(iv), we have $|H : H'| = p|\mathrm{Z}(H)| = p^2$ and so, by Lemma 136.2(xvi), H is of maximal class. In this case, all nonabelian members of the set Γ_1 are of maximal class and $\mathrm{d}(G) \le \mathrm{d}(H) + 1 = 2 + 1 = 3$.

Assume, by way of contradiction, that G is not of maximal class. Then it follows from Theorem 12.12(c) that $\mathrm{d}(G) = 3$ and the number of subgroups of maximal class and index p in G is equal to p^2. As we have noticed, all nonabelian members of the set Γ_1 are of maximal class. It follows that G has exactly $(p^2 + p + 1) - p^2 = p + 1 > 1$ pairwise distinct abelian maximal subgroups so $\mathrm{cl}(G) = 2$. In this case, $\mathrm{cl}(G) = 2$

hence $\mathrm{cl}(H) = 2$, and we conclude that $|H| = p^3$. Then $|G| = p|H| = p^4 < p^m$, which is a contradiction. Thus, if $n = m - 1$, then G is of maximal class.

(ii) Now suppose that $|G| = p^m > p^{n+1} \geq p^5$. Let $H < G$ be nonabelian of order p^n and $H < F < G$, where $|F : H| = p$. Then, by hypothesis, all nonabelian maximal subgroups of F have centers of the same order p so F is of maximal class by (i). Thus all subgroups of G containing H and having order $p|H|$ are of maximal class. In this case, by Lemma 136.2(iii), the group G is also of maximal class, completing case (ii) and thereby the proof of our theorem. □

Theorem 106.3 asserts that if a 2-group G and all its nonabelian maximal subgroups are two-generator, then G is either metacyclic or minimal nonabelian. The following theorem extends this result to p-groups, $p > 3$. Note that in Theorem 136.4 we do not assume that $\mathrm{d}(G) = 2$ (we deduce this from another additional condition).

Theorem 136.4. *Suppose that all nonabelian maximal subgroups of a non-absolutely regular p-group G, $p > 3$, are two-generator. If, in addition, there is $M \in \Gamma_1$ such that $|M : M'| = p^2$, then G is of maximal class with abelian subgroup of index p.*

Proof. One may assume that $\exp(G) > p$ (otherwise, the result follows from Theorem 136.1); then $\mho_1(G) > \{1\}$. We have $|G/\mho_1(G)| \geq p^p \geq p^5$ (the last inequality holds in view of $p \geq 5$). Then, by Lemma 136.2(ii), there is in $G/\mho_1(G)$ a nonabelian maximal subgroup $H/\mho_1(G)$ hence $\mathrm{d}(H) = 2$ by hypothesis, and we obtain that $\mathrm{d}(G) \leq \mathrm{d}(H) + 1 = 2 + 1 = 3$. Therefore, since $\mho_1(G) \leq \mho_1(G)G' = \Phi(G)$ and $|G/\mho_1(G)| > p^3$, it follows that $G/\mho_1(G)$ is nonabelian. If $K/\mho_1(G) < G/\mho_1(G)$ is nonabelian of index p (such a $K/\mho_1(G)$ exists since $G/\mho_1(G)$ is not minimal nonabelian in view of Lemma 136.2(ii)), then $\mathrm{d}(K) = 2$ by hypothesis, whence we get $\mathrm{d}(K/\mho_1(G)) = 2$. Thus any nonabelian maximal subgroup of the group $G/\mho_1(G)$ (of exponent p) is two-generator. It follows that $G/\mho_1(G)$ is of maximal class by Theorem 136.1. In particular, $\mathrm{d}(G) = 2$ since $\mho_1(G) \leq \Phi(G)$. By Lemma 136.2(i), there is $A/\mho_1(G) < G/\mho_1(G)$ of index p such that $\mathrm{d}(A/\mho_1(G)) > 2$; then $\mathrm{d}(A) > 2$ hence A is abelian by hypothesis. Next, there exists $M \in \Gamma_1$ such that $|M : M'| = p^2$ by hypothesis. In this case, $M \cap A$ is an abelian maximal subgroup of M, and it follows from Lemma 136.2(xvi) that M is of maximal class. As the two-generator p-group G contains a subgroup M of maximal class and index p, we infer that G is also of maximal class by Lemma 136.2(vii). □

Theorem 136.4 is an extension of Theorem 136.1.

Supplement to Theorem 136.4. *Let a p-group G of order $> p^4$ be neither abelian nor minimal nonabelian. If for all nonabelian $M \in \Gamma_1$ we have $|M : M'| = p^2$, then G is of maximal class.*

Proof. Let $N \lhd G$ be of index p^4. Then G/N possesses an abelian subgroup A/N of index p. As $|A : A'| > p^2$, it follows by hypothesis that $A \in \Gamma_1$ is abelian. Since G

is not minimal nonabelian, there is a nonabelian $M \in \Gamma_1$. Then $M \cap A$ is abelian of index p in M so, by Lemma 136.2(xvi), M is of maximal class since $|M : M'| = p^2$. Now, repeating word for word the last part of the proof of Theorem 136.3, we complete the proof. □

All maximal subgroups of a 3-group of maximal class and order $> 3^4$ are two-generator. The same is true for 2-groups of maximal class. However, there are infinitely many 2-groups G with $\mathrm{d}(G) = 3$ all of whose maximal subgroups are two-generator; see §§70, 113.

In the proof of Theorem 136.7 we use the following two lemmas.

Lemma 136.5. *Let G be a p-group of order $> p^p$, $p > 2$. If G contains a subgroup R of order p^p and exponent p and if all such subgroups are (elementary) abelian, then $\Omega_1(G)$ is also (elementary) abelian.*

Proof. Bringing to mind our aim, one may assume that $G = \Omega_1(G)$. It remains to prove that G is abelian. We proceed by induction on $|G|$. We have $R \le U \in \Gamma_1$ such that $\Omega_1(U) = U$ and $V \in \Gamma_1 - \{U\}$ such that $\Omega_1(V) = V$ (Lemma 136.2(xi)). By induction, U and V are elementary abelian. Then we obtain that $UV = G$ so $\mathrm{cl}(G) \le 2$ (Fitting's lemma). Since G is not minimal nonabelian, we conclude that it is abelian (Theorem 136.1). □

Lemma 136.6. *Let a non-absolutely regular nonabelian group G have order p^{p+1}, $p > 3$. Suppose that all nonabelian maximal subgroups of G are two-generator. Then one of the following holds:*

(a) *$\Omega_1(G)$ is elementary abelian of order p^p and $G/\mho_1(G)$ is of maximal class so $\mathrm{d}(G) = 2$. Next, G is regular, $|\mathrm{Z}(G)| = p^2$ and G/G' is abelian of type (p^2, p). If $B \in \Gamma_1 - \{\Omega_1(G)\}$, then B/B' is abelian of type (p^2, p).*

(b) *G is of maximal class with abelian subgroup of index p.*

Proof. By Lemma 136.2(ii), G is not minimal nonabelian as $|G/\mho_1(G)| \ge p^p > p^3$. Let a nonabelian $K \in \Gamma_1$; then $\mathrm{d}(K) = 2$. By Theorem 136.1, $G/\mho_1(G)$ is nonabelian of maximal class with an abelian subgroup of index p. It follows that $\mathrm{d}(G) = 2$ since $\mho_1(G) \le \Phi(G)$. If the quotient group $A/\mho_1(G)$ is maximal in $G/\mho_1(G)$ of rank > 2 (see Lemma 136.2(i)), then A is abelian.

Suppose that G is not of maximal class; then $|\mathrm{Z}(G)| = p^2$ so that

$$\mathrm{cl}(G) = p - 1 \ge 4.$$

In this case, G is regular (Theorem 7.1(b)), and we obtain that $\Omega_1(G) = M \in \Gamma_1$ (Theorem 7.2(d)) and $\exp(M) = p$.

Assume that $M \ne A$. Then, since $\mathrm{cl}(G) > 2$, the subgroup M is nonabelian. The intersection $A \cap M$ is an abelian subgroup of index p in M. Since $\exp(M) = p$ and $\mathrm{d}(M) = 2$, we get $M' = \Phi(M)$ so that $|M : M'| = p^2$, and Lemma 136.2(xvi)

implies that M is of maximal class. As $\mathrm{d}(G) = 2$, it follows that G is of maximal class (Lemma 136.2(vii)), contrary to the assumption.

Now let $M = A$; then $M(= \Omega_1(G))$ is elementary abelian of order p^p. As we have noticed, $|\mathrm{Z}(G)| = p^2$. In this case, by Lemma 136.2(iv), $|G : G'| = p|\mathrm{Z}(G)| = p^3$ so G/G' is abelian of type (p^2, p) since $\mathrm{d}(G) = 2$.

Let $R < G'$ be G-invariant of index p. By Lemma 65.2(a), the quotient group G/R is minimal nonabelian. As $R < M$ and $M/R \cong \mathrm{E}_{p^3}$, it follows that $\Omega_1(G/R) \cong \mathrm{E}_{p^3}$. Let $B \in \Gamma_1 - \{\Omega_1(G)\}$. Since B/R is abelian of type (p^2, p), we get $\mathrm{cl}(B) \leq p - 2$. We conclude from $BM = G$ that $\mathrm{cl}(B) \geq p - 2$ (Fitting's lemma). Thus we obtain $\mathrm{cl}(B) = p - 2$, and we infer that $R = B'$ so that B/B' is abelian of type (p^2, p). □

Theorem 136.7. *Let a p-group G of order $> p^p$, $p > 3$, be not absolutely regular, and let a fixed natural number n be such that $3 < n < p$. Suppose that all nonabelian subgroups of G of order p^n and exponent p and all nonabelian subgroups of G of order p^p and exponent p^2 are two-generator. Then one of the following holds:*

(a) *$\Omega_1(G)$ is elementary abelian.*

(b) *G is of maximal class; in that case, $\Omega_1(\Phi(G))$ is (elementary) abelian.*

Proof. Suppose that $\Omega_1(G)$ is nonabelian. By hypothesis, Theorems 9.5, 9.6, 9.8 and Lemma 136.2(xii), we get $|\Omega_1(G)| \geq p^{p-1}$ with equality if and only if G is of maximal class.

Suppose that G is of maximal class. Then G is irregular and $|\Omega_1(\Phi(G))| = p^{p-1}$ (Theorems 9.5, 9.6). Since, in view of $p > 3$, $R = \Omega_1(\Phi(G))$ is not metacyclic, we obtain $\mathrm{d}(R) > 2$ (Lemma 136.2(x)) so it is elementary abelian by Theorem 136.1 if $n < p - 1$ and hypothesis if $n = p - 1$.

Next we assume that G is not of maximal class. In this case, there is in G a nonabelian subgroup R of order p^p and exponent p (Lemma 136.5), and all such subgroups are of maximal class as $n < p$ (Theorem 136.1). Take $R < S \leq G$, where $|S| = p^{p+1}$. Assume that $\exp(S) = p$. Then all nonabelian subgroups of index p in S are two-generator so S is of maximal class (Theorem 136.1), contrary to Lemma 136.2(viii). Thus we get $\exp(S) = p^2$. By Lemma 136.6, S is of maximal class as $\Omega_1(S)(\geq R)$ is nonabelian. Since S runs over the set of all subgroups of G that contain R and have order $p|R|$, it follows, in view of Lemma 136.2(iii), that G is of maximal class. □

All p-groups of maximal class with an abelian subgroup of index p satisfy the hypothesis of Theorem 136.7; however, there is a group of maximal class and order p^{p+1}, $p > 3$, that does not satisfy this hypothesis [Bla3].

Theorem 136.8. *Let G be a nonabelian p-group of order $> p^4$ and suppose that all its nonabelian subgroups of order p^4 are generated by two elements. Then one of the following holds:*

(a) *G is of maximal class.*

(b) *The subgroup $\Omega_1(G)$ is abelian.*

Proof. Assume that $H = \Omega_1(G)$ is nonabelian.

(i) We claim that if G contains a nonabelian subgroup B of order p^3, then G is of maximal class. This is the case if $C_G(B) < B$ by Lemma 136.2(v). Suppose that there is in $C_G(B) - B$ an element y of minimal possible order. Since $y^p \in Z(B)$, we get $o(y) \leq p^2$ and the subgroup $K = \langle y, B\rangle$ has order p^4 and $d(K) = 3$, contrary to the hypothesis since K is nonabelian.

By Theorem 9.6(f), a p-group G of maximal class contains an element x such that $C_G(x)$ is of order p^2. Therefore, if $C_G(x) < A < G$ with $|A : C_G(x)| = p$, then A is nonabelian of order p^3.

Next we assume, in addition, that G is not of maximal class. Then, by the above, all subgroups of G of order p^3 are abelian. Since $H = \Omega_1(G)$ is assumed to be nonabelian, we get $|H| \geq p^4$.

Assume that G has no nonabelian subgroup of order p^4. If G is regular, then we have $\exp(H) = p$. Therefore, since H is nonabelian by assumption, we get $|H| = p^3$ (Lemma 136.2(ii)). But, by assumption, all subgroups of G of order p^4 which contain H are abelian, a contradiction. Now let G be irregular. As G is not of maximal class, it follows, by Lemma 136.2(xii), that there exists $R \lhd G$ of order p^p and exponent p. Assume that $p > 2$. We claim that R is abelian. Indeed, if $p = 3$ and $R < R_1 < G$, where $|R_1| = 3^4$, then R_1 is abelian by assumption; then R is also abelian. If $p > 3$, then R is abelian since it has no minimal nonabelian subgroup. Then, by Lemma 136.5, $\Omega_1(G)$ is abelian so G is as in case (a). Now let $p = 2$. Then there are in the nonabelian subgroup H two noncommuting involutions x, y. In this case, $\langle x, y\rangle$ is dihedral so it contains a dihedral subgroup B of order 8. Then B is contained in a nonabelian subgroup of order 2^4, contrary to the assumption.

In what follows we assume that G has a nonabelian subgroup of order p^4. By the above, all subgroups of G of order p^3 are abelian. It follows that all nonabelian subgroups of G of order p^4 are minimal nonabelian. Therefore, provided $p = 2$, G has a nonabelian (dihedral) subgroup of order 8 which is contained in some overgroup of order 16 which is not minimal nonabelian. Thus we must have $p > 2$.

(ii) To obtain a contradiction, it remains to prove that the subgroup $H(= \Omega_1(G))$ is abelian. Therefore, bringing to mind our aim, one may assume, without loss of generality, that $G = H(= \Omega_1(G))$. Let $E < G$ be a G-invariant elementary abelian subgroup such that $|E|$ is as large as possible. Let $x \in \Omega_1(G) - E$ be of order p. Then we infer that $K = \langle x, E\rangle$ is nonabelian (Lemma 136.2(xiii)). If $|E| < p^3$, then $|E| = p^2$ and K is nonabelian of order p^3 and exponent p, contrary to the assumption. Thus we get $|E| > p^2$. In this case, by Lemma 136.2(xiv), there is $a \in E$ such that $B = \langle a, x\rangle$ is minimal nonabelian; then $\Omega_1(B) = B$. Therefore, by Lemma 136.2(ii), B is nonabelian of order p^3 and exponent p, a contradiction. □

Theorem 136.9. *Let G be a nonabelian group of order $p^m > p^4$.*

(a) *If $\exp(G) = p$ and G possesses only one subgroup, say H, of order p^4 such that $d(H) > 2$, then G is of maximal class and $m = 5$.*

(b) *Let $p > 3$ and let G be an irregular p-group. If G has only one subgroup, say H, of order p^4 and exponent p such that $\mathrm{d}(H) > 2$, then one of the following holds:*

(b1) *G is 5-group of maximal class, all subgroups of G of order 5^5 and exponent 5 are of maximal class.*

(b2) *$G = C\Omega_1(G)$, where $\Omega_1(G)$ is of maximal class and of order 5^5 and exponent 5, C is absolutely regular.*

(b3) *G is a group of maximal class, $|\Omega_1(G)| = 5^4$.*

Proof. (a) Assume that G is of order $p^m > p^5$ and exponent p. Let $L \lhd G$ be of order p^2; then $C = \mathrm{C}_G(L)$ has index $\leq p$ in G. If $L < B < C$ is of order p^4, then $\mathrm{d}(B) > 2$ (Lemma 136.2(xvii)). Since C of order $> p^4$ has only one non-two-generator subgroup of order p^4, it follows that C is nonabelian. By Lemma 136.2(xv), there exists a nonabelian $T < C$ of order p^3 with $T \not\leq B$. If $U < L$ is of order p such that $U \not\leq T$, then $D = T \times U \neq B$, $|D| = p^4$, $\mathrm{d}(D) > 2$ and $D \neq B$, contrary to the hypothesis. Thus $m = 5$.

Due to Lemma 136.2(i), there is $B \in \Gamma_1$ satisfying $\mathrm{d}(B) > 2$. By hypothesis, all members of the set $\Gamma_1 - \{B\}$ are two-generator so they are of maximal class (Lemma 136.2(xiii)). Assume that G is not of maximal class. Then the set Γ_1 has exactly p^2 members of maximal class (Lemma 136.2(xxi)), and all other $p + 1 > 1$ members of Γ_1 are not of maximal class so they are not two-generator (Lemma 136.2(xiii)), contrary to the hypothesis. Thus G is of maximal class and order p^5, as was to be shown.

(b) We have $\exp(G) > p$ (Theorem 7.1(b)). If the subgroup $\Omega_1(G)$ is abelian, then we see that $|\Omega_1(G)| = p^4$ by hypothesis. In this case, G is a 5-group of maximal class (Lemma 136.2(xii)) so G is as in (b3). Next we assume that $\Omega_1(G)$ is nonabelian.

Assume that G is not of maximal class. Then there is in G a subgroup R of order p^p and exponent p (Lemma 136.2(xii)). Since $p > 3$, R is nonabelian (otherwise, R contains more than one subgroup isomorphic to E_{p^4}). Then, by part (a), R is of maximal class and $p = 5$. Thus all subgroups of G of order 5^5 and exponent 5 have maximal class. Then, by Lemma 136.2(i) or Theorem 136.1, G has no subgroup of order 5^6 and exponent 5. Let $L \lhd G$ be abelian of type $(5, 5)$. It is easy to see that $C = \mathrm{C}_G(L)$ has index 5 in G (otherwise, LR is of order $> 5^5$ and exponent p). Assume that C has a G-invariant subgroup M of order 5^5 and exponent 5. Since $\exp(LM) = 5$, we get $L \leq \mathrm{Z}(M)$, a contradiction since M, by the above, is of maximal class. Thus M does not exist. Therefore, by Lemma 136.2(xv), C is absolutely regular. Lemma 136.2(xi) then yields $R = \Omega_1(G)$. Now $G = CR$ is as in (b2).

Now let G be of maximal class. Then $K = \Omega_1(\Phi(G))$ is of order p^{p-1} and exponent p. Assume that $p > 5$; then K is nonabelian by hypothesis. Since $K \leq \Phi(G)$, it follows that $|\mathrm{Z}(K)| > p$ (see Lemma 1.4). Then, by (a), K has two distinct nonabelian non-two-generator subgroups of order p^4, contrary to the hypothesis. It follows that $p = 5$. If G has no subgroup of order 5^5 and exponent 5, it satisfies the hypothesis. Now assume that G has a subgroup R of order 5^5 and exponent 5. Then, by the above, R is of maximal class, completing the proof. □

Remark 2. We present another application of Lemma 136.2(xiv). Let $G = \Omega_k(G)$ be a p-group of exponent $\geq p^k$ such that G is nonabelian but $\Omega_k(H)$ is abelian for all $H \in \Gamma_1$. We claim that then G is minimal nonabelian. In view of Lemma 136.2(xi), there is $A \in \Gamma_1$ such that $\Omega_k(A) = A$. Then A is abelian by hypothesis. Let $x \in G - A$ be of order $\leq p^k$. By Lemma 2(xiv), there is $a \in A$ such that $H = \langle a, x \rangle$ is minimal nonabelian. Since $\Omega_k(H) = H$ is nonabelian, it follows $H = G$, and we are done.

Problems

Problem 1. Suppose that a group G is neither abelian nor minimal nonabelian with $|G| = p^m$ and $p^k = \min\{|A| \mid A < G \text{ is minimal nonabelian}\}$. Let a fixed integer n be such that $k < n < m$. Study the structure of G provided all its nonabelian subgroups of order p^n are two-generator.

If $p = 2$ and $n = m - 1$, then §70 shows that the set of 2-groups satisfying the condition of Problem 1 is infinite.

Problem 2. Study the p-groups of order $> p^3$ all of whose maximal subgroups except one have derived quotient groups of index p^2. This problem is not solved even for groups of exponent p.[2]

Problem 3. Study the p-groups all of whose nonabelian subgroups of index p^2 are two-generator. (Note that the p-groups all of whose subgroups of index p^2 are abelian, are classified; see Lemma 65.1 and §71. All p-groups of maximal class with abelian subgroup of index p and 3-groups of maximal class satisfy this condition.)

Problem 4. Study the p-groups all of whose nonabelian subgroups of order p^5 are two-generator. (See Theorem 136.8.)[3]

Problem 5. Study the p-groups of order p^m and exponent p all of whose nonabelian subgroups of order p^n, $2 < n < m - 1$ (n is fixed), are nonnormal. (All p-groups of maximal class and exponent $p > 5$ with abelian subgroup of index p satisfy this condition.)

Problem 6. Classify the p-groups all of whose nonabelian subgroups of class 2 are two-generator.

Problem 7. Classify the p-groups G with exactly one nonabelian subgroup H of order p^4 such that $\mathrm{d}(H) = 3$. (See Theorem 136.9.)

Some close results are contained in §§30, 135.

[2] If $p = 2$, then G is of maximal class. Indeed, by Taussky's theorem (Lemma 1.6), all nonabelian maximal subgroups of G are of maximal class (one may assume that $|G| > 8$). Assume that G is not of maximal class. Then, by Theorem 5.4, the number of members of maximal class in the set Γ_1 is divisible by 4. Therefore the number of remaining members, say M, of the set Γ_1 is equal to 3 since $\mathrm{d}(G) = 3$, and we get a contradiction since for these M we have $|M : M'| > 4$, again by Taussky's theorem.

[3] If G is a 2-group of order $\geq 2^5$ and all its subgroups of orders 2^4 and 2^5 are two-generator, then G is metacyclic. This Blackburn's result follows from Theorem 66.1.

§137

p-groups all of whose proper subgroups have its derived subgroup of order at most p

Here we give a characterization of the title groups. In the proofs we partly use some ideas of J. Q. Zhang, X. H. Li (Proposition 137.3) and V. Ćepulić, O. C. Piljavska (Proposition 137.5). To facilitate the proof of the main result (Theorem 137.7), we shall first prove some auxiliary results.

Proposition 137.1. *Let G be a title group. Then for all $x, y \in G$ such that $\langle x, y\rangle < G$ we have $o([x, y]) \leq p$ and $[x, y] \in \mathrm{Z}(G)$.*

Proof. Suppose that $[x, y] \neq 1$. Let X be a maximal subgroup of G containing $\langle x, y\rangle$. Then $X' = \langle [x, y]\rangle \trianglelefteq G$ with $o([x, y]) = p$ and so $[x, y] \in \mathrm{Z}(G)$. □

Proposition 137.2. *If G is a title group, then G' is abelian of order $\leq p^3$.*

Proof. We may assume that G is nonabelian. Let $X \neq Y$ be two maximal subgroups of G. Then $|X'| \leq p$ and $|Y'| \leq p$. By Exercise 1.69(a), we get $|G' : (X'Y')| \leq p$ and so $|G'| \leq p^3$. By Burnside, G is abelian. □

Proposition 137.3 (Zhang and Li). *If G is a title group and $|G'| \geq p^2$, then $\mathrm{d}(G) \leq 3$.*

Proof. Since $|G'| \geq p^2$, G is not minimal nonabelian (Lemma 65.1) so there exists a maximal subgroup A with $|A'| = p$; then $A' \triangleleft G$. Suppose that $M' \leq A'$ for each maximal subgroup M of G. Then G/A' is minimal nonabelian, and we get $\mathrm{d}(G/A') = 2$ (Lemma 65.1), $A' \leq \Phi(G)$ and so $\mathrm{d}(G) = 2$, completing this case.

We may assume that G has a maximal subgroup B such that $B' \not\leq A'$. In that case, we get $|A'| = |B'| = p$ and $A' \cap B' = \{1\}$. Let $a_1, a_2 \in A$ and $a_3, a_4 \in B$ be such that $A' = \langle [a_1, a_2]\rangle$ and $B' = \langle [a_3, a_4]\rangle$. Since $|\langle a_1, a_2, a_3, a_4\rangle'| \geq p^2$, we obtain $\langle a_1, a_2, a_3, a_4\rangle = G$ by hypothesis, and so $\mathrm{d}(G) \leq 4$.

We assume, by way of contradiction, that $\mathrm{d}(G) = 4$. Then we have $o([x, y]) \leq p$ and $[x, y] \in \mathrm{Z}(G)$ for any $x, y \in G$ by hypothesis, and we conclude that G' is elementary abelian and $G' \leq \mathrm{Z}(G)$. In particular, $\mathrm{cl}(G) = 2$.

For any $k \in \{1, 2\}$ and $l \in \{3, 4\}$ we have $\langle a_1, a_2, a_l\rangle < G$ and $\langle a_k, a_3, a_4\rangle < G$ hence

$$\langle a_1, a_2, a_l\rangle' = \langle [a_1, a_2]\rangle \quad \text{and} \quad \langle a_k, a_3, a_4\rangle' = \langle [a_3, a_4]\rangle.$$

It follows that

$$[a_k, a_l] \in \langle [a_1, a_2]\rangle \cap \langle [a_3, a_4]\rangle = \{1\}.$$

This implies

$$[a_1, a_2a_3] = [a_1, a_2][a_1, a_3] = [a_1, a_2]$$

and

$$[a_2a_3, a_4] = [a_2, a_4][a_3, a_4] = [a_3, a_4].$$

But then $\langle a_1, a_2a_3, a_4\rangle$ is a proper subgroup of G and we have $|\langle a_1, a_2a_3, a_4\rangle'| \geq p^2$, contrary to the hypothesis. The proof is complete. □

Proposition 137.4 (Berkovich). *Let G be a nonabelian p-group. If $\mathrm{d}(G) = 2$, then we have $H' < G'$ for each $H < G$.*

Proof. Let $R < G'$ be a G-invariant subgroup of index p in G'. Then $|(G/R)'| = p$ and $\mathrm{d}(G/R) = 2$. This implies that G/R is minimal nonabelian. For each maximal subgroup H of G we have $H' \leq R < G'$, and we are done. □

Proposition 137.5 (Ćepulić and Piljavska). *Let G be a title p-group with $p > 2$. Then for any $a, b \in G$ we have $[a^p, b] = [a, b^p] = [a, b]^p$.*

Proof. Set $g = [a, b]$. If g commutes with a, then for each $n \geq 1$ we prove by induction that $[a^n, b] = [a, b]^n$. Indeed, for $n > 1$,

$$\begin{aligned}[a^n, b] &= [aa^{n-1}, b] = [a, b]^{a^{n-1}}[a^{n-1}, b] = [a, b][a^{n-1}, b]\\ &= [a, b][a, b]^{n-1} = [a, b]^n.\end{aligned}$$

In particular, $[a^p, b] = [a, b]^p$.

Now assume that $[g, a] = z \neq 1$. Since $\langle g, a\rangle < G$, Proposition 137.1 implies that $o(z) = p$ and $z \in \mathrm{Z}(G)$. We note that

$$g^a = a^{-1}ga = g(g^{-1}a^{-1}ga) = g[g, a] = gz, \quad \text{and so} \quad g^{a^i} = gz^i \ \text{ for all } i \geq 1.$$

We have

$$\begin{aligned}[a^p, b] &= [a \cdot a^{p-1}, b] = [a, b]^{a^{p-1}}[a^{p-1}, b] = [a, b]^{a^{p-1}}[a \cdot a^{p-2}, b]\\ &= [a, b]^{a^{p-1}}[a, b]^{a^{p-2}}[a^{p-2}, b]\end{aligned}$$

and so continuing we finally get

$$\begin{aligned}[a^p, b] &= [a, b]^{a^{p-1}}[a, b]^{a^{p-2}} \dots [a, b]^a[a, b]\\ &= g^{a^{p-1}}g^{a^{p-2}} \dots g^a g = (gz^{p-1})(gz^{p-2}) \dots (gz)g\\ &= g^p z^{(p-1)+(p-2)+\cdots+1} = g^p z^{(p-1)\frac{p}{2}} = g^p = [a, b]^p,\end{aligned}$$

where we have used the fact that $p > 2$. Thus we have proved that in any case we get $[a^p, b] = [a, b]^p$. Now,

$$[a, b^p] = [b^p, a]^{-1} = [b, a]^{-p} = [a, b]^p,$$

and the proof is complete. □

Proposition 137.6. *Suppose that G is a p-group which has one of the following properties:*

(a) $|G'| \leq p$.

(b) $\mathrm{d}(G) = 2$, $|G'| = p^2$.

(c) $p > 2$, $\mathrm{d}(G) = 2$, $\mathrm{cl}(G) = 3$, $G' \cong \mathrm{E}_{p^3}$, $\mho_1(G) \leq \mathrm{Z}(G)$.

(d) $\mathrm{d}(G) = 3$, $\mathrm{cl}(G) = 2$, $G' \cong \mathrm{E}_{p^3}$ *or* E_{p^2}.

Then G has the title property, i.e., $|H'| \leq p$ for each proper subgroup H of G.

Proof. If G is a p-group with property (a), then obviously G has the title property. Suppose that G is a p-group in (b). By Proposition 137.4, for each $H < G$ we have $H' < G'$ and so G has the title property.

Now assume that G is a p-group with property (c). Since $\mathrm{cl}(G) = 3$, it follows that $\{1\} \neq \mathrm{K}_3(G) \leq \mathrm{Z}(G)$. But $\mathrm{d}(G) = 2$ and so $\{1\} \neq G'/\mathrm{K}_3(G)$ is cyclic and therefore $\mathrm{K}_3(G) \cong \mathrm{E}_{p^2}$. By assumption, $\mho_1(G) \leq \mathrm{Z}(G)$ and so $\Phi(G) = \mho_1(G)G'$ is abelian and $G/\Phi(G) \cong \mathrm{E}_{p^2}$. Also, $\mho_1(G)\mathrm{K}_3(G) \leq \mathrm{Z}(G)$ and in fact $\mho_1(G)\mathrm{K}_3(G) = \mathrm{Z}(G)$. Indeed, if $\mho_1(G)\mathrm{K}_3(G) < \mathrm{Z}(G)$, then $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$. But in that case, G has $p + 1$ abelian maximal subgroups and this implies (Exercise P1) $|G'| = p$, a contradiction. Let M be any maximal subgroup of G so that $|M : \Phi(G)| = p$. Then M is either abelian or satisfies $\mathrm{Z}(G) = \mathrm{Z}(M)$ and $M/\mathrm{Z}(M) \cong \mathrm{E}_{p^2}$. In the second case, we may use Lemma 1.1 because $\Phi(G)$ is an abelian maximal subgroup of M. Then we conclude from $|M| = p|\mathrm{Z}(M)||M'|$ that $|M'| = p$. We have proved that in this case G has the title property.

Suppose that G is a p-group with property (d). For any $x, y \in G$ we have $[x^p, y] = [x, y]^p = 1$ and so $\mho_1(G) \leq \mathrm{Z}(G)$. It follows that $\Phi(G) = \mho_1(G)G' \leq \mathrm{Z}(G)$ and $G/\Phi(G) \cong \mathrm{E}_{p^3}$. Let M be any maximal subgroup of G satisfying $M/\Phi(G) \cong \mathrm{E}_{p^2}$. Then $p + 1$ maximal subgroups of M containing $\Phi(G)$ are abelian. This implies that $|M'| \leq p$, and we are done. □

Theorem 137.7. *A p-group G has the property that each proper subgroup of G has its derived subgroup of order at most p if and only if one of the following holds:*

(a) $|G'| \leq p$.

(b) $\mathrm{d}(G) = 2$, $|G'| = p^2$.

(c) $p > 2$, $\mathrm{d}(G) = 2$, $\mathrm{cl}(G) = 3$, $G' \cong \mathrm{E}_{p^3}$, $\mho_1(G) \leq \mathrm{Z}(G)$.[1]

(d) $\mathrm{d}(G) = 3$, $\mathrm{cl}(G) = 2$, $G' \cong \mathrm{E}_{p^3}$ *or* E_{p^2}. *Here we have* $\Phi(G) = \mathrm{Z}(G)$.

Proof. If G is a p-group in (a)–(d), then Proposition 137.6 implies $|H'| \leq p$ for each subgroup $H < G$.

Suppose that G is a p-group all of whose proper subgroups have its derived subgroup of order $\leq p$. If $|G'| \leq p$, then we obtain the groups in part (a) of our theorem.

[1] Such p-groups G exist. See for example A_2-groups of order p^5, $p > 2$, in Proposition 71.5(b).

In what follows we assume that $|G'| \geq p^2$. By Proposition 137.2, G' is abelian of order p^2 or p^3. Due to Proposition 137.3, we have $\mathrm{d}(G) \leq 3$.

(i) First assume that $\mathrm{d}(G) = 2$. If $|G'| = p^2$, then we have obtained the groups in part (b) of our theorem. In the sequel we shall assume $|G'| = p^3$. By Exercise 1.69(a), all $p+1$ maximal subgroups M_i $(i = 1, 2, \ldots, p+1)$ of G are nonabelian, $|M_i'| = p$ and for any $i \neq j$ we have $M_i' \cap M_j' = \{1\}$ so that

$$M_i' \times M_j' \cong \mathrm{E}_{p^2} \quad \text{and} \quad M_i' \times M_j' \leq \mathrm{Z}(G).$$

If $\mathrm{cl}(G) = 2$, then $\mathrm{d}(G) = 2$ would imply that G' is cyclic, contrary to the existence of the subgroup $M_i' \times M_j' \cong \mathrm{E}_{p^2}$. Hence $\mathrm{cl}(G) \geq 3$. But

$$\{1\} \neq \mathrm{K}_3(G) = [G, G'] \leq M_i' \times M_j' \leq \mathrm{Z}(G)$$

and so $\mathrm{cl}(G) = 3$. Set $E = M_i' \times M_j' = G' \cap \mathrm{Z}(G) \cong \mathrm{E}_{p^2}$. Whenever $a, b \in G$ are such that $\langle a, b\rangle = G$, then $[a, b] \in G' - E$. Indeed, if $1 \neq [a, b] \in E$, then we have $o([a, b]) = p$ and $[a, b] \in \mathrm{Z}(G)$. But then $G/\langle [a, b]\rangle$ is abelian and so $G' = \langle [a, b]\rangle$ is of order p, a contradiction. Let $g = [a, b]$, where $\langle a, b\rangle = G$ and $g \in G' - E$. For any $x \in G$ we have $g^x = ge$ with some $e \in E$. Then

$$g^{x^i} = ge^i \quad \text{and so} \quad g^{x^p} = g.$$

It follows that $\mathfrak{V}_1(G)$ centralizes G' and so $\Phi(G) = \mathfrak{V}_1(G)G'$ centralizes G'.

(i1) Now assume $p > 2$. Suppose, in addition, that G' is not elementary abelian. Then we get $E = \Omega_1(G')$ and set $\{1\} \neq \mathfrak{V}_1(G') = \langle s\rangle < E$ so that $G'/\langle s\rangle \cong \mathrm{E}_{p^2}$. If $\mathrm{K}_3(G) = [G, G'] = \langle s\rangle$, then $\mathrm{cl}(G/\langle s\rangle) = 2$ so that $\mathrm{d}(G/\langle s\rangle) = 2$ would imply that $G'/\langle s\rangle = (G/\langle s\rangle)'$ is cyclic, a contradiction. Hence there is an element $c \in G - \Phi(G)$ such that $g^c = gl$ with $l = [g, c] \in E - \langle s\rangle$. Let $d \in G - \Phi(G)$ be such that $\langle c, d\rangle = G$ so that $[c, d] \in G' - E$. By Proposition 137.5, we get $[c, d^p] = [c, d]^p = s^j$, where $j \not\equiv 0 \pmod{p}$. Consider the maximal subgroup $C = \langle \Phi(G), c\rangle$. Since $g, c, d^p \in C$, we have

$$C' \geq \langle [g, c], [c, d^p]\rangle = \langle l, s^j\rangle = E \cong \mathrm{E}_{p^2},$$

which is a contradiction. We have proved that $G' \cong \mathrm{E}_{p^3}$. For any $x, y \in G$ we get, by Proposition 137.5, $[x^p, y] = [x, y]^p = 1$ and so $\mathfrak{V}_1(G) \leq \mathrm{Z}(G)$. We have obtained the groups given in part (c) of our theorem.

(i2) It remains to consider the case $p = 2$. Assume, in addition, that

$$\{1\} \neq \mathrm{K}_3(G) = [G, G'] < E$$

and set $[G, G'] = \langle u\rangle$, where u is an involution in $E \leq \mathrm{Z}(G)$. Note that $\Phi(G)$ centralizes G' and for each $x \in G - \Phi(G)$ and $y \in G' - E$ we have $y^x = yu'$ with $u' \in \langle u\rangle$. Set $G_0 = \mathrm{C}_G(G')$ so that $|G : G_0| = |G_0 : \Phi(G)| = 2$. Since $G/\langle u\rangle$ is of class 2 and $\mathrm{d}(G/\langle u\rangle) = 2$, we conclude that $G'/\langle u\rangle$ is cyclic. Hence if $g \in G' - E$, then $g^2 = v$

is an involution in $E - \langle u\rangle$ and therefore $E = \Omega_1(G') = \langle u, v\rangle$ and $\mho_1(G') = \langle v\rangle$. Take some elements $a \in G_0 - \Phi(G)$ and $b \in G - G_0$. Then $\langle a, b\rangle = G$ and therefore $[a, b] = h \in G' - E$ with $h^2 = v$, $h^a = h$ and $h^b = hu$. Consider the maximal subgroup $H = \langle \Phi(G), b\rangle$. Since

$$[a^2, b] = [a, b]^a[a, b] = h^a h = h^2 = v \quad \text{and} \quad [h, b] = u,$$

we get $H' \geq \langle u, v\rangle = E \cong \mathrm{E}_4$, a contradiction.

We have proved that

$$\mathrm{K}_3(G) = [G, G'] = E = G' \cap \mathrm{Z}(G) \cong \mathrm{E}_4.$$

Let $a, b \in G - \Phi(G)$ be such that $\langle a, b\rangle = G$. Then $g = [a, b] \in G' - E$, $[g, a] = c_1$, $[g, b] = c_2$, where $\langle c_1, c_2\rangle = E = \mathrm{K}_3(G)$. We set $c_3 = c_1c_2$ and get

$$[g, ab] = [g, b][g, a]^b = [g, b][g, a] = c_2c_1 = c_3.$$

We compute the commutator subgroups of our three nonabelian maximal subgroups

$$X_1 = \langle \Phi(G), a\rangle, \quad X_2 = \langle \Phi(G), b\rangle \quad \text{and} \quad X_3 = \langle \Phi(G), ab\rangle,$$

where we note that we must have $|X_i'| = 2$ for $i = 1, 2, 3$.

Since $[g, a] = c_1$ and

$$[a, b^2] = [a, b][a, b]^b = gg^b = g \cdot gc_2 = g^2c_2,$$

we infer that $X_1' = \langle c_1\rangle$ and so we must have $g^2c_2 \in \langle c_1\rangle$. This forces either $g^2 = c_2$ or $g^2 = c_3$.

As $[g, b] = c_2$ and

$$[a^2, b] = [a, b]^a[a, b] = g^a g = gc_1 \cdot g = g^2c_1,$$

we obtain $X_2' = \langle c_2\rangle$ and so we must have $g^2c_1 \in \langle c_2\rangle$. This forces either $g^2 = c_1$ or $g^2 = c_3$. With the above we get exactly $g^2 = c_3$.

Since $[g, ab] = c_3$ and

$$[a^2, ab] = [a, ab]^a[a, ab] = g^a g = gc_1 \cdot g = g^2c_1$$

(where we have used the fact that $[a, ab] = [a, b]$), we infer that $X_3' = \langle c_3\rangle$ and so we must have $g^2c_1 \in \langle c_3\rangle$. But we know that $g^2 = c_3$ and so $g^2c_1 = c_3c_1 = c_2 \in \langle c_3\rangle$, a contradiction. We have proved that such 2-groups do not exist!

(ii) Finally, assume that $\mathrm{d}(G) = 3$. For any $x, y \in G$ we have $\langle x, y\rangle < G$ and so Proposition 137.1 implies that $o([x, y]) \leq p$ and $[x, y] \in \mathrm{Z}(G)$. But then G' is elementary abelian (of order p^2 or p^3) and $G' \leq \mathrm{Z}(G)$ and so we have obtained the groups from part (d) of our theorem. For any $a, b \in G$ we have $[a^p, b] = [a, b]^p = 1$ and so $\Phi(G) \leq \mathrm{Z}(G)$. If $\mathrm{Z}(G) \not\leq \Phi(G)$, then there is a maximal subgroup M of G such that $G = \langle M, x\rangle$, where $x \in \mathrm{Z}(G)$. But then $G' = M'$ and so $|G'| = 2$, a contradiction. Hence $\Phi(G) = \mathrm{Z}(G)$. Theorem 137.7 is proved. □

§138

p-groups all of whose nonnormal subgroups have the smallest possible normalizer

1^o. A p-group G is called an S_1-*group* if $|N_G(H) : H| = p$ for all nonnormal subgroups H of G. We determine here up to isomorphism all non-Dedekindian S_1-groups by using the results (but not the proofs) from [ZG]. This solves Problem 116(i) stated by the first author.

Lemma 138.1. *Assume that G is a minimal nonabelian p-group of order $> p^3$. If G is an S_1-group, then*

$$G \cong \langle a, b \mid a^{p^2} = b^{p^2} = 1,\ a^b = a^{1+p} \rangle = M_p(2, 2).$$

Proof. Suppose that G has an elementary abelian subgroup E of order p^3. Then each subgroup of order p in E must be normal in G and so $E \leq Z(G)$. Let X be a cyclic nonnormal subgroup in G. But then $N_G(X) \geq E$ and so $|N_G(X) : X| \geq p^2$, a contradiction. We have proved that G is metacyclic and so

$$G \cong \langle a, b \mid a^{p^n} = b^{p^m} = 1,\ a^b = a^{1+p^{n-1}} \rangle,$$

where $n \geq 2$, $m \geq 1$, $n + m \geq 4$ and $G' = \langle [a, b] \rangle = \langle a^{p^{n-1}} \rangle$. Obviously, $\langle b \rangle$ is not normal in G and $N_G(\langle b \rangle) = \langle b \rangle \times \langle a^p \rangle$ which forces $n = 2$ and so $m \geq 2$. Assume $m \geq 3$ so that $b^{p^{m-2}} \in Z(G)$, $o(ab^{p^{m-2}}) = p^2$ and $\langle ab^{p^{m-2}} \rangle$ is not normal in G. Indeed, if $\langle ab^{p^{m-2}} \rangle \lhd G$, then we have $[G, \langle ab^{p^{m-2}} \rangle] \leq \langle ab^{p^{m-2}} \rangle \cap G' = \{1\}$ and so $ab^{p^{m-2}} \in Z(G)$ which forces $a \in Z(G)$, a contradiction. But

$$N_G(\langle ab^{p^{m-2}} \rangle) = \langle a \rangle \times \langle b^p \rangle$$

and therefore $|N_G(\langle ab^{p^{m-2}} \rangle) : \langle ab^{p^{m-2}} \rangle| \geq p^2$, a contradiction. Hence $m = 2$ and we are done. □

Theorem 138.2 ([ZG]). *Assume that G is a nonabelian p-group, $p > 2$, and $|G| > p^3$. Then G is an S_1-group if and only if*

$$G \cong \langle a, b \mid a^{p^2} = b^{p^2} = 1,\ a^b = a^{1+p} \rangle = M_p(2, 2).$$

Proof (Janko). Suppose that G is a nonabelian p-group, $p > 2$, $|G| > p^3$ and G is an S_1-group.

First assume that G is nonabelian of order p^4. Suppose, in addition, that G is not minimal nonabelian and let H be a minimal nonabelian subgroup of order p^3 in G. Then $\Omega_1(H)$ contains a G-invariant subgroup $E \cong \mathrm{E}_{p^2}$. Let E_0 be a noncentral subgroup of order p of H with $E_0 < E$. Then we must have $\mathrm{N}_G(E_0) = E$. On the other hand, $\mathrm{C}_H(E) = E$ and so $\mathrm{C}_G(E) \not\leq H$, a contradiction. Hence G is minimal nonabelian and so Lemma 138.1 implies that $G \cong \mathrm{M}_p(2,2)$.

Now we use induction on $|G|$. Let G be a nonabelian S_1-group of order $\geq p^5$, and let N be a subgroup of order p in $G' \cap \mathrm{Z}(G)$. Then G/N is an S_1-group and so (by induction) G/N is either abelian or $G/N \cong \mathrm{M}_p(2,2)$.

(i) First assume that G/N is abelian. Then $G' = N$ is of order p. Let K be a minimal nonabelian subgroup of G so that $K' = G' = N$ and K satisfies either $|K| = p^3$ or $K \cong \mathrm{M}_p(2,2)$ (Lemma 138.1). We get $G = K\mathrm{C}_G(K)$, where $K \cap \mathrm{C}_G(K) = \mathrm{Z}(K)$ and $\mathrm{C}_G(K) \not\leq K$ (since $|G| \geq p^5$). If Y is a nonnormal cyclic subgroup of K, then $|\mathrm{N}_G(Y) : Y| \geq p^2$, a contradiction.

(ii) Now suppose that $G/N \cong \mathrm{M}_p(2,2)$. Since G/N is metacyclic, it follows from Theorem 36.1 that G is also metacyclic. As $G' \cong \mathrm{C}_{p^2}$, we conclude that G is a metacyclic A_2-group of order p^5. By Proposition 71.2(a), we have

$$G \cong \langle a, b \mid a^{p^3} = 1,\ b^{p^2} = a^{\epsilon p^2},\ a^b = a^{1+p} \rangle,$$

where $\epsilon = 0, 1$. Consider the maximal subgroup $L = \langle a \rangle \langle b^p \rangle$ of G. Since $\langle a \rangle$ is a cyclic subgroup of index p in L (and L is obviously noncyclic), there is an element x of order p in $L - \langle a \rangle$. But $G/\langle a \rangle \cong \mathrm{C}_{p^2}$ acts faithfully on $\langle a \rangle$ and so x does not centralize $\langle a \rangle$ which implies that $\langle x \rangle$ is not normal in G. On the other hand, L is minimal nonabelian and so x centralizes $\langle a^p \rangle$ and therefore $|\mathrm{N}_G(\langle x \rangle) : \langle x \rangle| \geq p^2$, a contradiction. Since $\mathrm{M}_p(2,2)$ is obviously an S_1-group, our theorem is proved. □

Theorem 138.3. *Let G be a non-Dedekindian 2-group. Then G is an S_1-group if and only if one of the following holds:*

(a) *G is of maximal class distinct from Q_8.*

(b) *$G \cong \langle a, b \mid a^{2^n} = b^4 = 1,\ a^b = a^{-1+\epsilon 2^{n-1}} \rangle$, where $n \geq 2$, $\epsilon = 0, 1$, and if $\epsilon = 1$, then $n \geq 3$.*

Proof (Janko). Suppose that G is a non-Dedekindian 2-group and G is an S_1-group. By Lemma 138.1, each minimal nonabelian subgroup H of G is isomorphic to D_8, Q_8 or $\mathrm{M}_2(2,2) = \mathrm{H}_2$.

(i) Suppose that G possesses a subgroup $H \cong \mathrm{D}_8$. Let t be a noncentral involution in H. Since $|\mathrm{C}_H(t) : \langle t \rangle| = 2$, we have $\mathrm{C}_G(t) < H$ and so $\mathrm{C}_G(H) \leq H$. By Proposition 10.17, G is of maximal class. In what follows we may assume that D_8 is not a subgroup of G.

(ii) Now suppose that G possesses a subgroup $H \cong \mathrm{Q}_8$ so that in this case we must have $H < G$. Set $H = \langle a, b \rangle$ and $\mathrm{Z}(H) = \langle z \rangle$. First assume that H has a cyclic subgroup C of order 4 such that C is not normal in G. Then $\mathrm{N}_G(C) = H$ which implies

that $C_G(H) \leq H$ and so again (Proposition 10.17) G is of maximal class. In what follows we may assume that each cyclic subgroup of H is normal in G. This gives that $H \trianglelefteq G$ and $G = HK$, where $K = C_G(H)$ and $H \cap K = \langle z \rangle$. Suppose that K has a cyclic subgroup $K_1 = \langle k \rangle$ of order 4. If $k^2 = z$, then we have $HK_1 = H * K_1$ with $H \cap K_1 = \langle z \rangle$. But we know that in this case HK_1 possesses a subgroup isomorphic to D_8, a contradiction. Hence we must have $HK_1 = H \times K_1$, where we set $k^2 = z'$. In this case, we consider $\langle ak \rangle \cong C_4$, where $(ak)^2 = zz'$ and $(ak)^b = ak \cdot z$, which implies that $\langle ak \rangle$ is not normal in HK_1. But $\langle a, k \rangle \cong C_4 \times C_4$ centralizes $\langle ak \rangle$ and so HK_1 is not an S_1-group, a contradiction. We have proved that K is elementary abelian. But then G is Dedekindian, contrary to our assumption.

(iii) In the sequel we assume that each minimal nonabelian subgroup of G is isomorphic to H_2. Then we use Theorem 57.3, where such 2-groups are classified. If G is a group from part (b) of Theorem 57.3, then G is of exponent 4 and by inspection we see that the only S_1-group there is the group H_2 which appears in part (b1) of that theorem. We have obtained a group from part (b) of our theorem for the special case $n = 2$ and $\epsilon = 0$. Indeed, in case (b2) of Theorem 57.3, G contains the unique minimal nonmetacyclic group H of order 2^5 given in Theorem 66.1(d) with

$$H = \langle a, b, c \mid a^4 = b^4 = [a, b] = 1,\ c^2 = a^2,\ a^c = ab^2,\ b^c = ba^2 \rangle,$$

and here $\langle a \rangle$ is not normal in H, but $\langle a, b \rangle$ centralizes $\langle a \rangle$ and so H is not an S_1-group. In case (b3) of Theorem 57.3 the groups there contain a minimal nonmetacyclic group of order 2^5 as a subgroup. Finally, in case (b4) of Theorem 57.3, we have a subgroup $K = B\langle b \rangle$, where $o(b) = 4$, $\langle b \rangle \cap B = \{1\}$, b inverts each element of B, $\langle b \rangle$ is not normal in K, but $\Omega_1(B)$ is elementary abelian of order ≥ 4 and $\Omega_1(B)$ centralizes $\langle b \rangle$ and so such a group K is not an S_1-group.

It remains to consider the groups G in Theorem 57.3(a) which are of exponent ≥ 8. Here G has a unique abelian maximal subgroup A. We have $\exp(A) \geq 8$,

$$E = \Omega_1(A) = \Omega_1(G) = Z(G)$$

is of order ≥ 4. All elements in $G - A$ are of order 4 and if b is one of them, then $C_A(b) = E$ and b inverts each element of $\Phi(A)$ and of A/E. Since $\langle b \rangle$ is not normal in G and E centralizes $\langle b \rangle$, we get $E \cong E_4$ and therefore A is of rank 2. If $C = \langle c \rangle$ is any cyclic subgroup of order 4 in A, then $C \lhd G$ and so $c^b = c^{-1}$. In case $c^2 = b^2$, we infer that $\langle b, c \rangle \cong Q_8$, a contradiction. Thus we have proved that $b^2 = u$ is not a square in A and so $A = \langle u \rangle \times \langle a \rangle$ with $o(a) = 2^n$, $n \geq 3$, and we set $a^{2^{n-1}} = z$ so that $E = \Omega_1(A) = \Omega_1(G) = \langle u, z \rangle$. Since b inverts each element of A/E, we have $a^b = a^{-1}\zeta$ with $\zeta \in E$. If $\zeta = u$, then

$$(ba)^2 = ba \cdot ba = b^2 a^b a = u \cdot a^{-1} u \cdot a = 1,$$

a contradiction. In case $\zeta = uz$, we obtain

$$(ba)^2 = ba \cdot ba = b^2 a^b a = u \cdot a^{-1} uz \cdot a = z.$$

But ba inverts $v = a^{2^{n-2}}$ (of order 4) and so $\langle ba, v\rangle \cong Q_8$, a contradiction. We have proved that $a^b = a^{-1}z^\epsilon$, $\epsilon = 0, 1$, and so we have obtained all groups stated in part (b) of our theorem.

(iv) Conversely, if G is a 2-group of maximal class (distinct from Q_8), then G is obviously a non-Dedekindian S_1-group. Assume that G is a 2-group from part (b) of our theorem. If $n = 2$, then $\epsilon = 0$ and $G \cong H_2$, which is an S_1-group. Suppose that $n \geq 3$ and set $b^2 = u$ and $a^{2^{n-1}} = z$ so that $a^b = a^{-1}z^\epsilon$ and $\Omega_1(G) = Z(G) = \langle u, z\rangle$. Let $x = b\zeta^i a^j$ with $\zeta \in \Omega_1(G)$ (i, j are integers) be any element in $G - (\langle u\rangle \times \langle a\rangle)$. Then we compute

$$\begin{aligned} x^2 &= (b\zeta^i a^j)^2 = b\zeta^i a^j \cdot b\zeta^i a^j = b^2(b^{-1}a^j b)a^j = u(a^b)^j a^j \\ &= u \cdot (a^{-1}z^\epsilon)^j a^j = ua^{-j}z^{\epsilon j}a^j = uz^{\epsilon j}, \end{aligned}$$

and we see that $x^2 \in \Omega_1(G) - \langle z\rangle$. For any $y \in \Omega_1(G) - \langle z\rangle$ we infer that $G/\langle y\rangle$ is dihedral or semidihedral and so $G/\langle y\rangle$ is an S_1-group. Let M be any subgroup of G. If M contains an element $y \in \Omega_1(G) - \langle z\rangle$, then $M/\langle y\rangle$ is a subgroup of $G/\langle y\rangle$ and so either $M \trianglelefteq G$ or $|N_G(M) : M| = 2$. Suppose that M does not contain any element in $\Omega_1(G) - \langle z\rangle$. Then, by the above, $M \leq \langle u\rangle \times \langle a\rangle$ and so $M \trianglelefteq G$ since every subgroup of $\langle u\rangle \times \langle a\rangle$ is normal in G. Hence G is an S_1-group. Our theorem is proved. □

2^o. Below we prove a more general result.

Let G be a non-Dedekindian p-group and $C < G$ be nonnormal cyclic of minimal possible order. Write $|C| = p^{v(G)} = p^v$. Denote by $\mathcal{C}_v$ the set of all nonnormal cyclic subgroups of G of order p^v. Clearly, if $H < G$ is non-Dedekindian, then we obtain that $v(H) \geq v(G)$. If G satisfies the hypothesis of Theorem 138.4, then the members of the set $\mathcal{C}_v$ are maximal cyclic subgroups of G.

Our main aim is to prove the following

Theorem 138.4 (Berkovich). *Let G be a non-Dedekindian p-group of order $> p^3$ such that any nonnormal cyclic subgroup of order $p^v = p^{v(G)}$ has index p in its normalizer. Then one and only one of the following holds:*

(a) *If $p > 2$, then G is the unique nonabelian metacyclic group of order p^4 and exponent p^2, $v = 2$.*

(b) *G is a 2-group of maximal class. In this case, $v = 1$ unless G is generalized quaternion and $v = 2$.*

(c) *$G = \langle x, y \mid x^{2^n} = y^4 = 1, x^y = x^{-1+\mu 2^{n-1}}\rangle$ is metacyclic, where $\mu \in \{0, 1\}$, $n \geq 2$, and if $\mu = 1$, then $n > 2$. Here $|G| = 2^{n+2}$, $G = \langle y\rangle \cdot \langle x\rangle$ (semidirect product with kernel $\langle x\rangle$), $Z(G) = \langle x^{2^{n-1}}, y^2\rangle = \Omega_1(G)$, $\Phi(G) = \langle x^2, y^2\rangle = \langle y^2\rangle \times G'$ is abelian of type $(2^{n-1}, 2)$, G/G' ia abelian of type $(4, 2)$, $G/\langle y^2\rangle$ is of maximal class but not generalized quaternion. In this case, $v = 2$.*

Proof. If G is a 2-group of maximal class satisfying the hypothesis of the theorem, then all its abelian subgroups of order > 4 are normal cyclic and all its nonnormal sub-

groups of order > 4 are of maximal class. If $K < G$ is nonabelian, then a normal subgroup of K of index > 2 is contained in $\Phi(K) < \Phi(G)$ and so are normal in G. Therefore, if $U \in \mathcal{C}_\nu$, then $|U| \leq 4$ hence $\nu \leq 2$, and $|\mathrm{N}_G(U) : U| = 2$, and so G satisfies the hypothesis. This proves (b).

Next we assume that our group G is not a 2-group of maximal class.

(i) If we have $U \in \mathcal{C}_\nu$, then any abelian subgroup A of G containing U has order at most $p|U|$.[1]

Proof. Indeed, we have $A \leq \mathrm{N}_G(U)$ so that $|A : U| \leq |\mathrm{N}_G(U) : U| = p$. □

(ii) G has no elementary abelian subgroup of order p^3.

Proof. Assume, by way of contradiction, that a subgroup $E < G$ is elementary abelian of order p^3. Then, by (i), all subgroups of order p contained in E are normal in G, and we conclude that $E \leq \mathrm{Z}(G)$. Let $U \in \mathcal{C}_\nu$. Then $|E \cap U| \leq p$ hence, by the product formula, EU is abelian of order $\geq p^2|U|$, contrary to (i). □

(iii) All subgroups of order p are normal in G and $|\Omega_1(G)| = p^2$ (recall that we have assumed that G is not a 2-group of maximal class). In particular, $\nu > 1$.

Proof. Assume that a subgroup $T < G$ is nonnormal of order p. Then $\nu = 1$ hence $|\mathrm{N}_G(T)| = p|T| = p^2$ by hypothesis. Since $\mathrm{N}_G(T) = \mathrm{C}_G(T)$, it follows that G is of maximal class by Proposition 1.8 (then, by assumption, $p > 2$). This argument shows that any subgroup of G properly containing a nonnormal subgroup of order p is either of order p^2 or of maximal class. Then, since $p > 2$, G possesses a G-invariant abelian subgroup R of type (p, p) (Lemma 1.4). As $\mathrm{Z}(G)$ is cyclic, it follows that there is in R a non-G-invariant subgroup L of order p. Write $E = \mathrm{C}_G(R)$; then $|E| = \frac{1}{p}|G| \geq p^3$. Let $B/R \leq E/R$ be of order p. Then B is abelian of order $p^3 = p^2|L|$ (see (ii)), contrary to (i). Thus the group G has no nonnormal subgroups of order p, and we conclude that $\Omega_1(G) \leq \mathrm{Z}(G)$ so that $|\Omega_1(G)| = p^2$ by (ii). □

It follows from (iii) that G is not of maximal class also for $p > 2$.

(iv) The group G possesses a minimal nonabelian subgroup H such that $\nu(H) = \nu(= \nu(G))$. Moreover, H is metacyclic of order p^4 and exponent p^2 and $\nu = 2$.

Proof. Let $T \in \mathcal{C}_\nu$ and write $N = \mathrm{N}_G(T)$; then $|N : T| = p$ so that $|N| = p|T| = p^{\nu+1} \geq p^3$ since $\nu > 1$ by (iii). Assume that $N \cong \mathrm{Q}_8$. Then $\nu = 2$ and $\mathrm{C}_G(T) = T$ so G is of maximal class, a contradiction. Thus we have $N \ncong \mathrm{Q}_8$ so that N is abelian of type (p^ν, p) by Theorem 1.2. Denote by N_1 the normalizer of N in G; then N_1 is nonabelian. The subgroup $N \lhd N_1$ has exactly $\mathrm{c}_\nu(N) = p$ cyclic subgroups of index p (here $\mathrm{c}_\nu(N)$ is the number of cyclic subgroups of order p^ν in N). Let N_1 act via conjugation on cyclic subgroups of index p in N. Since the stabilizer of T in N_1 coincides

[1] By hypothesis, if $|\mathrm{N}_G(U) : U| > p$, then $U \lhd G$.

with $\mathrm{N}_{N_1}(T) = N$, we get $|N_1 : N| = \mathrm{c}_\nu(N) = p$. Therefore the normalizer of any cyclic subgroup of N of order $|T|$ in N_1 (even in G by hypothesis) coincides with N.

Assume that $p = 2$ and all minimal nonabelian subgroups of N_1 are $\cong \mathrm{Q}_8$ (G has no dihedral subgroup of order 8 by (iii)). Then, by Corollary A.17.3 and hypothesis, we get $N_1 = Q \times E$, where Q is generalized quaternion and $\exp(E) \leq 2$. By construction, $N_1 \neq Q$ (otherwise, all abelian subgroups of Q are cyclic but $N < Q$ is noncyclic abelian) so that $E > \{1\}$. If $|Q| > 8$, then there exists in Q a nonnormal cyclic subgroup M of order 4 (then $\nu = 2$), and the subgroup $\mathrm{N}_{N_1}(M) = \mathrm{N}_Q(M) \times E$ has order $8|E| > 2|M|$, contrary to the hypothesis. Thus $Q \cong \mathrm{Q}_8$ so that N_1 is Dedekindian. In this case, $T \lhd N_1$, a contradiction since $\mathrm{N}_G(T) = N < N_1$.

Now let p be arbitrary. By the previous paragraph, there is in N_1 a minimal nonabelian subgroup $H \ncong \mathrm{Q}_8$; then we have $|H| > p^3$ since $\Omega_1(H) \leq \mathrm{Z}(H)$ by (iii). By (ii) and Lemma 65.1, H is metacyclic. Assume that $\nu(H) > \nu$. Then $|H| \geq p^{\nu(H)+2} > p^{\nu+2} = |N_1|$, which is a contradiction. Thus $\nu(H) = \nu$. Let $L < H$ be nonnormal cyclic of order p^ν. By hypothesis, $|H| = p \cdot |\mathrm{N}_H(L)| = p^{\nu+2}$. Let $Z \lhd H$ be cyclic such that H/Z is cyclic; then $H' < Z$. It follows that $L \cap Z = \{1\}$, and we conclude that $H = L \cdot Z$, a semidirect product with kernel Z, and $|Z| = |H : L| = p^2$. Let $\Omega_2(L) = \langle b \rangle$ and $Z = \langle z \rangle$. Then the cyclic subgroup $U = \langle bz \rangle$ of order p^2 is not normal in H so that $\nu(H) = 2 \geq \nu(G) > 1$ hence $\nu = 2$ and $|H| = |L||Z| = p^4$ so H is metacyclic of exponent 4. As a by-product, we have also obtained $N_1 = H$. □

(v) The theorem is true if $p > 2$.

Proof. Indeed, by (ii), (iii) and Proposition 10.19, G is metacyclic. Take in G a minimal nonabelian subgroup H such that $\nu(H) = \nu$ (H exists in view of (iv)). By (iv), H is of order p^4 and exponent p^2. Let V be of order p such that $V \neq H'$; then we obtain $V \lhd G$ by (iii). In this case, H/V is a nonabelian subgroup of order p^3 in the metacyclic group G/V. It follows from Proposition 10.19 that $H/V = G/V$ so $G = H$, as was to be shown. □

In what follows we assume that $p = 2$. Let $H \leq G$ be minimal nonabelian with $\nu(H) = \nu(= \nu(G))$. By (iv), H is metacyclic of order 16 and exponent 4 and $\nu = 2$.

(vi) The group G is as in (c).

Proof. If G is minimal nonabelian, then it coincides with H so G is metacyclic of order 16 and exponent 4 by the paragraph preceding (vi).

Next we assume that G is not minimal nonabelian; then we get $H < G$ so $|G| > 16$. Set $|G| = 2^{n+2}$; then $n > 2$. As we know, $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle$. Let $L = \langle b \rangle < H$ be nonnormal cyclic of order 4; then L is not normal in G so that $\nu = 2$ by (iii). In this case, by hypothesis, we obtain $\mathrm{N}_H(L) = \langle a^2, b \rangle = \mathrm{N}_G(L)$ (the last equality holds by hypothesis). Therefore $\mathrm{N}_{G/\mathfrak{V}_1(L)}(L/\mathfrak{V}_1(L)) = \mathrm{N}_G(L)/\mathfrak{V}_1(L)$ is abelian of type $(2, 2)$. It follows from Proposition 1.8 that $G/\mathfrak{V}_1(L)$ is of maximal class. We claim that G is metacyclic. Assume that this is false. If $\mathfrak{V}_1(L) < G'$, then

$|G : G'| = 4$ so G is of maximal class by Proposition 1.6, contrary to the assumption. Thus $\mho_1(L) \not\leq G'$ so that $G' \cap L = \{1\}$. In this case, $G' \cong (G/\mho_1(L))'$ hence G' is cyclic of order 2^{n-1}. As $\mho_1(L) = \Phi(L) < \Phi(G)$, we get $\mathrm{d}(G) = \mathrm{d}(G/\mho_1(L)) = 2$ and so G/G' is abelian of type $(4, 2)$. The subgroup $F = L \cdot G'$ (semidirect product with kernel G') is a metacyclic maximal subgroup of G. Also, we have $\Omega_1(G) < F$ as $|\Omega_1(G)| = 4 = |\Omega_1(G') \times \Omega_1(L)|$. We obtain $G/G' = (F/G') \times (K/G')$, where $F/G' \cong L$ is cyclic of order 4 and $|K/G'| = 2$. Since $F \cap K = G'$ is cyclic, it follows that K has only one subgroup of order 2 since it does not contain $\mho_1(L)$, and we infer that K is either cyclic or generalized quaternion. We also have $G = L \cdot K$ (semidirect product with kernel K) and $|K| = 2^n$. Let $M/G' < G/G'$ be cyclic of order 4 such that $M \neq F$ (note that G/G' contains exactly two cyclic subgroups of order 4 and F/G' is one of them); then M is metacyclic. Since $\mathrm{d}(G) = 2$, we have

$$\Gamma_1 = \{F, M, K \times \mho_1(L)\},$$

where F and M are metacyclic.

Assume that $K \times \mho_1(L)$ is metacyclic. Then, by Theorem 66.1, we get $|G| = 2^5$ and $\exp(G) = 4$, a contradiction since, in this case, K is cyclic of order 8. Thus $K \times \mho_1(L)$ is nonmetacyclic so K is a generalized quaternion group of order 2^n, where $n > 2$, by the above. If $n > 3$, then K possesses a nonnormal cyclic subgroup D of order 4 and $\mathrm{N}_K(D) \times \mho_1(L) \leq \mathrm{N}_G(D)$ has order $16 = 4|D| > 2|D|$, contrary to the hypothesis. Hence $n = 3$, $K \cong \mathrm{Q}_8$ and b induces on K an involutory automorphism since b^2 centralizes K but b does not centralizes K. Let G', U, V be pairwise distinct cyclic subgroups of order 4 in K. Since $G' \lhd G$, it follows that $|G : \mathrm{N}_G(U)| \leq 2$ so $U \lhd G$. Similarly, $V \lhd G$. Then b inverts G', U, V so K, and we conclude that K is abelian (Burnside), a contradiction.

The obtained contradiction shows that G is metacyclic. Let $Z \lhd G$ be cyclic such that G/Z is cyclic. Then we get $G' < Z$ so $|G/Z| < |G/G'| = 8$. Since G has no cyclic subgroup of index 2 (Theorem 1.2), we obtain $|G/Z| = 4$. We have $G = L \cdot Z$ (semidirect product since $L \cap G' = \{1\}$). All the above allows us to write out defining relations for G in the following form:

$$G = \langle a^4 = z^{2^n} = 1,\ z^a = z^{-1+\mu 2^{n-1}} \rangle,$$

where $\mu \in \{0, 1\}$ (Theorem 1.2), and if $\nu = 1$, then $n > 2$, so G is as in (c). □

(vii) It remains to check that the groups (a)–(c) listed in the conclusion of our theorem satisfy the hypothesis.

The group from (a), obviously, satisfies the hypothesis.

As we have noticed, 2-groups of maximal class satisfy the hypothesis (see the first paragraph of the proof).

Now let G be a group from (c) and $|G| = 2^{n+2} > 2^4$. In this case, $\nu(G) = \nu = 2$ since $\Omega_1(G) = \mathrm{Z}(G)$ and the set $\mathcal{C}_2$ contains a nonnormal cyclic subgroup $\langle a \rangle$ of

order 4 (see the defining relations for G). Let $L < G$ be nonnormal cyclic of order 4 and $Z = \langle z \rangle$. We have to prove that $|\mathrm{N}_G(L) : L| = 2$. Since $\mathrm{cl}(G) > 2$, $\mathrm{C}_G(Z)$ is the unique abelian maximal subgroup of G and $LZ = G$ since $L \not\leq \mathrm{C}_G(Z)$, and so we obtain $L \cap Z = \{1\}$ by the product formula. It follows that $\mathrm{C}_G(L) = LZ(G)$ is abelian of type $(4, 2)$. Since $\mathrm{N}_G(L) = \mathrm{C}_G(L)$, we finally get $|\mathrm{N}_G(L) : L| = 2$. The proof is complete. □

To prove that Theorem 138.3 follows from Theorem 138.4, it suffices to show that all groups (a)–(c) from the conclusion of the latter theorem satisfy the hypothesis of Theorem 138.3. It suffices to check only the groups from Theorem 138.4(c). We omit this routine checking. Note only that if $H < G$ is nonnormal and contains $\Omega_1(G)$, then $|\mathrm{N}_G(H) : H| = 2$ since $G/\Omega_1(G)$ is of maximal class; therefore it suffices to assume that H is cyclic (see Proposition 10.19).

Let p be a prime and $n \geq 4$ be a natural number. Denote by $t_p(n)$ the number of pairwise nonisomorphic groups of order p^n satisfying the hypothesis of Theorem 138.4. If $p > 2$, then we have $t_p(n) = 1$ for $n = 4$ and $t_p(n) = 0$ for $n > 4$. Next, $t_2(n) = 4$ for $n = 4$ and $t_2(n) = 5$ for $n > 4$. This follows from Theorem 138.4.

Corollary 138.5. *If any nonnormal subgroup (cyclic subgroup) of a non-Dedekindian p-group G has index p in its normalizer, then G is one of the groups* (a)–(c) *from Theorem 138.4.*

Problems

Problem 1. Classify the non-Dedekindian p-groups G such that whenever $C \leq A < G$, where $C \in \mathcal{C}_v$ and A is abelian, then $|A : C| \leq p$.

Problem 2. Classify the non-Dedekindian p-groups such that whenever $C < G$ is nonnormal cyclic, then $|\mathrm{N}_G(C) : C| \leq p^2$.

Problem 3. Let H be a subgroup of a p-group G. Study the structure of G if for every maximal cyclic subgroup C of G not contained in H we have $|\mathrm{N}_G(C) : C| = p$.

Problem 4. Let H be a maximal subgroup of a non-Dedekindian 2-group G. Describe the structure of G provided all minimal nonabelian subgroups of G not contained in H (see Theorem 10.28) are isomorphic to Q_8.

Problem 5. Classify the non-Dedekindian p-groups G such that $|\mathrm{N}_G(C) : C| = p$ for all nonnormal maximal cyclic $C < G$.

Problem 6. Classify the non-Dedekindian p-groups G such that $|\mathrm{N}_G(H) : H| = p$ for all maximal nonnormal $H < G$.

Problem 7. Suppose that $H < G$ is noncyclic. Study the structures of H and G provided all maximal abelian (cyclic) subgroups of H are maximal abelian (cyclic) in G.

In conclusion we solve Problem 1 (see Theorem 138.7 and 138.8).

Lemma 138.6. *Let G be a non-Dedekindian metacyclic p-group of order $> p^3$ satisfying the hypothesis of Problem 1. Then G is one of the groups from Theorem 138.4.*

Proof. One may assume that G satisfies $|G| > p^4$. Also assume that G is not a 2-group of maximal class. Then $R = \Omega_1(G)$ is abelian of type (p, p) (Lemma 1.4 and Proposition 10.19). Since $\mathrm{C}_G(R)$ contains an abelian subgroup A of type (p^2, p), it follows that all subgroups of order p are normal in G whence $R \leq \mathrm{Z}(G)$. Let $H \leq G$ be minimal nonabelian. By what has just been said and Proposition 10.19, we get $|H| > p^3$. As in the proof of Theorem 138.4, we deduce that $|H| = p^4$ and $\exp(H) = p^2$. Let $K < \Omega_1(G)$ be of order p such that $K \neq H'$. Then H/K is a nonabelian subgroup of order p^3 in G/K so, since $|G/K| > p^3$, it follows that G/K is a 2-group of maximal class (Proposition 10.19). By Taussky's Proposition 1.6, we have $|G : G'| > 4$ so, by assumption, $K \not\leq G'$, and we conclude that G' is cyclic of index 8 in G hence G/G' is abelian of type $(4, 2)$. As above, there is a cyclic subgroup $Z > G$ such that G/Z is cyclic of order 4. Let L be a cyclic subgroup of order 4 in H such that $L \cap H' = \{1\}$. Then we have $L \in C_\nu$ $(\nu = 2)$ and $L \cap Z = L \cap G' = \{1\}$. Hence $G = LZ$ and $\mathrm{C}_Z(L) = \Omega_1(Z)$ shows that G is a group from Theorem 138.4(c). □

Theorem 138.7. *If a non-Dedekindian p-group G of order $> p^3$, $p > 2$, is a group of Problem 1, then G is metacyclic of order p^4 and exponent p^2.*

Proof. In view of Lemma 138.6, it suffices to show that G is metacyclic. Assume, by way of contradiction, that G is not metacyclic. As in the proof of Theorem 138.4, we have

(i) $\Omega_1(G) \leq \mathrm{Z}(G)$ is of order p^2. Then G is not a group of maximal class.

(ii) If $H \leq G$ is minimal nonabelian, it is metacyclic of order p^4 and exponent p^2.

By assumption, $H < G$. Let $R \leq H$ be of order p such that $R \neq H'$; then we have $R \lhd G$ by (i). In this case, H/R is a nonabelian subgroup of order p^3 in G/R. Write $N/R = \mathrm{N}_{G/R}(H/R)$; then $|N| > p^4$. By (i), N has no elementary abelian subgroup of order p^3. Then N is a group from Theorem 13.7. Therefore, by (i), N is metacyclic of order $> p^4$, contrary to Lemma 138.6. □

Not all arguments in the proof of Theorem 138.4 work under hypothesis of the following theorem (for example, one cannot assert that $G/\mathfrak{V}_1(L)$ is a 2-group of maximal class).

Theorem 138.8. *If G is a non-Dedekindian nonmetacyclic 2-group of Problem 1 and $|G| > 2^5$, then $\nu = 2$. Suppose that $G \ncong \mathrm{Q}_{2^n} \times \mathrm{C}_2$. Then*

(a) *There is in G an abelian subgroup, say A, of index 2. Let $G = \langle x, A\rangle$.*

(b) *$\Omega_1(G) = \mathrm{Z}(G)$ is of order 4 and all elements of the set $G - A$ have order 4. Also, we have $\mathrm{d}(A) = 2$.*

(c) *All subgroups of A of order* 4 *are normal in* G.

(d) *Any cyclic subgroup of G of order* 4 *not contained in A is nonnormal in* G.

Conversely, any group G satisfying conditions (a)–(d) *also satisfies the condition of Problem 1.*

Proof. Let $R \lhd G$ be abelian of type $(2, 2)$ (Lemma 1.4) and let $B/R < \mathrm{C}_G(R)/R$ be of order 2; then B is abelian of order 8. By hypothesis, all subgroups of R of order 2 are normal in G so that $R \leq \mathrm{Z}(G)$. As in part (ii) of the proof of Theorem 138.4, we obtain $|\Omega_1(G)| = 4$ so $\Omega_1(G) = R \leq \mathrm{Z}(G)$. Arguing as in the proof of Theorem 138.4, one proves that any minimal nonabelian subgroup of G is either isomorphic to Q_8 or metacyclic of order 16 and exponent 4.

As, by hypothesis, $G \ncong \mathrm{Q}_{2^m} \times \mathrm{C}_2$, there is in G a metacyclic minimal nonabelian subgroup H of order 16 and exponent 4 (H exists in view of Corollary A.17.3 and what has been said in the previous paragraph). Since H has a nonnormal cyclic subgroup, say L, of order 4, we have $v = 2$. By hypothesis, $\mathrm{C}_H(L)$ of order 8 is maximal abelian in G so that $\mathrm{C}_G(L) = \mathrm{C}_H(L)$. As $\Omega_1(G) \leq \mathrm{Z}(G) < \mathrm{C}_G(L)$, it follows that $\mathrm{Z}(G) = \Omega_1(G)$. Let A be a maximal normal abelian subgroup of G; then $\Omega_1(G) < A$ so that A is metacyclic but noncyclic since $|\Omega_1(G)| = 4$. For any $x \in G - A$ there exists an element $a \in A$ such that $U = \langle a, x\rangle$ is minimal nonabelian (Lemma 57.1). Since $\exp(U) = 4$, we get $o(x) = 4$ so that all elements of the set $G - A$ have the same order 4. Because $x^2 \in \Omega_1(G) = \mathrm{Z}(G)$ centralizes A, it follows that $x^2 \in A$, and we conclude that G/A is elementary abelian. Therefore, since $|G| > 2^5$, we get $|A| > 8$ (otherwise, $G/A \cong \mathrm{Aut}(A) \cong \mathrm{D}_8$). In this case, all cyclic subgroups of A of order 4 are normal in G by hypothesis. Let $R < A$ be cyclic of order 4. Then $|G : \mathrm{C}_G(R)| = 2$ since $R \ntriangleleft \mathrm{Z}(G)$ in view of $\exp(\mathrm{Z}(G)) = 2$. Assume that $|G/A| > 2$. Then we infer that $\mathrm{C}_G(R) > A$ hence there is $b \in \mathrm{C}_G(R) - A$ of order 4 (recall that all elements of the set $G - A$ have order 4). Clearly, $\langle b, A\rangle$ is nonabelian (indeed, A is maximal abelian in G) of order $2|A|$ and $R < \mathrm{Z}(\langle b, A\rangle)$. By Corollary A.17.3, $\langle b, A\rangle$ has a minimal nonabelian subgroup $H_1 \ncong \mathrm{Q}_8$ since $\langle b, A\rangle \ncong \mathrm{Q}_{2^n} \times \mathrm{E}_{2^s}$: the center of the last group has exponent $2 < 4 = \exp(R)$. By the above, H_1 is metacyclic of order 16 and exponent 4. Since R centralizes H_1 and $R \ntriangleleft H_1$, there is in $H_1 * R$ (of order 32) an abelian subgroup of order 16 containing a nonnormal cyclic subgroup of H_1 of order $4 = 2^v$, contrary to the hypothesis. Thus $|G : A| = 2$.

Let $D < G$ be cyclic of order 4 such that $D \ntriangleleft A$. Then we have $G = AD$. Assume that $D \lhd G$. Then $G/(A \cap D)$ is abelian so $A \cap D = G'$ is of order 2. In this case, by Lemma 1.1,

$$|G| = 2|G'||\mathrm{Z}(G)| = 16,$$

contrary to the hypothesis. Thus all cyclic subgroups of G of order 4 not contained in A are nonnormal in G.

It remains to show that our group G satisfies the condition of Problem 1 if it satisfies conditions (a)–(d) in the statement of the theorem. Note that the set $\mathcal{C}_v$ coincides with the set of all cyclic subgroups of G that are not contained in A.

Let $D \in \mathcal{C}_v (= \mathcal{C}_2)$. Assume that $D < B < G$, where B is abelian of order 16. As $|B \cap A| = 8$, the subgroup $B \cap A$ has a cyclic subgroup L of order 4. Then

$$\mathrm{C}_G(L) \geq AD = G$$

so that $L < \mathrm{Z}(G)$, a contradiction since $\exp(\mathrm{Z}(G)) = 2 < 4 = \exp(L)$. □

We claim that if the 2-group $G = \langle x \rangle A$ of order $\geq 2^6$ satisfying conditions (a)–(d) of Theorem 138.8 is metacyclic, then it is as in Theorem 138.4(c). Let $x \in G - A$ and write $X = \langle x \rangle$. We want to prove that then $A = \Omega_1(X) \times C$, where C is cyclic. If this is false, there is in A an element y of order 4 such that $y^2 = x^2$ (indeed, if all invariants of an abelian group, say B, are $> p$, then any element of B of order p is contained in a cyclic subgroup of B of order p^2; this follows from Theorem 6.1 with $G = Q$). Since $\langle y \rangle \lhd G$ by (d), one has $y^x = x^{-1}$ (otherwise, $y \in \mathrm{Z}(G) = \Omega_1(G)$), and we conclude that $\langle x, y \rangle \cong \mathrm{Q}_8$ so that G is of maximal class (Proposition 10.19), which is a contradiction. Thus

(e) $A = \Omega_1(X) \times C$, where C is cyclic (of index 2 in A).

(f) We claim that the quotient group $\bar{G} = G/\Omega_1(X)$ is of maximal class. Indeed, $\bar{G}$ has a cyclic subgroup $\bar{A} \cong C$ of index 2 by (e). Assume that $\bar{G}$ is not of maximal class. Then, by Theorem 1.2, $\bar{G}$ is either abelian of type $(2^n, 2)$ or isomorphic to $\mathrm{M}_{2^{n+1}}$. In the first case, we get $X \lhd G$, a contradiction. Thus $\bar{G} \cong \mathrm{M}_{2^{n+1}}$, $n \geq 4$, as $|G| \geq 2^6$. Let $\bar{B}$ be a noncyclic maximal subgroup of $\bar{G}$; then $\bar{X} < \bar{B}$. In this case, we get $\bar{X} \lhd \bar{B}$ since $\bar{B}$ is abelian, and $|\bar{B}| = 2^n \geq 2^4$. It then follows that B is nonabelian by hypothesis. The quotient group B/X is cyclic of order $2^{n-1} \geq 2^3$. Then $\mathrm{C}_B(X)$ is abelian of order $2^n \geq 2^4$, contrary to the hypothesis. Thus $\bar{G}$ is of maximal class.

As in the proofs of Theorems 138.4 and 138.8, we get (recall that G is not of maximal class)

(g) G' is cyclic and G/G' is abelian of type $(4, 2)$.

(h) G is as in Theorem 138.4(c).

Therefore, if A has no cyclic subgroup of index 2, then G is nonmetacyclic.

Now we present a nonmetacyclic 2-group G satisfying conditions (a)–(d) of Theorem 138.8. Let

$$G = \langle x, a, b \mid a^{2^m} = b^{2^n} = 1,\ m, n \geq 2,\ m + n \geq 5,$$
$$x^2 = a^{2^{m-1}},\ ab = ba,\ a^x = a^{-1},\ b^x = b^{-1} \rangle.$$

We have $\langle a, x \rangle \cong \mathrm{Q}_{2^{m+1}}$ and $\langle b, x \rangle \cong \mathrm{D}_{2^{n+1}}$. Further, we have $|G| = 2^{m+n+1} > 2^5$ and $c = [x, a^i b^j] = a^{2i} b^{2^j} \in G'$ with $c = 1$ if and only if $i \geq m - 1$ and $j \geq n - 1$. It follows that $\mathrm{Z}(G) = \langle a^{2^{m-1}} \rangle \times \langle b^{2^{n-1}} \rangle$ is abelian of type $(2, 2)$. Clearly, we have $G' = [\langle x \rangle, A]$. Since the noncyclic subgroup $\langle a^2 \rangle \times \langle b^2 \rangle$ of index 8 in G is contained in G' and $|G : G'| > 4$ (Proposition 1.6), it coincides with G' so that $G' = \langle a^2 \rangle \times \langle b^2 \rangle$ is abelian of type $(2^{m-1}, 2^{n-1})$, and we conclude that G is nonmetacyclic. If $y \in G - A$

is arbitrary, then y inverts A since $\mathrm{C}_G(y) = \langle y, \mathrm{Z}(G)\rangle$ is abelian of type $(4, 2)$. It follows that G satisfies the condition of Problem 1.

It is interesting to classify the nonnilpotent groups G such that whenever $H < G$ is nonnormal, then either $\mathrm{N}_G(H) = H$ or $|\mathrm{N}_G(H) : H|$ is a prime. There is a nonsolvable group satisfying this condition, for example, $\mathrm{PSL}(2, 5)$. Using Theorem 138.4, Frobenius' normal p-complement theorem for $p = 2$ (see Lemma 10.8), the Odd Order Theorem and the classification of simple groups with abelian Sylow 2-subgroup of type $(2, 2)$, it is easy to prove that $\mathrm{PSL}(2, 5)$ is the unique nonsolvable group satisfying the above condition.

§139

p-groups with a noncyclic commutator group all of whose proper subgroups have a cyclic commutator group

This section is written by the second author.

Here we give a characterization of the title groups (Theorem 139.A). The surprising and deep result is that if G is a title group, then G' is elementary abelian of order p^2 or p^3 and for each $H < G$ we have $|H'| \leq p$. We use here a corresponding characterization result of A. Leone (see Theorem B in [Leo]), but most of our proofs are simpler. At the beginning we prove two very useful lemmas, and then the main result (Theorem 139.A) will be proved in a series of propositions concerning the title groups.

Theorem 139.A. *A p-group G has a noncyclic commutator group G' and each proper subgroup H of G has a cyclic commutator group H' if and only if for each $H < G$ we have $|H'| \leq p$ and exactly one of the following holds:*

(a) $\mathrm{d}(G) = 2$, $\mathrm{cl}(G) = 3$, *and* $G' \cong \mathrm{E}_{p^2}$.

(b) $p > 2$, $\mathrm{d}(G) = 2$, $\mathrm{cl}(G) = 3$, $G' \cong \mathrm{E}_{p^3}$ *and* $\mathfrak{V}_1(G) \leq \mathrm{Z}(G)$.

(c) $\mathrm{d}(G) = 3$, $\mathrm{cl}(G) = 2$, $G' \cong \mathrm{E}_{p^3}$ *or* E_{p^2} *and* $\Phi(G) = \mathrm{Z}(G)$.

A p-group G is said be a *KC-group* if the commutator group G' is cyclic. Then the title groups are actually p-groups which are minimal non-KC-groups.

Lemma 139.1. *Let $G = \langle x, y\rangle$ be a nonabelian two-generator KC-group. If $p > 2$ or $p = 2$ and $[G', G] \leq \mathfrak{V}_2(G')$, then $\mathfrak{V}_1(G') = \langle [x, y]^p\rangle = \langle [x, y^p]\rangle$.*

Proof. By hypothesis, $G' = \langle [x, y]\rangle$. If $\mathfrak{V}_1(G') = \{1\}$, then $|G'| = p$ and G is minimal nonabelian (Lemma 65.2(a)), and the result follows from Lemma 65.1. Next we assume that $\mathfrak{V}_1(G') > \{1\}$ and consider the quotient group $\bar{G} = G/\mathfrak{V}_2(G')$. Then we get $\mathrm{d}(\bar{G}) = 2$ and $\bar{G}' \cong \mathrm{C}_{p^2}$. As $\bar{G}/\mathfrak{V}_1(\bar{G}')$ is minimal nonabelian (Lemma 65.2(a)), for each $H \in \Gamma_1$ we have $|\bar{H}'| \leq p$.

(i) Assume that $p > 2$. In this case, we may apply Proposition 137.5 for the group $\bar{G}$. We get $[x, y^p] = [x, y]^p \cdot \zeta$, where $\zeta \in \mathfrak{V}_2(G')$. But this gives

$$\langle [x, y^p]\rangle = \langle [x, y]^p\rangle$$

and we are done.

(ii) Suppose that $p = 2$. Then we compute

$$[x, y^2] = [x, y][x, y]^y = [x, y][x, y]([x, y]^{-1}[x, y]^y)$$
$$= [x, y]^2[[x, y], y].$$

By our assumption, we have $[[x, y], y] \in [G', G] \leq \mho_2(G')$ and so we obtain again $\langle [x, y^2] \rangle = \langle [x, y]^2 \rangle$. □

Lemma 139.2. *Let $G = \langle a, b, c \rangle$ be a p-group of Theorem 137.7*(d)*, i.e.,*

$$\mathrm{d}(G) = 3, \quad \mathrm{cl}(G) = 2, \quad G' \cong \mathrm{E}_{p^3} \text{ or } \mathrm{E}_{p^2} \quad \text{and} \quad \Phi(G) = \mathrm{Z}(G).$$

Then for each subgroup X of order p which is contained in G' there is a maximal subgroup L of G such that $L' = X$.

Proof. If $G' \cong \mathrm{E}_{p^3}$, then all $p^2 + p + 1$ maximal subgroups of G must have pairwise distinct commutator subgroups of order p. Indeed, if $L \neq K$ are two distinct maximal subgroups of G such that $L' = K'$, then Exercise 1.69(a) would imply $|G'| \leq p^2$, a contradiction. Hence in this case each subgroup of order p in G' is a commutator subgroup of a maximal subgroup of G. Assume now that $G' \cong \mathrm{E}_{p^2}$. We may choose the generators a, b, c of G so that setting $[a, b] = k$ and $[b, c] = l$ we have $G' = \langle k, l \rangle$. But then for any $i = 0, 1, \ldots, p-1$ we obtain $[ac^{-i}, b] = [a, b][c, b]^{-i} = kl^i$ and so again each subgroup of order p in G' is a commutator subgroup of one of the maximal subgroups $\Phi(G)\langle b, c \rangle$ and $\Phi(G)\langle ac^{-i}, b \rangle$ $(i = 0, 1, \ldots, p-1)$ of G. □

Proposition 139.3. *Let G be a p-group which is a minimal non-*KC*-group. Then we have:*

(i) $\mathrm{Z}(G) \leq \Phi(G)$.

(ii) *G is metabelian.*

(iii) $\mathrm{d}(G) \leq 3$.

Proof. (i) Suppose $\mathrm{Z}(G) \not\leq \Phi(G)$. Then there is a maximal subgroup M of G such that $G = \langle M, x \rangle$, where $x \in \mathrm{Z}(G)$. But then $G' = M'$ is cyclic, a contradiction.

(ii) Let M be a maximal subgroup of G so that M' is cyclic and $M' \trianglelefteq G$. Since $\mathrm{Aut}(M')$ is abelian, $G/\mathrm{C}_G(M')$ is abelian and so G' centralizes M'. Set

$$H = \langle M' \mid M \text{ is any maximal subgroup in } G \rangle$$

so that H is characteristic in G and $H \leq \mathrm{Z}(G')$. Each maximal subgroup M of G contains H and M/H is abelian. Thus G/H is either abelian or minimal nonabelian. This gives $|G'/H| \leq p$ and so G' is abelian.

(iii) We consider $G/\Phi(G')$ so that $G'/\Phi(G')$ is elementary abelian of order $\geq p^2$. Each maximal subgroup $M/\Phi(G')$ of $G/\Phi(G')$ has its derived subgroup of order $\leq p$ and so, by Proposition 137.3, $\mathrm{d}(G/\Phi(G')) \leq 3$ and therefore $\mathrm{d}(G) \leq 3$. □

Proposition 139.4. *A p-group G is a minimal non-KC-group with*

$$H = \langle M' \mid M \text{ is any maximal subgroup in } G\rangle$$

being cyclic if and only if $G' \cong \mathrm{E}_{p^2}$ and $\mathrm{d}(G) = 2$. Here we have $\mathrm{cl}(G) = 3$.

Proof. Suppose that G is a p-group which is a minimal non-KC-group and H is cyclic. Then $G' > H$ and each maximal subgroup of G/H is abelian. It follows that G/H is minimal nonabelian. This gives $\mathrm{d}(G/H) = 2$ and so $\mathrm{d}(G) = 2$ and $|G' : H| = p$ so that G' is abelian of type (p^n, p), $n \geq 1$, where $|H| = p^n$ and $\exp(G') = p^n$. We set $G = \langle a, b\rangle$, where $[a, b] \in G' - H$. The commutator group G' is generated by all conjugates of $[a, b]$ in G and since G' is abelian, we have $\exp(G') = p^n = o([a, b])$. Thus H and $\langle [a, b]\rangle$ are two distinct cyclic subgroups of order p^n (and index p) in G'.

Suppose, by way of contradiction, that $n > 1$. Then $\mathrm{c}_n(G') = p$ and since one of the cyclic subgroups, H, of order p^n is normal in G, it follows that all of them are normal in G. But then $\langle [a, b]\rangle$ is normal in G and so $G' = \langle [a, b]\rangle$ is cyclic, a contradiction. It follows that $n = 1$, $|H| = p$ and $o([a, b]) = p$ so that $G' \cong \mathrm{E}_{p^2}$.

Conversely, assume that G is a p-group with $\mathrm{d}(G) = 2$ and $G' \cong \mathrm{E}_{p^2}$. Let $N < G'$ be a G-invariant subgroup of order p contained in G'. Then we infer that $\mathrm{d}(G/N) = 2$ and $(G/N)' = G'/N$ is of order p and so G/N is minimal nonabelian. Hence, if M is any maximal subgroup of G, then $M \geq G'$ and M/N is abelian, which gives $M' \leq N$.

It is easy to see that such a p-group G is of class 3. Indeed, if $G' \leq \mathrm{Z}(G)$, then considering a subgroup $K < G'$ of order p with $K \neq N$, we conclude that G/K is minimal nonabelian and so for any maximal subgroup M of G we get also $M' \leq K$ and so $M' \leq N \cap K = \{1\}$. In this case, G would be minimal nonabelian and so $|G'| = p$, a contradiction. Hence we obtain that $G' \not\leq \mathrm{Z}(G)$ and so G is of class 3. Our proposition is proved. □

Proposition 139.5. *Let G be a p-group which is a minimal non-KC-group with*

$$H = \langle M' \mid M \text{ is any maximal subgroup in } G\rangle$$

being noncyclic and $\mathrm{d}(G) = 2$. Then

$$p > 2, \quad \mathrm{cl}(G) = 3, \quad G' \cong \mathrm{E}_{p^3}, \quad \textit{and} \quad \mho_1(G) \leq \mathrm{Z}(G).$$

Proof. Suppose that G is a p-group which is a minimal non-KC-group, H is noncyclic and $\mathrm{d}(G) = 2$. Then there exist maximal subgroups M and N such that $H_0 = M'N'$ is noncyclic. Then the factor group G/H_0 has two distinct abelian maximal subgroups M/H_0 and N/H_0 and this gives $|G' : H_0| \leq p$. Suppose for a moment that $G' = H_0$. Let X be a G-invariant subgroup such that $M' \leq X < H_0$ and $|H_0 : X| = p$. Since $\mathrm{d}(G/X) = 2$ and $(G/X)' = H_0/X$ is of order p, it follows that G/X is minimal nonabelian. But then N/X is abelian and so $N' \leq X$, a contradiction. We have proved that $|G' : H_0| = p$ and since $\mathrm{d}(G/H_0) = 2$ and $(G/H_0)' = G'/H_0$ is of order p, it follows that G/H_0 is minimal nonabelian. For each maximal subgroup L of G, $L' \leq H_0$

and so $H_0 = H$ and $\mathrm{d}(H) = 2$. Also, for any two distinct maximal subgroups K and L of G we have $K'L' = H$. Indeed, by Exercise 1.69(a), $|G' : (K'L')| \leq p$ and so $K'L' = H$.

Consider the factor group $G/\Phi(H)$ so that $H/\Phi(H) \cong \mathrm{E}_{p^2}$ and $|G'/\Phi(H)| = p^3$. Using Theorem 137.7 for $G/\Phi(H)$, we see that $G/\Phi(H)$ is a group from part (c) of that theorem. In particular, we have $p > 2$, $\mathrm{cl}(G/\Phi(H)) = 3$ and $G'/\Phi(H) \cong \mathrm{E}_{p^3}$ so that $\mathrm{d}(G') = 3$. Let M_i $(i = 1, 2, \ldots, p+1)$ be the set of all maximal subgroups of G and so we infer that G'/M_i' is noncyclic. For any fixed $i \in \{1, 2, \ldots, p+1\}$ we consider the factor group G/M_i'. We see that $\mathrm{d}(G/M_i') = 2$, $(G/M_i')' = G'/M_i'$ is noncyclic, but for each maximal subgroup M_j/M_i' $(j = 1, 2, \ldots, p+1)$ of G/M_i' we have $(M_j/M_i')' \leq (M_j'M_i')/M_i' \leq H/M_i'$ and so each maximal subgroup of G/M_i' has its commutator group contained in the same cyclic subgroup H/M_i'. We may apply Proposition 139.4 to conclude that $G'/M_i' \cong \mathrm{E}_{p^2}$. Thus M_i' $(i = 1, 2, \ldots, p+1)$ are pairwise distinct cyclic maximal subgroups of H. Set $|M_i'| = p^m$, $m \geq 1$, so that H is abelian of type (p^m, p). If $m > 1$, then such a group H has exactly p cyclic maximal subgroups (of order p^m) and a noncyclic maximal subgroup (of type (p^{m-1}, p)). This is a contradiction (because we need in H exactly $p+1$ pairwise distinct cyclic maximal subgroups) and so $m = 1$ and $|G'| = p^3$. But we have

$$\mathrm{d}(G') = 3 \quad \text{and so} \quad \Phi(G') = \Phi(H) = \{1\}.$$

Hence G is a group from part (c) of Theorem 137.7 and we are done. □

The following result is crucial for the whole investigation.

Proposition 139.6. *Let G be a p-group which is a minimal non-KC-group. Suppose that there exist nonabelian maximal subgroups M, N of G such that $M' \cap N' = \{1\}$. If $p > 2$ or $p = 2$ and $[L', L] \leq \mho_2(L')$ for all $L \in \Gamma_1$, then $H = \langle M' \mid M \in \Gamma_1 \rangle$ is elementary abelian and central in G.*

Proof. As $M \cap N$ is abelian, there are $m \in M \cap N$ and $n \in N - M$ with $N' = \langle [m, n] \rangle$. Indeed, if $N' = \langle [n', n] \rangle$ with $n, n' \in N - M$, then $n' = n^i m$ for some $m \in M \cap N$ and $[n', n] = [n^i m, n] = [m, n]$. We apply Lemma 139.1 on the group $\langle m, n \rangle$ which is a nonabelian two-generator group with a cyclic commutator group $\langle [m, n] \rangle$. It follows that $\langle [m, n]^p \rangle = \langle [m, n^p] \rangle$. But $n^p \in M$ and so $[m, n^p] \in N' \cap M' = \{1\}$ and therefore $\mho_1(N') = \{1\}$ which gives $|N'| = p$. In an analogous way, we also get $|M'| = p$. Let L be any maximal subgroup of G with $L' \neq \{1\}$. Then either $L' \cap M' = \{1\}$ or $L' \cap N' = \{1\}$ since $M' \cap N' = \{1\}$. This gives $|L'| = p$ and so $L' \leq \mathrm{Z}(G)$. Hence H is elementary abelian and central in G. □

In what follows we may assume that $\mathrm{d}(G) = 3$. This implies that

$$H = \langle M' \mid M \text{ is any maximal subgroup in } G \rangle = G',$$

i.e., G' is generated with commutator subgroups of all maximal subgroups of G.

Proposition 139.7. *Let G be a p-group which is a minimal non-KC-group satisfying $\mathrm{d}(G) = 3$. Suppose that there exist maximal subgroups M, N of G such that $M' \neq \{1\}$, $N' \neq \{1\}$ and $M' \cap N' = \{1\}$. If $p > 2$ or $p = 2$ and $[L', L] \leq \mho_2(L')$ for all maximal subgroups L of G, then G is a p-group in Theorem 137.7*(d)*, i.e.,*

$$\mathrm{d}(G) = 3, \quad \mathrm{cl}(G) = 2, \quad G' \cong \mathrm{E}_{p^3} \text{ or } \mathrm{E}_{p^2},$$

and $\Phi(G) = \mathrm{Z}(G)$.

Proof. By Proposition 139.6, G' is elementary abelian (noncyclic) and central in G. Due to Theorem 137.7, G is a p-group in Theorem 137.7 (d) and we are done. □

Proposition 139.8. *Let G be a p-group which is a minimal non-KC-group satisfying $\mathrm{d}(G) = 3$. If $p > 2$ or $p = 2$ and $[L', L] \leq \mho_2(L')$ for all maximal subgroups L of G, then there exist maximal subgroups M, N of G such that*

$$M' \neq \{1\}, \quad N' \neq \{1\} \quad \text{and} \quad M' \cap N' = \{1\}.$$

Proof. Suppose, by way of contradiction, that $L' \cap T' \neq \{1\}$ for any maximal subgroups L, T of G with $L' \neq \{1\}$, $T' \neq \{1\}$. Since G' is noncyclic, there exist maximal subgroups M and N of G such that $\langle M', N' \rangle$ is noncyclic and we have $M' \cap N' \neq \{1\}$. Applying Proposition 139.6 on the factor group $G/(M' \cap N')$, we get

$$|M'/(M' \cap N')| = p \quad \text{and} \quad |N'/(M' \cap N')| = p$$

so that $|M'| = |N'| = p^n$, $n > 1$. We may set $M' = \langle h \rangle$, $N' = \langle k \rangle$ so that $h^p = k^p$. Then we have $hk^{-1} \neq 1$ and $(hk^{-1})^p = 1$ so that $\langle hk^{-1} \rangle$ is a subgroup of order p in G' with $\langle hk^{-1} \rangle \not\leq M'$ and $\langle hk^{-1} \rangle \not\leq N'$ and we get $M' \cap N' = \langle h^p \rangle = \langle k^p \rangle$. Let L be any maximal subgroup of G. Then we have either $L' \leq M' \cap N'$ or $|L'| = p^n$, $L' > M' \cap N'$ and $|L'/(M' \cap N')| = p$.

We study the factor group $G/(M' \cap N')$ which is a minimal non-KC-group (noting that $\langle M', N' \rangle/(M' \cap N') \cong \mathrm{E}_{p^2}$), where each maximal subgroup of $G/(M' \cap N')$ has its commutator group of order at most p and $\mathrm{d}(G/(M' \cap N')) = 3$. It follows that $G/(M' \cap N')$ is a group from Theorem 137.7(d) and so we may apply Lemma 139.2 on this group. Hence there is a maximal subgroup L of G with $L' = \langle hk^{-1}, M' \cap N' \rangle$. But then L' is noncyclic, a contradiction. □

Lemma 139.9. *Suppose that G is a 2-group which is a minimal non-KC-group such that $\exp(G') = 4$ and $\mathrm{d}(G) = 3$. Assume, in addition, that there is a maximal subgroup M of G such that $M' \cong \mathrm{C}_4$ and $[M', M] \neq \{1\}$. If there exists another maximal subgroup N of G with $N' \neq \{1\}$ and $M' \cap N' = \{1\}$, then the following statements hold:*

(i) $M' \cap L' \neq \{1\}$ *for each maximal subgroup L of G with $L \neq N$.*

(ii) $N = \mathrm{C}_G(G') = \mathrm{C}_G(M')$.

(iii) $|N'| = 2$.

Proof. For any $a \in M'$ and $n \in N$ we have

$$[a,n] \in M' \cap N' = \{1\} \quad \text{and so} \quad \mathrm{C}_G(M') = N.$$

Hence, if L is any maximal subgroup of G with $L \neq N$, then $L \not\leq \mathrm{C}_G(M')$. Therefore $\{1\} \neq [M', L] \leq M' \cap L'$ and this gives (i).

If L is any maximal subgroup of G with $L \neq N$, then $M' \cap L' \neq \{1\}$ together with $M' \cap N' = \{1\}$ implies that $L' \cap N' = \{1\}$. Hence $[N', L] \leq N' \cap L' = \{1\}$ and so $N' \leq \mathrm{Z}(G)$. Also, $[L', N] \leq L' \cap N' = \{1\}$ and so $\mathrm{C}_G(L') \geq N$ which together with $\mathrm{C}_G(M') = N$ gives $\mathrm{C}_G(G') = N$ and (ii) is proved.

We may choose $m \in M \cap N$ and $n \in N - M$ so that $N' = \langle [m,n] \rangle$ (noting that $M \cap N$ is abelian). As $N' \leq \mathrm{Z}(G)$, we may apply Lemma 139.1 on the group $\langle m, n \rangle$. We get $\langle [m,n]^2 \rangle = \langle [m, n^2] \rangle = \{1\}$, which gives $|N'| = 2$ and this is (iii). □

Proposition 139.10. *Let G be a 2-group which is a minimal non-KC-group satisfying $\mathrm{d}(G) = 3$. Then $[M', M] \leq \mathfrak{V}_2(M')$ for all maximal subgroups M of G.*

Proof. Suppose, by way of contradiction, that there exists a maximal subgroup X of G such that $[X', X] \not\leq \mathfrak{V}_2(X')$. In particular, X' is cyclic of order ≥ 4 and so G' is of exponent ≥ 4. Note that the factor group $G/\mathfrak{V}_2(G')$ is a minimal non-KC-group such that $\mathrm{d}(G/\mathfrak{V}_2(G')) = 3$ and $(G/\mathfrak{V}_2(G'))'$ is noncyclic of exponent 4. We want to show that such a 2-group $G/\mathfrak{V}_2(G')$ does not exist and so we may assume in the sequel that $\mathfrak{V}_2(G') = \{1\}$. In other words, we may assume that G is 2-group which is a minimal non-KC-group with $\mathrm{d}(G) = 3$ and G' is noncyclic of exponent 4.

First suppose that for each maximal subgroup L of G we have $[L', L] \leq \mathfrak{V}_2(L')$. Then Proposition 139.8 implies that there exist maximal subgroups M, N of G such that $M' \neq \{1\}$, $N' \neq \{1\}$ and $M' \cap N' = \{1\}$. By Proposition 139.7, G' is elementary abelian of order 4 or 8, contrary to the fact that G' is noncyclic of exponent 4. Thus we have proved that there exists a maximal subgroup M of G that satisfies $M' \cong \mathrm{C}_4$ and $[M', M] \not\leq \mathfrak{V}_2(M')$, i.e., $[M', M] \neq \{1\}$.

(a) Assume that there is a maximal subgroup N of G such that

$$N' \neq \{1\} \quad \text{and} \quad M' \cap N' = \{1\}.$$

In this case, all assumptions of Lemma 139.9 are satisfied and so the statements (i), (ii) and (iii) of that lemma hold. Let L be any maximal subgroup of G with $L \neq N$. Then $L' \cap M' \neq \{1\}$, $L' \cap N' = \{1\}$, and either $L' \leq \mathrm{Z}(G)$ or $\mathrm{C}_G(L') = N$.

Assume that $L' \leq \mathrm{Z}(G)$. Here $N \cap L$ is abelian and so there are elements $l \in N \cap L$ and $l' \in L - N$ such that $L' = \langle [l, l'] \rangle$. By Lemma 139.1 applied to $\langle l, l' \rangle$, we obtain that $\langle [l,l']^2 \rangle = \langle [l, l'^2] \rangle = \{1\}$ (since $(l')^2 \in N \cap L$) which implies $|L'| = 2$ and so $L' = \Omega_1(M')$.

Suppose that $\mathrm{C}_G(L') = N$ so that in this case $L' \cong \mathrm{C}_4$ and $L' \cap M' \geq \Omega_1(M')$. We see that $G = \langle N, t \rangle$, where $t \in G - N$ and t inverts L'. Since $\mathrm{C}_G(G') = N$ and t inverts G' (noting that G' is generated by all X', where X is any maximal subgroup of G), it follows that each subgroup of G' is normal in G. Set $\Omega_1(M') = \langle z \rangle$ so that

$\mho_1(G') = \langle z\rangle$. Then we obtain $G' = \Omega_1(G')M'$ with $\Omega_1(G') \cap M' = \langle z\rangle$. We get $G' = M' \times N' \times K$ with $K \leq \Omega_1(G')$. Considering the factor group G/K, it follows that we may assume from the start that $G' = M' \times N'$ is abelian of type $(4, 2)$ (since we want to show that G/K does not exist).

Set $N' = \langle u\rangle$ so that $E = \Omega_1(G') = \langle u, z\rangle \leq \mathrm{Z}(G)$. We know that $N = \mathrm{C}_G(G')$. Also set $N = \Phi(G)\langle a, b\rangle$ so that $[a, b] \in \langle u\rangle$.

Consider $G/\langle z\rangle$ so that $G/\langle z\rangle$ is a group from Theorem 137.7(d). This implies that $\Phi(G/\langle z\rangle) = \Phi(G)/\langle z\rangle = \mathrm{Z}(G/\langle z\rangle)$. It follows that $(\Phi(G))' \leq \langle z\rangle \cap \langle u\rangle = \{1\}$ and for any $x \in N - \Phi(G)$, $[\Phi(G), x] \leq \langle z\rangle \cap \langle u\rangle = \{1\}$ so that the three maximal subgroups of N containing $\Phi(G)$ are abelian. This also forces $[a, b] = u$.

Take an element $c \in G - N$ so that $G = \langle a, b, c\rangle$. If $[a, c] \in E$ and $[b, c] \in E$, then G/E would be abelian and so $G' \leq E$, a contradiction. Hence (interchanging a and b if necessary), we may assume that $[a, c] \in G' - E$ so that $[a, c]^2 = z$.

We may assume that $[b, c] = z^\epsilon$ with $\epsilon = 0, 1$. Indeed, suppose that $[b, c] \notin \langle z\rangle$. Set $L = \Phi(G)\langle b, c\rangle$ so that L is a maximal subgroup of G which is distinct from N. By Lemma 139.9, $L' \cap M' \neq \{1\}$ and so $L' \geq \langle z\rangle$. It follows that $[b, c] \in G' - E$. Then we have (since $\Phi(G)\langle b\rangle$ is abelian)

$$[ab, c] = [a, c]^b[b, c] = [a, c][b, c] \in E.$$

The maximal subgroup $L_1 = \Phi(G)\langle ab, c\rangle$ of G is distinct from N and so, in view of Lemma 139.9, $L_1' \cap M' \neq \{1\}$ and so $L_1' \geq \langle z\rangle$ and $[ab, c] \in \langle z\rangle$. As $G = \langle a, ab, c\rangle$ and $[a, ab] = [a, b] = u$, we replace in this case b with ab so that we may assume from the start that $[b, c] = z^\epsilon$ with $\epsilon = 0, 1$.

We consider the proper subgroup $K = \langle ac, b, a^2\rangle$ of G (noting that $a^2 \in \Phi(G)$). Then we have

$$[ac, b] = [a, b]^c[c, b] = u^c z^\epsilon = uz^\epsilon$$

and

$$[a^2, ac] = [a^2, c] = [a, c]^a[[a, c]] = [a, c]^2 = z$$

as $a \in N$ commutes with $[a, c]$ (because $N = \mathrm{C}_G(G')$). But then $K' \geq \langle uz^\epsilon, z\rangle = E$ is noncyclic, a contradiction.

(b) Assume that for all maximal subgroups L of G with $L' \neq \{1\}$, $L' \cap M' \neq \{1\}$, where G' is noncyclic of exponent 4, $M' \cong \mathrm{C}_4$ and $[M', M] \neq \{1\}$. For each maximal subgroup L of G we have either $L' \leq M'$ or $L' \cong \mathrm{C}_4$ and $L' \cap M' = \langle i\rangle$, where we set $\langle i\rangle = \mho_1(M')$. Thus $\mho_1(G') = \langle i\rangle$ and $G'/\langle i\rangle$ is elementary abelian of order ≥ 4 (since G' is noncyclic). It follows that $G/\langle i\rangle$ is a group from Theorem 137.7(d) and so $G'/\langle i\rangle \cong \Omega_1(G') \cong \mathrm{E}_4$ or E_8. Let F be a four-subgroup contained in $\Omega_1(G')$ such that $F > \langle i\rangle$. Then Lemma 139.2 (applied on the group $G/\langle i\rangle$) gives that G possesses a maximal subgroup L_1 such that L_1' covers $F/\langle i\rangle$. But L_1' is cyclic and so $|L_1'| = 2$ and therefore $F = L_1' \times \langle i\rangle$, contrary to our assumption in (b). Our proposition is proved. □

We can now prove our main result.

Proof of Theorem 139.A. If G is a p-group from (a), (b) or (c) of Theorem 139.A, then Proposition 137.6 implies that $|H'| \leq p$ for each subgroup $H < G$. Conversely, if G is a p-group with G' being noncyclic but for each $H < G$ we have H' is cyclic, then Propositions 139.4, 139.5, 139.7, 139.8 and 139.10 show that $|H'| \leq p$ and we have one of the possibilities stated in parts (a), (b) or (c) of Theorem 139.A. □

§140

Power automorphisms and the norm of a p-group

An automorphism θ of a finite group G is called a *power automorphism* if it maps each subgroup of G onto itself. This will be the case if and only if θ maps each element $x \in G$ to some power x^i of x (therefore such a θ is called a power automorphism). We denote by $\mathrm{A}(G)$ the group of all power automorphisms of G and we shall prove here some elementary facts about $\mathrm{A}(G)$ (Theorem 140.7). Then, in Corollary 140.8, we obtain a result of E. Schenkman [Sc] asserting that the norm of a p-group G (which is the intersection of the normalizers of all subgroups of G) is contained in the second center $\mathrm{Z}_2(G)$ of G.

Lemma 140.1. *If $\theta \in \mathrm{A}(G)$ and $g \in G$, the inner automorphism induced by $g^{-1}g^\theta$ is a power automorphism.*

Proof. Let $H \leq G$ and $g \in G$. Then

$$H^g = (H^g)^\theta = (H^\theta)^{g^\theta} = H^{g^\theta}$$

whence (noting that g commutes with g^θ)

$$H = H^{g^\theta g^{-1}} = H^{g^{-1}g^\theta}$$

and so $g^{-1}g^\theta$ induces a power automorphism of G. □

Lemma 140.2. *If $\theta \in \mathrm{A}(G)$ and $g, h \in G$, then $[g^{-1}g^\theta, h][h^{-1}h^\theta, g] = 1$ and*

$$[g^{-1}g^\theta, h] \in \langle g \rangle \cap \langle h \rangle.$$

Proof. Since $g^\theta h^\theta = (gh)^\theta \in \langle gh \rangle$, it follows that $g^\theta h^\theta$ commutes with gh. Hence (noting that $[g, g^\theta] = 1$ and $[h, h^\theta] = 1$)

$$\begin{aligned}[g^{-1}g^\theta, h][hh^{-\theta}, g^{-1}] &= gg^{-\theta}h^{-1}g^{-1}(g^\theta h^\theta)(gh)h^{-\theta}g^{-1} \\ &= gg^{-\theta}h^{-1}g^{-1}(gh)(g^\theta h^\theta)h^{-\theta}g^{-1} = 1.\end{aligned}$$

We have proved

$$(*) \qquad [g^{-1}g^\theta, h][hh^{-\theta}, g^{-1}] = 1.$$

By Lemma 140.1, $g^{-1}g^{\theta}$ and $h^{-1}h^{\theta}$ induce inner power automorphisms on G and so $[g^{-1}g^{\theta}, h] \in \langle h\rangle$ and $[hh^{-\theta}, g^{-1}] \in \langle g\rangle$. Hence for all $g, h \in G$ we get

$$[g^{-1}g^{\theta}, h] \in \langle g\rangle \cap \langle h\rangle.$$

Interchanging g and h, we also have

$$[h^{-1}h^{\theta}, g] \in \langle g\rangle \cap \langle h\rangle$$

which shows that

$$\begin{aligned}[h^{-1}h^{\theta}, g] &= [h^{-1}h^{\theta}, g]^{hh^{-\theta}} = [h^{-1}h^{\theta}, h^{-1}h^{\theta}ghh^{-\theta}]\\ &= hh^{-\theta}\cdot h^{\theta}h^{-1}g^{-1}h^{-\theta}h\cdot h^{-1}h^{\theta}\cdot h^{-1}h^{\theta}ghh^{-\theta}\\ &= g^{-1}(h^{-1}h^{\theta})g(hh^{-\theta}) = g^{-1}g^{hh^{-\theta}} = g^{hh^{-\theta}}g^{-1} = [hh^{-\theta}, g^{-1}].\end{aligned}$$

Putting this into $(*)$, we finally get the required relation

$$[g^{-1}g^{\theta}, h][h^{-1}h^{\theta}, g] = 1. \qquad \square$$

Given an automorphism θ of a group G and $g, h \in G$, we set $[g, \theta] = g^{-1}g^{\theta}$ and $[g, \theta, h] = [[g, \theta], h]$.

Lemma 140.3. *If $\theta \in \mathrm{A}(G)$ and $[g_i, \theta, h_j] = 1$ for $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$, then*

$$[g_1g_2\ldots g_n, \theta, h_1h_2\ldots h_m] = 1.$$

Proof. By Lemma 140.2 which asserts that $[g, \theta, h][h, \theta, g] = 1$ $(g, h \in G)$, we may assume $m \geq n$. We prove this lemma by induction on m. If $m = 1$, then $n = 1$ and $[g_1, \theta, h_1] = 1$ by assumption. In case $m > 1$, we get

$$\begin{aligned}&[g_1g_2\ldots g_n, \theta, (h_1h_2\ldots h_{m-1})h_m]\\ &\qquad = [g_1g_2\ldots g_n, \theta, h_m][g_1g_2\ldots g_n, \theta, h_1h_2\ldots h_{m-1}]^{h_m} = 1\end{aligned}$$

by induction hypothesis. $\square$

Lemma 140.4. *If $\theta \in \mathrm{A}(\langle g, h\rangle)$ and $[g, \theta, h] = 1$, then θ is central in $\langle g, h\rangle$, i.e., for each $g_1 \in \langle g, h\rangle$ we have $g_1^{\theta} = g_1z$ for some $z \in \mathrm{Z}(\langle g, h\rangle)$.*

Proof. Set $G = \langle g, h\rangle$ and let $g_1, h_1 \in G$. Then

$$g_1 = a_1a_2\ldots a_n, \quad h_1 = b_1b_2\ldots b_m,$$

where each a_i and b_j is equal to g or h (noting that G is assumed to be finite). We claim that for each i, j we have $[a_i, \theta, b_j] = 1$. Indeed, $[g, \theta, g] = [g^{-1}g^{\theta}, g] = 1$ since $g^{-1}g^{\theta}$ is a power of g. Similarly, $[h, \theta, h] = 1$ and by our assumption $[g, \theta, h] = 1$. Finally, by Lemma 140.2, $[g, \theta, h][h, \theta, g] = 1$ and so also $[h, \theta, g] = 1$.

Using Lemma 140.3, we get

$$[g_1, \theta, h_1] = [a_1a_2\ldots a_n, \theta, b_1b_2\ldots b_m] = 1.$$

If we set $g_1^{-1}g_1^{\theta} = z$, then we get $[z, h_1] = 1$ and so $z \in \mathrm{Z}(\langle g, h\rangle)$. Hence θ is central in $\langle g, h\rangle$ and we are done. $\square$

Lemma 140.5. *Let G be a p-group which is either abelian or minimal nonabelian with $p > 2$ and $x, y \in G$ such that $o(x) \geq o(y)$. Then for some integer u we have*

$$\langle x\rangle \cap \langle x^u y\rangle = \{1\} \quad \textit{and} \quad o(x^u) = o(y).$$

Proof. If $\langle x\rangle \geq \langle y\rangle$, then there is an integer u with $x^u = y^{-1}$ so that $o(x^u) = o(y)$ and $x^u y = 1$ and we are done.

We may assume that $\langle x\rangle \not\geq \langle y\rangle$. Since $o(x) \geq o(y)$, we have

$$|\langle x\rangle/(\langle x\rangle \cap \langle y\rangle)| \geq |\langle y\rangle/(\langle x\rangle \cap \langle y\rangle)| = p^r$$

with $r \geq 1$. There exists an element $x^u = x' \in \langle x\rangle - \langle y\rangle$ of order $o(y)$ such that $(x')^{-p^r} = y^{p^r}$, where $|\langle x'\rangle/(\langle x\rangle \cap \langle y\rangle)| = p^r$. Since G is either abelian or minimal nonabelian with $p > 2$, we have for each $a, b \in G$ and $s \geq 1$,

$$(ab)^{p^s} = a^{p^s} b^{p^s} [b, a]^{\frac{1}{2}p^s(p^s-1)} = a^{p^s} b^{p^s}.$$

Hence $(x'y)^{p^r} = 1$ and so $o(x'y) \leq p^r$. If $(x'y)^{p^{r-1}} = 1$, then

$$(x')^{-p^{r-1}} = y^{p^{r-1}} \in \langle x\rangle \cap \langle y\rangle,$$

a contradiction. Hence $o(x'y) = p^r$ and the element $(x'y)^{p^{r-1}} = (x')^{p^{r-1}} y^{p^{r-1}}$ is of order p contained in $\langle x'y\rangle$. Suppose that $\langle x\rangle \cap \langle x'y\rangle \neq \{1\}$. Then

$$(x')^{p^{r-1}} y^{p^{r-1}} \in \langle x\rangle \quad \text{and so} \quad y^{p^{r-1}} \in \langle x\rangle \cap \langle y\rangle,$$

contrary to $|\langle y\rangle/(\langle x\rangle \cap \langle y\rangle)| = p^r$. Thus we have proved that $\langle x\rangle \cap \langle x^u y\rangle = \{1\}$ and $o(x^u) = o(y)$. □

Lemma 140.6. *For $a, b \in G$ and $\theta \in \mathrm{A}(G)$ we have $[ab, \theta] = [a, \theta]^b [b, \theta]$.*

Proof. We have

$$\begin{aligned}[a, \theta]^b [b, \theta] &= b^{-1} \cdot (a^{-1} a^\theta) \cdot b \cdot (b^{-1} b^\theta) \\ &= b^{-1} a^{-1} a^\theta b^\theta = (ab)^{-1} (ab)^\theta = [ab, \theta].\end{aligned}$$ □

Theorem 140.7. *Every power automorphism θ of a p-group G is central, i.e., for each $g \in G$ we have $g^\theta = gz$ for some $z \in \mathrm{Z}(G)$. In particular, θ fixes each element of G'.*

Proof. Let G be a p-group with a noncentral power automorphism θ. Then for some $g, h \in G$ we have $[g, \theta, h] \neq 1$. By Lemma 140.2, $d = [g, \theta, h] \in \langle g\rangle \cap \langle h\rangle \leq \mathrm{Z}(K)$, where $K = \langle g, h\rangle$. Since θ is noncentral in $K/\langle d^p\rangle$, we may assume $d^p = 1$.

We consider the subgroup $H = \langle [g, \theta], [h, \theta]\rangle$ of K. By Lemma 140.2,

$$[g, \theta, h][h, \theta, g] = 1$$

and so we may assume that $o([g,\theta]) \geq o([h,\theta])$. Now, $[h,\theta] = h^r$ for some integer r. Hence

$$[[g,\theta],[h,\theta]] = [[g,\theta],h^r] = d^r \in \langle d\rangle \leq \mathrm{Z}(H)$$

since $[g,\theta,h] = d \in \mathrm{Z}(K)$ and so $[g,\theta,h^r] = [g,\theta,h]^r$. This shows that H is either abelian or minimal nonabelian with $H' = \langle d\rangle$. In case $p = 2$, we can conclude that $[h,\theta] = h^{-1}h^\theta = h^{-1+i} = h^r$, where i is odd and so $r = -1 + i$ is even, which gives $d^r = 1$ and so in this case H is abelian.

We have proved that the subgroup $H = \langle [g,\theta],[h,\theta]\rangle$ is either abelian or minimal nonabelian with $p > 2$, where $H' = \langle d\rangle$ and $d = [g,\theta,h]$. As $o([g,\theta]) \geq o([h,\theta])$, we may use Lemma 140.5 for the group H. It follows that there is an integer u such that

$$(**) \qquad \langle [g,\theta]\rangle \cap \langle [g,\theta]^u[h,\theta]\rangle = \{1\} \quad \text{and} \quad o([g,\theta]^u) = o([h,\theta]).$$

Now, d and $[g,\theta]$ are both contained in $\langle g\rangle$ and so one is a power of the other. However, d commutes with h while $[g,\theta]$ does not. Hence d is a power of $[g,\theta]$, say $d = [g,\theta]^t$. Then setting $v = u(1-t)$, we get using Lemma 140.6

$$[g^v h,\theta] = [g^{-ut}g^u h,\theta] = [g^{-ut},\theta]^{g^u h}[g^u h,\theta]$$

(since $[g^{-ut},\theta]$ is a power of g)

$$= [g^{-ut},\theta]^h[g^u h,\theta]$$

(and since

$$[g^{-ut},\theta]^h = (g^{ut}(g^\theta)^{-ut})^h = (((g^{-1}g^\theta)^t)^{-u})^h = (([g,\theta]^t)^{-u})^h = (d^{-u})^h = d^{-u}$$

because $d \in \mathrm{Z}(K)$)

$$= d^{-u}[g^u h,\theta] = d^{-u}[g^u,\theta]^h[h,\theta] = d^{-u}[g^u,\theta][g^u,\theta,h][h,\theta]$$

(since

$$[g^u,\theta] = g^{-u}(g^\theta)^u = (g^{-1}g^\theta)^u = [g,\theta]^u$$

and

$$\begin{aligned}[g^u,\theta,h] &= [[g^u,\theta],h] = [[g,\theta]^u,h] = [g,\theta]^{-u}(h^{-1}[g,\theta]h)^u \\ &= [g,\theta]^{-u}([g,\theta]^h)^u = ([g,\theta]^{-1}[g,\theta]^h)^u = [g,\theta,h]^u = d^u\end{aligned}$$

because $[g,\theta]$ commutes with $d = [g,\theta]^{-1}[g,\theta]^h \in \langle g\rangle$ and so $[g,\theta]$ also commutes with $[g,\theta]^h$)

$$= d^{-u}[g,\theta]^u d^u[h,\theta] = [g,\theta]^u[h,\theta].$$

We have proved that

$$[g^v h, \theta] = [g, \theta]^u [h, \theta].$$

By $(**)$, we get $\langle [g, \theta] \rangle \cap \langle [g^v h, \theta] \rangle = \{1\}$. Since $d = [g, \theta]^t$ is of order p, we have $1 \neq [g, \theta] \in \langle g \rangle$. On the other hand, $[g^v h, \theta]$ is a power of $g^v h$. Hence we have either $[g^v h, \theta] = 1$ or $\langle g \rangle \cap \langle g^v h \rangle = \{1\}$. By Lemma 140.2,

$$[g^v h, \theta, g] = [[g^v h, \theta], g] \leq \langle g^v h \rangle \cap \langle g \rangle.$$

Thus, in any case, $[g^v h, \theta, g] = 1$. We get $\langle g^v h, g \rangle = \langle g, h \rangle$ and so, by Lemma 140.4, θ is central in $\langle g, h \rangle$. But this implies that $[g, \theta, h] = 1$, a contradiction. Our theorem is proved. □

The norm $\mathcal{N}(G)$ of a group G is the intersection of the normalizers of all subgroups of G.

Corollary 140.8. *The norm $\mathcal{N}(G)$ of a p-group G is contained in the second center $\mathrm{Z}_2(G)$ of G.*

Proof. Let $a \in \mathcal{N}(G)$. Then a induces in G an inner power automorphism. By Theorem 140.7, for all $g \in G$ we have $g^a = gz$ with some $z \in \mathrm{Z}(G)$. This implies that $a \in \mathrm{Z}_2(G)$ and we are done. □

Exercise 1. If $M \cong \mathrm{M}_{p^n}$, then $\mathcal{N}(G)$ is a noncyclic maximal subgroup of G.

Exercise 2. If G is a nonabelian metacyclic group of order p^4 and exponent p^2, then $\mathcal{N}(G) = \mathrm{Z}(G)$.

Exercise 3. If $G \ncong \mathrm{Q}_8$ is a 2-group of maximal class, then we have $\mathcal{N}(G) = \mathrm{Z}(G)$ unless $G \cong \mathrm{Q}_{2^n}$, $n > 3$ (then $\mathcal{N}(G) = \mathrm{Z}_2(G)$.

Exercise 4. Find $\mathcal{N}(G)$, where

(a) G is minimal nonabelian p-group.

(b) G is extraspecial.

(c) G is special.

(d) G is metacyclic.

(e) $|\Phi(G)| = p$.

(f) $|G'| = p$.

(g) G is a p-group of maximal class, $p > 2$.

(h) G is a Sylow p-subgroup of the holomorph of a cyclic p-group.

(i) G is an $\mathcal{A}_2$-group.

(j) G is minimal nonmetacyclic 2-group.

Exercise 5. Find $\mathcal{N}(A \times B)$ is terms of A and B.

§141

Nonabelian p-groups having exactly one maximal subgroup with a noncyclic center

Theorem 141.1 solves a problem posed by the first author. Note that if G is a nonabelian p-group all of whose maximal subgroups have a cyclic center, then $p = 2$ and G is a 2-group of maximal class.

Theorem 141.1. *A nonabelian p-group G has exactly one maximal subgroup with a noncyclic center if and only if $\mathrm{Z}(G)$ is cyclic and G has exactly one normal abelian subgroup of type (p, p).*

Proof. Suppose that G is a nonabelian p-group with exactly one maximal subgroup M such that $\mathrm{Z}(M)$ is noncyclic. If $\mathrm{Z}(G)$ is noncyclic, then $G/\mathrm{Z}(G)$ is cyclic since M is the only maximal subgroup of G containing $\mathrm{Z}(G)$. But then G is abelian, a contradiction. Hence $\mathrm{Z}(G)$ must be cyclic. Suppose that G has no normal abelian subgroup of type (p, p). Then $p = 2$ and G is of maximal class (Lemma 1.4). But in that case, either each maximal subgroup of G has a cyclic center or $G \cong \mathrm{D}_8$. In the last case, G has two distinct maximal subgroups with a noncyclic center, a contradiction. Thus we have proved that G has a normal abelian subgroup U of type (p, p). As $|G : \mathrm{C}_G(U)| = p$ (because $\mathrm{Z}(G)$ is cyclic), we get $\mathrm{C}_G(U) = M$. Also, $\Omega_1(\mathrm{Z}(G)) = \langle z\rangle < U$.

Assume that G possesses another normal abelian subgroup V distinct from U of type (p, p). Since $\mathrm{C}_G(V)$ is a maximal subgroup of G with a noncyclic center (recall that $\mathrm{Z}(G)$ is cyclic), we have $\mathrm{C}_G(V) = M$. In particular, we get $V \le M$, $U \cap V = \langle z\rangle$ and $UV \cong \mathrm{E}_{p^3}$ with $UV \le \mathrm{Z}(M)$. Take $x \in G - M$. We may choose $u \in U - \langle z\rangle$ and $v \in V - \langle z\rangle$ so that $u^x = uz$ and $v^x = vz^{-1}$. Indeed, if $u^x = uz^i$ and $v^x = vz^j$, where i, j are some integers with $i \not\equiv 0 \pmod p$ and $j \not\equiv 0 \pmod p$, we find integers i', j' so that $ii' \equiv 1 \pmod p$ and $jj' \equiv -1 \pmod p$. Then, replacing u with $u' = u^{i'}$ and v with $v' = v^{j'}$, we get (noting that $i' \not\equiv 0 \pmod p$, $j' \not\equiv 0 \pmod p$)

$$(u')^x = (u^{i'})^x = (u^x)^{i'} = (uz^i)^{i'} = u^{i'}z^{ii'} = u^{i'}z = u'z,$$

and

$$(v')^x = (v^{j'})^x = (v^x)^{j'} = (vz^j)^{j'} = v^{j'}z^{jj'} = v^{j'}z^{-1} = v'z^{-1}.$$

Thus, writing again u instead of u' and v instead of v', we can assume from the start that $u^x = uz$ and $v^x = vz^{-1}$. It follows that

$$(uv)^x = u^x v^x = uz \cdot vz^{-1} = uv.$$

But then $\langle z, uv\rangle \cong \mathrm{E}_{p^2}$ and $\langle z, uv\rangle \leq \mathrm{Z}(G)$, which contradicts the fact that $\mathrm{Z}(G)$ is cyclic. We have proved that U is the unique normal elementary abelian subgroup of order p^2 in G.

Suppose that G is a nonabelian p-group with a cyclic center $\mathrm{Z}(G)$ which possesses a unique normal abelian subgroup U of type (p, p). Since $\mathrm{Z}(G)$ is cyclic, we conclude that $|G : \mathrm{C}_G(U)| = p$ and so $M = \mathrm{C}_G(U)$ is a maximal subgroup of G with a noncyclic center.

Let N be any maximal subgroup of G with a noncyclic center $\mathrm{Z}(N)$. Since $\mathrm{Z}(N)$ is normal in G, it follows that $\Omega_1(\mathrm{Z}(N))$ contains an abelian subgroup V of type (p, p) which is normal in G. Because $\mathrm{Z}(G)$ is cyclic, we have $\mathrm{C}_G(V) = N$. By our assumption, $V = U$ and so $\mathrm{C}_G(U) = M = \mathrm{C}_G(V) = N$, and we are done. □

Theorem 141.2. *Let G be a nonabelian p-group all of whose nonabelian maximal subgroups have a cyclic center. Then one of the following holds:*

(a) *G is minimal nonabelian.*

(b) *G is a 2-group of maximal class.*

(c) *$G = L\mathrm{Z}(G)$, where $L \cong \mathrm{D}_8, \mathrm{Q}_8$ or M_{p^n}, $n \geq 3$ (if $p = 2$, then $n \geq 4$), and either $\mathrm{Z}(G)$ is cyclic with $\mathrm{Z}(G) > \mathrm{Z}(L)$ or $G = L \times \langle t\rangle$, where t is an element of order p.*

(d) *G has exactly one abelian maximal subgroup A of rank ≥ 2, $\mathrm{Z}(G)$ is cyclic, and G possesses exactly one normal abelian subgroup of type (p, p) (contained in A).*

Proof. We may assume that G is not minimal nonabelian. First assume that G contains more than one abelian maximal subgroup. Then we get $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ and $|G'| = p$. All $p + 1$ maximal subgroups of G containing $\mathrm{Z}(G)$ are abelian and therefore each maximal subgroup M of the group G which does not contain $\mathrm{Z}(G)$ is nonabelian. Set $Z_1 = M \cap \mathrm{Z}(G) = \mathrm{Z}(M)$ so that (by our assumption) Z_1 is cyclic and so $\mathrm{Z}(G)$ is of rank ≤ 2. Now let L be a minimal nonabelian subgroup of M so that $M = LZ_1$, $G = L\mathrm{Z}(G)$ and $L \cap Z_1 = \mathrm{Z}(L) \leq \Phi(G)$. It follows that L has a cyclic subgroup of index p and so $L \cong \mathrm{D}_8, \mathrm{Q}_8$ or M_{p^n}, $n \geq 3$ (if $p = 2$, then $n \geq 4$). Suppose that $\mathrm{Z}(G)$ is not cyclic. Let t be an element of order p in $\mathrm{Z}(G) - Z_1$. If $L\langle t\rangle < G$, then a maximal subgroup of G containing $L\langle t\rangle$ has a noncyclic center, a contradiction. Hence in this case $G = L \times \langle t\rangle$. Assume that $\mathrm{Z}(G)$ is cyclic. Then $Z_1 = \Phi(\mathrm{Z}(G)) = \Phi(G)$ and so each maximal subgroup M_1 of G which does not contain $\mathrm{Z}(G)$ contains $Z_1 = \Phi(G)$ and $\mathrm{Z}(M_1) = Z_1$ is cyclic.

Now assume that G has exactly one abelian maximal subgroup A. If A is cyclic, then all maximal subgroups of G have cyclic center and then $p = 2$ and G is a 2-group of maximal class. We may assume that A is of rank ≥ 2 and so, by Theorem 141.1, $\mathrm{Z}(G)$ is cyclic and G has exactly one normal abelian subgroup of type (p, p) (contained in $\Omega_1(A)$).

Finally, assume that all maximal subgroups of G are nonabelian. Then all maximal subgroups of G have cyclic center. But then $p = 2$ and G is a 2-group of maximal class and such groups have a cyclic subgroup of index 2, a contradiction. □

§142

Nonabelian p-groups all of whose nonabelian maximal subgroups are either metacyclic or minimal nonabelian

We solve here Problem 1535(i) and prove the following result.

Theorem 142.1. *Let G be a nonabelian p-group all of whose nonabelian maximal subgroups are either metacyclic or minimal nonabelian. Then one of the following holds:*

(a) *G is minimal nonabelian (= $\mathcal{A}_1$-group).*

(b) *G is an $\mathcal{A}_2$-group, i.e., G is not minimal nonabelian but all nonabelian maximal subgroups of G are minimal nonabelian (and such groups are completely determined in §71).*

(c) *G is metacyclic.*

Proof. Let G be a title group. If all maximal subgroups of G are abelian, then G is minimal nonabelian and we have obtained case (a) of our theorem.

We may assume that G has nonabelian maximal subgroups and they are all either metacyclic or minimal nonabelian. It follows that $\mathrm{d}(G) \leq 3$.

First assume that G has more than one abelian maximal subgroup. Then G contains exactly $p + 1$ abelian maximal subgroups, $\mathrm{d}(G) = 3$ and $|G'| = p$. Let H be any nonabelian maximal subgroup of G. Then $|H'| = p$ and H is either minimal nonabelian or H is metacyclic. But in the second case we have $\mathrm{d}(H) = 2$ which together with $|H'| = p$ implies that H is also minimal nonabelian. Hence in this case all nonabelian maximal subgroups of G are minimal nonabelian and so G is an $\mathcal{A}_2$-group from case (b) of our theorem.

From now on we may assume that G has at most one abelian maximal subgroup. If, in addition, all nonabelian maximal subgroups of G are minimal nonabelian, then again G is an $\mathcal{A}_2$-group from part (b) of our theorem.

Now suppose that all nonabelian maximal subgroups of G are metacyclic. We may also assume that G is nonmetacyclic (because of the possibility (c) of our theorem). If G is minimal nonmetacyclic, then, by the results of §66 and §69, G is either the minimal nonmetacyclic 2-group of order 2^5 or G is a 3-group of order 3^4 and maximal class. But these both groups are also $\mathcal{A}_2$-groups and so they are included in part (b) of our theorem. Assume now that G has exactly one nonmetacyclic maximal subgroup M

in which case M is the unique abelian maximal subgroup of G. If $p = 2$, then such groups are completely determined in §87. Considering all results of that section (Theorems 87.8, 87.10, 87.12, 87.14 to 87.17, and 87.19 to 87.21), we see in the case where G is not minimal nonabelian that the unique nonmetacyclic maximal subgroup of G is always nonabelian, a contradiction. Now suppose that $p > 2$. Then these groups are determined by Y. Berkovich in Proposition A.40.12. It follows that assuming $|G| > p^4$ (noting that in case $|G| \leq p^4$, G is an $\mathcal{A}_2$-group), G is an L_3-group, i.e., $\Omega_1(G) = E$ is of order p^3 and exponent p and G/E is cyclic of order $> p$. Let M be the unique maximal subgroup of G containing E. Since M is nonmetacyclic, M is abelian and $M = C_G(E)$. Let $a \in G - M$ so that $G = \langle E, a\rangle$ and $E \cap \langle a\rangle \neq \{1\}$. If $C_G(a) > \langle a\rangle$, then $|C_G(a) : \langle a\rangle| = p$ and $C_G(a)$ is another abelian maximal subgroup of G (distinct from M), a contradiction. Hence we get $C_G(a) = \langle a\rangle$. Let X be any maximal subgroup of G distinct from M. Then X covers G/E and $X \cap E \cong E_{p^2}$. Let $a' \in X$ be such that $X = \langle X \cap E, a'\rangle$ and $\langle a'\rangle \cap (X \cap E) \neq \{1\}$. Since $\langle a'\rangle$ is a cyclic subgroup of index p in X and X is nonabelian, we get $X \cong M_{p^n}$, $n \geq 4$, and so X is minimal nonabelian. Hence G is again an $\mathcal{A}_2$-group from part (b) of our theorem.

We have reduced our problem to a classification of the title groups with the following properties:

(i) G has at most one abelian maximal subgroup.

(ii) G has a nonabelian maximal subgroup H which is minimal nonabelian but not metacyclic.

(iii) G has a nonabelian maximal subgroup K which is metacyclic but not minimal nonabelian. In particular, K' is cyclic of order $\geq p^2$.

We have $E = \Omega_1(H) \cong E_{p^3}$. If $E \leq \Phi(H)$, then $E \leq \Phi(G)$ and then each maximal subgroup of G would be nonmetacyclic, which contradicts our assumption (iii). Hence $E = \Omega_1(H) \not\leq \Phi(H)$ and we may set

$$H = \langle a, b \mid a^{p^n} = b^p = 1,\ n \geq 2,\ [a, b] = z,\ z^p = [z, a] = [z, b] = 1\rangle,$$

where $E = \langle a^{p^{n-1}}, z, b\rangle$, $\Phi(H) = Z(H) = \langle a^p, z\rangle$ and $H' = \langle z\rangle$ is a maximal cyclic subgroup of H. In particular, H/E is cyclic of order p^{n-1}.

If G/E is abelian, then $G' \leq E$ and so G' is elementary abelian. But this contradicts our assumption (iii), where K' is cyclic of order $\geq p^2$. It follows that G/E is nonabelian with a cyclic subgroup of index p. In particular, we have $n \geq 3$ and so H/E is cyclic of order $\geq p^2$. All $p + 1$ maximal subgroups of G containing E are nonmetacyclic and so (by our assumption (iii)) $d(G) = 3$ which forces $\Phi(H) = \Phi(G)$ since $|G : \Phi(H)| = p^3$.

Suppose that G possesses an abelian maximal subgroup A. By a result of A. Mann, we have $|G' : (A'H')| \leq p$ and so $|G' : H'| \leq p$ which implies that $|G'| \leq p^2$ and so $G' = K' \cong C_{p^2}$. On the other hand, $G' \leq \Phi(G) = \Phi(H)$ and $G' > H'$, which contradicts the fact that $H' = \langle z\rangle$ is a maximal cyclic subgroup in H.

Thus we have proved that all maximal subgroups of G are nonabelian. In particular, all $p + 1$ maximal subgroups of G containing E are nonabelian and nonmetacyclic and so they all must be nonmetacyclic minimal nonabelian. Let $H_1 \neq H$ be another nonmetacyclic minimal nonabelian maximal subgroup of the group G containing E. Since $H_1 > \Phi(G) = \Phi(H)$ and $|H_1 : \Phi(H_1)| = p^2$ with $\Phi(H_1) \leq \Phi(G)$, we have

$$\Phi(H_1) = \Phi(H) = \Phi(G) = \mathrm{Z}(H) = \mathrm{Z}(H_1).$$

This implies that $\Phi(G) \leq \mathrm{Z}(G)$ and so G is of class 2.

For any $x, y \in G$ we have $[x, y]^p = [x^p, y] = 1$ and so G' is elementary abelian. But this contradicts our assumption (iii), where K' is cyclic of order $\geq p^2$. This is a final contradiction and our theorem is proved. □

§143

Alternate proof of the Reinhold Baer theorem on 2-groups with nonabelian norm

Recall that the norm $\mathcal{N}(G)$ of a group G is the intersection of the normalizers of all subgroups of G. Clearly, the subgroup $\mathcal{N}(G)$ is characteristic in G and Dedekindian, i.e., $\mathcal{N}(G) = Q \times E \times A$, where $Q \in \{\{1\}, \mathrm{Q}_8\}$, $\exp(E) \leq 2$ and A is abelian of odd order.

In this section we offer another proof of the following remarkable result due to Reinhold Baer.

Theorem 143.1. *If the norm $\mathcal{N}(G)$ of a 2-group G is nonabelian, then $\mathcal{N}(G) = G$.*

Proof (Berkovich). Assume, by way of contradiction, that $\mathcal{N}(G) < G$.

By Theorem 1.20, there is in $\mathcal{N}(G)$ a subgroup $Q \cong \mathrm{Q}_8$. We have, by assumption, $Q < G$ so that $|G| \geq 16$. Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be distinct cyclic subgroups of Q of order 4.

(i) If $Q \leq H \leq G$, then $Q \leq \mathcal{N}(H)$. This is obvious.

(ii) If $Q < H \leq G$ and $|H : Q| = 2$, then $H = Q \times C$ is Dedekindian. Assume that this is false. Then H has a nonnormal cyclic subgroup L of order ≤ 4 such that $L \not\leq Q$. As $QL = H$, it follows that Q does not normalize L, contrary to the hypothesis. This H is Dedekindian, and our claim follows.

(iii) $\mathrm{C}_G(Q)$ has no cyclic subgroup of order 4. Assume, however, that the subgroup $L = \langle x \rangle \leq \mathrm{C}_G(Q)$ is cyclic of order 4. Set $H = Q * L$; then we get $16 \leq |H| \leq 32$. If $|H| = 16$, our claim follows from (ii). Now let $|H| = 32$; then $H = Q \times L$ and $\langle ax \rangle$ is not b-invariant, a contradiction.

(iv) By (ii), $|G : Q| > 2$.

(v) It follows from hypothesis and (iii) that if $D = \langle d \rangle < G$ is cyclic of order 4, then $Q \cap D > \{1\}$. Indeed, assume that $Q \cap D = \{1\}$. Then, by (iii), Q is not normal in $F = QD$ so $F/Q_F \cong \mathrm{D}_8$. But the norm of D_8 coincides with its center, and this is a contradiction.

(vi) We claim that $\exp(G) = 4$. Assume that $T < G$ is cyclic of order 8. Since Q normalizes T, we get $H = QT \leq G$. Bringing to mind our aim, one may assume that $G = QT$. By (v), one has $Q \cap T > \{1\}$ so that $16 \leq |G| \leq 32$. From (iv) we deduce $|G| > 16$. Let $|G| = 32$. Write $H_1 = AT$ and $H_2 = BT$. Since, by (i), $A \leq \mathcal{N}(H_1)$,

it follows that H_1 is not of maximal class in view of $A \not\leq \Phi(H_1)$. Similarly, H_2 is not of maximal class. Then, by Theorem 1.2, $\mho_1(T) = \Phi(H_i) \leq \mathrm{Z}(H_i)$, $i = 1, 2$. Thus $\mho_1(T)$, a cyclic subgroup of order 4, centralizes $\langle A, B\rangle = Q$, contrary to (iii).

Now we are ready to complete the proof of our theorem.

By (v) and (vi), $\mho_1(G) = \mho_1(Q)$ so $G/\mho_1(G)$, being of exponent 2, is abelian, and we conclude that $G' = \mho_1(G)$ has order 2 since G is nonabelian. Then $G/\mathrm{C}_G(Q)$ is isomorphic to a subgroup of $\mathrm{D}_8 \in \mathrm{Syl}_2(\mathrm{Aut}(Q))$, and $G/\mathrm{C}_G(Q)$ contains a four-subgroup isomorphic to $Q/\mathrm{Z}(Q)$. As $\mho_1(Q) \leq \mathrm{C}_G(Q)$, we get

$$G/\mathrm{C}_G(Q) \cong Q/\mathrm{Z}(Q)$$

since $Q \cap \mathrm{C}_G(Q) = \mathrm{Z}(Q)$, and we infer that $G = Q\mathrm{C}_G(Q)$. Since $\exp(\mathrm{C}_G(Q)) = 2$ by (iii), we deduce that $\mathrm{C}_G(Q) = \mathrm{Z}(Q) \times E$, where $E < \mathrm{C}_G(Q)$. In that case, we obtain

$$G = Q\mathrm{C}_G(Q) = Q(\mathrm{Z}(Q) \times E) = QE,$$

where $Q \cap E = \{1\}$. Thus $G = Q \times E$ so G is Dedekindian as $\exp(E) = 2$. □

Remark. In the proof of Theorem 143.3 we do not use the finiteness of G. Thus that theorem is also true for infinite 2-groups.

The following theorem is a partial case of Schenkman's result (see Corollary 140.8).

Theorem 143.2. *Suppose that G is an arbitrary finite group with nonabelian $\mathcal{N}(G)$. Then $P \in \mathrm{Syl}_2(\mathcal{N}(G))$ centralizes all elements of G of odd order and $P \leq \mathrm{Z}_2(G)$.*

Proof. Let $\mathrm{Q}_8 \cong Q \leq \mathcal{N}(G)$, let $a \in Q^{\#}$ and let $x \in G$ be of order p^k, where $p > 2$ is a prime. Set $H = \langle a, x\rangle$. Let $y \in \langle x\rangle$ be of order p and $F = \langle a, y\rangle$. Assume that F is nonabelian. In case $o(a) = 2$, we see that F is a nonabelian group of order $2p$ so its norm equals $\{1\}$, a contradiction since $a \in \mathcal{N}(G)$. If $o(a) = 4$, then F is minimal nonabelian with norm of order 2, a contradiction again. Thus F is abelian. Hence Q centralizes all subgroups of G of odd order. As, by Theorem 10.28, $P \in \mathrm{Syl}_2(\mathcal{N}(G))$ is generated by its minimal nonabelian subgroups all of which are isomorphic to Q_8, it follows that P centralizes all subgroups of G of odd order.

Now let $P \leq P_1 \in \mathrm{Syl}_2(G)$. By Theorem 143.1, the subgroup P_1 is Dedekindian. Therefore $\mathrm{Z}(P) \leq \mathrm{Z}(P_1)$ (Theorem 1.20). Since, by the above, $\mathrm{Z}(P)$ centralizes all elements of G of odd order, we conclude that $\mathrm{Z}(P) \leq \mathrm{Z}(G)$. As $P/\mathrm{Z}(P) \leq P_1/\mathrm{Z}(P)$, $P_1/\mathrm{Z}(P)$ is abelian and $P/\mathrm{Z}(P)$ centralizes all elements of $G/\mathrm{Z}(P)$ of odd order, we get $P/\mathrm{Z}(P) \leq \mathrm{Z}(G/\mathrm{Z}(P))$ so that $P \leq \mathrm{Z}_2(G)$, proving the last assertion. □

Exercise 1. Let $\mathcal{N}_1(G)$ be the intersection of the normalizers of all cyclic subgroups of a 2-group G of order ≤ 8. If $\mathcal{N}_1(G)$ contains a subgroup isomorphic to Q_8, then we have $G = \mathcal{N}_1(G)$. (*Hint.* See the proof of Theorem 143.1.)

Exercise 2. Let $G \not\cong \mathrm{SD}_{16}$ be a 2-group, $D < G$ and $D \cong \mathrm{D}_8$. Then there exists in G a subgroup L of order 2 such that $L \not\leq D$ and $D \not\leq \mathrm{N}_G(L)$.

Exercise 3. Let M be a proper nonabelian subgroup of order p^3 of a p-group G, $p > 2$. Then, if $\Omega_1(G) > \Omega_1(M)$, there is a subgroup $L < G$ of order p such that $L \not\leq M$ and $M \not\leq \mathrm{N}_G(L)$.

Schenkman [Sc] has proved that $\mathcal{N}(G) \leq \mathrm{Z}_2(G)$ and $[G', \mathcal{N}(G)] = \{1\}$ for arbitrary groups G (finite and infinite).

§144

p-groups with small normal closures of all cyclic subgroups

A p-group G is called a $\mathrm{BI}(p^k)$-*group* ($G \in \mathrm{BI}(p^k)$ for short) with a fixed integer $k \geq 0$ if $|\langle x\rangle^G : \langle x\rangle| \leq p^k$ for all $x \in G$. Obviously, each p-group is a $\mathrm{BI}(p^k)$-group for some integer k and so we can only investigate such groups for some small k. Using to some extent the results of Heng Lv, Wei Zhou and Dapeng Yu [LZY], we shall establish here some remarkable properties of $\mathrm{BI}(p^2)$-groups for $p > 2$ (Theorems 144.6, 144.7 and 144.9). The corresponding problem for $p = 2$ is completely open. Look at similar problems stated in Problem 148.

Lemma 144.1. *Let $G \in \mathrm{BI}(p^k)$. Then $|G : \mathrm{N}_G(\langle a\rangle)| \leq p^k$ for all $a \in G$.*

Proof. Let $o(a) = p^n$, $n \geq 1$. Since G is a $\mathrm{BI}(p^k)$-group, we have $|\langle a\rangle^G| \leq p^{n+k}$. Hence there are at most

$$(p^{n+k} - p^{n-1})/(p^n - p^{n-1}) = (p^{k+1} - 1)/(p - 1) < p^{k+1}$$

cyclic subgroups of order p^n in $\langle a\rangle^G$. This gives $|G : \mathrm{N}_G(\langle a\rangle)| \leq p^k$. □

Lemma 144.2. *Suppose that $G = \langle a, b\rangle$ is a nonabelian p-group. If $|\langle a\rangle^G : \langle a\rangle| \leq p$ and $|\langle b\rangle^G : \langle b\rangle| \leq p$ with $\langle a\rangle \cap \langle b\rangle = \{1\}$, then G' is of order p.*

Proof. If one of $\langle a\rangle$ or $\langle b\rangle$, say $\langle a\rangle$, is normal in G, then G is a semidirect product of $\langle a\rangle$ and $\langle b\rangle$. In that case, we see that $\langle b\rangle$ is not normal in G and so $|\langle b\rangle^G : \langle b\rangle| = p$ and $|\langle a\rangle \cap \langle b\rangle^G| = p$. But $G' \leq \langle a\rangle \cap \langle b\rangle^G$ and so $|G'| = p$.

Hence we may assume that

$$|\langle a\rangle^G : \langle a\rangle| = |\langle b\rangle^G : \langle b\rangle| = p.$$

Set $A = \langle a\rangle^G$ and $B = \langle b\rangle^G$ which yields $|A : \langle a\rangle| = p$, $G/A \neq \{1\}$ and $A\langle b\rangle = G$. Similarly, $|B : \langle b\rangle| = p$, $G/B \neq \{1\}$ and $B\langle a\rangle = G$. Hence we obtain $G' \leq A \cap B$. If $\langle b\rangle \cap A = \{1\}$ or $\langle a\rangle \cap B = \{1\}$, then $|A \cap B| = p$ and so $|G'| = p$ and we are done.

It follows that we may assume $\langle b\rangle \cap A \neq \{1\}$ and $\langle a\rangle \cap B \neq \{1\}$. As $\langle a\rangle \cap \langle b\rangle = \{1\}$, we see that $\langle b\rangle \cap A = \langle b_1\rangle$ is of order p and $A = \langle a\rangle\langle b_1\rangle$ and similarly, $\langle a\rangle \cap B = \langle a_1\rangle$ is of order p and so $A \cap B = \langle a_1\rangle \times \langle b_1\rangle \cong \mathrm{E}_{p^2}$. In particular, $o(a) \geq p^2$, $o(b) \geq p^2$,

and $G = \langle a\rangle\langle b\rangle$ is a product of the two cyclic subgroups $\langle a\rangle$ and $\langle b\rangle$ with

$$G' \le \langle a_1\rangle \times \langle b_1\rangle.$$

For any $x \in G$, $\langle a\rangle^x \cap \langle a\rangle \ne \{1\}$ and so $\langle a\rangle_G \ge \langle a_1\rangle$ which implies $\langle a_1\rangle \trianglelefteq G$ and so $a_1 \in \mathrm{Z}(G)$. Similarly, $b_1 \in \mathrm{Z}(G)$ and so $G' \le \langle a_1\rangle \times \langle b_1\rangle \le \mathrm{Z}(G)$. In this case, $\langle [a,b]\rangle = G'$ is of order p and we are done. □

Lemma 144.3. *If* $|G| = p^{m+2}$ *and* $\exp(G) = p^m$ *with* $m \ge 3$ *and* $p > 2$*, then we have* $|G'| \le p^2$.

Proof. By Theorem 74.1, G is either metacyclic or an L_3-group. In the second case, $G' < \Omega_1(G)$ and so $|G'| \le p^2$. Let G be metacyclic, and let R be a normal elementary abelian subgroup of order p^2 in G and $a \in G$ of order p^m. Since $a^{p^{m-1}}$ centralizes R and G is metacyclic, we have $|\langle a\rangle \cap R| = p$ and so $(R\langle a\rangle)/R$ is a cyclic subgroup of index p in G/R and G/R is noncyclic. Therefore there exists $b \in G - (R\langle a\rangle)$ with $b^p \in R$ so that $o(b) \le p^2$. Also, $G/(R\langle a^p\rangle)$ is elementary abelian of order p^2 which gives $R\langle a^p\rangle = \Phi(G)$ and so $G = \langle a, b\rangle$.

Since metacyclic p-groups for $p > 2$ are regular, we obtain that $\exp(\langle b\rangle^G) \le p^2$. Then $G' \le \langle b\rangle^G$ gives $\exp(G') \le p^2$. On the other hand, G' is cyclic and so $|G'| \le p^2$ and we are done. □

Lemma 144.4. *Let* $G = \langle x, y\rangle \in \mathrm{BI}(p^2)$*,* $p > 2$*. If* $\langle x\rangle \cap \langle y\rangle = \{1\}$*, then the following hold:*

(i) $\mathrm{cl}(G) \le 4$. *In particular,* $\mathrm{cl}(G) \le 3$ *if* $o(x) \ge o(y) \ge p^3$.

(ii) $|G'| \le p^3$ *and* $\exp(G') \le p^2$.

(iii) $\mho_2(G) \le \mathrm{Z}(G)$.

Proof. We may assume that G is nonabelian. Let $o(x) = p^m$, $o(y) = p^n$. Since G is a $\mathrm{BI}(p^2)$-group, we have $|\langle x\rangle^G : \langle x\rangle| \le p^2$. Then from

$$|\langle x\rangle||\langle x^y\rangle|/|\langle x\rangle \cap \langle x^y\rangle| = |\langle x\rangle\langle x^y\rangle| \le |\langle x\rangle^G| \le p^{m+2}$$

we get $|\langle x\rangle \cap \langle x^y\rangle| \ge p^{m-2}$ and $x^{p^2} \in \langle x\rangle \cap \langle x^y\rangle$. Hence

$$\langle x^{p^2}\rangle = \langle (x^y)^{p^2}\rangle = \langle (x^{p^2})^y\rangle.$$

Let $M = \langle x^{p^2}, y\rangle$. Then $\langle x^{p^2}\rangle \trianglelefteq M$. By Lemma 144.1, we have $x^{p^2} \in \mathrm{N}_G(\langle y\rangle)$ and so $\langle y\rangle \trianglelefteq M$. But $\langle x\rangle \cap \langle y\rangle = \{1\}$ and so $[x^{p^2}, y] = 1$ and $x^{p^2} \in \mathrm{Z}(G)$. Similarly, we get $y^{p^2} \in \mathrm{Z}(G)$.

Set $H = \langle x\rangle^G$ and $K = \langle y\rangle^G$ so that $G' \le H \cap K$. If $|H \cap K| \le p^3$, then we obtain $\mathrm{cl}(G) \le 4$. Hence if $o(y) \le p^2$, then $|K| \le p^4$ and thus $H \cap K < K$ which yields that $\mathrm{cl}(G) \le 4$. In this case, we also conclude that $\exp(G') \le p^2$. Indeed, assume that $H \cap K = G'$ is cyclic of order p^3. Then the group G is regular and $K = \langle y\rangle^G$ is of

exponent $\leq p^2$, a contradiction. We have a similar situation if $o(x) \leq p^2$. So we need only consider the case where $o(x), o(y) \geq p^3$. Without loss of generality we may assume that $m \geq n \geq 3$. We shall prove that under this condition $\mathrm{cl}(G) \leq 3$ which will complete the proof of (1). Since G is a $\mathrm{BI}(p^2)$-group and $\langle x\rangle \cap \langle y\rangle = \{1\}$, we see that $|H \cap K| \leq p^4$. If $|H \cap K| = p^3$, then

$$x^{p^{m-1}} \in H \cap K, \quad y^{p^{n-1}} \in H \cap K$$

and, by the above, $x^{p^{m-1}}, y^{p^{n-1}} \in \mathrm{Z}(G)$. This implies that $H \cap K \in \mathrm{Z}_2(G)$ and then $\mathrm{cl}(G) \leq 3$ and $\exp(G') \leq p^2$. So we need to consider the case

$$|H \cap K| = p^4 \quad \text{where } x^{p^{m-2}}, y^{p^{n-2}} \in H \cap K$$

and so $H \cap K = \langle x^{p^{m-2}}\rangle\langle y^{p^{n-2}}\rangle$. Set $A = \langle x^{p^{m-1}}, y^{p^{n-1}}\rangle$ and so, by the above, we get $A \leq \mathrm{Z}(G)$ since $m, n \geq 3$. Now consider $\bar{G} = G/A$ and we use the "bar convention". Then $\bar{G} = \langle \bar{x}, \bar{y}\rangle$ and we obtain

$$|\langle \bar{x}\rangle^{\bar{G}} : \langle \bar{x}\rangle| = |\langle \bar{y}\rangle^{\bar{G}} : \langle \bar{y}\rangle| = p.$$

By Lemma 144.2, $|\bar{G}'| \leq p$ and so $|G'| \leq p^3$. If $|G'| \leq p^2$, then $\mathrm{cl}(G) \leq 3$. In case $|G'| = p^3$, we have $A \leq G'$. Since $A \leq \mathrm{Z}(G)$, we conclude that $[G, G'] \leq A \leq \mathrm{Z}(G)$ and so $\mathrm{cl}(G) \leq 3$. Obviously, in any of the above cases, $|G'| \leq p^3$ and $\exp(G') \leq p^2$. We have proved (1) and (2).

Let $g_1 = x^i y^j \in G$. By the Hall–Petrescu formula (see Appendix 1),

$$(x^i y^j)^{p^2} = (x^i)^{p^2}(y^j)^{p^2} a_2^{l_2} a_3^{l_3} a_4^{l_4},$$

where $a_i \in \mathrm{K}_i(G)$, $l_i = \binom{p^2}{i}$, $i = 2, 3, 4$. If $p > 3$, then $p^2 \mid l_i$ for $i = 2, 3, 4$. Since $\exp(G') \leq p^2$, it follows that

$$g_1^{p^2} = (x^i y^j)^{p^2} = (x^i)^{p^2}(y^j)^{p^2} \in \mathrm{Z}(G).$$

For any $g = x^{k_1} y^{m_1} \ldots x^{k_r} y^{m_r} \in G$, we see that

$$g^{p^2} = (x^{k_1})^{p^2}(y^{m_1})^{p^2} \ldots (x^{k_r})^{p^2}(y^{m_r})^{p^2} \in \mathrm{Z}(G).$$

Now we consider the case $p = 3$. We shall prove in the following four cases that $\exp(\mathrm{K}_3(G)) \leq 3$.

(i) Suppose that $o(y) = 3$. Then $K = \langle y\rangle^G$ is of order $\leq 3^3$. Since K is generated by elements of order 3, it follows that $\exp(K) \leq 3$. But $G' \leq K$ and so we are done.

(ii) Suppose that $o(x) = o(y) = 3^2$. Then $|H|, |K| \leq 3^4$ and so $|H \cap K| \leq 3^3$. Obviously, $\exp(\mathrm{K}_3(G)) \leq 3$ if $|H \cap K| \leq 3^2$ and so we need only consider the case $|H \cap K| = 3^3$. Now we have $|H| = |K| = 3^4$, $|G| = 3^5$ and $|G'| \leq |H \cap K| = 3^3$. If $|G'| \leq 3^2$, then $\exp(\mathrm{K}_3(G)) \leq 3$. It remains to consider the case that $G' = H \cap K$

is of order 3^3. If G' is cyclic, then G is regular and so $G = \langle x, y\rangle$ is of exponent 3^2, a contradiction. Therefore G' is noncyclic. By a result of Burnside, G' is abelian. Indeed, if G' were nonabelian, then $\mathrm{Z}(G')$ is cyclic and so G' would also be cyclic, a contradiction. It follows that $|\Omega_1(G')| \geq 3^2$, $|G/\Omega_1(G')| \leq 3^3$ and $\mathrm{K}_3(G) \leq \Omega_1(G')$, and we are done.

(iii) Suppose that $o(x) = 3^m \geq 3^3$ and $o(y) = 3^2$. (We argue similarly in the case $o(y) = 3^n \geq 3^3$ and $o(x) = 3^2$.) As above, we need only consider $|H \cap K| = 3^3$ and $G' = H \cap K$. If G' is cyclic, then G is regular and so $\exp(K) = 3^2$, a contradiction. Hence G' is noncyclic and then G' is noncyclic abelian with $|\Omega_1(G')| \geq 3^2$. In that case, $\mathrm{K}_3(G) \leq \Omega_1(G')$, and we are done.

(iv) Suppose that $o(x), o(y) \geq 3^3$. By (2), we get $|G'| \leq 3^3$ and we see by the above arguments that $\mathrm{K}_3(G) \leq \langle x^{3^{m-1}}\rangle \times y^{3^{n-1}}$ and so $\exp(\mathrm{K}_3(G)) \leq 3$.

Since $3^2 \mid l_2, l_4$ and $3 \mid l_3$ and $\exp(\mathrm{K}_3(G)) \leq 3$, it follows from the Hall–Petrescu formula that $\mathfrak{V}_2(G) \leq \mathrm{Z}(G)$. □

Lemma 144.5. *Suppose that $G = \langle x, y\rangle \in \mathrm{BI}(p^2)$ is noncyclic, $p > 2$, $o(x) = p^m$ and $o(y) = p^n$. If $m \geq n$ and $m \geq 3$, then there exists $y_1 \in G$ such that $G = \langle x, y_1\rangle$ and $\langle x\rangle \cap \langle y_1\rangle = \{1\}$ or $\langle x\rangle \cap \langle y_1\rangle = \langle y_1^p\rangle$ with $o(y_1) = p^2$, where $p = 3$.*

Proof. We proceed by induction on $m + n$. Let $H = \langle x\rangle^G$ and $K = \langle y\rangle^G$. We first prove our lemma in the special cases where $n = 2$ and $m = n = 3$, which illustrate the idea in the general case.

(a) $n = 2$ and $\langle x\rangle \cap \langle y\rangle = \langle y^p\rangle$. If $p = 3$, then $y_1 = y$ satisfies all the requirements. Hence we need only consider $p > 3$. Consider the subgroup $M = \langle x^{p^{m-2}}, y\rangle$. Since $|\langle x^{p^{m-2}}\rangle^G| \leq p^4$ and $y^p \in \langle x^{p^{m-2}}\rangle$, we have $|M| \leq p^5$ and so M is regular. As $y^p = x^{dp^{m-2}}$ for some integer d (by the assumption), we get $(yx^{-dp^{m-1}})^p = 1$ by the regularity of M (Theorem 7.2(a)). Set $y_1 = yx^{-dp^{m-1}}$. Then $G = \langle x, y_1\rangle$ and $\langle x\rangle \cap \langle y_1\rangle = \{1\}$.

(b) $m = n = 3$. We shall first prove that here G satisfies $\mathrm{cl}(G) \leq 5$, $\exp(G') \leq p^2$ and $\exp(\mathrm{K}_3(G)) \leq p$ in the following subcases.

(b1) $\langle x\rangle \cap \langle y\rangle = \langle x^p\rangle$. Then $x^p \in \mathrm{Z}(G)$ and $x^p = (x^p)^y = (x^y)^p$. Since G is a $\mathrm{BI}(p^2)$-group, we have $|H|, |K| \leq p^5$. By Theorem 74.1, either H is metacyclic (if $|H| \leq p^4$, then H is certainly metacyclic) or $|H| = p^5$, $|\Omega_1(H)| = p^3$ and $\exp(\Omega_1(H)) = p$. If H is metacyclic, then H is regular. Since $x, x^y \in H$, we see that $(x^{-1}x^y)^p = 1$ (Theorem 7.2(a)) and $\exp(G') \leq p$ as $G' \leq \Omega_1(H)$. Because H is metacyclic, $|\Omega_1(H)| \leq p^2$ and so $\mathrm{cl}(G) \leq 3$. So we need only consider the case that

$$|H| = |K| = p^5 \quad \text{and} \quad |\Omega_1(H)| = |\Omega_1(K)| = p^3$$

with $\exp(\Omega_1(H)) = \exp(\Omega_1(K)) = p$.

Set $\bar{G} = G/\Omega_1(H)$ and then $o(\bar{x}) = p^2$ and $\langle\bar{x}\rangle \trianglelefteq \bar{G}$ so that $\bar{G} = \langle\bar{x}\rangle\langle\bar{y}\rangle$ is metacyclic and so $\bar{G}' < \langle\bar{x}\rangle$. Therefore $|\bar{G}'| \leq p$ and so $\mathrm{K}_3(G) \leq \Omega_1(H)$. We have proved that in this case $\mathrm{cl}(G) \leq 5$, $\exp(G') \leq p^2$ and $\exp(\mathrm{K}_3(G)) \leq p$.

(b2) $\langle x\rangle \cap \langle y\rangle = \langle x^{p^2}\rangle$. If H or K is an L_3-group, then the argument in the second paragraph of (b1) can be applied to see that G satisfies $\mathrm{cl}(G) \le 5$, $\exp(G') \le p^2$ and $\exp(\mathrm{K}_3(G)) \le p$. So we need only consider the case where both H and K are metacyclic.

(b2.1) H and K are metacyclic and $H \cap K$ is cyclic. Since $G' \le H \cap K$, we obtain $G' = \langle [x, y]\rangle$. As $x, x^y \in H$ and $x^{p^2} = (x^{p^2})^y = (x^y)^{p^2}$, we see that the regularity of H implies $(x^{-1}x^y)^{p^2} = 1$ and so $[x, y]^{p^2} = 1$. Hence $|G'| \le p^2$, $|\mathrm{K}_3(G)| \le p$ and $\mathrm{cl}(G) \le 3$.

(b2.2) H and K are metacyclic and $H \cap K$ is noncyclic. Since p is odd, we have $|\Omega_1(H \cap K)| \ge p^2$. But H and K are metacyclic and so $\Omega_1(H) = \Omega_1(H \cap K) = \Omega_1(K)$ is elementary abelian of order p^2. Set $\bar{G} = G/\Omega_1(H)$ so that

$$\bar{G} = \langle \bar{x}, \bar{y}\rangle, \quad \langle \bar{x}\rangle \cap \langle \bar{y}\rangle = \{1\}, \quad |\langle \bar{x}\rangle^{\bar{G}} : \langle \bar{x}\rangle| \le p, \quad |\langle \bar{y}\rangle^{\bar{G}} : \langle \bar{y}\rangle| \le p.$$

By Lemma 144.2, we have $|\bar{G}'| \le p$ and so $\mathrm{K}_3(G) \le \Omega_1(H)$. Therefore $\mathrm{cl}(G) \le 4$, $\exp(G') \le p^2$ and $\exp(\mathrm{K}_3(G)) \le p$. Now,

$$\langle x\rangle \cap \langle y\rangle = \langle x^p\rangle \quad \text{or} \quad \langle x\rangle \cap \langle y\rangle = \langle x^{p^2}\rangle,$$

and so $x^{p^2} = y^{kp^2}$, where $1 \le k \le p-1$. Since $\mathrm{cl}(G) \le 5$, using the Hall–Petrescu formula we get

$$(xy^{-k})^{p^2} = x^{p^2} y^{-kp^2} c_2^{n_2} c_3^{n_3} c_4^{n_4} c_5^{n_5},$$

where $c_i \in \mathrm{K}_i(G)$, $n_i = \binom{p^2}{i}$, $i = 1, \ldots, 5$, and $p^2 \mid n_2$, $p \mid n_3$, $p \mid n_4$, $p \mid n_5$ since $p > 2$. Hence $(xy^{-k})^{p^2} = 1$. Let $y_0 = xy^{-k}$ so that $G = \langle x, y_0\rangle$ and $o(y_0) \le p^2$. By (a), there exists $y_1 \in G$ such that $\langle x\rangle \cap \langle y_1\rangle = \{1\}$ or $\langle x\rangle \cap \langle y_1\rangle = \langle y_1^3\rangle$ with $o(y_1) = 9$.

(c) $m = n \ge 4$.

(c1) $\langle x^{p^2}\rangle \le \langle x\rangle \cap \langle y\rangle$. Hence we obtain $x^{p^2} \in \mathrm{Z}(G)$ and $\langle x^{p^3}\rangle \trianglelefteq G$. Consider $\bar{G} = G/\langle x^{p^3}\rangle$ so that $\bar{G} = \langle \bar{x}, \bar{y}\rangle$ and $o(\bar{x}) = o(\bar{y}) = p^3$. By (b), there exists $y_1 \in G$ such that $\bar{G} = \langle \bar{x}, \bar{y_1}\rangle$ and $o(\bar{y_1}) \le p^2$. Thus we get $G = \langle x, y_1\rangle$ and $o(y_1) < o(x)$. Let $G_0 = \langle x^p, y_1\rangle$. By induction, there exists $y_2 \in G_0$ such that $G_0 = \langle x^p, y_2\rangle$ and $\langle x^p\rangle \cap \langle y_2\rangle = \{1\}$ or $\langle x^p\rangle \cap \langle y_2\rangle = \langle y_2^p\rangle$ with $p = 3$ and $o(y_2) = 9$. Therefore $G = \langle x, G_0\rangle = \langle x, y_2\rangle$ and $\langle x\rangle \cap \langle y_2\rangle = \{1\}$ or $\langle x\rangle \cap \langle y_2\rangle = \langle y_2^p\rangle$ with $o(y_2) = 9$.

(c2) $\langle x\rangle \cap \langle y\rangle = \langle x^{p^{m-1}}\rangle$. We shall prove in this part that $\mathrm{cl}(G) \le 6$, $\exp(G') \le p^3$, $\exp(\mathrm{K}_3(G)) \le p^2$ and $\exp(\mathrm{K}_4(G)) \le p$. By Theorem 74.1, H is either metacyclic or H is an L_3-group and the same holds for K.

(c2.1) First suppose that H (or K) is an L_3-group. Now consider the factor group $\bar{G} = G/\Omega_1(H) = \langle \bar{x}, \bar{y}\rangle$, where $\langle \bar{x}\rangle \cap \langle \bar{y}\rangle = \{1\}$. By Lemma 144.4, $\exp(\bar{G}') \le p^2$. Then $\bar{G}'$ is a cyclic group of order $\le p^2$ as $\bar{G}' \le \bar{H} = \langle \bar{x}\rangle$. Therefore $\exp(G') \le p^3$, $\exp(\mathrm{K}_3(G)) \le p^2$ and $\exp(\mathrm{K}_4(G)) \le p$. Since $|G'| \le p^5$, we have $\mathrm{cl}(G) \le 6$.

(c2.2) H and K are metacyclic and $H \cap K$ is cyclic. Since $G' \le H \cap K$, we see that G' is cyclic and $G' = \langle [x, y]\rangle$. Consider the factor group $\bar{G} = G/\langle x^{p^{m-1}}\rangle = \langle \bar{x}, \bar{y}\rangle$,

where $\langle\bar{x}\rangle \cap \langle\bar{y}\rangle = \{1\}$. By Lemma 144.4, $o[\bar{x}, \bar{y}] \le p^2$ and so $o[x, y] \le p^3$. Hence $\exp(G') \le p^3$, $\exp(\mathrm{K}_3(G)) \le p^2$, $\exp(\mathrm{K}_4(G)) \le p$ and $\mathrm{cl}(G) \le 4$.

(c2.3) H and K are metacyclic and $H \cap K$ is noncyclic. We have

$$\Omega_1(H) = \Omega_1(K) = \Omega_1(H \cap K) \cong \mathrm{E}_{p^2}.$$

Consider $\bar{G} = G/\Omega_1(H) = \langle\bar{x}, \bar{y}\rangle$, where $\langle\bar{x}\rangle \cap \langle\bar{y}\rangle = \{1\}$ and $|\langle\bar{x}\rangle^{\bar{G}} : \langle\bar{x}\rangle| \le p$, $|\langle\bar{y}\rangle^{\bar{G}} : \langle\bar{y}\rangle| \le p$. By Lemma 144.2, we have $|\bar{G}'| \le p$ and so $|G'| \le p^3$ which gives $\mathrm{cl}(G) \le 4$, $\exp(G') \le p^3$, $\exp(\mathrm{K}_3(G)) \le p^2$ and $\exp(\mathrm{K}_4(G)) \le p$.

Since $\langle x\rangle \cap \langle y\rangle = \langle x^{p^{m-1}}\rangle$, we have $x^{p^{m-1}} = y^{-lp^{m-1}}$ for some positive integer $l \le p-1$. By the Hall–Petrescu formula, we get

$$(xy^l)^{p^{m-1}} = x^{p^{m-1}} y^{lp^{m-1}} c_2^{n_2} c_3^{n_3} c_4^{n_4} c_5^{n_5} c_6^{n_6},$$

where $c_i \in \mathrm{K}_i(G)$, $n_i = \binom{p^{m-1}}{i}$, $i = 1, \dots, 6$, and $p^3 \mid n_2$, $p^2 \mid n_j$, $j = 3, \dots, 6$ since $p > 2$. It follows that $(xy^l)^{p^{m-1}} = 1$ and so $G = \langle x, xy^l\rangle$ with $o(x) > o(xy^l)$. By induction, there is an element $y_1 \in G$ such that $G = \langle x, y_1\rangle$ and $\langle x\rangle \cap \langle y_1\rangle = \{1\}$ or $\langle x\rangle \cap \langle y_1\rangle = \langle y_1^p\rangle$ with $o(y_1) = p^2$, where $p = 3$.

(c3) $\langle x\rangle \cap \langle y\rangle = \langle x^{p^{m-k}}\rangle$ for some $k \ge 2$. In this case, we consider the factor group $\bar{G} = G/\langle x^{p^{m-k+1}}\rangle$ so that $\bar{G} = \langle\bar{x}, \bar{y}\rangle$. Then we apply (c2) to find $g_0 \in G$ such that $\bar{G} = \langle\bar{x}, \bar{y_0}\rangle$ with $o(\bar{y_0}) < o(\bar{y})$. Hence we obtain $G = \langle x, y_0\rangle$ with $o(y_0) < o(y)$. By induction, there is $y_1 \in G$ satisfying all the requirements.

(d) $m > n \ge 3$. Let $G_1 = \langle x^{p^{m-n}}, y\rangle$. By induction, there exists an element y_1 such that $G_1 = \langle x^{p^{m-n}}, y_1\rangle$ and $\langle x^{p^{m-n}}\rangle \cap \langle y_1\rangle = \{1\}$ or $\langle x^{p^{m-n}}\rangle \cap \langle y_1\rangle = \langle y_1^p\rangle$ with $o(y_1) = p^2$, where $p = 3$. Hence $G = \langle x, G_1\rangle = \langle x, y_1\rangle$ satisfies all the requirements. □

Theorem 144.6. *Let $G \in \mathrm{BI}(p^2)$ with $p > 2$. Then $\mho_2(G) \le \mathrm{Z}(G)$ and $\exp(G') \le p^2$.*

Proof. We first prove that $\mho_2(G) \le \mathrm{Z}(G)$.

Let $x \in G$ be such that $o(x) = p^m \ge p^3$. For any $y \in G$ we consider $G_1 = \langle x, y\rangle$. It suffices to prove that $[x^{p^2}, y] = 1$. If $\langle x\rangle \cap \langle y\rangle = \{1\}$, then Lemma 144.4 implies that $\mho_2(G_1) \le \mathrm{Z}(G_1)$ and so $[x^{p^2}, y] = [x, y^{p^2}] = 1$.

(i) $o(y) \le p^2$. By the above argument, we need only consider the case $o(y) = p^2$ and $\langle x\rangle \cap \langle y\rangle = \langle y^p\rangle$. If $m = 3$, then $x^{p^2} \in \mathrm{Z}(G_1)$ and so $[x^{p^2}, y] = 1$. Let $m > 3$ and $x_0 \in \langle x\rangle$ be such that $x_0^p = y^{-p}$. By Lemma 144.1, $|\langle x\rangle : \mathrm{N}_{\langle x\rangle}(\langle y\rangle)| \le p^2$ and so $\langle x_0\rangle$ normalizes $\langle y\rangle$ and therefore $[x_0, y] \in \langle y^p\rangle$ so that $\langle x_0, y\rangle$ is of order p^3 and class ≤ 2. Now set $y_1 = x_0 y$ so that $y_1^p = x_0^p y^p = 1$ and $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$. By Lemma 144.4, $x^{p^2} \in \mathrm{Z}(G_1)$ and we are done.

(ii) $o(y) \ge p^3$. Without loss of generality we may assume $o(x) \ge o(y)$. If there is y_1 such that $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$ and $\langle x\rangle \cap \langle y_1\rangle = \{1\}$, then, by Lemma 144.4, we have $\mho_2(G_1) \le \mathrm{Z}(G_1)$ which gives $[x^{p^2}, y] = 1$. Due to Lemma 144.5, there is only one exceptional case where $p = 3$, $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$, $\langle x\rangle \cap \langle y_1\rangle = \langle y_1^3\rangle$ and $o(y_1) = 9$. By (i) applied to $G_1 = \langle x, y_1\rangle$, we see that $x^{3^2} \in \mathrm{Z}(G_1)$ and we are done.

Now we prove $\exp(G') \leq p^2$.

We claim that $o([x,y]) \leq p^2$ for all $x, x \in G$. If $o(y) \leq p^2$, then $|\langle y\rangle^G| \leq p^4$. Suppose that $\exp(\langle y\rangle^G) \geq p^3$. Then $\langle y\rangle^G$ is metacyclic and so regular which implies that $\exp(\langle y\rangle^G) = \exp(\langle y\rangle) \leq p^2$, a contradiction. Therefore we get $\exp(\langle y\rangle^G) \leq p^2$ and so $o([x,y]) \leq p^2$ since $[x,y] \in \langle y\rangle^G$ for each $x \in G$. If $o(x) \geq o(y) \geq p^3$, then consider $G_1 = \langle x, y\rangle$ so that, by Lemma 144.5, there exists an element y_1 such that $G_1 = \langle x, y\rangle = \langle x, y_1\rangle$ and $\langle x\rangle \cap \langle y_1\rangle = \{1\}$ or $\langle x\rangle \cap \langle y_1\rangle = \langle y_1^3\rangle$ and $o(y_1) = 9$. If $\langle x\rangle \cap \langle y_1\rangle = \{1\}$, then, by Lemma 144.4, $o([x,y]) \leq p^2$. In case $\langle x\rangle \cap \langle y_1\rangle \neq \{1\}$, we get $o(y_1) = 3^2$ and so we also see that $o([x,y]) \leq 3^2$. Indeed, by the above argument, we infer that $|\langle y_1\rangle^{G_1}| \leq 3^4$ and $\exp(\langle y_1\rangle^{G_1}) \leq 3^2$ and since $G_1' \leq \langle y_1\rangle^{G_1}$, we get $o([x,y]) \leq 3^2$.

It suffices to show that $\exp(\langle a,b\rangle) \leq p^2$ for any $a, b \in G$ with $o(a), o(b) \leq p^2$. Set $A = \langle a,b\rangle$, $H = \langle a\rangle^A$ and $K = \langle b\rangle^A$. Hence we get $|H| \leq p^4$, $|K| \leq p^4$ and $|A| \leq p^6$. If $|A| = p^6$, then $|H \cap K| \leq p^2$ and then $|A'| \leq p^2$, $|\mathrm{K}_3(A)| \leq p$ and $\mathrm{cl}(A) \leq 3$. By the Hall–Petrescu formula, $\exp(A) \leq p^2$. So it remains to consider the case $|A| \leq p^5$. Suppose that $\exp(A) \geq p^3$. By Theorem 74.1, A is either metacyclic or $|A| = p^5$ and A is an L_3-group so that $|\Omega_1(A)| = p^3$ and $\exp(\Omega_1(A)) = p$. If A is metacyclic, then A is regular, and therefore $\exp(A) \leq p^2$. In the second case, we get $\exp(\Omega_2(A)) \leq p^2$. But $a, b \in \Omega_2(A)$, a contradiction. Hence $\exp(A) \leq p^2$. We have proved that $\exp(G') \leq p^2$. □

Theorem 144.7. *Let $G \in \mathrm{BI}(p^2)$ with $p > 2$. Then $\mathrm{cl}(G) \leq 4$.*

Proof. It suffices to prove that $[x,y] \in \mathrm{Z}_3(G)$ for any $x, y \in G$. We set $o(x) = p^m$, $o(y) = p^n$, $H = \langle x\rangle^G$ and $K = \langle y\rangle^G$. If $|H \cap K| \leq p^3$, then $[x,y] \in \mathrm{Z}_3(G)$ since $[x,y] \in H \cap K \trianglelefteq G$.

(i) $m \leq 2$ and $n \leq 2$. Hence $|H|, |K| \leq p^4$ and $|H'|, |K'| \leq p^2$. If $y \in H$, then $[x,y] \in H'$ and so $[x,y] \in \mathrm{Z}_2(G) \leq \mathrm{Z}_3(G)$. Similarly, $[x,y] \in \mathrm{Z}_3(G)$ if $x \in K$. Now assume that $x \notin K$ and $y \notin H$. Then $|H \cap K| \leq p^3$ and then $[x,y] \in \mathrm{Z}_3(G$.

(ii) $m \leq 2$ and $n \geq 3$ (and similarly for $m \geq 3$ and $n \leq 2$). Since $|H| \leq p^4$, we need only consider $|H \cap K| = p^4$ and then $H \leq K$. By Lemma 144.3, $|K'| \leq p^2$ and therefore $[x,y] \in \mathrm{Z}_3(G)$.

(iii) $m \geq 3$ and $n \geq 3$. If $\langle x\rangle \cap \langle y\rangle = \{1\}$, then $|H \cap K| \leq p^4$. As before, we need only consider $|H \cap K| = p^4$. Then $x^{p^{m-1}}, y^{p^{n-1}} \in H \cap K$. By Theorem 144.6, $\langle x^{p^{m-1}}, y^{p^{n-1}}\rangle \leq \mathrm{Z}(G)$. Hence we get $H \cap K \leq \mathrm{Z}_3(G)$. We consider now the case $\langle x\rangle \cap \langle y\rangle \neq \{1\}$. Set $G_1 = \langle x, y\rangle$, where we can assume $m \geq n$. By Lemma 144.5, there exists $y_1 \in G_1$ such that $G_1 = \langle x, y_1\rangle$ and $\langle x\rangle \cap \langle y_1\rangle = \{1\}$ or $\langle x\rangle \cap \langle y_1\rangle = \langle y_1^p\rangle$ with $o(y_1) = p^2$, where $p = 3$. If $\langle x\rangle \cap \langle y_1\rangle = \{1\}$, we see that $G_1' \leq \mathrm{Z}_3(G)$ as above and then $[x,y] \in \mathrm{Z}_3(G)$. In the second case, $o(y_1) = 3^2$ and so, by (ii) above, we also have $[x,y] \in G_1' \leq \mathrm{Z}_3(G)$. □

Lemma 144.8. *Let $G \in \mathrm{BI}(p^2)$ with $p > 2$. Suppose that $x, y \in G$, $o(x) = p^m \geq p^3$ and $o(y) = p^n \geq p^3$. If $\langle x\rangle \cap \langle y\rangle = \{1\}$, then $[x,y] \in \mathrm{Z}_2(G)$.*

Proof. By Theorem 144.6, $x^{p^{m-1}}, y^{p^{n-1}} \in \mathrm{Z}(G)$. Set $H = \langle x\rangle^G$ and $K = \langle y\rangle^G$. Since G is a BI(p^2)-group, we have $|H \cap K| \leq p^4$. If $|H \cap K| \leq p^2$, then we have $[x, y] \in H \cap K \leq \mathrm{Z}_2(G)$. In case $|H \cap K| = p^3$, we get $x^{p^{m-1}}, y^{p^{n-1}} \in H \cap K$ and $x^{p^{m-1}}, y^{p^{n-1}} \in \mathrm{Z}(G)$ and so $H \cap K \leq \mathrm{Z}_2(G)$. We need only consider the case $|H \cap K| = p^4$ in which case

$$H \cap K = \langle x^{p^{m-2}}\rangle\langle y^{p^{n-2}}\rangle.$$

If $m \geq 4$, then, by Theorem 144.6, $x^{p^{m-2}} \in \mathrm{Z}(G)$. Since also $y^{p^{n-1}} \in \mathrm{Z}(G)$, we get $[x, y] \in H \cap K \leq \mathrm{Z}_2(G)$. Similarly, we have $[x, y] \in H \cap K \leq \mathrm{Z}_2(G)$ in case $n \geq 4$.

We may assume that $|H \cap K| = p^4$ and $m = n = 3$. Since $\langle x\rangle \cap \langle y\rangle = \{1\}$, we have $|H \cap \langle y\rangle| = p^2$ and so $y^p \in H$. Thus $H = \langle x, y^p\rangle = \langle x\rangle\langle y^p\rangle$ is of order p^5 and $HK \trianglelefteq G$ is of order p^6 since $HK = H\langle y\rangle$ with $y^p \in H$. But

$$|\langle x\rangle\langle y\rangle| = |\langle x\rangle||\langle y\rangle| = p^6$$

and so $HK = \langle x\rangle\langle y\rangle$ is a product of two cyclic subgroups. By Corollary 36.8, H is metacyclic and so H is also regular. Thus HK is metacyclic of exponent p^3 which implies that $(HK)'$ is cyclic of order $\leq p^2$. Since $[x, y] \in (HK)'$ and $(HK)' \leq \mathrm{Z}_2(G)$, we are done. □

Theorem 144.9. *Let $G \in \mathrm{BI}(p^2)$ with $p > 2$. Then we have $\mathrm{cl}(G) \leq 3$ if and only if $[\Omega_2(G), G] \leq \mathrm{Z}_2(G)$.*

Proof. Obviously, we need only prove that our condition is sufficient. Let $x, y \in G$. If $o(y) \leq p^2$ (or $o(x) \leq p^2$), then $[x, y] \in \mathrm{Z}_2(G)$ by assumption. Hence we may assume that $o(x) \geq o(y) \geq p^3$. Let $G_1 = \langle x, y\rangle$. By Lemma 144.5, there is $y_1 \in G_1$ such that $G_1 = \langle x, y_1\rangle$ and $\langle x\rangle \cap \langle y_1\rangle = \{1\}$ or $\langle x\rangle \cap \langle y_1\rangle = \langle y_1^3\rangle$ with $o(y_1) = 9$. If $o(y_1) \leq p^2$, we have $[x, y_1] \in \mathrm{Z}_2(G)$ by assumption and $[x, y] \in G_1' \leq \mathrm{Z}_2(G)$. In case $o(y_1) \geq p^3$, we get $\langle x\rangle \cap \langle y_1\rangle = \{1\}$ and, by Lemma 144.8, $[x, y_1] \in \mathrm{Z}_2(G)$ and $[x, y] \in G_1' \leq \mathrm{Z}_2(G)$. Therefore $\mathrm{cl}(G) \leq 3$. □

Appendix 27

Wreathed 2-groups

In this section we study the subgroup structure of wreath products of some small 2-groups with a group of order 2.

Let $\mathrm{sol}_k(G)$ be the number of solutions of $x^{2^k} = 1$ in a group G.

Exercise 1. Let A be a finite group and $G = A \operatorname{wr} C$, where $C = \langle c \mid c^2 = 1\rangle \cong \mathrm{C}_2$. Then

$$\mathrm{sol}_1(G) = |A| + \mathrm{sol}_1(A)^2.$$

(We have $\mathrm{c}_1(G) = \mathrm{sol}_1(G) - 1$.) It follows that the set $G - (A \times A^c)$ contains exactly $|A|$ involutions. Since $\mathrm{C}_G(c) = \langle c\rangle \times \Delta$, where Δ is the diagonal of the base $A \times A^c$, all involutions of the set $G-(A\times A^c)$ are conjugate in G in view of $|G : \mathrm{C}_G(c)| = |A|$.

Solution. Let $B = A \times A^c$ be the base of $G = C \cdot B$ (a semidirect product with kernel B). An element $g \in G - B$ can uniquely be represented in the form $g = xy^c c$ for $x, y \in A$. We have

$$g^2 = xy^c cxy^c c = xcyxcy = x(yx)^c y = (xy)(yx)^c.$$

If $g^2 = 1$, then $xy = 1$, i.e., $y = x^{-1}$. It follows that $G - B$ contains exactly $|A|$ involutions and

$$\mathrm{sol}_1(G) = |A| + \mathrm{sol}_1(B) = |A| + \mathrm{sol}_1(A)^2.$$

In particular, if $A \cong \mathrm{C}_{2^n}$, then $\mathrm{sol}_1(G) = 2^n + 4$ so $\mathrm{c}_1(G) = 2^n + 3$. Next,

$$\mathrm{c}_1(\mathrm{D}_8 \operatorname{wr} \mathrm{C}_2) = 8 + 6^2 - 1 = 43, \quad \mathrm{c}_1(\mathrm{Q}_8 \operatorname{wr} \mathrm{C}_2) = 8 + 2^2 - 1 = 11.$$

1^o. Let $G = A \operatorname{wr} C$, where

$$A = \langle a \mid a^{2^n} = 1\rangle \cong \mathrm{C}_{2^n}, \quad C = \langle c \mid c^2 = 1\rangle \cong \mathrm{C}_2.$$

Then $|G| = 2^{2n+1}$ and

$$G = \langle a, b, c \mid a^{2^n} = b^{2^n} = c^2 = 1,\ [a, b] = 1,\ a^c = b\rangle.$$

The group $B = \langle a\rangle \times \langle a^c\rangle$ is the base of the wreath product G. Every element of B can be written uniquely in the form $a^i (a^c)^j$, where $i, j = 1, 2, \ldots, 2^n$. If $n = 1$, then we have $G \cong \mathrm{D}_8$. So, in what follows, we assume that $n > 1$. The abelian subgroup B

of type $(2^n, 2^n)$ is maximal in G so we get $\mathrm{Z}(G) = \mathrm{C}_B(c) < B$. Let $a^i(a^j)^c \in \mathrm{Z}(G)$, $0 \le i, j < p^n$. Then

$$a^i(a^j)^c = (a^i(a^j)^c)^c = a^j(a^i)^c.$$

It follows that $a^i = a^j$. It is easy to see that $(aa^c)^i = a^i(a^i)^c \in \mathrm{Z}(G)$ for all i. Thus we have proved assertion (a) of the following

Lemma A.27.1. (a) $\mathrm{Z}(G) = \langle aa^c \rangle \cong \mathrm{C}_{2^n}$.

(b) *G is not metacyclic unless $n = 1$.*

Proof. It remains to prove (b). Due to (a), $\langle \Omega_1(B), c \rangle$ is nonabelian so it is isomorphic to D_8. By Proposition 10.19, if a metacyclic 2-group contains a nonabelian subgroup of order 8, it is of maximal class. Since G is not of maximal class unless $n = 1$, it is not metacyclic for $n > 1$. □

Remark. Let $G = A$ wr B be a p-group. Then $\mathrm{d}(G) = \mathrm{d}(A) + \mathrm{d}(B)$. We claim that if $\{x_1, \dots, x_r\}$ and $\{y_1, \dots, y_s\}$ are minimal bases of the groups A and B, respectively, then $\mathcal{B} = \{x_1, \dots, x_r, y_1, \dots, y_s\}$ is a minimal basis of G. Indeed, we have $\langle \mathcal{B} \rangle = G$, $\langle \mathcal{B} - \{x_i\} \rangle < G$ and $\langle \mathcal{B} - \{y_j\} \rangle < G$ for all $i \le r$ and $j \le s$. In particular,

$$|G : \Phi(G)| = |A : \Phi(A)||B : \Phi(B)| = p^{r+s}.$$

It follows from Lemma 1.1 that

$$2^{2n+1} = |G| = 2|\mathrm{Z}(G)||G'| = 2^{n+1}|G'|$$

so that $|G'| = 2^n$. As $G = \langle a, c \rangle$, we have $\mathrm{d}(G) = 2$. Since $\Phi(G)$ is a subgroup of index 2 in an abelian group B of type $(2^n, 2^n)$, we get the following

Lemma A.27.2. (a) $|G'| = 2^n$.

(b) *$\Phi(G)$ is abelian of type $(2^n, 2^{n-1})$.*

Lemma A.27.3. *$G/\mathrm{Z}(G) \cong \mathrm{D}_{2^{n+1}}$. In particular,* $\mathrm{cl}(G) = n + 1$.

Proof. We have

$$(a\mathrm{Z}(G))^c = a^c\mathrm{Z}(G) = a^{-1}(aa^c\mathrm{Z}(G)) = a^{-1}\mathrm{Z}(G)$$

(Lemma A.27.1(a)). Since $\langle a, \mathrm{Z}(G) \rangle = B$ and $G = \langle B, c \rangle$, the result follows. □

Since $G/[B, C]$ is abelian, we get $G' = [B, C]$.

Lemma A.27.4. *Let $n > 1$.*

(a) *$G' = \langle a^{-1}a^c \rangle \cong \mathrm{C}_{2^n}$ and G/G' is abelian of type $(2^n, 2)$.*[1]

(b) *$D = \langle c, G' \rangle \cong \mathrm{D}_{2^{n+1}}$ and G/D is cyclic; then $|\Omega_1(G)| = 2|D| = 2^{n+2}$.*

[1] This agrees with the Ito–Ohara result; see Corollary 36.11 (indeed, as we shall prove, our nonmetacyclic group G is a product of two cyclic subgroups).

(c) $\Omega_1(G) = D\Omega_1(B)$ *is of order* 2^{n+2}, $D \cap \Omega_1(B) = \Omega_1(\mathrm{Z}(G))$.

(d) $D < \Omega_2(G)$, $|G : \Omega_{n-1}(G)| = 2$.

Proof. We have $a^{-1}a^c = [a, c] \in G'$ and $o(a^{-1}a^c) = 2^n = |G'|$ which proves (a) (Lemma A.27.2(a)).

Since $(a^{-1}a^c)^c = (a^{-1}a^c)^{-1}$, we see that $D = \langle c, G'\rangle \cong \mathrm{D}_{2^{n+1}}$. As $\mathrm{d}(G) = 2$, $D \lhd G$ and $\mathrm{Z}(D)$ is cyclic, it follows that $D \not\leq \Phi(G)$ (Lemma 1.4) so that the quotient group G/D is cyclic. By Exercise 1, $\mathrm{c}_1(G) = 2^n + 3 = \mathrm{c}_1(D) + 2$. It follows from $n > 1$ that $|D \cap \Omega_1(B)| = 2$ so $\Omega_1(G) = D\Omega_1(B)$ (see Proposition 1.17(a)) is of order $2|D| = 2^{n+2}$, completing the proof of (b) and (c).

Note that $D = \Omega_2(D)$ and $\Omega_1(B) \not\leq D$ so we obtain $\Omega_2(G) > D$. It follows from the cyclicity of $G/\Omega_1(G)$ as an epimorphic image of G/D and $|\Omega_1(G)| = 2^{n+2}$ that $|\Omega_{n-1}(G)| = 2^{2n}$ hence $|G : \Omega_{n-1}(G)| = 2$, completing the proof of (d). □

Lemma A.27.5. *The class number of* G *is equal to* $\mathrm{k}(G) = 2^{2n-1} + 2^{n+1} - 2^{n-1}$.

Proof. We have $\mathrm{cd}(G) = \{1, 2\}$ (Introduction, Theorem 17) so that

$$\begin{aligned}\mathrm{k}(G) &= |G : G'| + \frac{|G| - |G : G'|}{2^2}\\ &= 2^{n+1} + \frac{2^{2n+1} - 2^{n+1}}{2^2} = 2^{2n-1} + 2^{n+1} - 2^{n-1},\end{aligned}$$

and the proof is complete. □

Lemma A.27.6. *We have* $o(ac) = 2^{n+1}$ *hence* $\exp(G) = 2^{n+1}$.

Proof. We obtain $\exp(G) \leq \exp(B)\exp(C) = 2^{n+1}$. The element $(ac)^2 = aa^c$ has order 2^n hence $o(ac) = 2^{n+1}$. □

Lemma A.27.7. *The subgroup* $G' \cap \mathrm{Z}(G) = \Omega_1(G')$ *is of order* 2 *and*

$$\Phi(G) = \langle a^2\rangle \times \langle aa^c\rangle = \langle a^2\rangle \times \mathrm{Z}(G) = G'\mathrm{Z}(G)$$

is abelian of type $(2^n, 2^{n-1})$.

Proof. Clearly, we see that $G' \cap \mathrm{Z}(G) = \Omega_1(G')$ since $G' < D$ and $D \lhd G$ is of maximal class. Further, we get $\Phi(G) = \mho_1(G)$ and so $a^2, aa^c \in \Phi(G)$ as $aa^c = a^2[a, c]$. Since $\langle a^2\rangle \cap \langle aa^c\rangle = \{1\}$, the first equality in the displayed line follows. Because of $G' \cap \langle a^2\rangle = \{1\}$, $B = G'\langle a\rangle$ and $a^2 \in \Phi(G)$, we get $\Phi(G) = \langle a^2\rangle \times G'$ (compare orders). Since $G'\mathrm{Z}(G) \leq \Phi(G)$ and $G' \cap \mathrm{Z}(G) = \Omega_1(G')$, we obtain $G'\mathrm{Z}(G) = \Phi(G)$ by the product formula. □

Let us compute $\mathrm{c}_k(G)$ for all positive integers k, $k \leq n + 1 = \log_2(\exp(G))$. Since

$$\mathrm{c}_k(B) = \frac{|\Omega_k(B) - \Omega_{k-1}(B)|}{2^{k-1}} = \frac{2^{2k} - 2^{2k-2}}{2^{k-1}} = 3 \cdot 2^{k-1}$$

for $k \le n$, it remains to compute the number $\mathrm{sol}_k(G-B)$ of elements of order $2^k > 2$ in the set $G - B$; then

$$\mathrm{c}_k(G) = 3 \cdot 2^{k-1} + \frac{\mathrm{sol}_k(G-B)}{2^{k-1}}$$

(here $2^{k-1} = \varphi(2^k)$, where $\varphi(*)$ is Euler's totient function).

Let $x = a^i (a^c)^j c \in G - B$, $i, j = 0, 1, 2, \ldots, 2^n - 1$. We have

$$x^2 = a^{i+j} (a^c)^{i+j} = (aa^c)^{i+j} \in \mathrm{Z}(G).$$

Suppose that $x^2 = 1$. Then $a^{i+j} = 1$ so $i + j \equiv 0 \pmod{2^n}$. We see that there are in $G - B$ exactly 2^n elements of order 2, i.e., $\mathrm{c}_1(G) = 2^n + \mathrm{c}_1(B) = 2^n + 3$ (this coincides with the result of Exercise 1).

Now suppose that $x^4 = 1$. In that case, we have $1 = x^4 = a^{2(i+j)}(a^c)^{2(i+j)}$ so $a^{2(i+j)} = 1$. It follows that $i + j \equiv 0 \pmod{2^{n-1}}$. If $i = 0$, then $j \in \{0, 2^{n-1}\}$. Similarly, for arbitrary i we have $j \in \{2^{n-1} - i, 2^n - i\}$. Thus $G - B$ contains exactly $2 \cdot 2^n$ elements of order ≤ 4 so exactly $2 \cdot 2^n - 2^n = 2^n$ elements of order 4.

Now we prove for $k \in \{2, \ldots, n\}$ that $G - B$ contains exactly $2^{n+(k-2)}$ elements of order 2^k. By the previous paragraph, this is true for $k = 2$. Let $x^{2^k} = 1$ ($x \in G - B$). Then

$$a^{(i+j)2^{k-1}} (a^c)^{(i+j)2^{k-1}} = 1 \quad \text{so that} \quad i + j \equiv 0 \pmod{2^{n-(k-1)}}.$$

It follows that for arbitrary i we have

$$j = s \cdot 2^{n-(k-1)} - i, \quad \text{where } s = 1, 2, \ldots, 2^{k-1}.$$

Thus for a fixed i there are in $G - B$ exactly 2^{k-1} elements $a^i (a^c)^j c$ of order $\le 2^k$ whence the set $G - B$ contains exactly $2^{k-1} \cdot 2^n = 2^{n+(k-1)}$ elements of order $\le 2^k$, $k < n + 1$. By induction, the set $G - B$ has 2^{n+k-2} elements of order $\le 2^{k-1}$. Thus the set $G - B$ possesses exactly $2^{n+k-1} - 2^{n+k-2} = 2^{n+k-2}$ elements of order 2^k.

Now let $o(x) = 2^{n+1}$; then $o(x^2) = 2^n$, where $x^2 = a^{i+j}(a^c)^{i+j} = (aa^c)^{i+j}$. It follows that $i + j$ is odd, and we conclude that $G - B$ has exactly $2^{n-1} \cdot 2^n = 2^{2n-1}$ elements of order 2^{n+1}. Since

$$2^n + 2^n + 2^{n+1} + 2^{n+2} + \cdots + 2^{2n-1} = 2^{2n} = |G - B|,$$

we have found all elements of the set $G - B$. Let $\mathrm{N}_k(X)$ be the number of elements of order 2^k in a set X; then, with $k = 3, \ldots, n$,

$$\mathrm{N}_k(B) = 3 \cdot 2^{2(k-1)}, \quad \mathrm{N}_1(G-B) = \mathrm{N}_2(G) = 2^n, \quad \mathrm{N}_k(G-B) = 2^{n+k-2}.$$

We obtain the number $\mathrm{c}_k(G)$ from the following equality:

$$\mathrm{N}_k(G) = \mathrm{N}_k(G-B) + \mathrm{N}_k(B) = 2^{k-1} \cdot \mathrm{c}_k(G).$$

Thus we have

$$\begin{aligned}
&\mathrm{c}_1(G) = 2^n + 3, \quad \mathrm{c}_2(G) = 3 \cdot 2 + 2^{n-1},\\
&\mathrm{c}_k(G) = 3 \cdot 2^{k-1} + 2^{n-1} \quad \text{for } k = 3, \dots, n,\\
&\mathrm{c}_n(G) = 3 \cdot 2^{n-1} + 2^{n-1} = 2^{n+1}, \quad \mathrm{c}_{n+1}(G) = 2^{2n-1}/2^n = 2^{n-1}.
\end{aligned}$$

Since $(ac)^2 = aa^c \in \mathrm{Z}(G)$ is of order 2^n, we infer that $\mathrm{Z}(G)$ has index 2 in $\langle ac \rangle$ so $\mathrm{Z}(G)$ is not a maximal cyclic subgroup of G. It follows from the proof of Lemma 27.3 that $\mathrm{Z}(G/\mathrm{Z}(G)) = \langle a^{2^{n-1}}\mathrm{Z}(G)\rangle$. However, the subgroup $\langle a^{2^{n-1}}, \mathrm{Z}(G)\rangle$ is abelian of type $(2^n, 2)$. Since $G/\mathrm{Z}(G) \cong \mathrm{D}_{2^{n+1}}$ has only one minimal normal subgroup, it follows that $\langle ac \rangle$ is not normal in G; moreover, it has exactly 2^{n-1} conjugates in G.

We claim that all cyclic subgroups of the group G that are not contained in $\Phi(G)$ are not G-invariant. Indeed, assume that $X \lhd G$ is cyclic and $X \not\leq \Phi(G)$. Since $\mathrm{d}(G) = 2$, it follows that G/X is cyclic, and hence G is metacyclic, a contradiction.

Let cG', uG' and cuG' be all involutions in the quotient group G/G'. Then we get $\mathrm{c}_1(\langle c, G'\rangle) = 2^n + 1$ (Lemma A.27.4(b)). Since $\mathrm{c}_1(G) = 2^n + 3$, it follows that the subgroups $L_1 = \langle u, G'\rangle$ and $L_2 = \langle cu, G'\rangle$ contain together exactly four involutions (one of them is an element of G'). Therefore one may assume that the subgroup L_1 contains exactly one involution so L_1 is cyclic or generalized quaternion. Since G' is contained in an even number of subgroups of maximal class and order $2|G'| = 2^{n+1}$ and $D = \langle c, G'\rangle \cong \mathrm{D}_{2^{n+1}}$ is dihedral so of maximal class, we obtain $L_1 \cong \mathrm{Q}_{2^{n+1}}$. As $\mathrm{C}_G(G') > G'$, it follows that L_2 is abelian of type $(2^n, 2)$, and so G' is a maximal cyclic subgroup of G. Then $\Omega_1(G) = DL_1 = D\Omega_1(B)$ (compare the number of involutions and use Theorem 1.17(a); DL_1 is not of maximal class since $\Omega_1(B) \lhd DL_1$).

Now we shall find all three members of the set Γ_1. We have $B \in \Gamma_1$. Since G satisfies $\mathrm{cl}(G) = n + 1 > 2$, B is the unique abelian maximal subgroup of G and two remaining members of the set Γ_1 have class at least n (Fitting's lemma). The subgroup

$$\Phi(G) = \langle a^2\rangle \times \langle (ac)^2\rangle = \langle a^2\rangle \times \langle aa^c\rangle = \langle a^2\rangle \times \mathrm{Z}(G)$$

is abelian of type $(2^n, 2^{n-1})$. Since $c \notin B$, the subgroup

$$M = \langle c, \Phi(G)\rangle = \langle c, a^2, aa^c\rangle$$

is another maximal subgroup of G. It then follows from Lemma A.27.3 that $M/\mathrm{Z}(G)$ is abelian of type $(2, 2)$ if $n = 2$ and isomorphic to D_{2^n} if $n > 2$. By the above, we have $\mathrm{cl}(M) = n$; then $\mathrm{Z}(M) = \mathrm{Z}(G)$. Since $\langle c, G'\rangle \cap \mathrm{Z}(G) = \Omega_1(G')$, we obtain $M = \langle c, G'\rangle\mathrm{Z}(G)$ by the product formula so $\mathrm{d}(M) = 3$.

As $(ac)^2 = aa^c \in \mathrm{Z}(G)$, we get $G' \cap \langle ac\rangle = \Omega_1(G')$ so $N = \langle ac\rangle G'$ is the third (metacyclic) member of the set Γ_1. Indeed, we have $N \neq B$ since $\exp(N) = 2^{n+1} > 2^n = \exp(B)$.[2]

[2]This agrees with the known result that a nonmetacyclic two-generator 2-group has an even number of metacyclic subgroups of index 2 (see Theorem 107.1).

As $\langle ac\rangle \cap \langle a\rangle = \{1\}$, we get $G = \langle ac\rangle\langle a\rangle$ by the product formula.

Since all members of the set Γ_1 are pairwise nonisomorphic, they are characteristic in G. It follows that $\mathrm{Aut}(G)$ is a 2-group.[3]

Let $\Delta = \{xx^c \mid x \in A\}$ be the diagonal subgroup of B. Then $\Delta = \mathrm{Z}(G)$.

Assume that G has an elementary abelian subgroup E of order 8. Then $G = BE$ so $E \cap B = \Omega_1(B) \cong \mathrm{E}_4$, $\mathrm{C}_G(E \cap B) \geq BE = G$ hence $E \cap B \leq \mathrm{Z}(G)$, a contradiction since $\mathrm{Z}(G) = \langle aa^c\rangle$ is cyclic. Thus E does not exist.

2^o. Let $G = M \operatorname{wr} C$, where M is a 2-group of maximal class and order > 8 and $C = \langle c\rangle \cong \mathrm{C}_2$. Set $B = M \times M^c$ (B is the base of G). Since

$$B' = M' \times (M')^c \leq G' \leq \Phi(G)$$

is G-invariant and $\Omega_1(G/B') = G/B'$, we deduce that $G' = \Phi(G)$. Therefore, since $\mathrm{d}(G) = 3$ (see the remark following Lemma A.27.1), we obtain $G/G' \cong \mathrm{E}_8$ hence $B' < G'$ (compare indices!). Next, $\Delta = \{xx^c \mid x \in M\}$ is the diagonal subgroup of B which is isomorphic to M and $\Delta < \Phi(G) = G'$ so that $\Delta M' \leq \Phi(G) = G'$. Clearly, $B' \cap \Delta$ has index 4 in Δ and $|G : B'| = 2^5$. It follows that $|G : \Delta B'| = 8 = |G : G'|$ whence $\Delta B' = G'$. Since $M' \cap \Delta = \{1\}$, the subgroup $\Delta \cdot M'$ is a semidirect product with kernel M' and has index $8 = |G : G'|$ in G. Thus $G' = \Delta \cdot M'$.

Assume that G possesses a normal subgroup $E \cong \mathrm{E}_8$. Clearly, $E \not\leq B$ since B has no normal elementary abelian subgroup of order 8 in view of $|M| > 8$. Then we have $E \cap B = \mathrm{Z}(B)$ so that $\mathrm{C}_G(\mathrm{Z}(B)) \geq BE = G$, and hence $\mathrm{Z}(B) = \mathrm{Z}(G)$ is noncyclic. Since $\mathrm{C}_B(c) = \Delta$, it follows that $\mathrm{Z}(G) < \Delta$ hence $\mathrm{Z}(G)$ is cyclic, and this is a contradiction. Thus E does not exist. In the case under consideration, the subgroup $Z \times Z^c$, where $Z < M$ is cyclic of index 2, is a G-invariant metacyclic subgroup, and we have $G/(Z \times Z^c) \cong \mathrm{D}_8$ since $Z \times Z^c \not\leq G'$ and $\Omega_1(G/(Z \times Z^c)) = G/(Z \times Z^c)$. Thus the result of Theorem 50.1 is best possible. Also, the result of Theorem 50.3 is also best possible.

3^o. In this subsection $G = Q \operatorname{wr} C$, where

$$Q = \langle a, b \mid a^{2^{n-1}} = 1,\ a^{2^{n-2}} = b^2,\ a^b = a^{-1}\rangle \cong \mathrm{Q}_{2^n}, \quad C = \langle c \mid c^2\rangle \cong \mathrm{C}_2.$$

We have

$$|G| = 2^{2n+1}, \quad \mathrm{Z}(G) = \langle b^2(b^2)^c\rangle, \quad |\mathrm{Z}(G)| = 2, \quad G = \langle a, b, c\rangle$$

and $\mathrm{d}(G) = 3$ by the remark following Lemma A.27.1. The subgroup $B = Q \times Q^c$ is the base of the wreath product G. Let $A = \langle a\rangle$; then $A_1 = A \times A^c$ is an abelian normal subgroup of G (indeed, A_1 is B-invariant and c-invariant and $G = \langle B, c\rangle$). It is easy to

[3] Another proof: If $\phi \in \mathrm{Aut}(G)$ is of odd order, then $\phi = \mathrm{id}_G$ for $n = 1$; if $n > 1$, then ϕ stabilizes the chain $G > \mathrm{Z}(G) > \{1\}$ so $\phi = \mathrm{id}_G$ again.

see that $G/A_1 \cong \mathrm{D}_8$ so $A_1 \not\leq \Phi(G)$. Since $(ac)^2 = aa^c$ is of order $2^{n-1} = \exp(B)$, we have $o(ac) = 2^n = \exp(G)$. We obtain that $(bc)^2 = bb^c \notin A_1$, $(bb^c)^c = bb^c$ so $\langle bb^c A_1\rangle = \mathrm{Z}(G/A_1)$. Set $T/A_1 = \langle bb^c A_1\rangle$. Then $T \lhd G$ and G/T is abelian of type $(2,2)$. By Exercise 1, $\mathrm{c}_1(G) = 2^n + 3$ and all involutions of the set $G - B$ are conjugate in G.

By the previous paragraph,

$$\mathrm{N}_1(G-B) = 2^n, \quad \mathrm{N}_1(G) = 2^n + 3, \quad \mathrm{sol}_1(G) = 2^n + 4.$$

Every element of $G - B$ can be presented uniquely in the form $z = xy^c c$ for some $x, y \in Q$. Note that $xy^c = y^c x$ for all $x, y \in Q$. We have

$$(xy^c c)^2 = xy^c cxy^c c = xy^c x^c y = (xy)(yx)^c, \tag{1}$$

$$(xy^c c)^{2^k} = (xy)^{2^{k-1}}((yx)^c)^{2^{k-1}}. \tag{1a}$$

Note that

$$\mathrm{sol}_1(Q) = 2 \quad \text{and, for } k > 1, \quad \mathrm{sol}_k(Q) = 2^{n-1} + 2^k. \tag{2}$$

It follows from (2) that

$$\mathrm{N}_2(B) = \mathrm{sol}_2(Q)^2 - \mathrm{sol}_1(Q)^2 = (2^{n-1} + 4)^2 - 4 = 2^{2(n-1)} + 2^{n+2} + 12 \tag{3}$$

and, for $2 < k < n$,

$$\mathrm{N}_k(B) = (2^{n-1} + 2^k)^2 - (2^{n-1} + 2^{k-1})^2 = (2^n + 3 \cdot 2^{k-1})2^{k-1}. \tag{4}$$

Now let $z = xy^c c \in G - B$, $x, y \in Q$ and $z^4 = 1$. Then, by (1), $(xy)^2 = 1$ so $x = y^{-1}u$, where $u^2 = 1$ and $u \in Q$, and we infer that $\mathrm{sol}_2(G-B) = 2|Q| = 2^{n+1}$ and hence

$$\mathrm{N}_2(G-B) = \mathrm{sol}_2(G-B) - \mathrm{sol}_1(G-B) = 2^n.$$

It follows that

$$\mathrm{N}_2(G) = 2^{2(n-1)} + 2^{n+2} + 2^n + 12 \tag{5}$$

so that

$$\mathrm{c}_2(G) = \frac{1}{2}\mathrm{N}_2(G) = 2^{2n-3} + 2^{n+1} + 2^{n-1} + 6.$$

Let $2 < k < n$, $z \in G - B$ with $z^{2^k} = 1$. Then we get $x = y^{-1}u$, where $u \in Q$ and $o(u) \leq 2^{k-1}$ (see (1a)). It follows that

$$\mathrm{sol}_k(G-B) = |Q|\mathrm{sol}_{k-1}(Q) = 2^n(2^{n-1} + 2^{k-1})$$

(see (2)). Then

$$\mathrm{N}_k(G-B) = 2^n(2^{n-1} + 2^{k-1}) - 2^n(2^{n-1} + 2^{k-2}) = 2^{n+k-2} \tag{6}$$

and we obtain

$$\begin{aligned} \mathrm{N}_k(G) &= \mathrm{N}_k(B) + \mathrm{N}_k(G-B) = (2^n + 3\cdot 2^{k-1})2^{k-1} + 2^{n+k-2} \\ &= 3(2^{n-1} + 2^{k-1})2^{k-1}, \\ \mathrm{c}_k(G) &= 3(2^{n-1} + 2^{k-1}) \quad (2 < k \le n). \end{aligned} \tag{7}$$

Since $\exp(G) = 2^n$, all elements of G of order 2^n lie in the set $G - B$ in view of $\exp(B) = 2^{n-1}$. If $o(xy^c c) = 2^n$, then $y = x^{-1}u$, where $u \in Q$ with $o(u) = 2^{n-1}$. It follows that the number of elements of order 2^n in G is equal to $|Q| \cdot 2^{n-2} = 2^{2n-2}$ so that

$$\mathrm{c}_n(G) = \frac{2^{2n-2}}{\varphi(2^n)} = 2^{n-1}.$$

We state the obtained results in the following

Proposition A.27.8. *Suppose that $G = Q \operatorname{wr} \mathrm{C}_2$, where $Q \cong \mathrm{Q}_{2^n}$. Then $G' = \Phi(G)$ is of index 8 in G and*

(a) $\mathrm{c}_1(G) = 2^n + 3$.

(b) $\mathrm{c}_2(G) = 2^{2n-3} + 2^{n+1} + 2^{n-1} + 6$.

(c) *If $2 < k < n$, then $\mathrm{c}_k(G) = 3 \cdot (2^{n-1} + 2^{k-1})$.*

(d) $\mathrm{c}_n(G) = 2^{n-1}$.

Exercise 2. Let $G = D \operatorname{wr} \mathrm{C}_2$ be a 2-group, where D has a cyclic subgroup of index 2. Find $\mathrm{c}_k(G)$ and describe all maximal subgroups of G.

Exercise 3. Let $G = A \operatorname{wr} \mathrm{C}_2$, where A is an arbitrary (finite) group, $\mathrm{C}_2 = \langle c \rangle$. Is it true that all involutions in the set $G - (A \times A^c)$ are conjugate in G?

Exercise 4. Let $G = M \operatorname{wr} \mathrm{C}_2$ be a 2-group, where M has a cyclic subgroup of index 2. Find $\mathrm{cl}(G)$.

Exercise 5. Consider the standard wreath product $G = E_1 \operatorname{wr} E_2$, where E_1, E_2 are elementary abelian groups of order 2^n, 2^m, respectively. Find $\mathrm{c}_1(G)$.

Exercise 6. Let A be a 2-group, $G = A \operatorname{wr} \mathrm{C}_{2^m}$. Express $\mathrm{c}_1(G)$ in terms of A.

Exercise 7. Let $G = A \operatorname{wr} \mathrm{C}_p$ be a p-group. Express $|G : G'|$ in terms of A.

Exercise 8. Let $G = M_1 \times M_2$, where M_1 and M_2 are 2-groups of maximal class. Find the number of subgroups of maximal class and given order in G.

Exercise 9. Let $G = M \operatorname{wr} \mathrm{C}_2$, where M is a 2-group of maximal class. Find the number of nonabelian subgroups of order 8 in G.

Exercise 10. Study the subgroup structure of the standard wreath product

$$G = \mathrm{E}_{2^n} \operatorname{wr} M,$$

where M is a 2-group of maximal class.

Exercise 11. Study the subgroup structure of $G = \mathrm{C}_{2^m} \operatorname{wr} \mathrm{C}_{2^n}$.

Exercise 12. Study the subgroup structure of the standard wreath product

$$G = \mathrm{C}_{2^n} \operatorname{wr} M,$$

where M is a 2-group of maximal class.

Exercise 13. Let $G = A \operatorname{wr} B$ be the standard wreath product. Is it true that G satisfies $\exp(G) = \exp(A) \cdot \exp(B)$?

Solution. Let $a \in A$, $b \in B$, $o(a) = m$, $o(b) = n$. Then

$$(ab)^n = aa^{b^{-1}} a^{b^{-2}} \cdot a^{b^{-(n-1)}}$$

is of order $o(a) = m$.

Exercise 14. Describe the structure of $\mathrm{Aut}(\mathrm{C}_{2^n} \operatorname{wr} \mathrm{C}_2)$.

Exercise 15. Describe the structure of $\mathrm{Aut}(Q \operatorname{wr} \mathrm{C}_2)$, where Q is a 2-group of maximal class.

Exercise 16. Let $G = \mathrm{C}_{p^n} \operatorname{wr} \mathrm{C}_p$. Describe the structure of $\Omega_1(G)$.

Exercise 17. Prove an analog of Proposition A.27.8 for the groups $G = \mathrm{D}_{2^n} \operatorname{wr} \mathrm{C}_2$ and $G = \mathrm{SD}_{2^n} \operatorname{wr} \mathrm{C}_2$.

Appendix 28

Nilpotent subgroups

1^o *Theorems of Sylow, Hall, Carter etc.* We prove Sylow's theorem in the following form:

Theorem A.28.1 (Sylow). *All maximal p-subgroups of a group G are conjugate and have order $|G|_p$, and their number is $\equiv 1 \pmod{p}$.*

A subgroup $P \leq G$ is a Sylow p-subgroup of G provided $|P|$ is a power of p and p does not divide $|G : P|$. According to Theorem A.28.1, the Sylow p-subgroups coincide with the maximal p-subgroups of G and are conjugate in G. Let $\mathrm{Syl}_p(G)$ denote the set of all Sylow p-subgroups of G and $\pi(G)$ be the set of the prime divisors of $|G|$.

Lemma A.28.2 (Cauchy). *If $p \in \pi(G)$, then G contains a subgroup of order p. In particular, a maximal p-subgroup of G is $> \{1\}$.*

Proof. Suppose that G is a counterexample of minimal order. Then G has no proper subgroup C of order divisible by p and $|G| \neq p$. If G has only one maximal subgroup, say M, then it is cyclic. Indeed, if $x \in G - M$, then $\langle x \rangle$ is not contained in M so we get $\langle x \rangle = G$. Then $\langle x^{o(x)/p} \rangle < G$ is of order p, a contradiction. If G is abelian and $A \neq B$ are maximal subgroups of G, then $G = AB$ so

$$|G| = \frac{|A||B|}{|A \cap B|},$$

and p does not divide $|G|$, a contradiction. In case that G is nonabelian, we obtain that $|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} h_i$, where $h_1, \ldots, h_k$ are sizes of noncentral G-classes. Since the h_i are indices of proper subgroups in G, we see that p divides h_i for all i. Then p divides $|\mathrm{Z}(G)|$ so $\mathrm{Z}(G)$ contains an element of order p, and hence G is not a counterexample. □

The set $\mathcal{S} = \{A_i\}_{i=1}^{n}$ of subgroups of a group G is said to be *G-invariant* if $A_i^x \in \mathcal{S}$ for all $i \leq n$ and $x \in G$. All members of a G-invariant set $\mathcal{S}$ are conjugate if and only if $\mathcal{S}$ has no nonempty proper G-invariant subset.

Lemma A.28.3. *Let $\mathcal{S} \neq \varnothing$ be a G-invariant set of subgroups of a group G. Suppose that whenever $\mathcal{N} \neq \varnothing$ is a G-invariant subset of $\mathcal{S}$, then $|\mathcal{N}| \equiv 1 \pmod{p}$. Then all members of the set $\mathcal{S}$ are conjugate in G.*

Proof. Assume that $\mathcal{S}$ has a proper G-invariant subset $\mathcal{N} \neq \varnothing$. Then $\mathcal{S} - \mathcal{N} \neq \varnothing$ is G-invariant so

$$|\mathcal{S}| = |\mathcal{N}| + |\mathcal{S} - \mathcal{N}| \equiv 1 + 1 \not\equiv 1 \pmod{p},$$

a contradiction. Thus $\mathcal{S}$ is a minimal G-invariant subset so all its members are conjugate in G. □

Let P be a maximal p-subgroup of a group G and P_1 be a p-subgroup of G. In case $PP_1 \leq G$, we see that PP_1 is a p-subgroup by the product formula, and we conclude that $P_1 \leq P$. If P_1 is a maximal p-subgroup of G, then $\mathrm{N}_P(P_1) = P \cap P_1$.

Proof of Theorem A.28.1. One may assume that p divides $|G|$. Let

$$\mathcal{S}_0 = \{P = P_0, P_1, \ldots, P_r\}$$

be a G-invariant set of all maximal p-subgroups of G; then we have $P_i > \{1\}$ for all i (Lemma A.28.2). Let $r > 0$ and let P act on the set $\mathcal{S}_0 - \{P\}$ via conjugation. Then the size of every P-orbit on the set $\mathcal{S}_0 - \{P\}$ is a power of p greater than 1 because the P-stabilizer of a 'point' P_i is equal to $P \cap P_i < P$. Thus p divides r hence

$$|\mathcal{S}_0| = r + 1 \equiv 1 \pmod{p},$$

and the first assertion follows (Lemma A.28.3). Then p does not divide $|G : \mathrm{N}_G(P)|$. Since P is a maximal normal p-subgroup of $\mathrm{N}_G(P) = N$, the prime p does not divide $|N/P|$ (Lemma A.28.2) whence p does not divide $|G : N||N : P| = |G : P|$, i.e., $|P| = |G|_p$. □

A standard statement of Sylow's theorem is as follows:

(a) A group G contains a subgroup of order $|G|_p$.

(b) The number of subgroups from (a) is $\equiv 1 \pmod{p}$.

(c) All maximal p-subgroups of G have order $|G|_p$.

Remark 1. (1) (Frobenius) Let P be a p-subgroup of a group G and suppose that the set $\mathcal{M} = \{P_1, \ldots, P_r\} \subset \mathrm{Syl}_p(G)$ is P-invariant and $P \not\leq P_i$ for all i. Then we obtain that $|\mathcal{M}| \equiv 0 \pmod{p}$ (let P act on $\mathcal{M}$ via conjugation) so, by Theorem A.28.1, the number of Sylow p-subgroups of G containing P is $\equiv 1 \pmod{p}$ (indeed, take as $\mathcal{M}$ the set of all Sylow p-subgroups not containing P). Similarly, if $P \in \mathrm{Syl}_p(G)$, then the number of p-subgroups of G of given order that are not contained in P is divisible by p (let P act on the set of the above p-subgroups!).

(2) (Frobenius) Let $\mathcal{M} = \{M_1, \ldots, M_s\}$ be the set of all subgroups of order p^k in a group G of order p^m, $k < m$. We claim that $s = |\mathcal{M}| \equiv 1 \pmod{p}$. To prove this, we use induction on m. Let $\Gamma_1 = \{G_1, \ldots, G_r\}$ be the set of all maximal subgroups of G. Because the number of subgroups of index p in the elementary abelian p-group

$G/\Phi(G)$ of order, say p^d, is equal to

$$\frac{p^d-1}{p-1} = 1 + p + \cdots + p^{d-1} \equiv 1 \pmod{p},$$

we get $r = |\Gamma_1| \equiv 1 \pmod{p}$, so one may assume that $k < m-1$. Let α_i be the number of members of the set $\mathcal{M}$ contained in G_i and β_j the number of members of the set Γ_1 containing M_j for all i, j. Then, by double counting,

$$\alpha_1 + \cdots + \alpha_r = \beta_1 + \cdots + \beta_s,$$

By the above, $r \equiv 1 \pmod{p}$, and by induction, $\alpha_i \equiv 1 \pmod{p}$ for all i. Next, β_j is the number of maximal subgroups in $G/M_j\Phi(G)$ so $\beta_j \equiv 1 \pmod{p}$ for all j. By the displayed formula, $|\mathcal{M}| = s \equiv r \equiv 1 \pmod{p}$.

(3) (Frobenius; see also [Bur, Theorem 9.II]) It follows from (1) and (2) that the number of p-subgroups of order p^k in a group G of order $p^k m$ is $\equiv 1 \pmod{p}$.

(4) Suppose that the subsets $\mathcal{S}_1, \mathcal{S}_2 \subset \mathrm{Syl}_p(G)$ are nonempty and disjoint. Further, let $P_i \in \mathcal{S}_i$ be such that the set $\mathcal{S}_i$ is P_i-invariant, $i = 1, 2$; then $|\mathcal{S}_i| \equiv 1 \pmod{p}$, $i = 1, 2$ (see the proof of Theorem A.28.1). It follows that $\mathcal{S}_2$ is not P_1-invariant (otherwise, considering the action of P_1 on $\mathcal{S}_2$ via conjugation, we get $|\mathcal{S}_2| \equiv 0 \pmod{p}$ since $P_1 \notin \mathcal{S}_2$).

(5) (Burnside) Let G be a non-p-closed group (i.e., we have $\mathrm{O}_p(G) \notin \mathrm{Syl}_p(G)$) and $P \in \mathrm{Syl}_p(G)$. Suppose that $Q \in \mathrm{Syl}_p(G) - \{P\}$ is such that $D = P \cap Q$ is a maximal, by inclusion, intersection of Sylow p-subgroups of G. Assume that $D > \{1\}$. We claim that $N = \mathrm{N}_G(D)$ is not p-closed. Assume that this is false. Then $P_1 \in \mathrm{Syl}_p(N)$ is nonnormal in N. It follows from the properties of p-groups that $P \cap P_1 > D$ and $Q \cap P_1 > D$ so P_1 is not contained in P. Therefore, if $P_1 \leq U \in \mathrm{Syl}_p(G)$, then we get $U \neq P$. However, $P \cap Q = D < P \cap P_1 \leq P \cap U$, a contradiction.

The following assertion is easily checked. If R is an abelian minimal normal subgroup of a group G and $G = HR$, where $H < G$, then H is maximal in G and we have $H \cap R = \{1\}$.

Theorem A.28.4 (P. Hall [Hal1]). *If π is a set of primes, then all maximal π-subgroups of a solvable group G are conjugate.*

By Theorems A.28.1 and A.28.4, a maximal π-subgroup of a solvable group G is its π-Hall subgroup, and this gives the standard form of Hall's theorem. Let $\mathrm{Hall}_\pi(G)$ be the set of all π-Hall subgroups of G.

Given $H \leq G$, the subgroup

$$H_G = \bigcap_{x \in G} H^x$$

is said to be the *core* of H in G.

The proofs of Theorems A.28.4, A.28.6 and A.28.7 are based on the following

Lemma A.28.5 ([Ore]). *If distinct maximal subgroups F and H of a solvable group $G > \{1\}$ have equal cores, then they are conjugate in G.*

Proof. One may assume that $F_G = \{1\}$; then G is not nilpotent (otherwise, $|G|$ is a prime and $F = H = \{1\}$). Let R be a minimal normal, say a p-subgroup, of G; then we have $RF = G = RH$, $R \cap F = \{1\} = R \cap H$. Let K/R be a minimal normal, say a q-subgroup, of G/R, q is a prime. In this case, K is nonnilpotent (otherwise, we get $\mathrm{N}_G(K \cap F) > F$ and so $\{1\} < K \cap F \leq F_G = \{1\}$, contrary to the assumption) whence $q \neq p$. Then, by the product formula, $F \cap K$ and $H \cap K$ are nonnormal Sylow q-subgroups of K hence they are conjugate in K (Theorem A.28.1) so are in G. It follows that then $\mathrm{N}_G(F \cap K) = F$ and $\mathrm{N}_G(H \cap K) = H$ are also conjugate in G, as was to be shown. □

Proof of Theorem A.28.4.[1] We use induction on $|G|$. Let F and H be maximal π-subgroups of G and R a minimal normal, say p-subgroup, of G. If $p \in \pi$, then $R \leq F$ and $R \leq H$ by the product formula, and F/R, H/R are maximal π-subgroups of G/R so they are conjugate by induction; then F and H are also conjugate. Now assume that $\mathrm{O}_\pi(G) = \{1\}$; then $p \in \pi'$. Let F_1/R, H_1/R be maximal π-subgroups of G/R containing FR/R, HR/R, respectively; then we get $F_1^x = H_1$ for some $x \in G$ and $F_1/R, H_1/R \in \mathrm{Hall}_\pi(G/R)$ by induction.

Assume that $F_1 < G$. Then, by induction, we obtain $F \in \mathrm{Hall}_\pi(F_1)$ as a maximal π-subgroup of F_1 so $F_1 = F \cdot R$. Similarly, $H_1 = H \cdot R$. Therefore $F^x \in \mathrm{Hall}_\pi(H_1)$. Then $H = (F^x)^y = F^{xy}$ for some $y \in H_1$ by induction, and we are done.

Now let $F_1 = G$; then G/R is a π-group. Suppose that K/R is a minimal normal, say a q-subgroup, of G/R; then $q \in \pi$ hence $q \neq p (\in \pi')$. Let $Q \in \mathrm{Syl}_q(K)$; then we have $K = Q \cdot R$. By the Frattini argument,

$$G = \mathrm{N}_G(Q)K = \mathrm{N}_G(Q)QR = \mathrm{N}_G(Q)R$$

hence $\mathrm{N}_G(Q) \in \mathrm{Hall}_\pi(G)$ is maximal in G. Assume $FR < G$; then $F \notin \mathrm{Hall}_\pi(G)$. In this case, $\mathrm{N}_G(Q) \cap FR$, as a π-Hall subgroup of FR (product formula!), is conjugate with F, contrary to the choice of F. Thus $FR = HR = G$ and $F_G = \{1\} = H_G$ by assumption; then F and H are maximal in G (see the paragraph preceding the statement of the theorem). In this case, by Lemma A.28.5, F and H are conjugate in G. □

Let us prove, for completeness, by induction on $|G|$ that a group G is solvable if it has a p'-Hall subgroup for all $p \in \pi(G)$ (Hall–Chunikhin). Let $G_{p'} \in \mathrm{Hall}_{p'}(G)$, where $p' = \pi(G) - \{p\}$, and let $q \in p'$. If $G_{q'} \in \mathrm{Hall}_{q'}(G)$, then we conclude that $G_{p'} \cap G_{q'} \in \mathrm{Hall}_{q'}(G_{p'})$ by the product formula, so $G_{p'}$ is solvable by induction. Let R be a minimal normal, say an r-subgroup, of $G_{p'}$; then $r \in p'$. In view of Burnside's two-prime theorem, we may assume that $|\pi(G)| > 2$, so there exists $s \in \pi(G) - \{p, r\}$. Let $G_{s'} \in \mathrm{Hall}_{s'}(G)$; then we have $G = G_{p'}G_{s'}$. By Theorem A.28.1, one may assume

[1] This proof is independent of the Schur–Zassenhaus theorem. See also Theorem A.43.5.

that $R < G_{s'}$; then we get $R \leq (G_{s'})_G$. Next, $(G_{s'})_G$ is solvable as a subgroup of $G_{s'}$. Thus G has a minimal normal, say an r-subgroup, which we denote by R again. In case $R \in \mathrm{Syl}_r(G)$, we conclude that $G/R \cong G_{r'}$ is solvable so is G. If $R \notin \mathrm{Syl}_r(G)$, then $G_{r'}R/R \in \mathrm{Hall}_{r'}(G/R)$. Let $q \in \pi(G) - \{r\}$; then $R < G_{q'}$ so $G_{q'}/R \in \mathrm{Hall}_{q'}(G/R)$. In this case, by induction, G/R is solvable, and the proof is complete.

A subgroup K is said to be a *Carter subgroup* (= C-subgroup) of G if it is nilpotent and coincides with its normalizer in G.

Theorem A.28.6 (Carter [Car]). *A solvable group G possesses a* C*-subgroup and all C-subgroups of G are conjugate.*

Proof. We use induction on $|G|$. One may assume that G is not nilpotent. Let R be a minimal normal, say p-subgroup, of G.

Existence. By induction, G/R contains a C-subgroup S/R so $\mathrm{N}_G(S) = S$. Let T be a p'-Hall subgroup of S (Theorem A.28.4); then TR is normal in S since TR/R is a p'-Hall subgroup in the nilpotent subgroup S/R, and $S = T \cdot P$, where $P \in \mathrm{Syl}_p(S)$. One may assume that $T > \{1\}$ (otherwise, we see that $S = P$ is a C-subgroup of G). Set $K = \mathrm{N}_S(T)$; then $K = T \times \mathrm{N}_P(T)$ is nilpotent and $KR = S$ (Theorem A.28.4 and the Frattini argument). If $y \in \mathrm{N}_S(K)$, then $y \in \mathrm{N}_S(T) = K$ since T is characteristic in K, and so $\mathrm{N}_S(K) = K$. If $x \in \mathrm{N}_G(K)$, then $x \in \mathrm{N}_G(KR) = \mathrm{N}_G(S) = S$ so $x \in \mathrm{N}_S(K) = K$, and hence K is a C-subgroup of G.

Conjugacy. Let K, L be C-subgroups of G; then KR/R, LR/R are C-subgroups of G/R so, by induction, $LR = (KR)^x$ for some $x \in G$, and we have $K^x \leq LR$. One may assume that R is not contained in K (otherwise, $K^x = LR$ so $R < L = \mathrm{N}_G(L)$ since LR is nilpotent, and we obtain $K^x = L$, as desired); then RK is nonnilpotent whence R is not contained in L. If $LR < G$, then $(K^x)^y = L$ for $y \in LR$ by induction, and we are done. Now let $G = LR$; then $G = KR$ (recall that $(KR)^x = LR$) so G/R is nilpotent, and this is true for each choice of R. Thus R is the unique minimal normal subgroup of G so K and L are maximal in G and $K_G = L_G$. Then K and L are conjugate in G (Lemma A.28.5). □

Theorem A.28.7. *Let $G = N_1 \dots N_k$ be a nonnilpotent group, where $N_1, \dots, N_k$ are proper pairwise permutable and nilpotent subgroups. Then there exists an index $i \leq k$ such that the normal closure $N_i^G < G$.*

Lemma A.28.8 ([Ore]). *If $G = AB$, where $A, B < G$, then A and B are not conjugate.*

Proof. Assume that $B = A^g$ for $g \in G$. Then $g = ab$, $a \in A$ and $b \in B$, so we obtain $B = A^{ab} = A^b$ and $A = B^{b^{-1}} = B$, $G = A$, a contradiction. □

Proof of Theorem A.28.7.[2] Assume that G is a minimal counterexample. Then G is nonnilpotent. By [Wiel2] and [Keg1], G is solvable. Let $R < G$ be a minimal normal

[2] For $k = 2$, Theorem A.28.7 was proved by Janko and Kegel [Keg1], independently.

subgroup, say a p-subgroup; then we have $G/R = (N_1R/R)\dots(N_kR/R)$, where all N_iR/R are nilpotent.

If G/R is not nilpotent, we get $(N_iR)^G < G$ for some i by induction so $N_i^G < G$.

Now let G/R be nilpotent. Then, by hypothesis, we get $N_iR = G$ for all i so N_i is maximal in G and $(N_i)_G = \{1\}$ for all i. Therefore $N_1N_2 = G$. By Lemma A.28.5, N_1 and N_2 are conjugate in G, contrary to Lemma A.28.8. □

Exercise 1. If K, L are distinct Carter subgroups of a solvable group G, then we have $KL \neq LK$.

Solution. Write $M = \langle K, L\rangle$. Then K, L, being Carter subgroups of M, are conjugate in M (Theorem 28.6) so they are not permutable by Theorem 28.8.

Exercise 2. (a) Let $K, L < G$, where G is an arbitrary group. If K and L are conjugate in $\langle K, L\rangle$, then $KL \neq LK$. (This is restatement of Lemma 28.8.)

(b) Suppose that $K \leq H < G$, where K is a Carter subgroup of a solvable group G and $x \in G - H$. Is it true that $HH^x \neq H^xH$?

Exercise 3. Let G be solvable and $H < G$ be such that all subgroups of G containing H coincide with their normalizers and $x \in G - H$. Is it true that $HH^x \neq H^xH$?

Supplement 1 to Lemma A.28.5. *If for arbitrary maximal subgroups F and H of a group G with equal cores we have $\pi(|G:F|) = \pi(|G:H|)$, then G is solvable.*

Proof. Assume that G is a minimal counterexample. As the hypothesis is inherited by epimorphic images, G has only one minimal normal subgroup R, and G/R is solvable so R is nonsolvable (the equality $R = G$ is possible). Let $p \in \pi(R)$, $P \in \mathrm{Syl}_p(R)$ and $\mathrm{N}_G(P) \leq F < G$, where F is maximal in G. By Frattini's lemma, $G = RF$ so $|G:F| = |R:(F \cap R)|$ and $p \notin \pi(|G:F|)$. Let $q \in \pi(|R:(F \cap R|)$; then $q \neq p$. Take $Q \in \mathrm{Syl}_q(R)$ and let $\mathrm{N}_G(Q) \leq H < G$, where H is maximal in G. Then we get $FR = G = HR$ so $F_G = \{1\} = H_G$. However, $q \in \pi(|G:F|)$ and $q \notin \pi(|G:H|)$, a contradiction. □

A group G is said to be *p-solvable*, if every its composition factor is either a p- or p'-number.

Supplement 2 to Lemma A.28.5. *Suppose that G is a p-solvable group with minimal normal p-subgroup R. Assume that G possesses a maximal subgroup H that satisfies $H_G = \{1\}$. Then all maximal subgroups of G with core $\{1\}$ are conjugate.*

Proof. By hypothesis, we have $|\pi(G)| > 1$. Let F be another maximal subgroup of G with $F_G = \{1\}$; then $G = FR = HR$ and $F \cap R = \{1\} = H \cap R$. If $R \in \mathrm{Syl}_p(G)$, we are done (Schur–Zassenhaus). Now let $p \in \pi(G/R)$; then G/R is not simple. Let K/R be a minimal normal subgroup of G/R. Then, as in the proof of Lemma A.28.5, $|\pi(K)| > 1$ so, taking into account that $H_G = \{1\}$ and G/R is p-solvable, we conclude that K/R is a p'-subgroup. In that case, $F \cap K$ and $H \cap K$ as p'-Hall subgroups

of K are conjugate in K so in G (Schur–Zassenhaus) whence $F = \mathrm{N}_G(F \cap K)$ and $H = \mathrm{N}_G(H \cap K)$ are also conjugate in G. □

Supplement 3 to Lemma A.28.5 ([Gas4]). *Let M be a minimal normal subgroup of a solvable group G. Suppose that K^1 and K^2 are complements of M in G such that $K^1 \cap \mathrm{C}_G(M) = K^2 \cap \mathrm{C}_G(M)$. Then K^1 and K^2 are conjugate in G.*

Proof (compare with [Weh, Theorem 3.7]). From $K^i M = G$ we conclude that K^i is maximal in G, $i = 1, 2$. We have $K^i \cap M = \{1\}$ so that $(K^i)_G \leq \mathrm{C}_G(M)$, $i = 1, 2$. By the modular law, we get $\mathrm{C}_G(M) = M \times \mathrm{C}_{K^i}(M)$; then $K^i \cap \mathrm{C}_G(M) = \mathrm{C}_{K^i}(M)$ so $\mathrm{C}_{K^1}(M) = \mathrm{C}_{K^2}(M)$ by hypothesis, and hence $\mathrm{C}_{K^i}(M) = (K^i)_G$, $i = 1, 2$. Then $(K^1)_G = (K^2)_G$ so K^1 and K^2 are conjugate in G by Lemma A.28.5. □

2^o *Groups with a cyclic Sylow p-subgroup.* Here we prove two results on groups with a cyclic Sylow p-subgroup.

Theorem A.28.9 (compare with [Wiel3]). *Let $P \in \mathrm{Syl}_p(G)$ be cyclic. If $H \lhd G$ and p divides* $\mathrm{GCD}(|H|, |G : H|)$*, then H is p-nilpotent and G is p-solvable.*

Remark 2. Suppose that $P \in \mathrm{Syl}_p(G)$ is cyclic.

(1) Suppose, in addition, that $p \mid |\mathrm{Z}(G)|$. Set $N = \mathrm{N}_G(P)$. Since N has no minimal nonnilpotent subgroup S satisfying $S' \in \mathrm{Syl}_p(S)$ (Lemma 10.8), it follows that N is p-nilpotent so $P \leq \mathrm{Z}(N)$. In this case, G is p-nilpotent (Burnside's normal p-complement theorem).

(2) Suppose that G, p, P and H are given as in Theorem A.28.9 and assume that the subgroup $P_1 = P \cap H (\in \mathrm{Syl}_p(H))$ is normal in H so in G. Let $T \in \mathrm{Hall}_{p'}(H)$ (Schur–Zassenhaus); then, by Schur–Zassenhaus and Frattini,

$$H = P_1 T, \quad G = H\mathrm{N}_G(T) = P_1 T \mathrm{N}_G(T) = P_1 \mathrm{N}_G(T).$$

It follows from the last equality, the cyclicity of P and $P_1 < P$ that $\mathrm{N}_G(T) = G$. Thus $T \lhd G$ so $H = P_1 \times T$ is p-decomposable.

(3) If $\{1\} < H < G$ are arbitrary and $R \leq \Phi(H)$ is normal in G, then $R \leq \Phi(G)$. Indeed, assuming that this is false, we get $G = RM$ for some maximal subgroup M of G. Then, by the modular law, we get $H = R(H \cap M)$ so $H = H \cap M$ and $R < H \leq M$, a contradiction.

(4) If $H \lhd G$ are arbitrary and $G = AH$, where A is as small as possible, then we have $A \cap H \leq \Phi(A)$. Indeed, if this is false, then $A = B(A \cap H)$, where $B < A$ is maximal. Then $G = AH = B(A \cap H)H = BH$, contrary to the choice of A.

Proof of Theorem A.28.9. By the product formula, we have $P_1 = P \cap H \in \mathrm{Syl}_p(H)$. Set $N = \mathrm{N}_G(P_1)$; then $P \leq N$. Further, set $N_1 = \mathrm{N}_H(P_1) = N \cap H$. Then, by Remark 2(2) applied to the pair $N_1 < N$, we get $N_1 = P_1 \times T$, where $T \in \mathrm{Hall}_{p'}(N_1)$, and so H is p-nilpotent (Burnside's normal p-complement theorem).[3] By Frattini's

[3] Since $H \cap P \leq \Phi(P)$, it follows, by the deep Tate's theorem [Hup, Satz 4.4.7], that H is p-nilpotent.

lemma, $G = HN$ so $G/H \cong N/(N \cap H) = N/N_1$. Therefore it remains to prove that N/N_1 is p-solvable. To this end, we may assume that $N = G$; then P_1 is normal in G. In this case, $G/\mathrm{C}_G(P_1)$ as a p'-subgroup of $\mathrm{Aut}(P_1)$ is cyclic of order dividing $p-1$. By Remark 2(1), we see that $\mathrm{C}_G(P_1)$ is p-nilpotent, and we conclude that G is p-solvable. □

Theorem A.28.10 ([Hal3, Theorem 4.61]). *If $P \in \mathrm{Syl}_p(G)$ is cyclic of order p^m and $k \leq m$, then $\mathrm{c}_k(G) \equiv 1 \pmod{p^{m-k+1}}$.*

Proof. Let $\mathcal{C} = \{Z_1, \ldots, Z_r\}$ be the set of all subgroups of order p^k in G not contained in P. Let P act on the set $\mathcal{C}$ via conjugation. Then the P-stabilizer of Z_i equals $P \cap Z_i$ which is of order p^{k-1} at most. Thus $r = |\mathcal{C}| \equiv 0 \pmod{p^{m-(k-1)}}$. □

3^o *Subgroup generated by some minimal nonabelian subgroups.* Let $p \in \pi(G)$ and let $\mathcal{A}_p(G)$ be the set of all minimal nonabelian subgroups A of an arbitrary (finite) group G such that A' is a p-subgroup (in this case, A is either a p-group or p-closed and minimal nonnilpotent). Set

$$\mathrm{L}_p(G) = \langle H \mid H \in \mathcal{A}_p(G) \rangle \quad \text{and} \quad \mathrm{L}(G) = \prod_{p \in \pi(G)} \mathrm{L}_p(G).$$

It is known (Exercise 10.6 and Theorem 10.28) that $\mathrm{L}(G) = G$ if G is a nonabelian p-group and $G' \leq \mathrm{L}(G)$ for arbitrary G.

Theorem A.28.11. *Given an arbitrary group G, the quotient group $G/\mathrm{L}_p(G)$ is p-nilpotent. Moreover, if $p \mid |G/\mathrm{L}_p(G)|$, then the Sylow p-subgroups of G are abelian.*

Proof. Take $P \in \mathrm{Syl}_p(G)$. One may assume that P is not contained in $\mathrm{L}_p(G)$. Then P is abelian (Theorem 10.28), proving the last assertion. Assume that $G/\mathrm{L}_p(G)$ is not p-nilpotent. Then $G/\mathrm{L}_p(G)$ has a minimal nonnilpotent subgroup $H/\mathrm{L}_p(G)$ such that $(H/\mathrm{L}_p(G))'$ is a p-subgroup (Frobenius' normal p-complement theorem; see Lemma 10.8). Let $T \leq H$ be minimal such that $T\mathrm{L}_p(G) = H$; then $T \cap \mathrm{L}_p(G) \leq \Phi(T)$ by Remark 2(4), and $T/(T \cap \mathrm{L}_p(G)) \cong H/\mathrm{L}_p(G)$. Using the properties of Frattini subgroups, we get $T = Q \cdot P_0$, where $P_0 = T' \in \mathrm{Syl}_p(T)$, $Q \in \mathrm{Syl}_q(T)$ is cyclic and $|Q : (Q \cap \mathrm{Z}(T))| = q$. Since P_0 is abelian and the indices of minimal nonabelian subgroups in T are not multiples of q and Sylow q-subgroups generate T, we obtain that $T = \mathrm{L}_p(T) \leq \mathrm{L}_p(G)$, which is a contradiction. □

4^o *Characterization of p-nilpotent groups.* We need the following

Lemma A.28.12. *Suppose that a p-subgroup P_0 is normal in a group G. If, for each $x \in P_0$, $|G : \mathrm{C}_G(x)|$ is a power of p, then we have $P_0 \leq \mathrm{H}(G)$, the hypercenter of G (= the last member of the upper central series of G; in some cases, this subgroup is denoted by $Z_\infty(G)$).*

Proof. Suppose that $P_0 \leq P \in \mathrm{Syl}_p(G)$ and $x \in (P_0 \cap \mathrm{Z}(P))^{\#}$; then $x \in \mathrm{Z}(G)$ by hypothesis. Set $X = \langle x \rangle$. Take $yX \in (P_0/X)^{\#}$ and set $Y = \langle y, X \rangle$. Let $r \in \pi(G) - \{p\}$

and $R \in \mathrm{Syl}_r(\mathrm{C}_G(y))$; then $R \in \mathrm{Syl}_r(G)$ by hypothesis, so R centralizes $Y = \langle y, X\rangle$. It follows that $RX/X \leq \mathrm{C}_{G/X}(yX)$ so r does not divide $d = |(G/X) : \mathrm{C}_{G/X}(yX)|$. Since $r \neq p$ is arbitrary, d is a power of p, and the pair $P_0/X \leq G/X$ satisfies the hypothesis. By induction on $|G|$, we get $P_0/X \leq \mathrm{H}(G/X)$. Since $X \leq \mathrm{Z}(G)$, we obtain $P_0 \leq \mathrm{H}(G)$. □

Recall the following known fact. If $G = AB$, $B_0 \lhd B$ and $B_0 < A$, then $B_0 \leq A_G$. Indeed,

$$A_G = \bigcap_{x \in B} A^x \geq B_0.$$

Remark 3 (Wielandt). Let $x \in G^{\#}$ be a p-element and $|G : \mathrm{C}_G(x)|$ be a power of p. Then we have $G = \mathrm{C}_G(x)P$, where $x \in P \in \mathrm{Syl}_p(G)$, and so $x \in P_G = \mathrm{O}_p(G)$ (see the paragraph preceding this remark).

Theorem A.28.13 ([BK]). *Set $\mu_p = 1$ for $p > 2$ and $\mu_2 = 2$. If $|G : \mathrm{C}_G(x)|$ is a power of p for each p-element x of order $\leq p^{\mu_p}$, then the group G is p-nilpotent.*

Proof. By Remark 3, the subgroup $\mathrm{O}_p(G)$ contains all p-elements of orders $\leq p^{\mu_p}$ in G. Assume that G is not p-nilpotent. Then G has a minimal nonnilpotent subgroup S such that $S' \in \mathrm{Syl}_p(S)$ (Frobenius' normal p-complement theorem). Let a be a generator of a nonnormal, say, q-Sylow subgroup of S. Then $S\mathrm{O}_p(G) = \langle a\rangle \mathrm{O}_p(G)$ since $S' \leq \mathrm{O}_p(G)$ and $\exp(S') \leq p^{\mu_p}$ (Lemma 10.8). Let T be the Thompson critical subgroup of $\mathrm{O}_p(G)$ (see Theorem 14.1). Then a induces a nonidentity automorphism on T so $\langle a\rangle T$ contains a minimal nonnilpotent subgroup which we denote by S again. Since $T/\mathrm{Z}(T)$ is elementary abelian, it follows that $\exp(T') \leq p$. Set $P_0 = \Omega_{\mu_p}(T)$; then $\exp(P_0) \leq p^{\mu_p}$. It follows from $P_0 \leq \mathrm{H}(G)$ (Lemma A.28.12) that a centralizes P_0, a contradiction since $S' \leq P_0$. □

5^o *On a factorization theorem of Wielandt–Kegel.* Wielandt and Kegel [Wiel2, Keg1] have proved that a group $G = AB$, where A and B are nilpotent, is solvable. Below, using the Odd Order Theorem, we prove the following

Theorem A.28.14 ([Ber45]). *Consider a group $G = AB$, where $\mathrm{GCD}(|A|, |B|) = 1$. Let $A = P \times L$, where $P \in \mathrm{Syl}_2(G)$, and let B be nilpotent. Then G is solvable.*

In the proof of Theorem A.28.14 we use the Odd Order Theorem.

Recall that a subgroup K of $G = AB$ is said to be *factorized* (in G) if K is of the from $K = (K \cap A)(K \cap B)$. If, in addition, $\mathrm{GCD}(|A|, |B|) = 1$ and K is normal in G, then K is always factorized (apply the product formula!).

Lemma A.28.15 ([Wiel2]). *Let $G = AB$, $\mathrm{GCD}(|A|, |B|) = 1$, A_0 be normal in A and B_0 be normal in B. Then the subgroups $H = \langle A_0, B_0\rangle$ and $\mathrm{N}_G(H)$ are factorized.*

Proof. Let $x = ab^{-1} \in \mathrm{N}_G(H)$ ($a \in A$, $b \in B$); then $H^a = H^{xb} = H^b$. We have

$$A_0 = A_0^a \leq H^a, \quad B_0 = B_0^b \leq H^b = H^a$$

hence $H = \langle A_0, B_0\rangle \leq H^a = H^b$. It follows that

$$H^a = H = H^b, \quad a \in \mathrm{N}_A(H) = \mathrm{N}_G(H) \cap A, \quad b \in \mathrm{N}_B(H) = \mathrm{N}_G(H) \cap B$$

hence

$$\mathrm{N}_G(H) \leq (\mathrm{N}_G(H) \cap A)(\mathrm{N}_G(H) \cap B) \leq \mathrm{N}_G(H),$$

and so $\mathrm{N}_G(H)$ is factorized. Next, H is normal in $\mathrm{N}_G(H)$ and

$$\mathrm{GCD}(|\mathrm{N}_G(H) \cap A|, |\mathrm{N}_G(H) \cap B|) \leq \mathrm{GCD}(|A|, |B|) = 1$$

so

$$H = (H \cap \mathrm{N}_G(H) \cap A)(H \cap \mathrm{N}_G(H) \cap B) = (H \cap A)(H \cap B),$$

completing the proof. □

If K and L are Hall subgroups of a solvable group X, then we have $KL^u = L^u K$ for some $u \in X$. Indeed, set $\sigma = \pi(K) \cup \pi(L)$ and let $K \leq H$, where $H \in \mathrm{Hall}_\sigma(X)$. By Theorem A.28.4, $L^u \leq H$ for some $u \in X$. Now, $KL^u = H$ by the product formula.

Lemma A.28.16 (Wielandt). *Suppose that $A, B < G$ satisfy $AB^g = B^g A$ for all elements $g \in G$. If $G = A^G B = AB^G$, then $G = AB^g$ for some $g \in G$.*

Proof. Suppose that A is not normal in G (otherwise, $G = A^G B = AB = AB^1$). Then $A \neq A^x$ for some $x = b^g$, where $b \in B$ and $g \in G$. We have

$$A < A^* = \langle A, A^x\rangle \quad \text{and} \quad A^* B^g = B^g A^*$$

for all $g \in G$. Working by induction on $|G : A|$, we get $G = A^* B^g$. However,

$$A^* B^g = \langle A, A^x, B^g\rangle = \langle A, B^g\rangle = AB^g$$

since $x \in B^g$. □

Remark 4 ([Keg1]). If $A, B < G$ and $AB^g = B^g A < G$ for all $g \in G$, then either $A^G < G$ or $B^G < G$. Indeed, if $A^G = G = B^G$, then we have $G = AB^g$ for some $g \in G$ (Lemma A.28.16), contrary to the hypothesis.

Exercise 1. Suppose that A is a proper subgroup of a group G such that $AA^x = A^x A$ for all $x \in G$. Then A is subnormal in G.

Solution. If $y, z \in G$, then

$$A^y A^z = (A^{yz^{-1}} A)^z = (AA^{yz^{-1}})^z = A^z A^y.$$

In case $B = A^y A^z$, it is easy to see that we have $BB^x = B^x B$ for all $x \in G$. Assume that $A^x \neq A$ for some $x \in G$ (otherwise, there is nothing to prove). Then we obtain that $B = AA^x > A$. Using induction on $|G : A|$, we see that B is subnormal in G. By Lemma 28.8, $B < G$. Therefore, again by induction, we see that A is subnormal in B; then A is subnormal in G, as was to be shown.

Lemma A.28.17 (Wielandt). *Let $A = P \times Q$ be a nilpotent Hall subgroup of G, where $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$, p and q are distinct primes. Then every $\{p, q\}$-subgroup of G is nilpotent.*

Proof. We proceed by induction on $|G|$. Assume that there exists in G a nonnilpotent $\{p, q\}$-subgroup H of minimal possible order. Then H is minimal nonnilpotent so, say, $H = P_1 \cdot Q_1$, where $P_1 \in \mathrm{Syl}_p(H)$, $Q_1 = H' \in \mathrm{Syl}_q(H)$. One may assume that $Q_1 \leq Q$ (Sylow) and $\mathrm{N}_Q(Q_1) \in \mathrm{Syl}_q(\mathrm{N}_G(Q_1))$. However, we have $P < \mathrm{N}_G(Q_1)$ so $N_A(Q_1)$ is a nilpotent $\{p, q\}$-Hall subgroup of $\mathrm{N}_G(Q_1)$. Because the nonnilpotent $\{p, q\}$-subgroup $H \leq \mathrm{N}_G(Q_1)$, we get $\mathrm{N}_G(Q_1) = G$ by induction, and so $Q_1 \lhd G$ hence $\mathrm{C}_G(Q_1)$ is also normal in the group G. Then p does not divide $|G : \mathrm{C}_G(Q_1)|$, i.e., all p-elements of G centralize Q_1. In that case, H is nilpotent, a contradiction. □

Recall that a group generated by two noncommuting involutions is dihedral.

Proof of Theorem A.28.14. Suppose that the group G is a counterexample of minimal order. Then we have $P > \{1\}$ and $B > \{1\}$ by the Odd Order Theorem, and all proper factorized subgroups and epimorphic images of G are solvable. It then follows that G is simple. By Burnside's p^α-lemma [Isa1, Theorem 3.9], $L \neq \{1\}$ and $|\pi(B)| > 1$.

(i) Assume that for $A_0 \in \{P, L\}$ and $\{1\} < B_0 \in \mathrm{Syl}(B)$ we have

$$H = \langle A_0, B_0 \rangle < G.$$

Then, by Lemma A.28.15, H is factorized so solvable. By virtue of the paragraph preceding Lemma A.28.16, one may assume that $H = A_0 B_0 = B_0 A_0$. Let $g = ba \in G$, where $a \in A$ and $b \in B$. We have

$$(2) \quad A_0 B_0^g = A_0 B_0^{ba} = A_0 B_0^a = (A_0 B_0)^a = (B_0 A_0)^a = B_0^{ba} A_0 = B_0^g A_0.$$

Since $A_0 B_0^g < G$ for all $g \in G$ by the product formula, G is not simple by Remark 4, a contradiction. Thus $H = G$.

(ii) Let $u \in \mathrm{Z}(P)$ be an involution, $r \in \pi(B)$ and $R \in \mathrm{Syl}_r(B)$. Set $H = \langle u, R \rangle$ and assume that $H < G$. By Lemma A.28.15, H is factorized so solvable. Let F be a $\{2, r\}$-Hall subgroup of H containing R. Replacing A by its appropriate G-conjugate, one may assume that $u \in P_0 \in \mathrm{Syl}_2(A \cap F)$; then $F = P_0 R$. Let M be a minimal normal subgroup of F; then either $M \leq P_0$ or $M \leq R$. In the first case, we obtain that $\mathrm{N}_G(M) \geq \langle L, R \rangle = G$ by (i), a contradiction. Now assume that $M \leq R$. Then we get $\mathrm{N}_G(M) \geq T = \langle u, B \rangle$ so $G = AT$. Since $u \in \mathrm{Z}(A)$, we obtain $1 \neq u \in T_G$ (see the paragraph preceding Remark 3), a contradiction.

(iii) Let $u \in \mathrm{Z}(P)$ be an involution. We claim that $\mathrm{C}_G(u) = A$. Assume that this is false. By the modular law, $\mathrm{C}_G(u)$ is factorized so solvable, and $\mathrm{C}_B(u)$ contains an element b of prime order, say q. Then $\mathrm{C}_G(b) \geq H = \langle u, R \rangle$, where $R \in \mathrm{Syl}_r(B)$ for some $r \in \pi(B) - \{q\}$. In that case, $H < G$, contrary to (ii).

(iv) Let $u \in \mathrm{Z}(P)$ and $v \in G$ be distinct involutions. Assume that $D = \langle u, v \rangle$ is not a 2-subgroup; then D is dihedral with $|\pi(D)| > 1$ and $u \notin \mathrm{Z}(D)$. Let $\{1\} < T < D$

with $|T| = p \in \pi(D) - \{2\}$; then $\langle u \rangle \cdot T$ is dihedral of order $2p$. By Lemma A.28.17, $2p$ does not divide $|A|$ so we may assume that $T < B$. Take $\{1\} < Q \in \mathrm{Syl}_q(B)$ with $q \in \pi(B) - \{p\}$. Then $\mathrm{N}_G(T) \geq \langle u, Q \rangle = G$ by (i), and this is a contradiction.

(v) Let u and v be as in (iv). Then, by (iv), there is $g \in G$ such that

$$\langle u, v \rangle \leq P^g < A^g = P^g \times L^g$$

so that $L^g < \mathrm{C}_G(u) = A$ by (iii). In this case, we get $L^g = L$ and $v \in \mathrm{C}_G(L) < G$. It follows that $\mathrm{C}_G(L)$ contains all involutions v of G so G is not simple, a final contradiction.[4] □

In particular, $G = AB$, where A and B are nilpotent of coprime orders, is solvable (Wielandt).

Theorem A.28.18 ([Keg1]). *If a group G is a product of two nilpotent subgroups, then it is solvable.*

Moreover, Kegel has proved that a product of a finite number of pairwise permutable nilpotent subgroups is solvable.

[4] Repeating word for word the proof of Theorem A.28.14, we get the following result of A. N. Fomin [Fom]. Let $G = AB$, where $(|A|, |B|) = 1$, $A = P \times L$ with $P \in \mathrm{Syl}_2(G)$ and $B = Q \times M$ with $Q \in \mathrm{Syl}_q(G)$, q is a prime. Then G is q-solvable.

Appendix 29

Intersections of subgroups

The proofs of Theorems A.29.2, A.29.4 and A.29.8 are taken from unpublished notes of Isaacs.

1^o. Theorem A.29.1 has numerous important applications and some of them are presented below.

Theorem A.29.1. (a) (Wielandt; see [KS, Theorem 6.7.4]) *Let A be a subgroup of a group G. If A is subnormal in $\langle A, A^g\rangle$ for all $g \in G$, then A is subnormal in G.*

(b) (Baer–Suzuki; see [KS, Theorem 6.7.6]) *Let K be a conjugacy class of a group G containing an p-element. If $\langle x, y\rangle$ is a p-group for all $x, y \in K$, then $K \subset \mathrm{O}_p(G)$.*

Statement (b) follows easily from (a). Indeed, setting $A = \langle x\rangle$, we see that A is subnormal in a p-subgroup $\langle A, A^g\rangle$ so A is subnormal in G. Thus it remains to show that $A \leq \mathrm{O}_p(G)$. It suffices to show that $A \leq \mathrm{F}(G)$, where $\mathrm{F}(G)$ is the Fitting subgroup of G. To this end, we note that $A^G < G$. By induction, $A \leq \mathrm{F}(A^G)$. Since $\mathrm{F}(A^G)$ is characteristic in $A^G \lhd G$ and nilpotent, we get $\mathrm{F}(A^G) \leq \mathrm{F}(G)$, and we are done.

2^o. The following theorem generalizes Zenkov's result [Zen].

Theorem A.29.2 (Isaacs). *Let $A, B \leq G$ and let $A \cap B$ be a minimal, by inclusion, member of the set $\{A^g \cap B \mid g \in G\}$. If, for each $x \in G$, $A^x \cap B$ is nilpotent and normal in $\langle A^x, B\rangle$, then $A \cap B \leq \mathrm{F}(G)$.*

Proof. We use induction on $|G|$. Write $D = A \cap B$ and assume that $D \not\leq \mathrm{F}(G)$. Then, for some prime p, the Sylow p-subgroup P of D is not contained in $\mathrm{F}(G)$, and it follows that $\langle P, P^x\rangle$ is not a p-group for some $x \in G$ (Theorem A.29.1(a)). Let us write $H = \langle P^x, B\rangle$ and $Z = A^x \cap B$; then $Z \leq B \leq H$. By hypothesis, both $P^x (\leq A^x)$ and B normalize Z hence Z is H-invariant.

(i) Suppose that $H = G$. Then (the nilpotent) subgroup Z is normal in G so we get $Z \leq \mathrm{F}(G)$ and, since $Z \leq A^x$, we obtain $Z = Z^{x^{-1}} \leq A$. Since also $Z \leq B$, we see that $Z \leq A \cap B = D$ and hence, by the minimality of D, we have $D = Z \leq \mathrm{F}(G)$, as required.

(ii) Now suppose that $H < G$ and note that $D \leq B \leq H$. Assume that $D \leq \mathrm{F}(H)$. Then $P \leq \mathrm{O}_p(H)$ and $\langle P, P^x\rangle \leq \mathrm{O}_p(H)P^x$, which is a p-group since P^x is a p-subgroup of H. This contradicts the choice of x and we thus have $D \not\leq \mathrm{F}(H)$. Note

that

$$D = (A \cap H) \cap B = A \cap (H \cap B) = A \cap B$$

since $B \leq H$. If $y \in H$, then

$$(A \cap H)^y \cap B = A^y \cap H \cap B = A^y \cap B$$

and so, by hypothesis, the nilpotent subgroup $(A \cap H)^y \cap B$ is normalized by $(A \cap H)^y$ $(\leq A^y)$ and B. As $H < G$, we get $(A \cap H) \cap B \leq \mathrm{F}(H)$ by induction. Since $(A \cap H) \cap B = D$, it follows that $D \leq \mathrm{F}(H)$, contrary to what has just been proved. □

Corollary A.29.3 (Zenkov). *Let A and B be Dedekindian subgroups of a group G and suppose that $A \cap B$ is a minimal member of the set $\{A^g \cap B \mid g \in G\}$. Then we have $A \cap B \leq \mathrm{F}(G)$.*

In the original version of Zenkov's theorem A and B were abelian.

In particular, we can obtain the following Brodkey's theorem (see Theorem A.3.13): If $P \in \mathrm{Syl}_p(G)$ is abelian, then $P \cap P^g = \mathrm{O}_p(G)$ for some $g \in G$. Indeed, we have $P \cap P^g \leq \mathrm{F}(G)$ for some $g \in G$ by Corollary A.29.3. Since

$$\mathrm{O}_p(\mathrm{F}(G)) = \mathrm{O}_p(G) \leq P \cap P^g \leq \mathrm{O}_p(\mathrm{F}(G)),$$

we get $P \cap P^g = \mathrm{O}_p(G)$.

Recall that a group G is said to be a Z-*group* if all its Sylow subgroups are cyclic. Normal subgroups of a Z-group are characteristic.

Now we are ready to prove Theorem A.29.4, which is a generalization of the theorem from [DemW].

Theorem A.29.4 (Isaacs). *Let $X, Y \leq G$ be Z-subgroups of a group G and let D be a minimal member of the set $\{X^g \cap Y \mid g \in G\}$. Suppose that $X^g \cap Y$ is normal in $\langle X^g, Y \rangle$ for all $g \in G$. Then D is normal in* $\mathrm{F}(G)$.

Proof. Write $F = \mathrm{F}(G)$, and note that $D \leq F$ by Theorem A.29.2, and so D is cyclic. We proceed by induction on $|G|$ and assume that D is not normal in $\mathrm{F}(G)$; then we get $D > \{1\}$. One can replace X by a conjugate if necessary and assume that $D = X \cap Y$. Since $D \lhd \langle X, Y \rangle$, all subgroups of D are normal (even characteristic) in X and Y.

(i) We claim that $E = D_G = \{1\}$. Assume that this is false. Note that $E \leq X^g \cap Y$ for all $g \in G$, and we see that $(X/E) \cap (Y/E) = D/E$ is a minimal member of the set $\{(X^g/E) \cap (Y/E) \mid g \in G\}$. It follows, by induction, that D/E is normal in $\mathrm{F}(G/E)$, and thus D is normal in the preimage of $\mathrm{F}(G/E)$ in G. This preimage contains F, and thus D, being a subgroup of F, is normal in F, a contradiction.

(ii) We claim that $E = D_F = \{1\}$. Assume that $E > \{1\}$. Write $N = \mathrm{N}_G(E)$ and note that $F \leq N$, thus $F \leq \mathrm{F}(N)$. Also, E is not normal in G by (i), and so $N < G$. As we have noticed, $X, Y \leq N$, and D is minimal in the set $\{X^z \cap Y \mid z \in N\}$, hence D is normal in $\mathrm{F}(N)$ by induction. Since $F \leq \mathrm{F}(N)$ and $D \leq F$, it follows that D is normal in F, contrary to the assumption.

(iii) We claim that (F$(G) =) F = G$, i.e., G is nilpotent. Assume that $F < G$ and note that

$$D = (X \cap F) \cap (Y \cap F)$$

(recall that $D < F$) is a member of the set $\{(X \cap F)^f \cap (Y \cap F) \mid f \in F\}$. Let $E = (X \cap F)^f \cap (Y \cap F) = X^f \cap Y \cap F$ be a minimal member of the set above contained in D. Then E is normal in F by induction and, by (ii), we infer that $E = \{1\}$. Thus $X^f \cap Y$ meets F trivially and it follows, by Theorem A.29.2, that $X^f \cap Y = \{1\}$. This contradicts the minimality of $D > \{1\}$. Thus G is nilpotent.

It remains to prove that $D \lhd G$. Now X and Y are cyclic as Z-subgroups of the nilpotent group G.

(iv) We claim that $X_G = \{1\}$. Indeed, write $E = X_G$ and assume $E > \{1\}$. Choose $g \in G$ with the property that $(X^g/E) \cap (YE/E)$ is minimal, and apply induction to deduce that $X^g \cap (YE)$ is a normal (cyclic since X is cyclic) subgroup of G containing $X^g \cap Y$, which is therefore also normal in G (indeed, by hypothesis, $X^g \cap Y$ is normal in X^g so normal in $X^g \cap YE$; because $X^g \cap Y$ is characteristic in $X^g \cap YE$ which is G-invariant, our claim follows). It follows that $X^g \cap Y \leq X$, and thus

$$X^g \cap Y \leq X \cap Y = D.$$

By the minimality of D, we have $X^g \cap Y = D$ and $D \lhd G$, contrary to the assumption.

(v) We claim that for each prime $p \in \pi(G)$ there is a p-element $g_p \in G$ such that p does not divide $|X^{g_p} \cap Y|$. Indeed, one can assume that $p \mid |Y|$, and we let U be the subgroup of order p in Y. By (iv), there exists $g \in G$ such that $U \not\leq X^g$, and we write $g = st = ts$, where s is the p-part of g and t the p'-part of g. Then $U = U^{t^{-1}} \not\leq X^s$, where the equality holds because G is nilpotent. It follows that $X^s \cap Y$ has no subgroup of order p (by hypothesis and (iii), X and Y are cyclic so U is a unique subgroup of order p in Y), and we conclude that p does not divide $|X^s \cap Y|$. Our claim follows with $g_p = s$.

(vi) We have a contradiction. Indeed, let g be the product of the elements g_p from part (v), where p runs through all prime divisors of $|Y|$. Now, we have $X^g \cap Y > \{1\}$ (see the first paragraph of the proof), and let p be a prime dividing $|X^g \cap Y|$. We write $g = st = ts$, where s and t are as in (v). Let U be a subgroup of order p in Y, and note that $U \leq X^g$. Then we obtain $U = U^{t^{-1}} \leq X^s \cap Y$, and hence p divides $|X^s \cap Y|$, contrary to (v). □

Corollary A.29.5. *Let X, Y be cyclic subgroups of G and let D be a minimal member of the set $\{X^g \cap Y \mid g \in G\}$. Then D is normal in* F(G).

Corollary A.29.6 (Dempwolff–Wong [DemW]). *Let X, Y be cyclic subgroups of G. Then $X^g \cap Y$ is normal in* F(G) *for some $g \in G$.*

Corollary A.29.7. *Let X, Y be cyclic subgroups of a p-group G. If $X_G = \{1\}$, then $X^g \cap Y = \{1\}$ for some $g \in G$.*

We suggest the reader give a direct proof of Corollary A.29.7.

3^o. Theorem A.29.1 has also the following consequence due to E. Pennington:

Theorem A.29.8 ([Pen]). *Suppose that $G = AB$, where A and B have normal Sylow p-subgroups (= p-closed). Then $\mathrm{O}_p(G) = (A \cap \mathrm{O}_p(G))(B \cap \mathrm{O}_p(G))$.*

The presented proof is due to Isaacs (unpublished note).

Lemma A.29.9. *If $G = AB$, then $\mathrm{O}_p(A) \cap \mathrm{O}_p(B) \leq \mathrm{O}_p(G)$.*

Proof. We can choose $S \in \mathrm{Syl}_p(A)$ and $T \in \mathrm{Syl}_p(B)$ such that $S, T \leq P \in \mathrm{Syl}_p(G)$ (Sylow). By the product formula, $|ST| = |P|$ so $ST = P$. Write

$$U = \mathrm{O}_p(A)\,(\leq S), \quad V = \mathrm{O}_p(B)\,(\leq T), \quad D = U \cap V.$$

We have to prove that $D \leq \mathrm{O}_p(G)$. By Theorem A.29.1(a), it is sufficient to show that $\langle D, D^g \rangle$ is a p-group for all $g \in G$. Write $g = ba^{-1}$, where $a \in A$ and $b \in B$. Then $\langle D, D^g \rangle^a = \langle D^a, D^b \rangle$. But $D^a \leq U^a = U$ and $D^b \leq V^b = V$, so that

$$\langle D^a, D^b \rangle \leq \langle U, V \rangle \leq ST = P$$

which is a p-group. □

Lemma A.29.10. *Suppose that $G = AB$, where A and B are p-closed, and assume that $|G : A|$ and $|G : B|$ are powers of p. Then G is p-closed and we have $P = ST$, where P, S and T are Sylow subgroups of G, A and B, respectively.*

Proof. Note that $ST = P \in \mathrm{Syl}_p(G)$ (see the proof of Lemma A.29.9). Since $A \cap B$ is p-closed, it has a p-complement H (Schur–Zassenhaus). By the product formula, $|G : (A \cap B)| = |G : A||G : B|$, and this is a p-number by hypothesis. It follows that H is a p-complement in G. Now, $H \leq A \leq \mathrm{N}_G(S)$ and $H \leq B \leq \mathrm{N}_G(T)$, and thus H normalizes $ST = P$ so that $P \lhd G$. □

Proof of Theorem A.29.8. We proceed by induction on $|G|$. Due to Lemma A.29.10, one may assume without loss of generality that $|G : A|$ is not a power of p. Therefore, if $U = \mathrm{O}_p(G)$ and $H = AU$, then $H < G$. Let $V = \mathrm{O}_p(H)$; then we get $V \geq U$ and $V \in \mathrm{Syl}_p(H)$.

By the modular law, $H = A(H \cap B)$, and so induction applies to H. We have

$$V = (A \cap V)((H \cap B) \cap V) = (A \cap V)(B \cap V)$$

as $V \leq H$. Note that $B \cap V$ is a p-subgroup of B and hence lies in its Sylow p-subgroup $\mathrm{O}_p(B)$. Then

$$B \cap V \leq \mathrm{O}_p(B) \cap \mathrm{O}_p(H) \leq \mathrm{O}_p(G) = U$$

by Lemma A.29.9 since $HB = UAB = G$. Thus $B \cap V = B \cap U$ since $U \leq V$ and, by the above,

$$V = (A \cap V)(B \cap V) = (A \cap V)(B \cap U).$$

It follows that

$$\begin{aligned} U = V \cap U &= ((A \cap V)(B \cap U)) \cap U \\ &= (A \cap V \cap U)(B \cap U) \\ &= (A \cap U)(B \cap U) \end{aligned}$$

by the modular law (recall that $U = \mathrm{O}_p(G)$). □

Zenkov's theorem has the following useful

Corollary A.29.11. *Suppose that an abelian group A acts faithfully and coprimely on a nontrivial group N (i.e.,* $\mathrm{GCD}(|A|, |N|) = 1$*). Then $|A| < |N|$.*

Proof. Let $G = A \cdot N$ be a natural semidirect product and $\pi(A) = \pi$. Since N is a π'-group and A acts faithfully on N, it follows that $\mathrm{O}_\pi(G) = \{1\}$ so $A \cap \mathrm{F}(G) = \{1\}$ (indeed, $A \cap \mathrm{F}(G)$ is a π-Hall subgroup of $\mathrm{F}(G)$ so normal in G). By Corollary A.29.3, there exists $g \in G$ such that $A \cap A^g = \{1\}$. Since $A < G$, we get $AA^g \neq G$ (Ore's Lemma 28.8), and it follows that $|A||N| = |G| > |AA^g| = |A|^2$ so $|N| > |A|$. □

4^o. Now we are ready to prove the following

Theorem A.29.12 ([Isa20, Theorem A]). *Suppose that A is a point stabilizer in a transitive permutation group G of degree m. If A is abelian, then* $\exp(A) \leq m$ *with strong inequality provided $m > 1$.*

Exercise 1. Give a short proof of Theorem A.29.12 in the case where G is a p-group.

Solution (Mann). Assume that $\exp(A) \geq m = |G : A|$. Let Z be a cyclic subgroup of A of maximal order; then we see that $|Z| = \exp(A) \geq |G : A|$. For $g \in G$ we get $ZA^g \subseteq AA^g \subset G$ (Ore's Lemma A.28.8) so $Z \cap A^g > \{1\}$ by the product formula. If Z_0 is a subgroup of prime order p in $Z \cap A^g$, then $\{1\} < Z_0 \leq \bigcap_{g \in G} A^g = A_G$, which is a contradiction since $A_G = \{1\}$.

Proof of Theorem A.29.12. Let G be a transitive permutation group of degree m and suppose that a point stabilizer A is abelian. We show by induction on m that A satisfies $\exp(A) \leq m$ and that this inequality is strict if $m > 1$. One may assume from the start that $m > 1$ and $A > \{1\}$.

If $\mathrm{F}(G) = \{1\}$, then, by Corollary A.29.3, we have $A \cap A^g = \{1\}$ for some $g \in G$, and then $m|A| = |G| > |A|^2$ (Ore's Lemma A.28.8) so $\exp(A) \leq |A| < m$. Therefore we can assume that $\mathrm{F}(G) > \{1\}$, and we choose in $\mathrm{F}(G)$ a minimal G-invariant subgroup N; then N is an elementary abelian p-group for some prime p.

Since $A_G = \{1\}$, we get $N \not\leq A$ and thus $NA > A$. Writing $u = |G : NA|$, we see that $u < |G : A| = m$; clearly, $u \mid m$ since

$$m = |G : A| = |G : NA||NA : A| = u|NA : A|.$$

Let $K = (NA)_G$ so that G/K is a transitive permutation group of degree $|G : NA| = u$

with a point stabilizer NA/K. As $N \leq K$, we see that $NA = KA$ and

$$NA/K = KA/K \cong A/(K \cap A) = A/J,$$

where we have written $J = K \cap A$. Since A/J is abelian, it follows, by induction, that $\exp(A/J) \leq u$, with equality only if $u = 1$. By the modular law,

$$K = N(K \cap A) = NJ.$$

Next,

$$\frac{m}{u} = \frac{|G : A|}{|G : NA|} = |NA : A| = |N : (N \cap A)|$$

is a power of p since N is a p-subgroup.

(i) First suppose that K is nonabelian. Write $Z = \mathrm{Z}(K)$; then $Z \lhd G$ since $K \lhd G$. Note that ZJ is abelian since $J \leq A \cap K$ is abelian as a subgroup of A. It follows that $N \not\leq Z$ since $K = NJ$ is nonabelian. Because N is a minimal normal subgroup of G and $Z \lhd G$, we get $N \cap Z = \{1\}$.

Now write

$$V = NZ \cap J \ (= NZ \cap A \cap K \leq A).$$

We get $N \leq NZ \leq K = NJ$ and thus, by the modular law,

$$NZ = N(NZ \cap J) = NV.$$

Also, $NZ = N \times Z$ is abelian and thus V centralizes both N and $J(\leq A)$. Therefore

$$V \leq \mathrm{Z}(NJ) = \mathrm{Z}(K) = Z < NZ = NV.$$

By the modular law again, we get $Z = V(N \cap Z) = V < A$ (recall that $N \cap Z = \{1\}$). But $Z(< A)$ is normal in G and $A_G = \{1\}$, and hence $\{1\} = Z = \mathrm{Z}(K) = \mathrm{Z}(NJ)$. Since J is abelian, we have $\mathrm{C}_J(N) = \{1\}$, and J acts faithfully on N. In particular, we see that $N \cap A \leq \mathrm{C}_J(N) = \{1\}$ (note that $J \leq A$). Thus

$$\frac{m}{u} = |N : (N \cap A)| = |N|.$$

Now recall that N is a p-subgroup, and let $P \in \mathrm{Syl}_p(J)$. Then we conclude that NP is a Sylow p-subgroup of $NJ = K$ so it is characteristic in K since J is abelian. As $N \leq K < NA$ and $NA/N \cong A/(N \cap A)$ is abelian, so is K/N. Since NP/N is characteristic in K/N, we infer that NP/N is normal in G/N since $K/N \lhd G/N$ and hence $\mathrm{Z}(NP)$ is normal in G. But $N \cap \mathrm{Z}(NP) > \{1\}$ as NP is a p-group and $N \lhd NP$, and it follows from the minimality of N that $N \leq \mathrm{Z}(NP)$. Thus $P \leq \mathrm{C}_J(N) = \{1\}$, and therefore J is a p'-subgroup. But J is abelian and acts faithfully on the p-group N and so, by Corollary A.29.11, we have $|J| < |N| = \frac{m}{u}$. Since

$$\exp(A) \leq \exp(A/J)|J| < u \cdot \frac{m}{u} = m,$$

we are done in this case.

(ii) We can now assume that K is abelian. Observe that $(|G : NA| =)\, u > 1$ since otherwise $NA = G$ and thus $K = (NA)_G = G$ is abelian which yields that $A = \{1\}$, contrary to the assumption. We will show that $\exp(J) \leq p$, and thus (since $u > 1$) we have

$$\exp(A) \leq \exp(A/J)\exp(J) < up.$$

Also, since $1 < \frac{m}{u}$ is a power of p, we obtain $p \leq \frac{m}{u}$, and the result will follow.

Let $x \in K = NJ$ and write $x = ab$, where $a \in N$ and $b \in J$. Since K is abelian and N is an elementary abelian p-group, we have $x^p = b^p \in J$. Thus J contains the subgroup $L = \langle x^p \mid x \in K\rangle$, which is characteristic in K. Since $A_G = \{1\}$, it follows that this subgroup L is trivial (note that $J \leq A$) and thus K is an elementary abelian p-group. In particular, as $J < K$, we see that $\exp(J) \leq p$, as claimed, and the proof is complete. □

In particular, if A from Theorem A.29.12 is cyclic, we obtain $|A| < m$; moreover, $|G| = m|A| < m^2$ [Luc].

5^o. In conclusion we shall prove Theorems A.29.14 and A.29.15 due to Herzog and Kaplan [HK]. We closely follow [HK].

The proof of Theorem A.29.14 is based on the following

Lemma A.29.13 ([HK]). *Let G be a group with subgroups A_i such that $G = \bigcup_{i=1}^n A_i$ is an irredundant union.*[1] *Assume that q is a prime with $q \geq n$. Then all the q-elements of G are contained in $\bigcap_{i=1}^n A_i$.*

Proof. Assume that the lemma is not true; then $n > 1$ and $q \in \pi(G)$ (note that $1 \in G$ is a q-element). In this case, after an appropriate renumbering, there exist a q-element $g \in G$ and a subscript m, $1 \leq m \leq n-1$, such that $g \in \bigcap_{i=1}^m A_i$ but $g \notin A_j$ for each $m+1 \leq j \leq n$. Since the union is irredundant, there exists $u \in G$ satisfying $u \in A_n$ and $u \notin A_i$ for each $1 \leq i \leq n-1$.

Consider now n (pairwise distinct in view of $q \geq n$) elements

$$u,\ gu,\ g^2u,\ \ldots,\ g^{n-1}u.$$

If one of these elements is contained in A_i for some $1 \leq i \leq m$, then it follows (since $g \in A_i$) that $u \in A_i$, a contradiction. Thus all the elements in the displayed list are contained in the set $\bigcup_{j=m+1}^n A_j$. By the "pigeon-hole principle", there exist s, t such that $0 \leq s < t \leq n-1$ and j_0 with $m+1 \leq j_0 \leq n$ such that $g^s u, g^t u \in A_{j_0}$. In this case, we have $g^t u(g^s u)^{-1} = g^{t-s} \in A_{j_0}$. Since $1 \leq t-s \leq n-1 \leq q-1$, there is an integer v such that $(t-s)v \equiv 1 \pmod{o(g)}$. It follows that

$$g = g^{(t-s)v} \in A_{j_0} \subseteq \bigcup_{i=m+1}^{n} A_j,$$

contrary to the choice of g. □

[1] This means that if we delete one of the A_i's, then the union of the remaining components is a proper subset of G; see §116.

Theorem A.29.14 (Herzog–Kaplan [HK]). *Let G be a group with a cyclic subgroup A such that $|A|^2 > |G|$. Then A contains a nonidentity subgroup U which is characteristic in G.*

Proof. Let H denote the holomorph of G, i.e., the natural semidirect product of G and $\mathrm{Aut}(G)$ with kernel G. Note that each H-invariant subgroup of G is characteristic in G. For $h \in H$ we see that $A, A^h \leq G$ and $A \cap A^h > \{1\}$ by hypothesis and the product formula. Thus there exists a subgroup P of A with $|P| = p$, a prime, such that $P \leq A \cap A^h$. Therefore P, P^h are both subgroups of order p of the cyclic group A^h, which implies $P = P^h$ and $h \in \mathrm{N}_H(P)$. Denote the family of all subgroups of A of prime orders by Π; obviously, we get $|\Pi| = |\pi(A)|$. Then, by what has just been said, $H = \bigcup_{P\in\Pi} \mathrm{N}_H(P)$. If $\mathrm{N}_H(P) = H$ for some $P \in \Pi$, then P is characteristic in G, and we are done. Thus we assume from now on that $\mathrm{N}_H(P) < H$ for each $P \in \Pi$. Choose $\Pi_0 \subseteq \Pi$ such that the union $H = \bigcup_{P\in\Pi_0} N_H(P)$ is irredundant. Then we conclude that $|\Pi_0| \geq 3$ since H is not a union of two of its proper subgroups. Denote $q = \max\{|P| \mid P \in \Pi_0\}$; then $q \geq 5$ is a prime. Since 1 and 4 are not primes, we get $|\Pi_0| \leq q - 2$ whence, by Lemma A.29.13, each q-element of H is contained in $\bigcap_{P\in\Pi_0} N_H(P)$. It follows that each q-element of H is contained in $\bigcap_{P\in\Pi_0} \mathrm{C}_H(P)$ since q does not divide $|\mathrm{Aut}(P)| = |P| - 1$ for $P \in \Pi_0$. Let $H_q \in \mathrm{Syl}_q(H)$ and let $(H_q)^H$ be its normal closure in H. Then $(H_q)^H \leq \bigcap_{P\in\Pi_0} \mathrm{C}_H(P)$ since $(H_q)^H$ is generated by q-elements. Let $Q \in \Pi_0$, $|Q| = q$; then we have $(H_q)^H \leq \mathrm{C}_H(Q)$ by the above. In particular, $Q \leq \mathrm{Z}((H_q)^H) \lhd G$ so the normal closure Q^G is an elementary abelian normal q-subgroup of G, and so $\mathrm{O}_q(G) > \{1\}$.

Suppose first that $A\mathrm{O}_q(G) = G$. Choose $P \in \Pi_0$ with $P \neq Q$, $|P| = p$ (P exists since $|\Pi_0| \geq 3$). By the above, we have $\mathrm{O}_q(G) \leq \mathrm{C}_G(P)$ and $A \leq \mathrm{C}_G(P)$ as $P \leq A$, and we conclude that $P \leq \mathrm{Z}(G)$. Furthermore, a (cyclic) Sylow p-subgroup of A is a Sylow p-subgroup of $G(= A\mathrm{O}_q(G))$. Therefore P is the unique subgroup of order p in G. Thus P is characteristic in G, completing this case.

Next we assume that $A\mathrm{O}_q(G) < G$.

Let C be a characteristic subgroup of G which is maximal such that $\mathrm{O}_q(G) \leq C$ and $AC \neq G$. Since $|A| > |G|^{1/2}$, it follows that at least one of the following holds:

(i) $|AC/C| > |G/C|^{1/2}$.

(ii) $|A \cap C| > |C|^{1/2}$.

Indeed, assume that $|AC/C| \leq |G/C|^{1/2}$ and $|A\cap C| \leq |C|^{1/2}$. Multiplying these inequalities and using the product formula, we get $|A| \leq |G|^{1/2}$, contrary to the hypothesis.

(i) We apply now induction on $|G|$. Suppose that $|AC/C| > |G/C|^{1/2}$. We have $|G/C| < |G|$ and AC/C is a cyclic subgroup of G/C. Thus, by induction, there exists a characteristic subgroup K/C of G/C such that $C/C < K/C \leq AC/C$. As K/C and C are characteristic in G/C and G, respectively, it follows that K is characteristic in G. Moreover, we have $AK \leq AC < G$. This contradicts our maximality assumption on C, and so we deduce that (i) cannot hold.

(ii) Hence $|A \cap C| > |C|^{1/2}$. Since $|C| < |G|$, our induction hypothesis implies the existence of a nonidentity subgroup D such that $D \leq A \cap C$ and D is characteristic in C. But C is characteristic in G so D is. The proof is complete. □

Let $G = A \times B$, where $A \cong \mathrm{C}_{p^2} \cong B$. Since $|A| = |G : A|$ and A has no nonidentity characteristic subgroup of G, Theorem A.29.14 does not hold under condition $|A|^2 = |G|$ even if G is an abelian p-group.

Theorem A.29.15 ([HK]). *Let $G > \{1\}$ be a group with a proper cyclic subgroup A such that $|A|^2 \geq |G|$ (or, what is the same, $|A| \geq |G : A|$). Then $|A : A_G| < |G : A|$ (in particular, $A_G > \{1\}$.*

Proof. Consider a representation of G by permutations of left cosets of A. Then A_G is the kernel of this representation. By Theorem 29.12, $\exp(A/A_G) < |G : A|$. Since A is cyclic, we get $|A : A_G| < |G : A|$. □

Example. Suppose that G is the uniquely determined minimal nonnilpotent group of order $5 \cdot 7^4$; then $G' \in \mathrm{Syl}_7(G)$ is elementary abelian. If A is maximal in G', then we obtain that $A_G = \{1\}$ and $|A| > |G|^{1/2}$. Therefore it is impossible to replace in Theorems A.29.14 and A.29.15 the assumption on cyclicity of A by its commutativity.

Exercise 2. Suppose that $Z \leq G$ is a cyclic p-subgroup and assume that $A \leq G$ satisfies $|G : A| < |Z|$. Prove that A has a characteristic subgroup $A_0 \geq \Omega_1(Z)$.

Solution. By the product formula, we have $Z \cap A^\alpha \geq \Omega_1(Z)$ for all $\alpha \in \mathrm{Aut}(G)$ so $\Omega_1(Z) \leq \bigcap_{\alpha \in \mathrm{Aut}(G)} A^\alpha$.

Lemma A.29.16 ([HK]). *Suppose that G is a group with a cyclic subgroup A such that $A \cap A^g > \{1\}$ for all $g \in G$. Then we have $A \cap \mathrm{F}(G) > \{1\}$; in particular, $\mathrm{F}(G) > \{1\}$. Moreover, one of the following holds:*

(i) $A_G > \{1\}$.

(ii) *There exist subgroups $Q, R < A$ satisfying the following: $|Q| = q$, $|R| = r$, where q and r are different primes, and the normal closures Q^G and R^G are elementary abelian q- and r-groups, respectively.*

Proof. Let Π be the family of all subgroups of A of prime orders. Since $A \cap A^g > \{1\}$ for all $g \in G$, we obtain (as in the proof of Theorem A.29.14) that $G = \bigcup_{P \in \Pi} \mathrm{N}_G(P)$. If $\mathrm{N}_G(P) = G$ for some $P \in \Pi$, then we get $A_G > \{1\}$ and (i) holds. Next assume that $\mathrm{N}_G(P) < G$ for all $P \in \Pi$, and choose $\Pi_0 \subseteq \Pi$ such that $G = \bigcup_{P \in \Pi_0} N_G(P)$ is irredundant. Then $|\Pi_0| \geq 3$ (see the proof of Lemma A.29.13). Denote

$$\pi_0 = \{|P| \mid P \in \Pi_0\}, \quad q = \max\{p \mid p \in \pi_0\}, \quad r = \max\{p \mid p \in \pi_0 - \{q\}\}.$$

We have $|\Pi_0| \leq q-2$ and $|\Pi_0| \leq r$ whence, by Lemma A.29.13, all the q-elements and r-elements of G are contained in $D = \bigcap_{P \in \Pi_0} \mathrm{N}_G(P)$. Let $Q, R \in \Pi_0$ be such that $|Q| = q$ and $|R| = r$. Then we deduce that each q-element of G centralizes Q and

each r-element of G centralizes R. Thus it follows that Q^G is an elementary abelian q-group and R^G is an elementary abelian q-group (see the proof of Theorem A.29.14). Hence (ii) holds. □

Note that the assertion $A \cap \mathrm{F}(G) > \{1\}$ stated in Lemma A.29.16 follows from Corollary A.29.6.

Our next corollary is related to *regular orbits* of automorphism groups. For a subgroup $A \leq \mathrm{Aut}(G)$ we say that A has a *regular orbit* on G if A has an orbit of size $|A|$ on G, i.e., there is $g \in G$ such that $|\{g^\alpha \mid \alpha \in A\}| = |A|$.

Corollary A.29.17 ([HK]). *Let G be a group and let $\alpha \in \mathrm{Aut}(G)$ be such that $o(\alpha)$ and $|\mathrm{F}(G)|$ have at most one common prime divisor. Then the subgroup $A = \langle \alpha \rangle$ has a regular orbit on G.*

Proof. Consider the natural semidirect product $S = A \cdot G$. Let $g \in G$ and define L by $L = A \cap A^g$. Then L and L^g are subgroups of same order in a cyclic group A^g so $L = L^g$. Since $D = \langle L, g \rangle \cap G$ is normal in $\langle L, g \rangle$ and $g \in D$, we get $L \leq \mathrm{C}_A(g)$ so for each $g \in G$ we have $A \cap A^g = \mathrm{C}_A(g)$ whence $|g^A| = |A : (A \cap A^g)|$, where g^A is the A-orbit of g. Suppose that the corollary is not true; then we obtain $|g^A| < |A|$ and so $A \cap A^g > \{1\}$ for each $g \in G$. Hence $A \cap A^s > \{1\}$ for each $s \in S (= A \cdot G)$ and Lemma A.29.16 may be applied. Since the core A_S centralizes G, we have $A_S = \{1\}$. Thus possibility (ii) of Lemma A.29.16 holds, and we choose $Q, R < A$ as described in that lemma. If $Q^S \cap G = \{1\}$, then Q^S centralizes G and, in particular, Q centralizes G, contradicting $A_S = \{1\}$. Thus we get $Q^S \cap G > \{1\}$ and, similarly, we have $R^S \cap G > \{1\}$. Since Q^S is a q-group and R^S is an r-group for suitable primes $q \neq r$, we have

$$\mathrm{O}_q(G) \geq Q^S \cap G > \{1\} \quad \text{and} \quad \mathrm{O}_r(G) \geq R^S \cap G > \{1\}.$$

Thus the primes q and r divide $|\mathrm{F}(G)|$ and the desired contradiction has been reached (recall that $\mathrm{GCD}(|A|, |\mathrm{F}(G)|)$ is a prime power by hypothesis). □

Let us prove that the maximal possible order of an automorphism α of a nontrivial group G is $|G| - 1$. Indeed, set $A = \langle \alpha \rangle$ and consider the natural semidirect product $S = A \cdot G$; then we see that $A_S = \{1\}$. It follows that

$$|A| < |S|^{1/2} = |A|^{1/2} |G|^{1/2}$$

so $|A| \leq |G| - 1$. It is known that elementary abelian groups G indeed have automorphisms of order $|G| - 1$ (the Singer cycles). We show now that these are indeed the only possible examples.

Corollary A.29.18 ([HK]). *If $\alpha \in \mathrm{Aut}(G)$, then the following hold:*

(a) $o(\alpha) < |G|$.

(b) *If $o(\alpha) = |G| - 1$, then $\langle \alpha \rangle$ is fixed-point-free and G is an elementary abelian p-group for a certain prime p.*

Proof. Let $A = \langle\alpha\rangle$ and $S = A \cdot G$ be the natural semidirect product.

Statement (a) was proved in the paragraph preceding the corollary.

(b) Now let $|A| = |G|-1$. By Corollary A.29.17, $\langle\alpha\rangle$ has a regular orbit on G. This orbit must be $G^{\#} = G - \{1\}$ whence $\langle\alpha\rangle$ is fixed-point-free. Furthermore, it follows that every element of $G-\{1\}$ has the same order p for a certain prime p. Finally, since G does not possess any characteristic subgroup except G itself and $\{1\}$, we infer that G is elementary abelian. □

Exercise 3. Classify the groups G possessing an automorphism α of order $|G| - 2$.

Exercise 4. Classify the groups G possessing an automorphism α of order $|G| - 3$.

Exercise 5. Let G be a p-group and let $A < G$ be cyclic with $|A| = |G : A|$. Suppose that A contains no nonidentity characteristic subgroup of G. If $p > 2$, then G is metacyclic. In case that G is metacyclic, one of the invariants of G/G' is equal to $|A|$. If $p = 2$ and G is nonmetacyclic, then G/G' contains a cyclic subgroup of index 2.

Hint. By hypothesis, there exists an $\alpha \in \mathrm{Aut}(G)$ such that $\Omega_1(A) \not\leq A^\alpha$. It follows that $A \cap A^\alpha = \{1\}$ so $G = AA^\alpha$. Therefore, if $p > 2$, then G is metacyclic (Theorem 9.11). In the case under consideration, $A \cap G' = \{1\}$ so one of the invariants of G/G' is equal to $|A|$. If $p = 2$ and G is nonmetacyclic, the result follows from Theorem 36.11 of Ito–Ohara.

Below we formulate, without proofs, the following consequences and generalizations of Theorems A.29.12, A.29.14 and A.29.15.

Corollary A.29.19 ([HK]). *Let G be a primitive permutation group which is neither regular nor Frobenius of prime degree.*[2] *Then for each $g \in G$ there exists $h \in G$ such that $\langle g\rangle \cap \langle g^h\rangle = \{1\}$. In particular, $o(g) < |G|^{1/2}$ for all $g \in G$.*

Theorem A.29.20 ([HKL2]). *Let $A < G$ be such that $\mathrm{C}_G(A)$ has a cyclic subgroup of order $> |G : A|$. Then A has a nonidentity characteristic subgroup of G.*

Theorem A.29.21 ([HKL2]). *Suppose that $A > \{1\}$ is a subgroup of a group G such that $\mathrm{C}_G(A)$ has a cyclic subgroup of order $|G : A|$. Then $A_G > \{1\}$.*

Theorems A.29.20 and A.29.21 generalize Theorems A.29.14 and A.29.15, respectively. These theorems are nontrivial even for p-groups.

In conclusion we state the following related result.

Theorem A.29.22 (A. Goren [Gore1]). *Let G be a transitive permutation group on the set Ω. Then $|G : \mathrm{C}_G(A)| \geq |G|^{|\Lambda|/|\Omega|}$ for each $\Lambda \subseteq \Omega$. Here*

$$\mathrm{C}_G(\Lambda) = \{g \in G \mid \lambda^g = \lambda \text{ for all } \lambda \in \Lambda\}.$$

[2] Note that a Frobenius group of prime degree $p(> 2)$ is a subgroup of the holomorph of the group C_p.

Appendix 30

Thompson's lemmas

In this section we present the proofs of certain Thompson's lemmas from his seminal paper [Tho3]. These lemmas show the role of p-groups in general finite group theory.

In the proof of Lemma A.30.1 we use the following observation. Suppose that p, q are distinct primes and $G = Q \cdot P$, where P is minimal normal p-subgroup of G and $Q \cong \mathrm{E}_{q^2}$ (in this case, Q is maximal in G). Then we get $G = X_1 \times (X_2 P)$, where $|X_1| = |X_2| = q$ and $X_2 P$ is a Frobenius group. Indeed, we have $\mathrm{C}_G(x) > Q$ for some $x \in Q^{\#}$ since G is not a Frobenius group. Then $\mathrm{C}_G(x) \cap P > \{1\}$ is P- and Q-invariant so normal in G, and we conclude that $P < \mathrm{C}_G(x)$ hence $x \in \mathrm{Z}(G)$. It follows that $G = \langle x \rangle \times \langle y, P \rangle$, where $Q = \langle x \rangle \times \langle y \rangle$, and we are done since $\langle y, P \rangle$ is a Frobenius group.

Lemma A.30.1 ([Tho3, Lemma 5.58]). *Let p, q be distinct primes and $G = Q \cdot P$, where P is a normal Sylow p-subgroup of G and $Q \cong \mathrm{E}_{q^2}$. Let $\{X_1, \ldots, X_r\}$ be the set of all subgroups of Q of order q which have nontrivial fixed points on P. If $r = 2$, then $P = \mathrm{C}_P(X_1) \times \mathrm{C}_P(X_2)$.*

Proof. We use induction on $|P|$. Since $r = 2 < q + 1$, the number of subgroups of order q in Q, it follows that p does not divide $|\mathrm{Z}(G)|$ (otherwise, $r = q + 1 > 2$). If $q \mid |\mathrm{Z}(G)|$, then $\mathrm{C}_P(Q) > \{1\}$ so that $r = 1 < 2$ again. Thus $\mathrm{Z}(G) = \{1\}$ hence $Q_G = \{1\}$.

Let N be a minimal normal subgroup of G; then N is a p-subgroup by the previous paragraph. Since $N \leq \mathrm{Z}(P)$ (indeed, $[N, P] < N$), it follows that N is a minimal normal subgroup of the subgroup $Q \cdot N$. Then $\mathrm{Z}(Q \cdot N) > \{1\}$ (Schur's lemma; also see the paragraph preceding the theorem) and $\mathrm{Z}(QN)$ is of order q since $r = 2$. One may assume that a notation is chosen so that $X_1 = \mathrm{Z}(QN)$. Let B be a maximal normal p-subgroup of G that is centralized by X_1. Since $\mathrm{Z}(G) = \{1\}$, we obtain $B < P$ and, obviously, $N \leq B$. By the choice of B, X_1 has no fixed points on P/B (see Lemma J(f), below). Let $Q = X_1 \times X_2$, where $X_2 < Q$ of order q has a nontrivial fixed point on P. Then X_2 has no fixed points on B (otherwise, we get $\mathrm{C}_P(Q) > \{1\}$ so that $r = q + 1 > 2$). Since the action of Q on P/B is not Frobenius, X_2 has a nontrivial fixed point on P/B (otherwise, $X_2 P$ is a Frobenius group, contrary to the choice of X_2). Let $P > P_1 > \cdots > B$ be a segment of a chief series of G. Since $X_1 P/B$ is a Frobenius group, X_1 has no nontrivial fixed point on factors of this segment, and we conclude that X_2 centralizes P/B (indeed, X_2 stabilizes all factors of this segment;

otherwise, $r > 2$, contrary to the hypothesis). Therefore, by Frattini's lemma applied to $X_2B \lhd X_2P$, we get

$$X_2P = \mathrm{N}_{X_2P}(X_2)X_2B = \mathrm{N}_{X_2P}(X_2)B,$$

and the last product is semidirect with kernel B since X_2B is a Frobenius group. We have $\mathrm{N}_{X_2P}(X_2) = X_2 \times \mathrm{C}_P(X_2)$. Therefore, by the modular law, we get

$$P = B(\mathrm{N}_{X_2P}(X_2) \cap P) = B\mathrm{C}_P(X_2) = \mathrm{C}_P(X_1)\mathrm{C}_P(X_2)$$

since $\mathrm{C}_P(X_1) = B$. Set $\mathrm{C}_P(X_2) = A$; then $P = AB$. Since $r = 2 < q + 1$, we get $A \cap B = \mathrm{C}_P(Q) = \{1\}$. Set $X_i = \langle x_i \rangle$, $i = 1, 2$ and take $a \in A$, $b \in B$. Then

$$[a^{x_1}, b] = [a, b]^{x_1} = [a, b]$$

since x_1 centralizes B and $[a, b] \in B$. It follows that $a^{x_1}a^{-1}$ centralizes b for all a, b. Next, $(a^{x_1}a^{-1})^{x_2} = a^{x_1}a^{-1}$ since $x_1x_2 = x_2x_1$ and x_2 centralizes $a \in A$. It follows that $a^{x_1}a^{-1} \in \mathrm{C}_P(x_2) = A$. If $a_1 \in A$ and $a^{x_1}a^{-1} = a_1^{x_1}a_1^{-1}$, then $(a_1^{-1}a)^{x_1} = a_1^{-1}a$ so $a_1 = a$ since X_1A is a Frobenius group. It follows that $\{a^{x_1}a^{-1} \mid a \in A\} = A$, and so $AB = A \times B$ since, by the above, all elements of A centralize B. □

Lemma A.30.2 (= Proposition 10.19). *If a metacyclic 2-group G has a nonabelian subgroup M of order 8, then it is of maximal class.*

Lemma A.30.3 (see Corollary A.9.2). *Suppose that G is a metacyclic p-group. If G satisfies $\pi(\mathrm{Aut}(G)) \not\subseteq \pi(p(p-1))$, then either we have $G \cong \mathrm{Q}_8$ or G is abelian of type (p^n, p^n). We have $\pi(\mathrm{Aut}(\mathrm{Q}_8)) = \{2, 3\}$ and $\pi(\mathrm{Aut}(\mathrm{C}_{p^n} \times \mathrm{C}_{p^n})) = \pi(p(p^2-1))$.*

Exercise 1. Let G be a metacyclic p-group, $p > 2$. If G has a nonabelian subgroup M of order p^3, then $M = G$. (*Hint*. See Proposition 10.19.)

In Lemma J we gather some known results which we use in what follows.

Lemma J. (a) (= Proposition 10.17) *Let B be a nonabelian subgroup of order p^3 in a p-group G. If $\mathrm{C}_G(B) < B$, then G is of maximal class.*

(b) *Let G be a p-group generated by two elements. Then*

$$\pi(|\mathrm{Aut}(G)|) \subseteq \pi(p(p^2 - 1)).$$

In particular, p is the maximal prime divisor of $|\mathrm{Aut}(G)|$ unless $p = 2$. If, in addition, G has a characteristic subgroup of index p, then $\pi(|\mathrm{Aut}(G)|) \subseteq \pi(p(p-1))$. In particular, if G is a 2-group of maximal class and $\mathrm{Aut}(G)$ is not a 2-group, then $G \cong \mathrm{Q}_8$ and $\mathrm{Aut}(\mathrm{Q}_8) \cong \mathrm{S}_4$.

(c) *Let α be a p'-automorphism of a p-group G acting trivially on $\Omega_1(G)$. If $p > 2$ or G is abelian, then $\alpha = \mathrm{id}_G$.*

(d) *If a p-group G has no normal abelian subgroup of type (p, p), then one of the following holds:* (i) *G is cyclic,* (ii) *G is a 2-group of maximal class nonisomorphic with* D_8. *(This follows from Lemma 1.4.)*

(e) (Theorem 13.7) *Let G be a p-group, $p > 2$. Suppose that G has no normal elementary abelian subgroup of order p^3. Then one of the following holds:*

(i) *G is metacyclic,*

(ii) *G is an irregular 3-group of maximal class not isomorphic to a Sylow 3-subgroup of the symmetric group of degree 3^2,*

(iii) *$G = EC$, where $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent p and C is cyclic.*

(f) *Let A be a π'-group acting on a π-group G. Let $\mathcal{C} : G = G_0 > G_1 > \cdots > G_n = \{1\}$ be a chain of A-invariant normal subgroups of G. If A centralizes all factors of the chain $\mathcal{C}$ (i.e., A stabilizes $\mathcal{C}$), then A centralizes G.*

(g) (Transfer theorem) *Suppose that a Sylow p-subgroup of a group G is abelian. If p divides $|Z(G)|$, then G has a normal subgroup of index p.*

According to Hall–Burnside, if α is a p'-automorphism of a p-group G inducing the identity on $G/\Phi(G)$, then $\alpha = \mathrm{id}_G$. Indeed, assuming, without loss of generality, that $o(\alpha)$ is a power of a prime, say q, we see that α fixes an element of every coset $x\Phi(G)$. Since these fixed elements generate G, our claim follows.

If d is a minimal number of generators of a p-group G, then (Hall) $|\mathrm{Aut}(G)|$ divides the number

$$(p^d - 1)(p^d - p) \ldots (p^d - p^{d-1})|\Phi(G)|^d;$$

this remark justifies the main assertion of Lemma J(b). If a two-generator p-group G possesses a characteristic subgroup H of index p and $\alpha \in \mathrm{Aut}(G)$ has prime order $q \notin \pi(p(p-1))$, then α stabilizes the chain $\{1\} < H/\Phi(G) < G/\Phi(G)$ (Maschke's theorem) so $\alpha = \mathrm{id}_G$ by what has just been said and (f), a contradiction. In (c), the partial holomorph $\langle\alpha\rangle \cdot G$ has no minimal nonnilpotent subgroup so it is p-nilpotent by Frobenius' normal p-complement theorem (here we use the structure of minimal nonnilpotent groups; see Lemma 10.8), and we conclude that $\alpha = \mathrm{id}_G$. Lemma J(g) follows from Wielandt's theorem [Hup, Satz 4.8.1] and Fitting's lemma (see Corollary 6.5). As to Lemma J(f), assume that A does not centralize G and $|AG|$ is as small as possible. Then AG is minimal nonnilpotent. In this case, such a chain as $\mathcal{C}$ does not exist (see Lemma 10.8), contrary to the hypothesis.

Recall that there are two representation groups of the symmetric group S_4, both of order 48, Sylow 2-subgroups of these groups are generalized quaternion and semidihedral, respectively (the second group is isomorphic to $\mathrm{GL}(2, 3)$).

Lemma A.30.4 ([Tho3, Lemma 5.41]). *Suppose that the following hold:*

(a) *G is a nonnilpotent solvable group.*

(b) $O_{2'}(G) = \{1\}$.

(c) *G has a proper noncyclic abelian subgroup of order* 8.

(d) *If K is any proper subgroup of G of index a power of* 2*, then K has no noncyclic abelian subgroup of order* 8.

Let $T \in \mathrm{Syl}_2(G)$. Then $T \lhd G$ and one of the following holds:

(i) *T is either elementary abelian or abelian of type* $(4,4)$.

(ii) *T is extraspecial of order 2^{2m+1}, $m > 1$.*

(iii) *T has a subgroup $T_0 \cong \mathrm{Q}_8$ of index* 2 *and $T = T_0\mathrm{Z}(T)$.*

(iv) *T is special and $\mathrm{Z}(T) \cong \mathrm{E}_4$.*

We omit the proof since the following theorem yields a more general result.

Theorem A.30.5. *Suppose that the following holds*

(a) *G is a nonnilpotent solvable group with a Sylow* 2*-subgroup T and a $2'$-Hall subgroup H.*

(b) $\mathrm{O}_{2'}(G) = \{1\}$.

(c) *Whenever K is a proper subgroup of G such that $|G : K|$ is a power of* 2*, then K has no noncyclic abelian subgroup of order* 8.

Then one and only one of the following assertions is true:

A. *If T is not normal in G, then either $G \cong \mathrm{S}_4$ or G is one of two representation groups of* S_4.

B. *If $T \lhd G$, then one of the following holds:*

B.1 *If T is abelian, then $T \in \{\mathrm{E}_{2^m}, \mathrm{C}_4 \times \mathrm{C}_4\}$.*

(B.1.1) *If $T \cong \mathrm{C}_4 \times \mathrm{C}_4$, then G is a Frobenius group with $|G : T| = 3$.*

(B.1.2) *Let $T \cong \mathrm{E}_{2^m}$ be not a minimal normal subgroup of G. Then either $G \in \{\mathrm{A}_4 \times \mathrm{C}_2, \mathrm{A}_4 \times \mathrm{A}_4\}$ or $m = 4$ and G is a Frobenius group with $|G : T| = 3$.*

B.2 *T is extraspecial of order 2^{2m+1}, $m \geq 1$. If $m = 1$, then $G \cong \mathrm{SL}(2,3)$. Next assume that $m > 1$.*

(B.2.1) *If $m > 2$, then $T/\mathrm{Z}(T)$ is a minimal normal subgroup of $G/\mathrm{Z}(T)$.*

(B.2.2) *If $T/\mathrm{Z}(T)$ is not a minimal normal subgroup of $G/\mathrm{Z}(T)$, then T is of the form $T = U * V$, where $U \cong V \cong \mathrm{Q}_8$, $U, V \lhd G$; in this case, $G/T \cong H$ is isomorphic to a subgroup of E_{3^2}. Moreover, in case that $H \cong \mathrm{E}_{3^2}$, we have $G = A*B$, where A, B satisfy $A \cong B \cong \mathrm{SL}(2,3)$ and $A \cap B = \mathrm{Z}(A) = \mathrm{Z}(B)$. If $|H| = 3$, then $UH \cong \mathrm{SL}(2,3) \cong VH$.*

B.3 *T has a G-invariant subgroup $T_0 \cong \mathrm{Q}_8$ of index* 2 *and $T = T_0\mathrm{Z}(T)$. In this case, $G/T' \cong \mathrm{A}_4 \times \mathrm{C}_2$, $G' = T_0$, and if $D/T_0 < G/T_0$ is of order* 3*, then $D \cong \mathrm{SL}(2,3)$.*

B.4 *T is special with $\mathrm{Z}(T) = \mathrm{Z}(G) \cong \mathrm{E}_4$ and $T/\mathrm{Z}(T)$ is a minimal normal subgroup of $G/\mathrm{Z}(T)$.*

Proof. Since $O_{2'}(G) = \{1\}$, a subgroup $T \in \mathrm{Syl}_2(G)$ is noncyclic (Lemma J(b)), $C_G(O_2(G)) \leq O_2(G)$ (Hall–Higman) so $O_2(G)$ is noncyclic and, if T is abelian, it is normal in G.

Suppose that T is abelian and $\exp(T) > 2$; then we get $T \lhd G$, $C_G(T) = T$ and $\Omega_1(T) \lhd G$. Next, $|G : \Omega_1(T)H| > 1$ is a power of 2 so $\Omega_1(T) \cong E_4$ since T is noncyclic. The number $|G : H\Omega_2(T)|$ is a power of 2 and $H\Omega_2(T)$ contains a noncyclic abelian subgroup of order 8, so we get $\Omega_2(T)H = G$ by hypothesis, and hence we obtain $\exp(T) = 4$. Since G has no normal 2-complement, T is abelian of type $(4, 4)$ (Lemma J(b)). Then $\Omega_1(T)H$ is a Frobenius group with kernel $\Omega_1(T)$ (otherwise, by Lemma J(c), $\{1\} < H \lhd G$) so $|H| = 3$; in this case, G is also a Frobenius group with kernel T, i.e., G is as in (B1.1).

Now suppose that $T \cong E_{2^m}$; then $m > 1$. If $m = 2$, then $G \cong A_4$. Let $m > 2$ and suppose that T is not a minimal normal subgroup of G. Then $T = R \times R_1$, where $R, R_1 > \{1\}$ are normal in G (Maschke) and, since $|G : RH| > 1$ and $|G : R_1H| > 1$ are powers of 2, we conclude that $|R| \leq 4$, $|R_1| \leq 4$ so $m \in \{3, 4\}$. In case $m = 3$, we get $G \cong A_4 \times C_2$. If $m = 4$, then G is either a Frobenius group with kernel $T \cong E_{2^4}$ of index 3 in G or $G \cong A_4 \times A_4$. Indeed, assume that G is not a Frobenius group; then $|H| > 3$. Setting $Z = C_H(R)$, $Z_1 = C_H(R_1)$, we get

$$|H : Z| = 3 = |H : Z_1| = 3 \quad \text{and} \quad Z \cap Z_1 \leq O_{2'}(G) = \{1\}$$

whence

$$H = Z_1 \times Z_2 \cong E_9, \quad RZ_1 \cong A_4 \cong R_1Z \quad \text{and} \quad G = (RZ_1) \times (R_1Z)$$

(here we used the fact that $\mathrm{Aut}(A_4) \cong S_4$).

Next we assume that T is nonabelian.

A. Suppose that $T \lhd G$.

(i) If T has no noncyclic abelian subgroup of order 8, then it has no normal abelian subgroup of type $(2, 2)$ unless $T \cong D_8$, hence, by Lemma J(d), T is of maximal class and, by Lemma J(b), $T \cong Q_8$, which is extraspecial; in this case, $G \cong \mathrm{SL}(2, 3)$.

Next we assume that T has a noncyclic abelian subgroup of order 8 so T is not of maximal class; then $|T| > 8$ since T is nonabelian.

(ii) Suppose that $K < G$ and $|G : K| = 2$; then K has no noncyclic abelian subgroup of order 8 by hypothesis. We obtain $O_{2'}(K) \leq O_{2'}(G) = \{1\}$, $T \cap K \lhd K$ is noncyclic and $T \cap K \ncong D_8$ (otherwise, K is 2-nilpotent since $\mathrm{Aut}(D_8) \cong D_8$) so that $T \cap K$ has no normal abelian subgroup of type $(2, 2)$ and we conclude that $T \cap K$ is of maximal class (Lemma J(d)). Since $\mathrm{Aut}(T \cap K)$ is not a 2-group, it follows that $T \cap K \cong Q_8$ and, since T is not of maximal class and $|T| = 16$, we get

$$T = (T \cap K)C_T(K \cap T) = (T \cap K)Z(T),$$

by Lemma J(a). Then, in view of Lemma J(b) and (a) (see the theorem), we conclude

that

$$|H| = |G : T| = 3, \quad (T \cap K)H \cong \mathrm{SL}(2,3), \quad G' = T \cap K, \quad G/G' \cong \mathrm{C}_6,$$

and so G is as in part (B3).

Next we assume that G has no subgroup of index 2; then we have $T \leq G'$. Let, in (iii–v), R be a G-invariant subgroup of T such that T/R is a minimal normal subgroup of G/R; then $R > \{1\}$ since T is nonabelian.

(iii) Since $|G : RH| > 1$ is a power of 2, R has no noncyclic abelian subgroup of order 8 by hypothesis (see (c)), so we have for R the following possibilities: either R is cyclic or $R \leq 4$ or $R \cong \mathrm{Q}_8$ (here we use Lemma J(b,d)).

(iv) Suppose that H centralizes R. Then $G/\mathrm{C}_G(R)$ is a 2-group so $\mathrm{C}_G(R) = G$ by part (ii). Thus we have $R \leq \mathrm{Z}(G)$. By hypothesis, $\mathrm{Z}(G)$ is a 2-subgroup and, in view of the maximal choice of R, we get $\mathrm{Z}(T) = R = \mathrm{Z}(G)$ (recall that $\mathrm{Z}(T) \lhd G$ since $T \lhd G$). Assume that $T' < R$. Then, by Lemma J(g) applied to the pair $T/T' < G/T'$, the group G/T' has a normal subgroup of index 2, contrary to (ii). Thus we obtain that $T' = R = \mathrm{Z}(T) = \Phi(T)$ so T is special since $\exp(T') \leq \exp(T/T') = 2$, and $R \in \{\mathrm{C}_2, \mathrm{E}_4, \mathrm{Q}_8\}$ by hypothesis. Therefore, if $|R| = 2$, then T is extraspecial.

(v) Suppose that T is extraspecial of order 2^{2m+1}, $m > 1$, and $|R| > 2$; then, by (iv), H does not centralize R (otherwise, $G/\mathrm{C}_G(R) > \{1\}$ is a 2-group). If $|R| = 4$, then $|T : \mathrm{C}_T(R)| = 2$ and $\mathrm{C}_T(R)H$ has index 2 in G, contrary to (ii) (note that $\mathrm{C}_T(R)$ is normal in G since R and T are; next, in view of $m > 1$, $\mathrm{C}_T(R)$ contains a noncyclic abelian subgroup of order 8). Thus $|R| > 4$ so $R \cong \mathrm{Q}_8$ by (iv). Let $R_1 = \mathrm{C}_T(R)$; then $R_1 \cong R \cong \mathrm{Q}_8$ by what has just been said. In this case, $T = R * R_1$ is extraspecial of order 2^5. Suppose that $|H|$ is not a prime. Setting $\mathrm{C}_H(R) = Z$ and $\mathrm{C}_H(R_1) = Z_1$, we get, by Lemma J(b),

$$|H/Z| = 3 = |H/Z_1|, \quad Z \cap Z_1 = \{1\}$$

and so

$$H = Z \times Z_1, \quad RZ_1 \cong \mathrm{SL}(2,3) \cong R_1 Z,$$

and we conclude that $G = (RZ_1) * (R_1 Z)$ with $(RZ_1) \cap (R_1 Z) = \mathrm{Z}(RZ_1)$. If $|H|$ is a prime, then $|G : T| = 3$ and, as above, $RH \cong \mathrm{SL}(2,3) \cong R_1 H$. Thus G is as in part (B2.2).

In what follows we assume that T is not extraspecial.

(vi) Suppose that T has a maximal G-invariant cyclic subgroup Z of order ≥ 4. One may choose in T a proper maximal G-invariant subgroup R (see (iii)) so that it contains Z. Then H centralizes Z so, by (iv), $Z \leq \mathrm{Z}(G)$. By Lemma J(d), R must be cyclic since.otherwise, R would have a noncyclic abelian subgroup of order 8; then H centralizes R, contrary to (iv) (by (iv), one has $R \in \{\mathrm{C}_2, \mathrm{E}_4, \mathrm{Q}_8\}$).

Thus T has no G-invariant cyclic subgroup of order 4 and so R is noncyclic. Therefore, by (iv), $R \in \{\mathrm{E}_4, \mathrm{Q}_8\}$.

(vii) Let $R \cong \mathrm{E}_4$. In this case, $\mathrm{C}_T(R)$ is normal in G and $|T : \mathrm{C}_T(R)| \leq 2$. As $|G : \mathrm{C}_T(R)H| \leq 2$, we get $\mathrm{C}_T(R) = T$ by (ii). Since T is nonabelian, it follows that $R = \mathrm{Z}(T)$ and T/R is elementary abelian by the maximal choice of R. As in (iv), we get $T' = R$ so $\Phi(T) = R$ and T is special.

(viii) Now let $R \cong \mathrm{Q}_8$. By (iv), we have $[R, H] > \{1\}$. In view of Lemma J(b), $G/\mathrm{C}_T(R)$ is a subgroup of the symmetric group S_4 containing a subgroup isomorphic to $R/\mathrm{Z}(R) \cong \mathrm{E}_4$. Since T is normal in G, it follows that $G/\mathrm{C}_T(R) \ncong \mathrm{S}_4$. Thus we have $|T : \mathrm{C}_T(R)| = 4 = |R : \mathrm{Z}(R)|$ so $|H| = 3$ and $T = R * \mathrm{C}_T(R)$ by the product formula. Hence we get $T/\mathrm{C}_T(R) \cong \mathrm{E}_4$. By (ii), $|T : R| > 2$ so $\mathrm{C}_T(R)$ is noncyclic of order > 4. Then, by Lemma J(d), $\mathrm{C}_T(R) \cong \mathrm{Q}_8$ so $T \cong \mathrm{Q}_8 * \mathrm{Q}_8 (\cong \mathrm{D}_8 * \mathrm{D}_8)$ is extraspecial of order 2^5. (Note that both factors of the second decomposition of R are not normal in G since $\mathrm{Aut}(\mathrm{D}_8) \cong \mathrm{D}_8$.)

The case where T is normal in G, is complete.

B. Now suppose that T is not normal in G. Then we infer that $T_0 = \mathrm{O}_2(G) > \{1\}$ since $\mathrm{O}_{2'}(G) = \{1\}$ and G is solvable. Since $|G : T_0H| > 1$ is a power of 2, T_0 is a group from Lemma J(d). It follows from $\mathrm{C}_G(T_0) \leq T_0$ that T_0 is noncyclic, and if T_0 is of maximal class, then $T_0 \cong \mathrm{Q}_8$ (Lemma J(b)). Thus $T_0 \in \{\mathrm{E}_4, \mathrm{Q}_8\}$.

If $T_0 \cong \mathrm{E}_4$, then $G \cong \mathrm{S}_4$ since $\mathrm{Aut}(\mathrm{E}_4) \cong \mathrm{S}_3$.

Now let $T_0 \cong \mathrm{Q}_8$. As $\mathrm{Aut}(T_0) \cong \mathrm{S}_4$ (Lemma J(b)), we see that $G/\mathrm{Z}(T_0)$ is isomorphic to a nonnilpotent subgroup of S_4 containing the subgroup $T_0/\mathrm{Z}(T_0) \cong \mathrm{E}_4$ of even index (by assumption, $T_0 < T$). We conclude that $\mathrm{C}_T(T_0) < T_0$ so T is of maximal class, namely, T is generalized quaternion or semidihedral of order 16 (Lemma J(a)). It follows that $G/\mathrm{Z}(T_0) \cong \mathrm{S}_4$ so G is a representation group of the group S_4.

Since all groups listed in the conclusion of the theorem satisfy the hypothesis, the proof is complete. □

Of course, it is possible to make the proof of Theorem A.30.5 shorter using Theorem A.30.4, however, we preferred to give an independent proof.

Next we expand Theorem A.30.5 to groups of odd order.

Theorem A.30.6. *Let G be a nonnilpotent group and let $p > 2$ be the least prime divisor of $|G|$. Suppose that the following hold:*

(a) $\mathrm{O}_{p'}(G) = \{1\}$.

(b) *Whenever K is a proper subgroup of G such that $|G : K|$ is a power of p, then K has no subgroup $\cong \mathrm{E}_{p^3}$.*

Let $T \in \mathrm{Syl}_p(G)$. Then T is normal in G and one and only one of the following assertions holds:

A. *T is a minimal normal subgroup of G, $\mathrm{d}(T) > 2$.*

B. *T is special of exponent p with $\mathrm{Z}(T) = \mathrm{Z}(G)$ of order at most p^2, $T/\mathrm{Z}(T)$ is a minimal normal subgroup of $G/\mathrm{Z}(T)$.*

Proof. Since G has odd order, it is solvable by the Odd Order Theorem, hence, in view of (a), $C_G(O_p(G)) \leq O_p(G)$ and so, if T is abelian, it is normal in G. Conditions (a) and (b) restrict the structure of $O_p(G)$. By Lemma J(b), $O_p(G)$ is not two-generator. Let H be a p'-Hall subgroup of G.

$(*)$ (1) Let U be two-generator p-group, $p > 2$. Then the number $|\mathrm{Aut}(U)|$ divides $(p^2-1)(p-1)p^k$ for some integer k. It follows that p is the largest prime divisor of $|\mathrm{Aut}(U)|$. (2) Let $M < T$ be nonidentity G-invariant. We contend that H centralizes M. Indeed, since $|G : MH| > 1$ is a power of p, it follows that M is a group from Lemma J(e) by hypothesis. Then, by (1), H centralizes M if $d(M) \leq 2$. Now let $d(M) > 2$. Then, by Lemma J(e), we obtain that $M = \Omega_1(M) * C$ (central product), where $\Omega_1(M)$ is nonabelian of order p^3 and exponent p and C is cyclic of order $> p$. Note that we have $\Omega_1(M) \lhd G$. By (1), H centralizes $\Omega_1(M)$ so H centralizes M by Lemma J(c).

1. Let $T \lhd G$.

(i) Assume that T is a group from Lemma J(e). Then, as in $(*)$, H centralizes T so H is normal in G, which is a contradiction. Thus T possesses a subgroup $\cong E_{p^3}$; then, by Theorem 10.4, T has a normal subgroup $\cong E_{p^3}$.

(ii) Suppose that T is abelian. Since $|G : H\Omega_1(T)|$ is a power of p and, by part (i), $\Omega_1(T)$ has a subgroup $\cong E_{p^3}$, we obtain $T = \Omega_1(T)$ hence T is elementary abelian. Assume that $T = V_1 \times V_2$, where $V_1 > \{1\}$ and $V_2 > \{1\}$ are normal in G. Then we get $|V_i| \leq p^2$ $(i = 1, 2)$ since $V_i H$ has no subgroup $\cong E_{p^3}$, so, by part (1) of $(*)$, H centralizes V_i, $i = 1, 2$ (Lemma J(b)). In this case, H centralizes T by part (2) of $(*)$, which is not the case. Thus T is a minimal normal subgroup of G (Maschke).

Next we assume that T is nonabelian; then $|T| \geq p^4$ by part (1) of $(*)$.

(iii) Assume that p divides $|G : G'|$. In this case, G has a normal subgroup F of index p. By hypothesis, $T \cap F$ has no subgroup $\cong E_{p^3}$, so that $T \cap F$ is as in Lemma J(e). As above, H centralizes $T \cap F$. Then H stabilizes the chain $\{1\} < T \cap F < T$ so that $H \lhd G$ (Lemma J(f)), a contradiction. Thus p does not divide $|G : G'|$, and we conclude that $T < G'$.

(iv) Let $A < T$ be a G-invariant subgroup. We claim that $A \leq Z(G)$. Assume that this is false. Since H centralizes A by $(*)$, $C_G(A)$ is normal in G and $G/C_G(A)$ is a p-group $> \{1\}$ (indeed, $p > 2$ is the least prime divisor of $|G|$ and $|G/C_G(A)|$ divides $|\mathrm{Aut}(A)|$), contrary to (iii).

(v) Let $R < T$ be G-invariant and such that T/R is minimal normal in G/R. Then, by (iv), $R \leq Z(T)$; moreover, $R = Z(T)$ by the maximal choice of R since T is nonabelian. It follows that $\mathrm{cl}(T) = 2$ so, since $p > 2$, we get $\exp(\Omega_1(T)) = p$. By (i), T possesses a subgroup $E \cong E_{p^3}$. Since $E \leq \Omega_1(T)$ and $|G : H\Omega_1(T)|$ is a power of p, we get $G = H\Omega_1(T)$ so $T = \Omega_1(T)$ is of exponent p. It remains to show that T is special. Since $|G : RH| > 1$ is a power of p, it follows that R is elementary abelian of order $\leq p^2$. If $T' < R$, then, by Lemma J(g) applied to the pair $T/T' < G/T'$, the

quotient group G/T' has a normal subgroup of index p, contrary to (iii). Thus we get $T' = R$. Since $\exp(T) = p$, we have $T' = \Phi(T)$. Hence $\mathrm{Z}(G) = R = T' = \Phi(T)$ so T is special.

We see that if T is nonabelian, then it is special of exponent p with $R = T'$ of order $\leq p^2$. By the maximal choice of R, T/R is a minimal normal subgroup of G/R so the case where T is normal in G, is complete.

It remains to show that $T \lhd G$.

2. Now assume that T is not normal in G. Since $\mathrm{O}_{p'}(G) = \{1\}$ and G is solvable, we get $T > T_0 = \mathrm{O}_p(G) > \{1\}$. Therefore we have $\mathrm{C}_G(T_0) \leq T_0$ so H acts faithfully on T_0. Since $|G : T_0H| > 1$ is a power of p, T_0 has no elementary abelian subgroup of order p^3. It follows that T_0 is a group of Lemma J(e). However, as the argument in part (i) shows, H centralizes T_0, a final contradiction.

Since groups from parts A and B satisfy the hypothesis, the proof is complete. □

Note that if G is a 2-group without normal elementary abelian subgroup of order 8, then it has a normal metacyclic subgroup M such that G/M is isomorphic to a subgroup of D_8 (§50). Therefore it is natural to classify the nonnilpotent solvable groups G satisfying (i) $\mathrm{O}_{2'}(G) = \{1\}$ and (ii) if $K < G$ is such that $|G : K|$ is a power of 2, then K has no elementary abelian subgroup of order 8. However, the proof of such result would be very long since the groups appearing in §50 are not so small as groups from Lemma J(e).

Theorem A.30.6 also holds for each odd prime divisor p of $|G|$ such that $|G|$ and $p^2 - 1$ are coprime (in this case, $|G|$ is odd so solvable; if, for example, $p = 11$ is not the minimal prime divisor of $|G|$, then 7 is the minimal prime divisor of $|G|$). To prove this, we have to repeat word for word the proof of Theorem A.30.6.

Lemma A.30.7 ([Tho3, Lemma 5.35]). *Suppose that M is a subgroup of even order of a group G such that M_G is of odd order and M contains the centralizer of each of its involutions (therefore, $|G : M|$ is odd). Then the following hold:*

(a) *All involutions are conjugate in G.*

(b) *If, in addition, M contains $\mathrm{N}_G(T)$ for $T \in \mathrm{Syl}_2(M)$, then all involutions are also conjugate in M.*

Proof. We have $M < G$ since $|M_G|$ is odd and $|M|$ is even.

(a) Let $x \in M$ be a fixed involution and $y \in G$ be any involution which is not conjugate to x. Then $D = \langle x, y\rangle$ is either abelian of type $(2, 2)$ or a dihedral group of order divisible by 4 (indeed, if 4 does not divide $|D|$, then all involutions are conjugate in D by Sylow). In any case, D has a central involution $z \notin \{x, y\}$. We get $z \in \mathrm{C}_G(x) \leq M$ and $y \in \mathrm{C}_G(z) \leq M$. Thus all involutions that are not conjugate with x in G are contained in M so in M_G since the set of such involutions is a union of G-classes. It follows that M_G has even order, contrary to the hypothesis. Thus y does not exist hence all involutions are conjugate in G, proving (a).

Let, in addition, $\mathrm{N}_G(T) \le M$ for $T \in \mathrm{Syl}_2(M)$.

(b) Let $x \in \mathrm{Z}(G)$ and $y \in M$ be involutions. Then $y = x^g$ for some $g \in G$ by (a). We have

$$T^g \le \mathrm{C}_G(x)^g = \mathrm{C}_G(x^g) = \mathrm{C}_G(y) \le M$$

by hypothesis, so $T^g \in \mathrm{Syl}_2(M)$. By Sylow, we get $T^g = T^u$ for some $u \in M$ so that $T^{gu^{-1}} = T$. It follows that $gu^{-1} \in \mathrm{N}_G(T) \le M$ hence $g \in M$. Thus x, y are conjugate in M, proving (b). □

Exercise 2 ([Tho3, Lemma 5.38(a)]). Suppose that G is a group of even order without subgroups of index 2. Let $T \in \mathrm{Syl}_2(G)$ and let M be a maximal subgroup of index 2 in T. Then for each involution a of G there is an element $g \in G$ such that $a^g \in M$.

Solution. Consider the representation P of G by permutations of left cosets of M in G. If a has no fixed points, then the permutation $P(a)$ is a product of $\frac{1}{2}|G : M| = |G : T|$ independent transpositions so it is an odd permutation; in this case, G has a subgroup of index 2 (consider the intersection of G with $\mathrm{A}_{|G:M|}$, the alternating group of degree $|G : M|$), a contradiction. Thus a has a fixed point, say gM for some $g \in G$, i.e., we have $agM = gM$; then $a^g \in M$, as desired.

Let G and T be as in Exercise 2. Suppose, in addition, that T is of maximal class. Then all involutions are conjugate in G. Indeed, let M be a cyclic subgroup of index 2 in T and $x \in M$ the involution. Then, by Exercise 2, all involutions of G are conjugate with x, as required.

Exercise 3 ([Tho3, Lemma 5.38(b)]). Suppose that $G = A \cdot T$ is a semidirect product, where $T \in \mathrm{Syl}_2(G)$ is elementary abelian and normal in G, A is of odd order. Suppose that $\mathrm{C}_G(A) \le A$. Let $x \in T^{\#}$ and $M < T$ be of index 2. Then there is an element $a \in A$ with $x^a \in M$.

Lemma A.30.8. *Let $G = E \cdot P$ be a semidirect product with kernel $P \in \mathrm{Syl}_p(G)$ which is elementary abelian for $p > 2$, $E \in \mathrm{Syl}_2(G)$ is extraspecial of order 2^{2n+1}. If E acts faithfully on P, then $\mathrm{d}(P) \ge 2^n$.*

Proof. Since $\mathrm{Z}(E)$ is the unique minimal normal subgroup of E, one may assume that P is a minimal normal subgroup of G (here we use Maschke's theorem). From the fact that $E \le \mathrm{C}_G(\mathrm{Z}(E))$ is maximal in G it follows that $P \cap \mathrm{C}_G(\mathrm{Z}(E))$ is E-invariant so G-invariant, and we infer that $\mathrm{C}_G(\mathrm{Z}(E)) = E$ whence $\mathrm{Z}(E)P$ is a Frobenius group. Therefore $\mathrm{C}_G(P) = P$ so that $\mathrm{d}(P) > 1$ since E is noncyclic. Hence the lemma holds for $n = 1$.

Now suppose that $n > 1$ and let $x \in E - \mathrm{Z}(E)$ be such that $V = \mathrm{C}_P(x) > \{1\}$ (x exists since $E \cdot P$ is not a Frobenius group in view of $n > 1$; see [BZ, Lemma 10.3]). Then x is an involution (indeed, if $o(x) = 4$, then $\langle x^2 \rangle$, being generator of $\mathrm{Z}(E)$, acts fixed-point-freely of P). Then V is H-invariant, where $H = \mathrm{C}_E(x)$, and $|E : H| = 2$. By Lemma 4.2, $H = F\mathrm{Z}(H)$, where F is extraspecial of order 2^{2n-1} and $\mathrm{Z}(H)$ is

abelian of type $(2,2)$. Let V_1 be a minimal F-invariant subgroup of V. Since $\mathrm{Z}(H)$ is noncyclic, P is not a minimal normal subgroup of $H \cdot P$ so that P is not a minimal normal subgroup of $F \cdot P$. By Maschke's theorem, we get $P = V_1 \times V_2$, where V_2 is F-invariant. Working by induction on n and taking into account that F acts faithfully on V_1 and V_2 (indeed, $\mathrm{Z}(E)P = \mathrm{Z}(F)P$ is a Frobenius group), we obtain

$$\mathrm{d}(P) = \mathrm{d}(V_1) + \mathrm{d}(V_2) \geq 2^{n-1} + 2^{n-1} = 2^n,$$

as required. □

A small modification of the above argument with reference to the exercise in §1 of [Hup3] shows that if E acts faithfully and irreducibly on P, then $\mathrm{d}(P) = 2^n$ (by that exercise, if $E \cong \mathrm{Q}_8$, then $\mathrm{d}(P) = 2$).

Exercise 4. A Sylow 3-subgroup of $\mathrm{GL}(4,2)$ is elementary abelian of order 3^2.

Hint. It is easy to check that $|\mathrm{GL}(4,2)|_3 = 3^2$. Now the result follows from the fact that $\mathrm{GL}(4,2)$ has a subgroup isomorphic to $\mathrm{GL}(2,2) \times \mathrm{GL}(2,2) \cong \mathrm{S}_3 \times \mathrm{S}_3$.

Exercise 5. An extraspecial group of order 2^5 has exactly 20 nonabelian subgroups of order 8.

Exercise 6. An extraspecial group of order 2^{2n+1} has exactly $2^{2n-2}(2^{2n}-1)/3$ nonabelian subgroups of order 8. The same question holds for extraspecial groups of order p^{2n+1} with odd p. (*Hint*. See Example 76.1.)

The following result is a variant of [Shu, Theorem 1].

Theorem A.30.9. *Let A be an abelian subgroup of a group G and suppose that whenever $A \leq K \leq S \leq G$, where K is nilpotent and $|S : K|$ is a prime power, then A satisfies $A \leq \mathrm{Z}(S)$. Then $A \leq \mathrm{Z}(G)$.*

Proof. The hypothesis is inherited by subgroups containing A.

Suppose that G is nilpotent. If $p \in \pi(A)$ and $S \in \mathrm{Syl}_p(G)$, then we get $A \leq \mathrm{Z}(AS)$ by hypothesis. It follows that A is centralized by the $\pi(A)$-Hall subgroup of G. In case $p \in \pi(G) - \pi(A)$, we see that the Sylow p-subgroup of G centralizes A. Thus we get $A \leq \mathrm{Z}(G)$.

Let G be a counterexample of minimal order. Then, by the previous paragraph, G is nonnilpotent. If $A \leq M$, where M is maximal in G, then we get $A \leq \mathrm{Z}(M)$ by induction. It follows that $\mathrm{C}_G(A) = M$ is the unique maximal subgroup of G containing A.

(i) Assume that $A^G < G$, where A^G is the normal closure of A in G. Then we get $A \leq \mathrm{Z}(A^G) \lhd G$ by induction, so $A \leq \mathrm{Z}(A^G) \lhd G$. It follows that A^G is abelian. Let P be an arbitrary Sylow subgroup of G. Then A^G is a nilpotent subgroup of prime power index in $A^G P$, so $A \leq \mathrm{Z}(A^G P)$ by assumption. We see that all Sylow subgroups of G centralize A so $A \leq \mathrm{Z}(G)$, contrary to the assumption. Thus $A^G = G$ so the maximal subgroup M of G containing A is not normal in G.

(ii) Assume that G has an abelian minimal normal subgroup N. By hypothesis, we have $A \leq \mathrm{Z}(AN)$ since $|AN : A|$ divides $|N|$ which is a power of a prime. Then we see that $\mathrm{C}_G(N)$ is a normal subgroup of G containing A. In this case, we obtain that $G = A^G \leq \mathrm{C}_G(N)$ hence $N \leq \mathrm{Z}(G)$, and we conclude that $|N| = p$ is a prime. Let S/N be a subgroup of G/N containing a nilpotent subgroup K/N of prime power index such that $AN/N \leq K/N$. Then K is a nilpotent subgroup (since $N \leq \mathrm{Z}(G)$) containing A so we get $A \leq \mathrm{Z}(S)$ by hypothesis. It follows that $AN/N \leq \mathrm{Z}(S/N)$ hence $AN/N \leq \mathrm{Z}(G/N)$ by induction. In particular, AN is normal in G. By (i), we get $AN = G$, and G is abelian since AN is. This is a contradiction. Thus G has no nontrivial normal abelian subgroup.

(iii) Now suppose that $1 \neq y \in M \cap M^g < M$ for some $g \in G$ (about M, see the paragraph preceding (i)). Then $A, A^g \leq \mathrm{C}_G(y)$ since $A \leq \mathrm{Z}(M)$ and $A^g \leq \mathrm{Z}(M^g)$, and $\mathrm{C}_G(y) < G$ since G has no nontrivial abelian normal subgroup by (ii). From the fact that $A \leq \mathrm{C}_G(y)$ we infer $\mathrm{C}_G(y) \leq M$ by (i). But also M^g is the unique maximal subgroup of G containing A^g and y centralizes A^g; then we have $A \leq \mathrm{C}_G(y) \leq M^g$ and $M = M^g$, contrary to the choice of g. Thus $M \cap M^g = \{1\}$ for all $g \in G - M$. By Frobenius' theorem (see [BZ, §10.2, page 271]), G is a Frobenius group with complement M and kernel, say N. Then N is an abelian minimal normal subgroup of G (here we use Thompson's theorem on the nilpotence of the Frobenius kernel), contrary to part (ii). □

Since the subgroups S from Theorem A.30.9 are solvable (Wielandt–Kegel), we get the following

Corollary A.30.10 ([Shu, Theorem 1]). *Let A be an abelian subgroup of a group G and suppose that A lies in the center of every solvable subgroup of G which contains A. Then A lies in the center of G.*

Corollary A.30.11 (I. N. Herstein). *A group G containing an abelian maximal subgroup is solvable.*

Indeed, assuming that G is nonsolvable, we get $A \leq \mathrm{Z}(G)$ by Corollary A.30.10, and this is a contradiction since then $|G : A|$ is a prime.

Exercise 7. Prove Corollary A.30.11, using (i) Frobenius' theorem on the existence of the Frobenius kernel, (ii) Burnside's normal p-complement theorem.

Exercise 8. Try to prove an analog of Lemma A.30.8 in the case where E is an extraspecial q-group with $q > 2$. Is it true that in this case $\mathrm{d}(P) \geq q^{n\beta}$, where β is a positive integer minimal such that q divides $p^\beta - 1$?

Appendix 31

Nilpotent p'-subgroups of class 2 in GL(n, p)

In this section we classify the nilpotent p'-subgroups of class at most 2 and order at least $(p^{\frac{1}{2}n}-1)^2$ in the general linear group $\mathrm{GL}(n, p)$ of degree n over the field $\mathrm{GF}(p)$. First we prove that the order of an abelian p'-subgroup in $\mathrm{GL}(n, p)$ is at most $p^n - 1$ (Lemma A.31.1). It appears that the same inequality holds in the case where A is of class at most 2.

Lemma A.31.1. *If A is an abelian p'-subgroup in* $\mathrm{GL}(n, p)$*, then we have $|A| < p^n$. If, in addition, $|A| = p^n - 1$, then A is cyclic and irreducible.*

Proof. The group A given in the statement above acts faithfully on the n-dimensional vector space $V = V(n, \mathrm{GF}(p))$. We have to prove that $|A| < |V|$.

Suppose that A acts irreducibly on V. Assume that there are $a \in A^{\#}$ and $v \in V - \{0\}$ such that $av = v$. Then we have $\mathrm{C}_{AV}(a) > A$ so $\mathrm{C}_{AV}(a) = AV$ since A is maximal in AV by assumption. This is a contradiction since A acts faithfully on V. Thus AV is a Frobenius group with kernel V and complement A so A is cyclic (Schur's lemma). In this case, $|A|$ divides $|V| - 1$, proving the claim.

Now suppose that A acts reducibly on V. Then, by Maschke's theorem, we conclude that $V = V_1 \oplus V_2$, where V_1 and V_2 are nontrivial A-invariant subspaces of V. The equality $\mathrm{C}_A(V_1) \cap \mathrm{C}_A(V_2) = \{1\}$ implies that A is isomorphic to a subgroup of $(A/\mathrm{C}_A(V_1)) \times (A/\mathrm{C}_A(V_2))$. Clearly, $A/\mathrm{C}_A(V_i)$ acts faithfully on V_i, $i = 1, 2$. Therefore, by induction,

$$|A| \leq |A/\mathrm{C}_A(V_1)||A/\mathrm{C}_A(V_2)| < |V_1||V_2| = |V|,$$

as desired. (According to the remark of Isaacs, the first assertion of the lemma also follows from Brodkey's theorem: if $P \in \mathrm{Syl}_q(G)$ is abelian, then there exists $x \in G$ such that $P \cap P^x = P_G$; see Appendix 3.)

Next, suppose that $|A| = |V| - 1$. Then it follows from the argument of the previous paragraph that A acts irreducibly on V. Then A is cyclic (see [BZ, Exercise 10.3(b)]) since AV is a Frobenius group by the second paragraph of the proof. □

Theorem A.31.2 (Glauberman [Gla3]). *Let A be a nilpotent p'-subgroup in* $\mathrm{GL}(n, p)$ *of class at most* 2*. Then $|A| \leq p^n - 1$.*

Proof (P. Shumyatsky). One may assume that A acts faithfully on the vector space $V = V(n, \mathrm{GF}(p))$. We must prove that $|A| < |V|$. We proceed by induction on n.

As in the proof of Lemma A.31.1, one may assume that

(i) A is irreducible. In particular, A is maximal in AV.

By (i) and Schur's lemma,

(ii) $\mathrm{Z}(A)$ is cyclic.

Since A acts faithfully on V, it follows that

(iii) $\mathrm{Z}(A)V$ is a Frobenius group. In particular, $|\mathrm{Z}(A)|$ divides $|V^{\#}| = p^n - 1$.

Assuming that AV is a counterexample of minimal order, i.e., $|A| > |V|$ ('>' since $(|A|, |V|) = 1$), we get, in view of (iii),

(iv) A is nonabelian, i.e., $\mathrm{cl}(A) = 2$.

If AV is a Frobenius group, then we conclude that $|A|$ divides $|V^{\#}| = p^n - 1$ (see [BZ, Exercise 10.3]). Therefore, since G is a counterexample, we get

(v) AV is not a Frobenius group.

Then there exists an element $a \in A$ of prime order q such that $V_1 = \mathrm{C}_V(a) \neq \{0\}$. Since $a \notin \mathrm{Z}(A)$ by (iii), we get

(vi) A Sylow q-subgroup of A is nonabelian. In particular, q^3 divides $|A|$.

Put $N = \mathrm{C}_A(a)$. Since q divides $|\mathrm{Z}(A)|$ (indeed, $\pi(\mathrm{Z}(A)) = \pi(A)$ since A is nilpotent) and $\langle a, \mathrm{Z}(A)\rangle = \langle a\rangle \times \mathrm{Z}(A)$ (recall that $o(a) = q$ is a prime), it follows by (ii) that $\langle a, \mathrm{Z}(A)\rangle$ possesses a characteristic subgroup $\langle a, z\rangle = \langle a\rangle \times \langle z\rangle$ of type (q, q), where $z \in \Omega_1(\mathrm{Z}(A))^{\#}$. Because A is of class 2, we infer that $\langle a, \mathrm{Z}(A)\rangle$ is normal in the group A, and therefore $\langle a, z\rangle$, being characteristic in $\langle a, \mathrm{Z}(A)\rangle$, is normal in A so $|A : \mathrm{C}_A(\langle a, z\rangle)| = q$ ('=' since $a \in A - \mathrm{Z}(A)$ and q^2 does not divide the order of the automorphism group of the abelian group of type (p, p)). Hence

(vii) $|A : N| = q$ ('=' since $\mathrm{C}_A(a) = \mathrm{C}_A(\langle a, z\rangle)$ and $z \in \Omega_1(\mathrm{Z}(A)^{\#})$, where we set $N = \mathrm{C}_A(a)$.

Put $C = \mathrm{C}_N(V_1)$ (since $V_1 = \mathrm{C}_V(a)$, one has $a \in C$). Since N normalizes V_1, the subgroup $C > \{1\}$ is normal in N. It then follows from (iii) that $C \cap \mathrm{Z}(A) = \{1\}$. In particular, since $A' \leq \mathrm{Z}(A)$, we get $C \cap A' = \{1\}$; therefore, $[C, N] \leq C \cap A' = \{1\}$ so that

(viii) $C \leq \mathrm{Z}(N)$ is abelian.

Take $b \in A - N$; then $A = \langle b, N\rangle$ and $b^q \in N$ by (vii). Since

$$V_0 = V_1 + V_1^b + \cdots + V_1^{b^{q-1}}$$

is invariant with respect to $\langle b, N\rangle = A$, we have $V_0 = V$. It is clear that

(ix) $V = V_1 \oplus V_1^b \oplus \cdots \oplus V_1^{b^{q-1}}$. Thus $\dim(V_1) = \frac{n}{q}$.

Assume that $C = \langle a\rangle$. As $o(a) = q = |A : N|$, we get $|N : C| = \frac{1}{q}|N| = \frac{1}{q^2}|A|$ (see (vii)). Next, since N/C acts faithfully on V_1 because $C = \mathrm{C}_N(V_1)$, it follows by

induction that

$$\frac{1}{q^2}|A| = |N/C| < |V_1|.$$

Considering the q-th powers of both sides of the displayed inequality and taking into account that AV is a minimal counterexample, we obtain, by induction (see (ix)),

$$(|A|/q^2)^q < |V_1|^q = |V| < |A|$$

so that $|A|^{q-1} < q^{2q}$. Since, by (vi), q^3 divides $|A|$, we get $q^{3(q-1)} < q^{2q}$, hence $q^q < q^3$, and we conclude that $q = 2$. Then

$$|A| = |A|^{q-1} < q^{2q} = 2^4, \quad |A| = 8 > |V|.$$

But $|V| < 8$ implies that a Sylow 2-subgroup of the group $\mathrm{GL}(V)$ is abelian, contrary to (iv). Thus

(x) $C > \langle a \rangle$.

Assume that $\mathrm{C}_N(V_1) = C$ contains a subgroup Q of type (r, r) for some prime r. Then $\mathrm{C}_V(x) = V_1$ for every $x \in Q^\#$. Indeed, let $\mathrm{C}_V(x) = V_2$; then $V_2 \geq V_1$. Arguing with x as with a, we obtain $\dim(V_2) = \frac{n}{r}$ and $|A : \mathrm{C}_A(x)| = r$. Since $\mathrm{C}_A(x) \geq N$ by (viii) and $\mathrm{C}_A(x) < A$, we get $r = q$. It follows that $\dim(V_2) = \frac{n}{q} = \dim(V_1)$ so $V_1 = V_2$. Next, we have $V = \sum_{x \in Q^\#} \mathrm{C}_V(x)$ (see [BZ, p. 351]). But $\mathrm{C}_V(x) = V_1$ for all $x \in Q^\#$, and therefore $V_1 = V$, contrary to (vii). By (viii), C is abelian so, since it has no subgroup of type (q, q), we get

(xi) C is cyclic, $|C| > q$ (the last inequality follows from (x)).

Put $C = \langle y \rangle$. Since $y \in C \leq \mathrm{Z}(N)$ by (viii) and $b^q \in N$, where $b \in A - N$, we conclude that $[y^q, b] = [y, b^q] = 1$ as $\mathrm{cl}(A) = 2$. Therefore $\mathrm{C}_A(y^q) \geq \langle b, N \rangle = A$, i.e., $y^q \in \mathrm{Z}(A)$. But $\mathrm{C}_{AV}(y^q) \geq \langle A, V_1 \rangle = AV$ since A is maximal in AV. This proves that $1 \neq y^q \in \mathrm{C}_A(V)$, i.e., A does not act faithfully on V. This contradiction proves the theorem. □

Exercise 1. Let A be an abelian p'-subgroup of $\mathrm{GL}(n, p^m)$. Prove that

(a) $|A| \leq p^{mn} - 1$.

(b) If $|A| = p^{mn} - 1$, then A is irreducible so cyclic.

Consider the case where A is a nilpotent p'-subgroup of class at most 2 in $\mathrm{GL}(n, p^m)$.

Exercise 2 ([BZ, Lemma 7.65]). Let A be a nilpotent p'-subgroup of $\mathrm{GL}(n, p)$ of class at most 2, and $|A| = p^n - 1$. Check if it is true that A is irreducible and one of the following holds:

(a) A is cyclic.

(b) $A \cong \mathrm{D}_8$.

(c) $A = \mathrm{Q}_8 \times C$, where C is cyclic of odd order.

Elements of Glauberman's original proof can be found in the proof of the following theorem.

Theorem A.31.3 ([BZ, Theorem 7.66]). *If A is a nilpotent p'-subgroup of* GL(n, p) *of class at most* 2 *and order* $\geq (p^{\frac{1}{2}n} - 1)^2$*, then one of the following holds:*

(a) *A is the direct product of two groups of degree $p^{n/2}$ and order $p^{\frac{1}{2}n} - 1$ (see Exercise* 2*; obviously, A is reducible since its center is noncyclic).*

(b) $A \cong \mathrm{D}_8$, $p^n = 3^2$.

(c) *A is an irreducible subgroup of* GL$(2, 5)$ *of order* 16, $\mathrm{Z}(\mathrm{GL}(2, 5)) = \mathrm{Z}(A)$.

(d) *Either $A = \mathrm{Q}_8 \times C$, where C is cyclic of odd order, or A is cyclic.*

Proof. One may assume that A acts faithfully on the vector space $V = V(n, \mathrm{GF}(p))$ (we will also regard V as E_{p^n}). We proceed by induction on $|AV|$.

Assume that A is reducible. Then, by Maschke's theorem, $V = V_1 \oplus V_2$, where V_1 and V_2 are proper A-invariant subspaces of V. Set $A_i = \mathrm{C}_A(V_i)$, $i = 1, 2$. Since

$$A_1 \cap A_2 = \mathrm{C}_A(V_1) \cap \mathrm{C}_A(V_2) = \mathrm{C}_A(V) = \{1\},$$

it follows that A is isomorphic to a subgroup of the direct product $(A/A_1) \times (A/A_2)$. By Theorem A.31.2, we have $|A/A_i| \leq |V_i| - 1$, $i = 1, 2$. Therefore

$$(|V|^{\frac{1}{2}} - 1)^2 \leq |A| \leq |A/A_1||A/A_2| \leq (|V_1| - 1)(|V_2| - 1)$$

and so

$$|V_1| + |V_2| \leq 2|V|^{\frac{1}{2}} = 2(|V_1||V_2|)^{\frac{1}{2}}.$$

It follows that $|V_1| = |V_2| = |V|^{\frac{1}{2}}$ and

$$|A| = (|V|^{\frac{1}{2}} - 1)^2, \quad |A/A_i| = |V|^{\frac{1}{2}} - 1, \quad i = 1, 2.$$

Therefore A is the direct product of two groups of order $p^{\frac{1}{2}n} - 1$ of Exercise 2.

Now assume that A is irreducible; then A is maximal in the semidirect product AV, $\mathrm{Z}(A)V$ is a Frobenius group so $\mathrm{Z}(A)$ is cyclic [BZ, Lemma 10.3]. Assume that A is nonabelian. If $x \in \mathrm{Z}(A)^{\#}$, then x induces a fixed-point-free automorphism on V (otherwise, $\mathrm{C}_V(x) \neq \{0\}$ is a normal subgroup of $\mathrm{C}_{AV}(x) = A\mathrm{C}_V(x)$; then $\mathrm{C}_V(x) = V$ and x induces the identity automorphism on V, contrary to the assumption).

Let $F_0 = \mathrm{C}_{\mathrm{End}(V)}(A)$. Then F_0 is a finite division algebra over GF(p) (Schur) and therefore commutative (Wedderburn). Let F be a subfield of F_0 generated by the elements of $\mathrm{Z}(A)$; $F = \mathrm{GF}(q)$, where q is a power of p; set $d = \dim_F(V)$.

If all subgroups of order r^2 ($r \in \pi(A)$) of A are cyclic, then A is one of the groups in (d) by Lemma 1.4 (recall, that A is of class 2 and this explain the term Q_8). We therefore assume that there exists an element g of order r in $A - \mathrm{Z}(A)$, where r is a prime divisor of $|A|$ (g exists since $\mathrm{Z}(A)$ is cyclic). Observe that r divides $|\mathrm{Z}(A)|$ since A is

nilpotent. Then we conclude that $B_1 = \langle g, \mathrm{Z}(A)\rangle = \langle g\rangle \times \mathrm{Z}(A)$ is not cyclic. From $A' \leq \mathrm{Z}(A) < B_1$ (indeed, $\mathrm{cl}(A) = 2$) we infer that B_1 is a proper normal subgroup in A (by the above, the Sylow r-subgroup of B_1 is abelian and the Sylow r-subgroup of A is nonabelian). Since $B_1 = \mathrm{O}_r(B_1)\mathrm{Z}(A)$ and $\mathrm{O}_r(B_1)$ is normal in A, it follows that $\mathrm{C}_A(B_1) = \mathrm{C}_A(\mathrm{O}_r(B_1))$ (indeed, $\mathrm{C}_A(B_1) = \mathrm{C}_A(g)$). But $|A : \mathrm{C}_A(\mathrm{O}_r(B_1))| = r$ since $B_1 = \langle g\rangle \times \mathrm{Z}(A)$. Therefore, putting $B = \mathrm{C}_A(B_1)$, we obtain $|A : B| = r$. Take an irreducible FB_1-submodule U_1 in the FB_1-module V, and let V_1 be the sum of all of the FB_1-submodules of V isomorphic to U_1. Since the kernels of the actions of B_1 on U_1 and V_1 coincide, they are nontrivial since B_1 is noncyclic abelian (Schur's lemma), it follows that $V_1 < V$. By Clifford's theorem, $V = V_1 \oplus \cdots \oplus V_m$, where the submodules $V_1, \ldots, V_m$ are conjugate with respect to A.

Put $K = \mathrm{C}_B(V_1)$ (recall that $B = \mathrm{C}_A(B_1)$ has index r in A).

If $b \in B$, then bV_1 is isomorphic to V_1 as an FB_1-module. Therefore $bV_1 = V_1$ for any $b \in B$, and since $|A : B| = r$, it is clear that B is the inertia group of V_1 in A. Hence $m = |A : B| = r$.

Take $x \in A - B$. Then $x^r \in B$, $\langle x, B\rangle = A$ and $\langle x\rangle$ acts transitively on the set $\{V_1, \ldots, V_r\}$. Observe that $K = \mathrm{C}_B(V_1)$ acts trivially on V_1. Therefore $\mathrm{C}_K(x)$ acts trivially on $V_1, \ldots, V_r$. Indeed, if $v_i \in V_i$, $v_i = x^i v_1$, $y \in \mathrm{C}_K(x)$, then, for all i,

$$y v_i = y(x^i v_1) = x^i (y v_1) = x^i v_1 = v_i.$$

It follows that $\mathrm{C}_K(x)$ acts trivially on $V_1 \oplus \cdots \oplus V_r = V$, and so $\mathrm{C}_K(x) = \{1\}$. Since K is normal in B, we obtain

$$[B, K] \leq K \cap A' \leq K \cap \mathrm{Z}(A) = \{1\}$$

since $\mathrm{Z}(A)V$ is a Frobenius group with kernel V. This means that $K \leq \mathrm{Z}(B)$.

Take $y \in K$; then $z = [y, x] \in A' \leq \mathrm{Z}(A)$. We have $x^{-s} y x^s = y z^s$ for any positive integer s. Taking $s = r$, we obtain $z^r = 1$ since $x^r \in B = \mathrm{C}_A(K) = \{1\}$. Hence $[y, x] \in \Omega_1(\mathrm{O}_r(\mathrm{Z}(A))$ for $y \in K$.

Define a mapping $\phi : K \to \Omega_1(\mathrm{O}_r(\mathrm{Z}(A))$ by $\phi(y) = [y, x]$ $(y \in K)$. Since A is of class 2, ϕ is a homomorphism. Next,

$$\ker(\phi) = \{y \in K \mid [y, x] = 1\} \leq \mathrm{C}_K(x) = \{1\}.$$

Therefore $|K| \leq |\Omega_1(\mathrm{O}_r(\mathrm{Z}(A)))| = r$. Put $c = \dim_F(V_1)$. Then $\dim_F(V) = d = cr$. From the fact that B/K acts faithfully on V_1, it follows that $|B/K| \leq |V_1| - 1 = q^c - 1$ (Theorem A.37.2). Therefore

$$|A| = |A/B| \cdot |B/K| \cdot |K| \leq r^2(q^c - 1).$$

Since r divides $|\mathrm{Z}(A)|$ and $|\mathrm{Z}(A)| \leq |F| - 1 = q - 1$, we have $r \leq q - 1$. By hypothesis,

$$(|V|^{\frac{1}{2}} - 1)^2 \leq |A| \leq r^2(q^c - 1).$$

(i) Let $r = 2$. Then $p > 2$ since A is a p'-group. Therefore

$$(q^c - 1)^2 \leq |A| \leq 4(q^c - 1),$$

and hence $q^c \leq 5$. Thus $q^c \in \{3, 5\}$ since q is odd, $|V| \in \{3^2, 5^2\}$.

(1i) Suppose that $|V| = 3^2$. Then we infer that A is a subgroup of class 2 in GL$(2, 3)$ (of order 48). Since a Sylow 2-subgroup of GL$(2, 3)$ is semidihedral of order 16, it follows that $|A| = 8$. If $A = \mathrm{Q}_8$, then $AV = (\mathrm{Q}_8, \mathrm{E}_{3^2})$, a Frobenius group of order 72. In case $A \ncong \mathrm{Q}_8$, we get $A \cong \mathrm{D}_8$.

(2i) Suppose that $|V| = 5^2$. Then we see that A is a $\{2, 3\}$-subgroup in GL$(2, 5)$ and $|A| \geq (5 - 1)^2 = 16$. As $|A| < |V| = 25$ (Theorem A.31.2) and A is nonabelian, it follows that A is a 2-group by the structure of GL$(2, 5)$. Since A is a maximal nilpotent subgroup of class 2 in GL$(2, 5)$, we have $\mathrm{Z}(\mathrm{GL}(2, 5)) \leq A$. From the structure of the quotient group $\mathrm{GL}(2, 5)/\mathrm{Z}(\mathrm{GL}(2, 5)) \cong \mathrm{PGL}(2, 5) \cong \mathrm{S}_5$ it is evident that only two types of groups of order 16 may be "candidates" for the role of A.

(ii) Suppose that $r > 2$. Then

$$(q - 1)^2(q^c - 1) \geq r^2(q^c - 1) \geq |A| \geq (q^{\frac{1}{2}cr} - 1)^2 > (q^{\frac{1}{2}cr} - 1)(q^c - 1)$$

whence

$$(q^{\frac{1}{2}cr} - 1) < (q - 1)^2, \quad \frac{cr}{2} < 2.$$

It follows that $cr = 3$, $c = 1$, $r = 3$, and we have

$$(q^{\frac{3}{2}} - 1)^2 \leq (q - 1)^3, \quad 3q^2 + 2 \leq 2q^{\frac{3}{2}} + 3q,$$

but this is impossible for $q \geq 2$. The proof is complete. □

Problems

Problem 1. Prove an analog of Theorem A.31.2 for S_{p^n}.

Problem 2. Find the maximum of orders of abelian subgroups (nilpotent subgroups of class at most 2, nilpotent subgroups) in GL(n, p).

Problem 3. Find the maximum of ranks of abelian (nilpotent) subgroups in GL(n, p).

Problem 4. Find the maximum of orders of solvable subgroups (resp. solvable p'-subgroups) in GL(n, p).

Problem 5. Find the maximum of orders of p'-subgroups in GL(n, p).

Problem 6. Investigate analog situations for subgroups of GL(n, p^m), SL(n, p) and PGL(n, p).

Appendix 32

On abelian subgroups of given exponent and small index

In this section we present some results on the existence of abelian normal subgroups of given exponent and index in a p-group. Let $a_{1,k}(X)$ be the number of abelian subgroups of index $p = p^1$ and exponent $\leq p^k$ in a p-group X. By $a_1(X)$ we denote the number of abelian subgroups of index p in a p-group X.

Lemma A.32.1. *Suppose that a p-group G possesses an abelian subgroup of exponent $\leq p^k$ and index p.*

(a) *If $p > 2$, then $a_{1,k}(G) \equiv 1 \pmod{p}$.*

(b) *If $p = 2$, then the number $a_{1,k+1}(G)$ is odd.*

Proof. Let A, A_1 be distinct abelian subgroups of exponent $\leq p^k$ and index p in G. Then $A \cap A_1 \leq \mathrm{Z}(G)$ so that $G = AA_1$ is of class at most 2 (we do not assume that G is nonabelian), and we conclude that $\exp(G) \leq p^k$ if $p > 2$ and $\exp(G) \leq 2^{k+1}$ if $p = 2$ (obviously, $\exp(G) \leq p \exp(A)$). Now the result follows by Exercise 1.6(a) since our numbers are equal to $a_1(G)$. □

Lemma A.32.2. *Let G be a group of order p^m. If G possesses an abelian subgroup A of exponent $\leq p^k$ and index p^2, then G possesses a normal abelian subgroup of same index and exponent $\leq p^k$ if $p > 2$ and exponent $\leq 2^{k+1}$ if $p = 2$.*

Proof. Let $A < M < G$; then $M \in \Gamma_1$ and $|M : A| = p$. Now the result follows from Lemma A.32.1 since $M \lhd G$. □

Below we use the following remark. In case that T is a subgroup of exponent p^k and index p^s, then $\exp(G) \leq p^{k+s}$. Moreover, $x^{p^s} \in T$ for all $x \in G - T$. Indeed, let $x \in G - T$ and $T \leq M \in \Gamma_1$; then $|M : T| = p^{s-1}$. We have $x^p \in M$ so, using induction on $|G|$, we obtain $(x^p)^{p^{s-1}} \in T$ whence $o(x^{p^s}) \leq \exp(T) \leq p^k$. It follows that $o(x) \leq p^{k+s}$, as claimed.

Theorem A.32.3. *Suppose that a normal subgroup H of a p-group G, $p > 2$, possesses an abelian subgroup A of index p^2 and exponent $\leq p^k$. Then the following hold:*

(a) *If $p > 3$, then H possesses a G-invariant abelian subgroup of exponent $\leq p^k$ and index p^2.*

(b) *If $p = 3$, then H possesses a G-invariant abelian subgroup of exponent $\leq 3^{k+1}$ and index 3^2.*

Proof. Due to Lemma A.32.2, H possesses an H-invariant abelian subgroup, say B, of index p^2 and exponent $\leq p^k$. One may assume that B is not normal in G. By Lemma A.32.1, we get $|B^G : B| > p$ hence $B^G = H$ since $H \lhd G$. Since $|H : B| = p^2$ and $B \lhd H$, it follows that there exist $x, y \in G - H$ such that $BB^xB^y = H$. From Fitting's lemma (see Introduction, Theorem 21) we infer that $\mathrm{cl}(H) \leq 3$ so H is regular if $p > 3$, and then H of exponent $\leq p^k$ contains a G-invariant abelian subgroup of index p^2 by Theorem 103.5(iii). In what follows we assume that $p = 3$. In this case, $\exp(BB^x) \leq 3^k$ so, by the remark, preceding the theorem, $\exp(H) \leq 3^{k+1}$, and the result follows from Theorem 103.5(iii). □

In particular, if a p-group G, $p > 2$, possesses an abelian subgroup A of index p^3 and exponent $\leq p^k$, then A^G possesses a G-invariant abelian subgroup A_1 of order $|A|$ and exponent $\leq p^k$ if $p > 3$ and exponent 3^{k+1} if $p = 3$.

Denote by $p^{e_k(G)}$ the maximum of orders of regular subgroups of exponent $\leq p^k$ in a p-group G.

Theorem A.32.4. *Let G be a p-group, $p > 2$. Then*

(a) *If G has an abelian subgroup A of exponent $\leq p^k$ and order $p^{e_k(G)}$, then A^G has a G-invariant abelian subgroup B of order $p^{e_k(G)}$ and exponent $\leq p^k$. Moreover, B contains all normal abelian subgroups of G of exponent $\leq p^k$.*

(b) *If G has an abelian subgroup A of exponent $\leq p^k$ and order $p^{e_k(G)-1}$ and $p > 3$, then A^G possesses a G-invariant abelian subgroup of order $p^{e_k(G)-1}$ and exponent $\leq p^k$.*

(c) *If G has an abelian subgroup A of exponent $\leq p^k$ and order $p^{e_k(G)-2}$ and $p > 3$, then A^G possesses a G-invariant abelian subgroup of order $p^{e_k(G)-2}$ and exponent $\leq p^k$.*

Proof. We use induction on $|G|$. One may assume that $A < G$. Then we have $A^G < G$. Clearly, $e_k(A^G) = e_k(G)$.

(a) By induction, A^G has a normal abelian subgroup B of order $p^{e_k(G)}$ and exponent $\leq p^k$ containing all normal abelian subgroups of A^G of exponent $\leq p^k$. Since B is also *characteristic* in A^G, it is normal in G. Let E be a normal abelian subgroup of G of exponent $\leq p^k$. Since $\mathrm{cl}(BE) \leq 2$ and $p > 2$, BE is regular so $\exp(BE) \leq p^k$, and we get $E \leq B$ since B is a maximal regular subgroup of G.

(b) By induction, A^G has a normal abelian subgroup B of order $p^{e_k(G)-1}$ and exponent $\leq p^k$. Suppose that B is not normal in G. Then $B^g \neq B$ for some $g \in G$. In this case, by Fitting's lemma, $\mathrm{cl}(BB^g) \leq 2$ since $B, B^g \lhd A^G$, and so $\exp(BB^g) \leq p^k$ since $p > 2$. Set $H = BB^g$; then $H < G$ since $BB^g \leq B^G < G$. Since H is regular, we get, by hypothesis, $|H| = p^{e_k(G)}$. If H is normal in G, it contains a G-invariant abelian subgroup of index p, so of order $p^{e_k(G)-1}$, and exponent $\leq \exp(H) \leq p^k$ by

Lemma A.32.1. So suppose that H is not normal in G. Then we have $H^x \neq H$ for some $x \in G$. By Fitting's lemma, we infer that $\mathrm{cl}(HH^x) \leq 4$ so it is regular since $p \geq 5$ (we have $H, H^x \lhd A^G$). We get a contradiction since $|HH^x| > |H| = p^{e_k(G)}$ and $\exp(HH^x) \leq p^k$.

(c) By induction, A^G has a normal abelian subgroup B of order $p^{e_k(G)-2}$ and exponent $\leq p^k$. Suppose that B is not normal in G and let H be defined as in (b). Then we obtain that $p^{e_k(G)-1} \leq |H| \leq p^{e_k(G)}$ since H is regular of exponent $\leq p^k$. In case that H is normal in G of order $p^{e_k(G)-1}$, we are done by Lemma A.32.1. If $H \lhd G$ of order $p^{e_k(G)}$, then we see that the number of abelian subgroups of index p^2 in H is either $\equiv 1 \pmod p$ or $\equiv 2 \pmod p$ by Theorem 103.5(iii), and we are done since one of these subgroups is G-invariant of exponent $\leq \exp(H) \leq p^k$. Suppose that H is not normal in G. Then there exists $x \in G$ such that $B^x \not\leq H$. In this case, we obtain $\mathrm{cl}(HB^x) \leq 3$ by Fitting's lemma (we have $H, B^x \lhd A^G$, so HB^x is regular since $p > 3$ and $\exp(HB^x) \leq p^k$ by Theorem 7.1(b)). We have $|HB^x| = p^{e_k(G)}$ by hypothesis. Assume that HB^x is not normal in G. Then there exists $y \in G$ such that $B^y \not\leq HB^x$. In this case, HB^xB^y is of class at most 4 so regular since $p \geq 5$, and we obtain that $\exp(HB^xB^y) \leq p^k$. Since $|HB^xB^y| > p^{e_k(G)}$, we get a contradiction. □

Corollary A.32.5. *Let G be a p-group of maximal class, $p > 2$ and $k > 1$.*

(a) *If G has an abelian subgroup A of order $p^{(p-1)k}$ and exponent p^k, then A is the unique abelian subgroup of order $p^{(p-1)k}$ and exponent p^k.*

(b) *If G has an abelian subgroup A of order $p^{(p-1)k-1}$ and exponent p^k, then it has a normal abelian subgroup of same order and exponent.*

(c) *If $p > 3$ and G has an abelian subgroup A of order $p^{(p-1)k-2}$ and exponent p^k, then it has a normal abelian subgroup of same order and exponent.*

Proof. If $\exp(G) = p^k$, we conclude that $|G| = p^{(p-1)k+1}$. In this case, (a) follows from Fitting's lemma and (b), (c) follow from Theorem 103.5(iii) and Lemma A.32.2. In what follows we assume that $\exp(G) > p^k$. In the case under consideration, we get $e_k(G) = p^{(p-1)k}$ (see Theorems 9.6).

(a) It follows from Theorems 9.6 and A.32.4(a) that G has a normal abelian subgroup, say A, of order $p^{(p-1)k}$ and exponent p^k and $A = \Omega_k(G_1)$, where G_1 is the fundamental subgroup of G.

(b) Let $p = 3$. Then $(3-1)k - 1 \geq 3$ so $A \leq \Omega_k(G_1)$ (see §9). Then $\Omega_k(G_1)$ has a G-invariant abelian subgroup of order $3^{(3-1)k-1}$ since $\Omega_k(G_1)$ is either abelian or minimal nonabelian. Let $p > 3$. Then $(p-1)k - 1 > p$ so again $A \leq \Omega_k(G_1)$, and the same argument works.

(c) Let $p > 3$. Then, as in (b), A has index p^2 in $\Omega_k(G_1)$. By Theorem 103.5(iii), the number of abelian subgroups of index p^2 in $\Omega_k(G)$ is not divisible by p hence the result follows. □

Appendix 33

On Hadamard 2-groups

Let G be a group of order $4n$ containing a central involution e^*, and let T be a transversal of G with respect to $\langle e^* \rangle$. If T and Tr intersect in n elements, where r is any element of G outside of $\langle e^* \rangle$, then T and G are called an *Hadamard subset* and *Hadamard group* (with respect to $\langle e^* \rangle$), respectively. A cyclic group of order 4 is an Hadamard group with $n = 1$, and n is even for other Hadamard groups. As a rule, it is difficult to check whether G is or is not an Hadamard group. In this section we are interested in Hadamard 2-groups.

The following theorem allows us to build new Hadamard groups from known ones.

Theorem A.33.1 (Ito). *Suppose that a 2-group G of order $8n$ contains an Hadamard subgroup H of index 2 with respect to an involution $e^* \in \mathrm{Z}(H)$. If there is $r \in G - H$ such that $r^2 = e^*$, then G is also an Hadamard group with respect to e^*.*

Proof. Since $\mathrm{C}_G(e^*) \geq \langle r, H \rangle = G$, we get $e^* \in \mathrm{Z}(G)$. Let E be an Hadamard subset of H with respect to e^* and put $D = Ee^* \cup Er$. We show that D is an Hadamard subset of G. Let s be an element of H outside of $\langle e^* \rangle$. Then $rs = rsr^{-1}r$ and rsr^{-1} is an element of H outside of $\langle e^* \rangle$ since $H, \langle e^* \rangle \lhd G$. So we have

$$\begin{aligned} |D \cap Ds| &= |Ee^* \cap Ee^*s| + |Ersr^{-1}r \cap Er| \\ &= |(E \cap Es)e^*| + |(Ersr^{-1} \cap E)r| = n + n = 2n \end{aligned}$$

since E is an Hadamard subset of H. Now any element of the set $G - H$ is of the form tr for some $t \in H$. If $t = 1$, then $Dtr = Dr = Er^2 \cup Ee^*r = Ee^* \cup Ee^*r$ (recall that $r^2 = e^*$). Since Ee^* and Ee^*r are disjoint, we have $|D \cap Dr| = |Ee^*| = 2n$. If $t = e^*$, then

$$Dtr = De^*r = Ee^*e^*r \cup Ere^*r = Er \cup E.$$

We have

$$D \cap De^*r = (Ee^* \cup Er) \cap (Er \cup E) = Er,$$

so $|D \cap De^*r| = |Er| = 2n$. If $t \in G - \langle e^* \rangle$, then $rtr = rtr^{-1}r^2 = rtr^{-1}e^*$ and $rtr^{-1} \in H - \langle e^* \rangle$. So we have $Dtr = Ee^*tr \cup Ertr^{-1}e^*$ and hence

$$|D \cap Dtr| = |(E \cap Ertr^{-1})e^*| + |(E \cap Ete^*)r| = n + n = 2n,$$

completing the proof. □

Exercise 1. Prove that Q_8 is an Hadamard group. (*Hint.* The Hadamard subgroup C_4 is maximal in Q_8. Use Theorem A.33.1.)

For definition and properties of one-stepped p-groups, see the text preceding Exercise 17 in Introduction (recall that a p-group is said to be *one-stepped* if it is generated by elements of order p). By Exercise 17(b) from Introduction, any p-group is isomorphic to a subgroup of an appropriate one-stepped p-group (namely, a Sylow p-subgroup of S_{p^n} for a sufficiently large positive integer n).

Proposition A.33.2 (Ito). *Let G be an Hadamard 2-group with respect to $\langle e^* \rangle$ such that $e^* = r^2$ for some $r \in G$ and let H be a one-stepped 2-group. Then $G \times H$ is an Hadamard group with respect to $\langle e^* \rangle$.*

Proof. Suppose that $|H| = 2^n$ and let $r_1, \ldots, r_n$ be n distinct involutions in H such that $|\langle r_1, \ldots, r_i \rangle| = 2^i$ for $i = 1, \ldots, n$. Then we have $(rr_i)^2 = r^2 r_i^2 = e^*$ for each i. By Theorem A.33.1, $G_1 = \langle G, rr_1 \rangle$ is Hadamard. Again, by the same theorem, we see that $G_2 = \langle G_1, rr_2 \rangle$ is Hadamard. Finally, $G \times H = \langle G, rr_1, \ldots, rr_n \rangle$ is Hadamard, as desired. □

Theorem A.33.3 (Ito). *Every 2-group is a subgroup of an Hadamard 2-group.*

Proof. Let F be a 2-group. Then there exists a positive integer n such that F is isomorphic to a subgroup of Σ_{2^n}, a Sylow 2-subgroup of the symmetric group of degree 2^n. Let $H \cong Q_8$; then H is Hadamard with respect to $\langle e^* \rangle$, where e^* is the unique involution of H by Exercise 1. If r is an arbitrary element of H of order 4, then $r^2 = e^*$. By Proposition A.33.2, $H \times \Sigma_{2^m}$ is Hadamard since Σ_{2^m} is one-stepped (Lemma 64.2); that group possesses a subgroup which is isomorphic to F. □

Exercise 2. Prove that Q_{2^m} is Hadamard.

Solution. In view of Exercise 1, one may assume that $m > 3$. Assume that we have proved that $Q_{2^{m-1}}$ is Hadamard and let $Q_{2^{m-1}} \cong H < G \cong Q_{2^m}$ be of index 2; then we see that H is Hadamard with respect to its unique involution e^*. If $r \in G - H$ is of order 4, then $r^2 = e^*$, and hence G is Hadamard with respect to e^* (Theorem A.33.1).

Exercise 3. Let $H \cong Q_{2^n}$ be a maximal subgroup of a 2-group G. If G is not of maximal class, then it is Hadamard.

Solution. Let e^* be the unique involution of H. As G is not of maximal class, there exists in G an even number of cyclic subgroups of order 4 by Theorem 1.17(b). Let $C = \langle r \rangle$ be a cyclic subgroup of order 4 in G that is not contained in H; such a C exists since H possesses an odd number of cyclic subgroups of order 4. As r^2 is an involution in H, we get $r^2 = e^*$. By Theorem A.33.1, G is Hadamard, as required.

Exercise 4. Prove that the abelian group of type $(2^2, 2)$ is Hadamard.

Hint. The cyclic group of order 4 is Hadamard. But G has exactly two cyclic subgroups of order 4. Use Theorem A.33.1.

Theorem A.33.4 (Ito). *The semidihedral group* SD_{2^n} *is not Hadamard.*

Corollary A.33.5. (a) *The cyclic group* C_{2^n} *is not Hadamard for* $n > 2$.

(b) *The dihedral group* D_{2^n} *is not Hadamard.*

Proof. (a) $C = \mathrm{C}_{2^n}$ is a maximal subgroup of $G = \mathrm{SD}_{2^{n+1}}$. The set $G - C$ possesses an element r of order 4 such that r^2 is the unique involution in C. If C is Hadamard, then $\mathrm{SD}_{2^{n+1}}$ is (Theorem A.33.1), contrary to Theorem A.33.4.

(b) $D = \mathrm{D}_{2^n}$ is a maximal subgroup of $G = \mathrm{SD}_{2^{n+1}}$. Repeat the argument in (a) with D instead of C and G being the same. □

Theorem A.33.6 (Ito). *The group* M_{2^n} *is not Hadamard.*

This follows from Corollary A.33.5(a) and Theorem A.33.1 since $n < 3$.

Exercise 5. The group $\mathrm{Q}_{2^n} \times \mathrm{E}_{2^m}$ is Hadamard. (*Hint*. Use Theorem A.33.1.)

Exercise 6. Let $G = A \times B$, where A and B are 2-groups of maximal class. Classify the pairs A, B such that G is Hadamard.

Exercise 7. Classify the extraspecial 2-groups G of order 2^{2m+1}, $m > 1$, which are Hadamard.[1]

Exercise 8. Suppose that $G = \langle x_1, \ldots, x_n \rangle$ is such that $|\Phi(G)| = 2$ and $o(x_i) = 4$ for $i = 1, \ldots, n$. Then G is a Hadamard group. (*Hint*. Use Theorem A.33.1.)

Proposition A.33.7. *Let* H *be a maximal subgroup of a* 2*-group* G*. Suppose that* H *is not Hadamard with respect to any of its central involutions, let* $G = \langle r, H \rangle$*, where* r *is an element of order* 4 *such that* $r^2 = e^*$ *with* e^* *being an involution in* $\mathrm{Z}(H)$*. Then* G *is not Hadamard with respect to* $\langle e^* \rangle$.

Proof. Assume that this is false and T is an Hadamard subset of G with respect to $\langle e^* \rangle$. In this case, $E = T \cap H$ is a transversal of H with respect to $\langle e^* \rangle$; then E is not an Hadamard subset of the subgroup H. Using the last fact, we can prove, as in the proof of Theorem A.33.1, that T is not an Hadamard subset with respect to $\langle e^* \rangle$. □

Problem 1 (Ito). Classify the abelian Hadamard groups.

Problem 2 (Ito). Classify the Hadamard groups with cyclic subgroup of index 2.

Problem 3. Classify the minimal nonabelian 2-groups that are Hadamard.

[1] It follows from Exercise 8 below that G is Hadamard if it is generated by elements of order 4.

Appendix 34

Isaacs–Passman's theorem on character degrees

In this section we will classify the p-groups G with $\mathrm{cd}(G) = \{1, p\}$. We closely follow [Isa1, Chapter 12].

S. Amitsur was the first who studied the groups G satisfying $\mathrm{cd}(G) = \{1, 2\}$. Then Isaacs and Passman [IsaP1] have obtained the general result classifying the groups G with $\mathrm{cd}(G) = \{1, p\}$ for arbitrary prime p.

Exercise 1 ([Isa1, Theorem 12.3]). Let G be a nonabelian p-group. If G' is the unique minimal normal subgroup of G, then $|G : \mathrm{Z}(G)| = f^2$, where $\mathrm{cd}(G) = \{1, f\}$.

Exercise 2. (a) (Taketa) Let G be an M-group satisfying $\mathrm{cd}(G) = \{f_1, \dots, f_k\}$, where $1 = f_1 < \cdots < f_k$. Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = f_i$. Then $G^{(i)} \le \ker(\chi)$, where $G^{(i)}$ is the i-th term of the derived series of G.[1]

(b) If G is a p-group with $\mathrm{cd}(G) = \{1, p^e\}$, e a positive integer, then G' is abelian.

Solution. (a) Since this is true for $i = 1$, assume that $i > 1$ and work by induction on i. If $\psi \in \mathrm{Irr}(G)$ and $\psi(1) = f_j < f_i$, then we have $G^{(i-1)} \le G^{(j)} \le \ker(\psi)$. There exist a subgroup $H < G$ and $\lambda \in \mathrm{Lin}(G)$ such that $\chi = \lambda^G$. Now, the degrees of all irreducible constituents of $(1_H)^G$ are less than $|G : H| = f_i$ (indeed, $1_G \in \mathrm{Irr}((1_H)^G)$) so $G^{(i-1)} \le \ker((1_H)^G) = H_G \le H$. Since

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \le H' \le \ker(\lambda)_G = \ker(\chi),$$

we are done.

Statement (b) follows from (a) since G is monomial by [BZ, Theorem 7.61].

Lemma A.34.1 ([Isa1, Theorem 12.7]). *Let $N \lhd G$ and suppose that $\vartheta_1, \vartheta_2 \in \mathrm{Irr}(N)$ are G-invariant and $\vartheta_1\vartheta_2 \in \mathrm{Irr}(N)$. Let $\chi_i \in \mathrm{Irr}(\vartheta_i^G)$, $i = 1, 2$, and $\psi \in \mathrm{Irr}(\chi_1\chi_2)$. Then $\psi(1)\chi_1(1) \ge \chi_2(1)\vartheta_1(1)^2$.*

Proof. We have $0 \ne \langle \chi_1\chi_2, \psi\rangle = \langle \chi_2, \psi\bar{\chi}_1\rangle$ so that $\chi_2 \in \mathrm{Irr}(\psi\bar{\chi}_1)$. By Clifford's theorem, since ϑ_2 is G-invariant, we have $(\chi_2)_N = e\vartheta_2$, where $e = \frac{\chi_2(1)}{\vartheta_2(1)}$. Thus we get $(\chi_2)_N = \frac{\chi_2(1)}{\vartheta_2(1)}\vartheta_2$. Therefore we have

$$\frac{\chi_2(1)}{\vartheta_2(1)} = \langle \vartheta_2, (\chi_2)_N\rangle \le \langle \vartheta_2, (\psi\bar{\chi}_1)_N\rangle \le \langle \vartheta_2(\chi_1)_N, \psi_N\rangle. \tag{1}$$

[1] It follows that our M-group G is solvable. Indeed, $G^{(k)} \le \ker(\rho_G) = \{1\}$, where ρ_G is the regular character of G.

As in (1), since ϑ_1 is G-invariant, we get $(\chi_1)_N = \frac{\chi_1(1)}{\vartheta_1(1)}\vartheta_1$, and (1) implies

$$\frac{\chi_2(1)}{\vartheta_2(1)} \leq \frac{\chi_1(1)}{\vartheta_1(1)}\langle \vartheta_1\vartheta_2, \psi_N\rangle. \tag{2}$$

Now, by Clifford's theorem, being G-invariant, $\vartheta_1\vartheta_2$ is the unique irreducible constituent of ψ_N, and thus $\langle \vartheta_1\vartheta_2, \psi_N\rangle = \frac{\psi(1)}{\vartheta_1(1)\vartheta_2(1)}$. Substituting this in (2), we get

$$\frac{\chi_2(1)}{\vartheta_2(1)} \leq \frac{\chi_1(1)}{\vartheta_1(1)}\frac{\psi(1)}{\vartheta_1(1)\vartheta_2(1)}$$

hence $\psi(1)\chi_1(1) \geq \chi_2(1)\vartheta_1(1)^2$, as desired. □

Corollary A.34.2 ([Isa1, Corollary 12.8]). *Let $N \lhd G$ and suppose that $\beta \in \mathrm{Irr}(G)$ with $N \leq \mathrm{Z}(\beta)$, where $\mathrm{Z}(\beta)$ denotes the quasikernel of β. Let $\vartheta \in \mathrm{Irr}(N)$. Then there exists a positive integer c such that $c\vartheta(1) \in \mathrm{cd}(G)$ and $c^2 \geq \beta(1)t$, where $t = |G : \mathrm{I}_G(\vartheta)|$ (here $\mathrm{I}_G(\vartheta)$ is the inertia subgroup of ϑ in G).*

Proof. Let $T = \mathrm{I}_G(\vartheta)$ and $\gamma \in \mathrm{Irr}(\beta_T)$. Then we get $\beta \in \mathrm{Irr}(\gamma^G)$ by reciprocity, and so $\beta(1) \leq \gamma^G(1) = \gamma(1)t$, where $t = |G : \mathrm{I}_G(\vartheta)|$. Since $N \leq \mathrm{Z}(\gamma)$, one can write $\gamma_N = \gamma(1)\lambda$ with $\lambda \in \mathrm{Lin}(N)$. Let $\xi \in \mathrm{Irr}(\vartheta^T)$ and let $\eta \in \mathrm{Irr}(\xi\gamma)$. Note that η_N is a multiple of ϑ since $(\xi\gamma)_N = \xi_N\gamma_N$, ξ_N is a multiple of $\vartheta\lambda$ and γ_N is a multiple of the linear character λ by reciprocity. Since $\vartheta\lambda \in \mathrm{Irr}(N)$, Lemma A.34.1 applies to the above characters of T, and so

$$\xi(1)\eta(1) \geq \gamma(1)\vartheta(1)^2.$$

Thus

$$\xi^G(1)\eta^G(1) = \xi(1)t\,\eta(1)t \geq \gamma(1)t^2\vartheta(1)^2 \geq \beta(1)t\,\vartheta(1)^2.$$

Now $T = \mathrm{I}_G(\vartheta) = \mathrm{I}_G(\vartheta\lambda)$ since λ is G-invariant, and hence $\xi^G, \eta^G \in \mathrm{Irr}(G)$ by Theorem 7.2.2(a). Let χ be whichever of ξ^G, η^G has larger degree. Then we obtain $\chi(1) = c\vartheta(1)$ for some positive integer c and

$$c^2\vartheta(1)^2 = \chi(1)^2 \geq \xi^G(1)\eta^G(1) \geq \beta(1)t\,\vartheta(1)^2$$

and the result follows since $c^2 \geq \beta(1)t$ by the displayed formula. □

Theorem A.34.3 ([Isa1, Corollary 12.9]). *Let G be a p-group with $\mathrm{cd}(G) = \{1, p\}$. Then there exists in G a normal abelian subgroup Z of index $\leq p^2$.*

Proof. Let K be a maximal normal subgroup of G such that G/K is nonabelian and let $Z/K = \mathrm{Z}(G/K)$; then $Z \lhd G$. By Exercise 1, $|G : Z| = p^2$. It remains to show that Z is abelian.

Let $\beta \in \mathrm{Irr}(G/K)$ with $\beta(1) = p$ and let $\vartheta \in \mathrm{Irr}(Z)$; then $\ker(\beta) = K$ (note that $(G/K)'$ is the unique minimal normal subgroup of G/K so β is a faithful character of G/K). In the case under consideration, since $Z \leq \mathrm{Z}(\beta)$, Corollary A.34.2 yields the existence of an integer c such that $c^2 \geq \beta(1) = p$ and $c\vartheta(1) \in \mathrm{cd}(G) = \{1, p\}$. Since $c > 1$, this forces $\vartheta(1) = 1$. Thus Z is abelian and the proof is complete. □

Lemma A.34.4 ([Isa1, Lemma 12.10]). *Suppose that $A \leq G$ is an abelian subgroup and let $b = \max\{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$. Then*

$$|A|^{-1} \sum_{a \in A} |\mathrm{C}_G(a)| \geq |G| b^{-1}.$$

Proof. Since for $a \in A$ we have $|\mathrm{C}_G(a)| = \sum_{\chi \in \mathrm{Irr}(G)} |\chi(a)|^2$ by the Second Orthogonality Relation, it follows that

$$|A|^{-1} \sum_{a \in A} |\mathrm{C}_G(a)| = |A|^{-1} \sum_{a \in A} \sum_{\chi \in \mathrm{Irr}(G)} |\chi(a)|^2 = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi_A, \chi_A \rangle.$$

However, χ_A is a sum of $\chi(1)$ linear characters and hence $\langle \chi_A, \chi_A \rangle \geq \chi(1)$. Thus

$$|A|^{-1} \sum_{a \in A} |\mathrm{C}_G(a)| \geq \sum_{\chi \in \mathrm{Irr}(G)} \chi(1).$$

Furthermore,

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \leq b \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)$$

and thus $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \geq |G| b^{-1}$, and the result follows. □

Now we are ready to prove the main result of this section.

Theorem A.34.5. *Let G be a p-group. Then $\mathrm{cd}(G) = \{1, p\}$ if and only if one of the following holds:*

(a) *There exists in G an abelian subgroup A of index p.*

(b) *$G/\mathrm{Z}(G)$ is of order p^3 and exponent p.*

Proof. Since the groups G from (a) and (b) obviously satisfy $\mathrm{cd}(G) = \{1, p\}$ (here we use Theorem 7.2.3 and the relation $\chi(1)^2 \leq |G : \mathrm{Z}(G)|$ for all $\chi \in \mathrm{Irr}(G)$), it remains to prove the reverse implication. Thus we suppose that $\mathrm{cd}(G) = \{1, p\}$ and assume that (a) is false.

By Corollary A.34.3, there exists in G an abelian normal subgroup A of index p^2. In view of Lemma A.34.4, we have, since there is $b = p$,

$$|A|^{-1} \sum_{a \in A} |\mathrm{C}_G(a)| \geq \frac{1}{p} |G|.$$

Now A acts on $G - A$ via conjugation and let π be the character of this action. Then $\pi(a) = |\mathrm{C}_G(a)| - |A|$ for $a \in A$ ($\pi(a)$ is the number of points of $G - A$ fixed by a). Let k be the number of orbits of the above action. By the Cauchy–Frobenius–Burnside lemma and the previous displayed formula, we have

$$k = \langle \pi, 1_A \rangle = |A|^{-1} \sum_{a \in A} (|\mathrm{C}_G(a)| - |A|) \geq \frac{1}{p} |G| - |A|.$$

It follows that the average size α of these orbits satisfies

$$\alpha \le \frac{|G|-|A|}{\frac{1}{p}|G|-|A|} = \frac{|G|-\frac{1}{p^2}|G|}{\frac{1}{p}|G|-\frac{1}{p^2}|G|} = \frac{p^2-1}{p-1} = p+1 < p^2,$$

and so A has an orbit of size 1 or p on $G-A$. Since G has no abelian subgroup of index p, we get $\mathrm{C}_G(A) = A$ so A has no orbit of size 1. Thus there exists $x \in G-A$ in an A-orbit of size p. Set $K = \langle x, A\rangle$; then K is maximal in G. In this case, we see that $\mathrm{Z}(K) = \mathrm{C}_A(x)$ has index p in A and index p^3 in G. We shall show that $\mathrm{Z}(K) = \mathrm{Z}(G)$ to complete the proof.

Let $Z = \mathrm{Z}(K)$. Being characteristic in K, Z is normal in G. Take $\chi \in \mathrm{Irr}(G)$. Suppose that χ_K is irreducible. Then $Z \le \mathrm{Z}(\chi)$ and, since $\mathrm{Z}(\chi)/\ker(\chi) = \mathrm{Z}(G/\ker(\chi))$, we get $[G,Z] \le [G,\mathrm{Z}(\chi)] \le \ker(\chi)$. Now suppose that χ_K is reducible. Since $K \lhd G$, all irreducible constituents of χ_K are linear (Clifford; recall that $\chi(1) = p$, a prime) so $K' \le \ker(\chi)$. Thus for every $\chi \in \mathrm{Irr}_1(G)$ we have either $[G,Z] \le \ker(\chi)$ or else $K' \le \ker(\chi)$. Assume that $Z \ne \mathrm{Z}(G)$. We also have $K' > \{1\}$ since (a) is false and $[G,Z] \cap K' \le \ker(\chi)$ for every $\chi \in \mathrm{Irr}(G)$ by the above, so that $K' \cap [G,Z] = \{1\}$ since the intersection of kernels of irreducible characters of G equals $\{1\}$ (this intersection coincides with $\ker(\rho_G)$, where ρ_G is the regular character of G which is faithful). Now the subgroup $K'[G,Z] = K' \times [G,Z]$ with nontrivial direct factors and so it has an irreducible character ϑ with $K' \not\le \ker(\vartheta)$ and $[G,Z] \not\le \ker(\vartheta)$. Let $\chi \in \mathrm{Irr}(\vartheta^G)$. Then we get $K' \not\le \ker(\chi)$ and $[G,Z] \not\le \ker(\chi)$, contrary to what has already been proved. Thus $[G,Z] = \{1\}$ so $Z = \mathrm{Z}(G)$. By the above, $|G/Z| = p^3$. If G/Z possesses a cyclic subgroup B/Z of index p, then B is abelian of index p in G, contrary to the assumption that (a) be false. Thus $\exp(G/\mathrm{Z}(G)) = p$, completing the proof. □

In the same paper all finite groups G (not necessarily of prime power order) satisfying $\mathrm{cd}(G) = \{1, p\}$ are classified. For these groups the same assertion as for p-groups holds.

The main theorem of Chapter 11 in [BZ], where the p-groups G with

$$\mathrm{f}(G) = |G|^{-1}\mathrm{T}(G) = |G|^{-1} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) > \frac{1}{p}$$

are classified, is an essential generalization of Theorem A.34.5. Indeed, in the notation of that chapter, provided G ia a group from Theorem 34.5, we have

$$\begin{aligned}\mathrm{f}(G) &= |G|^{-1}\mathrm{T}(G)\\ &= |G|^{-1}\left(|G:G'| + \frac{1}{p}(|G| - |G:G'|)\right)\\ &= |G|^{-1}\frac{1}{p}\left(|G| + (p-1)|G:G'|\right) > \frac{1}{p}.\end{aligned}$$

Theorem A.34.6 ([Isa1, Theorem 12.26]). *Let G be a p-group and let $b = \mathrm{b}(G) = \max\{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$. Then there is an abelian $A \leq G$ such that $|G : A| \leq b^4$.*

Proof. Choose in G a maximal normal subgroup K such that G/K is nonabelian. By Exercise 1, we have $|G : Z| = f^2$, where $Z/K = \mathrm{Z}(G/K)$, and $Z = \mathrm{Z}(\beta)$ for some $\beta \in \mathrm{Irr}(G)$ with $\beta(1) = f$ (in fact, one can take as β every nonlinear irreducible character in G/K). Let $\vartheta \in \mathrm{Irr}(Z)$ with $\vartheta(1) = \mathrm{b}(Z)$. By Corollary A.34.2, we conclude that $c\vartheta(1) \in \mathrm{cd}(G)$ for some positive integer c with

$$c^2 \geq \beta(1)|G : \mathrm{I}_G(\vartheta)| \geq \beta(1) = f \quad \text{and} \quad c\vartheta(1) \leq \mathrm{b}(G) = b.$$

It follows that

$$\mathrm{b}(Z) = \vartheta(1) \leq \frac{\mathrm{b}(G)}{c} \leq \frac{b}{f^{1/2}} < b$$

(recall that $f > 1$). By induction, there exists an abelian subgroup $A \leq Z$ satisfying $|Z : A| \leq \mathrm{b}(Z)^4 \leq \frac{b^4}{f^2}$. Then

$$|G : A| = |G : Z||Z : A| \leq f^2 \frac{b^4}{f^2} = b^4,$$

and we are done. □

Let G be a p-group. We write

$$\bar{\delta}(G) = \{a_0 \cdot p^{c_0}, a_1 \cdot p^{c_1}, \ldots, a_t \cdot p^{c_t}\}, \quad \text{where } 0 = c_0 < c_1 < \cdots < c_t,$$

if $\mathrm{Irr}(G)$ has exactly a_i characters of degree p^{c_i}, where $i = 0, 1, \ldots, t$. Here we have $a_0 = |G : G'|$, $|G| = \sum_{i=0}^{t} p^{2c_i}$. It is known that the numbers $a_1, \ldots, a_t$ are multiples of $p - 1$ (Mann).

Exercise 3. Let G be a group of order p^4. Show the following:

(a) G is of maximal class if and only if $|G : G'| = p^2$.

(b) If G_0 is a group such that $\bar{\delta}(G_0) = \bar{\delta}(G)$, then G_0 is of maximal class and order p^4 if and only if G is.

Solution. (a) Let $|G : G'| = p^2$. We have to prove that G is of class 3. Assume that $\mathrm{cl}(G) = 2$. It follows from Exercise 1.8(a) (see also Lemma 65.1) that G contains a nonabelian subgroup B of order p^3. By Proposition 10.17, we have $G = B\mathrm{Z}(G)$; then $|G : G'| = p^3$, a contradiction.

(b) By hypothesis, $|G_0 : G_0'| = p^2$, so G is of maximal class by (a).

Exercise 4. Suppose that G is a p-group of maximal class. If $\mathrm{cd}(G) = \{1, p\}$, then G has an abelian subgroup of index p.

Hint. By Theorem A.34.5, either G has an abelian subgroup of index p or $G/\mathrm{Z}(G)$ is of order p^3 and exponent p. In the second case, $|G| \leq p^4$ so G also contains an abelian subgroup of index p.

Exercise 5. Let G be a group of maximal class and order p^5. Then one of the following holds:

(a) $\bar{\delta}(G) = \{p^2 \cdot 1, (p^3 - 1) \cdot p\}$. (In this case, G has an abelian subgroup of index p by Theorem 34.5).

(b) $\bar{\delta}(G) = \{p^2 \cdot 1, (p^2 - 1) \cdot p, (p - 1) \cdot p^2\}$.

Hint. Let $\bar{\delta}(G) = \{a_0 \cdot p^{c_0}, a_1 \cdot p^{c_1}, \ldots, a_t \cdot p^{c_t}\}$. Since $p-1 \mid a_i$ for $i > 0$ (Mann) and $a_0 = p^2$, our result follows.

Exercise 6. Let G and G_0 be two groups of order p^5 and let G be of maximal class. If $\bar{\delta}(G_0) = \bar{\delta}(G)$, then G_0 is either of maximal class or $\mathrm{cd}(G) = \{1, p\}$.

Solution. Let $\chi \in \mathrm{Irr}(G_0)$ with $\chi(1) = p^2$. Since $p^4 = \chi(1)^2 \leq |G_0 : \mathrm{Z}(G_0)|$, we get $|\mathrm{Z}(G_0)| = p$. It follows from $|G_0/G_0'| = |G/G'| = p^2$ that $G_0/\mathrm{Z}(G_0)$ is nonabelian. By Exercise 3(a), $G_0/\mathrm{Z}(G_0)$ is of maximal class. Then G_0 is also of maximal class since $|\mathrm{Z}(G_0)| = p$.

Exercise 7. Let G be a p-group with $\mathrm{cd}(G) = \{1, p\}$ and suppose that N is a nonabelian normal subgroup of G such that all proper G-invariant subgroups of N are abelian. Prove that $G' \leq N$.

Solution. Let $\phi \in \mathrm{Irr}_1(N)$. Then all irreducible constituents of ϕ^G have the same degree p. Let $\chi \in \mathrm{Irr}(\phi^G)$; then $\chi_N = \phi$. Take $\tau \in \mathrm{Irr}(G/N)$. By Gallagher (see [Isa1, Corollary 6.17]), we have $\chi\tau \in \mathrm{Irr}_1(G)$ so $(\chi\tau)(1) = p$. It follows that $\tau(1) = 1$ so that G/N is abelian.

Exercise 8. Suppose that G is a p-group of maximal class with abelian subgroup of index p and G_0 is a p-group of order $|G|$ such that $\bar{\delta}(G_0) = \bar{\delta}(G)$. Is it true that G_0 is also of maximal class?

Appendix 35

Groups of Frattini class 2

Below we closely follow §3.2 of Mann's book "Finite p-Groups" (in preparation).

Definition. A p-group G is said to be of *Frattini class* 2 if $\Phi(G)$ is an elementary abelian subgroup of $\mathrm{Z}(G)$.

Special p-groups, abelian groups of exponent p^2 and the nonabelian metacyclic group of order p^4 and exponent p^2 are of Frattini class 2. Next, the minimal nonabelian group of order p^5 and exponent p^2 is also of Frattini class 2.

If G is a p-group of Frattini class 2 such that $\mathrm{d}(G) = d$ and $|\Phi(G)| = p^e$, we say that G has type $\{d, e\}$. This group G has order p^{d+e} and satisfies the laws

$$(*) \qquad [x, y, z] = 1, \quad x^{p^2} = 1, \quad [x^p, y] = 1, \quad [x, y]^p = 1.$$

Note that the last two laws, in the presence of the first one, are equivalent to each other.

Let $F(d)$ be the free d-generator group in the variety defined by the laws $(*)$.

Theorem A.35.1. *$F = F(d)$ is a p-group of Frattini class 2 and type $(d, \frac{1}{2}d(d+1))$.*

Proof. Let $x_1, \ldots, x_d$ be free generators of F. Then F' is the normal closure of the set of all commutators $[x_i, x_j]$. The given laws imply that F' is central, so it is generated by $\frac{1}{2}d(d-1)$ elements $[x_i, x_j]$ and $\mathfrak{V}_1(F)F'/F'$ is generated by the cosets $x_i^p F'$. Therefore $\mathfrak{V}_1(F)F'$ is generated by the $d + \frac{1}{2}d(d-1) = \frac{1}{2}d(d+1)$ elements $[x_i, x_j]$ and x_i^p, which are central and of order p while $F/\mathfrak{V}_1(F)F'$ is an elementary abelian p-group. Thus F is a p-group of Frattini class 2 satisfying the laws $(*)$. It also follows that $|F| = p^k$, where $k \leq d + \frac{1}{2}d(d+1)$, and it will suffice to show that this is the exact order of F. To this end, it is sufficient to construct one group $G = G(d)$ of type $\{d, \frac{1}{2}d(d+1)\}$ because then F maps onto G and hence has at least the same order.

For $G(1)$ we take the cyclic group of order p^2. Assuming the proposition to be already proven for some d, consider the group $H = F(d) \times E$, where E is an elementary abelian p-group with basis $y_1, \ldots, y_{d+1}$; then define $G(d+1)$ as a cyclic extension of H by x_{d+1}, where

$$x_i^{x_{d+1}} = x_i y_i, \quad y_i^{x_{d+1}} = y_i \ (1 \leq i \leq d), \quad \text{and} \quad x_{d+1}^p = y_{d+1}. \qquad \square$$

Now let G be any group of Frattini class 2 and type $\{d, e\}$. Then G is isomorphic to some quotient group F/N, where $N \leq \Phi(F)$ and $|N| = p^k$ with $k = \frac{1}{2}d(d+1) - e$.

Here $\Phi(F)$ can be considered as a vector space of dimension $r = \frac{1}{2}d(d+1)$, and N as a subspace of codimension e. The number of such subgroups N is

$$\varphi_{r,e} = \frac{(p^r - 1)\dots(p^r - p^{e-1})}{(p^e - 1)\dots(p^e - p^{e-1})} < p^{re-(e-1)e},$$

and this number is also an upper bound for the number of groups of type $\{d, e\}$. Indeed,

$$(p^r - 1)\dots(p^r - p^{e-1}) < p^{re}$$

and

$$(p^e - 1)\dots(p^e - p^{e-1}) > p^{(e-1)e},$$

and this proves the displayed inequality. Therefore the number of p-groups of Frattini class 2 and type $\{d, e\}$ is less than $p^{re-(e-1)e}$, where $r = \frac{1}{2}d(d+1)$.

On the other hand, given any e-codimensional subspace N of $\Phi(F)$, we conclude that F/N is a p-group of type $\{d, e\}$. It is possible that another such subspace, say M, leads to an isomorphic quotient group $H = F/M$. Suppose this is the case. Then the canonical map of F onto G can be combined with the isomorphism between G and H to give a homomorphism of F onto F/M. In this homomorphism N is mapped to the identity, so, by comparing orders, N is the kernel. Now if the generators x_i are mapped in this homomorphism to cosets $a_i M$, then these cosets generate F/M, and since we have $M \leq \Phi(F)$, the elements a_i generate F. The above homomorphism can be lifted to an endomorphism sending x_i to a_i and which maps N onto M. This endomorphism is surjective since $F = \langle a_1, \dots, a_d \rangle$, so it is an automorphism. Thus we have proved the main part of the following

Theorem A.35.2. *Let N and M be subgroups of $\Phi(F)$. Then F/N and F/M are isomorphic if and only if there exists an automorphism of F mapping M onto N. Therefore the number of groups of type $\{d, e\}$ is equal to the number of orbits of e-codimensional subspaces under the action of* $\mathrm{Aut}(F)$.

It remains to obtain a lower estimate of the number of such orbits, and to this end we have to study the action of $\mathrm{Aut}(F)$. Now $\mathrm{Aut}(F)$ induces an action on $F/\Phi(F)$, and the freeness of F implies that each automorphism of $F/\Phi(F)$ is induced by $\mathrm{Aut}(F)$. An element in the kernel K of this action transforms each generator x_i to $x_i z_i$, where z_i is a central element of order dividing p, and therefore both x_i^p and $[x_i, x_j]$ are fixed. Thus the kernel K is trivial on $\Phi(F)$ which shows that the size of each orbit is at most

$$|\mathrm{Aut}(F)/K| = |\mathrm{Aut}(F/\Phi(F))| = |\mathrm{GL}(d, p)|,$$

so the number of orbits is at least the number of subspaces, as given above, divided by

$$|\mathrm{GL}(d, p)| = (p^d - 1)\dots(p^d - p^{d-1}) < p^{d^2}.$$

Thus the wanted number is at least $p^{re-e^2-d^2}$. We have proved the following theorem.

Theorem A.35.3. *The number of p-groups of Frattini class 2 and of type $\{d, e\}$, where $e < r = \frac{1}{2}d(d+1)$, is between $p^{re-e^2-d^2}$ and $p^{re-e(e-1)}$, where $r = \frac{1}{2}d(d+1)$.*

G. Higman and C. Sims obtained asymptotic estimates for the number of isomorphism types of groups of order p^n. If $f(p^m)$ is the number of isomorphism classes of groups of order p^m, then

$$p^{\frac{2}{27}m^2(m-6)} \leq f(p^m) \leq f^{\frac{2}{27}m^3+O\left(p^{m^{\frac{5}{2}}}\right)}.$$

We presented the improved upper bound due to M. Newman and C. Seeley.

Appendix 36

Hurwitz' theorem on the composition of quadratic forms

To facilitate the proof of Theorem A.36.2, we first prove the following

Theorem A.36.1. *If $m > 2$ and $n = 2^t s$, where s is odd, and there exist m matrices B_i of size $n \times n$ over complex numbers such that*

$$(1) \quad B_m = \mathrm{I}_n, \quad B_i' B_i = \mathrm{I}_n, \quad B_i' B_j + B_j' B_i = 0 \quad (i \neq j,\ i, j = 1, \ldots, m-1)$$

(here I_n is the identity $n \times n$ matrix and M' is the transpose to an $n \times n$ matrix M), then $m \leq 2t + 2$.

Proof (B. Eckmann). For $j = m$ we get $B_i' + B_i = 0$ ($i = 1, \ldots, m-1$), i.e., the $m-1$ matrices $B_1, \ldots, B_{m-1}$ are skew-symmetric.

Let a group $G = \langle a_1, \ldots, a_{m-1}, \epsilon \rangle$ satisfy the following relations:

$$a_i^2 = \epsilon \neq 1, \quad \epsilon^2 = 1, \quad [a_i, a_j] = \epsilon \quad \text{for all } i \neq j,\ i, j \in \{1, \ldots, m-1\}.$$

It follows from $\mathrm{C}_G(\epsilon) \geq \langle a_1, \ldots, a_{m-1} \rangle = G$ that $\epsilon \in \mathrm{Z}(G)$. Since G is nonabelian and the elements $a_1, \ldots, a_{m-1}$ pairwise commute modulo $\langle \epsilon \rangle$, we obtain $G' = \langle \epsilon \rangle$ and $G/G' \cong \mathrm{E}_{2^{m-1}}$ so that $|G| = 2^m$. Because the sizes of conjugacy G'-classes do not exceed $|G'| = 2$, we get

(a) If $g \in G - \mathrm{Z}(G)$, then the conjugacy class of g contains exactly two elements g and $g\epsilon$. Indeed, if $g^x \neq g$, then $[g, x] = \epsilon$ hence $g^x = g\epsilon$.

(b) If m is odd, then G is extraspecial with

$$\mathrm{Z}(G) = \langle \epsilon \rangle \quad \text{and} \quad \mathrm{k}(G) = 2 + \frac{|G| - |\mathrm{Z})G)|}{2} = 1 + 2^{m-1}$$

and, in this case, G has exactly one nonlinear irreducible character of degree $2^{(m-1)/2}$. It suffices, in view of Theorem 4.7(d), to show that G satisfies $\mathrm{Z}(G) = \langle \epsilon \rangle$. We have $[a_1 \ldots a_{m-1}, a_1] = \epsilon^{m-2} \neq 1$ since $m-2$ is odd. If $k < m-1$, then we obtain that $[a_1 \ldots a_k, a_{k+1}] = \epsilon^k$ and $[a_1 \ldots a_k, a_k] = \epsilon^{k-1}$. It follows that $G - \langle \epsilon \rangle$ has no central elements.

(c) If m is even, then $\mathrm{Z}(G) = \{1, \epsilon, a_1 \ldots a_{m-1}, a_1 \ldots a_{m-1}\epsilon\}$ and G is the product of an extraspecial group of order 2^{m-1} and a cyclic group $\mathrm{Z}(G)$ of order 4. In this case,

we conclude that

$$\mathrm{k}(G) = |\mathrm{Z}(G)| + \frac{|G| - |\mathrm{Z}(G)|}{2} = 2 + 2^{m-1}$$

so that $|\mathrm{Irr}_1(G)| = 2$ and $\mathrm{cd}(G) = \{1, 2^{(m-2)/2}\}$.

If matrices the B_i exist, then the map $a_i \to B_i, \epsilon \to -\mathrm{I}_n$ $(i = 1, \ldots, m-1)$ yields a faithful representation of G of degree n (so $\mathrm{Z}(G)$ is cyclic). Let χ be a character of this representation. Then we see that χ vanishes outside G' since B_i are skew-symmetric and $\chi(\epsilon) = -n = -\chi(1)$. It follows that χ has no linear constituents (otherwise, we have $\chi(\epsilon) > -n$ since $\lambda(\epsilon) = 1$ for every linear constituent λ of χ). Let $k = |\mathrm{Irr}(\chi)|$. Recall that all irreducible constituents of χ have the same degree.

If m is odd, we have $2^t s = n = \chi(1) = k2^{(m-1)/2}$ so $\frac{1}{2}(m-1) \leq t$ and hence $m \leq 2t + 1$. In case that m is even, we obtain that $2^t s = n = \chi(1) = k2^{(m-2)/2}$ so $\frac{1}{2}(m-2) \leq t$ and hence $m \leq 2t + 2$. (In both cases, we have used the oddness of s.) In any case, $m \leq 2t + 2$. □

We apply these results to prove the following remarkable Hurwitz' theorem on the composition of quadratic forms.

Theorem A.36.2 (A. Hurwitz). *Suppose that there exist polynomials $f_1, f_2, \ldots, f_n$ with complex coefficients which are bilinear in $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ and such that*

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = f_1^2 + \cdots + f_n^2. \tag{2}$$

Then $n \in \{1, 2, 4, 8\}$.

Proof. Write $f_i = \sum_{j=1}^n a_{ij}(x) y_j$, where $a_{ij}(x)$ are linear functions on the variable $x = (x_1, \ldots, x_n)$. Substituting the expressions for the f_i's in (2) and comparing the coefficients at $y_\alpha y_\beta$, we obtain the following identities:

$$\sum_{i=1}^n a_{i\alpha}(x) a_{i\beta}(x) = 0 \quad (\alpha \neq \beta),$$

$$\sum_{i=1}^n a_{i\alpha}(x)^2 = x_1^2 + \cdots + x_n^2,$$

where $\alpha, \beta = 1, \ldots, n$. If $A = (a_{ij}(x))$ is the $n \times n$ matrix, then we can rewrite the above relations in the following matrix form:

$$A'A = (x_1^2 + \cdots + x_n^2)\mathrm{I}_n.$$

Since $a_{ij}(x)$ are linear functions, we can write $A = A_1 x_1 + \cdots + A_n x_n$, where $A_1, \ldots, A_n$ are $n \times n$ matrices. It follows from $A'A = (x_1^2 + \cdots + x_n^2)\mathrm{I}_n$ that

$$A_i' A_i = \mathrm{I}_n,\ A_i' A_j + A_j' A_i = 0 \quad (i \neq j). \tag{3}$$

Set $B_i = A_n' A_i$ for all i; then

$$B_n = A_n' A_n = \mathrm{I}_n,\ B_i' B_i = A_i' A_n A_n' A_i = A_i' A_i = \mathrm{I}_n$$

and

$$\begin{aligned} B_i' B_j + B_j' B_i &= A_i' A_n A_n' A_j + A_j' A_n A_n' A_i \\ &= A_i' A_j + A_j' A_i = 0 \quad (i \neq j,\ i, j < n). \end{aligned}$$

These are exactly relations (1) for $m = n$. Therefore, if $n = 2^t s$, where s is odd, then, by Theorem A.36.1, $2^t \leq 2^t s = n \leq 2t + 2$. It follows that $t \in \{0, 1, 2, 3\}$.

- If $t = 0$, then $s \leq 2$ so $s = 1$ and $n = 1$ since s is odd
- If $t = 1$, then $2s \leq 4$ so $s = 1$ (s is odd) and $n = 2$.
- If $t = 2$, then $4s \leq 6$ so $s = 1$ and $n = 4$.
- If $t = 3$, then $8s \leq 8$ so $s = 1$ and $n = 8$. □

Theorem A.36.2 is also true over every field F that satisfies char(F) $\neq 2$. All cases $m = n = 1, 2, 4, 8$ are actually realizable as the existence of known algebraic systems shows. See [KaS].

Appendix 37

On generalized Dedekindian groups

This is a digest of [HLMM]

Definition. A group G is said to be a J-*group* if for each $x \in G$ one of the subgroups $\langle x\rangle$ and $\langle x, x^g\rangle$ is G-invariant for any $g \in G - \mathrm{N}_G(\langle x\rangle)$.

Clearly, the so-defined property is inherited by subgroups and quotient groups. Here are some examples of non-Dedekindian J-groups: Q_{16}, $\mathrm{SL}(2,3)$, a minimal nonnilpotent group with a normal Sylow subgroup of order q^2, and $\langle a, b \mid a^{p^2} = b^{p^2} = 1, a^b = b^{1+p}\rangle$.

Lemma A.37.1. *For a group G the following conditions are equivalent:*

(a) *G is a* J*-group.*

(b) *For each $H < G$ one of the subgroups H and $\langle H, H^g\rangle$ is G-invariant for all elements $g \in G - \mathrm{N}_G(H)$.*

Proof. Clearly, (b) $\Rightarrow$ (a). It remains to prove the reverse implication.

Suppose that G is a J-group and $H < G$ is not normal. We must show that $\langle H, H^g\rangle$ is normal in G for all $g \in G - \mathrm{N}_G(H)$. One may assume that $H_G = \{1\}$. If F_1, F_2 are g-invariant subgroups of H, then $\langle F_1, F_2\rangle$ is also g-invariant. Therefore H contains the unique maximal g-invariant subgroup T, and we have $T < H$ by the choice of g. If $h \in H - T$, then $\langle h\rangle^g \neq \langle h\rangle$ so $\langle h, h^g\rangle$ is normal in G. Thus $h^g \notin H$ (otherwise, $\langle h, h^g\rangle \leq H_G = \{1\}$). As G is a J-group, the subgroup $D = \langle h, h^g \mid h \in H - T\rangle$ is normal in G. Since $\langle H - T\rangle = H$ and $\langle H^g - T\rangle = H^g$ (note that $T = T^g < H^g$), it follows that $D = \langle H, H^g\rangle$ is normal in G, as was to be shown. □

Recall that if $X \leq Y$, then X^Y is the normal closure of X in Y.

Proposition A.37.2. *Let G be a* J*-group.*

(a) *Let $F < H < G$ and F be not normal in H. Then $F^H = F^G$.*

(b) *All nonnilpotent subgroups are normal in G. In particular, G is solvable.*

(c) *Let H be a nonnormal subgroup of G. Then, if F is a subgroup of H not contained in H_G, then F is normal in H (in particular, H/H_G is Dedekindian), H is nilpotent of class at most 2, H is a product of normal cyclic subgroups.*

(d) *If G is nonnilpotent, then its Carter subgroup, say C, is maximal in G and satisfies $\mathrm{cl}(C) \leq 2$. In particular, the derived length of G is at most 4.*

Proof. (a) It suffices to show that F^H is normal in G. Let T be a left transversal of cosets of $N_H(F)$ in H; then $|T| > 1$ by hypothesis. By Lemma A.37.1, $\langle F, F^t \rangle$ is normal in G for $t \in T^{\#}$. It follows that $F^H \lhd G$.

(b) Let $H < G$ be nonnilpotent. Then the subgroup H possesses a nonnormal maximal subgroup F. Since $H = F^H$ and $F^H = F^G$ by (a), it then follows that $H \lhd G$. By what has just been proved, G/H is Dedekindian so, taking H to be minimal nonnilpotent (H is solvable; see Appendix 22), we see that G is solvable, and so (b) is proven.

(c) Suppose that $F < H$ is not normal in H and $F \not\leq H_G$. Then $F^G = F^H$ by (a), so $F < F^H \leq H_G$, contrary to the choice of F. Thus all subgroups of H not contained in H_G are normal in H so that H/H_G is Dedekindian. Therefore, if Z is a cyclic subgroup of H not contained in H_G, then we get $Z \lhd H$ so $H' \leq C_H(Z)$. It follows from $H = \langle H - H_G \rangle$ that H is a product of all H-invariant cyclic subgroups not contained in H_G, and we conclude that $H' \leq Z(H)$ so $\mathrm{cl}(H) \leq 2$.

(d) Let C be a Carter subgroup of G. Assume that $C < M < G$, where M is maximal in G. Then M is nonnilpotent so normal in G by (b). This is a contradiction since every proper subgroup of G containing C coincides with its normalizer. Thus C is maximal in G. It follows from (c) that $\mathrm{cl}(C) \leq 2$. Let $U = P \cdot Q \leq G$ be minimal nonnilpotent, where P is a nonnormal Sylow subgroup of U. Since U is normal in G by (b), we have $Q \lhd G$, and $G = UN_G(P) = N_G(P)Q$ by Frattini's lemma. Because $N_G(P)$ is not normal in G (otherwise, P were normal in U), we see that $N_G(P)$ is nilpotent by (b) and self-normalizing in G, so it is a Carter subgroup of G. By the above, $N_G(P)$ is maximal in G. As the derived lengths of Q and $N_G(P)$ are at most 2, it follows that $\mathrm{dl}(G) \leq 2 + 2 = 4$. □

Theorem A.37.3. *The following assertions on a group $G > \{1\}$ with $Z(G) = \{1\}$ are equivalent:*

(a) *All nonnormal subgroups of G are nilpotent.*

(b) *$G = C \cdot P$ is a Frobenius group with an elementary abelian kernel P of order p^e and a complement C which is either cyclic or isomorphic to $Q_8 \times C_1$, where C_1 is cyclic of odd order. If $q \in \pi(C)$, then e is the order of p modulo q.*

Proof. By hypothesis, G is nonnilpotent. It is easy to check that (b) implies (a).

Now assume that (a) holds. If $H \leq G$ is minimal nonnilpotent, then G/H is Dedekindian so G is solvable since H is solvable. Let C be a Carter subgroup of G. Since every subgroup of G containing C coincides with its normalizer, C is maximal in G. Let $|G : C| = p^e$. Then we get $G = PC$, where $P \in \mathrm{Syl}_p(G)$. By Carter's theorem, $N_G(P)$ is nonnilpotent so normal in G. It follows that $P \lhd G$ and $P \cap C \in \mathrm{Syl}_p(C)$. Then $N_G(P \cap C) > C$ so $P \cap C \lhd G$. Therefore $C_G(P \cap C)$ is normal in G; then $(P \cap C)C_G(P \cap C)$ is normal in G. Since $C \leq (P \cap C)C_G(P \cap C)$, we conclude that

$$(P \cap C)C_G(P \cap C) = G.$$

It follows that if $P \cap C > \{1\}$, then

$$(P \cap C) \cap \mathrm{Z}(G) > \{1\},$$

and we infer that $P \cap C = \{1\}$ since $\mathrm{Z}(G) = \{1\}$ by hypothesis. Thus C is a p'-Hall subgroup of G. Since $G = C \cdot P$ is the semidirect product and C is maximal in G, it follows that P is a minimal normal subgroup of G so it is an elementary abelian p-group of order p^e. The subgroup C_G centralizes P. Let $M_1 = C_G \cap \mathrm{Z}(C)$; then

$$\mathrm{C}_G(M_1) \geq CP = G$$

so $M_1 \leq \mathrm{Z}(G) = \{1\}$ whence $C_G = \{1\}$. Let $U = \mathrm{C}_C(P)$ and assume that $U > \{1\}$. Then $U_1 = U \cap \mathrm{Z}(C) > \{1\}$ as $U \lhd C$ and $\mathrm{C}_G(U_1) \geq PC = G$ so $U_1 \leq \mathrm{Z}(G) = \{1\}$, a contradiction. Thus we get $U = \{1\}$. Assume that T is a nonnormal subgroup of C; then PT is nonnormal in G so PT is nilpotent, and so $T \leq \mathrm{C}_C(P) = \{1\}$, a contradiction. Thus C is Dedekindian. If $C \cap C^x > \{1\}$ for some $x \in G - C$, then

$$\mathrm{N}_G(C \cap C^x) \geq \langle C, C^x \rangle = G$$

since C is maximal in G. It follows that $C \cap C^x \leq C_G = \{1\}$, a contradiction. Thus G is a Frobenius group with kernel P and complement C.

Assume that G is not minimal nonnilpotent. Let $Q_1 \cdot P_1 = H < G$ be minimal nonnilpotent, where $P_1 = H' \in \mathrm{Syl}_p(H)$ and $Q_1 \in \mathrm{Syl}_q(H)$; then $H \lhd G$ so $P_1 \lhd G$, and we conclude that $P_1 = P$. One may assume that $Q_1 \leq C$; then we have $Q_1 \lhd C$. If $F/P < G/P$ is of prime order, then F is minimal nonabelian. Assume that this is false. Let $K < F$ be minimal nonabelian, $P_2 \in \mathrm{Syl}_p(K)$. Then K is normal in G (Proposition A.37.2(b)) so $P_2 \lhd G$, a contradiction since $P_2 < P$ and P is a minimal normal subgroup of G. Thus, if $q \in \pi(C)$ and $|P| = p^e$, then e is the order of p modulo q. □

Corollary A.37.4 ([HLMM, Theorem 5]). *If $G > \{1\}$ is a nonnilpotent* J*-group with $\mathrm{Z}(G) = \{1\}$, then $G = C \cdot P$ is a Frobenius group with cyclic complement C and kernel P of order p^e, where $e \leq 2$. If $e = 2$, then the odd number $|C|$ divides $p + 1$.*

Proof. Let us prove that $e \leq 2$. Assume that $e > 1$. Let $x \in P^{\#}$. There is $g \in C^{\#}$ such that $\langle x \rangle^g \neq \langle x \rangle$. Then $\langle x, x^g \rangle$ of order p^2 is G-invariant so coincides with P since P is minimal normal in G; whence $e = 2$.

Let $e = 2$. If $2 \in \pi(C)$, then there exists in G a minimal nonnilpotent subgroup $H = Q_1 \cdot P_1 \lhd G$ of order $2p$. Since $P_1 = P$, we get a contradiction. Thus $2 \notin \pi(C)$ so C is cyclic of odd order. In this case, all prime divisors of $|C|$ does not divide $p-1$, and since $|C| \mid (p^2 - 1)$, it follows that $|C|$ is an odd divisor of $p + 1$. □

Exercise. Let G be a nonnilpotent group. Check whether the following assertions are equivalent:

(a) All nonnilpotent subgroups of G are subnormal.

(b) $G/\mathrm{Z}_\infty(G)$ is a group from Theorem A.37.3(b).

Lemma A.37.5. *If $x \in G$, where a p-group G is a* J*-group, then $\langle x\rangle$ is normal in $\langle x\rangle^G$.*

Proof. One may assume that $\langle x\rangle$ is not normal in G. Take

$$g \in \mathrm{N}_G(\mathrm{N}_G(\langle x\rangle)) - \mathrm{N}_G(\langle x\rangle).$$

Then we have $x^g \le \mathrm{N}_G(\langle x\rangle)^g = \mathrm{N}_G(\langle x\rangle)$ by the choice of g, and so the normal closure $\langle x\rangle^G = \langle x, x^g\rangle$ normalizes $\langle x\rangle$. □

Lemma A.37.6. *Suppose that a p-group G is a* J*-group. Then the following hold:*

(a) *An element $a \in G$ of order p satisfies either $a \in \mathrm{Z}(G)$ or $\langle a\rangle^G = \langle a\rangle \times \langle a^g\rangle$ for each $g \in G - \mathrm{C}_G(a)$, and we have $|G : \mathrm{C}_G(a)| = p$.*

(b) $\Omega_1(G) \le \mathrm{Z}_2(G)$.

Proof. Statement (a) is obvious since, if $E \lhd G$ is abelian of type (p, p), then we have $|G : \mathrm{C}_G(E)| \le p$.

Statement (b) follows from (a). Indeed, assume that $a \notin \mathrm{Z}(G)$; then $|\langle a, a^g\rangle| = p^2$ for all $g \in G - \mathrm{C}_G(a)$ so $a \in \langle a, a^g\rangle \le \mathrm{Z}_2(G)$. □

Theorem A.37.7. *Suppose that a p-group G is a* J*-group. Then for all $a \in G$ we have $|G : \mathrm{N}_G(\langle a\rangle)| \le p$.*

Proof. One may assume that $C = \langle a\rangle$ is not normal in G. If $g \in G - \mathrm{N}_G(C)$, then we have $A = \langle a, a^g\rangle = C^G$. Thus $|A/\Phi(A)| = p^2$ and hence A contains exactly $p + 1$ maximal subgroups. Each maximal subgroup of A contains at most one conjugate of C (otherwise, it contains C^G) so A contains exactly p subgroups conjugate with C in G. It follows that $|G : \mathrm{N}_G(C)| = p$. □

Recall that $\mathcal{N}(G)$ (the norm of G) denotes the intersection of normalizers of all subgroups of G. It is known that $\mathcal{N}(G) \le \mathrm{Z}_2(G)$, the second member of the upper central series of G (see Corollary 140.8). By Theorem 143.1, if $\mathcal{N}(G)$ is nonabelian, then it coincides with G, i.e., the norm of a non-Dedekindian group must be abelian.

Theorem A.37.8. *Let a non-Dedekindian p-group G be a* J*-group. Then the following hold:*

(a) $\Phi(G) \le \mathcal{N}(G)$ *so* $\Phi(G)$ *is abelian.*

(b) $\mathrm{cl}(G) \le 3$.

(c) *The derived length of G is at most* 2.

Proof. (a) It follows from Theorem A.37.7, that $\Phi(G)$ normalizes all cyclic subgroups of G so $\Phi(G) \le \mathcal{N}(G)$. Now (a) follows from the remark preceding the theorem.

Since $\mathcal{N}(G) \le \mathrm{Z}_2(G)$, (b) follows from (a).

Statement (c) follows from (a). □

The paper [HLMM] contains some additional information on J-groups. The proofs of the following two theorems from [HLMM] are omitted.

Theorem A.37.9. *If a p-group G is a* J*-group, then* $\exp(G') \leq p^2$.

Theorem A.37.10. *Suppose that a nonabelian p-group G is a* J*-group. Then the following hold:*

(a) *If $p > 2$, then G' is elementary abelian and $|G'| \leq p^2$. If $p = 2$, then $|G'| \leq 2^6$.*

(b) *If $p > 3$, then* $\mathrm{cl}(G) = 2$.

(c) $\mathfrak{V}_\epsilon(G) \leq \mathrm{Z}(G)$, *where $\epsilon = 1$ if $p > 2$ and $\epsilon = 2$ if $p = 2$.*

(d) *If* $\mathrm{cl}(G) = 2$, *then* $\Phi(G) \leq \mathrm{Z}(G)$.

(e) $\mathrm{b}(G) \leq \mu$, *where $\mu = 2$ if $p > 2$ and $\mu = 3$ if $p = 2$. Here* $\mathrm{b}(G)$ *is the breadth of G (see* §133*).*

(f) *If $p > 2$ and* $\mathrm{cl}(G) = 3$, *then $p = 3$,* $\exp(G) = 9$ *and* $|G'| \leq 9$.

Appendix 38

Some results of Blackburn and Macdonald

In this section we state some important theorems of Blackburn and Macdonald about p-groups with prescribed subgroups of given order or index. Most of them were proved by heavy calculations.

1^o. All results in this subsection are due to Blackburn.

Theorem A.38.1 ([Bla1, Theorem 1]). *Let G be a p-group for which G' is generated by two elements, and suppose that the invariants of the abelian group G'/G'' are p^m, p^n, where $m \le n$. Then G' is a metacyclic group of class at most 2, and we have $|G''| = p^k$, where $2k \le m$. When $k > 0$, G' is generated by two elements a, b with generating relations*

$$a^{p^m} = b^{p^{n+k}} = 1, \quad [a,b] = b^{p^n}. \tag{1}$$

It is known (Theorem 43.12) that if N is a 2-generator normal subgroup of a p-group G and $N \le \Phi(G)$, then N is metacyclic; see also [Kin1]. Note that the assertion on the class of G' is trivial since $G/\mathrm{C}_G(G'')$ is abelian and $G' \le \mathrm{C}_G(G'')$. Other assertions of the theorem are fairly deep. The subgroup G'' is a subgroup of the Schur multiplier of the abelian group G'/G'' so $k \le m$ (Schur). Blackburn's estimate $2k \le m$ is better.

Theorem A.38.2 ([Bla1, Theorem 3]). *Let H be a group generated by two elements a, b with defining relations* (1)*, where $0 < 2k \le m \le n$. Then there exists a p-group G such that $G' \cong H$.*

Theorem A.38.3 ([Bla1, Theorem 2]). *If G is a p-group such that $\mathrm{d}(G') \le 2$, then we have $\mathrm{K}_3(G) \le \mathrm{Z}(G')$.*

Corollary A.38.4 ([Bla1, Theorem 4]). *Let G be a p-group. If G and G' are generated by two elements, then G' is abelian. In particular, 3-groups of maximal class are metabelian. (Moreover, as we know, in this case, the fundamental subgroup of our group is either abelian or minimal nonabelian.)*

Proof. Let $G = \langle x, y\rangle$. Then $G' = \langle \mathrm{K}_3(G), [x,y]\rangle$. Now the claim follows from Theorem A.38.3. □

Theorem A.38.5 ([Bla2, Theorem 2.1]). *If G is a p-group with two generators and the invariants of the abelian group G'/G'' are p^m, p^n, then $\mathrm{K}_{p^m+p^n-1}(G) \le \Phi(G')$ and $\mathrm{d}(G') \le (p^m-1)(p^n-1)$. These estimates are best possible.*

Lemma A.38.6 ([BlaEs, Lemma 1]). *Suppose that G is a p-group of class at most p and $|\mathfrak{V}_1(G)| = p$. Then $\exp(G') \le p$ and $|G : \Omega_1(G)| \le p^p$.*

Theorem A.38.7 ([BlaEs, Theorem 2]). *Let G be a p-group for $p \le 3$. If $|\mathfrak{V}_1(G)| \le p$, then $|G : \Omega_1(G)| \le p^p$.*

Proof. We prove the theorem only for $p = 2$. We will prove more: The number of involutions in G is at least $\frac{1}{4}|G| - 1$. Indeed, then we have $|\Omega_1(G)| \ge \frac{1}{4}|G|$ so that G satisfies $|G : \Omega_1(G)| \le 4$ with equality if and only if $\Omega_1(G)$ is elementary abelian. Set $|G| = 2^m$. One may assume that G is nonabelian (otherwise, $|G : \Omega_1(G)| \le 2$). Let $\mathrm{T}(G) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)$. By [BZ, Chapter 11], $\mathrm{T}(G) \le \frac{3}{4}|G| = 3 \cdot 2^{m-2}$. Therefore

$$\mathrm{T}_1(G) = \sum_{\chi \in \mathrm{Irr}_1(G)} \chi(1) = \mathrm{T}(G) - |G : G'| \le \frac{1}{4}|G| = 2^{m-2}$$

since $\sum_{\chi \in \mathrm{Lin}(G)} \chi(1) = \frac{1}{2}|G| = 2^{m-1}$. By the Frobenius–Schur formula for the number of involutions $\mathrm{t}(G)$ (see [BZ, Theorem 4.13]), we get

$$\mathrm{t}(G) + 1 = \sum_{\chi \in \mathrm{Irr}(G)} \nu_2(\chi)\chi(1) \ge |\mathrm{Lin}(G)| - \mathrm{T}_1(G) \ge 2^{m-2} - 1$$

since $\nu_2(\chi) \in \{0, -1.1\}$. Thus $|\Omega_1(G)| \ge 2^{m-2}$ so $|G : \Omega_1(G)| \le 4$, as required. □

Theorem A.38.8 ([BlaEs, Corollary 2]). *Let G be a p-group satisfying $|\mathfrak{V}_1(G)| \le p$. If $G'' \le \mathrm{Z}(G)$ and $\mathrm{K}_{p-1}(G) \le \mathrm{Z}(G')$, then $|G : \Omega_1(G)| \le p^p$. In particular, this is so if G is metabelian.*

Exercise 1. Study the power structure of groups of order $p^n > p^{p+1}$ containing an element of order p^{n-p+1}.

Hint. If G possesses a normal subgroup of order p^p and exponent p, then G is an L_p-group; see §§17, 18. Otherwise, G is absolutely regular; see §§9, 12.

Theorem A.38.9 ([Bla5, Theorem 4.3]). *Suppose that, for $p > 3$, G is a p-group such that $\mathfrak{V}_1(G) = \mathrm{K}_3(G)$ has index p^3 in G. Then the indices of the lower central series of G are $p^2, p, p^2, p, \ldots, p^2, p, f$, where $1 \le f \le p^2$.*

Exercise 2. Let G be a 2-group of order $> 2^n$, $n > 2$. Then the number of normal subgroups N of G such that G/N is a 2-group of maximal class and order 2^n is even unless G is of maximal class.

2^o. All results in this subsection are due to Macdonald [Macd5].

Theorem A.38.10. *Let G be a metabelian p-group of class precisely $2n$ with every proper subgroup of class at most n. Then $n = 1$, i.e., G is minimal nonabelian.*

Theorem A.38.11. *If every proper subgroup of a p-group G has class at most 2, then* $\mathrm{cl}(G) \leq 3$.[1]

Theorem A.38.12. *Let G be a group of order p^{r+m} in which every subgroup of order p^r has class $\leq n$, while $\mathrm{cl}(G) > n$. Then the following hold:*

(a) $\mathrm{d}(G) \leq m + n$.

(b) $\mathrm{cl}(G) \leq f(m, n)$.

(c) *The order of $\mathrm{K}_{n+1}(G)$ is a factor of $p^{g(m,n)}$.*

(d) *The order of $G/\mathrm{Z}_n(G)$ is a factor of $p^{h(m,n)}$.*

Here f, g, h are certain functions of m, n but not of r.

Theorem A.38.13. *Suppose that every subgroup of index p^2 in a p-group G has class at most 2. Then $\mathrm{cl}(G) \leq 4$ and G is metabelian if $p = 2$.*[2]

Corollary A.38.14. *If all subgroups of index p^3 in a p-group G are abelian, then the class of G is at most 4 and G is metabelian.*[3]

Theorem A.38.15. *Given a prime $p \geq 5$, there is a p-group of class precisely 6 with every proper subgroup of class at most 3.*[4]

Theorem A.38.16. *Let a prime $p > 2$ and natural numbers m and n be given. Then there is a metacyclic p-group of class precisely $m+n$ with every subgroup of index p^m having class n. In addition, the group may be chosen so that $\mathrm{Z}_n(G)/\mathrm{K}_{n+1}(G)$ has arbitrarily large order when $m = 1$.*

[1] Fitting's lemma (see Introduction, Theorem 21) gives $\mathrm{cl}(G) \leq 4$.

[2] Theorem A.38.12 and Fitting's lemma give $\mathrm{cl}(G) \leq 6$.

[3] Groups G of this theorem are $\mathcal{A}_3$-groups; see §72. By Proposition 72.2, $|G'| \leq p^4$, and this estimate is attained for $p = 5$.

[4] In this case, the estimate of Fitting's lemma is best possible.

Appendix 39

Some consequences of Frobenius' normal p-complement theorem

Let p, q be distinct primes, G be a finite group, $\pi(G)$ be the set of all prime divisors of $|G|$, π be a set of primes, and $\mathrm{F}(G)$ be the Fitting subgroup of G. In what follows, Θ is a group-theoretic property inherited by subgroups and epimorphic images and such that there exist non-Θ-groups and nonidentity Θ-groups.

On minimal nonnilpotent groups see Appendix 22. Sometimes $\mathrm{S}(p^a, q^b, q^c)$-groups are called $\mathrm{S}(p, q)$-groups. An S-group is an $\mathrm{S}(p, q)$-group for some p, q.

A group G is said to be *p-nilpotent* if it has a normal p-complement. By Frobenius' normal p-complement theorem [Isa5, Theorem 9.18], G is p-nilpotent if and only if it has no $\mathrm{S}(q, p)$-subgroups for all $q \neq p$. A group G is said to be *p-closed* if its Sylow p-subgroup is normal.

Let $\mathrm{O}^p(G)$ be the subgroup generated by all p'-elements of G, $\mathrm{O}^{p'}(G)$ be the subgroup generated by all p-elements of G and $\mathrm{O}^{p,p'}(G)$ be the subgroup generated by all p-elements of $\mathrm{O}^p(G)$. Then $G/O^p(G)$, $G/\mathrm{O}^{p'}(G)$ is a p-, p'-group, respectively. If N denotes a proper G-invariant subgroup of $\mathrm{O}^p(G)$ (of $\mathrm{O}^{p'}(G)$), then G/N is not a p-group (p'-group). Next, $G/\mathrm{O}^{p,p'}(G)$ is p-nilpotent but, for every G-invariant subgroup N properly contained in $\mathrm{O}^{p,p'}(G)$, G/N is not p-nilpotent.

Denote by $\mathrm{K}_\infty(G)$ the last member of the lower central series of G. Then we have $\mathrm{K}_\infty(G) = \bigcap_{p\in\pi(G)} \mathrm{O}^p(G)$. It is clear that $\mathrm{O}^{p,p'}(G) \leq \mathrm{K}_\infty(G)$.

By $\mathrm{Hall}_\pi(G)$ we denote the set of all π-Hall subgroups of G. We have the equality $\mathrm{Hall}_p(G) = \mathrm{Syl}_p(G)$.

Let $\mathrm{Z}_\infty(G)$ be the last member of the upper central series of a group G. The subgroup $\mathrm{Z}_\infty(G)$ is said to be the *hypercenter* of the group G and sometimes it also denoted by $\mathrm{H}(G)$. Clearly, $\mathrm{Z}(G/\mathrm{Z}_\infty(G)) = \{1\}$. If $H < G$ is such that $\mathrm{N}_G(H) = H$, then we have $\mathrm{Z}_\infty(G) < H$. This equality is proved by induction as $\mathrm{Z}_\infty(G) = \mathrm{Z}_n(G)$ for some n.

Suppose that $\Phi(G) \leq N$ and N is normal in G. If $N/\Phi(G)$ has a normal π-Hall subgroup $K_1/\Phi(G)$, then N has a normal π-Hall subgroup as well. Indeed, there is $K \in \mathrm{Hall}_\pi(K_1)$ and all members of the set $\mathrm{Hall}_\pi(K_1)$ are conjugate in K_1 (Schur–Zassenhaus), $K_1 = K\Phi(G)$ and

$$G = K_1\mathrm{N}_G(K) = K\Phi(G)\mathrm{N}_G(K) = \mathrm{N}_G(K)$$

(Frattini's argument), and our claim follows since $K \in \mathrm{Hall}_\pi(N)$. It follows from what has just been proved and the Schur–Zassenhaus theorem that $\pi(G/\Phi(G)) = \pi(G)$.

Definition 1. A group G is said to be a $\mathrm{B}(p,q)$-*group* if $G/\Phi(G)$ is an $\mathrm{S}(p,q)$-group for some primes p, q (in fact, our $G/\Phi(G)$ has the trivial center so it is minimal non-abelian).

A B-group is a $\mathrm{B}(p,q)$-subgroup for some p and q. For such a group G we have $G = PQ$, where $P \in \mathrm{Syl}_p(G)$ is cyclic, $Q = G' \in \mathrm{Syl}_q(G)$, $|P : (P \cap \mathrm{Z}(G))| = p$. Obviously, an $\mathrm{S}(p,q)$-group is a $\mathrm{B}(p,q)$-group. If, in addition, $p = 2$, then Q is cyclic of order q.

Definition 2. A group G is said to be a Θ_1-*group* (= minimal non-Θ-group) if it is not a Θ-group but all its proper subgroups are Θ-groups.

It is clear that a group G is a Θ-group if and only if it has no Θ_1-subgroups. Obviously, S-groups are Θ_1-groups, where Θ is nilpotence.

If a $\mathrm{B}(p,q)$-group $G = PQ$, then $Q/\Phi(Q)$ is a unique minimal normal q-subgroup of $G/\Phi(Q)$. It is clear that a nonnilpotent epimorphic image of a $\mathrm{B}(p,q)$-group is also a $\mathrm{B}(p,q)$-group and it has only one normal subgroup of prime index, namely p. Let $Q > \{1\}$ be a q-group. There exists a $\mathrm{B}(p,q)$-group with Sylow subgroup Q if and only if Q possesses an automorphism of order $p \neq q$ that acts irreducibly on $Q/\Phi(Q)$. For any distinct p, q there exists an $\mathrm{S}(p,q)$- so a $\mathrm{B}(p,q)$-group. For $q > 2$ the dihedral group of order $2q^n$ is a $\mathrm{B}(2,q)$-group. Since every S-subgroup of a $\mathrm{B}(p,q)$-group contains its Sylow p-subgroup, $\mathrm{B}(p,q)$-groups are generated by S-subgroups.

In this and the following paragraph we define some characteristic subgroups of a group G. Let $\mathcal{B}_q(G)$ (q is fixed) be the subgroup generated by normal Sylow q-subgroups (= derived subgroups) of all $\mathrm{B}(p,q)$-subgroups of G ($p \in \pi(G) - \{q\}$). By the Frobenius normal p-complement theorem, $\mathcal{B}_q(G) = \{1\}$ if and only if G is q-nilpotent. Set

$$\mathcal{B}(G) = \prod_{q \in \pi(G)} \mathcal{B}_q(G).$$

Theorem 39.2(b) shows that $\mathcal{B}(G)$ is the last member of the lower central series of G.

Let $\Theta_1(G)$ be the (characteristic) subgroup generated by all Θ_1-subgroups of G; $\Theta_1(G) = \{1\}$ if and only if G is a Θ-group. We shall show (see Lemma A.39.1) that $G/\Theta_1(G)$ is a Θ-group for appropriate Θ's.

Let $G = A\Theta_1(G)$, where $A \leq G$ is as small as possible. Then we conclude that

$$\Theta_1(A) \leq A \cap \Theta_1(G) \leq \Phi(A)$$

is nilpotent. Hence, if $G/\Theta_1(G)$ is not a Θ-group, there exists in G a non-Θ-subgroup A such that $\Theta_1(A) \leq \Phi(A)$; in particular, all Θ_1-subgroups of A are nilpotent. Let, in addition, Θ be nilpotence. It follows from the remark above that then A is nilpotent so $G/\Theta_1(G)$ is nilpotent. We generalize this observation in the following lemma.

Lemma A.39.1. *Suppose that G is not a Θ-group and all Θ_1-subgroups of G are nonnilpotent. Then G has a Θ-subgroup A such that $G = A\Theta_1(G)$. In particular, the quotient group $G/\Theta_1(G) \cong A/(A \cap \Theta_1(G))$ is a Θ-group.*

Proof. Suppose that the lemma has been proved for all proper subgroups of G. By hypothesis, $\Theta_1(G) > \{1\}$. Let A be a subgroup of G minimal such that $G = A\Theta_1(G)$. Since $\Theta_1(G)$ is nonnilpotent, it is not contained in $\Phi(G)$ so $A < G$. By induction, we see that $A/\Theta_1(A)$ is a Θ-group. In view of $\Theta_1(A) \leq A \cap \Theta_1(G) \leq \Phi(A)$, we obtain that $\Theta_1(A) = \{1\}$ since all Θ_1-subgroups of G are nonnilpotent. It follows that A is a Θ-group so $G/\Theta_1(G) \cong A/(A \cap \Theta_1(G))$ is also a Θ-group, as was to be shown. □

In particular, Lemma A.39.1 is true for properties Θ such that all nilpotent groups are Θ-groups, but the assumption in the lemma is weaker. In fact, consider the case when Θ is commutativity and G is a nonabelian group all of whose Sylow subgroups are abelian. Then all Θ_1-subgroups of G are nonnilpotent; moreover, all minimal nonnilpotent subgroups of G are minimal nonabelian. By Lemma A.39.1, in our case, we see that $G/\Omega_1(G)$ is abelian.

It is easy to show that Lemma A.39.1 is not true for Θ's such that some Θ_1-groups are nilpotent. In fact, if Θ is such that only the identity group is a Θ-group, then $\Theta_1(G)$ is the subgroup of G generated by the elements of prime orders; in this case, the structure of $G/\Theta_1(G)$ may be very complicated [Ito10].

For some properties Θ one can say more than in Lemma A.39.1. Indeed, let in the lemma Θ be solvability and let G be nonsolvable. Then $G/\Theta_1(G)$ is solvable by the lemma. In particular, if $X = X' > \{1\}$, then we get $X = \Theta_1(X)$. We claim that, in fact, $\Theta_1(G)$ is equal to $G^\infty = K$, the last member of the derived series of G. Since G/K is solvable and $K' = K$, we get $K \leq \Theta_1(G)$. Assume that $K < \Theta_1(G)$. Then G has a Θ_1-subgroup L such that $L \not\leq K$. Since all proper subgroups of L are solvable but L is not solvable, it follows that $L' = L$, and so $LK/K \cong L/(L \cap K)$ is nonsolvable, contrary to the solvability of G/K. Therefore $K = \Theta_1(G)$, as claimed.

Let $\mathcal{N}_1(G)$ be the subgroup generated by all S-subgroups of a nonnilpotent group G. By Lemma A.39.1, the last member of the lower central series of G, the subgroup $\mathrm{K}_\infty(G)$, is contained in $\mathcal{N}_1(G)$. It follows that if all minimal nonnilpotent subgroups are normal in G, then $G/\mathrm{F}(G)$ is an extension of direct product of elementary abelian groups by a nilpotent group. Indeed, if K is generated by normal maximal subgroups of all minimal nonnilpotent subgroups of G (a maximal normal subgroup of an S-group L is characteristic in L), then $K \leq \mathrm{F}(G)$ and so the quotient group $\mathcal{N}_1(G)/K$ is generated by normal subgroups of prime orders.

Given a set π of primes, a group G is said to be *π-decomposable* if its π-Hall subgroup is a direct factor of G. Let K be the subgroup generated by all minimal nonnilpotent subgroups of G of orders divisible by a fixed prime p. We claim that then the quotient group G/K is p-decomposable. Indeed, let Θ be p-decomposability. By the Frobenius normal p-complement theorem (see [Isa5, Theorem 9.18]) and basic properties of p-solvable groups, Θ_1-groups are minimal nonnilpotent of orders divisible

by p. Therefore $K = \Theta_1(G)$. By Lemma A.39.1, G/K is a Θ-group, i.e., it is p-decomposable, as claimed. Similarly, if K is generated by all minimal non-π-decomposable subgroups of G, then by Lemma A.39.1, G/K is π-decomposable.

It follows from the Frobenius normal p-complement theorem [Isa5, Theorem 9.18] that a non-q-nilpotent group possesses an $\mathrm{S}(p,q)$-subgroup for some $p \neq q$. Indeed, G has a q-subgroup Q such that $\mathrm{N}_G(Q)/\mathrm{C}_G(Q)$ is not a q-subgroup by the mentioned result. Then $\mathrm{N}_G(Q)$ contains an element of prime power order, say a p-element a for some $p \neq q$, that does not centralize Q. Set $H = \langle a, Q\rangle$. In that case, H possesses a minimal nonnilpotent subgroup that is an $\mathrm{S}(p,q)$-subgroup, as claimed. In particular, a group G is nilpotent if and only if every two conjugate elements of G of prime power order generate a nilpotent subgroup. Next, if all elements from G' of order q if $q > 2$ and 2 and 4 if $q = 2$ are contained in $\mathrm{Z}(G)$, then G is q-nilpotent. Indeed, then G has no $\mathrm{S}(p,q)$-subgroup for all $p \in \pi(G) - \{q\}$ (otherwise, the q-Sylow subgroup of that subgroup, say H, would be contained in $\mathrm{Z}(G)$ so H is nilpotent), and our claim follows from what has already been proved. The same conclusion is true if $Q \in \mathrm{Syl}_q(G)$ is abelian and $\Omega_1(Q) \leq \mathrm{Z}(G)$.

Our principal result is the following

Theorem A.39.2. (a) $\mathcal{B}_q(G) = \mathrm{O}^{q,q'}(G)$, *i.e., the subgroup* $\mathrm{O}^{q,q'}(G)$ *is generated by the derived subgroups of all* $\mathrm{B}(p,q)$*-subgroups of a group* G.

(b) $\mathcal{B}(G) = \mathrm{K}_\infty(G)$, *i.e., the subgroup, generated by derived subgroups of all* B*-subgroups of* G, *coincides with the last member of the lower central series of* G.

Proof. (a) Assume that $\mathcal{B}_q(G) \not\leq \mathrm{O}^{q,q'}(G)$. Then we infer that G has a $\mathrm{B}(p,q)$-subgroup $F = P \cdot Q$, where $p \in \pi(G) - \{q\}$, $P \in \mathrm{Syl}_p(F)$ and $F' = Q \in \mathrm{Syl}_q(F)$ such that $Q \not\leq \mathrm{O}^{q,q'}(G)$. Set $\bar{G} = G/\mathrm{O}^{q,q'}(G)$. In this case, we see that

$$\bar{F} = F/(F \cap \mathrm{O}^{q,q'}(G))(\cong F\mathrm{O}^{q,q'}(G)/\mathrm{O}^{q,q'}(G))$$

is of order divisible by q; therefore $\bar{F}$ is not q-nilpotent (otherwise, F has a normal subgroup of index q which is not the case since $|F : F'|$ is a power of $p \neq q$). Since every epimorphic image of F is either nilpotent or a $\mathrm{B}(p,q)$-group, it follows that $\bar{F}$ is a $\mathrm{B}(p,q)$-group. Thus a non-q-nilpotent group $\bar{F}$ is isomorphic to a subgroup of the q-nilpotent group $G/\mathrm{O}^{q,q'}(G)$, which is a contradiction. Hence $\mathcal{B}_q(G) \leq \mathrm{O}^{q,q'}(G)$. Recall that $\mathrm{O}^{q,q'}(G)$ is contained in every normal subgroup N of G such that G/N is q-nilpotent. Therefore, to prove the reverse inclusion, it suffices to show that $G/\mathcal{B}_q(G)$ is q-nilpotent.

Assume that the quotient group $G/\mathcal{B}_q(G)$ is not q-nilpotent. In that case, it has an $\mathrm{S}(p,q)$-subgroup $\bar{S} = S/\mathcal{B}_q(G)$ by the Frobenius normal q-complement theorem (see [Isa5, Theorem 9.18] and Theorem A.22.1). Let A be a smallest subgroup of S such that $S = A\mathcal{B}_q(G)$. Then we get $A \cap \mathcal{B}_q(G) \leq \Phi(A)$ and $A/(A \cap \mathcal{B}_q(G))$ is an $\mathrm{S}(p,q)$-group since it is isomorphic to $\bar{S}$. Therefore $A/\Phi(A)$ is an $\mathrm{S}(p,q)$-group as a nonnilpotent epimorphic image of the $\mathrm{S}(p,q)$-group $\bar{S}$. It follows that, by Definition 1, A is a $\mathrm{B}(p,q)$-subgroup of G. Since q divides $|\bar{S}| = |A\mathcal{B}_q(G)/\mathcal{B}_q(G)|$, the Sylow

q-subgroup of A is not contained in $\mathcal{B}_q(G)$, contrary to the definition of the last subgroup. Thus $\bar{S}$ does not exist whence $G/\mathcal{B}_q(G)$ is q-nilpotent so $\mathrm{O}^{q,q'}(G) \leq \mathcal{B}_q(G)$, and (a) follows since the reverse inclusion has proved.

(b) Let us prove that $K = \prod_{q\in\pi(G)} \mathrm{O}^{q,q'}(G)$ is equal to $\mathrm{K}_\infty(G)$, the last member of the lower central series of G. As G/K is q-nilpotent for all $q \in \pi(G)$ by (a), it is nilpotent, and so $\mathrm{K}_\infty(G) \leq K$. The reverse inclusion is evident since $\mathrm{O}^{q,q'}(G) \leq \mathrm{K}_\infty(G)$ for all $q \in \pi(G)$ since $G/\mathrm{K}_\infty(G)$ is nilpotent. Therefore $K = \mathrm{K}_\infty(G)$. By (a),

$$\mathcal{B}(G) = \prod_{p\in\pi(G)} \mathcal{B}_p(G) = \prod_{p\in\pi(G)} \mathrm{O}^{p,p'}(G) = K = \mathrm{K}_\infty(G),$$

completing the proof of (b). □

For a further development of the theme of Theorem 39.2, see [AB-B].

If K is the subgroup generated by normal Sylow subgroups of all minimal nonnilpotent subgroups of G, then G/K is not necessarily nilpotent (let G be the dihedral group of order $2p^n$, $p > 2$, $n > 1$; then G/K is dihedral of order $2p^{n-1}$). Moreover, we cannot prove that, in the case under consideration, G/K is solvable.

If G is a $\mathrm{B}(p,q)$-group and a minimal nonnilpotent $S \leq G$ is subnormal, then S coincides with G. Indeed, if $S < G$, then the index of S in G is a power of q so G has a normal subgroup of index q which is impossible since $|G : G'|$ is a power of p.

Lemma A.39.3. *Let q be a prime divisor of $|G'|$. Suppose that for every non-G-invariant q-subgroup A of G one has $A \leq \mathrm{Z}_\infty(\mathrm{N}_G(A))$. Then G is an extension of a q-group $\mathcal{B}_q(G)$ by a q-nilpotent group, i.e., $G = \mathrm{O}^{q,q',q}(G)$.*

Proof. Suppose that G is not q-nilpotent. Then G contains a $\mathrm{B}(p,q)$-subgroup D for some prime $p \neq q$ by [Isa5, Theorem 9.18] and Theorem A.22.1. Since $D' \not\leq \mathrm{Z}_\infty(D)$ and $D \leq \mathrm{N}_G(D')$, we conclude that $D' \not\leq \mathrm{Z}_\infty(\mathrm{N}_G(D'))$. In this case, by hypothesis, $D' \lhd G$. By what has just been proved, $\mathcal{B}_q(G)$ is a normal q-subgroup of G contained in G'. In view of Theorem 39.2(a), $G/\mathcal{B}_q(G)$ is q-nilpotent. □

Let G be a group. If for every abelian subgroup A of G one has $\mathrm{N}_G(A) = \mathrm{C}_G(A)$, then G is abelian. Indeed, assume that this is false. Then there is in G a minimal nonabelian subgroup B. Let A be a normal maximal subgroup of B; then we obtain that $A \not\leq \mathrm{Z}(B)$ so that $B \not\leq \mathrm{C}_G(A)$ and since $B \leq \mathrm{N}_G(A)$, we get a contradiction. Thus B does not exist, and we conclude that G is abelian. Zassenhaus has used this result in his proof of Wedderburn's theorem on commutativity of finite skew fields. It is a starting point for Proposition A.39.4 and the Supplement to Theorem A.39.5.

Proposition A.39.4. *Let $q \in \pi(G')$ be fixed. Suppose that a group G satisfies the following condition:*

(∗) *Whenever $H \leq G'$ is either an elementary abelian q-subgroup or a cyclic subgroup of order 4 if $q = 2$, then $H \leq \mathrm{Z}(\mathrm{N}_G(H))$.*

Then G is q-nilpotent. There exists a nonabelian 2-group satisfying the above condition for $q = 2$.

Proof. Suppose that G is a counterexample of minimal order. Then, by induction, all proper subgroups of G are q-nilpotent (notice that if $H < G$ is such that $q \notin \pi(H')$, then H is q-nilpotent). Therefore, by [Isa5, Theorem 9.18] and Theorem A.22.1, we see that $G = P \cdot Q$ is an $\mathrm{S}(p,q)$-group for some prime $p \neq q$,

$$P = \langle y \rangle \in \mathrm{Syl}_p(G), \quad y^p \in \mathrm{Z}(G), \quad Q = G' \in \mathrm{Syl}_q(G).$$

Since $G' = Q \not\leq \mathrm{Z}(G)$, it follows that G' is nonabelian (if G' is abelian, it is of exponent p by Theorem A.22.1 and so must lie in $\mathrm{Z}(G)$ by hypothesis, but this is impossible). If $\mathrm{Z}(G') < A \leq G'$ and $|A : \mathrm{Z}(G')| = q$, then $A \not\leq \mathrm{Z}(G')$ hence $A \not\leq \mathrm{Z}(\mathrm{N}_{G'}(A))$ since $A \lhd G'$. It follows that $A \not\leq \mathrm{Z}(\mathrm{N}_G(A))$ hence the abelian subgroup A is not elementary abelian by hypothesis, and we conclude that $\Omega_1(G') = \mathrm{Z}(G')$ is elementary abelian. If $q > 2$, then we get $\exp(G') = q$ (Theorem A.22.1), therefore $q = 2$. Then for every $u \in G' - \mathrm{Z}(G')$ we have

$$o(u) = 4, \quad y^{-1}uy = v \neq u \quad \text{and} \quad v^2 = y^{-1}u^2y = u^2$$

since $u^2 \in \mathrm{Z}(G') \leq \mathrm{Z}(G)$. Next, $u^{-1}v \notin \mathrm{Z}(G')$ since $G'/\mathrm{Z}(G')$ is a minimal normal subgroup of $G/\mathrm{Z}(G')$. It follows that $uv = u^2(u^{-1}v) \notin \mathrm{Z}(G')$ so that $o(uv) = 4$. We have

$$(uv)^2 = [u,v]u^2v^2 = [u,v]u^4 = [u,v].$$

Since $o(uv) = 4$, we get

$$\begin{aligned}(uv)^{-1} &= (uv)(uv)^2 = uv[u,v] = u[u,v]v = uu^{-1}v^{-1}uvv \\ &= v^{-1}uv^2 = v^{-1}v^2u = vu.\end{aligned}$$

It follows that $u^{-1}(uv)u = vu = (uv)^{-1} \neq uv$ so that u normalizes but not centralizes the cyclic subgroup $\langle uv \rangle$ of order 4, and this is a contradiction. Thus G must be 2-nilpotent.

We repeat some definitions and notation from §46. Let $\mathrm{F} = \mathrm{GF}(2^s)$, where $s > 1$ is odd, and let $\theta : \alpha \mapsto \alpha^2$ be the Frobenius automorphism of F; then we have $o(\theta) = s$ (indeed, if $a \in \mathrm{F}$, then $a^{\theta^s} = a^{2^s} = a$). Let G be the set of all pairs (x,y) $(x,y \in \mathrm{F})$ with multiplication defined as follows:

$$(x,y)(x_1,y_1) = (x + x_1, y + y_1 + x\theta(x_1)).$$

It is easy to check that G is a nonabelian group of order 2^{2s} with identity element $(0,0)$ and

$$(x,y)^{-1} = (x, y + x\theta(x)).$$

Next, G is special and $\mathrm{Z}(G) = \langle (0,y) \mid y \in \mathrm{F} \rangle = \Omega_1(G)$ is elementary abelian of order 2^s. Let $A = \langle (x,y) \rangle$ be a cyclic subgroup of order 4 in G; then $x \neq 0$. Assume that $(x_1,y_1) \in \mathrm{N}_G(A) - \mathrm{C}_G(A)$. Then

$$(x_1,y_1)^{-1}(x,y)(x_1,y_1) = (x,y)^{-1} = (x, y + x\theta(x)).$$

It follows that

$$(x + x_1, y + y_1 + x\theta(x_1)) = (x + x_1, y + y_1 + x\theta(x) + x_1\theta(x)),$$

and we get

$$\theta\left(\frac{x_1}{x}\right) = 1 + \frac{x_1}{x}.$$

Since s is odd, we have

$$\langle\theta^2\rangle = \langle\theta\rangle = \mathrm{Aut}(\mathrm{F}/\mathrm{F}_0),$$

where F_0 is a prime subfield of F, and we get

$$\theta^2\left(\frac{x_1}{x}\right) = \theta\left(1 + \frac{x_1}{x}\right) = 1 + 1 + \frac{x_1}{x} = \frac{x_1}{x}.$$

It follows that $\frac{x_1}{x} \in \mathrm{F}_0$, i.e., $\frac{x_1}{x} = 1$ and $x_1 = x$. Then

$$\theta(1) = \theta\left(\frac{x}{x}\right) = 1 + \frac{x}{x} = 1 + 1 = 0,$$

which is a contradiction since $x = x_1 \neq 0$. Thus we get $\mathrm{N}_G(A) = \mathrm{C}_G(A)$, as claimed. (Note, that G is a Suzuki 2-group; see §46.) □

Now we are ready to prove the following

Theorem A.39.5. *Let G be a nonnilpotent group all of whose nonnormal nilpotent subgroups have nilpotent normalizers. Then $\bar{G} = G/\mathrm{Z}_\infty(G)$ is a Frobenius group with kernel $\mathrm{F}(\bar{G})$.*

Proof. If H is a B-subgroup of G, then we have $\mathrm{N}_G(H') > H$ so $\mathrm{N}_G(H')$ is nonnilpotent. It follows that $H' \lhd G$, and we conclude that $\mathcal{B}(G)$ is nilpotent. By Lemma A.39.3, $G/\mathcal{B}(G)$ is nilpotent. Therefore G is solvable so G possesses a Carter subgroup K. As $\mathrm{N}_G(K) = K$, we have $\mathrm{Z}_\infty(G) < K$. Since $G/\mathcal{B}(G)$ is nilpotent, we get $G = K\mathcal{B}(G) = K\mathrm{F}(G)$ since $\mathcal{B}(G)$, being normal nilpotent, is contained in $\mathrm{F}(G)$.

Suppose that a prime p divides $|K|$ and $|G : K|$; then we see that p divides $|\mathrm{F}(G)|$ since $G = K\mathrm{F}(G)$. Let $P_1 \in \mathrm{Syl}_p(K)$ and $P_1 < P \in \mathrm{Syl}_p(G)$. Then $\mathrm{N}_P(P_1) > P_1$ so $\mathrm{N}_G(P_1) > K$ since K is nilpotent. It follows that $\mathrm{N}_G(P_1)$ is nonnilpotent so, by hypothesis, we have $\mathrm{N}_G(P_1) = G$, i.e., $P_1 \lhd G$. We claim that $P_1 \leq \mathrm{Z}_\infty(G)$. Indeed, since K is nilpotent, we get $K \leq P_1\mathrm{C}_G(P_1)$. Next, $P_1\mathrm{C}_G(P_1)$ is normal in G since P_1 and $\mathrm{C}_G(P_1)$ are, whence $P_1\mathrm{C}_G(P_1) = G$. The last equality means that P_1 is contained in $\mathrm{Z}_\infty(G)$, as claimed. Since $\mathrm{Z}_\infty(G) \leq K \cap \mathrm{F}(G)$, we see that

$$\mathrm{GCD}(|K/\mathrm{Z}_\infty(G)|, |\mathrm{F}(G)/\mathrm{Z}_\infty(G)|) = 1.$$

Write $\bar{G} = G/\mathrm{Z}_\infty(G)$; then $\bar{G}$ is nonnilpotent. If $\bar{L} = L/\mathrm{Z}_\infty(G)$ is a nonnormal nilpotent subgroup of $\bar{G}$, then $\mathrm{N}_{\bar{G}}(\bar{L})$ is nilpotent. Indeed, since L is nilpotent and nonnormal in G, it follows that $\mathrm{N}_G(L)$ is nilpotent by hypothesis. Then we conclude

that $\mathrm{N}_G(L)/\mathrm{Z}_\infty(G) = \mathrm{N}_{\bar{G}}(\bar{L})$ is also nilpotent, as claimed. Therefore, to complete the proof, one can assume that $\mathrm{Z}_\infty(G) = \{1\}$.

We have to show that $G = K\mathrm{F}(G)$ is a Frobenius group with kernel $F = \mathrm{F}(G)$ and complement K. By the above, we infer that $G = K \cdot F$ is the semidirect product and K, F are Hall subgroups of G. So to prove that G is a Frobenius group, it suffices to show that $K \cap K^x = \{1\}$ for every $x \in G - K$.

Since K is nilpotent, we get $K_G = \bigcap_{x\in G} K^x = F \cap K = \{1\}$.

Assume that $M = K^x \cap K > \{1\}$ for some $x \in G - K$. Let p be a prime divisor of $|M|$. We can choose x so that $|M|_p$, the p-part of $|M|$, is as large as possible. We claim that $P \in \mathrm{Syl}_p(K)$ is not contained in M. Assume that this is false and $P \leq M$. Then $\langle K, K^x\rangle$ is not nilpotent and contained in $\mathrm{N}_G(P)$. In this case, by hypothesis, $P \lhd G$ so $P \leq K_G = \{1\}$, a contradiction. Therefore $P \neq P^x$ and $P_1 = P \cap P^x$ is a Sylow p-subgroup of M. We have $\mathrm{N}_P(P_1) > P_1$, $\mathrm{N}_{P^x}(P_1) > P_1$. It follows that $R = \langle \mathrm{N}_P(P_1), \mathrm{N}_{P^x}(P_1)\rangle$ is nonnilpotent. Then, by assumption, we obtain $P_1 \lhd G$ so $P_1 \leq K_G = \{1\}$, which is a contradiction. Thus we get $K \cap K^x = M = \{1\}$ for all $x \in G - K$ so that G is a Frobenius group with complement K and kernel F. □

Supplement to Theorem A.39.5. *Suppose that every nonnormal prime power abelian subgroup of G is contained in the center of its normalizer. Then the following hold:*

(a) *For every $p \in \pi(G)$, G is either p-nilpotent or p-closed. All nonabelian Sylow subgroups of G are normal.*

(b) *$G/\mathrm{F}(G)$ is abelian.*

Proof. Let $p \in \pi(G)$ be such that $P \in \mathrm{Syl}_p(G)$ is nonabelian. We claim that P is normal in G. In view of Theorem 10.28, P is generated by its minimal nonabelian subgroups. Therefore it suffices to show that all minimal nonabelian subgroups M of P are normal in the group G. Indeed, if A is a maximal subgroup of M, then A is abelian and $M \leq \mathrm{N}_P(A)$ so $A \trianglelefteq \mathrm{Z}(\mathrm{N}_P(A))$ hence $A \trianglelefteq \mathrm{Z}(\mathrm{N}_G(A))$; this shows that $A \lhd G$. Then $M \lhd G$ since M is generated by its maximal subgroups.

Thus all nonabelian Sylow subgroups of G are normal. Let Q be a Sylow, say q-subgroup, of G that is not contained in $\mathrm{F}(G)$. Then Q is abelian and non-G-invariant so $Q \leq \mathrm{Z}(\mathrm{N}_G(Q))$. By Burnside's normal q-complement theorem [Isa5, Theorem 9.13], G is q-nilpotent, completing the proof of (a). Now (b) follows from (a). □

Let $q \in \pi(G')$ be fixed and let $e = 1$ if $q > 2$ and $e = 2$ if $q = 2$. Suppose that for every q-subgroup A of exponent $\leq q^e$ and class ≤ 2 in G' one has $A \leq \mathrm{Z}_\infty(\mathrm{N}_G(A))$. Then G is q-nilpotent. Indeed, assume that this is false. In that case, G must contain an $\mathrm{S}(p,q)$-subgroup $S = P \cdot Q$, where $Q = S' \in \mathrm{Syl}_q(S)$. Then we get $\mathrm{cl}(Q) \leq 2$ and $\exp(Q) \leq q^e$. Since $S \leq \mathrm{N}_G(Q)$ and $Q \notin \mathrm{Z}_\infty(S)$, we obtain $Q \trianglelefteq \mathrm{Z}_\infty(\mathrm{N}_G(Q))$, a contradiction.

Definition 3 (R. Baer). Let φ be a linear ordering of the set of primes, and let G be a group and $\pi(G) = \{p_1, p_2, \ldots, p_n\}$ be the set of prime divisors of $|G|$. Suppose that

$p_1 \varphi \cdots \varphi p_n$. If $\varphi = <$ is a natural ordering, then $p_1 < \cdots < p_n$ so p_1 is the least prime divisor of $|G|$. A group G is said to be *φ-dispersive* if it has a normal π_i-complement for all $i < n$, where $\pi_i = \{p_1, \ldots, p_i\}$.

It is known that supersolvable groups are $<$-dispersive. Obviously, subgroups and epimorphic images of φ-dispersive groups are φ-dispersive. It follows from Frobenius' normal complement theorem that a minimal non-φ-dispersive group is an S-group.

Proposition A.39.6. *Suppose that the normalizer in a group G of every non-G-invariant prime power subgroup of G' is φ-dispersive. Then $G/\mathrm{F}(G)$ is φ-dispersive.*

Proof. Let H be generated by (G-invariant) derived subgroups of all non-φ-dispersive B-subgroups of G; then $H \leq G'$ and H is nilpotent, hence $H \leq \mathrm{F}(G)$. As in the proof of Theorem A.39.2(a), all B-subgroups of G/H are φ-dispersive so G/H is φ-dispersive by [Isa5, Theorem 9.18] and Theorem A.22.1. Since $G/\mathrm{F}(G)$ is an epimorphic image of G/H, we are done. □

Let Θ, as always in this section, be a group-theoretic property inherited by subgroups and epimorphic images. Suppose that the normalizer of every nonnormal prime power subgroup of G is a Θ-subgroup. If $G/\mathrm{F}(G)$ has a nonidentity normal abelian p-subgroup $K/\mathrm{F}(G)$, then $G/\mathrm{F}(G)$ is a Θ-group. Indeed, if $P \in \mathrm{Syl}_p(K)$, then we obtain that $K = P\mathrm{F}(G)$ so P is not normal in G; in that case, by hypothesis, $\mathrm{N}_G(P)$ is a Θ-group. We have

$$G = \mathrm{F}(G)P\mathrm{N}_G(P) = \mathrm{F}(G)\mathrm{N}_G(P)$$

by Frattini's lemma. Then $G/\mathrm{F}(G)$ is a Θ-group as an epimorphic image of a Θ-group $\mathrm{N}_G(P)$.

Remark 1. We prove by induction that if G has no $\mathrm{S}(2, q)$-subgroup for all odd prime divisors $q \in \pi(G)$, it is 2-closed. Let P, P_1 be distinct Sylow 2-subgroups of G such that $D = P \cap P_1$ is as large as possible. Suppose that $D = \{1\}$ and take an involutions $u \in P$ and $u_1 \in P_1$. Then $R = \langle u, u_1 \rangle$ is not a 2-group by assumption; moreover, R is dihedral. If Q is a subgroup of odd prime order q in R, then $\langle u, Q \rangle$ is dihedral of order $2q$ so it is an $\mathrm{S}(2, q)$-subgroup, contrary to the hypothesis. Now suppose that $D > \{1\}$. Then $\mathrm{N}_G(D)$ is non-2-closed (Burnside; see the proof of Theorem A.39.5). Hence $\mathrm{N}_G(D)/D$ is also non-2-closed. Therefore, by induction, $\mathrm{N}_G(D)/D$ possesses an $\mathrm{S}(2, q)$-subgroup H/D for some odd prime q. Let T be a subgroup of D minimal such that $TD = H$. Since $T \cap D \leq \Phi(T)$ and $T/(T \cap D) \cong H/D$ is an $\mathrm{S}(2, q)$-subgroup, it follows that T is a $\mathrm{B}(2, q)$-subgroup. Then a minimal nonnilpotent subgroup of T is an $\mathrm{S}(2, q)$-subgroup, a contradiction. Thus G is 2-closed.

For $T \leq G$, let T^G denote the normal closure of T in G.

We know (see §10) that G' is contained in the subgroup generated by all minimal nonabelian subgroups of G. In addition, we will prove the following deeper

Proposition A.39.7. *Let $G = G' > \{1\}$. Then there exists in G an $\mathrm{S}(2, q)$-subgroup T for an appropriate odd prime q such that $T^G = G$.*

Proof. We use induction on $|G|$.

Let us prove that G possesses an $S(2,q)$-subgroup T such that $T^G = G$. If G is simple, our proposition asserts not more than the existence of an $S(2,q)$ in G for some odd prime q; this is true by Remark 1. Let G be not simple and N a minimal normal subgroup of G. As $(G/N)' = G/N > \{1\}$, there exists in G/N an $S(2,q)$-subgroup H/N such that $(H/N)^{G/N} = G/N$ by induction; then we have $H^G = G$. Let F be a subgroup of H minimal such that $FN = H$. Then we conclude that $F \cap N \leq \Phi(F)$ and $F/\Phi(F)$ is an $S(2,q)$-subgroup; in that case, F is an $B(2,q)$-subgroup. We have $F^G N = (FN)^G = H^G = G$ so either $F^G = G$ or else $F^G \cap N = \{1\}$ since N is a minimal normal subgroup of G. In the first case, we are done. Indeed, if $S \leq F$ is an S-subgroup, then S is an $S(2,q)$-subgroup and $S^F = F$; in that case, we obtain $S^G = (S^F)^G = F^G = G$.

Thus one may assume that the second case always holds. In this case, $G = F^G \times N$. We see that every minimal normal subgroup of G has a direct complement. It follows that $G = N_1 \times \cdots \times N_r$, where $N_1, \ldots, N_r$ are simple and nonabelian since $G' = G$. Let u_i be an involution in N_i, $i = 1, \ldots, r-1$; set $u = u_1 \ldots u_{r-1}$. It is clear that $\langle u \rangle^G = N_1 \times \cdots \times N_{r-1}$. By the above, N_r possesses an $S(2,q)$-subgroup K. Let v be a generator of a Sylow 2-subgroup of K and let $Q \in \mathrm{Syl}_q(K)$. Then uv normalizes but does not centralize Q and $(uv)^2 = u^2 v^2 = v^2$ centralizes Q since v^2 generates the center of K. It follows that $T = \langle uv, Q \rangle$ is an $S(2,q)$-subgroup. Further, we have $TN_r = \langle uv, Q, N_r \rangle = \langle u, N_r \rangle$ since $v \in N_r$ and $Q < N_r$. It follows that

$$T^G N_r = (TN_r)^G = \langle u, N_r \rangle^G = \langle u^G, N_r \rangle = \langle N_1 \times \cdots \times N_{r-1}, N_r \rangle = G.$$

Since $N_r = Q^G \leq T^G$, we get $G = T^G N_r = T^G$, completing the proof. □

It follows from Proposition A.39.7 that if G is a nonsolvable group, then G/T^G is solvable for some $S(2,q)$-subgroup $T < G$. Indeed, let D be the last member of the derived series of G. Then $D' = D$ so $D = T^D$ for some $S(2,q)$-subgroup T of D. Since $T^G = T^D$, our claim follows.

Let $G = A \times B$, where $A \cong A_5$, $B \cong Sz(2^3)$. Assume that, for some $q \in \pi(G)$, G possesses an $S(q,2)$-subgroup H with $H^G = G$. Note that all $S(q,2)$-subgroups in A have order $12 = 3 \cdot 2^2$ and in B — order $56 = 7 \cdot 2^3$. If $A \cap H = \{1\}$, then $7 \mid |H|$ since H is isomorphic to an $S(q,2)$-subgroup in $G/A \cong B$, and $H < B$ since 7 does not divide $|G : B|$, and so $H^G = B < G$ since B is generated by subgroups of order 7, a contradiction. Thus $A \cap H > \{1\}$. Similarly, $B \cap H > \{1\}$. If $A \cap H \in \mathrm{Syl}_2(H)$, then $A \cap H \in \mathrm{Syl}_2(A)$ has order 4 so that $q = 3$, and then $H < A$ so $H^G = A < G$, a contradiction. Thus we obtain $A \cap H \not\leq \mathrm{Syl}_2(H)$. It follows that $H/(A \cap H) \cong HA/A$ is isomorphic to an $S(q,2)$-subgroup in $G/A \cong B$ so $q = 7$. Then 7 divides $|H \cap B|$ so $H^G = B < G$, a contradiction. Thus H does not exist.

Remark 2. Kegel [Keg1] has proved that if $A, B < G$, $AB < G$ and $AB^g = B^g A$ for all $g \in G$, then either $A^G < G$ or $B^G < G$ (see Appendix 28, Remark 4). It follows

from that result that if $A < G$ and $AA^g = A^g A$ for all $g \in G$, then A is subnormal in G (see Appendix 28, Exercise 4). Next we use the following obvious assertion. If $A, B_1, \ldots, B_n \leq G$ and $AB_i = B_i A$ for all i, then $A\langle B_1, \ldots, B_n\rangle = \langle B_1, \ldots, B_n\rangle A$.

We use Remark 2 to prove the following

Proposition A.39.8. *Let $M < G$. Suppose that M is permutable with all minimal nonnilpotent subgroups of G. Then either $G' < G$ or $M^G < G$.*

Proof. Let $N \triangleleft G$. We claim that MN/N is permutable with all minimal nonnilpotent subgroups of G/N. Let H/N be a minimal nonnilpotent subgroup of G/N and let C be minimal such that $H = CN$. Then $C \cap N \leq \Phi(C)$ and $H/N \cong C/(C \cap N)$ so $C/\Phi(C)$ is minimal nonnilpotent. It follows that C is a B-subgroup. If S is a minimal nonnilpotent subgroup of C, then $S^C = C$. Since M is permutable with S and all its conjugates, we get $MC = CM$ (Remark 2). It follows that MN/N is permutable with $CN/N = H/N$, and our claim follows.

Next we assume that G is a counterexample of minimal order; then $M^G = G = G'$.

Let $N \triangleleft G$ be such that $MN < G$. By the first paragraph of the proof, MN/N is permutable with all minimal nonnilpotent subgroups of G/N. Since $(G/N)' = G/N$ and $(MN/N)^{G/N} = G/N$, we have $|G/N| = |G|$ by induction. Thus, if $N > \{1\}$ is normal in G, then $MN = G$.

Assume that M is nilpotent and $HM = G$ for all minimal nonnilpotent subgroups H of G. Let H be $\mathrm{S}(p, q)$-subgroup. Then we obtain that $\pi(|G : M|) = \{p, q\}$ since $|\pi(|G : M|)| > 1$ by the Kegel–Wielandt factorization theorem (see Theorems A.28.14 and A.28.18). By Burnside's two-prime theorem, there exists $r \in \pi(G) - \{p, q\}$; then G possesses an $\mathrm{S}(t, r)$-subgroup F for some $t \in \pi(G) - \{r\}$ (Frobenius' theorem [Isa5, Theorem 9.18] and Theorem A.22.1) since $G' = G$. Then we get $FM < G$ as $r \notin \{p, q\} = \pi(|G : M|)$, contrary to our assumption.

Thus, if M is nilpotent, there exists in G a minimal nonnilpotent subgroup H such that $HM < G$. Then $H^g M = MH^g$ for all $g \in G$ hence, by Kegel (see Remark 2), $H^G < G$ in view of $M^G = G$. Since $G' = G$, we get $H^G M < G$, contrary to the result of the third paragraph of the proof.

Thus M is nonnilpotent. Let $\mathcal{N}(M)$ be a subgroup generated by all minimal nonnilpotent subgroups of M; then $\mathcal{N}(M) > \{1\}$. In this case, $\mathcal{N}(M)M^g = M^g\mathcal{N}(M)$ for all $g \in G$ (Remark 2). It follows that $\mathcal{N}(M)M^g < G$. Indeed, otherwise we have $MM^g = G$ since $\mathcal{N}(M)M^g \leq MM^g$, which is not the case (Ore's Lemma 28.8). Since $M^G = G$, we get $\mathcal{N}(M)^G < G$ (Kegel; see Remark 2). By the third paragraph of the proof, $M\mathcal{N}(M)^G = G$. Then $\{1\} < G/\mathcal{N}(M)^G \cong M/(M \cap \mathcal{N}(M)^G)$ is nilpotent as an epimorphic image of $M/\mathcal{N}(M)$, and we conclude that $G = \mathcal{N}(M)^G$ since $G' = G$. This contradicts to what has just been proved. □

Suppose that all minimal nonnilpotent subgroups are subnormal in G. We will prove that then the nilpotent length of G is at most 2. Indeed, if H is a $\mathrm{B}(p, q)$-subgroup of G, then H is subnormal in G since it is generated by (subnormal in G) minimal non-

nilpotent subgroups. Then H' is a subnormal q-subgroup so $H' \leq \mathrm{F}(G)$, and hence, by Theorem A.39.2(b), $G/\mathrm{F}(G)$ is nilpotent.

Proposition A.39.9. *Let $\mathcal{S}(2,*)$ be the set of all minimal nonnilpotent subgroups of G with nonidentity cyclic Sylow 2-subgroups. If any two minimal nonnilpotent subgroups F, H of G such that $F \in \mathcal{S}(2,*)$ and $|F| \neq |H|$ are permutable, then G is solvable.*

Proof. Suppose that G is a counterexample of minimal order.

(a) Assume that G is simple. By Remark 1, there exists an $\mathrm{S}(2,q)$-subgroup $F < G$, $q \in \pi(G) - \{2\}$. In view of Burnside's two-prime theorem, there is $p \in \pi(G) - \{2,q\}$. Let H be an $\mathrm{S}(r,p)$-subgroup of G for some $r \in \pi(G) - \{p\}$. Then $FH^x = H^x F$ for all $x \in G$ since $|F| \neq |H|$. As G is simple, $G = FH$ by Remark 2. Since a Sylow 2-subgroup of G is not cyclic and $p > 2$, we get $r = 2$. In view of Theorem A.22.1 and the product formula, we obtain $|G| = 2^\alpha pq$. By the classification of finite simple groups, there exist exactly two simple groups S having orders of this form, namely, $\mathrm{L}_2(5)$ and $\mathrm{L}_2(7)$. The group $G = \mathrm{L}_2(5)$ has exactly three distinct orders of S-subgroups, namely, 6, 12 and 10. The product of any of the last two subgroups with the first one is not equal to G. In the group $S = \mathrm{L}_2(7)$ all $\mathrm{S}(2,q)$-subgroups have order 6, other minimal nonnilpotent subgroups have orders 12 and 21; it is clear that S does not satisfy the hypothesis. It follows from what has just been proved that G has no nonabelian simple subgroup.

(b) We claim that whenever F, H are $\mathrm{B}(2,q)$- and $\mathrm{B}(p_1,q_1)$-subgroups of G with distinct pairs $\{2,q\}$ and $\{p_1,q_1\}$, then $FH = HF$. Indeed, if L, M are S-subgroups of F, H, respectively, then $LM = ML$ by hypothesis. Since B-groups are generated by minimal nonnilpotent subgroups, our claim follows (Remark 2).

(c) Let N be a minimal normal subgroup of G. We claim that G/N satisfies the hypothesis. Indeed, let F/N and H/N be $\mathrm{S}(2,q)$- and $\mathrm{S}(p_1,q_1)$-subgroups of G/N such that the pairs $(2,q)$ and (p_1,q_1) are distinct. Let L and M be subgroups minimal such that $LN = F$ and $MN = H$. Then L, M are $\mathrm{B}(2,q)$- and $\mathrm{B}(p_1,q_1)$-subgroups, respectively, so $LM = ML$ by (b). In that case, $F = LN$ and $H = MN$ are permutable by Remark 2, and our claim follows. By induction, G/N is solvable. Since G has no nonabelian simple subgroups, the subgroup N is solvable. It follows that G is solvable, as required. □

Appendix 40

Varia

In this section we report a number of new results and improve some proofs from Volumes 1 and 2. Some results of this appendix became starting points of theorems in the main text. The section also contains numerous exercises, most of them with solutions.

1^o. We begin with the following

Definition 1 ([QT]). A group G is said to be an NC-*group* if, whenever $H < G$ is abelian and $x \in H^{\#}$, then $\mathrm{C}_G(x) \leq \mathrm{N}_G(H)$.

The property NC is inherited by subgroups. The following groups are NC-groups: (i) M_{p^n}, (ii) the Frobenius group of order pq^n with abelian kernel of order q^n.

In this subsection we prove the following

Theorem A.40.1 (compare with [QT]). *If a non-Dedekindian p-group G of order $> p^3$ is an* NC-*group, then G' is the unique minimal normal subgroup of G and one of the following holds:*

(a) $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ *and* $\mathrm{Z}(G)$ *is cyclic. Then either* $G \cong \mathrm{M}_{p^n}$ *or* $G = M * C$, *where* $|M| = p^3$ *with* $\Omega_1(M) = M$ *and* C *is cyclic*

(b) $G = \mathrm{D}_8 * \mathrm{Q}_8$ *is extraspecial of order* 2^5.

Below we list some properties of a non-Dedekindian NC-group G which is also a p-group. One may assume that $|G| > p^3$.

(1) A subgroup $A < G$ is G-invariant if and only if $A \cap \mathrm{Z}(G) > \{1\}$. Indeed, let $L = \langle x \rangle \leq A \cap \mathrm{Z}(G)$ be of order p and let $U/L \leq A/L$ be cyclic; then U is abelian and $G = \mathrm{C}_G(x) \leq \mathrm{N}_G(U)$ so $U \lhd G$, and hence $A \lhd G$ since it is generated by all such U. The converse assertion is known.

(2) If G is non-Dedekindian, then $\mathrm{Z}(G)$ is cyclic and $|G'| = p$. Indeed, there is a nonnormal cyclic $U < G$. Assume that there is $R \times S \leq \mathrm{Z}(G)$, where $|R| = p = |S|$. By (1), we get $(R \times S) \cap U = \{1\}$ and the abelian subgroups $UR, US \lhd G$ hence $U = UR \cap US \lhd G$, a contradiction. Thus $\mathrm{Z}(G)$ is cyclic. Assume that $|G'| > p$, and let $R \leq G' \cap \mathrm{Z}(G)$ be of order p. Then, by (1), G/R is Dedekindian and, by assumption, nonabelian so that $p = 2$ (Theorem 1.20). In that case, there is $Q/R \leq G/R$ with $Q/R \cong \mathrm{Q}_8$. By Theorem 1.2, Q is not of maximal class so $|Q'| = 2$ (Taussky). Since $Q \lhd G$, we get $Q' \lhd G$ so $R \times Q' \leq \mathrm{Z}(G)$, i.e., $\mathrm{Z}(G)$ is noncyclic, contrary to what has just been proved. Thus $|G'| = p$.

(3) If G is extraspecial of order p^5, then we have $p = 2$ and $G = \mathrm{Q}_8 * \mathrm{D}_8$. Indeed, let $G = A * B$, where A and B are nonabelian of order p^3. One may assume that $\Omega_1(A) = A$. Assume that there is $y \in B - A$ of order p. Since $K = A \times \langle y \rangle$ is an NC-group with noncyclic $\mathrm{Z}(K)$, we get a contradiction since K is non-Dedekindian. Thus B has only one subgroup of order p, so $p = 2$ and $B \cong \mathrm{Q}_8$ (Proposition 1.3). Assume that $A \cong \mathrm{Q}_8$. Then $G = \mathrm{D}_8 * \mathrm{D}_8$, contrary to what has just been proved. Thus we get $A \cong \mathrm{D}_8$. Then all subgroups of G of order > 2 are G-invariant hence G is an NC-group.

(4) If $G/\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$ and $|G| > p^3$, then we have $G = M\mathrm{Z}(G)$, where $|M| = p^3$ and $\Omega_1(M) = M$. Indeed, let $U < G$ be of order $> p$. Then we must have $U \lhd G$ since $U \cap \mathrm{Z}(G) > \{1\}$ (otherwise, $G = U \times \mathrm{Z}(G)$ is abelian); see (1). Thus all nonnormal subgroups of G have order p. By Theorem 1.25, either $G \cong \mathrm{M}_{p^n}$ or $G = M\mathrm{Z}(G)$.

Proof of Theorem A.40.1 (Berkovich). By (1) and (2), in view of Lemma 4.2, we have $G = (A_1 * \cdots * A_k)\mathrm{Z}(G)$, where $A_1, \ldots, A_k$ are minimal nonabelian and $\mathrm{Z}(G)$ is cyclic. If $k = 1$, then $\mathrm{Z}(A_1) \leq \mathrm{Z}(G)$ so $|G : \mathrm{Z}(G)| = p^2$ and so, by (4), G is as in (a).

Now let $k > 1$. We use induction on k. By induction, $k = 2$; then $G = B\mathrm{Z}(G)$, where $B = A_1 * A_2$.

If $A_1 \cong \mathrm{M}_{p^n}$ and $U < A_1$ is noncyclic maximal, then $A_2 * U$ is a non-Dedekindian NC-group with noncyclic center, contrary to (2). Thus we get $|A_i| = p^3$, $i = 1, 2$. Since $\mathrm{Q}_8 * \mathrm{Q}_8 \cong \mathrm{D}_8 * \mathrm{D}_8$ of order 32 is not an NC-group, one may assume that $A_1 \ncong \mathrm{Q}_8$. If $p > 2$, then $A_2 U$ is a non-Dedekindian NC-group with noncyclic center, a contradiction. Thus $p = 2$. By the above, $A_1 \ncong A_2$. Thus

$$B := A_1 * A_2 \cong \mathrm{D}_8 * \mathrm{Q}_8.$$

Assume that $\mathrm{Z}(G) \not\leq B$. Let $R \leq \mathrm{Z}(G)$ be cyclic of order 4 (recall that $\mathrm{Z}(G)$ is cyclic by (2)). Then $\mathrm{Q}_8 * R \cong D * R$, where $D \cong \mathrm{D}_8$. Note that $[\mathrm{Q}_8 * R, \mathrm{D}_8] = \{1\}$ and $(\mathrm{Q}_8 * R) \cap \mathrm{D}_8 = \mathrm{Z}(\mathrm{D}_8)$. Then G contains a subgroup $\mathrm{D}_8 * D \cong \mathrm{Q}_8 * \mathrm{Q}_8$ which, as we know, is not an NC-group, a contradiction. Thus $\mathrm{Z}(G) \leq B$, as was to be shown. □

Exercise 1. If in the definition of a NC-group we consider only two-generator abelian subgroups H, we obtain the definition of NC_2-groups. Is it true that NC_2-groups coincide with NC-groups?

2^o. Here we prove the following

Theorem A.40.2. *Suppose that $G = \mathrm{ES}(m, 2)$ is an extraspecial group of order 2^{1+2m} and let G_0 be a 2-group. If $\phi : G \to G_0$ is a lattice isomorphism, then G_0 is also extraspecial. (This solves Exercise 25.6 for $p = 2$.)*

Proof. We have $|\Phi(G_0)| = 2$. If $E \leq G$ is minimal nonabelian (of order 8), $E^\phi \cong E$ is also minimal nonabelian. Thus G_0 is nonabelian hence $G_0' = \Phi(G_0)$.

Let X be a group and let $\varphi_2(X)$ denote the number of noncommuting ordered pairs $(x, y) \in X \times X$ such that $\langle x, y \rangle = X$ (it follows that $\varphi_2(X) > 0$ if and only if X is

nonabelian and two-generator; this function φ_2 was introduced by Mann). Let $\mathrm{k}(X)$ be the class number of X. Then (see §76, formulas (1) and (2)) we have

$$\sum_{H \le X} \varphi_2(H) = |X|(|X| - \mathrm{k}(X)). \tag{1}$$

Let $\alpha_1(G)$ be the number of minimal nonabelian subgroups of G. By the first paragraph of the proof, $\alpha_1(G_0) = \alpha_1(G)$. We have $\mathrm{k}(G) = 2^{2m} + 1$. Let $E \le G$ be nonabelian and two-generator. Then $E' = G'$ and $E/E' \cong \mathrm{E}_{2^2}$. It follows that $|E| = 2^3$ so E is minimal nonabelian. By §76, formula (1) and Example 1, we have

$$\varphi_2(E) = (|E - \Phi(E)|)(|E| - 2|\Phi(E)|) = (2^3 - 2)(2^3 - 2^2) = 24. \tag{2}$$

It follows from (1) and (2) that

$$2^{2m+1}(2^{2m+1} - \mathrm{k}(G)) = 24\alpha_1(G) = 24\alpha_1(G_0) = 2^{2m+1}(2^{2m+1} - \mathrm{k}(G_0))$$

so that $\mathrm{k}(G_0) = \mathrm{k}(G) = 2^m + 1$. Let $|\mathrm{Z}(G_0)| = 2^z$. We have

$$2^{2m} + 1 = \mathrm{k}(G_0) = |\mathrm{Z}(G_0)| + \frac{|G_0 - \mathrm{Z}(G_0)|}{2} = 2^z + \frac{2^{2m+1} - 2^z}{2} = 2^{2m} + 2^{z-1}.$$

It follows that $z = 1$ so that G_0 is extraspecial. □

The above argument does not work in the case when $\exp(G) = p^2$ and $p > 2$ since M_{p^3} is lattice isomorphic to the abelian group of type (p^2, p).

3^o. In this subsection we present three easy exercises.

Exercise 2. Classify the p-groups G with $\mathrm{d}(G) > 2$ all of whose normal subgroups of index p^2 have exponent p.

Solution (Mann). We prove that $\exp(G) = p$. Assume, however, that there is $x \in G$ of order $> p$. Then the normal closure $H = \langle x \rangle^G \in \Gamma_1$ by hypothesis. Take $y \in G - H$ and set $K = \langle x, y \rangle$; then $K < G$ since $\mathrm{d}(G) > 2$, so $K \le L \in \Gamma_1$. Since $x \in K$, we get $H = \langle x \rangle^G \le L$. Comparing the orders, we obtain $L = H$ so $y \in L = H$, contrary to the choice of y.

Exercise 3. Given k, let G be a p-group with $\mathrm{d}(G) > 2$. If all normal subgroups of index p^2 in G have exponent $\le p^k$, then $\exp(G) \le p^k$.

Solution. Assume that $\exp(G) > p^k$. Since the members of the set Γ_2 cover G, there is $N \in \Gamma_2$ with $\exp(N) > p^k$, contrary to the hypothesis. (Exercise 2 is a partial case of this exercise.)

Exercise 4. Given a positive integer k, study the p-groups G with $\mathrm{d}(G) > 2$ and such that all normal subgroups of index p^2 in G, except one, have exponent $\le p^k$.

4^o. Suppose that G is a 2-group such that $\Gamma_1 = \{H = H_1, H_2, A\}$, where H_2 is an $\mathcal{A}_1$-group and A is abelian. If G is not an $\mathcal{A}_2$-group, then, according to Janko's report, we have

$$G = \langle a, x \mid [a, x] = v,\ v^4 = 1,\ v^2 = z,\ a^{2^r} = z^\epsilon, x^2 = z^\eta, v^x = v^{-1}, v^a = v^{-1} \rangle,$$

where $r > 1, \epsilon, \eta = 0, 1$. Here $|G| = 2^{r+3}$, $E = \langle v, x \rangle \cong \mathrm{D}_8$ or Q_8 (depending on $\eta = 0$ or 1) is normal in G,

$$G = E\langle a \rangle, \quad E \cap \langle a \rangle = \langle z^\epsilon \rangle, \quad G' = \langle v \rangle, \quad \Phi(G) = G'\langle a^2 \rangle,$$

$\mathrm{Z}(G) = \langle a^2, z \rangle$ is of order 2^r. If $\epsilon = 1$, then $\mathrm{Z}(G) = \langle a^2 \rangle$ is cyclic and if $\epsilon = 0$, then $\mathrm{Z}(G) = \langle z \rangle \times \langle a^2 \rangle$ is noncyclic. In addition, we have $H = H_1 = E\langle a^2 \rangle$, $H_2 = \langle v, a \rangle$ is metacyclic and if $\epsilon = 1$, then $H_2 \cong \mathrm{M}_{2^{r+2}}$ and $A = \langle a^2, v, ax \rangle$ is abelian of rank 2. Finally, $G = \langle ax \rangle \langle x \rangle$ is a product of two cyclic subgroups.

5^o. In this subsection we prove the following easy

Proposition A.40.3. *Suppose that G is a group of exponent $p^e > p$. Then any two elements of G of distinct orders are permutable if and only if $\Omega_{e-1}(G) \leq \mathrm{Z}(G)$.*

Proof. If $\Omega_{e-1}(G) \leq \mathrm{Z}(G)$, then G satisfies the hypothesis.

Now we assume that any two elements of G of distinct orders are permutable. Assume also that G is nonabelian. Set $H = \Omega_{e-1}(G)$. Assume that $\exp(H) = p^e$. Then, by hypothesis, all elements of H of order p^e, being permutable with all generators of H of orders $< p^e$, are contained in $\mathrm{Z}(H)$. Let $h \in H$ be of order p^e and let $y \in H$ be of order $< p^e$. Then we get $o(hy) = p^e$ so $hy \in \mathrm{Z}(H)$. It follows that $y \in \mathrm{Z}(H)$, and we conclude that H is abelian, a contradiction since the abelian $H = \Omega_{e-1}(H)$ cannot be of exponent p^e. Thus $\exp(H) = p^{e-1}$. It follows that

$$\Omega_e^*(G) = \langle v \in G \mid o(v) = p^e \rangle = \langle G - H \rangle = G.$$

If $g \in G - H$, then $o(g) = p^e$ and g commutes with all elements of H, and we conclude that $H \leq \mathrm{Z}(G)$, as required. □

6^o. In a letter to the first author, Mann noticed that the following result holds.

Theorem A.40.4. *Let $\chi \in \mathrm{Irr}(G)$ be faithful and $\{1\} < \mathrm{Z}(G) < \mathrm{Z}_2(G)$. Then we have $\mathrm{Z}_2(G) - \mathrm{Z}(G) \subseteq \mathrm{T}_\chi$, where T_χ is the set of zeros of χ.*

Proof (this proof is the same as the proof of Theorem 2.31 in [Isa1]). Take some elements $x \in \mathrm{Z}_2(G) - \mathrm{Z}(G)$ and $y \in G$ such that $[x, y] = z \neq 1$. Then $x^y = xz$, where $z \in \mathrm{Z}(G)$. We have $\chi(x) = \chi(x^y) = \chi(xz)$. If T is a representation of G affording χ, then $T(xz) = T(x)T(z) = \epsilon T(x)$ since $T(z) = \epsilon \mathrm{I}_{\chi(1)}$, where $\mathrm{I}_{\chi(1)}$ is the identity $\chi(1) \times \chi(1)$ matrix. It follows that $\chi(x) = \chi(xz) = \epsilon\chi(x)$, and we can conclude that $\chi(x) = 0$ since $\epsilon \neq 1$ (indeed, T is faithful). □

Proposition A.40.5. *Suppose that the Frattini subgroup of an irregular p-group G has no subgroup of order p^{p+1} and exponent p. Then $|\Omega_1(\Phi(G))| \in \{p^{p-1}, p^p\}$.*

Proof. By Theorem 9.8(d), $|\Omega_1(\Phi(G))| \geq p^{p-1}$. Assume that $|\Omega_1(\Phi(G))| > p^{p-1}$. Then $\Phi(G)$ possesses a subgroup of order p^p and exponent p (Theorem 7.1) so $\Phi(G)$ is not absolutely regular. Since $|\mathrm{Z}(\Phi(G))| > p$, it follows that $\Phi(G)$ is not of maximal class. Therefore the number of subgroups of order p^p and exponent p in $\Phi(G)$ is $\equiv 1 \pmod p$ by Theorem 13.5. It follows that there is in $\Phi(G)$ a G-invariant subgroup R of order p^p and exponent p. Assume that there is $x \in \Phi(G) - R$ of order p. By hypothesis, $T = \langle x, R\rangle (\leq \Phi(G))$ is of exponent $> p$ so T is irregular (Theorem 7.2(b)). Since $|T| = p^{p+1}$, we conclude that T is of maximal class (Theorem 7.1(b)). On the other hand, $|R \cap \mathrm{Z}(\Phi(G))| \geq p^2$ so that $|\mathrm{Z}(T)| \geq p^2$, and T is not of maximal class. The obtained contradiction shows that $R = \Omega_1(\Phi(G))$. □

Proposition A.40.6. *Suppose that any nonabelian subgroup of a nonabelian p-group G is contained in only one maximal subgroup of G. Then one and only one of the following holds:*

(a) $\mathrm{d}(G) = 2$ *and* $\Phi(G)$ *is abelian.*

(b) $\mathrm{d}(G) = 3$ *and* $\Phi(G) \leq \mathrm{Z}(G)$.

Proof (Janko). Obviously, $\Phi(G)$ is abelian. If $\mathrm{d}(G) = 2$, then G satisfies the hypothesis. Now let $\mathrm{d}(G) > 2$. If $S/\Phi(G) < G/\Phi(G)$ is of order p, then S is abelian since S is contained in more than one maximal subgroup of G. This gives $\mathrm{C}_G(\Phi(G)) = G$ and so $\Phi(G) \leq \mathrm{Z}(G)$. Since G is nonabelian, there are $x, y \in G - \Phi(G)$ such that $[x, y] \neq 1$. Set $T = \Phi(G)\langle x, y\rangle$ so that $T/\Phi(G) \cong \mathrm{E}_{p^2}$ and T is nonabelian. This implies $|G/T| = p$ and so $\mathrm{d}(G) = 3$, and G is as in (b). Conversely, any group in (b) satisfies the hypothesis. □

7^o. If $\phi : G \to H$ is a lattice isomorphism of a nonabelian p-group G onto H, then H is also nonabelian p-group (Theorem 25.5)

Proposition A.40.7. *Let G be an U_2-group (see §§17, 18) and a 2-group H be lattice isomorphic to G. Then H is also an U_2-group.*

Proof. Let $R \lhd G$ be abelian of type $(2, 2)$ and G/R be of maximal class. Let H and G be lattice isomorphic via ϕ and T/R be cyclic of index 2. Then T is either abelian of type $(2^n, 2)$ or $\cong \mathrm{M}_{2^{n+1}}$. In this case, T^ϕ is abelian of type $(2^n, 2)$ or $\cong \mathrm{M}_{2^{n+1}}$. It follows that $R^\phi = \Omega_1(T^\phi) \lhd G^\phi = H$. Then $H/R^\phi \cong G/R$ so H/R^ϕ is of maximal class. It is clear now that H is a U_2-group. □

Let $p > 2$ and let G be a nonabelian p-group all of whose nonnormal subgroups are cyclic. Then $\mathrm{Z}(G)$ has no subgroup $\cong \mathrm{E}_{p^3}$ so G has no such a subgroup. It follows that G is a group from Theorem 13.7. If G is metacyclic, then G is minimal nonabelian. Indeed, $G/\Omega_1(G)$ is abelian so $|G'| = p$ since G', being cyclic, is a proper subgroup

of $\Omega_1(G)$, and now the assertion follows from Lemma 65.2(a). If G is a 3-group of maximal class and $|G| > 3^3$, then $|G| = 3^4$, $\Omega_1(G) \cong \mathrm{E}_9$. In case $G = EC$, where $E = \Omega_1(G) \cong \mathrm{S}(p^3)$ and C is cyclic, all subgroups of G of type (p, p) are normal so $|G'| = p$. Then, by Lemma 4.2, $G = E * \mathrm{C}_G(E)$, where $\mathrm{C}_G(E)$ is cyclic.

8^o. A non-Dedekindian p-group all of whose nonnormal subgroups of same order are conjugate is termed a CO-*group*. Janko has reported about the classification of CO-groups; this solves Problem 1261. Below we offer another proof of this nice result (see Corollary A.40.9).

A non-Dedekindian p-group G is termed a CCO-*group* if all its nonnormal cyclic subgroups of same order are conjugate. Obviously, a CO-group is a CCO-group. The group SD_{2^n} is a CCO-group, but it is not a CO-group. The property CO is inherited by epimorphic images, but this is not true for the property CCO.

Lemma A.40.8. *Suppose that a p-group G is a* CCO-*group and $|G'| = p$. Then we have $G \cong \mathrm{M}_{p^t}$.*

Proof. In view of Lemma 96.1(c), one may assume that G has a proper minimal nonabelian subgroup, say B; then $B \lhd G$ since $B' = G'$. In that case, we have $G = B * C$, where $C = \mathrm{C}_G(B)$ (Lemma 4.2) and we conclude that B is either Dedekindian or a CCO-group; in the first case $B \cong \mathrm{Q}_8$, in the second case $B \cong \mathrm{M}_{p^t}$ (Lemma 96.1(c)). The size of every noncentral G-class is equal to $p(= |G'|)$. Therefore, by hypothesis, if $U < G$ is nonnormal cyclic, there are exactly p nonnormal cyclic subgroups of order $|U|$ in G.

(i) Assume that $B = \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ x^y = x^3 \rangle \cong \mathrm{Q}_8$. We obtain that $\exp(C) > 2$ since G is not Dedekindian. Let $L = \langle z \rangle \le C$ be cyclic of order 4. Write $H = BL$; then $H \lhd G$. If $B \cap L = \mathrm{Z}(B)$, then H has exactly $6 > 2$ nonnormal subgroups of order 2, a contradiction. Thus $B \cap L = \{1\}$; then $H = B \times L$ has $3 > 2$ distinct nonnormal cyclic subgroups $\langle xz \rangle$, $\langle yz \rangle$, $\langle xyz \rangle$ of the same order 4, a contradiction. It follows that G has no subgroup $\cong \mathrm{Q}_8$.

(ii) Now let $B = \langle u, v \mid u^{p^{t-1}} = v^p = 1, u^v = u^{1+p^{t-2}} \rangle \cong \mathrm{M}_{p^t}$. Assume that $X = \langle x \rangle < G$ of order p is such that $X \not\le B$; then X is not conjugate with $\langle v \rangle$ so $X \lhd G$ and $F = B \times X$ has exactly $p^2 > p$ noncentral so non-G-invariant subgroups of order p; then G is not a CCO-group, a contradiction. Thus $\Omega_1(G) = \Omega_1(B) \cong \mathrm{E}_{p^2}$ so C has exactly one subgroup of order p; then C is cyclic by (i). In that case, there is a cyclic $W = \langle w \rangle \le C$ such that $W \not\le B$ and $w^p \in \mathrm{Z}(B)$. Let $A < B$ be cyclic of index p. Then A has index p in the noncyclic abelian group AW, and so $AW = A \times Y$, where $Y \not\le B$ has order p, contrary to what has just been proved. □

Corollary A.40.9. *If a p-group G is a* CO-*group, then $G \cong \mathrm{M}_{p^t}$.*

Proof. We use induction on $|G|$. By Lemma A.40.8, one may assume that $|G'| > p$. In view of Lemma 96.2, there is $K_1 \le G' \cap \mathrm{Z}(G)$ of order p such that G/K_1 is not Dedekindian. Since G/K_1 is a CO-group, we obtain that $G/K_1 \cong \mathrm{M}_{p^t}$ by induction.

As $K_1 < G' \leq \Phi(G)$, we get

$$\mathrm{d}(G) = \mathrm{d}(G/K_1) = 2.$$

Let A/K_1 and B/K_1 be two distinct cyclic subgroups of index p in G/K_1; then A and B are abelian maximal subgroups of G. It follows that $A \cap B = \mathrm{Z}(G)$ so $|G'| = p$ (Lemma 1.1), contrary to the assumption. □

Corollary A.40.10. *Suppose that all nonnormal subgroups of same order of a nilpotent non-Dedekindian group G are conjugate. Then there is only one prime p for which G has a Sylow p-subgroup, say P, that is non-Dedekindian; then $P \cong \mathrm{M}_{p^n}$. In this case, all other Sylow subgroups are cyclic.*

Proof. Assume that $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$ are distinct and P, Q are not Dedekindian. Let $U < P$ be nonnormal, let $V < Q$ be nonnormal and let $W < Q$ be normal, $|V| = |W|$. Then UV and UW are not G-invariant of the same order, but $(UV)_G \neq (UW)_G$. It follows that UV and UW are not conjugate in G. Thus one may assume that Q is Dedekindian. If, in addition, Q is noncyclic, it has two distinct subgroups, say A and B, of same order. Then AU and BU have the same order and are not conjugate in G. Thus Q is cyclic. The proof is complete. □

Theorem A.40.11. *Suppose that all nonnormal cyclic subgroups of same order of a non-Dedekindian p-group G belong to the same conjugate class of size p. Then we have $G \cong \mathrm{M}_{p^t}$.*

Proof. In the light of Lemma A.40.8, one may assume that $|G'| > p$. By hypothesis, whenever $L < G$ is nonnormal cyclic, then G contains exactly p conjugate cyclic subgroups of order $|L|$. We proceed by induction on $|G|$.

Assume that G is a 2-group of maximal class. Then $|G| > 8$. If $G \cong \mathrm{Q}_{2^n}$, $n > 3$, then G has > 2 nonnormal cyclic subgroups of order 4. In case $G \ncong \mathrm{Q}_{2^n}$, G has > 2 nonnormal subgroups of order 2. Thus G is not a 2-group of maximal class.

By Lemma 96.2, there is in G' a G-invariant subgroup R of order p such that G/R is non-Dedekindian. Let $X/R < G/R$ be nonnormal cyclic. Assume that X is noncyclic. Then we have $X = X_i \times R$, where X_i is cyclic of index p in X, $i = 1, \ldots, p$. The subgroup X_i is nonnormal in G (otherwise, $X = X_i \times R \lhd G$). By hypothesis, the subgroups $X_1, \ldots, X_p$ form a conjugate class in G so $X = X_1 X_2 \lhd G$, a contradiction. Thus X must be cyclic. By hypothesis, there are in G exactly p nonnormal cyclic subgroups of order $|X|$. Therefore there are exactly p nonnormal cyclic subgroups of order $|X/R|$ in G/R so G/R satisfies the hypothesis. By induction, the non-Dedekindian group $G/R \cong \mathrm{M}_{p^n}$. Then G/R has two distinct cyclic subgroups A/R and B/R of index p. In that case, A and B are two distinct abelian maximal subgroups of G, so we get $A \cap B = \mathrm{Z}(G)$. Then, by Lemma 1.1,

$$|G'| = \frac{1}{p}|G : \mathrm{Z}(G)| = p$$

contrary to the assumption. □

9^o. The 2-groups with exactly one nonmetacyclic maximal subgroup are classified by the second author (see §87). Here we do the same for p-groups with p being odd.

Proposition A.40.12. *A p-group G of order $> p^4$, $p > 2$, has exactly one nonmetacyclic maximal subgroup if and only if it is an* L_3*-group (see §§17, 18).*[1]

Proof. Suppose that G has no normal subgroup of order p^3 and exponent p. Then, by Theorem 69.3, it is either metacyclic or a 3-group of maximal class. By hypothesis, G is nonmetacyclic. In view of Theorem 9.6, G has exactly three subgroups of maximal class and index 3, and these subgroups are nonmetacyclic, a contradiction.

Now suppose that R is a G-invariant subgroup of order p^3 and exponent p. Since all maximal subgroups of G containing R are nonmetacyclic, we conclude that G/R must be cyclic. Since G has a metacyclic maximal subgroup, it follows that G has no subgroup of order p^4 and exponent p. Let $H/R < G/R$ be of order p; then we have $\exp(H) = p^2$. Since $\Omega_1(H) = \Omega_1(G)$, we have to consider two possibilities.

(i) $\Omega_1(H) = R$; then $\Omega_1(G) = R$ and G is an L_3-group.

(ii) $\Omega_1(H) = H$ so H is irregular of maximal class. It follows that $|H| \geq p^{p+1}$ (Theorem 9.5) so $p = 3$. By Exercise 13.10(a), G must be of maximal class, a contradiction since G/R is cyclic of order $> p$.

Let $M < G$ be a maximal subgroup of G such that $R \not\leq M$. Then M has a cyclic subgroup of index p so metacyclic. □

Exercise 5. If a p-group G, $p > 2$, contains at most p nonmetacyclic subgroups of index p, it is either an L_3-group or 3-group of maximal class.

10^o. Here we prove the following

Lemma A.40.13 ([GLS_5, Lemma 7.1, page 37]). *Let $p > 2$ and let G be a nonabelian p-group containing an element x of order p such that $\mathrm{C}_G(x)$ is of order p^2. Further, let $\mathrm{m}_p(G) = \max\{\mathrm{d}(H) \mid H \leq G\}$. Then $\mathrm{m}_p(G) \leq 2p-3$. If $\mathrm{m}_p(G) = 2p-3$, then $p = 3$ and G is a Sylow 3-subgroup of the symmetric group of degree 3^2.*

Proof. By Proposition 1.8, G is of maximal class. In view of Exercise 9.13, we have $\mathrm{m}_p(G) \leq p$ so $\mathrm{m}_p(G) \leq 2p-3$ since $p > 2$. If $\mathrm{m}_p(G) = 2p-3$, then $p \geq 2p-3$ hence $p = 3$ and so $\mathrm{m}_p(G) = 3 (= p)$. It follows that G is a Sylow 3-subgroup of the symmetric group of degree 3^3 (Exercise 9.13). □

11^o. Below we present a number of exercises.

Exercise 6. Let p, G and x be as in Lemma A.40.13. Then $\mathrm{m}_p(G) \leq p$. If $\mathrm{m}_p(G) = p$, then G is isomorphic to a Sylow p-subgroup of the symmetric group of degree p^2.

Solution. As above, G is of maximal class. Now the result follows from Theorem 9.6 and Exercise 9.13.

[1] A group G of order p^4, $p > 2$, has exactly one nonmetacyclic maximal subgroup if and only if $|\Omega_1(G)| = p^3$.

Exercise 7 ([GLS$_5$, Lemma 7.3, page 38]). If G is a p-group of maximal class and $G = AB$, where $A, B < G$, then $[A, B] > \{1\}$.

Solution. Assume that $[A, B] = \{1\}$. Then $A \cap B \leq \mathrm{Z}(G)$ so $|A \cap B| \leq p$ and A, B are nonabelian. Set $\bar{G} = G/(A \cap B)$ so $\bar{G} = \bar{A} \times \bar{B}$. Obviously, $|G| > p^3$. Then we get $p^2 = |G : G'| \geq |\bar{G} : \bar{G}'| > p^2$, a contradiction.

Exercise 8. Let G be a p-group of order $> p$ and $G = AB$ with $A, B < G$. If $\mathrm{Z}(G)$ is of order p and $|G : G'| = p^2$, then $[A, B] > \{1\}$.

Exercise 9. Classify the p-groups all of whose maximal cyclic subgroups are self-centralizing.

Solution. If G is abelian, it is cyclic. Now let G be nonabelian. If $U \leq G$ is maximal cyclic, then we have $\mathrm{Z}(G) < U$, so $\mathrm{Z}(G)$ is cyclic and $\Omega_1(U) \leq \mathrm{Z}(G)$. It follows that $\Omega_1(G) \leq \mathrm{Z}(G)$ and so $|\Omega_1(G)| = p$, and we conclude that $p = 2$ and G is generalized quaternion.

Exercise 10. If G be a nonabelian p-group of exponent $> p$ all of whose maximal cyclic subgroups of composite orders are self-centralizing, then $|\mathrm{Z}(G)| = p$.

Solution. By hypothesis, $\mathrm{Z}(G)$ is contained in all maximal cyclic subgroups of G of orders $> p$ so $\mathrm{Z}(G) = \langle z \rangle$ is cyclic. Assume that $|\mathrm{Z}(G)| > p$. Then G is not of maximal class, so there is $a \in G - \mathrm{Z}(G)$ of order p (Proposition 1.3). Let $X = \langle az \rangle$; then $|X| = |\mathrm{Z}(G)| > p$. Let $X \leq Y$, where Y is a maximal cyclic subgroup of G. Since X and $\mathrm{Z}(G)$ are distinct cyclic subgroups of the same order and $\mathrm{Z}(G) \not\leq Y$, we have a contradiction.

Exercise 11. If G is a holomorph of a cyclic group L of order 8, then G contains exactly eight elements of order 4 and eight elements of order 8.

Solution. Denote by $N_k(G)$ the number of elements of order 2^k in G. Let H_1, H_2, H_3 be all members of the set Γ_1 containing L. Let $H_1 \cong \mathrm{D}_{16}$, $H_2 \cong \mathrm{SD}_{16}$ and $H_3 \cong \mathrm{M}_{16}$. Then

$$\mathrm{c}_k(G) = \sum_{i=1}^{3} \mathrm{c}_k(H_i) - 2 \cdot \mathrm{c}_k(L) = \sum_{i=1}^{3} \mathrm{c}_k(H_i) - 2.$$

We have $\mathrm{c}_2(L) = \mathrm{c}_3(L) = 1$ and

$$\mathrm{c}_2(H_1) = 1, \quad \mathrm{c}_2(H_2) = 3, \quad \mathrm{c}_2(H_3) = 2$$

so that $\mathrm{c}_2(G) = 1 + 3 + 2 - 2 = 4$. Next,

$$\mathrm{c}_3(H_1) = \mathrm{c}_3(H_2) = 1, \quad \mathrm{c}_3(H_3) = 2$$

so that $\mathrm{c}_3(G) = 1 + 1 + 2 - 2 = 2$. It follows that

$$N_2(G) = \varphi(4)\mathrm{c}_2(G) = 2 \cdot 4 = 8, \quad N_3(G) = \varphi(8)\mathrm{c}_3(G) = 4 \cdot 2 = 8,$$

where φ is Euler's totient function. Similarly, $N_1(G) = 8$ so that $\exp(G) = 8$.

Exercise 12. Let $L \cong C_{2^m}$, $m > 3$, $P = \mathrm{Aut}(L)$ and $G = \Omega_1(P) \cdot L$. Find $c_k(G)$ for all k.

Hint. If H_1, H_2, H_3 are all maximal subgroups of G containing L, then, under appropriate numbering, $H_1 \cong D_{2^{m+1}}$, $H_2 \cong SD_{2^{m+1}}$, and $H_3 \cong M_{2^{m+1}}$. Use Hall's enumeration principle as in Exercise 11. For example, if $t \in \{3, \ldots, m\}$, then we obtain that $c_t(G) = 1 + 1 + 3 - 2 \cdot 1 = 2$.

Exercise 13. Use character theory to prove Lemma 1.1.

Solution. Let A be an abelian maximal subgroup of a nonabelian p-group G. We have to prove that $|G : G'| = p|Z(G)|$. Set

$$|G| = p^m, \quad |G : G'| = p^k, \quad |Z(G)| = p^z.$$

Then $|\mathrm{Lin}(G)| = p^k$. We have to prove that $k = z + 1$. By Ito's theorem on degrees (see Introduction, Theorem 17), all nonlinear irreducible characters of G have the same degree p. Then

$$|\mathrm{Irr}(G)| = p^k + \frac{p^m - p^k}{p^2} = p^k + p^{m-2} - p^{k-2}.$$

Now we make use of the equality $|\mathrm{Irr}(G)| = k(G)$. It remains to find $k(G)$. The group G has exactly p^z central classes. Every noncentral G-class in the set $G - A$ has size $\frac{p^m}{p^{z+1}} = p^{m-z-1}$, so the set $G - A$ is the union of

$$\frac{p^m - p^{m-1}}{p^{m-z-1}} = p^{z+1} - p^z$$

G-classes. Every noncentral G-class in the set $A - Z(G)$ has size p hence this set is the union of $\frac{p^{m-1} - p^z}{p} = p^{m-2} - p^{z-1}$ G-classes. Thus

$$k(G) = p^z + p^{z+1} - p^z + p^{m-2} - p^{z-1} = p^{z+1} + p^{m-2} - p^{z-1}.$$

Therefore we get

$$p^k + p^{m-2} - p^{k-2} = p^{z+1} + p^{m-2} - p^{z-1}.$$

Thus $p^{k-2}(p^2 - 1) = p^{z-1}(p^2 - 1)$, and so $k - 2 = z - 1$ hence $k = z + 1$.

Exercise 14. Find the ranks of maximal subgroups of the holomorph of $U \cong C_8$.

Solution. We have $\mathrm{Aut}(U) \cong E_4$. Set

$$\Psi = \mathrm{Aut}(U) = \{1, \alpha, \beta, \gamma = \alpha\beta\}, \quad U = \langle u \rangle,$$

where $u^\alpha = u^{-1}$, $u^\beta = u^3$; then $u^\gamma = u^5$. It follows that

$$A = \langle U, \alpha \rangle \cong D_{16}, \quad B = \langle U, \beta \rangle \cong SD_{16}, \quad C = \langle U, \gamma \rangle \cong M_{16}.$$

By Exercise 11, we have $c_3(G) = 2$. Let $U_1 = \langle u_1 \rangle < G$ be another cyclic subgroup of order 8, $u_1 = u\gamma$. Then $U_1 \lhd G$ and

$$u_1^\alpha = u^{-1}\gamma = u_1^{-1}, \quad u_1^\beta = u_1^3, \quad u_1^\gamma = u^5,$$
$$A_1 = \langle U_1, \alpha \rangle \cong D_{16}, \quad B_1 = \langle U_1, \beta \rangle \cong SD_{16}.$$

The maximal subgroups A, B, C, A_1, B_1 are pairwise distinct and two-generator. Set $G = \Psi \cdot U$. Since

$$\bar{G} = G/\mathfrak{V}_1(U) = \bar{\Psi} \times \bar{U} \cong E_8,$$

we have $d(G) = 3$. It follows that $\Phi(G) = \mathfrak{V}_1(U)$. Set $D = \Psi \cdot \mathfrak{V}_1(U)$; then we get $d(D) = 3$ (the proof is the same as for G). It remains to find the last, seventh member, say E, of the set Γ_1. Since $c_3(G) = 2$ and all maximal subgroups of G which have exponent 8 are known, we get $\exp(E) = 4$. As $A \cong D_{16}$, it follows that $E \cap A \cong D_8$. Since E is not of maximal class (Theorem 5.6), we get $d(E) = 3$ (Theorem 12.12(a)). Thus G has exactly five two-generator members and two members of rank 3. (Since $E \cap B \cong Q_8$ and $C_E(E \cap A) = Z(E) \not\leq E \cap A$, it follows that $Z(E)$ is cyclic of order 4 and $E = (E \cap A) * Z(E)$.)

Exercise 15. Find the ranks of maximal subgroups of the holomorph G of the cyclic group $C \cong C_{2^n}$, $n > 3$.

Solution (Janko). We set $C = \langle c \rangle$, where $\mathrm{Aut}(C) = \langle a, b \rangle$ is abelian of type $(2, 2^{n-2})$ with $c^a = c^{-1}$, $c^b = c^5$ so that we may put

$$G = \langle a, b, c \mid a^2 = b^{2^{n-2}} = c^{2^n} = 1,\ [a,b] = 1,\ [a,c] = c^2,\ [c,b] = c^4 \rangle,$$

where $n > 3$, $G' = \langle c^2 \rangle$, G/G' is abelian of type $(2, 2, 2^{n-2})$ and $\Phi(G) = \langle b^2, c^2 \rangle$ so that $d(G) = 3$. We check the seven maximal subgroups H_i of G:

- $H_1 = \langle a, b \rangle \Phi(G) = \langle a, b \rangle \langle c^2 \rangle$, where $H_1' = \langle c^4 \rangle$ and therefore H_1/H_1' is abelian of type $(2, 2, 2^{n-2})$ which gives $d(H_1) = 3$.
- $H_2 = \langle a, c \rangle \Phi(G) = \langle a, c \rangle \langle b^2 \rangle$, where $H_2' = \langle c^2 \rangle$ and so H_2/H_2' is abelian of type $(2, 2, 2^{n-3})$ which gives $d(H_2) = 3$. (Note that here, in case $n = 3$, we get $d(H_2) = 2$.)
- $H_3 = \langle b, c \rangle \Phi(G) = \langle b, c \rangle$ (since $\langle b, c \rangle \geq \Phi(G)$) and so $d(H_3) = 2$.
- $H_4 = \langle ab, c \rangle \Phi(G) = \langle ab, c \rangle$ (since $\langle ab, c \rangle \geq \Phi(G)$) and so $d(H_4) = 2$.
- $H_5 = \langle a, bc \rangle \Phi(G) = \langle a, bc \rangle$ and so $d(H_5) = 2$. Indeed,

$$(bc)^2 = b(cb)c = b \cdot bc[c,b] \cdot c = b^2 c^6,$$
$$[a, bc] = [a,c][a,b]^c = [a,c] = c^2$$

and so $\langle a, bc \rangle \geq \Phi(G)$.

- $H_6 = \langle b, ac\rangle\Phi(G) = \langle b, ac\rangle\langle c^2\rangle$, where
$$(ac)^2 = 1, \quad [b, ac] = [b, c][b, c]^c = [b, c] = c^{-4}$$
and so $H_6' = \langle c^4\rangle$ so that H_6/H_6' is abelian of type $(2, 2, 2^{n-2})$ which gives that $\mathrm{d}(H_6) = 3$.
- $H_7 = \langle ab, ac\rangle\Phi(G) = \langle ab, ac\rangle$ and so $\mathrm{d}(H_7) = 2$. Indeed, $(ab)^2 = b^2$,
$$\begin{aligned}[ab, ac] &= [ab, c][ab, a]^c = [ab, c] = [a, c]^b[b, c]\\ &= (c^2)^b c^{-4} = (c^b)^2 c^{-4} = c^{10}c^{-4} = c^6\end{aligned}$$
and so $\langle ab, ac\rangle \geq \Phi(G)$.

We have proved that the minimal numbers of generators of the maximal subgroups of G are 2, 2, 2, 2, 3, 3, 3.

12^o. In this subsection we state, without proofs, some results of Mann [Man5.II].

Theorem A.40.14. *Let G be a p-group, $p > 2$, and let p^k be the maximal order of subgroups of exponent p in G. Then $|G : \mathfrak{V}_1(G)| \leq p^{k(2+\log_2 k)}$.*

Theorem A.40.15. *Let G be a p-group, $p > 2$, and let $E < G$ be maximal normal elementary abelian. If $|E| = p^r$, then $|G : \mathfrak{V}_1(G)| \leq p^{r(r+1)/2}$.*

Theorem A.40.16. *Let G be a 2-group and let $E < G$ be maximal normal elementary abelian. If $|E| = 2^s$, then $|G : \mathfrak{V}_1(G)| \leq 2^{s(3s+1)/2}$. Equality holds only if G is of maximal class $\ncong \mathrm{D}_8$.*

A p-group G is called *p-central* provided $\Omega_{\epsilon_p}(G) \leq \mathrm{Z}(G)$, where $\epsilon_2 = 2$ and $\epsilon_p = 1$ if $p > 2$.

Proposition A.40.17. *In a p-central p-group G we have $|G : \mathfrak{V}_1(G)| \leq |\Omega_1(G)|$.*

Proposition A.40.18. *If G and k are as in Theorem A.40.14 and $p = 3$, then we have $|G : \mathfrak{V}_1(G)| \leq 3^{2k}$.*

Proposition A.40.19. *If G and k are as in Theorem A.40.14, then every subgroup of G can be generated by k elements.*

Exercise 16. If, in Theorem A.40.16, $s = 2$, then $|G : \mathfrak{V}_1(G)| \leq 2^4$. (*Hint.* Use Theorem 50.3.)

13^o. In Exercises 17–24, G is a non-Dedekindian p-group all of whose nonnormal subgroups are cyclic. Such groups are classified in §16. We offer another approach which, as we hope, may simplify the classification of such groups.

Exercise 17. G has no subgroup which is isomorphic to E_{p^3}.

Solution. Assume that $\mathrm{E}_{p^3} \cong E < G$. If $X < E$ is of order p, it is contained in two distinct subgroups $U, V < E$ of order p^2. Then $U, V \lhd G$ since they are noncyclic. In this case, $X = U \cap V \lhd G$ so $X \leq \mathrm{Z}(G)$. It follows that $E \leq \mathrm{Z}(G)$. Let $C < G$

be nonnormal (cyclic); then CE/C contains a subgroup $(X/C) \times (Y/C) \cong \mathrm{E}_{p^2}$, and we get $C = X \cap Y$. In this case, $X, Y \lhd G$ since X, Y are noncyclic. Then $C \lhd G$, a final contradiction.

Exercise 18. If $p > 2$, then G is one of the following groups:

(i) G is metacyclic minimal nonabelian,

(ii) G is of maximal class and order 3^4 with $\Omega_1(G) \cong \mathrm{E}_9$,

(iii) $G = S(p^3) * C$, where C is cyclic and $S(p^3) = \Omega_1(G)$ is nonabelian of order p^3 and exponent p.

(*Hint*. Use Exercise 17, Theorem 13.7 = Theorem 69.4 and Theorem 9.6.)

In what follows we assume, in addition, that G is a 2-group. If G is of maximal class and order > 8, then $G \cong \mathrm{Q}_{16}$. Next we assume that G is not of maximal class. Then G contains a normal abelian subgroup R of type $(2, 2)$. In this case, G/R is Dedekindian, so we get $|G'| \leq 8$ (Theorem 1.20). It follows that G' is abelian (Burnside; see also Lemma 1.4). As G has no subgroup $\cong \mathrm{E}_8$, we see that G' is abelian of type $(4, 2)$ provided $|G'| = 8$.

Exercise 19. There is a G-invariant cyclic subgroup C of index ≤ 4 in G' such that G/C is non-Dedekindian.

Hint. The assertion is trivial in case that $|G'| \leq 4$ (Theorem 1.23). If G' is abelian of type $(4, 2)$, then $G/\Omega_1(G)$ is Dedekindian. As all maximal subgroups of G different from $\Omega_1(G')$ are cyclic, our claim follows from Theorem 1.23.

Since the non-Dedekindian p-groups all of whose nonnormal subgroups have order p are classified in Theorem 1.25, we may assume that the maximal order 2^ν of nonnormal cyclic subgroups of G is > 2.

Exercise 20. Let $C < G$ be a nonnormal cyclic subgroup of maximal order 2^ν. Then $|C : C_G| = 2$ and all nonnormal subgroups of G/C_G are of order 2 so that G/C_G is one of the following groups:

(i) M_{2^n},

(ii) $G/C_G = D * L$, where $D \cong \mathrm{D}_8$, L is cyclic and $|D \cap L| = 2$,

(iii) $G/C_G = \mathrm{D}_8 * \mathrm{Q}_8$ is extraspecial of order 32.

Solution. By assumption, G is not of maximal class. Then obtain that $C < K \leq G$, where $|K : C| = 2$ and K is neither of maximal class (Exercise 13.10(a)) nor cyclic. By hypothesis, $K \lhd G$ so $\Phi(K) \lhd G$ since K is noncyclic. Since $|C : \Phi(K)| = 2$, it follows that $C_G = \Phi(K)$ has index 2 in C. The assertion about the structure of G/C_G now follows from Theorem 1.25.

In what follows C is as in Exercise 20. Since $C_G = \Phi(C) \leq \Phi(G)$, it follows that $\mathrm{d}(G) = \mathrm{d}(G/C_G)$.

Exercise 21. If $G/C_G \cong \mathrm{M}_{2^n}$, then G is metacyclic.

Solution. Let $M/C_G < G/C_G$ be maximal. If M/C_G is cyclic, then M is metacyclic so $\mathrm{d}(M) = 2$. Now suppose that M/C_G is abelian of type $(2^{n-2}, 2)$. In that case, we have $C_G = \Phi(C) \leq \Phi(M)$ and hence $\mathrm{d}(M) = \mathrm{d}(M/C_G) = 2$. Thus G and all its maximal subgroups are two-generator so G is metacyclic (Corollary 36.6).

Exercise 22. Let $|C| > 2$ and $\bar{G} = G/C_G = \bar{D} * \bar{L}$, where $\bar{L}$ is cyclic and $\bar{D} \cong \mathrm{D}_8$. Let $\bar{H} = \bar{D} * \Omega_2(\bar{L})$. Then $C_G \leq \mathrm{Z}(H)$ and D is metacyclic.

Solution. The group $\bar{H}$ has exactly six nonnormal subgroups of order 2 which generate $\bar{H}$ so $C_G \leq \mathrm{Z}(H)$ since the inverse images of these six subgroups are cyclic by hypothesis. We have $C_G = \Phi(C) \leq \Phi(D)$ so $\mathrm{d}(D) = 2$. By what has just been said and the structure of $\bar{D}$, we see that all maximal subgroups of D are metacyclic so D is metacyclic (Corollary 36.6).

Exercise 23. If $V < G$ is nonnormal cyclic, then $|V : V_G| = 2$, V is maximal cyclic in G and $\mathrm{N}_G(V)/V$ is either cyclic or ordinary quaternion group.

Solution. Let $V \leq U < G$, where U is maximal cyclic. Then U is not G-invariant. Let $U < K \leq G$, where $|K : U| = 2$. Then $K \lhd G$ and so $\Phi(K) \lhd G$ is cyclic. Since $V \not\leq \Phi(K)$ and $|K : \Phi(K)| = 4$, we obtain $|V : \Phi(K)| = 2$. In particular, $V = U$ is maximal cyclic in G. Now assume that A/V is an abelian subgroup of type $(2, 2)$ in $\mathrm{N}_G(V)/V$. If S/B and T/B are two distinct subgroups of order 2 in A/V, then, being noncyclic, $S, T \lhd G$ so $V = S \cap T \lhd G$, a contradiction. Thus $\mathrm{N}_G(V)/V$ is either cyclic or generalized quaternion. Since all subgroups in $\mathrm{N}_G(V)/V$ are normal, it is isomorphic to Q_8 provided it is noncyclic.

Exercise 24. If U is a maximal (by inclusion) normal cyclic subgroup of G, then all nonnormal subgroups of G/U (if they exist) have order 2.

Solution. Assume that $T/U < G/U$ is a nonnormal subgroup of order > 2; then T is nonnormal cyclic by hypothesis. In that case, $|T : T_G| = 2$ (Exercise 23) so $U < T_G$ is characteristic hence $U \lhd G$, contrary to the hypothesis.

Exercise 25. Study the p-groups G, $p > 2$, such that $\mathrm{N}_G(C)/C$ is cyclic for all nonnormal cyclic $C < G$. (*Hint.* Prove that G has no normal subgroup $\cong \mathrm{E}_{p^3}$. Use Theorem 13.7.)

Exercise 26. All nonnormal subgroups of a minimal nonabelian p-group G are cyclic if and only if G is either metacyclic or has exponent p.

Hint. Assume that $\exp(G) > p$. The group G has no subgroup $\cong \mathrm{E}_{p^3}$ so it is metacyclic. If $H < G$ is noncyclic, then $G' < \Omega_1(G) = \Omega_1(H) \leq H$ (Lemma 65.1) so $H \lhd G$.

Exercise 27. If G is a non-Dedekindian minimal nonmetacyclic 2-group, then all nonnormal subgroups of G are cyclic. (*Hint.* See Theorems 66.1 and 69.1, where minimal nonmetacyclic p-groups are classified.)

14^o. In this subsection we present three exercises.

Exercise 28. Let $Q_{2^n} \cong Q < G$, where G is a 2-group. Then there is in G a cyclic subgroup L of order 2 or 4 such that $L \not\leq Q$ which is not normalized by Q.

Exercise 29. Let a 2-group of maximal class $M < G$ have order $2^n > 8$, where G is a 2-group, M is not a generalized quaternion group. Suppose that M normalizes any subgroup of G of order 2 not contained in M. Then M is dihedral and $G \cong SD_{2^{n+1}}$. (*Hint.* If G is not of maximal class, it contains a subgroup X of order 2 not contained in M.)

Exercise 30. Let G be a nonabelian group of exponent p. Suppose that for any $x \in G$ we have $|\langle x\rangle^G : \langle x\rangle| \leq p$. Then $Z(G) \leq G'$.

15^o. A solution of the following exercise is due to Janko.

Exercise 31. Let $n \geq 2$. Determine the automorphism group of the abelian group G of type $(2^n, 2^n)$.

Solution (Janko). Let $G = \langle a, b \mid a^{2^n} = b^{2^n} = [a, b] = 1\rangle$, $n \geq 2$, be abelian of type $(2^n, 2^n)$; then $\Phi(G) = \langle a^2\rangle \times \langle b^2\rangle$ is abelian of type $(2^{n-1}, 2^{n-1})$. Define the automorphisms σ of order 3 and τ of order 2 which act faithfully on $G/\Phi(G)$ by

$$a^\sigma = b, \quad b^\sigma = a^{-1}b^{-1}; \quad a^\tau = b, \quad b^\tau = a$$

so that

$$S = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \sigma^\tau = \sigma^{-1}\rangle \cong S_3.$$

Let A_0 be the normal subgroup of $\mathrm{Aut}(G)$ which acts trivially on $G/\Phi(G)$. Then we have $\mathrm{Aut}(G) = S \cdot A_0$, a semidirect product with kernel A_0 and complement S, and $A = \langle\tau\rangle \cdot A_0$ is a Sylow 2-subgroup of $\mathrm{Aut}(G)$. For any $\alpha \in A_0$ one has

$$(*) \qquad a^\alpha = a(a^{2i}b^{2j}) = a^{2i+1}b^{2j}, \quad b^\alpha = b(a^{2k}b^{2l}) = a^{2k}b^{2l+1},$$

and conversely, for any $i, j, k, l \pmod{2^{n-1}}$, the relations $(*)$ determine an automorphism $\alpha = \alpha(i, j, k, l)$ in A_0. It follows that $|A_0| = 2^{4(n-1)}$ and so $|A| = 2^{4n-3}$ and $|\mathrm{Aut}(G)| = 3 \cdot 2^{4n-3}$. We compute

$$a^{\tau\alpha\tau} = b^{\alpha\tau} = a^{2l+1}b^{2k}, \quad b^{\tau\alpha\tau} = a^{\alpha\tau} = a^{2j}b^{2i+1},$$

and so $(\alpha(i, j, k, l))^\tau = \alpha(l, k, j, i)$ for all $\alpha \in A_0$, which together with $(*)$ determines the structure of a Sylow 2-subgroup $A = A_0\langle\tau\rangle$ of $\mathrm{Aut}(G)$.[2]

Exercise 32. Let G be a two-generator metabelian p-group of order $> p^3$ and suppose that $H = \Omega_1(G)$ is a two-generator maximal subgroup of G. Prove that G is of maximal class.

[2] It is known that for any p-group X of rank d, $|\mathrm{Aut}(X)|$ divides the number $|\mathrm{GL}(d, p)||\Phi(X)|^d$. Thus in the case under consideration, the last number (with $d = 2$) is equal to $|\mathrm{Aut}(G)|$.

Solution. Obviously, H is nonabelian. By hypothesis, $\Phi(H) = H'$ is G-invariant of index p^2 in H so of index p^3 in G. Since $H' \le G'$, we get $|G : G'| \le p^3$. Assume that $G' < \Phi(G)$; then G/G' is abelian of type (p^2, p) since $\mathrm{d}(G/G') = \mathrm{d}(G) = 2$. As $|G'| = |H'|$, we obtain that $G' = H'$. Let $L < G'$ be G-invariant of index p. Then $H/L < G/L$ is nonabelian of order p^3. Since $\mathrm{d}(G/L) = \mathrm{d}(G) = 2$, we conclude that $\mathrm{C}_{G/L}(H/L) < H/L$, so G/L is of maximal class (Proposition 10.17) and order p^4. In this case, $|G/L : (G/L)'| = p^2$. However, since $L < G'$, we get

$$|G/L : (G/L)'| = |G/L : G'/L| = |G : G'| = p^3$$

(by assumption), contrary to the equality obtained in the previous sentence. Thus we see that $|G : G'| = p^2 = |G : \Phi(G)|$ so $G' = \Phi(G)$ is abelian, by hypothesis, and $|H : \Phi(G)| = p$. Then, by Lemma 1.1, $|\mathrm{Z}(H)| = \frac{1}{p}|H : H'| = p$ and, as we know, in this case, H is of maximal class. Now, by Theorem 12.12(a), G is of maximal class as well.

In a letter to the first author, A. Mann noticed that there is an error in statement of Corollary 7.7. Here we correct the statement and present the proof of Mann's original result.

Corollary 7.7. *Let N be a central subgroup of type (p, p) of a p-group G. If G/Z is regular for all $Z < N$ of order p, then G is also regular.*

Proof. We use induction on $|G|$. We claim that all proper sections K/L of G are regular. To this end, it suffices to show the following:

(i) All proper subgroups of G are regular.

(ii) All proper epimorphic images of G are regular.

(i) Let $K < G$. We have to prove that K is regular. Suppose that $Z < N$ of order p is not contained in K. Then we see that $K \cong KZ/Z$ is regular as a subgroup of the regular group G/Z. If $Z \le K$, then K/Z is also regular. Now let $N \le K$. Then K/Z as a subgroup of G/Z is regular for all $Z < N$ of order p so, by induction, K is regular.

(ii) We have to prove that G/U is regular for all $U < \mathrm{Z}(G)$ of order p. Since this is true for $U < N$, one may assume that $U \not\le N$; then $NU/U \cong N$. In this case, for every $Z < N$ of order p, the quotient group $G/ZU \cong (G/Z)/(ZU/Z)$ as an epimorphic image of G/Z is regular. We have $G/ZU \cong (G/U)/(ZU/U)$. Therefore, by induction, G/U is regular, and this proves (ii).

Assume, however, that G is irregular. Then G is a minimal irregular p-group, in the sense of §7. In this case, by Theorem 7.4, $\mathrm{Z}(G)$ must be cyclic, a contradiction since $\mathrm{E}_{p^2} \cong N \le \mathrm{Z}(G)$. □

In particular, if the center of a p-group G is noncyclic and all proper epimorphic images of G are regular, then G is also regular.

This result is fairly surprising in the light of Wielandt's example. In his example the irregular group G is of the form $G = A \times B$, where A and B are isomorphic metacyclic groups of order 3^5 with $|A'| = 9$. Then $G/\Omega_1(A')$ and $G/\Omega_1(B')$ are regular since $|(A/\Omega_1(A'))'| = 3$ and $|(B/\Omega_1(B'))'| = 3$ (Grün). It follows from Corollary 7.7 that there is in $N = \Omega_1(A') \times \Omega_1(B')$ a subgroup Z of order 3 such that G/Z is irregular. Note that $G/Z = (A \times B)/Z$ is the central product with amalgamated subgroup Z.

We use the opportunity and correct two misprints in Volume 1.

- In Theorem 7.1(b), instead of $|G| < p^p$ must be $|G| \leq p^p$.
- In Lemma 42.1(c), instead of $\Omega_2(G) = \langle a^{2^{m-4}}, b^4 \rangle$ must be $\Omega_2(G) = \langle a^{2^{m-4}}, b^2 \rangle$.

Exercise 33. Let $N \leq \mathrm{Z}(G)$ be an elementary abelian subgroup of order $> p$, where G is a p-group. If the quotient groups G/M are regular for all maximal subgroups M of N, then G is also regular.

Solution. By Corollary 7.7, one may assume that $|N| > p^2$. Then, if $Z < N$ is of order p, then G/Z is regular by induction. Let $K < N$ be abelian of type (p, p). Applying Corollary 7.7 to the pair $K < G$, we complete the proof.

Problem. Does there exist a positive integer k such that whenever G/Z is regular for exactly k minimal normal subgroups Z of G, then G is also regular? (In view of Wielandt's example, $k > 2$.)

Exercise 34. Let G_1 be the fundamental subgroup of a p-group G of maximal class and order $> p^{p+1}$, $p > 2$. Suppose that $K \lhd G$ of order p^p is abelian. Then all subgroups of order p^p that are not contained in G_1 are of maximal class.

Solution. Clearly, we have $K < G_1$ (Exercise 9.1(b)). Let $F < G$ be of order p^p such that $F \not\leq G_1$. Set $H = FK$. By Theorem 13.19(c), we see that H is of maximal class. If $|H| > p^{p+1}$, then $K \leq \Phi(H)$ so $F = H$, a contradiction. Thus $|H| = p^{p+1}$ and $\mathrm{cl}(H) = p$. Then, by Fitting's lemma, $\mathrm{cl}(F) = p - 1$ so F is of maximal class.

Exercise 35. Classify the nonabelian p-groups all of whose proper nonabelian three-generator subgroups are metacyclic.

Solution (Mann). If G is nonabelian minimal nonmetacyclic, then one of the following holds: (i) G is of order p^3 and exponent p, (ii) G is of maximal class and order 3^4, (iii) $G = \mathrm{D}_8 * \mathrm{C}_4$ is of order 16, (iv) $G = \mathrm{Q}_8 \times \mathrm{C}_2$, (v) G is the special group of order 2^5 with $|G'| = 4$ (Theorems 66.1 and 69.1). Since all these G are generated by three elements, it follows that G has no proper nonabelian minimal nonmetacyclic subgroups. If $X < G$ is nonabelian and has the minimal number $d \geq 3$ generators, then we can find three among these generators which generate a nonabelian subgroup, therefore that subgroup is metacyclic and has two generators, and thus X has $< d$ generators, a contradiction. Thus every proper nonabelian subgroup of G is two-generator and since it is also three-generator, it is metacyclic by hypothesis. If all maximal subgroups of G are nonabelian, they are metacyclic; then G is either metacyclic or minimal non-

metacyclic. It remains to consider the case when G contains a nonmetacyclic abelian maximal subgroup, say A. One may assume that G is not minimal nonabelian. Then all nonabelian maximal subgroups are metacyclic so, considering their intersections with A, we get $E = \Omega_1(A) \cong E_{p^3}$. In this case, if B/E is maximal in G/E, then B is abelian since it is nonmetacyclic. If $B \neq A$, then $Z(G) = A \cap B$ has index p^2 in G. If A is the unique abelian subgroup of index p in G, then either G is a group from §87 or G/E is cyclic. In the second case, G has a cyclic subgroup of index p^2 (such groups are classified in §89).

Exercise 36. Classify the abelian p-groups G of exponent $> p$ all of whose maximal subgroups are isomorphic.

Solution (Mann). If G is not homocyclic, let $\exp(G) = p^e$ (then $e > 1$) and assume that in the direct decomposition of G as a direct product of cyclic subgroups there are exactly k factors of order p^e. Then G contains a maximal subgroup, say A, with k factors of order p^e in its decomposition, and another one, say B, with only $k-1$ such factors. Then $A \ncong B$. Thus, if G is an abelian p-group with all maximal subgroups isomorphic, it is homocyclic. Conversely, if G is homocyclic, then all its maximal subgroups are isomorphic.

Exercise 37. Suppose that a p-group G, $p > 2$, contains a subgroup of order p^p and exponent p. Study the structure of G if all its subgroups of order p^p and exponent p are of maximal class.

Solution. Let $R \lhd G$ be abelian of type (p, p) and let $H \leq C_G(R)$ be maximal in G and such that $R < H$. Assume that there is $U \leq H$ of order p^p and exponent p. Since $\exp(RU) = p$ (Theorem 7.1(b)), it follows that $V \leq RU$ of order p^p such that $R < V$ is not of maximal class. Therefore U does not exist. By Theorem 12.1(a), H is absolutely regular (H is not of maximal class since $R \leq Z(H)$ is of order p^2). In this case, by Theorem 12.1(b), either G is of maximal class or $G = H\Omega_1(G)$, where $\Omega_1(G)$ is of maximal class and order p^p since $\exp(\Omega_1(G)) = p$.

Exercise 38. Suppose that a p-group G of order $> p^{p+1}$, $p > 2$, contains a normal subgroup of order p^p and exponent p. Study the structure of G if all its normal subgroups of order p^p and exponent p are of maximal class.

Solution. Let $R \lhd G$ be of maximal class and of order p^p and exponent p. Let $L < R$ be G-invariant of order p^2. Then we have $G = RC_G(L)$. In that case, $C_G(L) \in \Gamma_1$ has no G-invariant subgroup of order p^p and exponent p (otherwise, $C_G(L)$ contains a G-invariant subgroup S of order p^p and exponent p with $R < S$). It follows from Theorem 12.1(b) that C is absolutely regular and $R = \Omega_1(G)$.

Exercise 39. If the derived subgroup of a p-group G of class 2 is elementary abelian, then $\Phi(G) \leq Z(G)$.

Hint. We have $\Phi(G) = G'\mho_1(G)$ and $G' \leq Z(G)$. If $x, y \in G$, then $1 = [x, y]^p = [x, y^p]$ so $y^p \in Z(G)$. Thus $\mho_1(G) \leq Z(G)$ and so $\Phi(G) \leq Z(G)$.

Exercise 40. Prove that if a p-group G of order $> p^{p+1}$, $p > 5$, has no normal subgroup isomorphic to E_{p^4}, it is absolutely regular.

Solution. Assume that G has no normal subgroup of order p^7 and exponent p. Then it is either absolutely regular or an irregular 7-group of maximal class (Theorem 12.1(b)). Let G be an irregular 7-group of maximal class. Then it contains a normal subgroup $R = \Omega_1(\Phi(G))$ of order 7^6 and exponent 7. By Theorems 13.7 and 10.4, R contains a G-invariant subgroup $E \cong \mathrm{E}_{7^3}$. In view of Theorem 10.1, $\mathrm{C}_R(E) = E$ so that $\mathrm{Z}(R)$ is of order 7. As we know, every G-invariant subgroup of $\Phi(G)$ of order p^2 is contained in $\mathrm{Z}(\Phi(G))$. Let $U < R$ be a G-invariant subgroup of order 7^2. Then $U \leq \mathrm{Z}(R)$, contrary to what has just been proved. Thus G is absolutely regular.

Exercise 41. If G is a nonabelian p-group such that $|G : G'| = p^2$ and any nonabelian epimorphic image of G has cyclic center, then G is of maximal class.

Solution. Assume that G is not of maximal class. Then $|G| > p^3$ and $p > 2$ (Taussky). By hypothesis, $\mathrm{Z}(G)$ is cyclic. We proceed by induction on $|G|$. Let $K \leq \mathrm{Z}(G)$ be of order p. Then G/K is nonabelian since $|G/K| > p^2 = |G/G'|$ and, by induction, it is of maximal class. Since G is a counterexample, $|\mathrm{Z}(G)| > p$. By Lemma 1.4, there is in G a normal subgroup R of type (p, p). We have $R \cap \mathrm{Z}(G) = K$. Let $L \leq \mathrm{Z}(G)$ be of order p^2. Then $LR/K \cong \mathrm{E}_{p^2}$ is a central subgroup of G/K, and this is a contradiction.

Exercise 42. Suppose that a p-group G, $p > 2$, possesses an abelian subgroup U of exponent $p^e \geq p$ and index p^2. Then G contains a normal abelian subgroup A of index p^2 and exponent $\geq p^{e-1}$.

Solution. One may assume that U is not G-invariant. Let $U < H < G$; then $H \in \Gamma_1$. The number of G-conjugates of U is divisible by p. If $U_1 \neq U$ is a G-conjugate of U, then $H = UU_1$ is of class at most 2 since $U_1 \lhd H$ (Fitting's lemma). Since $p > 2$, H is regular so $\exp(H) = p^e$. One may assume that H is nonabelian (otherwise, the result is obvious). Then H has exactly $p + 1$ abelian subgroups of index p (Exercise 1.6(a)), and one of them, say A, satisfies $A \lhd G$. Clearly, $\exp(A) \geq \frac{1}{p}\exp(H) = p^{e-1}$.

Exercise 43 (Mann; see his commentary to Problem 115). Let $p > 2$ and let G be a nonabelian p-group of exponent $> p$. Suppose that all minimal nonabelian subgroups of G have exponent p. Prove that $\mathrm{H}_p(G)$ is maximal abelian and $\mathrm{Z}_2(G) \leq \mathrm{H}_p(G)$, $\exp(\mathrm{Z}_2(G)) = p$. (In fact, Mann has shown that $\mathrm{H}_p(G)$ has index p in G.)

Solution. All minimal nonabelian subgroups of G have order p^3 (Lemma 65.1). Let A be a maximal G-invariant abelian subgroup of G. By Lemma 57.1, for every $z \in G - A$ there is $a \in A$ such that $\langle z, a\rangle$ is minimal nonabelian so of exponent p. It follows that all elements of the set $G - A$ have order p so $\mathrm{H}_p(G) \leq A$. Since A is generated by elements of order $> p$, we obtain that $\mathrm{H}_p(G) = A$. Let $x \in A$ be of order $> p$ and $y \in \mathrm{Z}_2(G) - \mathrm{Z}(G)$. Then $\mathrm{cl}(\langle x, y\rangle) \leq 2$ (indeed, $[x, y] \in \mathrm{Z}(G)$) so $B = \langle x, y\rangle$ is

regular since $p > 2$. Assume that B is nonabelian. Since B is generated by minimal nonabelian subgroups, we get $\exp(B) = p$, a contradiction since $o(x) > p$. Thus B is abelian. Since $A = \langle A - \Omega_1(A)\rangle$, it follows that A centralizes $\mathrm{Z}_2(G)$, and we conclude that $\mathrm{Z}_2(G) \leq A$. It remains to show that $\exp(\mathrm{Z}_2(G)) = p$. Assume that there exists $u \in \mathrm{Z}_2(G) - \mathrm{Z}(G)$ of order $> p$. Take $v \in G - A$ and set $L = \langle u, v\rangle$. Then we get $L = \langle L - A\rangle$ so $\exp(L) = p$ since $\Omega_1(L) = L$ (all elements in $G - A$ have order p by the above), $\mathrm{cl}(L) \leq 2$ and $p > 2$, and this is a contradiction. Thus all elements of $\mathrm{Z}_2(G) - \mathrm{Z}(G)$ have order p hence $\exp(\mathrm{Z}_2(G)) = p$ since $\langle \mathrm{Z}_2(G) - \mathrm{Z}(G)\rangle = \mathrm{Z}_2(G)$ and $\mathrm{Z}_2(G) < A$.

Exercise 44. Classify the abelian p-groups G of exponent $> p$ such that $\mathrm{Aut}(G)$ acts transitively on the set Γ_1.

Solution. By hypothesis, all members of the set Γ_1 are isomorphic so G is homocyclic by Exercise 36. Conversely, if G is homocyclic, then $\mathrm{Aut}(G)$ is transitive on Γ_1 (even on Γ_i, $i \leq \mathrm{d}(G)$).

Exercise 45. Prove that if G is extraspecial of order p^{1+2m}, then all its maximal subgroups have centers of order p^2.

Solution. One may assume that $m > 1$. Let $M \in \Gamma_1$. Then $|M/M'| = p^{2m-1}$ so M is not extraspecial since $2m - 1$ is odd. It follows that $|\mathrm{Z}(M)| > p$. Assume that $|\mathrm{Z}(M)| > p^2$. If $\phi \in \mathrm{Irr}(M)$, then $\phi(1)^2 \leq |M/\mathrm{Z}(M)| \leq p^{2m-3}$ so $\phi(1) \leq p^{m-2}$. However, there is $\chi \in \mathrm{Irr}(G)$ of degree p^m, therefore, by Clifford theory, there is in $\mathrm{Irr}(M)$ a character of degree $\geq p^{m-1}$, and this is a contradiction. Thus $\mathrm{Z}(M)$ has order p^2. (Clearly, if $M, N \in \Gamma_1$ are different, then $\mathrm{Z}(M) \neq \mathrm{Z}(N)$.)

Exercise 46. Let a p-group G of maximal class contain a subgroup of order p^p and exponent p. Then all subgroups of G of exponent p maximal by inclusion have order p^p.

Solution. One may assume that $\exp(G) > p$; then G is irregular (Theorem 9.5). Let $E < G$ be maximal (by inclusion) of exponent p. Assume that $|E| < p^p$. If $E \lhd G$ and $x \in G - E$, then $\langle x, E\rangle$ is of exponent p (Theorems 7.1 and 7.2), contrary to the choice of E. Thus E is not G-invariant. If $\Omega_1(\Phi(G)) < E$, then $|E| = p^p$ since, by Theorems 9.5 and 9.6, we have $|\Omega_1(\Phi(G))| = p^{p-1}$ (consider $E \cap G_1$). Let $R < \Omega_1(\Phi(G))$ be G-invariant of minimal order not contained in E. Then we get $\Omega_1(RE) = RE$ and $|RE| = p|E| \leq p^p$, so $\exp(RE) = p$ (Theorems 7.1 and 7.2), contrary to the choice of E. Thus $|E| \geq p^p$. As we know (see Theorems 9.5 and 9.6), $|E| \leq p^p$.

Exercise 47. Suppose that G is a p-group of maximal class and order p^{p+1} and there is $a \in G$ of order p such that $\mathrm{C}_G(a)$ is of order p^2. If ϕ is a lattice isomorphism of G and a p-group G_0, then G_0 is of maximal class.

Solution. By Theorem 9.5, G is irregular. It suffices to show that G_0 is also irregular: then G_0 is of maximal class. Assume, by way of contradiction, that G_0 is regular. Then

$$|\Omega_1(G)| = |\Omega_1(G_0)| = |G_0/\mathfrak{V}_1(G_0)| = |G/\mathfrak{V}_1(G) = p^p.$$

By hypothesis, we get $C_G(a) \cong E_{p^2}$. It follows that $C_G(a) < \Omega_1(G)$ since $a \in \Omega_1(G)$ so $\Omega_1(G)$ is of maximal class (Proposition 1.8). However, $\Omega_1(G_0) = \Omega_1(G)^\phi$ so that $\Omega_1(G_0)$ is of maximal class (Proposition 25.8(b)). We have $d(G_0) = d(G) = 2$ and $|G_0 : \Omega_1(G_0)| = p$. It follows from Theorem 12.12(a) that G_0 is of maximal class.

Exercise 48. Let G be a p-group of maximal class, $p > 2$. Then there are $x, y \in G$ of equal order $\leq p^2$ such that $G = \langle x, y \rangle$.

Solution. We proceed by induction on $|G|$. If $\Omega_i^*(G) = G$, $i \in \{1, 2\}$, the result holds since, in the case under consideration, G is generated by elements of order p^i and satisfies $d(G) = 2$. Now let $\Omega_i(G) < G$ for $i = 1, 2$. By Theorem 13.19, $\Omega_2(G) = G$. Since all elements in $G - G_1$, where G_1 is the fundamental subgroup of G, have orders $\leq p^2$, we get $|\Omega_1(G)| > p^{p-1}$. Set $\Omega_i^*(G) = H_i$, $i = 1, 2$. If $H_2 \leq G_1$, then, by Theorem 13.19, $H_1 \geq \langle G - G_1 \rangle = G$, contrary to what has been said in the first sentence of the solution. Thus we have $H_1, H_2 \in \Gamma_1$. Let $H_3 \in \Gamma_1 - \{G_1, H_1, G_2\}$. If $|H_3| > p^{p+1}$, then $\Omega_i^*(H_3) = H_3$ for some $i \leq 2$ by induction. Since $H_3 \neq H_i$, we get a contradiction. Thus $|H_3| = p^{p+1}$; then $|G| = p^{p+2}$. Again, as we know (see Theorem 9.5), $\Omega_i^*(H_3) = H_3$ for some $i \leq 2$, and we get again a contradiction.

The result of Exercise 48 is not true for $p = 2$ as the semidihedral group $G = SD_{2^m}$ shows.

Exercise 49. Let $p > 2$. If G is a metacyclic p-group of exponent p^e, then we have $\mho_{e-1}(G) \leq Z(G)$.

Solution. One may assume that $e > 1$. Since G is regular and $G' \leq \Phi(G) = \mho_1(G)$, it follows that $\exp(G') \leq p^{e-1}$ (Theorem 7.2(b)). By Theorem 7.2(f) with $M = N = G$, $r = e - 1$ and $s = 0$, we have

$$[\mho_{e-1}(G), G] = \mho_{e-1}([G, G]) = \mho_{e-1}(G') = \{1\},$$

and we are done.

Exercise 50. Let G be a regular p-group of exponent p^e such that $\exp(G') = p^k < p^e$. Prove that $\mho_k(G) \leq Z(G)$. (*Hint.* Using Theorem 7.2(f) with $M = N = G$, $r = k$ and $s = 0$, we get $[G, \mho_k(G)] = \mho_k(G') = \{1\}$.)

16^o. Below we find the numbers $s_2(G)$ and $s_3(G)$ of subgroups of order 4 and 8, respectively, in a metacyclic 2-group G of order $2^m > 2^3$. (For a more detailed investigation, see §124.)

16.1. First we find $s_2(G)$. Assume that G is noncyclic.

Case 1. Let G be of maximal class. If $H < G$ is of order 4, then we get $Z(G) < H$ so $s_2(G)$ is equal to the number $s_1(G/Z(G))$. Since $G/Z(G)$ is dihedral of order 2^{m-1}, we obtain $s_2(G) = 2^{m-2} + 1$.

Next we assume that G is not of maximal class. Then $R = \Omega_1(G) \cong E_4$. In this case, R is the unique noncyclic subgroup of G of order 4, and so it suffices to find the

number $c_2(G)$ of cyclic subgroups of G of order 4. The group G has no nonabelian subgroups of order 8 (Proposition 10.19). Therefore, if $H < G$ is cyclic of order 4, then HR is abelian of type $(4, 2)$ so it contains exactly two cyclic subgroups of order 4.

Case 2. Suppose that G/R is not of maximal class. Then, since $|\Omega_2(R)| \in \{8, 16\}$, we get

$$c_2(G) = \frac{|\Omega_2(G)| - |R|}{2(2-1)} \in \{2, 6\}$$

so that $s_2(G) = 1 + c_2(G) \in \{3, 7\}$.

Case 3. Suppose that G/R is of maximal class. Then

$$s_1(G/R) \in \{1, 1 + 2^{m-3}, 1 + 2^{m-4}\},$$

and we get

$$s_2(G) = 1 + 2s_1(G/R) \in \{3, 3 + 2^{m-2}, 3 + 2^{m-3}\}.$$

16.2. Here we find the number $s_3(G)$. One may assume that $m > 4$ (if $m = 4$, then $s_3(G) = 3$ since $d(G) = 2$).

Case 1. Suppose that G is of maximal class. Then $s_3(G) = 1 + 2^{m-3}$.

Case 2. Suppose that G/R is not of maximal class. If G/R is cyclic, then $s_3(G) = 3$ since G has a cyclic subgroup of index 2 and $cl(G) \leq 2$. Now assume that G/R is neither cyclic nor of maximal class. Then $F/R = \Omega_1(G/R) \cong E_4$. We have $s_3(F) = 3$. If H is noncyclic of order 8, then $R < H < F$ so G contains exactly three noncyclic subgroups of order 8. Thus it remains to find $c_3(G)$. In case that $L/F \leq G/F$ is of order 2, we conclude that $c_3(L) = \frac{|L-F|}{4} = 4$. Therefore $c_3(G) = 4c_1(G/F)$.

Case 3. Suppose that G/R is of maximal class. If $H < G$ of order 8 is noncyclic, then the number of such H is equal to $c_1(G/R) \in \{1, 2^{m-3} + 1, 2^{m-4} + 1\}$. It remains to find $c_3(G)$. If $H < G$ is cyclic of order 8, then HR/R is cyclic of order 4. In case that $L/R < G/R$ is cyclic of order 4, we get $c_3(L) = 2$ since L has a cyclic subgroup of index 2 and class ≤ 2. Therefore

$$c_3(G) = 2c_2(G/R) \in \{2, 2(2^{m-4} + 1), 2(2^{m-5} + 1)\}.$$

We have $s_3(G) = s_1(G/R) + 2c_2(G/R)$.

17^o. In this subsection we compute $s_n(G) \pmod{p^3}$ for a noncyclic metacyclic p-group G of order p^m, $p > 2$, $n < m - 1$. Note that the number $c_n(G)$ of cyclic subgroups of order p^n in G is equal to

$$c_n(G) = \frac{|\Omega_n(G)| - |\Omega_{n-1}(G)|}{p^{n-1}(p-1)} \tag{3}$$

since G is regular, in view of $p > 2$.

If $n = 1$, then $s_1(G) = 1 + p$. In what follows we assume that $n > 1$.

If $n = 2$, then $\Omega_1(G) \cong \mathrm{E}_{p^2}$ is the unique noncyclic subgroup of G of order p^2 so that

$$\mathrm{s}_2(G) = 1 + \mathrm{c}_2(G) = 1 + \frac{|\Omega_2(G)| - |\Omega_1(G)|}{p(p-1)}$$

thus

$$\mathrm{s}_2(G) \in \left\{1 + \frac{p^3 - p^2}{p(p-1)}, 1 + \frac{p^4 - p^2}{p(p-1)}\right\} = \{1 + p, 1 + p + p^2\}.$$

Next we assume that $n > 2$. In view of formula (3), it suffices to find the number $\nu_n(G)$ of noncyclic subgroups of order p^n in G. All noncyclic subgroups of G contain $\Omega_1(G)$ so that $\nu_n(G) = \mathrm{s}_{n-2}(G/\Omega_1(G))$. Since

$$\mathrm{s}_n(G) = \mathrm{c}_n(G) + \mathrm{s}_{n-2}(G/\Omega_1(G)), \tag{4}$$

it suffices to find both summands in the right-hand side of (4).

(i) If G has a cyclic subgroup of index p, then $\mathrm{s}_n(G) = 1 + p$, so in what follows we assume that G has no cyclic subgroup of index p.

(ii) Suppose that G has a cyclic subgroup of index p^2. In that case, $|\Omega_n(G)| = p^{n+2}$ and $|\Omega_{n-1}(G)| = p^{n+1}$. Therefore, in view of (3), (i) and (4), we have

$$\mathrm{c}_n(G) = \frac{p^{n+2} - p^{n+1}}{p^{n-1}(p-1)} = p^2, \quad \mathrm{s}_{n-2}(G/\Omega_1(G)) = p + 1$$

(the second equality is due to the fact that the noncyclic quotient group $G/\Omega_1(G)$ has a cyclic subgroup of index p; see Theorem 1.2) so that $\mathrm{s}_n(G) = p^2 + p + 1$.

Next we assume that G has no cyclic subgroup of index p^2. Then $|\Omega_n(G)| \geq p^{n+3}$.

(iii) Suppose that $n = 3$. Then $|\Omega_3(G)| = p^6$ and $|\Omega_2(G)| = p^4$ whence

$$\mathrm{c}_3(G) = \frac{p^6 - p^4}{p^2(p-1)} = p^2(p+1), \quad \mathrm{s}_3(G) = s_1(G/\Omega_1(G)) = p + 1$$

so that $\mathrm{s}_3(G) = (p^3 + p^2) + (p + 1) \equiv p^2 + p + 1 \pmod{p^3}$ by (4).

In what follows we assume that $n > 3$. It follows from (3) and $|\Omega_{n-1}(G)| \geq p^{n+2}$ that $\mathrm{c}_n(G) \equiv 0 \pmod{p^3}$. Therefore $\mathrm{s}_n(G) \equiv \mathrm{s}_{n-2}(G/\Omega_1(G)) \pmod{p^3}$.

Next we use induction on $|G|$ and n ($n > 1$) assuming that if G has no cyclic subgroup of index p, then we have $\mathrm{s}_n(G) \equiv 1 + p + p^2 \pmod{p^3}$. For $n = 2$ and $n = 3$ our assertion is true; therefore one may assume that $n > 3$. By the above, one can also assume that our group G has no cyclic subgroup of index p^2. Since $n-2 > 1$, $\mathrm{s}_n(G) \equiv \mathrm{s}_{n-2}(G/\Omega_{n-2}(G)) \pmod{p^3}$ and $G/\Omega_{n-1}(G)$ has no cyclic subgroup of index p, we can finally conclude that $\mathrm{s}_{n-2}(G/\Omega_{n-2}(G)) \equiv 1 + p + p^2 \pmod{p^3}$ so that $\mathrm{s}_n(G) \equiv 1 + p + p^2 \pmod{p^3}$.

Thus we have proved the following

Theorem A.40.20. *Let $p > 2$ and $1 < n < m-1$. Suppose that G is a noncyclic metacyclic p-group of order p^m. Then $\mathrm{s}_n(G) \equiv 1+p+p^2$ unless G has a cyclic subgroup of index p in which case $\mathrm{s}_n(G) = 1 + p$.*

Ideas of this and the previous subsection are developed in §124 (see there the proof of Mann's theorem, which was proved before writing this subsection; however, Mann's proof is based on entirely other ideas).

18^o. In this subsection we will find $\mathrm{s}_n(G) \pmod{p^3}$, where G is an extraspecial group of order p^{1+2m}, $p > 2$ and $n < 2m-1$. One may assume that $m > 1$. We have $|G : \Omega_1(G)| = |G : \mho_1(G)| \le p$ with equality if and only if $\exp(G) = p^2$. Indeed, since $\mathrm{cl}(G) = 2$ and $p > 2$, G is regular (see Theorem 7.2(b)).

If $\exp(G) = p$, then we have $\mathrm{s}_1(G) = 1 + p + \cdots + p^{m-1}$ and if $n > 1$, then we get $\mathrm{s}_n(G) \equiv 1 + p + 2p^2 \pmod{p^3}$ (Theorem 5.9).

In what follows we assume that $\exp(G) = p^2$; then $|G : \Omega_1(G)| = p$. By Theorem 5.9, we have $\mathrm{s}_n(\Omega_1(G)) \equiv 1 + p + 2p^2 \pmod{p^3}$ unless $n = 2m-1$ in which case $\mathrm{s}_n(\Omega_1(G)) \equiv 1+p+p^2 \pmod{p^3}$. Therefore we have to find in G the number of subgroups of order p^n and exponent p^2.

Let $\mathcal{M}_n(G) = \{H_1, \ldots, H_k\}$ denote the set of all subgroups of order p^n and exponent p^2 in G and let $\mathcal{C} = \{Z_1, \ldots, Z_t\}$ be the set of all cyclic subgroups of order p^2 in G. Note that all $Z_i (> G')$ are G-invariant. We have

$$\mathrm{s}_n(G) = \mathrm{s}_n(\Omega_1(G)) + k \equiv 1 + p + p^2 + k \pmod{p^3} \quad (n = 2m-1), \tag{5}$$

$$\mathrm{s}_n(G) = \mathrm{s}_n(\Omega_1(G)) + k \equiv 1 + p + 2p^2 + k \pmod{p^3} \quad (n < 2m-1), \tag{6}$$

so it remains to find $k \pmod{p^3}$. We compute

$$t = \mathrm{c}_2(G) = \frac{p^{2m+1} - p^{2m}}{p(p-1)} = p^{2m-1}, \quad \mathrm{c}_2(H_i) = \frac{p^n - p^{n-1}}{p(p-1)} = p^{n-2}.$$

One may assume that $n > 2$ (otherwise, $\mathrm{c}_k(G) = t$).

There are exactly $\mathrm{s}_{n-2}(G/Z_i)$ members of the set $\mathcal{M}_n(G)$ containing Z_i, where $i = 1, \ldots, t$. Therefore, by double counting of the pairs $Z_i < H_j$, we get

$$t\,\mathrm{s}_{n-2}(G/Z_i) = kp^{n-2},$$

i.e.,

$$p^{2m-1}\varphi_{2m-1,n-2} = kp^{n-2}, \tag{7}$$

where $\varphi_{u,v} = \mathrm{s}_v(\mathrm{E}_{p^u})$. It follows from (7) that $k = p^{2m-n+1}\varphi_{2m-1,n-2}$. Therefore, if $n < 2m-1$, then $k \equiv 0 \pmod{p^3}$ so that $\mathrm{s}_n(G) \equiv 1 + p + 2p^2 \pmod{p^3}$ by (6).

Now let $n = 2m-1$. In this case, $k = p^2\varphi_{n,n-2}$ (see (7)). Since, by Kulakoff's theorem (see Theorem 5.3),

$$\varphi_{n,n-2} = s_{n-2}(E_{p^{n-2}}) \equiv 1 + p + sp^2 \quad (s \geq 0),$$

it follows that $k \equiv p^2 \pmod{p^3}$. Then, by (5),

$$s_n(G) \equiv 1 + p + p^2 + p^2 \equiv 1 + p + 2p^2 \pmod{p^3}.$$

Thus we have proved the following result.

Theorem A.40.21. *Let $p > 2$ and $1 < n < 2m$, and let G be an extraspecial group of order p^{2m+1}. Then $s_n(G) \equiv 1 + p + 2p^2 \pmod{p^3}$.*

19^o. Recall that a 2-group G is said to be a U_2-*group* if it satisfies the following properties:

($U_2 1$) There is in G a normal subgroup $R \cong E_4$ such that G/R is of maximal class.

($U_2 2$) If T/R is cyclic of index 2 in G/R, then $\Omega_1(T) = R$.

Note that T has a cyclic subgroup of index 2 and satisfies $\mathrm{cl}(T) \leq 2$ so that either T is noncyclic abelian with cyclic subgroup of index 2 or $T \cong M_{2^k}$ for some $k > 3$. If $G/R \ncong Q_8$, the subgroup T is determined uniquely.

U_2-groups were classified in §66. Below we do not use this classification and present simple proofs of some properties of U_2-groups.

($U_2 3$) R is a unique normal four-subgroup of G. Indeed, assume that R_1 is another normal four-subgroup of G. Let $L/R = Z(G/R)$; then we obtain that $|L| = 8$ so $L = RR_1 = \Omega_1(L)$ by the modular law. Since G/R is of maximal class, we get $L < T$, a contradiction.

($U_2 4$) The subgroup G' is cyclic and $|G : G'| = 8$. By Taussky's theorem, we have $|G : G'| > 4$ so that $R \not\leq G'$. Since $G' < T$, the subgroup G' is cyclic. Then $|G : G'| = |G : G'R||G'R : G'| = 4 \cdot 2 = 8$.

($U_2 5$) Suppose that A, denoting a maximal abelian normal subgroup of G, is cyclic. Since $G/A = G/C_G(A)$ is abelian, it follows that $G' \leq A$. As G/R is of maximal class, we obtain $RA = T$ so that T is nonabelian. Since R centralizes G', it follows that $G' < A$, and we conclude that $|G : A| = 4$.

($U_2 6$) Let A, denoting a maximal abelian normal subgroup of G, be noncyclic. Then $R < A$ by ($U_2 3$). It follows that $A \leq T$, and we conclude that $|G : A| \leq 4$.

($U_2 7$) We have $R \not\leq \Phi(G)$ if and only if $d(G) = 3$ and the set Γ_1 contains exactly four members of maximal class, $G' = \Phi(G)$. It suffices to prove only that the set Γ_1 contains a member of maximal class (Theorems 5.4 and 12.12(a)). Let $R \not\leq M \in \Gamma_1$. Then M has no G-invariant four-subgroup by ($U_2 3$), so M is of maximal class since it is noncyclic (Lemma 1.4).

20^o. We prove the following theorem:

Theorem A.40.22. *Let G be a non-Dedekindian 2-group. Suppose that every nonnormal subgroup of G is either cyclic or generalized quaternion. Then one of the following holds:*

(a) *Either $G \cong \mathrm{D}_8$ or G is a generalized quaternion group of order > 8.*

(b) *$G = D * C$, where $D \cong \mathrm{D}_8$ and $C = \mathrm{Z}(G)$ is cyclic.*

(c) *$G = D * Q$ is extraspecial of order 2^5, where $D \cong \mathrm{D}_8$ and $Q \cong \mathrm{Q}_8$.*

(d) *$\Omega_1(G) \cong \mathrm{E}_4$.*

Proof. If G is of maximal class, it is as in (a). Next assume that G is not of maximal class. Then there is $\mathrm{E}_4 \cong R \lhd G$. In this case, G/R is Dedekindian. Otherwise, G/R contains a nonnormal cyclic subgroup L/R. Since L is neither cyclic nor generalized quaternion, we get a contradiction.

(i) G has no subgroup of maximal class and order > 8. Assume that this is false and $K < G$ is of maximal class and order > 8. Then $R \not\leq K$ and the nonabelian subgroup $KR/R \leq G/R$ is not isomorphic to Q_8 so G/R is not Dedekindian (Theorem 1.20), a contradiction.

(ii) G has no subgroup isomorphic to E_8. Assume that this is false and G contains a subgroup $E \cong \mathrm{E}_8$. Then all maximal subgroups of E are noncyclic so G-invariant. If $L < E$ is of order 2, then L is contained in two distinct maximal subgroups U and V of E, and we get $L = U \cap V \leq \mathrm{Z}(G)$, and so $E \leq \mathrm{Z}(G)$. Let $C < G$ be nonnormal cyclic. Then $CE \geq C \times L_1 \times L_2$, where $|L_1| = 2 = |L_2|$. Since $C \times L_i$, $i = 1, 2$, are G-invariant, it follows that $(C \times L_1) \cap (C \times L_2) = C \lhd G$, contrary to the choice of C.

(iii) Suppose that $|\Omega_1(G)| > 4$. Then, in view of (ii), there are in G two noncommuting involutions u, v so that $D = \langle u, v\rangle \cong \mathrm{D}_8$ by (i). By hypothesis, we get $D \lhd G$. The involutions u, v are contained in two distinct maximal subgroups A, B of D, respectively. Since A, B are G-invariant, we obtain $|G : \mathrm{C}_G(u)| = 2 = |G : \mathrm{C}_G(v)|$, so that $\mathrm{C}_G(D) = \mathrm{C}_G(u) \cap \mathrm{C}_G(v)$ has index 4 in G since $\mathrm{C}_G(u) \neq \mathrm{C}_G(v)$. Because $D \cap \mathrm{C}_G(D) = \mathrm{Z}(D)$ is of index 4 in D, we get $G = D * \mathrm{C}_G(D)$ by the product formula. By (ii), $\mathrm{C}_G(D)$ has only one involution so that $\mathrm{C}_G(D)$ is either cyclic or generalized quaternion. In the second case, $\mathrm{C}_G(D) \cong \mathrm{Q}_8$ by (i), and then $G \cong \mathrm{D}_8 * \mathrm{Q}_8$ is extraspecial of order 32, the group from (e). In the first case, G is a group from (b). □

Thus it remains to classify the groups from part (d). For information on such groups, see §82. Note that, in the case under consideration, $G/\Omega_1(G)$ is Dedekindian and we have $\mathrm{d}(G) \leq 4$ (Theorem 50.3). Note that the group of order 2^5 from Lemma 42.1(c) satisfies the hypothesis of the theorem. Suppose that a metacyclic group G is a group from Theorem A.40.22(d). Then all nonnormal subgroups of such a group G are cyclic (Proposition 10.19). In this case, $G/\Omega_1(G)$ is either abelian or isomorphic to Q_8. In the first case, $|G'| = 2$ so G is minimal nonabelian (Lemma 65.2(a)); such G satisfies

the hypothesis. In the second case, we get $|\Omega_2(G)| = 8$ so G is the group of order 2^5 from Lemma 42.1(c).

21^o. Let G be a p-group and $H \leq G$. Set

$$|G : \mathrm{N}_G(H)| = p^{\mathrm{sb}(H)} \quad \text{and} \quad \mathrm{sb}(G) = \max\{\mathrm{sb}(H) \mid H \leq G\}.$$

The number $\mathrm{sb}(G)$ is said to be the *subgroup breadth* of G. In this subsection we compute $\mathrm{sb}(G)$, where G is an extraspecial group of order p^{1+2m}.

Suppose that G is a nonabelian p-group such that G' is its unique minimal normal subgroup. Then $\mathrm{Z}(G)$ is cyclic. We claim that $\Phi(G) \leq \mathrm{Z}(G)$. Indeed, for all $x, y \in G$ we have $1 = [x, y]^p = [x, y^p]$ so that $\Phi(G) = G'\mho_1(G) \leq \mathrm{Z}(G)$. Such a G is called an *$\mathcal{E}_p$-group*.

Lemma A.40.23. *If G is an $\mathcal{E}_p$-group and $H < G$ of order p^h is nonnormal, then the following hold:*

(a) *H is elementary abelian.*

(b) *The subgroups $\mathrm{N}_G(H)$ and $\mathrm{C}_G(H)$ coincide.*

(c) *$|G : \mathrm{N}_G(H)| \leq p^h$, i.e., $\mathrm{sb}(H) \leq h$.*

Proof. Since $|G'| = p$ and $\Phi(G)$ is cyclic, we get $H \cap \Phi(G) = \{1\}$ so H is isomorphic to a subgroup of the elementary abelian group $G/\Phi(G)$, and this proves (a).

Assume that $x \in \mathrm{N}_G(H) - \mathrm{C}_G(H)$. Then there is $a \in H$ such that $[a, x] \neq 1$ so that $\langle [a, x]\rangle = G'$. It follows that $a^{-1}a^x = [a, x] \notin H$ or, what is the same, $a^x \notin H$, and we conclude that $x \notin \mathrm{N}_G(H)$, a contradiction.

Let $H = \langle b_1\rangle \times \cdots \times \langle b_h\rangle$, where $o(b_i) = p$ for all i. Then $\mathrm{C}_G(H) = \bigcap_{i=1}^h \mathrm{C}_G(b_i)$. Since $|G : \mathrm{C}_G(b_i)| \leq |G'| = p$, we get $|G : \mathrm{C}_G(H)| \leq p^h$, and now (c) follows from (b). □

The following lemma is well known (it is possible to prove this lemma by induction on m; see also Lemmas 4.2 and 4.7).

Lemma A.40.24. *Let G be an extraspecial group of order p^{1+2m}, $m > 1$. All maximal abelian subgroups of G have the same order p^{m+1} and are G-invariant. All nonnormal subgroups of G are elementary abelian. If $m = 1$, then $G \in \{S(p^3), \mathrm{M}_{p^3}, \mathrm{D}_8, \mathrm{Q}_8\}$. In what follows we assume that $m > 1$. The group G is one of the following types:*

(a) *$p > 2$, $G = S(p^3) * \cdots * S(p^3)$ (m times).*

(b) *$p > 2$, $G = \mathrm{M}_{p^3} * S(p^3) * \cdots * S(p^3)$ ($m - 1$ times).*

(c) *$p = 2$, $G = \mathrm{D}_8 * \cdots * \mathrm{D}_8$ (m times).*

(d) *$p = 2$, $G = \mathrm{Q}_8 * (\mathrm{D}_8 * \cdots * \mathrm{D}_8)$ (D_8 appears $m - 1$ times).*

(e) *If $A < G$ is maximal non-G-invariant, then either $A \cong \mathrm{E}_{p^m}$ and $\mathrm{C}_G(A) = A \times G'$ or $A \cong \mathrm{E}_{2^{m-1}}$ and $\mathrm{C}_G(A) = A \times \mathrm{Q}_8$.*

Corollary A.40.25. *Suppose that G is an extraspecial group of order p^{1+2m}, $m > 1$. Then* $\mathrm{sb}(G) \in \{m-1, m\}$. *Moreover,* $\mathrm{sb}(G) = m-1$ *if and only if G is as in Lemma A.40.24*(d).

Proof. Let $H < G$ be nonnormal of order p^h. By Lemma A.40.23(c), $\mathrm{sb}(H) \le h$. In part (a–c) of Lemma A.40.24, $h \le m$. If $h = m$, then we get $\mathrm{C}_G(H) = H \times G'$ so $\mathrm{sb}(H) = m$ by Lemma A.40.23(b). In part (d) of Lemma A.40.24, we have $h \le m-1$, and if $H \cong \mathrm{E}_{2^{m-1}}$, then $\mathrm{C}_G(G) = H \times \mathrm{C}_4$ so $\mathrm{sb}(H) = m-1$. □

In particular, if $G = \mathrm{Q}_8 * \mathrm{Q}_8 \cong \mathrm{D}_8 * \mathrm{D}_8$, then $\mathrm{sb}(G) = 2$. However, if $G = \mathrm{Q}_8 * \mathrm{D}_8$, then $\mathrm{sb}(G) = 1$.

22^o. G. Glauberman wrote in a letter at 17/7/09 that he and N. Mazza had proved the following

Theorem A.40.26. *Suppose that a p-group G, $p > 2$, possesses a maximal elementary abelian subgroup of order p^2. Then G has no elementary abelian subgroup of order p^{p+1}.*

This estimate is best possible as a Sylow p-subgroup of the symmetric group of degree p^2 shows. Below we present some exercises related to this theorem (see also §134).

Exercise 51. Suppose that a p-group G contains a maximal elementary abelian subgroup E of order p^2 (here we do not assume that $p > 2$). Then G has no normal subgroup of order p^{p+1} and exponent p.

Solution. Assume that $R \le G$ is normal of order p^{p+1} and exponent p. Set $H = ER$. Then $\mathrm{C}_H(E) = E$ by the modular law, so H is of maximal class, contrary to Theorems 9.5 and 9.6.

Exercise 52. Let G be as in Exercise 51 and $p = 2$. Then every subgroup of G is four-generator (this estimate is best possible as the wreath product $G = Q \operatorname{wr} C$, where $Q \cong \mathrm{Q}_8$ and $|C| = 2$, shows). In particular, G has no elementary abelian subgroup of order 2^5.

Solution. By Exercise 51, G has no normal subgroup isomorphic to E_8. Now the result follows from Theorem 50.3.

The 2-groups with a maximal elementary abelian subgroup of order 4 and a subgroup isomorphic to E_{16} are described in §127.

Exercise 53 (see §134). Let G and E be as in Exercise 51 with $p > 2$. Then $\mathrm{C}_G(E)$ is metacyclic. Next suppose that G is not metacyclic and $\mathrm{C}_G(E) > E$. Then one of the following holds:

(i) $\mathrm{N}_G(E) = RC$, where $R = \Omega_1(RC)$ is nonabelian of order p^3 and exponent p and C is cyclic, $\mathrm{C}_G(E)$ is abelian with cyclic subgroup of index p.

(ii) $p = 3$ and $G = \mathrm{N}_G(E)$ is a 3-group of maximal class, $\mathrm{C}_G(E)$ is either abelian or minimal nonabelian.

This follows easily from Theorem 13.7. See also §134.

Exercise 54. Suppose that p, G and E are as in Exercise 51 and assume that G is nonmetacyclic. Then $L = E \cap \mathrm{Z}(G)$ is of order p. Next suppose that $E/L < F/L \leq G/L$, where $F/L \cong \mathrm{E}_{p^3}$. Then $F = \Omega_1(F)\mathrm{Z}(F)$, where $\Omega_1(F)$ is nonabelian of order p^3 and $\mathrm{Z}(F)$ is cyclic of order p^2.

23^o. This subsection contains a number of exercises.

Exercise 55. Let $p > 2$. Given n, show that there is a regular p-group of class n with cyclic center.

Solution. There exists, even among metacyclic p-groups, groups of arbitrary high class. Let G be a regular p-group with $\mathrm{cl}(G) > n$ and let $N \lhd G$ be as large as possible such that $\mathrm{cl}(G/N) = n$. Then G/N has the desired property. To prove this, one may assume that $N = \{1\}$. Indeed, assume that A, B are distinct central subgroups of order p in G. Then $\mathrm{cl}(G/A) = n - 1 = \mathrm{cl}(G/B)$, hence $\mathrm{cl}(G) = \mathrm{cl}(G/(A \cap B)) = n - 1$, a contradiction.

Exercise 56. The result of Exercise 55 holds also for $n > p$ and irregular p-groups.

Exercise 57. Given $n > 1$, every regular p-group G of class $\geq n$ has an irreducible character χ such that $\mathrm{cl}(G/\ker(\chi)) = n$. Is this also true for irregular p-groups G of class $n > p$?

Exercise 58. Let G be a nonabelian p-group. Suppose that every G-invariant subgroup $\neq G'$ is a kernel of an irreducible character of G. Prove that G is of maximal class.

Solution. It is easy to see that $|G/G'| = p^2$. Obviously, p-groups of maximal class satisfy the hypothesis. Next assume that G is not of maximal class. We proceed by induction on $|G|$. By induction, any proper nonabelian epimorphic image of G is of maximal class so it will suffice to prove that $|\mathrm{Z}(G)| = p$. Since, by hypothesis, $\{1\}$ is the kernel of some irreducible character of G, we see that $\mathrm{Z}(G)$ is cyclic. Suppose that $|\mathrm{Z}(G)| > p$. Then we have $|G| > p^3$. Let L be a subgroup of order p^2 in $\mathrm{Z}(G)$. By Lemma 1.4, G contains a normal subgroup R of type (p, p). Set $R_0 = R \cap L$. Then RL/R_0 is a subgroup of type (p, p) of $\mathrm{Z}(G/R_0)$. Therefore G/R_0 has no faithful irreducible character, so that $R_0 \neq \ker(\chi)$ for any $\chi \in \mathrm{Irr}(G)$. This means that $R_0 = G'$. Since $|R_0| = p$, we have $|G| = |G : G'||G'| = p^2 \cdot p = p^3$, a contradiction.

Exercise 59. If a nonabelian p-group G is such that $\Omega_1(G) \cong \mathrm{E}_{p^2}$ and $\mathrm{C}_G(\Omega_1(G))$ is abelian, then any of its minimal nonabelian subgroups has a cyclic subgroup of index p.

Solution. Let $H < G$ be minimal nonabelian. Assume that H has no cyclic subgroup of index p. Then $\Omega_1(G) = \Omega_1(H) \leq \mathrm{Z}(H)$ so that $H \leq \mathrm{C}_G(\Omega_1(G))$, a contradiction.

Exercise 60. Let G be a metacyclic p-group, $p > 2$, of order $> p^3$ such that there is $L \lhd G$ such that G/L is nonabelian of order p^3. Suppose that $\mho_1(G)(= \Phi(G))$ is such that $\mho_1(G)/\mho_3(G)$ is nonabelian of order p^4. Prove that $\mathrm{Z}(G/\mho_3(G))$ is cyclic.

Solution. One may assume that $\mho_3(G) = \{1\}$. Assume, by way of contradiction, that $\mathrm{Z}(G)$ is noncyclic. Then there is $R \lhd G$ of order p such that $R \not\leq \mho_1(G)'$. In this case, we see that $\mho_1(G)/R$ is nonabelian of order p^3. It follows from Proposition 10.19 that $|G/R| = p^3$, a contradiction since $|G/R| = p^5$.

Recall that $\varphi_{m,n} = \mathrm{s}_n(\mathrm{E}_{p^m})$.

Exercise 61 ([Hal1, (1.41)]). Let $G \cong \mathrm{E}_{p^{n+1}}$, $k \leq n$. Prove that

$$\varphi_{n+1,k} = \varphi_{n,k} + p^{n-k+1}\varphi_{n,k-1}. \tag{8}$$

Solution. Let $B < G$ be maximal. Then $\mathrm{s}_k(B) = \varphi_{n,k}$. It remains to find the number of $H < G$ of order p^k that are not contained in B. Let H be one of such subgroups and set $S = H \cap B$; then $|S| = p^{k-1}$. Set $\bar{G} = G/S$. We have

$$|\bar{G}| = p^{(n+1)-(k-1)} = p^{n-k+2}, \quad |\bar{B}| = p^{n-k+1}, \quad |\bar{H}| = p$$

so that the number of subgroups of $\bar{G}$ of order p not contained in $\bar{B}$ is equal to

$$\frac{p^{n-k+2} - p^{n-k+1}}{p-1} = p^{n-k+1}.$$

The number of choices of S in B equals $\varphi_{n,k-1}$. As for any $S < B$ of order p^{k-1} there is $H < G$ of order p^k such that $S = H \cap B$, it follows that the desired number equals $\mathrm{s}_k(B) + p^{n-k+1}\varphi_{n,k-1}$.

Exercise 62. Classify the nonabelian 2-groups G such that whenever $H \leq G$ is nonabelian, then all irreducible representations of H are realized over the field of real numbers.

Solution. If $H \leq G$ is nonabelian, then we have $\exp(H/H') = 2$ (otherwise, H/H' has a linear character λ with $o(\lambda) = 4$ so not all its values are real). Now let $H \leq G$ be minimal nonabelian. It follows from the above that $\exp(H/H') = 2$ so $|H'| = 8$. By the Frobenius–Schur formula, we infer that the number of involutions in H is equal to $\sum_{\chi \in \mathrm{Irr}(H) - \{1_H\}} \chi(1) > 1$ so that $H \ncong \mathrm{Q}_8$. It follows that $H \cong \mathrm{D}_8$ so G is generalized dihedral, i.e., $|G : \mathrm{H}_2(G)| = 2$, where $\mathrm{H}_2(G)$ is the Hughes subgroup of G (Theorem 10.33). All such G satisfy the hypothesis.

Exercise 63. Suppose that a p-group G is neither absolutely regular nor of maximal class. If every G-invariant subgroup of order p^p and exponent p has cyclic center, then $G = RH$, where $R = \Omega_1(G)$ is of order p^p and exponent p and H is absolutely regular with noncyclic center.

Solution. In view of Lemma 1.4, there is an abelian $L \lhd G$ of type (p, p) so $p > 2$. Put $H = \mathrm{C}_G(L)$. It is easy to show that H has no G-invariant subgroup of order p^p

and exponent p. Indeed, if K is such a subgroup, then $L < M < KL$, where M is a G-invariant of order p^p and exponent p. Then $\mathrm{Z}(M)$ is noncyclic, a contradiction. In view of Theorem 13.5, H is absolutely regular. By Theorem 12.1(a), $G = \Omega_1(G)H$, where $|\Omega_1(G)| = p^p$ (Theorem 12.1(b)). Then $L \leq \mathrm{Z}(H)$ is noncyclic.

Exercise 64. Classify the p-groups G satisfying $\Phi(G)' = G'$.[3]

Exercise 65. Let H be a subgroup of a homocyclic p-group G. Then $G = H_1 \times H_2$, where $H \leq H_1$ and $\mathrm{d}(H_1) = \mathrm{d}(H)$.

Solution. Let G be homocyclic of exponent p^e and $\mathrm{d}(G) = d$. One may assume that $e > 1$ and $d > 1$. If H is homocyclic of exponent p^e, it is complemented in G as Exercise 4(b) in Introduction shows. Now assume that H is not homocyclic of exponent p^e. Let $H = Z_1 \times \cdots \times Z_k$, where Z_i are cyclic. Then there are in G cyclic subgroups U_i of order p^e such that $Z_i \leq U_i$ for $i = 1, \ldots, k$. Set $H_1 = U_1 \times \cdots \times U_k$; then H_1 is homocyclic of exponent p^e so complemented in G.

Exercise 66. Let G be a nonabelian group of exponent p and order $\geq p^4$. Suppose that all nonabelian subgroups of G of order p^4 are two-generator. Then G is of maximal class with abelian subgroup of index p.

Solution. Let $B < G$ be minimal nonabelian; then $|B| = p^3$. Assume that $\mathrm{C}_G(B) \not\leq B$. Let $L \leq \mathrm{C}_G(B)$ be of order p and $L \neq \mathrm{Z}(B)$. Then we see that $B \times L$ is nonabelian of order p^4 and $\mathrm{d}(B \times L) = 3 > 2$, a contradiction. Thus $\mathrm{C}_G(B) < B$ so G is of maximal class (Proposition 10.17). Let $R \lhd G$ be of order p^2. As above, $\mathrm{C}_G(R)$ has no minimal nonabelian subgroup so it is abelian of index p is G.

Exercise 67. Let G be a nonabelian group of exponent p and order p^m, $3 < n < m-1$. Suppose that all nonabelian subgroups of G of order p^n are two-generator. Is it true that then G is of maximal class?

Exercise 68. Let G be a nonabelian group of exponent p and order $\geq p^4$. Suppose that all maximal subgroups of G except one are two-generator. Is it true that G is of maximal class?

Exercise 69. Let G be a nonabelian group of exponent p and order $\geq p^4$. Is it true that G is of maximal class if one of the following holds: (i) All maximal subgroups of G

[3] Commentary by Mann: Assume that p is odd. The assumption implies that

$$\Phi(G) = G'\mho_1(G) = \Phi(G)'\mho_1(G) \leq \Phi(\Phi(G))\mho_1(G) = \mho_1(G),$$

so that $\Phi(G) = \mho_1(G)$, i.e., G is powerful. But then, by properties of powerful groups, $\Phi(G)' = [\mho_1(G), \mho_1(G)] = \mho_2(G')$, and this subgroup can equal G' only if $G' = \{1\}$ so G is abelian. The property of powerful groups that I need, is that, if G is powerful and N is powerfully embedded in it, then $[\mho_1(N), G] = \mho_1([N, G])$. This is proved in Lemma 2.6 of [Sha1]. In that lemma there are stronger assumptions about N, but if H there is G, the proof is applicable under assumptions that I've stated (that was brought to my attention by E. I. Khukhro). (After obtaining this commentary, the exercise was solved for all finite groups; see Theorem 111.1. It appears that all these groups must be abelian.)

except one have center of order p? (ii) All maximal subgroups of G except one have commutator quotient group of order p^2.

For the results related to Exercises 67–70, see §136.

Exercise 70. Let G be a nonabelian p-group such that $G/\mathrm{K}_3(G)$ has a cyclic subgroup of index p. Then one of the following holds:

(a) G is a 2-group of maximal class.

(b) $G \cong \mathrm{M}_{p^n}$.

Solution. Assume that G is not a 2-group of maximal class. If $p > 2$ and G is of maximal class, then $G/\mathrm{K}_3(G)$ has no cyclic subgroup of index p (see §9). Thus G is not of maximal class for each p. By hypothesis, $\mathrm{d}(G) = 2$. Write $K = \mathrm{K}_3(G)$. Then G/K is minimal nonabelian with a cyclic subgroup of index p since $\mathrm{d}(G) = 2$ and G has two distinct abelian subgroups of index p. If $K > \{1\}$, take a G-invariant $L < K$ of index p. Then, as above, G/L is minimal nonabelian, so $K = \mathrm{K}_3(G) \leq L$, a contradiction. Thus $K = \{1\}$ so $G \cong \mathrm{M}_{p^n}$ by hypothesis and Theorem 1.2.

Exercise 71. Suppose that G is a nonabelian 2-group whose Hughes subgroup $\mathrm{H}_2(G)$ satisfies $\mathrm{H}_2(G) = H < G$. Then $G = \langle x \rangle \cdot H$, where $H = A \times E$, A is abelian and all invariants of A are > 2, $\exp(E) \leq 2$. In this case, we have $G = (\langle x \rangle \cdot A) \times E$, x inverts A. In particular, if G is special, then $E = \{1\}$ and A is homocyclic of exponent 4. If $G = \langle z \rangle \cdot A$, where $o(x) = 2$, A is homocyclic of exponent 4 and x inverts A, then G is special with $\mathrm{Z}(G) = \Omega_1(A)$.

Exercise 72. If $A < G$ is the unique $\mathcal{A}_2$-subgroup of a p-group G, i.e., $\alpha_2(G) = 1$ (see §§65, 71), then A has an abelian subgroup of index p.

Solution. (i) Suppose that $A \not\leq \Phi(G)$. Then there is $M \in \Gamma_1$ not containing A. In this case, M is either abelian or an $\mathcal{A}_1$-group since it has no $\mathcal{A}_2$-subgroups. Then $M \cap A$ is abelian of index p in A.

(ii) Now let $A \leq \Phi(G)$. By Theorem 10.28, there is in G an $\mathcal{A}_1$-subgroup F that is not contained in $\Phi(G)$. Suppose that $F < H \leq G$, where $|H : F| = p$. Then we get $A < H$ since H is neither abelian nor minimal nonabelian ($A \neq H$ since $F < H$). In this case, $F \cap A$ is an abelian subgroup of index p in A.

Exercise 73. Does there exist a metacyclic p-group G such that there is in G a maximal normal abelian subgroup A with nonabelian G/A?

Solution (Mann). The answer is 'yes'. Let G be a semidirect product of a cyclic group A of order p^n by a cyclic group B whose generator induces on A the automorphism $x \to x^{1+p^k}$. The order of B is the order of the automorphism. Choose $n = 2k + 2$. Then $G' = \mathfrak{V}_k(A)$ and $\mathrm{Z}(G) = \mathfrak{V}_{n-k}(A)$. Let C be the unique subgroup between G' and $Z(G)$, and let $D = \mathrm{C}_B(C)$. Then CD is a maximal normal abelian subgroup with nonabelian factor group. (Many more examples can be produced by choosing other values of n and k to make the distance between G' and $\mathrm{Z}(G)$ bigger.)

Exercise 74. Classify the 2-groups G such that $\Omega_1(H)$ is abelian for all $H \in \Gamma_1$ but $\Omega_1(G)$ is nonabelian.

Solution. Since $\Omega_1(G)$ is nonabelian, there are noncommuting involutions $x, y \in G$. It follows that $\langle x, y\rangle = G$, so G is dihedral. It is easily seen that $G \cong \mathrm{D}_8$.

Exercise 75. Given n, let a p-group G be such that $\Omega_n(H)$ is abelian for all $H \in \Gamma_1$ but $\Omega_n(G)$ is nonabelian. Then $\Omega_n(H) = H$ for some $H \in \Gamma_1$. Prove that $G/\mathrm{Z}(G)$ is abelian of rank 2 and $\mathrm{d}(G) = 2$.

Hint. Let $H \in \Gamma_1$ be such that $|\Omega_n(H)|$ is as large as possible. If $x \in G - \Omega_n(H)$ is of order $\leq p^n$ (by hypothesis, $\Omega_n(H) < \Omega_n(G)$), then $\langle x, \Omega_n(H)\rangle = G$ by the choice of H, so that $\Omega_n(G) = G$ and $G/\Omega_n(H)$ is cyclic. Let (the same) $x \in F \in \Gamma_1$, where $|\Omega_n(F)|$ is as large as possible; then we have $F \neq H$. Take $y \in G - \Omega_n(F)$ of order $\leq p^n$. Assume that $K = \langle y, \Omega_n(F)\rangle < G$. If $K \leq M \in \Gamma_1$, then $M \neq H$ and $|\Omega_n(M)| > |\Omega_n(F)|$, contrary to the choice of F. Thus we get $K = G$ so that $G/\Omega_n(F)$ is cyclic. We have $\Omega_n(H)\Omega_n(F) = G$. As $\Omega_n(H)$ and $\Omega_n(F)$ are abelian, we obtain that $\Omega_n(H) \cap \Omega_n(F) \leq \mathrm{Z}(G)$. Since $G/\Omega_n(H)$ and $G/\Omega_n(F)$ are cyclic, it follows that (the noncyclic) group $G/\mathrm{Z}(G)$ is abelian of rank 2. Since $x \notin \mathrm{Z}(G)$, there is an element $u \in \Omega_n(H)$ such that $xu \neq ux$. It follows that $\langle x, u\rangle = G$ since $\Omega_n(\langle x, u\rangle) = \langle x, u\rangle$ is nonabelian.

Exercise 76. Let $e_n'(G)$ be the number of nonabelian subgroups of order p^n and exponent p in a p-group G. If G is a nonabelian group of order p^m and exponent p, $3 \leq n < m$, then $e_n'(G) \geq p$. If $e_n'(G) = p$, then $n = m - 1$ and $\mathrm{d}(G) = 2$. In this case, G is of maximal class and so $m \leq p$ by Theorem 9.5.

Solution. In view of Lemma 30.5, it remains to prove the last assertion. We have, by the same lemma, $n = m-1$ and $\mathrm{d}(G) = 2$. By hypothesis, there is an abelian $A \in \Gamma_1$. As $\Phi(G) = G'$, we have $|G : G'| = p^2$. Then $|\mathrm{Z}(G)| = \frac{1}{p}|G : G'| = p$ (Lemma 1.1) so, by induction, $G/\mathrm{Z}(G)$ is of maximal class. It follows that G is also of maximal. In this case, $|G| \leq p^p$ (Theorem 9.5).

Exercise 77. Given n and a p-group G of order $> p^n$, put $\mathrm{D}_n(G) = \langle H' \mid H < G, |G : H| = p^n\rangle$. The subgroup $\mathrm{D}_n(G)$ is characteristic in G. Prove that:

(a) $\mathrm{D}_1(G) < G'$ if and only if $G/\mathrm{D}_1(G)$ is minimal nonabelian.

(b) All subgroups of index p^2 in $G/\mathrm{D}_2(G)$ are abelian.

Solution. (a) All maximal subgroups of $G/\mathrm{D}_1(G)$ are abelian. If $\mathrm{D}_1(G) < G'$, then the quotient group $G/\mathrm{D}_1(G)$ is nonabelian, and we conclude that $G/\mathrm{D}_1(G)$ is minimal nonabelian. Assertion (b) is obvious.

Exercise 78. Find the number of subgroups of given order in $G = \Sigma_{p^2} \in \mathrm{Syl}_p(\mathrm{S}_{p^2})$.

Solution. All nonabelian subgroups of G are of maximal class. The number of nonabelian subgroups of G of order p^n, $n \leq p + 1$, equals p^{p+1-n} (induction and Hall's enumeration principle). Next, since $e_p(G) = 2$ ($e_k(G)$ is the number of subgroups of

order p^k and exponent p in G), we get

$$\begin{aligned} \mathrm{s}_1(G) &= 2(1 + p + \cdots + p^{p-1}) - (1 + p + \cdots + p^{p-2}) \\ &= 1 + p + \cdots + p^{p-2} + 2p^{p-1}. \end{aligned}$$

All abelian subgroups of order p^s, $s > 2$, are contained in E, where $E \cong \mathrm{E}_{p^p}$, so that their number is equal to $\varphi_{p,s}$. There are exactly $p - 1$ members, say $M_1, \ldots, M_{p-1}$, of exponent p^2 in the set Γ_1. Since $M_i \cap M_j = \Phi(G)$ $(i \neq j)$, we get

$$\mathrm{c}_2(G) = (p-1) \cdot \frac{p^p - p^{p-1}}{p(p-1)} = p^{p-1} - p^{p-2}.$$

Let $A < G$ be of order p^2 and $A \not\leq E$. Then $\mathrm{Z}(G) < A$. There are exactly p^{p-1} subgroups of order p not contained in E. Thus

$$\mathrm{s}_2(G) = \mathrm{s}_2(E) + p^{p-1} = \varphi_{p,2} + p^{p-1}.$$

It follows that the number of abelian subgroups of type (p, p) in G is equal to

$$\mathrm{s}_2(G) - \mathrm{c}_2(G) = \varphi_{p,2} + p^{p-2}.$$

If $n \in \{3, \ldots, p\}$, then

$$\mathrm{s}_n(G) = \mathrm{s}_n(E) + p^{p+1-n} = \varphi_{p,n} + p^{p+1-n}.$$

Exercise 79. If a 3-group G of exponent 3 is of maximal class, then $|G| = 3^3$.

Solution. (This follows from Theorem 9.5, but we prefer to give an independent proof.) Assume that this is false. Then there exists a 3-group of maximal class of order 3^4 and exponent 3. In this case, G contains an abelian subgroup A of order 3^3, and we have $A = \mathrm{Z}(G) \times B$. Since $B_G = \{1\}$, it follows that A is isomorphic to $\Sigma_9 \in \mathrm{Syl}_3(\mathrm{S}_9)$. As $\exp(\Sigma_9) = 9 > 3$, we get a contradiction.

Exercise 80. Let G be an irregular p-group of maximal class, $p > 2$. Describe all factorizations $G = AB$, where $A, B < G$ are absolutely regular.

Exercise 81. Suppose that a p-group G of order $> p^p$ contains exactly one normal subgroup, say R, of order p^p and exponent p. If $R \not\leq \Phi(G)$, then $R = \Omega_1(G)$ and $G = RH$, where $H \in \Gamma_1$ is either absolutely regular or irregular of maximal class.

Solution. By hypothesis, there is $H \in \Gamma_1$ such that $R \not\leq H$ so $G = RH$. Since H has no G-invariant subgroup of order p^p and exponent p, it follows that H is either absolutely regular or irregular of maximal class (Theorem 13.5).

Exercise 82. Let H be a proper maximal regular subgroup of a p-group G. Suppose that H is absolutely regular, $H/\Omega_1(H)$ is noncyclic (in particular, $p > 2$) and all subgroups of order $p|H|$ in G are two-generator. Is it true that G is of maximal class?

Exercise 83. Describe the p-groups of exponent $> p$ all of whose nonabelian maximal subgroups have exponent p.

Exercise 84. If a noncyclic p-group G contains exactly one normal subgroup of any order $\leq |\mathrm{Z}(G)|$, then $|\mathrm{Z}(G)| = p$.

Solution. Clearly, $\mathrm{Z}(G)$ is cyclic. If $|\mathrm{Z}(G)| > p$, then we see that G has no normal subgroup of type (p, p), so it is a 2-group of maximal class (Lemma 1.4). However, then $|\mathrm{Z}(G)| = 2$, which is a contradiction.

Exercise 85. If a nonabelian group G of exponent p is not covered by elementary abelian subgroups of order p^3, it is of maximal class. Each group of maximal class and exponent p is not covered by elementary abelian subgroups of order p^3.

Solution. If $L < G$ of order p is not contained in all subgroups $\cong \mathrm{E}_{p^3}$ and $R > L$ is of order p^2, then $\mathrm{C}_G(R) = R$ so that G is of maximal class by Proposition 1.8. The last assertion follows from Lemma 9.6(f).

Exercise 86. A subgroup $A < G$ is said to be *generalized soft* if there is only one maximal chain connecting A with G (see §130). Study the p-groups all of whose nonnormal subgroups are generalized soft.

Hint. If G has a generalized soft subgroup of order p, it is either of maximal class or M_{p^n}. Show that G contains no elementary abelian subgroup of order p^3. Use Theorem 13.7 for $p > 2$ and §30 for $p = 2$.

Exercise 87. Classify the irregular p-groups G such that whenever $A < G$ is maximal absolutely regular, then A is a maximal regular subgroup of G.

Exercise 88. Prove that a nonabelian p-group $G = \Omega_n^*(G)$ possesses a minimal nonabelian subgroup of exponent $\geq p^n$.

Solution. Let $A \lhd G$ be maximal abelian. Then there exists $x \in G - A$ of order p^n. By Lemma 57.1, there is $a \in A$ such that $M = \langle x, a\rangle$ is minimal nonabelian. Since $\exp(M) \geq o(x) = p^n$, we are done. (We suggest presenting another proof independent of Lemma 57.1.)

Exercise 89. Show that there is no p-group G all of whose maximal subgroups except one have the same derived subgroup as G.

Solution. Assume that $H \in \Gamma_1$ is such that $H' < G'$. Let $H' \leq K < G'$, where K is G-invariant and such that $|G' : K| = p$. Then $\bar{G} = G/K$ has only one abelian maximal subgroup $\bar{H}$ and $|\bar{G}'| = p$. By Lemma 1.1, $|\bar{G} : \mathrm{Z}(\bar{G})| = p|\bar{G}'| = p^2$ so that $\bar{G}/\mathrm{Z}(\bar{G}) \cong \mathrm{E}_{p^2}$. It follows that $\bar{G}$ has at least $p+1$ abelian maximal subgroups, a contradiction.

Exercise 90. Classify the p-groups in which the intersection of any two nonincident metacyclic subgroups is cyclic.

Exercise 91. Given two p-groups F and H, is it true that there exists a p-group G containing H as a nonnormal subgroup and such that $G/H^G \cong F$?

Exercise 92. Classify the p-groups G containing a proper subgroup of maximal class and such that $|\mathrm{N}_G(M) : M| = p$ for all $M < G$ of maximal class.

Hint. Let $H < G$ be of maximal class and assume that $|H| > p^3$. Then, by Theorem 9.6(f), there exists in H a nonabelian subgroup F such that $\mathrm{N}_H(F)$ is of maximal class and order p^4. By hypothesis, $\mathrm{N}_H(F) = \mathrm{N}_G(F)$ so G is of maximal class (Proposition 10.17).

Exercise 93. Suppose that $\mathrm{Aut}(G)$ acts transitively on the set of maximal cyclic subgroups of a p-group G. Is it true that then all subgroups of G of order p are contained in the same number of maximal cyclic subgroups of G?

Commentary of Mann (letter at 8/10/10). Take a subgroup C of order p, and let D be a maximal cyclic subgroup containing C. Then $C = \Omega_1(D)$. Since $\mathrm{Aut}(G)$ is transitive on the D's, it is transitive on the C's, so of course the answer to your question is "yes". Moreover, there are papers on groups in which $\mathrm{Aut}(G)$ is transitive on groups of order p. They are called semi-p-automorphic, and they are completely determined. For odd p, they are abelian, see [Shul]. For $p = 2$, see [Wil4].

Exercise 94. Classify the p-groups of exponent $> p$ all of whose nonabelian maximal subgroups are either minimal nonabelian or of exponent p.

Hint. Assume that our group G is not an $\mathcal{A}_2$-group. Then there is $H \in \Gamma_1$ that is neither abelian nor minimal nonabelian so $\exp(H) = p$ by hypothesis. Assume, in addition, that there is a minimal nonabelian $A \in \Gamma_1$ (i.e., G is not a group from Exercise 83). Then $\exp(A \cap H) = p$ so that $|A| \leq p^4$ (see Lemma 65.1). In this case, we have $|G| \leq p^5$.

Exercise 95. Describe the irregular p-groups of maximal class generated by (two) elements of order p.

Exercise 96. Let G be a non-Dedekindian p-group such that $|\mathrm{N}_G(H) : H| = p$ for all nonnormal $H < G$. Then the following hold:

(a) If $p > 2$, then G is metacyclic of order p^4 and exponent p^2.

(b) If $p = 2$, then each minimal nonabelian subgroup, say H, of G is metacyclic of exponent 4 and has order ≤ 16. If $|H| = 16$, then there is in H an abelian subgroup U of type $(4, 2)$ such that $\mathrm{C}_G(U) = U$ (such G are described in §77). If all minimal nonabelian subgroups of G have order 8, then such groups are described in §90.

Exercise 97 ([ZG]; see also Theorem 138.3). Complete the classification of 2-groups from Exercise 96.

Exercise 98. Classify the $\mathcal{A}_2$-groups G such that whenever $A < G$ is nonnormal, then $|\mathrm{N}_G(A) : A| \leq p^2$.

Exercise 99. Classify the $\mathcal{A}_3$-groups G (see §72) such that whenever $A < G$ is nonnormal, then $|\mathrm{N}_G(A) : A| \leq p^2$.

Exercise 100. Given $k > 2$, classify the $\mathcal{A}_k$-groups G such that whenever $A < G$ is nonnormal, then $|\mathrm{N}_G(A) : A| \leq p^k$.

For another approach to this theme, see §138.

Exercise 101 (Janko). Let G be a group and let $M, N < G$ be nonabelian such that $M' \cap N' = \{1\}$. Then $M \cap N$ is abelian.

Solution. We have $(M \cap N)' \cap M' \leq N' \cap M' = \{1\}$. It follows that $(M \cap N)' = \{1\}$, and we are done. (See the proof of Proposition 139.6.)

Exercise 102. If G is a metacyclic p-group, $|G'| > p$, then there are distinct $F, H \in \Gamma_1$ such that $\Omega_1(\mathrm{Z}(F)) = \Omega_1(\mathrm{Z}(H))$.

Solution. One may assume that G has no cyclic subgroup of index p. In that case, we have $\Omega_1(G) \cong \mathrm{E}_{p^2}$. If $M \in \Gamma_1$, then $\Omega_1(M) = \Omega_1(G)$ (Proposition 10.19). Therefore one may assume that $\Omega_1(G) \not\leq \mathrm{Z}(G)$. Then we have $\mathrm{C}_G(\Omega_1(G)) = U \in \Gamma_1$. Therefore, if $F \in \Gamma_1 - \{U\}$, then $\Omega_1(\mathrm{Z}(F)) \neq \Omega_1(G)$. If $H \in \Gamma_1 - \{U, F\}$, then $\Omega_1(\mathrm{Z}(F)) = \Omega_1(\mathrm{Z}(H))$ (otherwise, $\Omega_1(G) = \Omega_1(\mathrm{Z}(F))\Omega_1(\mathrm{Z}(H)) \leq \mathrm{Z}(G)$).

Exercise 103. Classify the p-groups $G = A \times B$, $A > \{1\}$, $B > \{1\}$, admitting a nontrivial partition. Is it true that $\exp(G) = p$?

Exercise 104. Classify the groups $G = \langle x, y \mid x^{2^n} = y^2,\ x^y = x^{-1} \rangle$.

Exercise 105. Classify the groups $G = \langle x, y \mid x^{2^n} = y^2,\ x^y = x^{-1+2^{n-1}} \rangle$.

Exercise 106. Classify the groups $G = \langle x, y \mid p^{2^n} = y^p,\ x^y = x^{1+p^{n-1}} \rangle$.

Exercise 107 (Mann). Classify the nonabelian groups of exponent p all of whose nonabelian subgroups are normal.

Solution. Let $A < G$ be nonabelian of order p^3; then we get $A \lhd G$. If $\mathrm{C}_G(A) < A$, then G is of maximal class (Proposition 10.17); then $|G| = p^4$. Let $\mathrm{C}_G(A) \not\leq A$. Take $L < \mathrm{C}_G(A)$ of order p such that $L \neq \mathrm{Z}(A)$. Write $H = A \times L$. Then the intersection of all nonabelian subgroups of H of order p^3 is equal to H'. As G/A is elementary abelian, it follows that $|G'| = p$.

Exercise 108. Classify the nonabelian groups of exponent p all of whose nonnormal nonabelian subgroups are two-generator.

Exercise 109. Classify the nonabelian groups of exponent p such that the normalizers of all nonnormal subgroups of order p have orders $\leq p^4$.

Exercise 110. Classify the groups G of exponent p containing a subgroup L of order p^2 such that there is only one maximal chain connecting L and G.

Remark 1 (Janko). The defining relations for minimal nonmetacyclic 3-group G of order 3^4 are as follows:

$$G = \langle a, c \mid a^9 = c^9 = 1,\ a^3 = c^3,\ [a, c] = b,\ b^3 = [a, b] = 1,\ [b, c] = a^{-3} \rangle.$$

It follows that a minimal nonmetacyclic group G of order 3^4 is unique. Note that if $[b, c] = a^3$, then $(ac)^3 = 1$, and then $\langle ac, a^3, b \rangle \cong \mathrm{E}_{27}$, which is a contradiction. To compute $(ac)^3 = 1$, we use the following identity:

$$(rs)^3 = r^3 s^3 [s, [s, r]][[s, r], r],$$

which holds for all 3-groups of class 3 which have an elementary abelian commutator subgroup (see the proof in §101, identity $(*)$).

Remark 2 (reported by B. Sambale). Let $P \in \mathrm{Syl}_2(\mathrm{PSL}(3, 4))$. Then E_4 and P are unique 2-groups with exactly three involutions that meet as Sylow 2-subgroups of simple groups; see [Mas].

24^o. We offer a slightly different proof of Theorem 13.7 (see also Theorem 69.4). Below we use some ideas applied in the previous proofs.

Theorem 13.7. *Let G be a p-group, $p > 2$. Suppose that G has no normal elementary abelian subgroup of order p^3. Then one of the following holds:*

(a) *G is metacyclic.*

(b) *G is a 3-group of maximal class not isomorphic to Σ_{3^2}, a Sylow 3-subgroup of the symmetric group of degree 3^2.*

(c) *$G = EH$, where $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent p, H is cyclic of index p^2 in G, $\mathrm{Z}(G) \leq H$ is cyclic, $|G : \mathrm{Z}(G)| \leq p^3$, $|H : \mathrm{C}_G(E)| \leq p$.*

Proof. We proceed by induction on $|G|$. Assume that G is nonmetacyclic. By Theorem 10.4, G has no subgroup $\cong \mathrm{E}_{p^3}$. It follows that G has no subgroup of order p^4 and exponent p. By Lemma 1.4, there is in G a normal subgroup $R \cong \mathrm{E}_{p^2}$. Assume that $\Omega_1(G) = R$. Then, by Theorems 12.1(a) and 9.11, G is a 3-group of maximal class. Next assume that there is $x \in G - R$ of order p and set $E = \langle x, R \rangle$; then E is nonabelian of order p^3 and exponent p. Let $E \leq M \in \Gamma_1$. By induction, either $M = EC$, where $E = \Omega_1(M)$ and C is cyclic, or M is a 3-group of maximal class.

(i) In the first case, $E \lhd G$ and $E \not\leq \Phi(G)$ (Lemma 1.4). The subgroup $C = \mathrm{C}_G(E)$ is cyclic since it has only one subgroup of order p, namely, $\mathrm{Z}(E)$. By N/C-theorem, G/C is a subgroup of order $\geq p^2$ in a nonabelian group of order p^3 and exponent p. If $|G : \mathrm{C}_G(E)| = p^2$, then we see that $G = C * E$ is as in (c). Now let $|G/C| = p^3$. If $L/C < G/C$ is of order p such that $L/C \not\leq CE/C$, then $\Omega_1(L) = L \cap E$ has order p, so L is cyclic. Then $G = EL$ is as in (c).

(ii) Let M be a 3-group of maximal class. Then we conclude that $T = \mathrm{C}_G(R) \in \Gamma_1$ is metacyclic by Theorems 12.1(a) and 9.11. In this case, G is of maximal class by Proposition 12.13. □

A proof of the following theorem was omitted in §13.

Proposition 13.16. *Suppose that a nonabelian p-group G has a cyclic subgroup U of order p^2 such that $\mathrm{C}_G(U)$ is cyclic. Then G is of maximal class.*

Proof. If $\mathrm{C}_G(U) = U$, then the result follows from Proposition 1.8. Now suppose that $\mathrm{C}_G(U) = C > U$. Let $\mathrm{N}_G(U) = N$; then N is nonabelian and $|N/C| = p$. If N is of maximal class, so is G (Remark 10.5). Thus $N \cong \mathrm{M}_{p^n}$, $n > 3$ (Theorem 1.2). In this case, $U \leq \Phi(C) \leq \Phi(N) = \mathrm{Z}(N)$ so that $\mathrm{C}_G(U) = N$ is noncyclic, a contradiction. □

Proposition A.40.27 ([Man5.II]). *Let G be a p-group, $p > 2$. If $|\Omega_1(G)| = p^n$, then $|G : \mathfrak{V}_1(G)| \leq p^{n^2}$.*

Proof. Let $C = \mathrm{C}_G(\Omega_1(G))$. Then G/C is an automorphism group of $\Omega_1(G)$, and therefore its order is at most $p^{n(n-1)/2}$. In C, all elements of order p are central. Such groups are called p-central, and Thompson proved that C satisfies $\mathrm{d}(C) \leq \mathrm{d}(\mathrm{Z}(C))$ (Theorem 15.1). Here, we have $\mathrm{d}(\mathrm{Z}(C)) \leq n$. Moreover, the subgroups of p-central groups are also p-central, and therefore each subgroup of C can be generated by n elements. Write $H = C/\mathfrak{V}_1(C)$. Let A be a maximal normal abelian subgroup of H. Then A is elementary abelian of order at most p^n, and $H/A = H/\mathrm{C}_H(A)$ is a group of automorphisms of A, so again we have $|H/A| \leq p^{n(n-1)/2}$. Combining the inequalities, we get $|G/\mathfrak{V}_1(C)| \leq p^{n^2}$. □

Proposition A.40.28. *Let G be a nonabelian group of exponent p such that whenever $A < B$ with nonabelian B, then $A' < B'$. Then G is of maximal class with abelian subgroup of index p.*

Proof. Assume that G is not of maximal class. Then, if $A < G$ is nonabelian of order p^3, then $\mathrm{C}_G(A) \not\leq A$ (Proposition 10.17). Let $L < \mathrm{C}_G(A)$ be of order p such that $L \not\leq A$. Setting $B = A \times L$, we see that $B' = A'$, a contradiction. Thus G is of maximal class. Let $R \lhd G$ be of order p^2, and set $G_1 = \mathrm{C}_G(R)$. Assume that G_1 is nonabelian. Then there is a nonabelian $D < G_1$ of order p^3. If $M < R$ is of order p such that $M \not\leq D$, then we get $D < D \times M$ and $D' = (D \times M)'$, a contradiction. Thus G_1 is abelian. It is easy to see that such a G satisfies the hypothesis. □

25^o. According to N. Ito, a p-group G is said to be a *Macdonald p-group* if it is special and satisfies $\mathrm{k}(G) = |\mathrm{Z}(G)| + |G/\mathrm{Z}(G)| - 1$.

Theorem A.40.29 (Macdonald [Macd12]). *If G is a Macdonald p-group, then we have $|\mathrm{Z}(G)|^2 \leq |G/\mathrm{Z}(G)|$.*

Exercise 111. Let G be a Macdonald p-group of order p^{d+a}, where $|\mathrm{Z}(G)| = p^a$. Then G/M is extraspecial for any maximal subgroup M of $\mathrm{Z}(G)$ so that $d = 2b$ is even.

Solution. We have

$$p^a + p^d - 1 = \mathrm{k}(G) = p^d + |\mathrm{Irr}_1(G)| = p^d + \sum_{M \in \Gamma_1(\mathrm{Z}(G))} |\mathrm{Irr}_1(G/M)|. \tag{9}$$

Further, $|\mathrm{Irr}_1(G/M)| \geq p-1$ for all $M \in \Gamma_1(\mathrm{Z}(G))$ with equality if and only if G/M is extraspecial. We have $|\Gamma_1(\mathrm{Z}(G))| = \frac{p^a-1}{p-1}$. It follows from (9) that

$$p^a - 1 = \mathrm{k}(G) - p^d \geq (p-1)\frac{p^a-1}{p-1} = p^a - 1.$$

Therefore $|\mathrm{Irr}_1(G/M)| = p-1$ for all $M \in \Gamma_1(\mathrm{Z}(G)$ so that G/M is extraspecial for all such M. We conclude that $d = 2b$ is even.

Exercise 112. Let G be a special p-group of order p^{d+a} with $|\mathrm{Z}(G)| = p^a$ such that G/M is extraspecial for each maximal subgroup M of $\mathrm{Z}(G)$. Then G is a Macdonald p-group.

Solution. It follows that $d = 2b$. Next, M is the kernel of $p-1$ distinct nonlinear irreducible characters since G/M is extraspecial. Since $\mathrm{Z}(G)$ has exactly $\frac{p^{2b}-1}{p-1}$ maximal subgroups, we get

$$|\mathrm{Irr}_1(G)| = (p-1) \cdot \frac{p^{2b}-1}{p-1} = p^{2b} - 1,$$

and we conclude that

$$\mathrm{k}(G) = |\mathrm{Lin}(G)| + |\mathrm{Irr}_1(G)| = p^{2b} + p^a - 1 = |G/\mathrm{Z}(G)| + |\mathrm{Z}(G)| - 1.$$

It follows that G is a Macdonald p-group, and so $a \leq b$ by Theorem A.40.29.

Exercise 113. Now let G be a nonabelian normal Sylow p-subgroup of some minimal nonnilpotent group, say S. Then G is special. If $M < \mathrm{Z}(G)$ is maximal, then S/M is minimal nonnilpotent so G/M, being special with $|(G/M)'| = p$, is extraspecial, and we conclude that G is a Macdonald p-group by Exercise 112. Let $|G| = p^{2b+a}$, where $p^a = |\mathrm{Z}(G)|$ (see Theorem A.22.1). Then it follows from Theorem A.40.29 the following nice and important Golfand's result [Gol] (see also [Red] and [BBERR, Theorem 2]): $a \leq b$.

Exercise 114. Suppose that G is a special group of order p^{2b+a}, where $p^a = |\mathrm{Z}(G)|$ and $\mathrm{cd}(G) = \{1, p^b\}$. Then G is a Macdonald group.

Solution. In view of Exercise 112, it suffices to show that if $M < \mathrm{Z}(G)$ is maximal, then G/M is extraspecial. Assume that G/M is not extraspecial for some $M < \mathrm{Z}(G)$ of index p; then we have $|\mathrm{Z}(G/M)| > p$. Therefore, if $\chi \in \mathrm{Irr}_1(G/M)$, then we get $\chi(1)^2 \leq |(G/M) : \mathrm{Z}(G/M)| < p^{2b}$, which is a contradiction since $\mathrm{cd}(G) = \{1, p^b\}$.

Exercise 115. Let L be a normal metacyclic subgroup of a p-group G, $\exp(L) = p^e$, $e > 1$. Suppose that L has no G-invariant cyclic subgroup of order p^2. Then one of

the following holds:

(a) $L \cong Q_8$.

(b) L is abelian of type (p^e, p^k), where $e - k \leq 1$.

(c) L is minimal nonabelian such that $|L : \Omega_{e-1}(L)| \leq p$.

(*Hint.* By hypothesis, we have $|L'| \leq p$ so L is either abelian or minimal nonabelian (Lemma 65.2(a).)

Exercise 116. Let $D < G$, where D is nonabelian of order 8 and G is a 2-group. Suppose that D normalizes any subgroup of G of order 2 not contained in D. Prove that if $D \cong D_8$, then $G \cong SD_{16}$.

26^o. Suppose that G is a p-group of order p^n and exponent $p^{n-3} > p^2$, $p > 2$; then $n > 5$. Our aim is to clear up the power structure of G. For the description of such G, see [ZL1].

Let $Z < G$ be cyclic of order p^{n-3}; then $|Z| \geq p^3$ by hypothesis. Clearly, G has no subgroup of order p^5 and exponent p and $|G/\mho_1(G)| \leq p^4$. It follows that if $p > 3$, then G is regular (Theorem 9.8(a)).

(i) Suppose that G has no normal subgroup isomorphic to E_{p^3}. Then G is a group from Theorem 13.7(a, b), i.e., it is either metacyclic or a 3-group of maximal class. In the second case, $|G| = 3^6$ (Theorem 9.6). If G is metacyclic, then $G/\Omega_3(G)$ is cyclic of order p^{n-6}.

(ii) Next we suppose that G possesses a normal subgroup $R \cong E_{p^3}$.

(ii1) Suppose that G/R is cyclic. Then we see that $R < \Omega_1(G)$ (otherwise, we have $\exp(G) = p^{n-2} > p^{n-3}$). In that case, $|\Omega_1(G)| = p^4$ since $\Omega_1(G)/R \leq \Omega_1(G/R)$. If $\exp(\Omega_1(G)) = p$, then $G = \Omega_1(G)Z$ satisfies the hypothesis. Now suppose that $\exp(\Omega_1(G)) > p$; then $\Omega_1(G)$ is irregular so $p = 3$ and $\Omega_1(G)$ is of maximal class (Theorems 7.1(b) and 7.2(b)). In that case by Theorem 13.5, G is a 3-group of maximal class since $1 < e_3(G) < 3 + 1$, contrary to Theorem 9.6(c) (here $e_k(G)$ is the number of subgroups of order p^k and exponent p in G).

(ii2) Now suppose that G/R is noncyclic; then we see that G/R is either abelian of type (p^{n-4}, p) or isomorphic to $M_{p^{n-3}}$. In that case, $R \cap Z$ is of order p and we have $G/R = (L/R) \cdot (K/R)$, where $K/R = RZ/R$ is cyclic of index p in G/R and $|L/R| = p$. Then $\Omega_1(K) = R$, $K = ZR$, $\exp(L) \leq p^2$ and $G = KL = ZRL = ZL$ with $K \cap L = R$ and $|Z \cap L| = p$.

(iii) Suppose that G has a normal subgroup S of order p^4 and exponent p. Then $G = SZ$ by the product formula, so that G/S is cyclic. Suppose that $S < \Omega_1(G)$; then $|\Omega_1(G)| = p^5$ and G is irregular in view of $\exp(\Omega_1(G)) = p^2$ (indeed, G has no subgroup of order p^5 and exponent p). We conclude that $p = 3$ (Theorem 7.2(b)). In that case, as in (ii), G/R is noncyclic with cyclic subgroup $K/R = RZ/R$ of index 3. Then $K = RZ < G$ so $|R \cap Z| = 3$ since $|Z| = 3^{n-3}$ and $|K| = 3^{n-1}$, and we get $\Omega_1(K) = R$ (see (ii1)) since $|K : Z| = p^2$. Write $S_1/R = \Omega_1(G/R)$; then

$S_1/R \cong \mathrm{E}_{3^2}$. Assume that there is a cyclic $C < G$ of order 3^2 satisfying $C \cap R = \{1\}$. Then, by the product formula, $CR \cap K = \Omega_1(K)$ has order 3^4, contrary to what has just been said. Thus C does not exist, and we conclude that $S_1 = \Omega_2(G)$.

27^o. In a letter at March 24, 2011, Janko reported that he had proved the following fairly unexpected

Theorem A.40.30 (Janko). *Suppose that G is a two-generator p-group with $G' \cong \mathrm{C}_{p^2}$. If $p > 2$, then all maximal subgroups of G are nonabelian.*

Proof (Berkovich). We use induction on $|G|$. Assume that there is $L \leq \mathrm{Z}(G)$ of order p with $L \neq \Omega_1(G')$. In that case, $(G/L)' \cong G'$ and $\mathrm{d}(G/L) = 2$ hence, by induction, G/L has no abelian subgroup of index p; then G has no abelian subgroup of index p since $L \leq \Phi(G)$. Therefore one may assume that $\mathrm{Z}(G)$ is cyclic.

Assume that G has an abelian maximal subgroup. Then, by Lemma 1.1, we obtain $|G : \mathrm{Z}(G)| = p|G'| = p^3$. If $\exp(G/\mathrm{Z}(G)) = p^2$, there are in $G/\mathrm{Z}(G)$ two distinct cyclic subgroups, say $A/\mathrm{Z}(G)$ and $B/\mathrm{Z}(G)$, of index p. Then $A, B \in \Gamma_1$ are distinct abelian so $A \cap B \leq \mathrm{Z}(G)$ and $|G : (A \cap B)| = p^2 > p^3 = |G : \mathrm{Z}(G)|$, a contradiction. Thus $G/\mathrm{Z}(G)$ is nonabelian of order p^3 and exponent p (recall that $\mathrm{d}(G) = 2$).

Assume that $\mho_1(G) < \mathrm{Z}(G)$. Since $G' \cap \mho_1(G) > \{1\}$, we get $|(G/\mho_1(G))'| = p$ and $|G/\mho_1(G)| > p^3$ so that $\mathrm{d}(G/G') > 2$, a contradiction. Thus $\mho_1(G) = \mathrm{Z}(G)$ so $\mathrm{Z}(G) < T < G$, where T is cyclic of order $p|\mathrm{Z}(G)|$. By Theorem 7.1(c), G is regular so $\Omega_1(G)$ is of exponent p and order $|G/\mho_1(G)| = p^3$ (Theorem 7.2(b, d)). Then $G = T\Omega_1(G)$ by the product formula, and we infer that $G/\Omega_1(G) \cong T/(T \cap \Omega_1(G)$ is abelian. In this case, we get $G' < \Omega_1(G)$, a contradiction since $\exp(G') = p^2 > p = \exp(\Omega_1(G)$. □

Exercise 117. Suppose that G is a two-generator 2-group without dihedral sections of order 8. If $G' \cong \mathrm{C}_4$, then G has no abelian maximal subgroup.

We omit the proofs of the following related results.

Theorem A.40.31. *Suppose that G is a two-generator p-group of order $> p^4$ with abelian subgroup of index p, cyclic center and $|G'| = p^2$.*

(a) *If $p > 2$, then $G = C\Omega_1(G)$, where $\Omega_1(G)$ is of order p^3 and exponent p and C is non-G-invariant cyclic.*

(b) *If $p = 2$, then $G = CD$, where $D \cong \mathrm{D}_8$ is G-invariant, C is non-G-invariant cyclic, $|C \cap D| = \mathrm{Z}(D)$ and $G' \cong \mathrm{C}_4$.*

Theorem A.40.32. *Suppose that G is a two-generator p-group, $p > 2$. If there is in G' a G-invariant subgroup L such that G'/L is cyclic of order $> p$, then all maximal subgroups of G are nonabelian.*

Theorem A.40.33. *Let G be a nonabelian metacyclic p-group, $p > 2$.*

(a) *All minimal nonabelian subgroups of G have equal order depending on $|G'|$ only.*

(b) *If $|G'| = p^k$, then G contains exactly $\frac{p^k-1}{p-1}$ minimal nonabelian subgroups.*

Appendix 41

Nonabelian 2-groups all of whose minimal nonabelian subgroups have cyclic centralizers

Here is a solution of Problem 2047 for $p = 2$.

Theorem A.41.1 (Janko). *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups have cyclic centralizers. Then any two distinct maximal abelian subgroups of G have cyclic intersection, $\mathrm{Z}(G)$ is cyclic, G has (at least one) abelian maximal subgroup and G is isomorphic to one of the groups from Theorem 35.1. Conversely, any such group satisfies the assumption of our theorem.*

Proof. We may assume that G is not of maximal class. By our assumption, $\mathrm{Z}(G)$ is cyclic. Let U be a normal four-subgroup of G (Lemma 1.4) so that $M = \mathrm{C}_G(U)$ is of index 2 in G. If M would be nonabelian, then a minimal nonabelian subgroup K of M has a noncyclic centralizer, a contradiction. Hence M is an abelian maximal subgroup of G.

Let X be any maximal abelian subgroup of G which is distinct from M. In that case, $Z = X \cap M = \mathrm{Z}(G)$ is cyclic. Let $Y \neq X$ be another maximal abelian subgroup of G which is also distinct from M. Then $Y \cap M = Z = X \cap M$ and so $X \cap Y = Z$ is cyclic. We have proved that the group G satisfies the assumption of Theorem 35.1 and so G is isomorphic to one of the groups (a) to (e) from that theorem.

Conversely, we show that each group G from Theorem 35.1 with an abelian maximal subgroup M satisfies the assumption of our theorem. Recall that, in the case under consideration, $\mathrm{Z}(G)$ is cyclic. Let H be minimal nonabelian subgroup of G. Then $\mathrm{Z}(H) = \Phi(H) \leq \Phi(G) < M$, and so $\Phi(H) \leq \mathrm{Z}(G)$ since $\mathrm{C}_G(\Phi(H)) \geq HM = G$. One may set $H = \langle x, y \rangle$, where $x \in H - M$ and $y \in (H \cap M) - \Phi(H)$. We have $G = \langle M, x \rangle$ so, since $\mathrm{C}_G(x)$ is a maximal abelian subgroup of G, we conclude that $\mathrm{C}_M(x) = Z = \mathrm{Z}(G)$ and, as we have noticed, $\mathrm{C}_M(x)$ is cyclic. Since $y \notin \mathrm{Z}(H)$, we also have $\mathrm{C}_G(y) = M$. On the other hand,

$$\mathrm{C}_G(H) = \mathrm{C}_G(x) \cap \mathrm{C}_G(y) = \mathrm{C}_G(x) \cap M = \mathrm{C}_M(x) = Z$$

is cyclic and we are done since H is an arbitrary minimal nonabelian subgroup of our group G. □

Exercise. Let G be a nonabelian p-group, $p > 2$, all of whose minimal nonabelian subgroups have cyclic centralizers. Then any two distinct maximal abelian subgroups

of G have cyclic intersection, $\mathrm{Z}(G)$ is cyclic and $\mathrm{C}_G(H) = \mathrm{Z}(G)$ for any minimal nonabelian subgroup $H \leq G$. Next, G has (at least one) abelian maximal subgroup, say M.

All the above is proved exactly in the same way as in the proof of Theorem A.40.1. If $A < B \leq G$, where $A \neq M$ is a maximal abelian subgroup of G, $|B : A| = p$ and $x \in B - A$, then $|A| = p|\mathrm{Z}(G)|$ and $\mathrm{C}_A(x)$ is cyclic (indeed, $A \cap M = \mathrm{Z}(G)$ has index p in A since $M \in \Gamma_1$). If $y \in G - M$, then $y^p \in \mathrm{Z}(G)$. It follows that all elements of the set $(G/\mathrm{Z}(G)) - (M/\mathrm{Z}(G))$ have order p so either $\exp(G/\mathrm{Z}(G)) = p$ or $M/\mathrm{Z}(G)$ is the Hughes subgroup of $G/\mathrm{Z}(G)$. If $H < G$ is minimal nonabelian, then $\exp(H/\mathrm{Z}(G)) = p$. Indeed, we see that $H\mathrm{Z}(G)/\mathrm{Z}(G) \cong H/(H \cap \mathrm{Z}(G))$ is nonnilpotent so minimal nonnilpotent. All elements of the set $H/\mathrm{Z}(G) - M/\mathrm{Z}(G)$ have order p so $H/\mathrm{Z}(G)$ is generated by elements of order p, and hence we conclude that $|H/(H \cap \mathrm{Z}(G))| = p^3$. The same arguments are also applicable in the case $p = 2$; in that case, we have $H/(H \cap \mathrm{Z}(G) \cong \mathrm{D}_8$.

Let G and M be as in the exercise (recall that there $p > 2$). Take $x \in G - M$ of minimal possible order. Then $\mathrm{C}_M(x) = \mathrm{Z}(G)$ is cyclic and $\langle x \rangle < \mathrm{C}_G(x)$. It follows that $\mathrm{C}_G(x)$ is noncyclic. Since $|\mathrm{C}_G(x) : \mathrm{Z}(G)| = p$, we get $o(x) = p$ by the choice of x. Therefore one can almost complete the classification of such groups G using Blackburn's paper [Bla13]. The same considerations are also applicable to the 2-group of the theorem. We see that there is an involution $x \in G$ such that $\mathrm{C}_G(x) = \langle x \rangle \times \mathrm{Z}(G)$. Such G are described in §48.

Appendix 42

On lattice isomorphisms of p-groups of maximal class

This section contains some information on lattice isomorphisms of p-groups of maximal class. Basic information on lattice isomorphisms is contained in §25. Thus, if G is a p-group and $\phi : G \to G_0$ is a lattice isomorphism, then G_0 is a p-group of the same order unless G is cyclic or elementary abelian (Suzuki's Theorem 25.5).

Now let G be a group of maximal class and order p^n, $n > 2$, and let $\phi : G \to G_0$ be a lattice isomorphism. If G_0 is not of maximal class and $n = 3$, then $p > 2$ and G_0 is abelian of type (p^2, p) so that $G \cong \mathrm{M}_{p^3}$. In what follows we assume that $n > 3$.

Exercise 1. Let G be a group of maximal class and order 3^4 and $\phi : G \to G_0$ be a lattice isomorphism. Then G_0 is also a 3-group of maximal class.

Solution. Assume that the assertion is false. By Theorem 25.5, G_0 is of order 3^4. Assume that G_0 is regular. Then (see Theorem 7.2 and 9.5)

$$|\Omega_1(G_0)| = |G_0/\mho_1(G_0)| = |G/\mho_1(G)| = 3^3.$$

We have $\phi(\Omega_1(G)) \cong \Omega_1(G_0)$. If $\Omega_1(G) \cong \mathrm{E}_{3^3}$, then $G \cong \mathrm{C}_3 \operatorname{wr} \mathrm{C}_3$ (Exercise 9.13) and then $G \cong G_0$ (Proposition 25.8(d)), contrary to the assumption. Now let $\Omega_1(G)$ be nonabelian; then we see that $\Omega_1(G_0) \cong \Omega_1(G)$ is of maximal class. In that case, by Theorem 12.12(a), $\mathrm{d}(G_0) = 3 > 2 = \mathrm{d}(G)$, a final contradiction.

Suppose that $p = 2$. Then the group G of maximal class has a cyclic subgroup of index 2 and $\mathrm{c}_1(G) \equiv 1 \pmod 4$. Since the same holds for G_0, it follows that G_0 is of maximal class (Theorem 1.17(a)). Therefore, in what follows one may assume that $p > 2$.

Exercise 2 (= Proposition 10.24). Suppose that a nonabelian p-group G contains an element a of order p such that $|\mathrm{C}_G(a)| = p^2$. Then there exists only one maximal chain connecting $\langle a \rangle$ and G.

Exercise 3 (= Proposition 10.24). Let a be an element of order p in a p-group G, and suppose that there is only one maximal chain connecting $\langle a \rangle$ and G. Then either G has a cyclic subgroup of index p or G is of maximal class.

Exercise 4. Let G and an element a of order p be as in Exercise 2 and $|G| > p^3$. If G_0 is a group which is lattice isomorphic to G, then G_0 is also of maximal class.

Solution. By Exercise 3, there is only one maximal chain connecting $\langle a\rangle$ and G, and this is also true for G_0 since the above chain condition is lattice invariant. By Proposition 1.8, G is of maximal class. Assume that G_0 is not of maximal class. Then G_0 has a cyclic subgroup of index p (Exercise 3). In this case, G has also cyclic subgroup of index p. It follows that $p = 2$ since $|G| > p^3$. Since $\mathrm{c}_1(G_0) = \mathrm{c}_1(G) \equiv 1 \pmod 4$, we conclude that G_0 is nonabelian so of maximal class (Theorem 1.17(a)).

Proposition A.42.1. *Let G be a p-group of maximal class and order p^n, $n > p+1$, and let $\phi : G \to G_0$ be a lattice isomorphism. Then G_0 is also of maximal class.*

Proof. As above, $|G_0| = p^n$. It is clear that $\mathrm{c}_1(G_0) = \mathrm{c}_1(G)$, $\mathrm{d}(G_0) = \mathrm{d}(G) = 2$ and $|G_0/\mathfrak{V}_1(G_0)| = |G/\mathfrak{V}_1(G)| = p^p$. One may assume that $p > 2$ (see the paragraph after the solution of Exercise 1). By Theorem 12.3(a), we have $\mathrm{c}_1(G_0) = \mathrm{c}_1(G) \equiv 1 + p + \cdots + p^{p-2} \pmod{p^p}$ so G_0 is either absolutely regular or of maximal class (Theorem 13.2(a)). Since, by the above, $|G_0/\mathfrak{V}_1(G_0)| = p^p$, it follows that G_0 is not absolutely regular. □

Thus, if G of order p^n is of maximal class and $G_0 = G^\phi$ is not of maximal class, then $p > 3$ and $n \leq p+1$. However, A. Caranti [Ca] has proved that if $n = p+1$, then G_0 is also of maximal class. Thus, if G_0 is not of maximal class, we must have $n < p+1$, i.e., G is regular. Suppose that $\exp(G) = p^2$ (see Theorem 9.5). Then $\mathfrak{V}_1(G_0) = \mathfrak{V}_1(G^\phi) = \mathfrak{V}_1(G)^\phi$ is of order p (Theorem 9.5) and so $G_0/\mathfrak{V}_1(G_0)$ of exponent p is of maximal class (Proposition 25.8(b); recall that one has assumed that $n > 3$). It follows that $\mathrm{cl}(G_0) = n-2$. In this case, Caranti [Ca] has determined the structure of G which will be given in terms of generators and relations.[1]

Theorem A.42.2 (A. Caranti [Ca]). *Let G be a p-group of maximal class and order p^n, $n \geq 3$, $p > 2$. Let $\phi : G \to G^\phi$ be a lattice isomorphism of G onto G^ϕ with $\mathrm{cl}(G^\phi) = \mathrm{cl}(G) - 1$. Then G is metabelian and $(\Omega_1(G)' \leq \mathrm{Z}(G)$. In addition, G is regular and we have one of the following two possibilities:*

(i) *If $\Omega_1(G)$ is abelian, then $G = \langle s, s_1, s_2, \ldots, s_{n-1}\rangle$, where*

$$3 \leq n \leq p, \quad s^p = s_{n-1}, \quad s_i^p = 1 \text{ for } 1 \leq i \leq n-1,$$
$$[s_i, s] = s_{i+1} \text{ for } 1 \leq i \leq n-2, \quad \text{and} \quad [s_i, s_j] = 1 \text{ for } 1 \leq i, j \leq n-1.$$

It follows that

$$\langle x_1, \ldots, x_{n-2}\rangle \cong \mathrm{E}_{p^{n-2}} \quad \text{and} \quad \mathrm{Z}(G) = \langle x_1 \ldots x_{n-2}\rangle \times \langle x_{n-1}\rangle.$$

[1] Let G be a p-group of maximal class and order p^n, $p > 2$, which is not isomorphic to M_{p^3} and such that G possesses an element s of order p such that $|\mathrm{C}_G(s)| = p^2$. If $\phi : G \to G^\phi = G_0$ is any lattice isomorphism of G, then G_0 is also of maximal class with $\mathrm{K}_i(G^\phi) = (\mathrm{K}_i(G))^\phi$ for all $2 \leq i \leq n-2$. Indeed, there is only one maximal chain connecting $\langle x\rangle$ with G, and the same is true for $\langle x\rangle^\phi$ and G_0. Now the claim follows from Exercise 4 and Proposition 25.9.

(ii) *If* $(\Omega_1(G))' = \mathrm{Z}(G)$, *then* $G = \langle s, s_1, s_2, \ldots, s_{n-1}\rangle$, *where*

$$5 \le n \le p, \quad s^p = s_{n-1}, \quad s_i^p = 1 \text{ for } 1 \le i \le n-1,$$
$$[s_i, s] = s_{i+1} \text{ for } 1 \le i \le n-2, \quad [s_2, s_1] = s_{n-1}^a \text{ with } a \not\equiv 0 \pmod{p},$$
$$\text{and} \quad [s_i, s_j] = 1 \text{ for all } \{i, j\} \ne \{1, 2\}.$$

It follows from Theorem 12.12(a) that G_0 has no subgroups of index p that are of maximal class.

Exercise 5. Let a 2-group G be of the form $G = M \times E$, where M is of maximal class and $E > \{1\}$ is elementary abelian. Suppose that G and G_0 are lattice isomorphic via the lattice isomorphism ϕ. Show that $G_0 = M_0 \times E_0$, where $M^\phi = M_0 \cong M$ and $E^\phi = E_0 \cong E$.

Hint. Show that $E_0 < \mathrm{Z}(G_0)$. To this end, in view of $\Omega_2(M) = M$, it suffices to show that every element of E_0 centralizes all elements of M_0 of order ≤ 4. See the hint to the following exercise.

It is interesting to consider an analog of Exercise 5 for $p > 2$.

Exercise 6. Suppose that a 2-group G is of the form $G = A \times B$, where A and B are of maximal class. Show that every group that is lattice isomorphic to G is also isomorphic to G.

Hint. See the hint to the previous exercise. Note that every group which is lattice isomorphic to an abelian group of type $(4, 2)$ is also abelian of type $(4, 2)$; the same is true for an abelian group of type $(4, 4)$. Take into account that the unique nonabelian metacyclic group of order 16 and exponent 4 has a maximal cyclic subgroup of order 2, but an abelian group of type $(4, 4)$ has no such subgroup.

Exercise 7. Suppose that a 2-group G is of the form $G = M \times A$, where M is of maximal class and A is abelian of exponent 4. Is it true that every group that is lattice isomorphic to G is also isomorphic to G?

Appendix 43

Alternate proofs of two classical theorems on solvable groups and some related results

All groups considered in 1^o are solvable. All groups of 2^o are p-groups.

Suppose that a positive integer n divides the order $|G|$ of a group G and L_n is the set of solutions of the equation $x^n = 1$ in G. By the fundamental Frobenius' theorem (see Volume 1, Introduction, Theorem 8), $|L_n| = kn$ for some positive integer k. Frobenius posed the following problem: Is it true that if $k = 1$, then L_n is a subgroup of G? As we think, this problem aroused from Frobenius' study of the following situation. Let $H < G$ and $H > \{1\}$ be of index $n > 1$ and assume that $H \cap H^x = \{1\}$ for all $x \in G - H$. In this case, the set $(G - \bigcup_{x \in G-H} H^x) \cup \{1\}$ is of cardinality n and coincides with L_n. Using character theory, Frobenius succeeded to show that L_n is a (characteristic) subgroup of G. In general, Frobenius' problem was solved in the positive only after the classification of finite simple groups (see [IY] and the papers of the same authors listed there).

1^o. This subsection does not contain new results. Our aim is to produce easy proofs of some known theorems on solvable groups.

An important partial case of Frobenius' conjecture many years ago was proved in elementary way in the case when G is solvable. Below we present two other proofs of this result. In our proofs we use only those facts that were known before 1900 (otherwise, Lemma A.43.2 were superfluous), namely, sections of solvable groups are solvable. We also use Frattini's argument, an easy corollary of Sylow's theorem. In this sense, our exposition is self-contained.

Theorem A.43.1 ([HalM, Theorem 9.4.1]). *If a positive integer n is a divisor of the order of a finite solvable group G and the set L_n of solutions of the equation $x^n = 1$ in G has cardinality n, then L_n is a subgroup of G.*

Obviously, the subgroup L_n from Theorem A.43.1 is characteristic in G.

We need the following

Lemma A.43.2. *If p is a prime divisor of the order of a solvable group G, then there is in G a proper subgroup whose index in G is a power of p.*

Proof. We proceed by induction on $|G|$. Let R be a minimal normal subgroup of G; then R is an elementary abelian q-group for some prime q.

If p divides $|G/R|$, then, by induction, there is in G/R a proper subgroup H/R whose index is a power of p. Since $|G : H| = |G/R : H/R|$, we are done in this case. This is the case if $q \neq p$. Therefore, in what follows we assume that G has no non-identity normal p'-subgroups.

Now let p not divide $|G/R|$. Then R is a Sylow p-subgroup of G. Let S/R be a minimal normal subgroup of G/R; then S/R is an s-subgroup for some prime $s \neq p$. Let Q be a Sylow s-subgroup of S. Then the Frattini argument yields $G = S\mathrm{N}_G(Q)$. But

$$S\mathrm{N}_G(Q) = RQ\mathrm{N}_G(Q) = R\mathrm{N}_G(Q) \quad \text{and} \quad \mathrm{N}_G(Q) < G,$$

by the previous paragraph. Since $|G : \mathrm{N}_G(R)|$ divides (even equals) $|R|$, a power of p, the proof is complete. □

Clearly, Lemma A.43.2 follows immediately from Hall's Theorem A.28.4.

Remark 1. Let G be a solvable group and $n \mid |G|$, $|L_n| = n$ and R be a minimal normal subgroup of G. Let $|R| = p^\alpha$ and write $\bar{G} = G/R$. (i) If $|R| \mid n$, then the set $\bar{L}$ of solutions of $\bar{x}^{n/|R|} = \bar{1}$ in $\bar{G}$ has cardinality $n/|R|$ and $L = L_n$, where L is the inverse image of $\bar{L}$ in G. Indeed, let $\bar{L} = \{\bar{x}_1, \ldots, \bar{x}_s\}$. Then $\bar{x}_i = x_i R$ is a coset of R so that $L = x_1 R \cup \cdots \cup x_s R$. We compute $x_i^n = (x_i^{n/|R|})^{|R|} = 1$ since $x_i^{n/|R|} \in R$. There one can take, instead of x_i, any element of the coset $x_i R$. Thus $x_i R \in L_n$ so that $L \subseteq L_n$. By Frobenius' theorem, $n/|R|$ divides s so that $s \geq n/|R|$. One has

$$|L| = s|R| \geq (n/|R|)|R| = n = |L_n|,$$

and we conclude that $L = L_n$ whence $s = n/|R|$. (ii) Let $p \mid n$ but $|R|$ not divide n. Set $n = n_p n_{p'}$. Let $\bar{L}$ be the set of all solutions of $\bar{x}^{n_{p'}}$ in $\bar{G}$ and L the inverse image of $\bar{L}$ in G. By Frobenius, $|\bar{L}| \geq n_{p'}$; then

$$|L| \geq |R| n_{p'} > n_p n_{p'} = n = |L_n|$$

since $|R| > n_p$ by assumption. If $y \in L$, then $y^n = (y^{n_{p'}})^{n_p} = 1$ since $y^{n_{p'}} \in R$ and $\exp(R) = p \mid n_p$. Thus $L \subseteq L_n$, contrary to what has just been proved. We see that if $p \mid n$, then L_n is a union of cosets of R, i.e., $|R| \mid n$. (iii) Now suppose that p does not divide n. We claim that then the set $\bar{L}$ of solutions of $\bar{x}^n = \bar{1}$ has cardinality n. Write $\bar{L} = \{\bar{x}_1, \ldots, \bar{x}_s\}$. By Frobenius' theorem, $s \geq n$. Let $L = x_1 R \cup \cdots \cup x_s R$ be the inverse image of $\bar{L}$ in G. We have $x_i^n \in R$ so that $x_i = y_i z_i = z_i y_i$, where $o(y_i) = o(\bar{x}_i)$ and $z_i \in R$ (note that $o(\bar{x}_i) \mid n$). Since $y_i R = y_i z_i R = x_i R$ for all i, it follows that $y_i \neq y_j$ for $i \neq j$. Therefore the set $L^0 = \{y_1, \ldots, y_s\} \subseteq L_n$; moreover, $L^0 = L_n$ since $|L^0| = s \geq n = |L_n|$, completing this case.

Proof of Theorem A.43.1. We use induction on $|G| + n$. To that end, one may assume that $1 < n < |G|$.

Suppose that n divides the order of a proper subgroup M of G. Then the number of solutions of $x^n = 1$ in M is a nonzero multiple of n, and we infer that $L_n \subseteq M < G$; then $L_n \leq M$ by induction, and we are done. In what follows we assume that n does not divide the orders of all proper subgroups of G. Let p be an arbitrary prime divisor

of $|G|$. Then there is in G a proper subgroup H such that $|G : H|$ is a power of p (Lemma A.43.2). Since n does not divide $|H|$, we conclude that p divides n. Thus we get $\pi(n) = \pi(|G|)$, where $\pi(n)$ is the set of primes dividing n.

Let R be a minimal normal subgroup of G; then $|R| = p^\alpha$ for some prime p and positive integer α and $\exp(R) = p$. Since, by the previous paragraph, $p \mid n$, all elements of R satisfy $x^n = 1$ so that $R \subseteq L_n$. Write $\bar{G} = G/R$. By Remark 1(i, ii), we have $|R| = p^\alpha \mid n$, and if $\bar{L}$ is the set of solutions of $\bar{x}^{n/p^\alpha} = \bar{1}$ in $\bar{G}$, then its inverse image coincides with L_n and $|\bar{L}| = n/p^\alpha$. Therefore, by induction, $\bar{L}$ is a subgroup of $\bar{G}$. In this case, L_n, the inverse image of $\bar{L}$ in G, is also a subgroup of G. □

Remark 2. Suppose that G and L_n are such that L_n is a subgroup of G of order n (here we do not assume that G is solvable). Let $p \in \pi(|G : L_n|) \cap \pi(n)$; then $P \in \mathrm{Syl}_p(G)$ is not contained in L_n. In this case, $L_n \cap P$ is the unique subgroup of order n_p in P since all subgroups of P of exponent $\leq n_p$ are contained in L_n and so we obtain that $P \cap L_n \in \mathrm{Syl}_p(L_n)$. It follows that either P is cyclic or $p = 2 = n_2$ and P is a generalized quaternion group by Proposition 1.3. In the first case, L_n is p-nilpotent by Theorem A.28.9. In the second case, 4 does not divide $|L_n|$, so L_n is 2-nilpotent again.

Combining some arguments from the text above, we can produce another proof of Theorem A.43.1. We need two additional lemmas.

Lemma A.43.3. *Suppose that n is a divisor of the order of a solvable group G and $|L_n| = n$. If a prime p divides $|G|/n$, then the set L_n does not contain a subset of cardinality pn_p which is a subgroup of G.*

Proof (independent of Theorem A.43.1). We use induction on $|G|+n$. Let R be a minimal normal subgroup of G of order, say, q^α. Write $\bar{G} = G/R$.

Assume that $M < G$ has order divisible by n. Then $L_n \subseteq M$, and, by induction, there is no subgroup of order pn_p that is a subset of L_n (if p does not divide $|M|/n$, our claim follows from the Lagrange theorem). In what follows we assume that n does not divide the orders of all proper subgroups of G.

Suppose that q does not divide n. By Lemma A.43.2, there is a subgroup $M < G$ such that $|G : M|$ is a power of q. In this case, $n \mid |M|$, contrary to what has been said in the previous paragraph.

Thus $q \mid n$. By Remark 1(i, ii), $q^\alpha \mid n$ and the set $\bar{L}$ of solutions of $\bar{x}^{n/q^\alpha} = \bar{1}$ in $\bar{G}$ has cardinality n/q^α.

If $q \neq p$, then $(n/q^\alpha)_p = n_p$ so, by induction, the set $\bar{L}$ has no subset of cardinality pn_p which is a subgroup of $\bar{G}$. Assume that a p-subgroup $P < G$ of order pn_p is a subset of L_n. Then $PR/R \subseteq \bar{L}$ since all elements of PR/R satisfy $\bar{x}^{n/q^\alpha} = \bar{1}$. In this case, the p-subgroup PR/R of order $pn_p = p(n/|R|)_p$ is a subset of $\bar{L}$, contrary to what has just been said.

Now let $q = p$. By Remark 1(i, ii), the set $\bar{L}$ of solutions of $\bar{x}^{n/p^\alpha} = \bar{1}$ has cardinality n/p^α, hence the inverse image L of $\bar{L}$ in G has cardinality n so coincides with L_n. If a p-subgroup $\bar{P}$ is a subset of $\bar{L}_n = \bar{L}$ (see Remark 1(i)), then $|\bar{P}| \leq (n/p^\alpha)_p$ by induction, and we obtain $|P| = |\bar{P}||R| \leq (n/p^\alpha)_p \cdot p^\alpha = n_p$. □

Of course, Lemma A.43.3 follows from Theorem A.43.1, but we prefer giving an independent proof since our aim now is to produce another proof of Theorem A.43.1.

The following lemma is due essentially to Galois.

Lemma A.43.4. *Every index of a maximal subgroup of a solvable group G is equal to some index of a principal series of G.*

Proof. We proceed by induction on $|G|$. Let $H < G$ be maximal. One may assume that H is not normal in G (otherwise, $|G : H|$ is an index of a principal series of G containing H). Let R be a minimal normal subgroup of G; then $|R|$ is an index of a principal series of G containing R. If $R < H$, then $|G : H| = |G/R : H/R|$ is equal to an index of a principal series of G/R by induction, completing this case. If R is not contained in H, then $G = HR$, $H \cap R = \{1\}$ so that $|G : H| = |R|$. The proof is complete. □

It should be noticed that Lemma A.43.2 does not follow from Lemma A.43.4. Given an index m of a principal series of a solvable group G, it is not necessarily that G contains a maximal subgroup of index m.

The second proof of Theorem A.43.1. As in the first proof of Theorem A.43.1, it suffices to show that n divides the order of some maximal subgroup of G. Assume that this is false. In this case, as we have noticed in the second paragraph of the first proof of Theorem A.43.1, $\pi(n) = \pi(|G|)$. Let p be a prime divisor of $|G|/n$ and P be a Sylow p-subgroup of G; then P is not contained in the set L_n (Lemma A.43.3). Let $P_1 \leq P$ be of order pn_p. Since, by Lemma A.43.3, P_1 is not contained in the set L_n, we conclude that $\exp(P_1) > n_p$ hence P_1 is cyclic. As $p \mid n$, we get $|P_1| > p$. Thus all subgroups of order pn_p in P are cyclic, whence P is either cyclic or a generalized quaternion group and $|P_1| = 4$ (Proposition 1.3). In the second case, clearly, $n_2 = 2$. Note that all factors of a principal series of G are elementary abelian. Therefore all $\{p\}$-indices of a principal series of G are equal to p in the first case and equal 2 or 4 in the second case.

Suppose that $P \in \mathrm{Syl}_p(G)$ is cyclic. By the last sentence of the previous paragraph and Lemmas A.43.2 and A.43.4, G has a maximal subgroup H of index p. In this case, $n \mid |H|$, contrary to the assumption.

Now suppose that $p = 2$ and a Sylow 2-subgroup of G is generalized quaternion; then $n_2 = 2$. In this case, by the previous paragraph and Lemmas A.43.2 and A.43.4, G has a maximal subgroup H of index dividing 4. Since $|P| \geq 8$ and $n_2 = 2$, we obtain $n \mid |H|$, contrary to the assumption. □

Remark 3. If π is a nonempty set of prime divisors of the order of a π-solvable group G and $p \in \pi$, then G has a proper subgroup whose index is a power of p and a proper subgroup whose index is a π'-number (of course, all this follows from an analog of Theorem A.43.5 below for π-solvable groups; that result is due to A. S. Chunikhin). However, the proof of this result depends on the Schur–Zassenhaus theorem. In view

of the Odd Order Theorem, π-separable groups, in the sense of Hall–Higman, are either π- or π'-solvable, so one can state an analog of Lemma A43.2 for such groups.

Supplement to Theorem A.43.1. *Suppose that G is a π-solvable group and a positive integer n is divisible by $|G|_{\pi'}$. If $|L_n| = n$, then L_n is a subgroup of G.*

Proof. In view of Theorem A.43.1, one may assume that G is nonsolvable; then we obtain that $\pi \neq \pi(|G|)$. We also assume that $n < |G|$. Let $H \leq G$ be of order $|G_{\pi'}|$. If $n = |G|_{\pi'}$, then $L_n = H$. Next we assume that $|G_{\pi'}| < n$; then $\pi \cap \pi(|G|) \neq \varnothing$. Let R be a minimal normal subgroup of G. Write $\bar{G} = G/R$, $|R| = r$. Then r is either power of a prime from π or a π'-number.

As above, we use induction on $|G|+n$. By Remark 3, for every $p \in \pi \cap \pi(G)$, there is $M < G$ such that $|G : M|$ is a power of p. As in the proof of Theorem A.43.1, if $n \mid |M|$, the result follows by induction. So one may assume that $\pi \subset \pi(n)$.

(a) Suppose that $r = p^\alpha$, where $p \in \pi$. By what has been said in the previous paragraph, $p \mid n$; then $R \subset L_n$. By Remark 1(i, ii) (these parts also hold if $|R|$ is a prime power), the set $\bar{L}$ of solutions of the equation $\bar{x}^{n/p^\alpha} = \bar{1}$ has cardinality n/p^α so, by induction, $\bar{L}$ is a subgroup of $\bar{G}$; then its inverse image L in G is also a subgroup in G. Since $|L| = n$, we get $L = L_n$, completing this case.

(b) Now let r be a π'-number. By Remark 1(iii) (this part holds for arbitrary groups under the condition $\mathrm{GCD}(|R|, n) = 1$) and induction, $\bar{L} = \{\bar{x} \in \bar{G} \mid \bar{x}^{n/r} = \bar{1}\}$ is a subgroup of G of order n/r. Then (the subgroup) L, the inverse image of $\bar{L}$ in G, has order n so coincides with L_n. □

Now we use Lemma A.43.2 to prove the following

Theorem A.43.5 (P. Hall). *If m is a divisor of the order of a solvable group G such that $\mathrm{GCD}(m, |G|/m) = 1$, then all largest $\pi(m)$-subgroups of G have order m and are conjugate in G.*

Proof. We use induction on $|G| + m$. Let R be a minimal normal subgroup of G with $|R| = p^\alpha$ for some prime p.

(i) First we prove that G contains a subgroup of order m. Let q be a prime divisor of $|G|/m$; then there exists $H < G$ such that $|G : H|$ is a power of q (Lemma A.43.2). In this case, $m \mid |H|$ and $\mathrm{GCD}(m, |H|/m) = 1$ so, by induction, H contains a subgroup of order m.

(ii) We claim that all subgroups of order m are conjugate in G. Let $F, H < G$ be of order m. Then $\pi(m)$-Hall subgroups FR/R and HR/R are conjugate in G/R by induction, so $(FR)^x = HR$ for some $x \in G$ whence $F^x \leq HR$.

If $p \mid m$, then $R \leq F \cap H$ so $FR = F$, $HR = H$ and hence $F^x = H$. Next assume that $\mathrm{O}_{\pi(m)}(G) = \{1\}$.

If $HR < G$, there is $y \in HR$ such that $(F^x)^y = H$ by induction. Now assume that $HR = G$ for any choice of R; then also $FR = G$ and $R \in \mathrm{Syl}_p(G)$ is the unique minimal normal subgroup of G so H and F are maximal in G. Let Q/R be a minimal nor-

mal subgroup of G/R; then Q/R is a q-subgroup for some prime $q \neq p$. In this case, $H \cap Q, F \cap Q \in \mathrm{Syl}_q(Q)$ are not normal in G by assumption. Therefore we obtain $\mathrm{N}_G(H \cap Q) = H$ and $\mathrm{N}_G(F \cap Q) = F$. By Sylow's theorem, $F \cap Q = (H \cap Q)^y$ for some $y \in Q$. Then

$$F = \mathrm{N}_G(F \cap Q) = \mathrm{N}_G((H \cap Q)^y) = \mathrm{N}_G(H \cap Q)^y = H^y.$$

(iii) It remains to show that if $K < G$ is the greatest $\pi(m)$-subgroup, then $|K| = m$. By induction, $KR/R \leq H/R$, where H/R is a $\pi(m)$-Hall subgroup of G/R (see (ii)); then $K \leq H$.

If p divides m, then $|H| = m$, $R \leq K$ and $K = H$ by maximality of K.

Now let p not divide m. We have $K < KR \leq H$. If $H < G$, then, by induction, K is contained in a subgroup of order m in H so $|K| = m$ by maximality of K. Now let $H = G$. Then we have $G = FR$, where $F < G$ is of order m (F exists by (i)). Set $K_1 = KR \cap F$; then $|K_1| = |K|$ by the product formula. By (ii), $K = K_1^z$ for some $z \in KR$ so $K \leq F^z$ and, since $|F^z| = |F| = m$, we obtain $K = F^z$ by maximality of K. □

2^o. In this subsection G is a p-group.

Let k be a positive integer and $p^{k+1} < |G|$. If $|L_{p^k}| = p^k$, then G has exactly one subgroup of order p^k so G is either cyclic or $p = 2$, $k = 1$ and G is a generalized quaternion group (Proposition 1.3). Therefore, Frobenius' case is trivial for p-groups.

Next we assume that $|L_{p^k}| > p^k$. In this case, G is noncyclic so such group G contains a noncyclic subgroup H of order p^{k+1}. In what follows we assume that $|L_2| > 2$ if $p^k = 2$. Since $H \subseteq L_{p^k}$, we get $|L_{p^k}| \geq p^{k+1}$.

A. Assume that $|L_{p^k}| = p^{k+1} (< |G|)$. Then our group G is not of maximal class and $L_{p^k} = H$, where, as above, $H < G$ is noncyclic of order p^{k+1}. In this case, there is in G a subgroup F of order p^{k+1} that is not equal to H (Proposition 1.3). Since all subgroups of order p^k are subsets of L_{p^k}, it follows that F is not generated by its maximal subgroups so it is cyclic. Thus H is the unique noncyclic subgroup of order p^{k+1} in G. By Lemma 1.4, there is in G a normal abelian subgroup R of type (p, p) so we get $R \leq L_{p^k} = H$.

If $k = 1$, then $R = H = \Omega_1(G)$. In this case, G is either metacyclic or a 3-group of maximal class or has exactly three involutions (see Theorem 13.7 and §82).

Now let $k > 1$. In this case, H/R is the unique subgroup of order p^{k-1} in G/R so that either G/R is cyclic of $p = 2$, $k = 2$ and G/R is a generalized quaternion group; in both cases $R = \Omega_1(G)$. In the first case, G possesses a cyclic subgroup of index p so, by Theorem 1.2, either $G \cong \mathrm{M}_{p^n}$ or G is an abelian group of type (p^{n-1}, p). In the second case, $k = 2$, $p = 2$ and G is a metacyclic group of Lemma 42.1(c).

B. Now let $k = 1$ and $p^2 < |L_p| < p^3$. In this case, G has no subgroups of order p^3 and exponent p. It follows that $p = 2$ (see Theorems 12.1, 13.7 and §§9, 7). In the case under consideration, if G is of maximal class, it is easy to check that then $G \in \{\mathrm{D}_8, \mathrm{SD}_{16}\}$. Now assume that G is not of maximal class. Then it has a normal

abelian subgroup R of type $(2,2)$. By hypothesis, there is an involution $x \in G - R$; then $H = \langle x, R\rangle \cong \mathrm{D}_8$. Since the number of involutions in G is $\cong 3 \pmod 4$ (Theorem 1.17(a)), there are exactly seven involutions in G. In that case, $|L_2| = 7 + 1 = 8$, contrary to the hypothesis. Thus only the groups D_8 and SD_{16} satisfy $4 < |L_2| < 8$.

C. The case of a p-group G satisfying $|L_p| = p^3$ is not tractable for $p = 2$ in this time. Now let $p > 2$; then $L_p = \Omega_1(G)$ is of exponent p (Theorem 7.2(b)). We suggest the reader supply the case where G is a p-group, $k > 1$ and $|L_{p^k}| = p^{k+2}$. (As the following part D shows, this is more or less difficult for $p = 2$ only.)

D. Now let G be an irregular p-group of order $p^m \geq p^{2p}$, $p > 2$,

$$\exp(G) > p^k > p \quad \text{and} \quad |L_{p^k}| \leq p^{k+p-1} < p^m (= |G|).$$

D1. Suppose that G has no normal subgroup of order p^p and exponent p. Then G is of maximal class (Theorem 12.1(a)). In this case, $\exp(G) = p^e$, where

$$e = \left[\frac{m-1}{p-1}\right] + \epsilon$$

with $\epsilon = 0$ if $p - 1 \mid m - 1$ and 1 otherwise (here $[x]$ is the integer part of the real number x). Our group G has a maximal subgroup G_1 satisfying $|G_1/\mathfrak{V}_1(G_1)| = p^{p-1}$ (see Theorems 9.5 and 9.6 where such G_1 are called absolutely regular p-groups) and such that all elements of the set $G - G_1$ have orders $\leq p^2$ (Theorem 13.19(b)) so that $G - G_1 \subset L_{p^k}$. One has the equality $|G - G_1| = p^{m-1}(p-1)$. The subgroup $\Omega_k(G_1)$ of order $p^{k(p-1)}$ is contained in L_{p^k}. Thus

$$p^{k+p-1} \geq |L_{p^k}| = (p-1)p^{m-1} + p^{k(p-1)}.$$

It follows that $k + p - 1 > k(p-1)$ which is impossible. Thus G is not a group of maximal class if $p > 2$. The same is true if $p = 2$.

D2. By Theorem 12.1(a), G possesses a normal subgroup R of order p^p and exponent p. Let $H/R < G/R$ be of order p^{k-1}; then $|H| = p^{p+k-1}$ and $\exp(H) \leq p^k$ so that $H = L_{p^k}$. It follows that all elements of the set $G - H$ have orders $> p^k$ so that $L_{p^k} = \Omega_k(G)$ and L_{p^k}/R is the unique subgroup of order p^{k-1} in G/R, and we conclude that G/R is either cyclic or generalized quaternion group (in the second case, $k = 2$). By hypothesis, $|G/R| \geq p^p$.

Suppose that G/R is cyclic. Assume that $R < \Omega_1(G)$. Then $|\Omega_1(G)| = p^{p+1}$ and, by Exercise 13.10(a), we have $\exp(\Omega_1(G)) = p$. Let $M/\Omega_1(G) < G/\Omega_1(G)$ be of order p^{k-1}; then $|M| = p^{p+k}$ and $\exp(M) = p^k$. It follows that $M \subseteq L_{p^k}$, a contradiction since $|M| = p^{p+k} > p^{p+k-1} \geq |L_{p^k}|$. Thus $\Omega_1(G) = R$ so that G is an L_p-group (see §§17, 18).

Now suppose that G/R is a generalized quaternion group; then $p = 2$ and, as we have noticed, $k = 2$. In case $\Omega_1(G) < R$, we see that $\Omega_1(G)$ is elementary abelian of order 8 (Exercise 13.10(a)). If $H/\Omega_1(G) \leq G/\Omega_1(G)$ is noncyclic of order 2^2, then

$\exp(H) = 2^2$ hence $H \subseteq L_{2^k}$, a contradiction since $|H| = 2^{3+2} > 2^{2+1} = |L_{2^2}|$. Thus $\Omega_1(G) = R$ hence $|\Omega_2(G)| = 8$. It follows that G is as in Lemma 42.1(c).

We state the results obtained in this section in the following two propositions.

Proposition A.43.6. *Let G be a p-group. If $p < p^k < |L_{p^k}| \le p^{k+1} < |G|$, then one of the following holds:*

(a) *G is either abelian with cyclic subgroup of index p or isomorphic to M_{p^n}.*

(b) *$k = 2$, $p = 2$,*

$$G = \langle a, b \mid a^{2^{m-2}} = 1,\ b^4 = a^{2^{m-3}},\ a^b = a^{-1},\ m > 4\rangle.$$

Here

$$\mathrm{Z}(G) = \langle b^2\rangle, \quad G' = \langle a^2\rangle, \quad \Phi(G) = \langle a^2, b^2\rangle, \quad \Omega_2(G) = \langle a^{2^{m-4}}, b^4\rangle,$$

G/G' and $\Omega_2(G)$ are abelian of type $(4, 2)$.

Proposition A.43.7. *Suppose that G is an irregular p-group of order $p^m \ge p^{2p}$ and exponent p^e, $1 < k < e$. If $|L_{p^k}| \le p^{p+k-1}$, then one of the following holds:*

(a) *G is an L_p-group, i.e., $|\Omega_1(G)| = p^p$ and, in our case, $G/\Omega_1(G)$ is cyclic of order $\ge p^p$.*

(b) *$k = 2$, $p = 2$ and G is as in Proposition A.43.6*(b).

Problems

Problem 1. Let n be a proper divisor of the order of a solvable group G. Study the structure of L_n provided $|L_n| = 2n$. (The minimal nonabelian group G of order $3^2 \cdot 2^2$ is such that $|L_6| = 2 \cdot 6$.)

Problem 2. Let p be a minimal prime divisor of the order of a group G and n be a proper divisor of $|G|$. Study the structure of the set L_n provided $|L_n| \le pn$.

Problem 3. Let G be an irregular p-group and $k > 1$. Study the structure of G provided $|L_{p^k}| \le p^{k+p}$. (See 2^o.)

Problem 4. Suppose that G is a metacyclic p-group and H is a p-group such that $|L_{p^2}(H)| = |L_{p^2}(G)|$. Study the structure of H. Mann has solved a partial case of this problem for $p > 2$ when $\mathrm{s}_1(H) = \mathrm{s}_1(G)$ and $\mathrm{s}_2(H) = \mathrm{s}_2(G)$, where $\mathrm{s}_k(G)$ is the number of subgroups of order p^k in G (it appears that the similar problem for $p = 2$ is surprisingly difficult); a small modification of Mann's argument allows us to solve the general problem for $p > 2$ since, in the case under consideration, $|\Omega_2(G)| \le p^4$.

Appendix 44

Some of Freiman's results on finite subsets of groups with small doubling

This appendix was written by Moshe Roitman (University of Haifa). We consider here arbitrary groups (not necessarily finite). We describe results that Gregory Freiman obtained about 40 years ago.

Let A, B be nonempty subsets of a group G. We define set multiplication as usual:

$$AB = \{ab \mid a \in A,\, b \in B\}.$$

We let $A^2 = AA$ and $A^{-1} = \{a^{-1} \mid a \in A\}$. For a set A (not necessarily finite) we define its cardinality by $|A|$.

Definition A.44.1. Let A be a finite nonempty subset of a group G. The quotient

$$\sigma(A) = \sigma_G(A) = \frac{|A^2|}{|A|}$$

is called the *doubling coefficient* of A in G.

We first present some background material on doubling coefficients (items A.44.2–A.44.10 below).

Remark A.44.2. If $H \leq G$ are groups and A is a finite nonempty subset of H, then $\sigma_H(A) = \sigma_G(A)$.

Clearly, in the setting of Definition A.44.1, we have

$$1 \leq \sigma(A) \leq |A|.$$

Moreover, $\sigma(A) = |A|$ if and only if $|A^2| = |A|^2$. The condition $|A^2| = |A|^2$ is equivalent to the condition that every element of A^2 has a *unique* representation as a product ab, where $a, b \in A$. Thus we have two more equivalent conditions to the equality $\sigma(A) = |A|$:

(1) The sets aA for $a \in A$ are disjoint.

(2) The sets Aa for $a \in A$ are disjoint.

Example A.44.3. A subset T_n of cardinality n of a finite group G_n with $\sigma(T_n) = n$ for $n \geq 1$.

Solution. For $n \geq 1$, let $G_n = S_{2n+1}$, and let T_n be the set of 3-cycles in S_{2n+1}, the symmetric group of degree $2n+1$, of the form $(1, 2k, 2k+1)$ for $1 \leq k \leq n$. We have

$$(1,2k,2k+1)(1,2m,2m+1) = \begin{cases} (1,2m,2m+1,2k,2k+1) & \text{if } k \neq m, \\ (1,2k+1,2k) & \text{if } k = m. \end{cases}$$

Hence every element of T_n^2 has a unique representation as a product st, where $s, t \in T_n$.

Of course, for $n > 1$ the groups G_n in the previous example are not commutative. Indeed, if $\sigma(A) = |A|$, and $a \neq b$ in A, then $ab \neq ba$.

We will show that $\sigma(A) = 1$ if and only if A is a coset in Proposition A.44.5 below.

By a *coset* of a subgroup H of a group G we mean a set that is both a left and a right coset (in the usual sense) of H. Thus, if A is a coset of H, then A is a subset of $N_G(H)$.

We will use repeatedly the following remark.

Remark A.44.4. Let H be a subgroup of a group G. Then the set of the cosets of H in G is a group under set multiplication:

$$AB = \{ab \mid a \in A,\, b \in B\}.$$

Moreover, if A and B are subsets of G so that AH and BH are cosets of H, then $(AH)(BH) = (AB)H$ and $(AH)^{-1} = A^{-1}H$; hence for all integers m we have

$$(AH)^m = A^m H.$$

Proposition A.44.5. *Let A be a finite nonempty subset of a group G. Then*

$$\sigma_G(A) = 1 \iff A \text{ is a coset of a subgroup of } G.$$

Proof. $\Longrightarrow$: Assume that $\sigma_G(A) = 1$, that is, $|A^2| = |A|$. For all $a \in A$ we see that $|aA| = |A| = |A^2|$. Since $aA \subseteq A^2$, we obtain that $aA = A^2$. Similarly, $Aa = A^2$ for all $a \in A$. Hence for all $a, b \in A$ we have $Ab = aA$, so $a^{-1}A = Ab^{-1}$; thus we get $a^{-1}A = Aa^{-1} = AA^{-1}$. Let $H = AA^{-1}$. We have for $a \in A$:

$$HH = (AA^{-1})(AA^{-1}) = (Aa^{-1})(aA^{-1}) = AA^{-1} = H.$$

Since $H \neq \varnothing$ and $H = H^{-1}$, it follows that H is a subgroup of G (we could also use the finiteness of H). We have for $a \in A$ that $a^{-1}A = H$, so $A = aH$. Similarly, we get $A = Ha$, so A is a coset of H.

$\Longleftarrow$: Let A be a coset of a subgroup H of G. Thus, for all $a \in A$ we obtain that $A = aH = Ha$, so by Remark A.44.4, we get $A^2 = (aH)^2 = a^2H$. It follows that $|A^2| = |A|$, that is, $\sigma_G(A) = 1$. □

Remark A.44.6. Let A be a finite subset of a group G so that $\sigma_G(A) = 1$. Then, generally, the subgroup of G generated by A is not necessarily finite.

To show this, let a be an element of infinite order in a group G, and set $A = \{a\}$. □

Lemma A.44.7. *Let $q \geq 1$ be a rational number, and let $k \geq 1$ be an integer. Then there exists a finite cyclic group G containing a nonempty subset A so that the following conditions hold:*

(1) $\sigma_G(A) = q$.

(2) *k divides $|G|$.*

(3) *A contains the subgroup of G of order k.*

(4) $A^2 = G$.

Proof. Let $q = \frac{m}{n}$, where m and n are integers, and $n \geq 2$. Let $k' \geq m$ be an integer divisible by k. Since $n \geq 2$, we have $k' + m \leq 2k' \leq k'n$. Let G be a cyclic group of order $k'm$ and H be the subgroup of G of order k'. As $|H| + |G/H| = k' + m \leq k'n$, there exists a subset A of G of cardinality $k'n$ containing $H \cup R$, where R is a set of representatives for the cosets in G/H. We have $A^2 \supseteq (H \cup R)^2 \supseteq HR = G$, so $A^2 = G$, and condition (4) holds. It follows that condition (1) also holds. Conditions (2) and (3) are obvious. □

Corollary A.44.8. *For any rational $q \geq 1$ there exist a finite cyclic group G and a nonempty subset A of G so that $\sigma_G(A) = q$.*

We extend the previous corollary as follows:

Proposition A.44.9. *Let $(q_1, q_2, \dots)$ be an infinite sequence of rational numbers ≥ 1. Then there exists a sequence of ordered pairs $(G_n, A_n)_{n \geq 1}$, where G_n are finite cyclic groups and A_n is a nonempty subset of G_n, such that the following conditions hold for all $n \geq 1$:*

(1) $\sigma_{G_n}(A_n) = q_n$.

(2) $(A_n)^2 = G_n$.

(3) *$G_n \subseteq A_{n+1}$, so $G_n \leq G_{n+1}$ and $A_n \subseteq A_{n+1}$.*

Proof. Let $q_0 = 1$. We define the ordered pairs (G_n, A_n) by induction on $n \geq 0$. For $n = 0$, let $G_0 = A_0 = \{1\}$. Fix $n \geq 0$. By Lemma A.44.7, for $k_n = |G_n|$ there exists a finite cyclic group G_{n+1} containing a nonempty subset A_{n+1} so that the following conditions hold:

(i) $\sigma_{G_{n+1}}(A_{n+1}) = q_{n+1}$.

(ii) k_n divides $|G_{n+1}|$.

(iii) A_{n+1} contains the subgroup of G_{n+1} of order k_n.

(iv) $A_{n+1}^2 = G_{n+1}$.

As $|G_n|$ divides $|G_{n+1}|$, we may choose the group G_{n+1} so that it contains G_n. Clearly, the three conditions of the proposition are satisfied by the sequence $\{(G_n, A_n)\}_{n \geq 1}$. □

Remark A.44.10. In view of Remark A.44.2, it follows from Proposition A.44.9 that if $q_1 > q_2 \geq 1$ are rational numbers, then there exists a finite cyclic group G containing nonempty subsets $A_1 \subset A_2$ so that $\sigma_G(A_i) = q_i$ for $i = 1, 2$. Thus $A_1 \subseteq A_2$ is far from implying that $\sigma(A_1) \leq \sigma(A_2)$.

The main purpose of this appendix is to prove under certain assumptions on a finite nonempty subset A of a group G, in particular on the doubling coefficient $\sigma(A)$, the following:

$$H := AA^{-1} = A^{-1}A \text{ is a subgroup of } G, \text{ and } A^2 \text{ is a coset of } H$$

(Theorems A.44.22 and A.44.23 below).

We start with the set AA^{-1}:

Proposition A.44.11. *Let G be a group and let A be a nonempty subset of G such that $AA^{-1} = A^{-1}A$ and $H := AA^{-1}$ is a subgroup of G. Let $L = \langle A \rangle$. Then*

(1) *H is A-invariant, and $H \trianglelefteq L$.*

(2) *$AH = HA$ is a coset of H, so the group L/H is cyclic:*

$$L/H = \langle AH \rangle = \langle aH \rangle \quad \text{for each element } a \in A.$$

Also $AH = H$ if and only if $A \cap H \neq \varnothing$.

(3) *Let k be a nonzero integer so that A^k is a coset of H. Then*

(a) *A^n is a coset of H for all integers n such that $|n| \geq |k|$.*

(b) *$A^{m+n} = A^m A^n$ for all integers m and n such that $|m + n| \geq |k|$.*

Proof. (1) We have for all $a \in A$:

$$aHa^{-1} = a(A^{-1}A)a^{-1} = (aA^{-1})(Aa^{-1}) \subseteq HH = H.$$

Thus H is A-invariant. Similarly, H is A^{-1}-invariant, so $a^{-1}Ha \subseteq H$ for all $a \in A$. Hence $H \subseteq aHa^{-1}$, so $aHa^{-1} = H$ for all $a \in A$. It follows that $A \subseteq \mathrm{N}_L(H)$, so $H \trianglelefteq L$.

(2) We have for all $a, b \in A$: $a^{-1}b \in A^{-1}A = H$, so $aH = bH$. Thus AH is a coset of H in L. The group $L/H = \langle A \rangle / H$ is generated by the coset $AH = aH$ for all $a \in A$.

(3) Since A^k is a coset of H if and only if $(A^k)^{-1} = A^{-k}$ is a coset of H, we may assume that k is positive, thus $k \geq 2$.

(a) Let n be an integer such that $|n| \geq k$. If $n \geq k$, we obtain using Remark A.44.4:

$$A^n = A^{n-k}A^k = A^{n-k}A^k H = A^n H = (AH)^n$$

since AH is a coset of H by (2). Thus $A^n = (AH)^n$ is a coset of H. If $n \leq -k$, then $A^n = (A^{-n})^{-1}$ is a coset of H since $-n \geq k$.

(b) Since A^m is coset of H by (3, a) and since AH is a coset of H by (2), we obtain using Remark A.44.4 that

$$A^m A^n = A^m H A^n = (A^m H)(HA^n) = (AH)^m (AH)^n = (AH)^{m+n}. \qquad \square$$

Remark A.44.12 (cf. Proposition A.44.11). Let A be a finite nonempty subset of a group G. Then the following two conditions are independent even if G is finite:

(1) $AA^{-1} = A^{-1}A$.

(2) AA^{-1} and $A^{-1}A$ are subgroups of G.

Proof. Indeed, to show [(1) $\not\Longrightarrow$ (2)] see Remark A.44.25. To show [(2) $\not\Longrightarrow$ (1)], let a be an element of a (possibly finite) group G and let H be a finite subgroup of G that is not normal in G, thus $a^{-1}Ha \neq H$ for some element $a \in G$. Set $A = Ha$. Then we have $AA^{-1} = (Ha)(a^{-1}H^{-1}) = H$, and $A^{-1}A = a^{-1}Ha \neq H = AA^{-1}$. Hence AA^{-1} and $A^{-1}A$ are subgroups of G, but $AA^{-1} \neq A^{-1}A$. $\square$

Proposition A.44.13. *Let A be a nonempty subset of a group. Then*

(1) $AA^{-1} \subseteq A^{-1}A \iff Aa \cap Ab \neq \varnothing$ *for each two elements* $a, b \in A$.

(2) $A^{-1}A \subseteq AA^{-1} \iff aA \cap bA \neq \varnothing$ *for each two elements* $a, b \in A$.

(3) $A^{-1}A = AA^{-1} \iff Aa \cap Ab \neq \varnothing$ *and* $aA \cap bA \neq \varnothing$ *for each two elements* $a, b \in A$.

Proof. (1) $\Longrightarrow$: Let $a, b \in A$. Then we have $ab^{-1} \in AA^{-1} \subseteq A^{-1}A$. Hence there exist elements $c, d \in A$ so that $ab^{-1} = c^{-1}d$. It follows that $ca = db \in Aa \cap Ab$, so $Aa \cap Ab \neq \varnothing$.

$\Longleftarrow$: Let $h \in AA^{-1}$, thus $h = ab^{-1}$ for some elements $a, b \in A$. By assumption, there are elements $c, d \in A$ so that $ca = db$. Hence $h = c^{-1}d \in A^{-1}A$.

(2) Applying item (1) with A replaced by A^{-1}, we obtain that

$$\begin{aligned} A^{-1}A \subseteq AA^{-1} &\iff (A^{-1}a^{-1}) \cap (A^{-1}b^{-1}) \neq \varnothing \text{ for all } a, b \in A \\ &\iff [(A^{-1}a^{-1}) \cap (A^{-1}b^{-1})]^{-1} \neq \varnothing \text{ for all } a, b \in A. \end{aligned}$$

Since $(A^{-1}a^{-1} \cap A^{-1}b^{-1})^{-1} = aA \cap bA$ for all $a, b \in A$, we obtain the required equivalence.

Statement (3) follows from the previous two items. $\square$

Lemma A.44.14. *Let A be a nonempty subset of a group G. Then the following hold:*

(1) *For $H = AA^{-1}$ we have*

$$\{|Aa \cap Ab| \mid a, b \in A\} = \{|Ah \cap A| \mid h \in H\}.$$

(2) *For $K = A^{-1}A$ we have*

$$\{|aA \cap bA| \mid a, b \in A\} = \{|kA \cap A| \mid k \in K\}.$$

Proof. We prove just item (1). Let $a, b \in A$. Then $h := ab^{-1} \in H$, and

$$(*) \qquad |Aa \cap Ab| = |(Aa \cap Ab)b^{-1})| = |Aab^{-1} \cap A| = |Ah \cap A|.$$

For the converse, let $h \in H$, thus $h = ab^{-1}$ for some elements $a, b \in A$. By $(*)$, we have $|Ah \cap A| = |Aa \cap Ab|$. We conclude that the two above sets are equal. □

Remark A.44.15. We may add a further equivalent condition to each of the items in Proposition A44.13 by using Lemma A44.14. For example,

$$AA^{-1} \subseteq A^{-1}A \iff Ah \cap A \neq \varnothing \text{ for every element } h \in AA^{-1}.$$

Proposition A.44.16. *Let A be a nonempty subset of a group G. Then*

(1) AA^{-1} *is a subgroup of* $G \iff hA \cap kA \neq \varnothing$ *for each two elements* $h, k \in AA^{-1}$.

(2) $A^{-1}A$ *is a subgroup of* $G \iff Ah \cap Ak \neq \varnothing$ *for each two elements* $h, k \in A^{-1}A$.

Proof. We prove just item (1). Let $H = AA^{-1}$.

$\Longrightarrow$: Let h, k be two elements of H. Thus we have $h^{-1}k = ab^{-1}$ for some elements $a, b \in A$. Hence $ha = kb \in hA \cap kA$, so $hA \cap kA \neq \varnothing$.

$\Longleftarrow$: Let h, k be two elements of H. By assumption, there exist elements $a, b \in A$ so that $ha = kb$. Hence $h^{-1}k = ab^{-1} \in H$. It follows that H is a subgroup of G. □

Lemma A.44.17. *Let G be a group and let A be a finite nonempty subset of G such that $AA^{-1} = A^{-1}A$ and $H := AA^{-1}$ is a subgroup of G. Then $|A^2| \leq |H|$. We have equality if and only if A^2 is a coset of H.*

Proof. By Proposition A.44.11(2), AH is a coset of H in G. Hence, by Remark A.44.4, $(AH)^2$ is a coset of H, so

$$|A^2| \leq |A^2H| = |H|.$$

Assume that $|A^2| = |H|$. Since $A^2 \subseteq (AH)^2$ and $|A^2| = |H| = |(AH)^2|$, we conclude that $(AH)^2$ is a coset of H. □

Proposition A.44.18. *Let G be a group and let A be a finite nonempty subset of G such that $AA^{-1} = A^{-1}A$ and $H := AA^{-1}$ is a subgroup of G. Then the following three conditions are equivalent:*

(1) *A^2 is a coset of H in G.*

(2) *For all elements $h \in H$ and $x \in A^2$ we have $hA \cap xA^{-1} \neq \varnothing$.*

(3) *There exists an element $x \in A^2$ so that for all $h \in H$ we have $hA \cap xA^{-1} \neq \varnothing$.*

Proof. (1) $\Longrightarrow$ (2). For $x \in A^2$ we have $H = A^2x^{-1}$, so $H = (A^2x^{-1})^{-1} = xA^{-2}$. Hence, for $h \in H$ there exist elements $a, b \in A$ so that $h = xa^{-1}b^{-1}$. Thus we get $hb = xa^{-1} \in hA \cap xA^{-1}$, so $hA \cap xA^{-1} \neq \varnothing$.

(2) $\Longrightarrow$ (3). Clear.

(3) $\Longrightarrow$ (1). Let $x \in A^2$ so that $hA \cap xA^{-1} \neq \varnothing$ for all $h \in H$. For $h \in H$ there are elements $a, b \in A$ so that $h^{-1}a = xb^{-1}$. Hence $hx = ab \in A^2$. It follows that $Hx \subseteq A^2$, thus $|H| \leq |A^2|$. By Lemma A.44.17, A^2 is a coset of H. □

Lemma A.44.19. *Let A be a nonempty finite subset of a group G. Then there exists an element $x \in A^2$ so that $|A^{-1}x \cap A| \geq \frac{|A|}{\sigma(A)}$.*

Proof. Let x be an element of A^2. The set $A^{-1}x \cap A$ is the set of elements $b \in A$ so that $b = a^{-1}x$, that is, $x = ab$ for some element $a \in A$. Since the element b (for x fixed) determines the ordered pair (a, b), we see that $|A^{-1}x \cap A|$ is equal to the number of ordered pairs $(a, b) \in A \times A$ for which $x = ab$. Choose in A^2 an element x_0 with $m := |A^{-1}x_0 \cap A|$ being maximal. Hence

$$m|A^2| \geq |A|^2,$$

that is,

$$m \geq \frac{|A|^2}{|A^2|} = \frac{|A|}{\sigma(A)},$$

as required. □

Proposition A.44.20. *Let A be a finite nonempty subset of a group G. Assume*

$$|Aa \cap Ab| > \frac{|A|}{2} \quad \textit{and} \quad aA \cap bA \neq \varnothing$$

for all $a, b \in A$. Then $AA^{-1} = A^{-1}A$ is a subgroup of G.

Proof. By Proposition A.44.13(3), we have $AA^{-1} = A^{-1}A$. Let $H = AA^{-1}$.

By Lemma A.44.14, we have

$$|hA \cap A| > \frac{|A|}{2}$$

for all $h \in H$.

Let $h, k \in H$. Thus

$$(hA \cap A) \cap (kA \cap A) \subseteq hA \cap kA.$$

Since $hA \cap A$ and $kA \cap A$ are subsets of A and since $|hA \cap A| > \frac{|A|}{2}$ and $|kA \cap A| > \frac{|A|}{2}$, we obtain that $(hA \cap A) \cap (kA \cap A) \neq \varnothing$. Thus $hA \cap kA \neq \varnothing$. By Proposition A.44.16, H is a subgroup of G. □

Lemma A.44.21. *Let A be a finite nonempty subset of a group G. Then*

(1) $|Aa \cap Ab| \geq (2 - \sigma(A))|A|$ *for all $a, b \in A$.*

Similarly,

(2) $|aA \cap bA| \geq (2 - \sigma(A))|A|$ *for all $a, b \in A$.*

Proof. We prove just item (1). We have for all $a, b \in A$:

$$\begin{aligned} |aA \cap bA| &= |aA| + |bA| - |aA \cup bA| \\ &\geq 2|A| - |A^2| = 2|A| - \sigma(a)|A| = (2 - \sigma(A))|A|. \end{aligned}$$ □

Theorem A.44.22. *Let A be a finite nonempty subset of a group G such that $\sigma(A) < 2$. Then $AA^{-1} = A^{-1}A$. Moreover, for $H = AA^{-1}$ we have:*

(1) *If*

$$(\geq) \qquad |aA \cap bA| \geq \frac{|A|}{2} \quad \text{for all } a, b \in A$$

and if H is a subgroup of G, then A^2 is a coset of H.

(2) *If*

$$|aA \cap bA| > \frac{|A|}{2} \quad \text{for all } a, b \in A,$$

then H is a subgroup of G, and A^2 is a coset of H.

Proof. By Lemma A.44.21, for $a, b \in A$ we have $|Aa \cap Ab| > 0$, so $Aa \cap Ab \neq \varnothing$; similarly, $aA \cap bA \neq \varnothing$. By Proposition A.44.13(3), we obtain that $AA^{-1} = A^{-1}A$.

(1) Now assume that H is a subgroup of G and that condition $(\geq)$ holds.

By Lemma A.44.19, there exists an element $x \in A^2$ so that

$$|A^{-1}x \cap A| \geq \frac{|A|}{\sigma(A)} > \frac{|A|}{2}.$$

Let $h \in H = A^{-1}A$. By Lemma A.44.14, we have $|hA \cap A| \geq \frac{|A|}{2}$. Hence

$$hA \cap A^{-1}x \supseteq (hA \cap A) \cap (A^{-1}x \cap A) \neq \varnothing.$$

By Proposition A.44.18, it follows that A^2 is a coset of H.

(2) As shown at the beginning of the proof, we have $Aa \cap Ab \neq \varnothing$ for all $a, b \in A$. By Proposition A44.20, H is a subgroup of G. Hence, by (1), A^2 is a coset of H. □

Theorem A.44.23. *Let A be a finite nonempty subset of a group G, and let $H = AA^{-1}$. Then the following hold:*

(1) *If $\sigma(A) < 1.5$, then $AA^{-1} = A^{-1}A$ is a subgroup of G and A^2 is a coset of H.*

(2) *If $\sigma(A) = 1.5$ and if $H = AA^{-1}$ is a subgroup of G, then $A^{-1} = A^{-1}A$ and A^2 is a coset of H.*

Proof. (1) By Lemma A.44.21, we have $|Aa \cap Ab| > \frac{|A|}{2}$ for all $a, b \in A$. In view of Theorem A.44.22, $H = AA^{-1} = A^{-1}A$ is a subgroup of G, and A^2 is a coset of H.

(2) By Theorem A.44.22, we have $AA^{-1} = A^{-1}A$, and by Lemma A.44.21, we get $|aA \cap bA| \geq \frac{|A|}{2}$ for all $a, b \in A$. Hence A^2 is a coset of H by Theorem A.44.22. □

Example A.44.24. Let x be an element of order 3 in a group G, and let $A = \{x, x^2\}$. Then $A^2 = AA^{-1} = A^{-1}A = \{1, x, x^2\}$ is a subgroup of G, $|aA \cap bA| = 1 = \frac{|A|}{2}$ for all distinct $a, b \in A$, and $\sigma(A) = 1.5$. In particular, all the assumptions in Theorems A.44.22(2) and A.44.23(2) are satisfied.

Remark A.44.25 ([1, Remark 1]). The constant 1.5 in Theorem A.44.23(1) is sharp; if $A = \{1, x\}$, where x is an element of order larger than 2, then we have $\sigma(A) = 1.5$, but $AA^{-1} = A^{-1}A$ is not a subgroup of G.

Corollary A.44.26. *Suppose that A is a subset of a finite group G so that $|A| > \frac{2}{3}|G|$. Then $AA^{-1} = A^{-1}A$ is a subgroup of G and A^2 is a coset of AA^{-1}.*

Problem 1. Let A be a finite nonempty subset of a group G. Assume

$$|aA \cap bA| > \frac{|A|}{2} \quad \text{and} \quad |Aa \cap Ab| > \frac{|A|}{2}$$

for all $a, b \in A$. Estimate $|A^2|$. Is it true that there is a constant σ_0 (independent of A) such that $|A^2| < \sigma_0|A|$?

Note that $AA^{-1} = A^{-1}A$ is a subgroup of G by Proposition A44.20.

Problem 2. Let A be a nonempty finite subset of a group G. Describe the situation if $\sigma_G(A) = 1.5$ (cf. Theorem A.44.23(2), Example A.44.24 and Remark A.44.25 above).

References

[1] An elementary noncommutative Freiman theorem, Terence Tao's blog, http://terrytao.wordpress.com/2009/11/10/an-elementary-non-commutative-freiman-theorem/.

[2] Y. O. Hamidoune, Two inverse results, http://arxiv.org/abs/1006.5074.

Research problems and themes III

What we know is not much. What we do not know is immense.

Pierre-Simon Laplace (1749–1827), said to be his last words.

Quoted in Mark Ronan, *Symmetry and the Monster*, Oxford University Press, 2006.

A tremendous effort has been made by mathematicians for more than a century to clear up the chaos in group theory. Still, we cannot answer some of the simplest questions.

Richard Brauer

(see Michael Artin, *Algebra*, Prentice Hall, Englewood Cliffs, 1991.)

The important thing is not to stop questioning. Curiosity has its own reason for existing.

Albert Einstein

Imagination is more important than knowledge.

Albert Einstein

The only real valuable thing is intuition.

Albert Einstein

This is the third part of the list written by the first author (however, some problems were known before). Main aim of this and the two previous lists is to inspire development of methods of finite p-group theory. It is impossible to say from the start whether a given problem is important or not. A part of this list was written before publication of the first two volumes of the book.

Most problems are motivated by the results proved in the book.

Approximately 60 problems from the first two lists are solved. A number of problems from this list are also solved by the second author. All solutions are included in the book.

Many items present themes for investigations. The reader is suggested to consider also their variants.

In what follows G is always a p-group. The rank of G is equal to $\mathrm{d}(G)$, the minimal number of generators of G. If G is of maximal class, then G_1 is its fundamental subgroup. Next, m, n, k, e, s, t are positive integers.

I am indebted to Zvonimir Janko and Avinoam Mann for numerous constructive and fruitful discussions which allow me to improve this list considerably (indeed, they sent me hundreds letters with critics, comments, suggestions and other useful information). They read the list word for word and made numerous corrections and suggestions. Besides, Janko is a very active solver of problems contained in the book.

1401. Study the irregular (two-generator irregular) p-groups with absolutely regular derived subgroup. (Compare with Appendix 8. See Theorem 9.8(c).)

1402. Let G be a 2-group such that $\Phi(G)$ has no G-invariant subgroups isomorphic to E_8. Describe all possible structures of $\Phi(G)$. The same problem arises for a G-invariant subgroup $N < \Phi(G)$. Is it possible to get an upper estimate of $\mathrm{d}(N)$? (If $N = G$, then $\mathrm{d}(G) \leq 4$ by MacWilliams' result; see §50.)

1403. Describe the structure of a Sylow p-subgroup of the holomorph of an abelian p-group of rank 2.

1404. Describe the 2-groups G all of whose nonabelian maximal subgroups M are of the form $M = N * \mathrm{Z}(M)$, where N is (i) of maximal class, (ii) metacyclic, (iii) minimal nonabelian (three problems).

1405. Classify the groups H of order $\leq 2^5$ isomorphic to a G-invariant subgroup of $\Phi(G)$ for some 2-group G. (See §85.)

1406. Study the special p-groups isomorphic to a G-invariant subgroup of $\Phi(G)$ for some p-group G. (See §60.)

1407. Describe the metacyclic (special) p-groups M isomorphic to a Sylow p-subgroup of $\mathrm{Aut}(G)$ for some p-group G (two problems).

1408. Denote by $\mathcal{R}(G)$ the set of all representation groups of a p-group G. Find a condition which is sufficient for existence of a member in $\mathcal{R}(G)$ with trivial Schur multiplier.

1409. Classify the p-groups G of class 2 such that $p|G|$ does not divide $|\mathrm{Aut}(G)|$.

1410. Study the p-groups G such that all members of the set Γ_i are isomorphic (pairwise nonisomorphic) for some fixed $i \in \{1, \ldots, \mathrm{d}(G) - 1\}$. Is it true that if this holds for all such i, then $\mathrm{d}(G)$ is bounded? (See #2115.)

1411. Study the p-groups G such that (i) $\mathrm{Aut}(G)$ acts transitively on the set of maximal abelian subgroups of G (as Mann has noticed, there are a lot of such groups of class 2), (ii) all maximal abelian subgroups of G are isomorphic, (iii) all maximal abelian subgroups are normal in G, (iv) all nonnormal maximal abelian subgroups of G are conjugate.

1412. Classify the p-groups all of whose proper nonabelian subgroups have (i) cyclic centers, (ii) noncyclic centers. (According to Janko's letter at May 20, 2008, part (i) is solved for $p = 2$.)

1413 (Mann). Study the p-groups G such that $\mathrm{Aut}(G)$ acts transitively on the set (i) of cyclic subgroups of maximal order, (ii) nonnormal cyclic subgroups.

1414. Study the p-groups such that the kernels of all their nonlinear irreducible characters are characteristic.

1415. Study the p-groups all of whose nonnormal subgroups are Dedekindian.

1416. Suppose that there is a p-admissible Hall chain in a p-group H (see §88). Let $H \lhd G$, where G is a p-group. Find a sufficient condition for existence of a p-admissible Hall chain in H (all of whose members are G-invariant).

1417. Classify the 2-groups which has no 2-admissible Hall chain. (See §24.)

1418. Let E be a proper special subgroup of a p-group G. Study the structure of G if, whenever $E < E_1 \leq G$ with $|E_1 : E| = p$, then (i) E_1 is special, (ii) $\Omega_1(E_1) = E_1$ (two problems).

1419. Let $H \lhd G$. Given k, a chain $H = H_0 > H_1 > \cdots > H_n = \{1\}$ of G-invariant subgroups of H is said to be a lower k-admissible chain in H provided (i) H_{i-1}/H_i is of order $\leq p^k$ and exponent p and (ii) whenever $|H/H_i| < p^{ki}$, then $H_i = \mathfrak{V}_i(H)$. Is it true that whenever H is regular, it possesses a lower k-admissible Hall chain?

1420 (Old problem). Study the p-groups G such that whenever A is not normal in G, then $|\mathrm{N}_G(A)/\mathrm{C}_G(A)| = |\mathrm{Aut}(A)|_p$.

1421. Classify the 2-groups G satisfying one of the following conditions: (i) $\Omega_1(G) = D_1 \times D_2$ with dihedral groups D_1, D_2, (ii) $\Omega_2^*(G) = Q_1 \times Q_2$ with generalized quaternion groups Q_1, Q_2 (here $\Omega_n^*(G) = \langle x \in G \mid o(x) = p^n \rangle$).

1422. Classify the p-groups G such that whenever A and B are distinct noncyclic subgroups of G of order p^2 (of order p^3), then $A \cap B > \{1\}$ (two problems).

1423. Classify the special p-groups G satisfying $\Omega_1(G) = \mathrm{Z}(G) = \mathfrak{V}_1(G)$. (Sylow 2-subgroups of the simple Suzuki groups $\mathrm{Sz}(2^{2m+1})$ satisfy this condition.)

1424. Let G be not of maximal class and let $M < G$ with $|G : M| > p^k$. Is it true that the number of subgroups of G of order $p^k|M|$ that are of maximal class is a multiple of p? (See Proposition 13.18(b).)

1425. Study the p-groups G such that (i) $\Phi(\Phi(G)) = \mathfrak{V}_2(G)$, (ii) $\Phi(\Phi(G)) = \mathfrak{V}^2(G)$ $(= \mathfrak{V}_1(\mathfrak{V}_1(G)))$ (two problems).

1426. Given n, does there exist a p-group G such that the series $\{1\} < \Omega_1(G) < \Omega_2(G) < \cdots < G$ has length n and all factors of this series are irregular?

1427. Given $n > 1$, does there exist a p-group G of exponent p^n such that the following holds: $\exp(\mathfrak{V}_i(G)/\mathfrak{V}_{i+1}(G)) > p$ for $i = 1, \ldots, n-1$?

1428. Study the p-groups in which the number of subgroups of maximal class and order p^p is not a multiple of p. (See Theorem 13.6.)

1429. Classify the p-groups G such that $\Omega_2^*(G)$ is extraspecial. (This is solved by Janko; see Theorems 83.2 and 83.3.)

1430. Classify the 2-groups G such that (i) $\Omega_2^*(G) < G$ is metacyclic. (This is solved in §86. The similar problem is fairly easy for $p > 2$.) (ii) $\Omega_k^*(G)$, $k > 2$, is metacyclic.

1431. Classify the p-groups G such that (i) $\Omega_2(G) = M \times E$, (ii) $\Omega_2^*(G) = M \times E$, where M is of maximal class and E is elementary abelian.

1432. Study the nonmetacyclic p-groups G such that $\mathrm{N}_G(Z)$ is metacyclic for all maximal cyclic $Z < G$.

1433. Study the irregular p-groups G such that for any $x, y \in G$ there is $z \in G'$ such that $(xy)^p = x^p y^p z^p$.

1434. Study the nonabelian p-groups G such that $M' = G'$ for all $M \in \Gamma_1$.[1]

1435. Study the p-groups containing a cyclic soft subgroup Z. (See §130. This problem is open even if $|Z| = p^2$.)

1436. Study the p-groups G admitting an automorphism group A of order p^3 such that $|\mathrm{C}_G(A)| = p$ (for every p there are five problems).

1437. Study the p-groups G satisfying $|G/\mathrm{K}_4(G)| = p^4$. (If $p = 3$, then G is of maximal class, by Theorem 9.7.)

1438. Let H be a p-group not isomorphic to the Frattini subgroup of all p-groups. Does there exist a p-group G such that $\Phi(G) = U \times V$, where $U \cong V \cong H$?

1439. Given $n > 2$, study the p-groups G all of whose nonabelian subgroups of order p^n are isomorphic.

1440. Study the p-groups with only one maximal subgroup of rank > 2.

1441. Suppose that any two minimal nonabelian subgroups of G generate a subgroup of class 2. Is it true that $\mathrm{cl}(G)$ is bounded?

1442. Study the p-groups $G = \Omega_1(G)$, $p > 2$, in which every two noncommuting elements of order p generate a subgroup of order p^3.

[1] We must have $\mathrm{d}(G) > 2$. Assume that $\mathrm{d}(G) = 2$. Take in G' a G-invariant subgroup R of index p; then G/R is minimal nonabelian by Lemma 65.2(a). In that case, if $M \in \Gamma_1$, then $M' \leq R < G'$, a contradiction.

1443. Classify the p-groups G such that whenever $E < G$ is nonnormal (nonnormal abelian), then G/E^G is cyclic (two problems).

1444 (P. Hall). Given k, study the p-groups of derived length k that have minimal possible order. (See Appendix 6.)

1445. Classify the p-groups containing a maximal subgroup which is (i) minimal nonabelian, (ii) a U_2-subgroup, $p = 2$ (see §17, 18), (iii) an L_p-subgroup.

1446. Classify the p-groups $G = \Omega_1(G)$, $p > 2$, containing a normal subgroup R of order p^p and exponent p such that $\langle x, R\rangle$ is of maximal class for all $x \in G - R$ of order p. (Compare with Exercise 13.10(a).)

1447. Study the p-groups G such that $G/\mathrm{Z}(G)$ is minimal nonabelian (minimal nonmetacyclic, special).

1448. Study the p-groups of exponent p^e all of whose maximal metacyclic subgroups have the same order p^{2e}.

1449. Study the p-groups containing exactly one normal subgroup of index p^3. (Example: $G \in \mathrm{Syl}_2(\mathrm{Sz}(2^3))$.)

1450. Given k, find the minimal $n = n(k)$ such that there is a group G of order p^n such that whenever H is a group (a metacyclic group, an abelian group) of order $\leq p^k$, there exists in G a subgroup isomorphic to H (three problems).

1451. Does there exist a two-generator p-group G of exponent p^2, $p > 2$, such that $\mathfrak{V}_1(G)$ $(\Phi(\Phi(G)))$ is irregular?

1452. Let $M_1, \ldots, M_n$ be irregular p-groups of maximal class. Consider the central product $G = M_1 * \cdots * M_n$ with amalgamated centers. Describe all central decompositions of G in centrally indecomposable factors.

1453. Given n and e, study the regular p-groups G, $p > 2$, of class n and exponent p^e with $|\mathrm{Z}(G)| = p$.

1454. Let p, q be primes, $q \mid p - 1$, let $W = Q \cdot G$ be a (supersolvable, by [BZ, Exercise 3.19]) semidirect product with $Q \in \mathrm{Syl}_q(W)$ of order q and nonabelian kernel $G \in \mathrm{Syl}_p(W)$. Describe the structure of G (i) all of whose proper Q-invariant subgroups are abelian, (ii) provided G has no Q-invariant subgroup $\cong \mathrm{E}_{p^3}$.

1455. Study the subgroup structure of a p-group containing a self-centralizing abelian subgroup of order (i) p^3, (ii) p^4. (iii) Study the p-groups G containing an abelian subgroup A of type (p^2, p) which is a maximal abelian subgroup of G of exponent p^2. (See §§51, 77.)

1456. Study the p-groups all of whose maximal subgroups, except one, have (i) the same exponent, (ii) cyclic centers (two problems).

1457. Study the p-groups G such that whenever $A, B < G$ are nonnormal of same order, then (i) A and B are conjugate, (ii) $A \cong B$, (iii) $A \cap B$ is cyclic (three problems).

1458. Classify the p-groups all of whose nonnormal subgroups are (i) metacyclic, (ii) either absolutely regular or generated by elements of order p.

1459. Classify the p-groups all of whose nonnormal subgroups have order $\leq p^2$. (See Theorem 1.25.)

1460. Study the groups of exponent p^2 all of whose minimal nonabelian subgroups are metacyclic of order p^4.

1461. Study the p-groups all of whose metacyclic subgroups either of order p^4 or have a cyclic subgroup of index p.

1462. Classify the p-groups all of whose $\mathcal{A}_2$-subgroups are metacyclic. Does there exist in such a group a nonmetacyclic $\mathcal{A}_1$-subgroup?

1463. Study the p-groups satisfying (i) $\mathrm{H}_p(G) \in \{\Phi(G), \mho_1(G)\}$, (ii) $\mathrm{H}_p(G)$ is abelian, where $\mathrm{H}_p(G) = \langle x \in G \mid o(x) > p \rangle$ is the Hughes subgroup of G.

1464. Let $H \lhd G$, where G is a 2-group and let $\mathrm{E}_{16} < H$. Study the structure of H if it has no G-invariant subgroup $\cong \mathrm{E}_8$.

1465. Is it true that the order of a 2-group of rank 3 all of whose maximal subgroups are of rank 2 is bounded? (E. restani has obtained a negative answer to this question; see §113.)

1466. Estimate the number of groups G of order p^n and (i) of exponent p, (ii) absolutely regular, (iii) regular, (iv) irregular with $|G/\mho_1(G)| = p^p$, (v) $|G'| = p^2$, (vi) $|\Phi(G)| = p^2$, (vii) with cyclic center, (viii) with $G' = \Phi(G)$, (ix) with special Frattini subgroup (derived subgroup), (x) $\mathrm{Aut}(G)$ is not a p-group, (xi) $\Omega_n(G) = G$, (xii) without normal subgroups $\cong \mathrm{E}_{p^4}$, (xiii) $\Phi(G)$ is cyclic, (xiv) G' is cyclic, (xv) G contains an abelian subgroup of index p, (xvi) G has a metacyclic subgroup of index p.

1467. Classify the special p-groups G all of whose nonabelian epimorphic images are special.

1468. Study the p-groups G containing a subgroup H such that whenever $L < H$ is maximal cyclic (maximal abelian), then L is maximal cyclic (maximal abelian) in G.

1469. Study the E_p-groups (= equilibrated p-groups) containing a nonabelian subgroup of order p^3 and exponent p^2. (See Exercise 110.17.)

1470. Let G and H be p-groups. Let $\mathcal{MA}^n(G)$ be the set of all $\mathcal{A}_n$- subgroups of G. Suppose that there are one-to-one correspondences between the sets $\mathcal{MA}^n(G)$ and $\mathcal{MA}^n(H)$, $n = 1, 2$, such that the corresponding subgroups are isomorphic. Is it true that $G \cong H$?

1471. Classify the p-groups H of exponent $p > 2$ such that whenever G of exponent p is an extension of a group R of order p by H, then R is a direct factor of G.[2]

1472. Given $n > 1$, study the p-groups G such that $\mathrm{Z}_n(G)$ ($\Omega_n(G)$, $\Omega_n^*(G)$) is minimal nonabelian (three problems).

1473. Suppose that a p-group G, $p > 2$, contains a proper subgroup of maximal class and order $p^n > p^p$ and let $\alpha \in \mathrm{Aut}(G)$ be of order 2. Study the structure of G provided it has no α-invariant subgroup of maximal class and order p^n.

1474. Suppose that G is a nonabelian group of order p^m, α is an involutory automorphism of G and $n \in \{3, \ldots, m-1\}$. Study the structure of G provided it has no two-generator α-invariant subgroup of order p^n. Consider the case $\exp(G) = p$ in detail.

1475. Study the p-groups of exponent p^e that have no minimal nonabelian subgroups of exponent p^e. (For $p = 2$, see §95. See also Lemma 57.1.)

1476 (Old problem). Study the p-groups G such that whenever (i) $R \lhd G$, there is $H < G$ with $H \cong G/R$, (ii) $H < G$, there is $R \lhd G$ with $H \cong G/R$.

1477. Study the p-groups G with a nonabelian Frattini subgroup of order p^4. (For $p = 2$, see §85.)

1478. Study the p-groups G such that whenever $N \lhd G$ is maximal with nonabelian G/N, then N is cyclic.

1479. Study the p-groups G such that $\Phi(G) \cong \mathrm{E}_{p^2}$. (For $p = 2$, see Proposition 4.9.) Describe the orders of maximal abelian subgroups in terms of $\mathrm{d}(G)$.

1480. Classify the p-groups G with normal homocyclic subgroup H of index p^2.

1481. Study the 2-groups with metacyclic Frattini subgroup (derived subgroup). Consider the case $\mathrm{d}(G) = 2$ in most possible detail.

1482. Study the p-groups G with a special Frattini subgroup (derived subgroup). In case $\mathrm{d}(G) = 2$, find all possible parameters of $\Phi(G)$. (See §60, Theorem D(a).)

1483. Study the p-groups G with nonabelian $\Phi(G)$ and $\mathrm{Z}(\Phi(G)) \cong \mathrm{E}_{p^2}$.

1484. Classify the p-groups G such that $\mathrm{C}_G(H) < H$ for all nonabelian $H \leq G$.

[2]Solution by Mann (letter at 14/08/08). Let $d = \mathrm{d}(H)$ be the minimal number of generators of H, and write $H = F/N$, where F is a free group of rank d. There is a unique normal subgroup K of F, such that F/K is finite of exponent p, and if S is a normal subgroup of F such that F/S is finite of exponent p, then $K \leq S$. This is obvious from Kostrikin's solution of the Restricted Burnside Problem for exponent p; K is the intersection of all subgroups like S. Now suppose that $N \neq K$, and let $T \lhd F$, $K \leq T < N$, and $|N : T| = p$. Take $G = F/T$. Then G is an extension of H of the type that you want, and G is not a direct product of H and a group of order p because $\mathrm{d}(G) = \mathrm{d}(H)$. Thus the only groups satisfying your assumptions are the finite groups that are of maximal order among the ones of exponent p and d generators. There is [exactly] one such group for each d. All representation groups of such G have exponent $> p$.

1485. Study the p-groups whose Frattini subgroups are abelian of type (p^2, p).

1486. Study the p-groups all of whose nonnormal subgroups are either abelian of rank 2 or of maximal class. (See §117.)

1487. Classify the irregular L_p-groups. (See §§17, 18).

1488. Let G be a p-group, $p > 2$, and $\alpha \in \mathrm{Aut}(G)$ of order 2. Study the structure of G provided all members of the set Γ_1 are not α-invariant.

1489. Study the p-groups G in which the intersection of all minimal nonabelian subgroups is not contained in $\mathrm{Z}(G)$.

1490. Let M be a proper metacyclic subgroup of a 2-group G. Study the structure of G if, whenever $M < H \leq G$ is such that $|H : M| = 2$, then $\Omega_1(H) = H$.

1491. Does there exist a p-group G which is neither abelian nor minimal nonabelian all of whose nonabelian maximal subgroups are nontrivial direct products of two subgroups but G is not a nontrivial direct product?

1492. Study a p-groups $G = E_1E_2$, where $E_1, E_2 < G$ are extraspecial (special) and $E_1 \cap E_2 = \mathrm{Z}(E_1)$.

1493. Study the group $\mathrm{Aut}(G)$, where G is a special p-group with derived subgroup of order p^2.

1494. Study the nonabelian p-groups G generated by $[\frac{1}{2}(\mathrm{d}(G) + 1)]$ minimal nonabelian subgroups. (See §135.)

1495. Let $\alpha \in \mathrm{Aut}(G)$ be of order 2 and $p > 2$. Study the structure of an irregular p-group G if it has no α-invariant normal subgroup of order p^p and exponent p. (Note that $\langle\alpha\rangle \cdot G$ is supersolvable. See §31 and [BZ, Exercise 3.19].)

1496. Classify the p-groups G with $\mathrm{d}(G) > 2$ containing $\leq p$ maximal subgroups which are neither abelian nor metacyclic. (See §87.)

1497. Study the p-groups containing a special subgroup S such that $\mathrm{C}_G(x) \leq S$ for all $x \in S - \mathrm{Z}(G)$.

1498. Classify the p-groups G of order p^m with (i) $\alpha_1(G) = p^{\mathrm{d}(G)-1}$, (ii) $\alpha_1(G) = p^{m-2}$. (iii) Does there exist a p-group G of order p^m with $\alpha_1(G) \geq p^m$? (See §76.)

1499. Study the p-groups such that whenever $A, B < G$ are not conjugate, then A and B are permutable.

1500. Study the $\mathcal{A}_n$-groups with minimal possible $\alpha_1(G)$. (See §76.)

1501. Classify the p-groups all of whose noncyclic abelian subgroups are contained in minimal nonabelian subgroups. (All 2-groups of maximal class satisfy this condition. See #860.)

1502. Find all possible values of $\alpha_1(G) \pmod p$ and $c_2(G) \pmod{p^3}$ for special p-groups G. (See Example 76.1.)

1503. Study the nonabelian p-groups G such that whenever $A < B \leq G$ and B is nonabelian, then $A' < B'$.[3]

1504. Study the p-groups G all of whose subgroups of index p^2 are two-generator. (See §§70, 113.)

1505. Let a p-group G be of the form $G = A \times C$, where A is an $\mathcal{A}_1$-group and $C > \{1\}$ is cyclic. Express $\alpha_1(G)$ and $\alpha_2(G)$ in terms of A and C.

1506. Study the p-groups G such that whenever $C < G$ is nonnormal cyclic, then (i) $\exp(C^G) = |C|$, (ii) $|C^G| \leq p^2|C|$ (two problems).

1507. Study the p-groups G such that whenever $A < G$ is minimal nonabelian and $x \in G - A$, then $|A : C_A(x)| \leq p$ ($|A : N_A(\langle x\rangle)| \leq p$). (Compare with Exercise 2.7.)

1508. Study the $\mathcal{A}_{n+1}$-groups G, $n > 1$, such that $\alpha_n(G) = 1$. (See #895.[4])

1509. Study the p-groups G such that $d(H) > d(G)$ for all $H \in \Gamma_1$.

1510. Study the p-groups G all of whose cyclic subgroups not contained in $\Phi(G)$ (i) are complemented, (ii) have normal complements. (Example: D_{2^n}.)

1511. Let $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3\rangle$. Describe the maximal abelian subgroups of the group $G = H_1 * \cdots * H_n$ of order 2^{2n+2}, where $H_1, \ldots, H_n \cong \mathcal{H}_2$.

1512. Study the p-groups such that whenever $C < G$ is maximal cyclic, then every subgroup $B > C$ of order (i) $p|C|$ is abelian, (ii) $p^2|C|$ is metacyclic (two problems).

1513. Denoting by $\mathcal{J}_n$ the set of p-groups all of whose subgroups of index p^n are irregular, estimate $\min\{|G| \mid G \in \mathcal{J}_n\}$.

1514. Is it true that the set of pairs $H < G$ in #211 is finite? (#211 was solved by B. Sambale and Li Tianze [Li4] independently; see §126.)

1515. Estimate the minimal n (if it exists) such that whenever G has a subgroup of order p^n and exponent p, then there is in G a normal subgroup of order p^{p+1} and exponent p.

1516. Classify the groups of exponent p all of whose subgroups of order $> p^3$ are decomposable in a nontrivial direct product.

1517. Study the p-groups all of whose nonnormal subgroups have exponent p.

---

[3] All p-groups of maximal class with an abelian subgroup of index p satisfy this condition. In case $\exp(G) = p$, it is easy to show that G is of maximal class with an abelian subgroup of index p. See Exercise 13.10(a) and Lemma 124.27.

[4] An answer is not known even for $n = 2$. However, if A is a unique $\mathcal{A}_2$-subgroup of G and $A \not\leq \Phi(G)$, then $d(G) \leq 3$ since there is an $\mathcal{A}_1$-subgroup $B \in \Gamma_1$.

1518. Classify the 2-groups G such that whenever $\chi \in \mathrm{Irr}_1(G)$, then χ is the unique faithful irreducible character of the quotient group $G/\ker(\chi)$.

1519. Let $H < G$ be of exponent p such that $|H|$ is as large as possible. Study the structure of G provided $Z \cap H = \{1\}$ for every cyclic $Z < G$ of order $> p$.

1520. Classify the p-groups all of whose nonnormal cyclic subgroups of same order are conjugate.

1521. Classify the p-groups with exactly two conjugate classes of nonnormal cyclic subgroups. (See §§59, 96.)

1522. Classify the p-groups that are not generated by noncyclic abelian subgroups. (The semidihedral group SD_{2^n} satisfies this condition.)

1523. Study the p-groups G all of whose minimal nonabelian subgroups are (i) conjugate in $\mathrm{Hol}(G)$, the holomorph of G, (ii) isomorphic.

1524. Study the p-groups such that for all nonnormal noncyclic subgroup $A < G$ one has (i) $\mathrm{cl}(\mathrm{N}_G(A)) = \mathrm{cl}(A)$, (ii) $\mathrm{cl}(\mathrm{N}_G(A)) > \mathrm{cl}(A)$, (iii) $\mathrm{d}(\mathrm{N}_G(A)) = \mathrm{d}(A)$.

1525. Classify the p-groups all of whose proper subgroups which are neither abelian nor metacyclic (neither abelian nor minimal nonabelian) are generated by elements of order p (two problems).

1526. Study the p-groups all of whose maximal subgroups are either two-generator or have cyclic derived subgroups. (See §§113, 139.)

1527. Study the p-groups (regular p-groups) with two conjugate classes of subgroups of order p^p and exponent p.

1528. Study the p-groups G with $\mathrm{d}(G) > 2$ such that whenever $A < G$ is minimal nonabelian, then $|A\Phi(G) : \Phi(G)| \leq p$. (See #1494.)

1529. Study the p-groups all of whose metacyclic subgroups are abelian.

1530. Study the p-groups $G = \Omega_1(G)$ in which exactly one nonabelian maximal subgroup, say H, satisfies $\Omega_1(H) = H$. (See §30.)

1531. Study the p-groups G all of whose nonlinear irreducible characters are induced from the same proper subgroup (from G').

1532. Study the groups of exponent p all of whose maximal subgroups, except one, are two-generator.

1533. Study the p-groups all of whose nonlinear irreducible characters have cyclic kernels.

1534. Classify the p-groups G of exponent p containing only one normal subgroup D such that G/D is of maximal class and order p^p.

1535. Study the p-groups (i) in which any maximal subgroup is either abelian or minimal nonabelian or metacyclic, (ii) containing only one maximal subgroup which is neither abelian nor minimal nonabelian nor metacyclic.

1536. Estimate $\delta(G)$ (see #1538), where G is a p-group given by defined relations. Consider the metacyclic p-groups in detail.

1537. Classify the two-generator p-groups G such that $\Phi(G)$ is abelian of rank 2.

1538. Let $\delta(X)$ be the minimal degree of a faithful representation of a group X by permutations. Classify the p-groups G such that (i) $\delta(G) = \exp(G)$, (ii) $\delta(G) = \delta(M)$ for some $M < G$. (Examples: $G \in \{\Sigma_{p^2}, \mathrm{D}_{2^n}\}$.)

1539. Classify the p-groups G subjecting $|\mathrm{Aut}(G) : \mathrm{Inn}(G)| = p$.

1540. Study the p-groups G such that $|\mathrm{N}_G(A) : A| = p$ for all maximal nonnormal abelian subgroups $A < G$.

1541. Classify the p-groups G such that $G \cong P$, where $P \in \mathrm{Syl}_p(\mathrm{Aut}(G))$. Is it true that for such G we must have $p = 2$?[5]

1542. Let $A \lhd G$ be abelian. Study the structure of G provided all subgroups of G that contain A as a subgroup of index p are minimal nonabelian.

1543. Study the p-groups G such that the centralizers of all noncyclic subgroups of G are G-invariant.

1544. Study the 2-groups containing two distinct maximal subgroups which are Dedekindian.

1545. Study the p-groups G such that $\mathrm{Inn}(G)$ is a direct factor of $\mathrm{Aut}(G)$. (See #1906.)

1546. Study the p-groups G such that whenever $A, B < G$ are distinct of same order (nonincident), then $A \cap B \lhd \langle A, B\rangle$.

1547. Classify the p-groups G such that for any $D \lhd G$ of index p^{p+1} the quotient group G/D is of maximal class. (If $p = 2$, then G is of maximal class by Taussky's theorem. See Theorems 9.7 and 12.6.)

1548. Classify the p-groups all of whose nonnormal nonabelian subgroups are minimal nonabelian. Consider the case $\exp(G) = p$ in most possible detail.

1549. Classify the $\mathcal{A}_2$-groups that are Φ-subgroups of some p-groups.

1550. Study the p-groups G such that (i) $|H : H_G| \le p$ for all $H < G$ (for all cyclic H, for all abelian H), (ii) $|H/H_G|$ is cyclic for all $H \le G$. See #1308.

[5]The following partial case of this problem is due to Mann: classify the p-groups G that satisfy $\mathrm{Aut}(G) \cong G$. (Mann's problem is not solved yet. The dihedral group D_8 is the unique known prime power group satisfying this condition.)

1551. Classify the p-groups G such that whenever $A < G$ is minimal nonabelian, then all maximal subgroups of A are G-invariant.

1552. Study the p-groups G such that $A \cap \mathrm{Z}(G) = \mathrm{Z}(A)$ for all nonabelian $A < G$.

1553. Study the p-groups G of exponent p^2 that have no minimal nonabelian subgroup of order $> p^3$. (For $p = 2$, see §90.)

1554. (i) (Old problem) Study the 2-groups G generated by three involutions. (For $\exp(G) = 4$, see §61.) Does there exist a minimal nonabelian 2-group that is not involved in G? (ii) Study the Φ-groups generated by three involutions. (iii) Study the Φ-groups generated by involutions.

1555. Classify the p-groups covered by (i) special subgroups, (ii) subgroups of class 2.

1556. Study the p-groups all of whose outer p-automorphisms have order p.

1557. Study the p-groups all of whose maximal metacyclic subgroups are (i) normal, (ii) nonnormal (two problems).

1558 (Inspired by papers of O. Schmidt). Classify the p-groups G (i) with exactly two (three) sizes of classes of conjugate subgroups, (ii) which have no three nonnormal subgroups of pairwise distinct orders. (See §§96, 112.)

1559. Given $n > 1$, construct an $\mathcal{A}_n$-group G such that G/R is minimal nonabelian for some $R \lhd G$ of order p.

1560. Study the groups G of exponent p such that there is no p-group Γ of exponent p satisfying the following condition: Γ has no $R \leq \Gamma' \cap \mathrm{Z}(\Gamma)$ of order p with $\Gamma/R \cong G$. (Such G exist; see footnote to #1471.)

1561. Study the p-groups G such that $\exp(G/\mathcal{M}(G)) = p$, where $\mathcal{M}(G) = \langle x \in G \mid \mathrm{C}_G(x) = \mathrm{C}_G(x^p) \rangle$ is the Mann subgroup of G (see #1037).

1562. Study the p-groups G with $\mathrm{d}(G) > 2$ containing a nonabelian $F \in \Gamma_1$ such that $F \cap H$ is abelian for all $H \in \Gamma_1 - \{F\}$.

1563. Study the p-groups G such that whenever $\chi, \tau \in \mathrm{Irr}_1(G)$ with $\chi(1) = \tau(1)$, then $|\mathrm{T}_\chi| = |\mathrm{T}_\tau$. Here T_χ os the number of zeros of χ.

1564. (i) Study the p-groups G such that a Sylow p-subgroup of $\mathrm{Aut}(G)$ is regular. (ii) Is it possible to find the maximal value of n satisfying the following property: there exists a nonabelian group G of order p^n and exponent p such that a Sylow p-subgroup of $\mathrm{Aut}(G)$ is regular?

1565 (Mann). Obtain a good estimate for the order (for the class) of groups of exponent p and coclass n. (If G is such a group, then $\mathrm{d}(G) \leq n$ so $|G|$ is bounded in terms of n.)

1566. Classify the p-groups that are not generated by subgroups of index p^4 (of index p^5).

1567. Study the p-groups G all of whose metacyclic subgroups have orders smaller than or equal to $p \cdot \exp(G)$.

1568. Study the p-groups $G = ABC$, where A, B, C are pairwise permutable cyclic subgroups.

1569. Describe the structure of the representation groups of (a) minimal nonabelian p-groups, (b) p-groups of maximal class with $p > 2$, (c) special p-groups which are normal Sylow subgroups of minimal nonnilpotent groups (see Appendix 22).

1570 (Mann). Given an integer $r > 1$, does there exist a p-group that cannot be generated by elements of less than r pairwise distinct orders? (See #1814.)

1571. Study the p-groups all of whose minimal nonabelian subgroups are E_p-groups. (See §110.)

1572. Study the p-groups G such that whenever $A, B < G$ are distinct and conjugate, then $A \cap B$ is cyclic.

1573 (This problem is inspired by one of Passman's result.). Classify the p-groups having a faithful irreducible character of degree p^n and an irreducible character of degree $p^{j(n)}$, where $j(n) = 1 + p + \cdots + p^{n-1}$.

1574. Classify the p-groups G with pairwise nonisomorphic minimal nonabelian subgroups. (Example: SD_{16}). Is it true that all such G are 2-groups? Does there exist another p-group with this property? (Of course, we assume that G is neither abelian nor minimal nonabelian.)

1575. Suppose that a 2-group G has no normal subgroups $\cong \mathrm{E}_{2^n}$. As Mann in *J. Algebra* **318** (2007), 953–958, has shown, in this case, one has $\mathrm{d}(G) \leq 2(n-1)^2$. Does there exist linear estimates for $\mathrm{d}(G)$ and $\mathrm{d}(U)$ $(U < G)$?

1576. (i) Let $H \not\leq \Phi(G)$ be a normal subgroup of a p-group G. Study the structure of G provided all maximal subgroups of G not containing H are minimal nonabelian. (See §§100–102.) (ii) A similar problem arises for 'metacyclic' instead of 'minimal nonabelian'. (See §87.)

1577. Let $M \in \Gamma_1$ be such that $M \cap A \lhd G$ for all $A < G$ with $A \not\leq M$. Study the structures of G and M.

1578. Classify the p-groups all of whose subgroups (nonabelian subgroups) of index p^2 are isomorphic.

1579. Study the p-groups all of whose proper subgroups have an abelian (metacyclic) subgroup of index p (two problems).

1580 (Old problem). Study the nonmetabelian p-groups all of whose proper subgroups (two-generator subgroups) are metabelian.

1581. Study the p-groups, $p > 2$, without subgroup $\cong \mathrm{E}_{p^4}$.

1582. Study the $\mathcal{A}_n$-groups all of whose maximal subgroups are $\mathcal{A}_{n-1}$-groups. Is it true that the set of such groups is nonempty for all $n > 2$? (For $n = 2$, see §72.)

1583. Classify the p-groups admitting an irredundant covering by $\leq 2p$ subgroups. (See §116.)

1584. Study the p-groups with normal abelian (minimal nonabelian) subgroup of index p^2.

1585. Does there exist a p-group G admitting a nontrivial irredundant covering $G = \bigcup_{i=1}^{n} A_i$ such that (i) $|A_1| < |A_2| < \cdots < |A_n|$, (ii) $\exp(A_1) < \exp(A_2) < \cdots < \exp(A_n)$, (iii) $\mathrm{cl}(A_1) < \mathrm{cl}(A_2) < \cdots < \mathrm{cl}(A_n)$?

1586. Given k, study the p-groups $G = \Omega_k(G)$ containing exactly two distinct maximal subgroups U, V such that $\Omega_k(U) = U$ and $\Omega_k(V) = V$. (See §30.)

1587. Study the p-groups all of whose nonnormal cyclic subgroups have abelian (metacyclic) normalizers (two problems)

1588. Given $n > 1$, study the p-groups with exactly p^n nonnormal subgroups of order p.

1589. Study the p-groups G such that whenever $A \leq M \in \Gamma_1$, where A is a maximal abelian G-invariant subgroup of M, then (i) $\mathrm{C}_G(A) > A$, (ii) $\mathrm{C}_G(A) = A$.

1590. Classify the p-groups G such that $|G : H^G| \leq p^2$ for all nonnormal $H < G$. (See §62.)

1591. Classify the 2-groups G containing a maximal elementary abelian subgroup of order 4 and a subgroup $\cong \mathrm{E}_{2^4}$. (This is solved by Janko; see §127. For $p > 2$, see §134.)

1592. G. Glauberman and N. Mazza have proved that if $p > 2$ and a p-group G contains a maximal elementary abelian subgroup of order p^2, then G has no elementary abelian subgroup of order p^{p+1} and this estimate is best possible as a Sylow p-subgroup of the symmetric group of degree p^2 shows (Glauberman's letter at 17/7/09). The proof of the result above is not elementary. It is interesting to produce an elementary proof. Is it true that every subgroup of such G is generated by p elements? (See §134.)

1593. Classify the nonabelian d-generator p-groups that are not generated by $d - 1$ minimal nonabelian subgroups; see §135.

1594. Does there exist a p-group of class p that has no $\mathcal{H}_p$-chain? (See §88).

1595. Classify the $\mathcal{A}_3$-groups G such that $\alpha_1(G) < p^2 + p + 1$. (See §76).

1596. Let G and H be p-groups that satisfy: (i) $|G| = |H|$, (ii) $\mathrm{Z}(G) \cong \mathrm{Z}(H)$, (iii) $\Omega_k(G) \cong \Omega_k(H)$, $k = 1, 2$, (iv) $\Phi(G) \cong \Phi(H)$, (v) $G/\mho_k(G) \cong G/\mho_k(H)$, $k = 1, 2$. Is it true that $G \cong H$?

1597. Study the 2-groups G such that whenever $A < G$ is not normal, then A is contained in exactly one subgroup of G of order $p|A|$.

1598. Classify the 2-groups containing exactly one subgroup $\cong Q_8$.

1599. Study the special p-groups without normal cyclic subgroups of order p^2.

1600. Suppose that the lattices of normal subgroups of p-groups G and H are isomorphic. Study the structure of H provided G is $\mathfrak{A}_n$-group, $n = 1, 2$. (See §§65, 72.)

1601. Study the irregular p-groups, $p > 2$, which are lattice isomorphic to regular p-groups. (See Appendix 42.)

1602. Study the p-groups all of whose nonnormal cyclic subgroups have the same order. (Compare with §16.)

1603. Study the irregular p-groups $G = \Omega_1(G)$ such that every two elements of G of order p generate a subgroup of exponent p.

1604. Study the 2-groups of exponent 4 that are not generated by minimal nonmetacyclic subgroups.

1605. Let $G = U \times V$, where $\exp(U) = p$. Express $\alpha_1(G)$ in terms of U and V.

1606. Study the p-groups G such that whenever $A, B < G$ are conjugate in G, then A, B are conjugate in A^G.

1607. Study the p-groups G such that $\mathrm{Inn}(G) \cap \langle \alpha \rangle = \{1\}$ for any outer automorphism α of G.

1608. Let $M = G - \Phi(G)$. Study the structure of G if, for every $x, y \in M$, $\langle x, y \rangle$ is regular.

1609. Study the p-groups, $p > 3$, all of whose subgroups of order p^p and exponent p are pairwise nonisomorphic.

1610 (Zhmud). Let n_χ be the number of zeros of a character χ. Classify the p-groups of exponent p possessing a faithful nonlinear irreducible character χ with $n_\chi = 2p$ ($n_\chi = 2p^2 - p + 1$).

1611. Suppose that G is a p-group and $H < G$ is of maximal class such that every maximal set of pairwise noncommuting elements of H is a maximal set of pairwise noncommuting elements of G. Study the embedding of H in G. (See Lemma 116.4.)

1612. Study the p-groups all of whose minimal nonabelian subgroups have exponent p^2. (See §95.)

1613. Study the p-groups G of order p^m such that for any $n \in \{1, 2 \ldots, m-1\}$, G contains at most $p^2 + p + 1$ normal subgroups of order p^n. (See [BCS].)

1614. Suppose that G is an L_p-group (see §§17, 18). Is it true that G is regular if and only if $G/\mathfrak{V}_2(G)$ is regular?

1615. Study the p-groups G such that any maximal set of pairwise noncommuting elements of G does not generate G.

1616. Study the metacyclic p-groups, $p > 2$, with a nonabelian section of order (i) p^3, $p > 2$, (ii) p^4. (See §124.)

1617. Classify the p-groups G such that whenever $H < G$ is non-G-invariant and $A \leq H$, then $A^G \cap H = A^H$.

1618. Study the p-groups G such that $\Omega_1(G)$ is irregular of order p^{p+2}.

1619. Classify the irregular p-groups G, $p > 2$, such that $|\Omega_2^*(G)| = p^{p+1}$.

1620. Study the p-groups G such that $\chi(1)^3 \mid |G/\ker(\chi)|$ (resp. $\chi(1)^3 \mid |G|$) for all $\chi \in \mathrm{Irr}(G)$.

1621. Study the 2-groups G containing a maximal metacyclic subgroup M such that whenever $M < N \leq G$ and $|N : M| = 2$, then (i) $\Omega_1(N) = N$, (ii) $\Omega_2^*(N) = N$ (two problems).

1622. Study the p-groups G containing a subgroup M of maximal class (extraspecial, minimal nonabelian) such that whenever we have $M < N \leq G$ and $|N : M| = p$, then (i) $\Omega_1(N) = N$, (ii) $\Omega_2^*(N) = N$, (iii) $\mathrm{d}(N) = 2$. (If M is of maximal class in (iii), then G is also of maximal class by Proposition 12.12(a).)

1623. Study the p-groups G such that for all nonnormal cyclic $C < G$ the normal closure C^G is (i) either abelian or minimal nonabelian, (ii) metacyclic (two problems).

1624. Study the p-groups G such that $AB = BA$ for all $A, B < G$ of distinct orders.

1625. A p-group G is said to be a WE_p*-group* if it is not a product of two nonnormal subgroups. Study the WE_p-groups of class 2 (see §110).

1626. Classify the 2-groups G containing a minimal nonmetacyclic subgroup M of order 2^5 such that whenever $M < N \leq G$ and $|N : M| = 2$, then $\Omega_1(N) = N$.

1627. Study the p-groups G such that $P \in \mathrm{Syl}_p(\mathrm{Aut}(G))$ is minimal nonabelian.

1628. Study a p-group such that only one of its subgroups of order p is contained in a cyclic subgroup of order p^2.

1629. Does there exist a p-group of order > 8 covered by dihedral subgroups of order 8?

1630. (i) Is it true that if G is of maximal class and order $> p^{p+1}$ and G satisfies $|\Omega_1(G)| = p^{p-1}$, then G has a trivial Schur multiplier? (ii) Classify the p-groups of maximal class with trivial Schur multiplier. (iii) Classify the p-groups G of maximal class which are representation groups of $G/\mathrm{Z}(G)$.

1631. Let $\mathrm{E}_{p^p} \cong E < G = \Omega_1(G)$, $p > 2$. Suppose that for every $x \in G - E$ of order p the subgroup $\langle x, E\rangle \cong \Sigma_{p^2}$. Describe the structure of G.

1632. Given $k > 1$, study the p-groups H of class 2 such that there exists a p-group G of class $> k$ with $\mathrm{Z}_2(G) \cong H$.

1633. Given n, classify the p-groups G such that $\Omega_n(H)$ is regular for all $H \in \Gamma_1$ but $\Omega_n(G)$ is irregular.

1634. Study the groups G of order p^n such that $\mathrm{s}_k(G) = \mathrm{s}_{n-k}(G)$ for all $k \leq n$. (See §124.)

1635. (i) Study the groups of exponent p with Schur multiplier of order p. (See [Kar2, §13.6].) (ii) Estimate the number of representation groups of a group of order p^n and exponent p.

1636. Study the p-groups G such that whenever $A, B < G$ are distinct conjugate, then $\langle A, B\rangle \lhd G$.

1637. Given $k \in \{1, \ldots, p+1\}$, classify the metacyclic p-groups with exactly k characteristic subgroups of order p.

1638. Classify the metacyclic 2-groups that possess a maximal cyclic subgroup of order 2. (For $p > 2$, such a group has a cyclic subgroup of index p; see Theorem 7.2(c).)

1639 (Old problem). Study the p-groups G, $p > 2$, such that $\mathrm{Aut}(G)$ is a p-group.

1640. Given k, find a minimal n such that whenever G contains a subgroup $\cong \mathrm{E}_{p^n}$, then it contains a normal subgroup $\cong \mathrm{E}_{p^k}$. (See §10.)

1641 (Berkovich–Ito). Study the p-groups G having a faithful $\phi \in \mathrm{Irr}(G)$ of degree p^n such that $\mathrm{dl}(G) = n + 1$. (See Theorem 22.25.)

1642. Study the p-groups G such that $\exp(\langle x, y\rangle) = \max\{o(x), o(y)\}$ for all $x, y \in G$.

1643. Classify the abelian p-groups G having a representation group Γ of the same exponent as G.

1644. Let $\mathcal{N}$ be the set of all positive integers n such that there is an $\mathcal{A}_n$-group G that has no abelian subgroup of index p^{n-1}. It is known that $2 \in \mathcal{N}$. Is it true that the set $\mathcal{N}$ is finite? (See §§65, 71.)

1645. A p-group is said to be *minimal irregular* if it is irregular but all its proper subgroups are regular. (In §7 we have used another definition.) Let G be an irregular p-group and let $R = R(G)$ be generated by all minimal irregular subgroups of G. Is it true that (i) $R \not\leq \Phi(G)$? (ii) G/R is regular?

1646. Let $a(X)$ denote the number of maximal abelian subgroups of a nonabelian p-group X. Given k, find $\min\{a(G) \mid a(G) > k\}$, where G runs over all p-groups.

1647. Study the p-groups G containing exactly one normal subgroup of each order $\leq |H|$, where $H \in \{G', \Phi(G), \mho_1(G)\}$ (three problems).

1648. Classify the p-groups of order p^m admitting an automorphism of order p^{m-3} (see §33).

1649. Classify the p-groups all of whose maximal subgroups are special. (There is a special group of order 2^6 with this property; see §§41, 69. See #1418.)

1650. Study the irregular p-groups G, $p > 3$, such that $G/\mathrm{K}_{p-1}(G)$ is absolutely regular.

1651. Classify the p-groups possessing a pair of distinct extraspecial subgroups of index p.

1652. Classify the p-groups G of exponent p containing a nonabelian subgroup L of order p^2 such that there is only one maximal chain connecting L with G.

1653. Study the p-groups G all of whose subgroups that are not incident with $\Phi(G)$ (with G') are abelian (two problems).

1654. Study the p-groups G of exponent p satisfying $|G : \mathrm{Z}(G)| = p^3$.

1655. Study the p-groups G such that one of any two conjugate subgroups of G normalizes the other.

1656. Suppose that a p-group G contains a soft subgroup of order p^3. (i) Is it true that there exists a constant C such that $\mathrm{d}(A) \leq C$ for all $A < G$? (As K. Harada has shown, if $p = 2$, then $C = 4$; see §99.) (ii) Suppose that a p-group G contains a soft subgroup of order p^n. Is it true that for all $A \leq G$ we have $\mathrm{d}(A) \leq p^{n-1}$ if $p > 2$ and $\mathrm{d}(A) \leq 2^n$ if $p = 2$?

1657. Suppose that a 2-group G has no normal elementary abelian subgroups of order 16, and let $U < G$. Find the best possible constant C such that $\mathrm{d}(U) \leq C$. (See §15 and ##1575, 1656.)

1658. Study the p-groups of exponent p^e all of whose minimal nonabelian subgroups have order p^{2e+1}.

1659. Study the p-groups with exactly p nonnormal minimal nonabelian subgroups. (See Lemma 76.6.)

1660. Study the p-groups all of whose subgroups of order p, except one, are maximal cyclic. (Examples: D_{2^n}, SD_{2^n}.)

1661. Study the p-groups all of whose maximal cyclic subgroups are nonnormal.

1662. Study the p-groups all of whose maximal subgroups are WE_p-groups (see #1625 and §110.)

1663. Study the p-groups with a maximal set of pairwise noncommuting elements of cardinality k, where $p + 2 < k < 2p$. (See §116.)

1664. Study the p-groups G all of whose nonabelian epimorphic images have centers of order p.

1665. Study the p-groups G with $\mathrm{d}(G) > k > 1$ all of whose subgroups of index p^k contain $\Phi(G)$.

1666. Study the p-groups G with nonabelian G' and such that H' is elementary abelian for all $H \in \Gamma_1$.

1667. A group G is said to be *rational* if every irreducible character of G assumes rational values. Study the nonrational 2-groups all of whose nonabelian maximal subgroups are rational.

1668. Study the p-groups that are (i) not generated by nonnormal cyclic subgroups, (ii) generated by normal cyclic subgroups.

1669. Study the p-groups such that whenever $A, B < G$ are minimal nonabelian of distinct orders, then $A \cap B = \{1\}$.

1670. Classify the p-groups G containing a maximal subgroup M such that all non-G-invariant subgroups of M (a) are cyclic, (b) have the same order.

1671. Find all integers $n > p$ such that there exists an irregular p-group of class n all of whose proper epimorphic images are regular. Is the set of such n unbounded?[6]

1672. Study the p-groups that have no normal subgroups of class 2. (Example: all p-groups of maximal class and of order $> p^4$ with an abelian subgroup of index p.) Is it true that the derived length of such groups G is bounded? Consider the case $\exp(G) = p$ in most possible detail.

1673. Study the p-groups G such that whenever $x \in G - \Phi(G)$, then $|G : \mathrm{C}_G(x)| \leq p$.

1674. Study the p-groups G such that for all minimal nonabelian $A < G$ we have (i) $A_G = \{1\}$, (ii) A/A_G is minimal nonabelian, (iii) $A/A_G > \{1\}$ is cyclic.

1675. Study the p-groups G containing a noncentral normal abelian subgroup N such that whenever $A/N < G/N$ is abelian, then $\mathrm{cl}(A) \leq 2$.

1676. Study the two-generator p-groups G (p-groups G of exponent p) (i) without two-generator maximal subgroups, (ii) $\mathrm{d}(H) = p$ for all $H \in \Gamma_1$ (four problems).

1677. Study the p-groups G such that $\Phi(H) \lhd G$ ($\mho_1(H) \lhd G$) for all $H \leq G$.

1678. Study the p-groups G such that some maximal subgroup of H is G-invariant for all $H < G$.

[6]Commentary of Mann (letter at 25/7/09): Let $c(p)$ be the maximal class of a 2-generator finite p-group of exponent p ($c(p)$ exists, by Kostrikin). It is clear from my minimal irregular groups paper (see also §7, esp., Theorem 7.4) that the class of a minimal irregular p-group is at most $c(p) + 1$, and Groves improved the bound to $c(p)$. Then I showed that there exist minimal irregular p-groups (as defined in §7) of any class between p and $c(p)$. This can be found in my two papers on minimal irregular p-groups. Your question, for $n > c(p)$, is still open (maybe there is an approach; I have to think about it).

1679. Study the p-groups G such that all factors of lower (upper) central series of G, except one, are cyclic (two problems).

1680. Study the p-groups G such that every abelian subgroup of G is contained in a minimal nonabelian subgroup.

1681. Study the p-groups with characteristic (i) all normal cyclic subgroups, (ii) all normal abelian subgroups, (iii) all normal nonabelian subgroups, (iv) all normal noncyclic subgroups (four problems).

1682. Study the p-groups without soft subgroups.

1683. Given a p-group H, study the p-groups G containing H as a maximal subgroup and such that (i) $\mathrm{d}(G) \leq \mathrm{d}(H)$, (ii) $G' > H'$, (iii) $\mathrm{Z}(G) = \mathrm{Z}(H)$ (three problems).

1684. Given a p-group G, let $\tau_1(G)$ be the number of pairwise nonisomorphic minimal nonabelian subgroups of G. Find (i) $\tau_1(\Sigma_n)$, (ii) $\tau_1(\mathrm{UT}(n, p))$ (two problems).

1685. Given a p-group H, find a sufficient condition for existence of a p-group G containing H as a unique proper normal subgroup of order $|H|$. (By B. Wilkens, there is H for which a group G with above property does not exist.)

1686. State a necessary and sufficient condition for regularity of a p-group containing an abelian subgroup of index $p > 2$.

1687. Study the p-groups $G = \exp(\Omega_1(G))$ such that $|L^G| < p^p$ for all $L < G$ of order p.

1688. Study the p-groups G such that $\langle x, y\rangle$ is regular provided $x, y \in G$ are conjugate.

1689. Study the p-groups without special sections.

1690. Study the irregular p-groups G provided $|L_{p^k}| \leq p^{k+p}$, where k is fixed and $L_{p^k} = \{x \in G \mid o(x) \leq p^k\}$. (See Appendix 43.)

1691. Study the p-groups G such that whenever $x \in G - \mathrm{Z}(G)$, then $\mathrm{C}_G(x)$ is either abelian or minimal nonabelian.

1692. Study the p-groups G such that whenever $H < G$ is nonabelian, then one has $|\mathrm{C}_G(H) : \mathrm{Z}(H)| \leq p$.

1693. Study the p-groups G such that $\mathrm{N}_G(H) = H\mathrm{C}_G(H)$ for all nonabelian $H < G$.

1694. Study the p-groups G such that whenever $H < G$ is nonabelian, then the norm of H (see §§140, 143) is normal in G.

1695. Study the p-groups with $\leq p$ minimal nonabelian subgroups of minimal order. (See Lemma 76.6.)

1696. Study the p-groups covered by minimal irregular subgroups.

1697. Study the p-groups G containing an element x of order p such that $\mathrm{C}_G(x)$ is metacyclic minimal nonabelian. (See §132.)

1698. Let $M \in \Gamma_1$, where G is a p-group. Suppose that all minimal nonabelian subgroups of G that are not contained in M, (i) have order p^3, (ii) are isomorphic to M_{p^n} for some fixed n, (iii) are isomorphic to $\langle a, b \mid a^{p^2} = b^{p^2} = 1,\ a^b = a^{1+p}\rangle$. Study the structure of G.

1699. Given $k > 3$, study the p-groups of exponent p all of whose nonabelian subgroups of order p^k are normal.

1700. Study the p-groups G such that whenever $H < G$, then any proper characteristic subgroup of H is normal in G. Moreover, study the p-groups G such that whenever $H < G$, then $\mho_1(H) \lhd G$.

1701. Study the p-groups G such that whenever $A, B < G$ are distinct $\mathscr{A}_2$-subgroups, then $|A| \neq |B|$.

1702. Classify the 2-groups G containing a minimal nonmetacyclic subgroup H of order 2^5 such that (i) $\mathrm{C}_G(x) \leq H$ for all $x \in H$ of order 4, (ii) $\mathrm{C}_G(\mathrm{Z}(H)) = H$.

1703. Let G be a p-group. We define

$$\begin{aligned}
p^{\mathrm{eb}(G)} &= \max\{|G : \mathrm{C}_G(x)| \mid x \in G\},\\
p^{\mathrm{sb}(G)} &= \max\{|G : \mathrm{N}_G(H)| \mid H \leq G\},\\
p^{\mathrm{csb}(G)} &= \max\{|G : \mathrm{N}_G(H)| \mid H \leq G \text{ where H is cyclic}\},\\
p^{\mathrm{asb}(G)} &= \max\{|G : \mathrm{N}_G(H)| \mid H \leq G \text{ where H is abelian}\},\\
p^{\mathrm{masb}(G)} &= \max\{|G : \mathrm{N}_G(H)| \mid H \leq G \text{ where H is minimal nonabelian}\}.
\end{aligned}$$

Our notation is slightly differed from [Boh]. Mann has proved that $\mathrm{b}(G) \leq 3\mathrm{csb}(G)$, where $\mathrm{b}(G) = \mathrm{eb}(G)$ is the element breadth of G (see §40). If $p > 2$ and G is an extraspecial group of order p^{2m+1}, then $\mathrm{sb}(G) = m$ and $\mathrm{b}(G) = 1$. Therefore, there does not exist an upper bound of $\mathrm{sb}(G)$ in terms of $\mathrm{b}(G)$. Cutolo–Smith–Wiegold improved Mann's inequality as follows: $\mathrm{b}(G) \leq 2\mathrm{csb}(G) + 1$ if $p = 2$ and $\mathrm{b}(G) \leq 2\mathrm{csb}(G)$ if $p > 2$. If G is of exponent p^e, then $\mathrm{b}(G) \leq \mathrm{csb}(G) + (e-1)$ (this is due to the equality $|\mathrm{Aut}(\mathrm{C}_{p^n})| = (p-1)p^{n-1}$). J. Bohanon has predicted that if $\mathrm{sb}(G) = 1$, then for $p = 2$, $|G : \mathrm{Z}(G)| \leq 2^4$ (this was proved in §122) and proved that this number is $\leq p^3$ if $p > 2$ (see also §122 and [CSW]). Bohanon also conjectured that if $\mathrm{sb}(G) = k$, then $|G : \mathrm{Z}(G)| \leq 2^{3k+1}$ if $p = 2$ and $\leq p^{3k}$ if $p > 2$. (i) Classify the p-groups G satisfying $\mathrm{eb}(G) = \mathrm{sb}(G)$. (ii) Classify the p-groups G satisfying $\mathrm{csb}(G) = \mathrm{eb}(G)$. (The p-groups all of whose cyclic subgroups of order $> p$ are normal satisfy this condition; see §83.) (iii) Classify the p-groups G satisfying $\mathrm{csb}(G) = \mathrm{sb}(G)$. (iv) Classify the p-groups G satisfying $\mathrm{csb}(G) = \mathrm{asb}(G)$. (v) Consider problems (i) and (ii)

for groups of exponent p and metacyclic p-groups. (vi) Classify the p-groups satisfying $\mathrm{asb}(G) = \mathrm{masb}(G)$.

1704. Study the p-groups G admitting an automorphism α of order p^2 such that $\mathrm{C}_G(\alpha)$ has order p. (For $p = 2$, see §77.)

1705. Study the p-groups G such that whenever $A < G$ is nonabelian, then $\mathrm{C}_G(A)$ is also nonabelian.

1706. Study the nonabelian p-groups G of order p^{1+2s} containing exactly one character (exactly $p-1$ irreducible characters) of degree p^s.

1707. Given $k > 1$, classify the p-groups G such that there is a metacyclic p-group M satisfying $\mathrm{s}_k(G) = \mathrm{s}_k(M)$. (See §124. This is not solved even for $p = 2 = k$.)

1708. Given a nonabelian p-group G all of whose minimal nonabelian subgroups are isomorphic and their number is a power of p, does there exist an overgroup T of G such that all minimal nonabelian subgroups of G are conjugate in T?

1709. Classify the p-groups G with $\mathrm{d}(G) > 2$ all of whose nonabelian members of the set Γ_2 are metacyclic.

1710. Study the p-groups G containing a maximal subgroup M such that whenever C is a cyclic subgroup of G not contained in M, then $|C^G : C| = p$.

1711. Classify the p-groups all of whose nonnormal subgroups are abelian of rank 2. (See §16.)

1712 (Zhmud). Study the p-groups G such that whenever $\langle x\rangle^G = \langle y\rangle^G$ for some $x, y \in G$, then (i) $o(x) = o(y)$, (ii) $y = x^\phi$ for some $\phi \in \mathrm{Aut}(G)$. (Compare with #1; see also [BZ, Chapter 9].)

1713. Study the p-groups satisfying $|G : G'| \geq |A|$ for all abelian $A < G$.

1714. Is it true that if $E < G$ is elementary abelian and all subgroups of E are characteristic in G, then $|E|$ is bounded?

1715. Study the p-groups G such that for every abelian subgroup A of G and $A < B \leq G$ with $|B : A| = p$ we have $|B'| \leq p$.

1716. Study the pairs of p-groups $H < G$ such that H normalizes all cyclic $C < G$ with $C \not\leq H$.[7]

1717. Classify the p-groups, $p > 2$, all of whose minimal nonabelian subgroups are isomorphic to M_{p^3}. (Compare with #115, see #2264.)

1718. Study the p-groups G such that whenever A, B are distinct maximal abelian subgroups of G, then $A \cap B = \mathrm{Z}(G)$.

[7] For each H this is a separate problem. For example, if $p = 2$ and $H \cong \mathrm{Q}_8$, then G is Dedekindian; see Theorem 143.1. However, if $p = 2$, then $H \ncong \mathrm{D}_8$.

1719. Let $\mathrm{L}_{p^k}(G) = \{x \in G \mid x^{p^k} = 1\}$. Study the p-groups G of given exponent $p^e > p$ with maximal possible $|G|^{-1}|\mathrm{L}_p(G)|$.

1720. Classify the special p-groups G such that all subgroups of $\mathrm{Z}(G)$ are characteristic. (See #1714.)

1721. Does there exist a p-group in which the intersection of normalizers of all cyclic subgroups is greater than the intersection of normalizers of all subgroups?

1722. Given $p > 2$ and $n > p$, study the pairs of p-groups $\{A, G\}$ of equal order p^n, where A is abelian (absolutely regular) and G is irregular, satisfying $\mathrm{s}_k(G) = \mathrm{s}_k(A)$ for all $k \in \{2, \ldots, n-1\}$?

1723. Study the groups G of exponent $p^e > p$ with absolutely regular $\Omega_e^*(G)$.

1724. Study the p-groups G such that whenever $H \in \Gamma_1$, then for each non-G-invariant $L < H$ we have $\mathrm{N}_G(L) \leq H$.

1725. Classify the 2-groups all of whose nonabelian subgroups are either minimal nonabelian or generated by involutions.

1726. Find the Schur multiplier and all representation groups of the group $G = A * B$, where A, B are of maximal class and orders $2^m, 2^n$ respectively and $|G| = 2^{m+n-1}$.

1727. Find automorphism groups and representation groups of U_2-groups (see §67).

1728. Study the nonabelian p-groups G all of whose minimal nonabelian subgroups have the same center.

1729. Let G be a special p-group with $\mathrm{d}(G) = d$ and $|\mathrm{Z}(G)| = p^{d(d-1)/2}$. Find the Schur multiplier of G and describe the representation groups of G.

1730. Study the p-groups G such that $\exp(G') > p$ but $\exp(H') \leq p$ for all $H < G$. Does there exist such a p-group G with $\exp(G') = p^3$? (See Exercise 1.69 and §§65, 71, 72.)

1731. Given $n > 1$, classify the 2-groups G with $\mathrm{c}_n(G) = 8$. (See §§13, 53, 54, 89.) Moreover, study the 2-groups G with $\mathrm{c}_n(G) \not\equiv 0 \pmod 8$ for $n > 2$.

1732. Classify the p-groups G such that $e_p(G) - 1$ is a power of p, where $e_p(G)$ is the number of subgroups of order p^p and exponent p in G.

1733. Classify the 2-groups with exactly three conjugate classes of abelian subgroups of type $(2, 2)$.

1734. Suppose that all subgroups of index p^k in a p-group G have derived subgroups of order at most p but $|G'| > p$. Find the least upper bound for $|G'|$ and $\mathrm{d}(G')$. (See Exercise 1.69 and §§72, 137.)

1735. Study the p-groups $G = \Omega_1(G)$ such that all their subgroups of order p^p and exponent p, except one, are of maximal class. (See Exercise A.40.38.)

1736. Suppose that any two minimal nonabelian subgroups of G, $p > 2$, generate a regular subgroup. Is it true that G is regular?

1737. Given $n > 1$, does there exist a p-group G such that $|G'| = p^{2n+1}$ provided $|H'| = p^n$ for all $H \in \Gamma_1$? (See Exercise 1.69(a).)

1738. Is it true that either the coclass or the derived length of G is bounded if one has $|H| \leq p^n$ for all minimal nonabelian subgroups $H < G$?

1739. Study the nonabelian p-groups all of whose normal subgroups of same index $> p$ are isomorphic.

1740. Classify the minimal nonabelian p-groups whose Schur multiplier is of order $\leq p$.

1741. Study the p-groups all of whose minimal nonabelian subgroups contain their centralizers.

1742. Study the p-groups G all of whose maximal subgroups H satisfy $|\Phi(H)| \leq p^2$.

1743. Find the maximal order of normal subgroups of exponent p in $\mathrm{UT}(n, p^m)$.

1744. Study the p-groups G containing a proper normal subgroup H such that for all $L \leq H$ one has $L^G \cap H = L^H$.

1745. Classify the p-groups G such that $|G : C^G| = p$ for all maximal cyclic $C < G$. (See §62.)

1746. Classify the groups G of order $p^m > p^4$ such that for each $n \in \{3, \ldots, m-1\}$ there is in G a nonabelian metacyclic subgroup (minimal nonabelian subgroup, metacyclic minimal nonabelian subgroup) of order p^n (three problems).

1747. Study the 2-groups $G = CM$, where $C < G$ is cyclic and $M < G$ is of maximal class. Consider the case $M \lhd G$ in most possible detail.

1748. Describe the power structure of irregular 3-groups $G = AB$, where A and B are metacyclic.

1749. Study the p-groups in which any two conjugate subgroups (subgroups of same order, of different orders) are permutable.

1750. Classify the p-groups G such that the automorphism group of G, $\mathrm{Aut}(G)$, is a Frobenius group. (Example: $\mathrm{Aut}(\mathrm{E}_4)$.)

1751. Study the p-groups having only one maximal subgroup of exponent $> p$.

1752. Classify the abelian p-groups A such that A is characteristic in the semidirect product $P \cdot A$, where P is a Sylow p-subgroup in $\mathrm{Aut}(A)$.

1753. Classify the abelian p-groups A such that $\mathrm{Z}(\Gamma) = \mathrm{M}(A)$, where Γ is a representation group of A and $\mathrm{M}(A)$ is the Schur multiplier of A. Is it true that this equality holds for remaining representation groups of G?

1754. Classify the p-groups G such that there is $t \in G$ of order p^2 with $\mathrm{C}_G(t) = \langle t \rangle \times Q$, where Q has exactly one subgroup of order p. (See §48, 49, 77, [Bla13].)

1755. Study the p-groups G of exponent $p^e > p$ such that $\mathrm{Aut}(G)$ acts transitively on the set of all cyclic subgroups of order p^e.

1756. Study the p-groups G that satisfy $|\mathfrak{V}_1(G)| = p$. Is it possible to estimate the number $|G : \Omega_1(G)|$?

1757. Classify the p-groups G, $p > 2$, containing two distinct $A, B \in \Gamma_1$ such that all elements of the set $G - (A \cup B)$ have order p. (For $p = 2$, see Theorem 43.12.)

1758. Given $m > 4$, does there exist a group of order p^m containing minimal nonabelian subgroups of orders $p^3, \ldots, p^{m-1}$?

1759. Describe the power structure of the p-groups containing $\geq p$ distinct maximal subgroups of exponent p.

1760. Study the p-groups G containing a nonnormal nonabelian subgroup H such that $H \cap H^x = \{1\}$ for all $x \in G - \mathrm{N}_G(H)$. (There are any restrictions on the structure of H; example: $G = H \operatorname{wr} \mathrm{C}_p$.)

1761. Study the 2-groups G containing a U_2-subgroup H (see §67) such that whenever $H < K \leq G$ with $|K : H| = 2$, then $\Omega_1(K) = K$ ($\Omega_2^*(K) = K$).

1762. Study the p-groups G such that for any nonnormal subgroup $H < G$ one has $|\langle H, H^x \rangle : H| = p$ for all $x \in G - \mathrm{N}_G(H)$.

1763. Present for every $p > 2$ a p-group G whose Φ-subgroup (derived subgroup) is irregular of order $\leq p^{2p+1}$.

1764. Study the p-groups having exactly $p - 1$ nonlinear irreducible characters of each degree.[8]

1765. Study the irregular p-groups G with $H \in \Gamma_1$ such that whenever $x \in G - H$, then $\langle x, y \rangle$ is regular for all $y \in H$.

1766. Classify non-E_p-groups whose proper subgroups are E_p-groups (see §110).

1767. Study the p-groups G such that $\mathfrak{V}_1(G)$ is irregular but $\mathfrak{V}_1(H)$ is regular for all $H < G$. The same problem arises for Φ-subgroups and derived subgroups instead of $\mathfrak{V}_1$-subgroups.

1768. Study the structure of the group of automorphisms fixing (as whole) all minimal nonabelian subgroups of a nonabelian p-group.

1769. Describe $\mathcal{N}(A \times B)$ and $\mathcal{N}(A * B)$ in terms of A and B (here $\mathcal{N}(X)$ is a norm of a group X; see §§140, 143).[9]

[8] According to Mann, $p - 1$ divides the number of nonlinear irreducible characters of given degree in a p-group.

[9] If $A \cong \mathrm{Q}_8 \cong B$ and $G = A * B$, the central product of order 32, then $\mathcal{N}(G) = \mathrm{Z}(G)$ is of order 2.

1770. For Σ_{p^n} and $\mathrm{UT}(n, p^m)$, describe all their epimorphic images with cyclic centers.

1771. Study the 2-groups G such that G' is minimal nonmetacyclic of order 2^5 (see Theorem 66.1). The same problem arises for G-invariant subgroups of $\Phi(G)$ instead of G'.

1772. For groups $\mathrm{UT}(n, p^m)$ and Σ_{p^n}, find the maximal k such that these groups have a k-admissible Hall chain (see §88).

1773. Classify the p-groups all of whose nonquasinormal subgroups are cyclic. (Compare with §16.)

1774. Classify the groups of order p^m such that for each $n \in \{3, \ldots, m-1\}$ there is in G a subgroup of order p^n and class 2.

1775. (i) Classify the abelian p-groups G such that p^3 does not divide $\exp(\mathrm{Aut}(G))$. (ii) Find $\exp(\mathrm{Aut}(G))_p$ and $\mathrm{d}(P)$, where $P \in \mathrm{Syl}_p(\mathrm{Aut}(G))$, for an abelian p-group G of given type.

1776. Given a group X, set $\mathrm{T}(X) = \sum_{\chi \in \mathrm{Irr}(X)} \chi(1)$. Let $H \in \Gamma_1$. Describe the structure of G provided $\mathrm{T}(G) - \mathrm{T}(H) \leq p^2(p-1)$. (See [BZ, Chapter 11].)

1777. Find all n such that provided G is an L_n-group (see §§17, 18), $\mho_1(G)$ is cyclic. Estimate $|G/\mho_1(G)|$ in general case.

1778. Suppose that $|\Omega_1(G)| = p^p$ and the quotient group $G/\Omega_1(G)$ is absolutely regular of exponent $> p$. Is it true that $\mho_1(G)$ is absolutely regular?

1779. Classify the p-groups G such that whenever $H < G$ is minimal nonabelian, then all subgroups (nonabelian subgroups) of G of order $|H|$ are also minimal nonabelian.

1780. Given $k > 1$, study the irregular p-groups covered by normal subgroups of order p^k.

1781. Is it true that a p-group possessing a k-admissible Hall chain possesses an admissible $(k-1)$-Hall chain? (See §88.)

1782. Given a p-group H, prove or disprove that there exists a p-group G containing H (containing H as a normal subgroup) and such that $|G/\mho_1(G)| = p^p$.

1783. Study the p-groups all of whose proper characteristic subgroups are abelian.

1784. Study the p-groups all of whose normal subgroups of order p^n have exponent p for all $n \leq p$.

1785. Given a p-group H, prove or disprove that there exists a p-group G containing a subgroup H (containing H as a normal subgroup) and such that all members of the set Γ_1 (all normal subgroups of G) are characteristic in G. (See [Wil6].)

1786. Study the p-groups G such that all nonnormal subgroups of G are characteristic in their normal closures.

1787. Study the p-groups G such that whenever $H < G$ is cyclic and $\phi \in \mathrm{Aut}(G)$, then there is $x \in G$ such that $H^{\phi} = H^{x}$.

1788. Given a p-group H of exponent p^n, does there exist a p-group G of exponent p^{n+1} satisfying $G/\mathfrak{V}_n(G) \cong H$?

1789. Given an integer $n > 1$, does there exist a p-group G such that $\mathrm{Aut}(G)$ is homocyclic of exponent p^n? (See #1906.)

1790. Study the p-groups G such that $p \cdot \exp(G) = \exp(\mathrm{Hol}(G))$, where $\mathrm{Hol}(G)$ is the holomorph of G.

1791. Classify the p-groups of maximal class, $p > 2$, all of whose representation groups are of maximal class.

1792. If G is a p-group of order p^{2n+e}, $e \in \{0, 1\}$, then, according to P. Hall, its class number $\mathrm{k}(G) = p^e(p^2 - 1)(n + t(G)(p - 1))$, where $t(G)$ is a nonnegative integer (see Theorem 2.1). Is it possible to estimate the derived length of G in terms of $t(G)$?

1793. (i) Does there exist a p-group which is a direct product of two proper characteristic subgroups? (ii) Classify the p-groups which are central products of two proper characteristic subgroups. (Example: $G = \mathrm{Q}_8 * \mathrm{C}_4$ of order 16.)

1794. Study the nonabelian p-groups G such that $\mathrm{Z}(G) \cap M = \mathrm{Z}(M)$ for all nonabelian $M \leq G$.

1795. Let $P \in \mathrm{Syl}_p(\mathrm{Hol}(G))$, where $\mathrm{Hol}(G)$ is a holomorph of an abelian group G of given type. Find $\mathrm{d}(P)$, $\mathrm{d}(P/G)$, P', $(P/G)'$, $\Phi(P)$, $\Phi(P/G)$, $\exp(P)$, $\exp(P/G)$, $\mathrm{cl}(P)$, $\mathrm{cl}(P/G)$ and the number of P-conjugacy classes of G (eleven problems).

1796. Is it true that in a two-generator 3-group G all of whose maximal subgroups are two-generator, the ranks of subgroups are bounded?

1797. Describe the representation groups of homocyclic p-groups. (See Lemma 21.7.)

1798. Describe the representation groups of abelian groups of type $(p, p^2, \ldots, p^n)$. (See Lemma 21.7.)

1799. Describe the representation groups of extraspecial p-groups.

1800. Classify the p-groups G all of whose maximal subgroups, except one, have derived subgroups of order $\leq p$. (In a letter at 29/3/2011, Janko reported that he had solved this problem.)

1801. Study the structure of G provided $\mathrm{Aut}(G)$ splits over $\mathrm{Inn}(G)$.

1802. Classify the p-groups G all of whose nonnormal subgroups H satisfying the inequality $|G : H^G| > p$ are conjugate. (See §62.)

1803. Classify the p-groups all of whose nonnormal subgroups have derived subgroups (Frattini subgroups) of orders $\leq p$.

1804. Study the p-groups G such that $H' = \Phi(G)'$ for all nonabelian $H \in \Gamma_i$, where $1 < i < \mathrm{d}(G)$, i is fixed (for all nonabelian of index p^i). (See §111.)

1805. Study the nonabelian p-groups G such that whenever $H < G$ is minimal nonabelian and $x \in H^{\#}$, then $\mathrm{C}_G(x) \leq \mathrm{N}_G(H)$.

1806. Is it possible to see if a given p-group is a representation group of some group?

1807. Study the p-groups all of whose subgroups of order p are characteristic. (Example: $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^3 \rangle$.)

1808. Study the p-groups G such that whenever $H \leq G$ is minimal nonabelian, then $\mathrm{N}_G(A) \leq \mathrm{N}_G(H)$ ($\mathrm{N}_G(H) \leq \mathrm{N}_G(A)$) for all maximal $A < H$.

1809. Study the 2-groups all of whose minimal nonmetacyclic subgroups are nonabelian. (See §§66, 69.)

1810. Study the p-groups G such that whenever $A < G$ is minimal nonabelian, then A/A' is a maximal abelian subgroup of $\mathrm{N}_G(A)/A'$. (This property holds for metacyclic p-groups G; see §124.)

1811. Study the 2-groups $G = \Omega_1(G)$ in which every two noncommuting involutions generate a subgroup $\cong \mathrm{D}_8$. Is it possible to estimate $\mathrm{cl}(G)$?

1812. Classify the p-groups G such that whenever $A < G$ is maximal abelian and $x \in A - \mathrm{Z}(G)$, then $\mathrm{C}_G(x) = A$.

1813. Study the p-groups G with $|H\mathrm{C}_G(H) : H| \leq p$ for all nonabelian $H < G$.

1814. Study the p-groups G such that whenever $\{a_1, \ldots, a_d\}$ is an arbitrary minimal system of generators of G, then the orders of the elements $a_1, \ldots, a_d$ are pairwise distinct. (Example: SD_{2^n}. See #1570.) Is it true that $\mathrm{dl}(G)$ and d are bounded? (See [O'B2].)

1815. Study the p-groups all of whose proper subgroups are either metacyclic or of class ≤ 2.

1816. Estimate $\delta(G)$ (see #1538), where G is a special group of order p^{d+z} with $d = \mathrm{d}(G)$.

1817. Given two p-groups H and N one of which, say N, is abelian, does there exist a p-group G with a characteristic subgroup N such that $G/N \cong H$?[10]

[10]Commentary of Mann: If we omit the restriction on the structure of N, then the answer is 'no'. Bettina Wilkens, answering another of your question, constructed p-groups that are never characteristic in any properly containing p-group. She showed that every p-group is contained in a p-group with this property. Such groups cannot be taken as N above. See [Wil5].

1818. Study the p-groups possessing a principal series all of whose members are characteristic.

1819. Study the p-groups G all of whose minimal nonabelian subgroups are characteristic.

1820. Does there exist a group of exponent p all of whose maximal subgroups are direct products of minimal nonabelian subgroups?

1821. Study the p-groups of exponent p all of whose minimal nonabelian subgroups are generalized soft. (See §130.)

1822. Study the p-groups G all of whose maximal abelian subgroups have orders smaller than or equal to $p^2|\mathrm{Z}(G)|$.

1823. Study the p-groups such that $G/\mathrm{Z}(G)$ is (i) of maximal class, (ii) metacyclic, (iii) minimal nonabelian, (iv) extraspecial, (v) special.

1824. Study the p-groups G such that $|H : H'| \leq p^3$ for all $H \in \Gamma_1$ (for all nonabelian $H < G$).

1825. Study the irregular p-groups of order p^{p+2} without irregular sections of order p^{p+1}. (See §§7, 11.)

1826. Study the irregular p-groups $G = \Omega_1(G)$ such that (i) all their subgroups of order p^p and exponent p are normal, (ii) all their nonnormal subgroups of order p^p and exponent p are of maximal class. (See #1735.)

1827. Does there exist p-groups G all of whose maximal subgroups have trivial Schur multipliers but the Schur multiplier of G is nontrivial?

1828. Study the 2-groups G such that G/G'' is (i) a U_2-group (see §§17, 18, 67), (ii) of maximal class, (iii) special.

1829. Study the p-groups G with exactly one regular (irregular) maximal subgroup. (As Mann noticed, in the second case, $\mathrm{d}(G) \leq 3$, but it is not known if equality is possible here.)

1830. Classify the p-groups all of whose nonnormal noncyclic subgroups have the same order. (See §112.)

1831. Study the p-groups $G = AB$, where $A, B < G$ with $|A'| \leq p$, $|B'| \leq p$.

1832. Study the p-groups G all of whose normal subgroups are incident with $\Phi(G)$ (with G').

1833. Study the irregular p-groups $G = AB$, where A and B are absolutely regular.

1834. Study the groups G of order p^m such that for each $n \in \{4, \ldots, m-1\}$ there is in G an $\mathcal{A}_2$-subgroup of order p^n.

1835. Suppose that the orders of minimal nonabelian subgroups of a p-group G are $p^{n_1}, \ldots, p^{n_k}$, $k > 1$ and $n_1 < \cdots < n_k$. Study the structure of G provided it has exactly one minimal nonabelian subgroup of every order $p^{n_2}, \ldots, p^{n_k}$.

1836. Study the irregular p-groups $G = \Omega_1(G)$ of order $> p^{p+1}$ all of whose subgroups of order p^p are normal.

1837. Study the groups of exponent p all of whose nonabelian two-generator subgroups are of maximal class.

1838. Classify the p-groups all of whose two noncommuting elements of different orders generate a metacyclic subgroup.

1839. Given $d > 1$, does there exist a p-group G of rank d whose set of maximal subgroups $\Gamma_1 = \{M_1, \ldots, M_k\}$ ($k = 1 + p + \cdots + p^{d-1}$) is such that M_i is an $\mathcal{A}_{n_i}$-group (we consider abelian groups as $\mathcal{A}_0$-groups) and $n_1 < \cdots < n_k$? Describe all possible values of d.

1840. Study the nonmetabelian p-groups G satisfying $|A\Phi(G) : A| = p$ for all minimal nonabelian $A < G$ that are not contained in $\Phi(G)$. (See #2093.)

1841. Study the nonabelian p-groups G such that whenever $A \lhd G$ is maximal abelian and $x \in G - A$, then $\mathrm{C}_A(x)$ is cyclic. (See Lemma 57.1.)

1842. Classify the p-groups G possessing a subgroup of order p^2 contained in only one subgroup of order p^3.

1843. Describe the p-groups H such that $G/\Omega_1(G) \cong H$ for some p-group G.

1844. Study the p-groups all of whose nonnormal subgroups are either absolutely regular or of maximal class or of exponent p.

1845. Study the p-groups G containing an abelian subgroup A of type (p, p) such that $|\mathrm{N}_G(A)| \leq p^4$.

1846. Study the p-groups G such that $\Omega_1(G)$ is special. (See §60.)

1847. Study the p-groups all of whose abelian (minimal nonabelian) subgroups are contained in two-generator maximal subgroups.

1848. Given an abelian p-group A, decide whether or not there is a p-group G such that $\mathrm{Aut}(G) \cong A$. (See #1906.)

1849. Study the p-groups G containing a maximal subgroup H such that all normal subgroups of H are normal in G. (See §125.)

1850. Study the 2-groups G such that $G/\mho_2(G)$ is (i) minimal nonmetacyclic, (ii) special, (iii) of maximal class.

1851. Classify the p-group that are lattice isomorphic to p-groups of maximal class with abelian subgroup of index p.

1852. Study the 2-groups with > 1 metacyclic maximal subgroups.

1853. Given n, does there exist a special p-group all of whose subgroups of index $\leq p^n$ are special?

1854. Study the p-groups with $\leq p+1$ conjugate classes of nonnormal (i) subgroups, (ii) abelian subgroups, (iii) cyclic subgroups (three problems).

1855. Study the p-groups such that whenever $A, B < G$ are (i) distinct conjugate, (ii) distinct of same order, then $|A : (A \cap B)| = p$ (two problems).

1856. Classify the p-groups G such that whenever $H < G$ is minimal nonabelian and $A < H$ is maximal, then $\mathrm{C}_G(A) = A$.

1857. Study the p-groups G satisfying $\mathrm{N}_G(H) = H^G$ for all nonnormal $H < G$.

1858. Classify the p-groups G such that whenever $A < G$ is nonnormal abelian, then $A \leq \mathrm{Z}(\mathrm{N}_G(A))$.

1859. Classify the 2-groups G satisfying $\mathrm{c}_1(\Omega_2^*(G)) = 3$.

1860. Study the p-groups G of exponent $p > 3$ such that whenever $A < G$ is nonabelian of order p^3, then $A < B < G$, where B is of maximal class and order p^p.

1861. Study the p-groups G of order p^m containing a subgroup L of order $p^n < p^{m-2}$ such that all members of the set Γ_1 that contain L are of maximal class.[11]

1862. Study the p-groups G such that the subgroup $\Phi(G)$ (the subgroup G') is the unique G-invariant subgroup of its order (two problems).

1863. Study the p-groups G, $p > 2$, such that whenever $A < G$ is maximal absolutely regular, then all subgroups of G of order $p|A|$ are irregular.

1864. Study the p-groups G all of whose subgroups of order $|\Phi(G)|$ are isomorphic.

1865. Study the p-groups in which any two noncommuting elements generate either a minimal nonabelian subgroup or a subgroup of maximal class or a metacyclic subgroup.

1866. Classify the 2-groups all of whose minimal nonabelian subgroups, except one, are $\cong \mathscr{H}_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^3 \rangle$.

1867. Study the p-groups G in which any two minimal nonabelian subgroups generate an $\mathscr{A}_2$-subgroup.

1868. Let G be a group of maximal class and order p^m, $p > 2$. Find

$$\max\{|H| \mid H < G,\ H_G = \{1\}\}.$$

[11] If $n = 1$, then G is of maximal class. Assume that this is false. Then we have $G/G' \cong \mathrm{E}_{p^3}$ (Theorem 12.12(a)) and $L \not\leq G' = \Phi(G)$ (Theorem 13.6). Write $F = LG'$; then $|G : F| = p^2$. In this case, all members of the set Γ_1 containing F are of maximal class by hypothesis. Then, by Exercise 13.10(a), G is of maximal class, contrary to the assumption.

1869. Classify the p-groups all of whose nonabelian maximal subgroups, except one, are metacyclic. (See §87.)

1870. Study the p-groups G containing a central cyclic subgroup R such that G/R is (i) minimal nonabelian, (ii) special, (iii) metacyclic.

1871. Study the groups of order p^{2m+1} with $\mathrm{cd}(G) = \{1, p, p^2, \ldots, p^m\}$ and describe the set $\mathrm{cd}(G/\mathrm{Z}(G))$.

1872. Study the p-groups G such that whenever $M < G$ is maximal cyclic, then G/M^G is cyclic.

1873. Study the p-groups G such that Sylow p-subgroups of $\mathrm{Aut}(G)$ are isomorphic to Sylow p-subgroups of $\mathrm{Aut}(A)$, where A is an abelian p-group.

1874. Study the p-groups G such that whenever $N \lhd G$ with nonabelian G/N, then $\mathrm{Z}(G/N)$ is cyclic.

1875. Let G be a p-group and $G = H_0 > H_1 > \cdots > H_s$ a normal series of G such that H_i/H_{i+1} is elementary abelian. Suppose that $s = s(G)$ is minimal possible. Now let $\{1\} = K_0 < K_1 < \cdots < K_u = G$ be a normal series of G such that K_i/K_{i-1} is elementary abelian. Suppose that $u = u(G)$ is minimal possible. Does there exist a connection between the numbers $s(G)$ and $u(G)$?

1876. Study the p-groups G whose Schur multipliers are elementary abelian.

1877. Let $G \in \{\Sigma_{p^n}, UT(m, p)\}$. Find

$$\max\{|\mathrm{N}_G(C) : C| \mid C < G \text{ is nonnormal cyclic of order } > p\}.$$

1878. Study the irregular p-groups all of whose nonnormal regular subgroups have regular normalizers.

1879. The intersection of the normalizers of all subgroups of a group G is said to be the *norm* of G and denoted by $\mathcal{N}(G)$. Classify the p-groups G with $\mathcal{N}(H) \leq \mathcal{N}(G)$ for all nonabelian $H \leq G$. In particular, classify the p-groups G such that $\mathcal{N}(H) = H \cap \mathcal{N}(G)$ for all nonabelian $H \leq G$.

1880. Let $G = B(d, p^n)$ be the restricted d-generator Burnside group of exponent $p^n > p$. Study the structure of $\Phi(G)$, $\mho_1(G)$, G', $\Omega_1(G)$, find the orders of (i) the maximal subgroups of G of exponent p, (ii) the maximal elementary abelian subgroups of G, (iii) the maximal normal elementary abelian subgroups of G. (See §60.)

1881. Study the p-groups G containing a maximal subgroup H such that whenever a minimal nonabelian $A < G$ is not contained in H, then one has $A \cap H \lhd G$. (See Theorem 10.28.)

1882. Classify the p-groups containing only one proper irregular subgroup. (In that case, $p > 2$; see Exercise 1.6.)

1883. Classify the p-groups G such that G and all members of the set Γ_1 have trivial Schur multiplier. (Example: Q_{2^n}.)

1884. Study the p-groups G all of whose normal abelian subgroups are contained in $Z_2(G)$.

1885. Study the p-groups G such that $|G' : \Phi(G)'| = p$. (See §111.)

1886 (Old problem). Find the maximal order (maximal rank) of nilpotent subgroups of class 2 in $GL(n, p^m)$ ($SL(n, p^m)$, S_{p^m}).

1887. Let H be a regular p-group with $\exp(H') > p$. Describe the regular p-groups G with $\exp(G') > p$ and such that $H \times G$ is regular. (See [Grov2].) Is it true that the class of such G is bounded?

1888. Study the p-groups G such that whenever $Z < G$ is maximal cyclic, $N_G(Z)$ is (i) abelian, (ii) minimal nonabelian, (iii) metacyclic, (iv) absolutely regular.

1889. Do there exist irregular p-groups, $p > 2$, containing exactly $p + 2$ nonabelian subgroups of order p^p and exponent p? (See Theorem 13.5.)

1890. Study the irregular p-groups G containing exactly p elementary abelian subgroups of order p^p. (If $p = 2$, then $G \in \{D_8, SD_{16}\}$; see Theorem 1.17(b).)

1891. Do there exist a prime p and a group G of order p^p and exponent p such that p^2 divides $\exp(\mathrm{Aut}(G))$?

1892. Do there exist p and an irregular p-group G of order p^{p+1} such that a Sylow p-subgroup of $\mathrm{Aut}(G)$ is regular?

1893. Study the p-groups G such that $\mathrm{cl}(P) < \mathrm{cl}(G)$, where $P \in \mathrm{Syl}_p(\mathrm{Aut}(G))$. (See #1906.)

1894. Classify the $\mathcal{A}_n$-groups with an abelian subgroup of index p.

1895. Study the p-groups such that centralizers of all their noncentral elements are of class ≤ 2.

1896. Given $n > 2$ and $p > 2$, classify the irregular p-groups G of exponent $\geq p^n$ such that $\Omega_n^*(G)$ is absolutely regular.

1897. Let G be a p-group having subgroup breadth $\mathrm{sb}(G) \leq k$ (see #1703). Estimate the number $|G'|$. (For $k = 1$, see §128.)

1898. Study the p-groups G containing a subgroup $H \cong M_{p^4}$ with $C_G(H) < H$.

1899. Let $G = B(p^n, d)$ be the restricted d-generator Burnside group of exponent p^n. Find $\mathrm{sb}(G)$ (see #1703). The same problem arises for Σ_{p^n} and $UT(n, p^m)$.

1900. Study the p-groups that are lattice isomorphic to $M \times E$, where a nonabelian M has a cyclic subgroup of index p and E is elementary abelian.

1901. Describe the p-groups that are lattice isomorphic to representation groups of elementary abelian p-groups. (See §21.)

1902. Study the 2-groups that are lattice isomorphic to 2-groups without normal subgroups $\cong \mathrm{E}_8$. Is it true that such groups have no normal subgroup $\cong \mathrm{E}_8$?

1903. Classify the metacyclic p-groups G such that all p-groups that are lattice isomorphic to G are isomorphic to G.

1904. Study the nonmetacyclic p-groups all of whose nonabelian metacyclic subgroups are of order p^4 and exponent p^2.

1905. Study the pairs of nonisomorphic irregular p-groups G and H of same order such that $\Omega_1(G) \cong \Omega_1(H)$ and $\Omega_2(G) \cong \Omega_2(H)$.

1906 (G.A. Miller). Study the p-groups G with elementary abelian (abelian) $\mathrm{Aut}(G)$.

1907. Let a p-group G be of the form $G = M * C$, where M is irregular of maximal class and C is cyclic, $M \cap C = \mathrm{Z}(M)$. Study the p-groups that are lattice isomorphic to G.

1908. Let G and H be lattice isomorphic p-groups. Is it true that if G has a normal subgroup of order p^{p+1} and exponent p, then H has also such a subgroup?

1909. Study the p-groups all of whose nonabelian two-generator subgroups are (i) metacyclic or of maximal class, (ii) minimal nonabelian or of maximal class, (iii) absolutely regular or of maximal class.

1910. Find the exact upper bound of the class of metacyclic p-groups all of whose maximal subgroups have class at most n. (See Theorem A.38.11.)

1911. Classify the p-groups G such that G and all its maximal subgroups have the same cyclic derived subgroup.

1912. Let p-groups G and H be lattice isomorphic and let G' be cyclic. Study the structure of H'.

1913. Classify the 2-groups G containing an element $t \neq 1$ such that $\mathrm{C}_G(t)/\langle t \rangle$ is of maximal class. (See §49.)

1914. Study the p-groups G such that whenever $A < B < G$ are nonnormal in G, then $|B^G : A^G| = |B : A|$.

1915. Estimate the number of subgroups $\cong \mathrm{Q}_8$ in an extraspecial 2-group of given order. (See Example 76.1.)

1916. Study the irregular p-groups G containing two distinct $F, H \in \Gamma_1$ such that F is of maximal class and H is abelian (minimal nonabelian, metacyclic, special).

1917. Construct a p-group G such that $\mathrm{d}(G) > 2$ and all members of the set Γ_2 (of index p^2) are special.

1918. Is it possible to estimate the derived length of a d-generator p-group G, $d > 2$ is fixed, in terms of n, where p^n is the maximal order of two-generator subgroups of G?[12]

1919. Describe the automorphism groups of Macdonald p-groups (see subsection 25^o of Appendix 40.)

1920. Classify the p-groups all of whose maximal cyclic subgroups of composite orders are self-centralizing. (This problem was solved for $p = 2$; see Theorem A.12.1.)

1921. Classify the p-groups G such that a Sylow p-subgroup of $\mathrm{Aut}(G)$ is of maximal class.

1922. Given d, does there exist a p-group G such that whenever $\{a_1, \ldots, a_d\}$ is an arbitrary minimal system of generators of G, then the breadths of the elements $a_1, \ldots, a_d$ are pairwise distinct? (See #1814.)

1923. Study the p-groups G such that $|G : \mathrm{N}_G(H)|$ is the same for all nonnormal subgroups $H < G$.

1924. Study the p-groups G, $p > 2$, such that $\mathrm{Z}_{p-1}(G)$ is absolutely regular.

1925. Study the p-groups such that whenever $H < G$ is minimal nonabelian, then $H \cap \mathcal{N}(G) = \{1\}$. Here $\mathcal{N}(G)$ is the norm of G.

1926. Study the p-groups of exponent p all of whose nonabelian subgroups of order p^3 are nonnormal.

1927 (Old problem). Given $n > 3$, study the nonabelian groups G of order p^n such that $\mathrm{k}(G) \geq \mathrm{k}(H)$ for all nonabelian groups H of order p^n.

1928. Classify the groups of exponent $p > 2$ all of whose two-generator subgroups have orders at most p^4.

1929. Study the p-groups G having an irreducible character of degree $|G|/\exp(G)$.

1930. Classify the special p-groups G with $\mathrm{Z}(G) \cong \mathrm{E}_{p^2}$. Given $\mathrm{d}(G) = d > 2$, find the maximal order of abelian subgroups and the order of the Schur multiplier of G.

1931. Find the Schur multiplier of a p-group G in which G' is the unique minimal normal subgroup.

1932. Classify the groups of exponent p (i) that have at least one representation group of exponent p, (ii) all of whose representation groups have exponent p.

1933. Let $H \not\leq \Phi(G)$ be a normal subgroup of a p-group G. Study the structure of G provided all maximal subgroups of G not containing H, are (i) extraspecial, (ii) of maximal class.

[12]Commentary of Mann: Without restriction on d, the answer is 'no'. Indeed, if $q \geq 4$ is a prime-power, the derived length of the maximal finite d-generator group of exponent q goes to infinity with d, by Razmyslov, but n above remains bounded, it depends only on q, by Kostrikin–Zelmanov.

1934. Study the p-groups G with $\mathrm{sb}(H) = 1$ for all nonabelian $H \in \Gamma_1$. (See §128.)

1935. Study the p-groups G satisfying $|G : A\mathrm{C}_G(A)| = p$ for all nonabelian $A < G$.

1936. Study the p-groups G such that H_G is characteristic for all nonnormal $H < G$.

1937. Classify the 2-groups all of whose maximal subgroups are either metacyclic or U_2-groups. (See §67.)

1938. Study the p-groups G such that $\exp(G)$ does not divide $\exp(\mathrm{Aut}(G))$. Consider such abelian G in most possible detail.

1939. Study the p-groups G containing a maximal subgroup H such that all subgroups of G not contained in H are two-generator.[13]

1940. Study the p-groups $G = \Omega_1(G)$ such that whenever noncommuting $x, y \in G$ of order p, the $\langle x, y\rangle$ is (i) minimal nonabelian, (ii) of maximal class.

1941. Given n, study the p-groups $G = \Omega_n^*(G)$ such that every element $u \in G$ of order p^n is contained in a minimal nonabelian subgroup.

1942. Study the p-groups G such that for every two nonincident nonabelian subgroups $A, B < G$ we have $A' \cap B' > \{1\}$.

1943. Given n, classify the p-groups of class 2 having the subgroup breadth n.

1944. Study the p-groups G of class $n > p > 2$ satisfying (i) $|\mathrm{Z}_{n-1}(G)| = p^{n-1}$, (ii) $\mathrm{Z}_{n-1}(G)$ is elementary abelian of order p^{n-1}. Is it true that G is irregular?

1945. Study the p-groups G such that whenever $A < G$ is nonnormal and nonincident with $\Phi(G)$ (with G'), then G/A^G is cyclic.

1946. Study the p-groups G satisfying $|G/\ker(\chi)| \le p^2\chi(1)^2$ for all $\chi \in \mathrm{Irr}(G)$.

1947. Study the p-groups G such that $C \le \mathrm{Z}(\mathrm{N}_G(C))$ for all cyclic $C < G$.

1948 (Isaacs–Passman). Classify the p-groups G all of whose nonlinear irreducible characters have the same degree.

1949. Study the p-groups G such that all representation groups of G have exponent $= \exp(G)$.

1950. Study the p-groups G such that any two distinct maximal metacyclic subgroups of G have cyclic intersection.

1951. B. Sambale (letters at 29/7/09 and 30/7/09) presented a pair $H < G$ of 2-groups such $\mathrm{Aut}(H) \cong \mathrm{Aut}(G)$; see §126. (i) Does there exist a pair of p-groups $H < G$, $p > 2$, such that $\mathrm{Aut}(H) \cong \mathrm{Aut}(G)$? (ii) Is it true that, for a fixed p, there is only a finite number of pairs of p-groups $H < G$ such that $\mathrm{Aut}(H) \cong \mathrm{Aut}(G)$?

[13] If $\exp(G) = p$, then G is of maximal class. Indeed, there is in G a minimal nonabelian $A \not\le H$ (Theorem 10.28). It is easy to see that $\mathrm{C}_G(A) < A$. It follows from Proposition 10.17 that G is of maximal class.

1952. Study the p-groups all of whose minimal nonabelian subgroups are either metacyclic or of exponent p.

1953. Study the p-groups G such that $\mathrm{Z}(A) \leq \mathrm{Z}(G)$ for all nonabelian $A < G$.

1954. Classify the p-groups G satisfying $\mathcal{N}(H) = \mathrm{Z}(H)$ for all non-Dedekindian $H \leq G$ (here $\mathcal{N}(G)$ is the norm of G).

1955. Study the nonabelian p-groups $G = \Omega_1(G)$ that are not generated by subgroups of exponent p and class 2. (See §135.)

1956. Study the p-groups satisfying $G' = H'$ for all $H \in \Gamma_1$.

1957. Study the p-groups all of whose maximal subgroups, except one, have class smaller than or equal to 2.

1958. Given $n > 1$, study the p-groups G such that $\Omega_n(H)$ is abelian for all $H \in \Gamma_1$ but $\Omega_n(G)$ is nonabelian.

1959. Let A be a maximal normal abelian subgroup of $G = \Omega_1(G)$. Study the structure of G provided $\mathrm{cl}(\langle x, A\rangle) = 2$ for all $x \in G - A$ of order p.

1960. Let M be a normal irregular subgroup of maximal class of a p-group $G = \Omega_1(G)$. Study the structure of G provided the subgroup $\langle x, M\rangle$ is of maximal class for all $x \in G - M$ of order p. (See Exercise 13.10(a) and Proposition 13.18(a).)

1961. Study the p-groups G such that whenever a subgroup $A < G$ is not normal, then (i) $\mathrm{N}_G(A) \leq A^G$, (ii) $A^G \leq \mathrm{N}_G(A)$ (two problems).

1962. Classify the p-groups G of maximal class, $p > 2$, whose groups of automorphisms are p-groups of maximal class. (In the case under consideration, one has the equality $|\mathrm{Aut}(G)| = |G|$ by Theorem 12.12(a) and Corollary 32.2.)

1963. Let A be a maximal normal abelian subgroup of a p-group G. Study the structure of G provided for every $a \in A - \mathrm{Z}(G)$ there is $x \in G - A$ such that $\langle a, x\rangle$ is minimal nonabelian. (Compare with Lemma 57.1.)

1964. Study the p-groups G such that whenever $G = \langle A, B\rangle$, where $A, B < G$, then $A_G B_G > \{1\}$.

1965. Study the p-groups G such that whenever $A < G$ is minimal nonabelian, then either $\Omega_1(A) = A$ or $A \cong \mathrm{M}_{p^n}$ for some n.

1966. Study the p-groups G such that for all $\mathcal{A}_1$-subgroups $A < G$ one has (i) $\mathrm{N}_G(A)$ is an $\mathcal{A}_2$-group, (ii) $|\mathrm{N}_G(A) : A| = p$.

1967. Is it true that the derived length of a p-group G is bounded provided for all nonnormal cyclic $H < G$ we have $|G : \mathrm{N}_G(H)| \leq p^2$?

1968. Study the p-groups G such that $|\mathrm{N}_G(A) : \mathrm{C}_G(A)| \leq p$ for all nonnormal abelian $A < G$.

1969. Classify the nonmetacyclic two-generator 2-groups G containing exactly two two-generator maximal subgroups. (See Theorem 71.6. This is solved in §129.)

1970. Study the nonabelian p-groups G with a nonabelian $A \in \Gamma_1$ such that whenever $x \in A - \mathrm{Z}(G)$, then $\mathrm{C}_G(x) \leq A$. (See #1812.)

1971. Classify the p-groups in which any two conjugate cyclic subgroups generate a metacyclic subgroup.

1972. Classify the p-groups G such that there are exactly $p-1$ minimal nonabelian subgroups not contained in $\mathrm{Z}_2(G)$. (See §76.)

1973. Study the p-groups G such that $\Phi(H)$ ($\mathfrak{V}_1(H)$) is cyclic (abelian, absolutely regular) for all $H \in \Gamma_1$ but $\Phi(G)$ ($\mathfrak{V}_1(G)$) is noncyclic (nonabelian, non-absolutely regular), respectively.

1974. Find all possible residues modulo p^3 of numbers of maximal chains in groups of exponent p.

1975. Study the p-groups G containing a maximal subgroup H such that whenever $A < G$ is abelian, then either $A \leq H$ or $A < M < G$, where M is a minimal nonabelian.

1976. Classify the groups of exponent p and coclass 2.

1977. Suppose that a p-group G contains an abelian subgroup of index p and G has no subgroup $\cong \Sigma_{p^2}$. Is it true that $\exp(\Omega_1(G)) = p$? (See §135.)

1978. Classify the 2-groups all of whose nonnormal subgroups are either cyclic or of maximal class. (This is solved in §117.)

1979. Classify the p-groups G of maximal class, $p > 2$, whose groups of automorphisms are p-groups of maximal class. (In the case under consideration, G satisfies $|\mathrm{Aut}(G)| = |G|$.)

1980. Let A be a maximal normal abelian subgroup of G. Study the structure of G provided, for any two noncommuting $a \in A - \mathrm{Z}(G)$ and $x \in G - A$, the subgroup $\langle a, x\rangle$ is (i) metacyclic, (ii) minimal nonabelian (see Lemma 57.1), (iii) of maximal class. Consider these three problems in the case where $A \lhd G$ is nonabelian.

1981. Study the p-groups G such that whenever $x \in A < G$, where A is minimal nonabelian, then $|G : \mathrm{C}_G(x)| \leq p$.

1982. Suppose that M is a 'large' generating subset of a nonabelian p-group G (for example, $|M| \geq \frac{1}{p}|G|$). Is it possible to estimate $\mathrm{cl}(G)$ and $\mathrm{dl}(G)$ if $|G : \mathrm{C}_G(x)| \leq p$ for all $x \in M$?

1983. Let $G = \mathrm{B}(d, p)$ be a maximal finite d-generator p-group of exponent $p > 2$. (i) Describe the structure of $\Phi(G)$. (ii) Estimate the maximal order of abelian (normal abelian, normal elementary abelian) subgroups of G.

1984. Study the p-groups G of exponent p^2 all of whose minimal nonabelian subgroups have order p^5.

1985. Given $k > 0$, study the nonabelian p-groups (i) $G = \Omega_k^*(G)$ that are not generated by minimal nonabelian subgroups of exponent p^k, (ii) $G = \Omega_k(G)$ that are not generated by minimal nonabelian subgroups of exponent $\leq p^k$. (For a number of related results, see §§30, 135.)

1986. A group is p-said to be a QE_p*-group* if it is not a product of two nonquasinormal subgroups. Classify the two-generator QE_p-groups. (See §110.)

1987. Let G be an irregular p-group all of whose proper sections are regular (see Mann's Theorem 7.4). Describe the Schur multiplier and representation groups of G.

1988. Find the Schur multiplier of a nonabelian p-group containing an abelian subgroup A of index p.

1989. Study the p-groups G possessing an automorphism ϕ of order p^2 such that $\mathrm{C}_G(\phi)$ is cyclic.

1990. Study the p-groups G with $\mathrm{d}(G) > 2$ that contain $\leq p + 1$ maximal subgroups which are not (i) metacyclic, (ii) absolutely regular ($p > 2$), (iii) extraspecial (three problems).

1991. Classify the p-groups G that contain exactly one maximal subgroup not generated by elements of order p. (See §§30, 135.)

1992. Suppose that the Schur multiplier of a representation group of a p-group G is trivial. Estimate the orders of the Schur multipliers of all other representation groups of G.

1993. Classify the p-groups G such that the norm $\mathcal{N}(G)$ is maximal in G. (If $G \cong \mathrm{M}_{p^n}$, then $|G : \mathcal{N}(G)| = p$.)

1994. Study the p-groups G containing an abelian subgroup A of type (p, p) such that $\mathrm{C}_G(A)$ is metacyclic.

1995. Classify the p-groups containing a nonabelian subgroup of order p^3 and exponent p and all such subgroups are conjugate.

1996. Study the p-groups G containing the same number of normal subgroups of every order $p, \ldots, \frac{1}{p}|G|$.

1997. Study the p-groups G of exponent $> p$ such that whenever $C > \{1\}$ is a nonmaximal cyclic subgroup of G, then C is contained in exactly p cyclic subgroups of G of order $p|C|$.

1998. Classify the metacyclic p-groups containing a proper subgroup $\cong \mathrm{M}_{p^n}$, $n > 3$. (See Proposition 10.19 and §124.)

1999. Classify the p-groups G such that A is a direct factor of $\mathrm{N}_G(A)$ for all nonnormal $A < G$. (See Theorem 1.25.)

2000. Study the p-groups G possessing nonnormal subgroup of order p^p and exponent p such that any two distinct such subgroups have intersection of order p^{p-1}.

2001. Study the p-groups G containing a maximal subgroup H such that normalizers of all maximal subgroups of H, except one, coincide with H.

2002. Given $k > 1$ and a p-group H, does there exist an overgroup G of H of order $p^k|H|$, $k > 1$, such that for all $H < F < G$ the subgroup F is characteristic in G?

2003. Classify the metacyclic p-groups all of whose normal subgroups are characteristic.

2004. Given $k > 1$, study the p-groups G all of whose subgroups of index p^k contain $\Phi(G)$.

2005. Study the p-groups G with only one representation group and nonidentity Schur multiplier.

2006. Study the irregular p-groups G all of whose maximal regular subgroups are members of the set Γ_1.

2007. Suppose that a p-group G has a maximal elementary abelian subgroup of order p^k. Is it true that the number of generators of subgroups of G is bounded? If not, find all k for which this takes place. (For $k = 2$, see §§127, 134 and #1592.)

2008. Study the p-groups G such that for every outer p-automorphism ϕ of G the subgroup $\mathrm{C}_G(\phi)$ has order p.

2009. Does there exist an irregular group G of order p^{p+2}, $p > 2$, such that $G_0 = G^\phi$ is regular, where $\phi : G \to G_0$ is a lattice isomorphism? (See Appendix 42.)

2010. Given $m > 1$, study the groups G of exponent p all of whose subgroups of index $\leq p^m$ are normal.

2011. Study the p-groups G such that $|G : \mathrm{C}_G(P)| \leq p^2$ for $P \in \mathrm{Syl}_p(\mathrm{Aut}(G))$.

2012. Classify the p-groups G satisfying $\mathcal{N}(H) \not\leq \mathcal{N}(G)$ for all non-Dedekindian $H < G$ (see #1769).

2013. Study the p-groups G such that whenever $x \in G - \Phi(G)$ ($x \in G - G'$), then all elements of the coset $x\Phi(G)$ (xG') are of equal order (two problems).

2014. Study the p-groups G such that $|\mathrm{N}_G(M) : M| = p$ and $\mathrm{C}_G(M) < M$ for some extraspecial $M < G$.

2015. Study the p-groups G such that whenever nonabelian $A, B < G$ are of same order, then $\alpha_1(A) = \alpha_1(B)$.

2016. Classify the nonabelian p-groups G such that a Sylow p-subgroup of $\mathrm{Aut}(G)$ is isomorphic to $\mathrm{UT}(n, p)$. (Compare with #35.)

2017. (i) Does there exist a p-group all of whose maximal subgroups have pairwise distinct classes? (ii) Study the p-groups G all of whose maximal subgroups have the same class.

2018. Classify the metacyclic (minimal nonabelian) p-groups with trivial Schur multiplier.

2019. Given $k \in \{3, \ldots, p\}$, find, modulo p^2, all possible numbers of p-subgroups of maximal class and order p^k in a p-group.

2020. Let G be a metacyclic 2-group and H be a 2-group with $|L_{2^2}(H)| = |L_{2^2}(G)|$ (see #1690). Study the structure of H. (See §§52, 124.)

2021. Study the p-groups, $p > 2$, all of whose minimal nonabelian subgroups, except one, (i) have exponent p, (ii) are isomorphic to M_{p^n} (two problems).

2022. Study the p-groups G such that $|L_{p^n}| = 2p^n$ for some n (see #1690).

2023 (Old problem). Study the p-groups $G = AB$ satisfying $\mathrm{k}(G) = \mathrm{k}(A)\mathrm{k}(B)$.

2024. Study the p-groups containing a nonnormal nonabelian metacyclic subgroup (extraspecial subgroup) whose normalizer is metacyclic (extraspecial).

2025. Let p-groups G and W of equal order be such that the lattice of subgroups of G is isomorphic to the lattice of normal subgroups of W and W is nonabelian. Study the structures of G and W.

2026. Does there exist a p-group G of maximal class, $p > 2$, with $|G| = |\mathrm{Aut}(G)|$?

2027. Find the Schur multipliers of special p-groups with center of order p^2.

2028. Study the p-groups G all of whose maximal subgroups have the same derived subgroup distinct of G'. (See Exercise 1.69.)

2029. Classify the p-groups G such that $\mathrm{C}_G(E)$ is metacyclic for some abelian subgroup $E < G$ of type (p, p).

2030 (P. Hall). Study the p-groups generated by normal abelian subgroups.

2031. Classify the p-groups G whose lattice of subgroups is isomorphic to the lattice of normal subgroups of a special p-group. (See #2025.)

2032. Does there exist a group of exponent p and order $> p$ all of whose maximal subgroups are characteristic?

2033. Study the p-groups G of exponent $> p$ containing an element x of order p and a subgroup E of order $> p^p$ which is maximal of exponent p and such that $|\mathrm{C}_E(x)| = p$. Consider the partial case when E is elementary abelian.

2034. Study the p-groups G such that whenever $x, y \in G - \mathrm{Z}(G)$ with $\langle x, \mathrm{Z}(G)\rangle \neq \langle y, \mathrm{Z}(G)\rangle$, then $\mathrm{C}_G(x) \neq \mathrm{C}_G(y)$.

2035. Study the p-groups G such that $\exp(G) = \exp(\Gamma)$, where Γ is a representation group of G.

2036. Study the power structure of the p-groups $G = AB$, where A and B are elementary abelian.

2037. Classify the characteristic subgroups of (i) abelian p-groups, (ii) minimal nonabelian p-groups and (iii) $\mathfrak{A}_2$-groups.

2038. Describe the set of positive integers n such that there is an elementary abelian p-group G admitting an irredundant covering by n maximal subgroups. (See §116.)

2039. Classify the E_p-groups containing a subgroup of index p which is (i) abelian, (ii) metacyclic. (See §110.)

2040. Classify the p-groups G such that whenever $H < G$ is nonnormal, then $H < M \in \Gamma_1$, where M is of maximal class. (Example: $G = D * C$, where $D = \Omega_1(G)$ is nonabelian of order p^3 and $C \cong \mathrm{C}_{p^2}$. See #1861.)

2041. Study the subgroup structure of the groups $G_\pm = \langle a, b \mid a^{2^m} = b^{2^n}, a^b = a^{\pm 1+2^{n-1}}, m > 1\rangle$.

2042. Study the structure of the intersection of normalizers of all minimal nonabelian subgroups.

2043. Study the p-groups G such that whenever $A < M < G$, where M is minimal nonabelian, then there exists $H < G$ such that $M \cap H = A$.

2044. Study the p-groups G such that whenever $A < G$ is maximal abelian, then $\Omega_1(A)$ is a maximal elementary abelian subgroup of G.

2045. Classify the nonabelian p-groups G such that $H' = \Phi(H)$ for all nonabelian $H \leq G$ (such G are classified for $p = 2$; see §90).

2046. Study the p-groups G containing a cyclic subgroup M of order p^2 such that $\mathrm{N}_G(M)$ is abelian of type (p^2, p).

2047. Classify the p-groups all of whose minimal nonabelian subgroups have cyclic centralizers. (This is solved in Appendix 41.)

2048. Study the p-groups all of whose maximal subgroups are not generated by elements of same order. (See [O'BSV-L].)

2049. Determine the possible numbers of generators of maximal subgroups of two-generator groups of exponent p.

2050 (Old problem). Study the p-groups in which every two conjugate subgroups have the same normalizer.[14]

2051. Study the 2-groups G all of whose maximal metacyclic subgroups are members of the set Γ_1.

2052. Find all possible values of

$$|\{H \in \Gamma_1 \mid \mathrm{d}(H) = 2\}|, \quad |\{H \in \Gamma_1 \mid H \text{ is minimal nonabelian}\}|,$$
$$|\{H \in \Gamma_1 \mid H \text{ is nonmetacyclic}\}|,$$

where G runs over all p-groups. (See §§71, 100, 66, 87, Exercise A.40.14.)

2053. Study the p-groups with only one normal maximal cyclic subgroup.

2054. Given n, does there exist a p-group G all of whose subgroups of order p^n are pairwise nonisomorphic?

2055. Describe the p-groups G containing a nonabelian subgroup M of order p^4 such that $\mathrm{C}_G(M) < M$.

2056 (Old problem). Study the p-groups containing a self-centralizing cyclic subgroup. (See #1920.)

2057. Study the p-groups G such that whenever $L \leq \mathrm{Z}(G)$ is of order p, then G/L is special.

2058. Let G be a 2-group of maximal class and V be a Sylow subgroup of its holomorph. (i) Describe the maximal subgroups of V. (ii) Let W be a nonsplit extension of G by a Sylow 2-subgroups of $\mathrm{Aut}(G)$. Find the ranks of all maximal subgroups of W. (See Theorem 34.8.)

2059. Given $n \in \{p+1, \ldots, m-2\}$, study the groups of order $p^m > p^{p+2}$ containing exactly p^2 subgroups of maximal class and order p^n. (See Theorems 12.12(c) and 13.6.)

2060. Let G be an abelian group of type $(2^n, 2)$, $n > 1$, and let V be its holomorph. (i) Describe the maximal subgroups of V. (See Exercise A.40.14.) (ii) Let W be a nonsplit extension of our G by a group $\cong \mathrm{Aut}(G)$. Describe the maximal subgroups of W.

2061. Study the p-groups all of whose nonabelian three-generator subgroups are $\mathcal{A}_2$-subgroups.

2062. Study the p-groups G such that whenever $H < G$, then the lattice of subgroups of G containing H is isomorphic to the lattice of subgroups of a certain group.

[14] Commentary of Mann: In this case, such groups are exactly the groups all of whose normalizers are normal. There are papers devoted to this problem, for example, [OP], and, for partial case, [M18].

2063 (Old problems). (i) Study the p-groups G such that whenever $N \lhd G$, there is in G a subgroup isomorphic to G/N. Classify the p-groups of maximal class (metacyclic p-groups) satisfying this condition. (ii) Study the p-groups G such that whenever $H < G$, there exists $N \lhd G$ such that $G/N \cong H$. (Example to both problems: $G = \mathrm{D}_{2^n}$.)

2064. Given a p-group G, does there exist an abelian p-group A such that for some nonsplit extension, say E, of A by G one has $\mathrm{C}_E(A) = A$?

2065. Classify the p-groups G such that all members of the set Γ_1, except one, are (i) of class ≤ 2, (ii) special.

2066. Classify the p-groups G such that every maximal abelian subgroup of G is contained in only one member of the set Γ_1. (Example: any p-group of maximal class with abelian subgroup of index p.)

2067. Study the 2-groups all of whose minimal nonabelian subgroups have exponent 4. (See Lemmas 65.1, 57.1 and 57.2.)

2068. Study the p-groups all of whose maximal subgroups, except one, are either $\mathscr{A}_1$- or $\mathscr{A}_2$-group.

2069. Study the nonabelian p-groups G of exponent p such that $A \cap \mathrm{Z}(G) = \{1\}$ for all minimal nonabelian $A < G$.

2070. Describe the representation groups of p-groups of maximal class and order p^{p+1}, $p > 2$.

2071. Study the p-groups G such that there are $A, M \in \Gamma_1$, where A is minimal nonabelian and M is irregular of maximal class.

2072. Study the p-groups G such that $\mathrm{N}_G(C)$ is abelian of type $(p, |C|)$ for all maximal cyclic $C < G$.

2073. Estimate $|\mathrm{Aut}(G) : \mathrm{Inn}(G)|$, where G is a p-group of maximal class. (For the case $p = 2$, see Theorem 34.8.)

2074. Let $L \cong \mathrm{C}_{2^n}$, $n > 2$, be a normal subgroup of a 2-group G such that $\mathrm{C}_G(L) = L$ and G/L is isomorphic to the abelian group of type $(2^{n-2}, 2)$. Describe all subgroups and epimorphic images of G.

2075. Suppose that a 2-group G contains a maximal abelian normal subgroup L of type $(2^n, 2^n)$ such that G/L is isomorphic to a Sylow 2-subgroup of $\mathrm{Aut}(L)$. Describe the structure of G and all its maximal subgroups. How many of such G exist?

2076. Study the p-groups G such that whenever $M \in \Gamma_1$, then all elements of the set $G - M$ have equal order.

2077 (Old problem). Study the normal and the subgroup structure of p-groups G of class p.

2078. Does there exist a p-group of class $p > 2$ all of whose maximal subgroups are irregular? If not, find the minimal n such that there is a p-group of class n all of whose maximal subgroups are irregular. (If $p = 2$, then $n = 2$ as a Sylow 2-subgroup of the simple Suzuki group $\mathrm{Sz}(2^3)$ shows.)

2079. Study the p-groups of exponent p that are not covered by nonabelian subgroups of rank 2.

2080 (Zhmud). Classify the p-groups G such that every irreducible character of G assumes at most four values. (In this case, $\exp(G/G') \leq 5$.)

2081. Study the p-groups G of exponent p such that H is a direct factor of the subgroup (i) $H\mathrm{C}_G(H)$ for all nonabelian $H \leq G$, (ii) $\mathrm{N}_G(H)$ for all nonnormal $H < G$ of order p.

2082. Classify the p-groups lattice isomorphic to the holomorphs of cyclic p-groups.

2083. Study the p-groups G such that $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is cyclic.

2084. Study the p-groups G such that whenever $A \leq G$ is minimal nonabelian, then $A' \lhd G$ and A/A' is a maximal abelian subgroup of G/A. (Metacyclic p-groups satisfy this condition; see Exercise 124.7.)

2085. Study the p-groups G such that $\mathrm{C}_G(x)$ is minimal nonabelian of order p^4 for some $x \in G$.

2086. Let $G = \Sigma_{p^n} \in \mathrm{Syl}_p(\mathrm{S}_{p^n})$, $n > 2$, and let $M \lhd G$ be of minimal order such that the quotient group G/M is regular. Estimate $\mathrm{cl}(G/M)$. The same problem arises for the group $\mathrm{UT}(n, p^m) \in \mathrm{Syl}_p(\mathrm{GL}(n, p^m))$.

2087. Given n, does there exist a group G of exponent p such that $|\mathrm{Z}_n(G)| = p^n$? If not, find the maximal n for which this equality is possible.

2088. Describe the p-groups that are lattice isomorphic to (i) the Burnside p-groups $B(p^n, m)$, (ii) the groups $\mathrm{UT}(n, p^m)$.

2089. Let G be a group of order p^m and exponent p, $m > 3$ and $1 < n < m - 1$. It is known (Theorem 5.9) that $\mathrm{s}_n(G) \equiv 1 + p + 2p^2 + rp^3 \pmod{p^4}$, where r is a nonnegative integer. Find all possible residues $r \pmod{p}$.

2090. Study the p-groups G satisfying $\alpha_2(G) = 2$. (See #895 and §§65, 71, 76.)

2091. Classify the 2-groups G such that $\mathrm{N}_G(C)/C$ is cyclic or generalized quaternion for all nonnormal cyclic $C < G$.

2092. Suppose that $G = A \times B$ is an irregular p-group, $p > 2$, where A and B are regular. Is it true that $A * B$ (central product) is also irregular?

2093. Study the p-groups G all of whose $\mathcal{A}_2$-subgroups are contained in $\Phi(G)$.

2094. A group H is said to be a Φ-*group* if $H \cong \Phi(G)$ for some p-group G. Given n, find the maximum c_n of nilpotence classes of the Φ-groups of order p^n.

2095. Study the nonabelian Φ-subgroups (derived subgroups) whose centers have order p^2.

2096 (I. D. Macdonald). Given $n > 1$, classify the p-groups G of class $2n$ all of whose maximal subgroups have class n. Study the case $\exp(G) = p$ is most possible detail.

2097. Study the irregular p-groups G such that $Z(G) = \mho_1(G)$ is cyclic and that satisfy $|G/\mho_1(G)| = p^p$.

2098. Classify the representation groups of abelian p-groups of rank 2.

2099. Study the p-groups G all of whose normal subgroups are ϕ-invariant for all p-automorphisms ϕ of G.

2100. Study the p-groups G such that for all abelian $A < G$, $N_G(A)/C_G(A)$ is isomorphic to a Sylow p-subgroup of $\mathrm{Aut}(A)$.

2101. Study the p-groups G with $\exp(G) = |G : (G' \cap Z(G))|$. (See Lemma 6.10.1.)

2102. Given $n > 1$, classify the p-groups $G = \Omega_n^*(G)$ such that (i) $C_G(x)$ is G-invariant for all $x \in G$ of order p^n, (ii) $N_G(C)$ is G-invariant for all cyclic $C < G$ of order p^n (two problems).

2103. Study the p-groups that are not generated by $\mathcal{A}_2$-subgroups.

2104. Does there exist a p-group $G = A \times B$ of exponent $> p$, $A' \neq \{1\} \neq B'$, admitting a nontrivial partition?

2105 (A variant of Alperin's problem). Suppose that a group G of exponent p has an abelian subgroup of index p^4. Is it true that G contains a normal abelian subgroup of index p^4?

2106. Given n, study the p-groups G such that $G/\mho_n(G)$ is minimal nonabelian.

2107. Study the representation groups of groups of maximal class and order p^p and exponent p.

2108. Study the p-groups all of whose minimal nonabelian subgroups are complemented in G (have normal complements in G).

2109. Given n and k, study the p-groups containing exactly one conjugate class of size p^k of nonnormal subgroups of order p^n.

2110. Study the p-groups G such that $d(G) > d(H)$ for all $H \in \Gamma_1$. Is it true that $\mathrm{cl}(G)$ is bounded?[15]

[15] E. Crestani has shown that the answer is 'no' if $p = 2$ and $d(G) = 3$; see §113.

2111. Classify the p-groups G all of whose (i) minimal nonabelian subgroups, (ii) proper normal subgroups, (iii) metacyclic subgroups have trivial Schur multipliers (three problems).

2112. Let $\mathrm{s}(X)$ be the number of subgroups of a p-group X. Classify the p-groups G such that $\mathrm{s}(G) \leq |G|$. (We have $\mathrm{s}(\mathrm{Q}_{16}) = 11 < 16$, $\mathrm{s}(\mathrm{SD}_{16}) = 15 < 16$, and $\mathrm{s}(\mathrm{D}_{16}) = 19 > 16$.) Classify the p-groups satisfying $\mathrm{s}(G) = |G|$.

2113. Study the pairs of p-groups $H < G$ such that whenever $F < H$, then either $\mathrm{N}_G(F) \leq H$ or $F \lhd G$. Consider the following partial cases: $H \in \{G', \Phi(G), \mho_1(G)\}$.

2114. Classify the p-groups G, $p > 2$, such that whenever $A < G$ is maximal abelian, then $A < B < G$, where B is irregular of order $p|A|$.

2115. Does there exist a p-group (a group of exponent p), $p > 2$, all of whose maximal subgroups are pairwise nonisomorphic?[16] Does there exist a p-group of exponent p satisfying the condition above?

2116. Study the irregular p-groups G such that $\mathrm{Z}_{p-1}(G) = \Phi(G)$ has order p^{p-1}.

2117. For a definition of U_s-groups, see Definition 18.2. (i) Classify the U_3-groups. (See §67.) (ii) Classify the 2-groups G containing a normal elementary abelian subgroup of order 2^s, $s \in \{2, 3\}$, such that G/R is of maximal class.

2118. Classify the 2-groups G such that whenever $A < G$ is metacyclic of order 2^4, then $A < B < G$, where B is minimal nonmetacyclic of order 2^5.

2119. Study the irregular p-groups G such that whenever $A < G$ is maximal absolutely regular, then $A < B < G$, where B is of maximal class and order $p|A|$. (Compare with Exercise 13.10(a).)

2120. Study the p-groups G such that whenever $A, B < G$ are nonconjugate maximal cyclic, then $|A| \neq |B|$.

2121. Study the nonabelian groups of exponent p all of whose nonabelian subgroups of order p^5 have class 2.

2122. Study the p-groups G such that whenever $A < G$ is maximal abelian and satisfies $A < B \leq G$ with $|B : A| = p$, then $|B'| = p$. (Compare with #1715.)

2123. Study the p-groups G such that $|\mathrm{N}_G(M) : M| = p$ for every maximal absolutely regular subgroup M of G.

[16] Solution by Mann for groups of exponent $> p$. O'Brien–Scoppola–Vaughan-Lee [O'BSV-L] constructed, for all primes p, p-groups which cannot be generated by elements of equal order. Let G be a minimal p-group of such type; then no two maximal subgroups of G are isomorphic. Indeed, assume that H and K are two maximal subgroups of G. By minimality, H can be generated by elements of equal order, say p^e. If $H \cong K$, then K is also generated by elements of order p^e so is $G = HK$, contrary to the hypothesis.

2124. Study the p-groups G such that whenever $F < H < G$, there exists $A < G$ such that $H \cap A = F$.

2125. Describe the automorphism group and the representation groups of a direct product G of two 2-groups of maximal class. List all types of minimal nonabelian subgroups of G.

2126 (Isaacs [Isa8]). Does there exist a p-group (group of exponent p) G admitting a nontrivial partition all of whose components are nonabelian.

2127. Study the 2-groups all of whose maximal elementary abelian subgroups are nonnormal. (For $p > 2$ this is impossible in view of Theorem 10.1.)

2128. Classify the p-groups that contain exactly $p + 1$ noncyclic abelian subgroups of order p^3.

2129. Suppose that a metacyclic p-group G is given by generators and defining relations. Work out an algorithm giving all normal and characteristic subgroups of G.

2130. Study the 2-groups with exactly two conjugate classes of subgroups $\cong \mathrm{E}_8$.

2131. Does there exist a group of exponent p and order p^p that is not a section of any p-group of maximal class.

2132. Classify the groups of exponent p and class > 2 all of whose proper subgroups have class ≤ 2.

2133. Given n, find the minimal possible $\mathrm{c}_n(G)$, where G runs through the set of all irregular p-groups $G = \Omega_n^*(G)$.

2134. Classify the p-groups with exactly two abelian subgroups of index p^2. (See [Kon1] and Theorem 103.5(iii).)

2135. Let G be a central product of n isomorphic minimal nonabelian p-groups with amalgamated derived subgroups. Estimate the subgroup breadth $\mathrm{sb}(G)$ of G.

2136. Classify the 2-groups G such that the subgroup $\mathrm{Z}_4(G)$ is minimal nonmetacyclic. (See §§66, 69.)

2137. Classify the p-groups, $p > 2$, all of whose subgroups of class 2 are either minimal nonabelian or of exponent p.

2138. Classify the 2-groups G such that the subgroup $\Omega_2^*(G)$ is minimal nonmetacyclic of order 2^5.

2139. A p-group G is said to be *generalized extraspecial of height n* if $\mathrm{Z}_n(G) = \Phi(G)$ has order p^n. (i) Study the generalized extraspecial p-groups of height 2. (By Proposition 4.9, $p > 2$.) (ii) Find all n for which there exists an irregular generalized extraspecial p-group, $p > 2$, of height n. (iii) Find all n such that the orders of the generalized extraspecial p-groups of height n and exponent p are not bounded. (iv) Sup-

pose that there is a generalized extraspecial p-group of height n. Is it true that then there exists a generalized extraspecial p-group of height $n+1$?

2140 (Old problem). Suppose that the p-groups G and G_1 are lattice isomorphic. Compare (i) the classes $\mathrm{cl}(G)$ and $\mathrm{cl}(G_1)$, (ii) the derived lengths $\mathrm{dl}(G)$ and $\mathrm{dl}(G_1)$.

2141. Classify the p-groups G such that $\mathrm{cl}(\mathrm{N}_G(A)) \leq 2$ for all nonnormal abelian $A < G$.

2142. Study the p-groups G such that, for any $H \in \Gamma_1$, all non-G-invariant subgroups of H of same order are conjugate in G.

2143. Describe a Sylow p-subgroup of the holomorph of $\mathrm{Hol}(\mathrm{E}_{p^n})(\cong \mathrm{AGL}(n.p))$.

2144. Find all integers $n > p$ such that there exists an irregular p-group of class n all of whose proper subgroups are regular. (See Theorem 7.4.)

2145. Let $\mathrm{sb}(G)$ be a subgroup breadth of a p-group G (see #1703). (i) Find $\mathrm{sb}(G)$ for special p-groups G. (ii) Find $\mathrm{sb}(\Gamma)$ for representation groups Γ of abelian p-groups.

2146. Study the p-groups G such that $\Phi(H) \leq \mathrm{Z}(G)$ for all $H < G$. What can one say about $G/\mathrm{Z}(G)$?

2147. It is known that if $\mathrm{sb}(G) = 1$ (see #1703), then one has $|G'| \leq p^2$ (see §128 and [CSW]). Estimate $|G'|$ for given $\mathrm{sb}(G)$. Study this problem for groups of exponent p and metabelian p-groups.

2148 (Problem from [BDM]). Study the equilibrated p-groups G (= E_p-groups) with $\mathrm{d}(G) > 2$. (See §110.)

2149 (Old problem). Find all n for which the orders of groups G of exponent p and coclass n are bounded. (For $n = 1$, see Theorem 9.5.)

2150. Study the p-groups G all of whose abelian subgroups of type (p, p) are automorphic, i.e., conjugate in the holomorph $\mathrm{Hol}(G)$.

2151. Suppose that a group G of maximal class has the Schur multiplier of order p. Is it true that the representation group of G is of maximal class?

2152. Study the absolutely regular p-groups all of whose representation groups are absolutely regular. (It is known that such representation groups are regular; see Remark 7.2.)

2153. Classify the metacyclic p-groups (groups of exponent p) all of whose normal subgroups of index $> p$ are characteristic.

2154 (Old problem). Classify the p-groups G such that $\mathrm{N}_G(\mathrm{N}_G(H)) = G$ for all subgroups $H < G$.

2155. Study the p-groups G admitting an automorphism α of order p such that $\mathrm{C}_G(\alpha)$ is cyclic. (See §48 and [Bla13].)

2156. Study the normal and power structure of the p-groups G containing a normal cyclic subgroup Z such that G/Z is irregular of maximal class.

2157. Study the normal and power structure of the p-groups G containing a normal subgroup M of maximal class (minimal nonabelian subgroup) such that G/M is cyclic of order $> p$.

2158. Let T be generated by the centers of all nonabelian maximal subgroups of a p-group G. Study the structure of G provided $T = G$.

2159. (i) Classify the two-generator p-groups G with a cyclic derived subgroup.[17] (ii) Study the p-groups G with cyclic G' (see [Che]).

2160. Describe $\mathrm{Aut}(\Sigma_{p^2})$ and all representation groups of Σ_{p^2}.

2161. Given n, study the nonabelian groups G of order p^n with Schur multiplier of maximal possible order.

2162. Study the p-groups G such that whenever a subgroup $M < G$ is of class 2, then $\mathrm{C}_G(M) < M$.

2163. Study the p-groups G all of whose maximal subgroups have metacyclic derived subgroups (Frattini subgroups) but G' ($\Phi(G)$) is not metacyclic.

2164. Study the p-groups G containing an abelian subgroup A of exponent $> p$ such that whenever $C < A$ is cyclic of order $> p$, then $\mathrm{N}_G(C) = A$.

2165. Does there exist a p-group such that the derived subgroups (Frattini subgroups) of all its maximal subgroups are minimal nonabelian (two problems)?

2166. Study the p-groups such that centralizers of all their nonnormal subgroups are cyclic. (See §16.)

2167. Study the p-groups in which every nonabelian maximal subgroup possesses a minimal nonabelian subgroup (metacyclic subgroup) of index p.

2168. Classify the p-groups containing exactly one nonmodular maximal subgroup (non-Dedekindian maximal subgroup). (See Theorem 1.20 and §73.)

2169. Classify the p-groups all of whose proper subgroups contain an abelian subgroup of index p.

2170. Study the p-groups G all of whose subgroups that are nonincident with $\Phi(G)$ are generalized soft (see §130 and #1821).

2171. Study the p-groups G with an abelian (regular) H_p-subgroup, say A. Estimate (if possible) $|G : A|$ in terms of A.

[17] Commentary of Mann: For odd p, it is proved in the paper of Mann and Posnick-Fradkin [MP-F] that a two-generator p-group G has a cyclic derived subgroup G' if and only if $G/\mathrm{Z}(G)$ is metacyclic.

2172 (Ito). Study the p-groups G with three class sizes. Treat the case $\exp(G) = p$ in most possible detail. Classify the p-groups with two class sizes.

2173. Study the p-groups G such that $\mathrm{C}_G(H) = \mathrm{Z}(G)$ for all nonabelian $H < G$.

2174. Classify the irregular p-groups G with $\mathrm{d}(G) > 2$ all of whose nonabelian members of the set Γ_2 are of maximal class.

2175. Study the p-groups G all of whose maximal abelian subgroups are normal and complemented in G. Consider the case $\exp(G) = p$ in most possible detail.

2176. Study the p-groups G all of whose subgroups of index p^2 have an abelian subgroup of index p. (Compare with definition of $\mathcal{A}_3$-groups; see §72.)

2177. Classify the p-groups G such that the set Γ_1 contains $\geq p$ minimal nonabelian (metacyclic) members. (See #861 and §§87, 100–102.)

2178. Given n, study the p-groups G such that $\Omega_n(G) = M \times E$, where M is minimal nonabelian and $\exp(E) \leq p$.

2179. Study the p-groups all of whose maximal subgroups, except one, are two-generator. (See §113.)

2180. Study the p-groups all of whose maximal subgroups are nontrivial direct products.

2181. Study the p-groups G with noncyclic $\Phi(G)$ and such that $M \cap \Phi(G)$ is cyclic for all $M < G$ nonincident with $\Phi(G)$.

2182. Study the p-groups G with $M \in \Gamma_1$ such that $M \cap A$ is cyclic for all abelian subgroups A of G that are not contained in M.

2183. Let $M < G$ be minimal nonabelian. Study the structure of G if for all maximal $A < M$, we have (i) $\mathrm{C}_G(A)$ is abelian, (ii) $\mathrm{N}_G(A)/A$ is cyclic (two problems).

2184. Study the groups G of exponent $p > 3$ such that $|G/\mathrm{K}_p(G)| = p^p$. (See Theorem 9.7.)

2185. Study the p-groups G of exponent $p > 7$ containing $E \cong \mathrm{E}_{p^p}$ but not containing a normal subgroup $\cong \mathrm{E}_{p-1}$. (See Theorem 10.4 and 10.5.)

2186 (Old problem, which is due, probably, to W. Lederman and B. H. Neumann). Is there a nonabelian p-group G such that $|G|$ does not divide $|\mathrm{Aut}(G)|$?

2187. Study the nonabelian p-groups G of exponent $> p$ such that whenever a noncyclic $A < G$ is maximal abelian, then all maximal cyclic subgroups of A are maximal cyclic in G.

2188. Does there exist a p-group all of whose maximal subgroups have special Frattini subgroups?

2189. Study the special p-groups all of whose maximal subgroups have the same center.

2190. Given n, classify the p-groups all of whose noncyclic subgroups of order p^n have equal rank.

2191. Study the p-groups in which every proper normal subgroup is a normal closure of an appropriate cyclic subgroup. (Such a normal closure is said to be an *antikernel* [BZ, Chapter 9].)

2192. Study the p-groups G such that whenever $\chi \in \mathrm{Irr}_1(G)$, then $G/\ker(\chi)$ is extraspecial.

2193. Study the p-groups all of whose nonnormal subgroups of same order have cores of equal rank.

2194. Classify the p-groups all of whose subgroups of class 2 are normal.

2195. Study the p-groups G such that $|\mathrm{N}_G(A) : \mathrm{N}_G(A)_G| \leq p$ for all $A < G$.

2196. Classify the 2-groups without five pairwise noncommuting elements. (See Lemma 116.2 and Theorem 116.10.)

2197 (Mann). Find the number of subgroups (cyclic subgroups) of given order in a metacyclic 2-group G. (This is solved in §124.)

2198. Let G be a special group of order p^{d+z}, where $|\mathrm{Z}(G)| = p^z$. Give lower and upper estimates of $\alpha_1(G)$.

2199. Classify the p-groups all of whose minimal nonabelian subgroups are nonmetacyclic of order p^4.

2200. Study the p-groups G such that whenever $M < G$ is a minimal nonabelian, then all subgroups of G of order $|M|$ and class 2 are also minimal nonabelian.

2201. Study the p-groups G of exponent p with cyclic Schur multiplier.

2202. Study the p-groups having exactly one maximal subgroup that is not special.

2203. Study the p-groups $G = \Omega_1(G)$ such that $|G : L^G| = p$ for all nonnormal $L < G$ of order p.

2204. Let G be a group of order p^m, $\mathrm{d}(G) = d$ and $1 < n < m - 1$. Is it possible to estimate $\mathrm{s}_n(G)$, the number of subgroups of order p^n in G?[18]

2205 (K. Harada). Let a four-group $E = \langle u \rangle \times \langle v \rangle$ act on a 2-group G. Is the following true: $|G| \leq |\mathrm{C}_G(u)||\mathrm{C}_G(v)||\mathrm{C}_G(uv)|$? Consider the similar problem for $p > 2$.

2206. Classify the p-groups G such that for any nonnormal (maximal nonnormal) $H < G$ we have $|\mathrm{N}_G(H) : H| \leq p^2$. (Compare with [ZG], §138 and #116(i)).

[18]Commentary of Mann: The number of subgroups of a given index in a free pro-p-group of rank d was determined by Ishai Ilani [Ila]. This gives the maximum of $\mathrm{s}_n(G)$.

2207. It is known that if $B = B(2,4)$ is the maximal finite two-generator group of exponent 4, then $\Phi(B)$ is special (see §60). It follows that all maximal subgroups of G are nonabelian (= irregular). Find the minimal order of a two generator p-group G all of whose maximal subgroups are irregular. (Mann has shown in a letter at 6/6/06 that if $p = 3$, then $|G| \leq 3^{29}$.)

2208. Classify the p-groups G such that whenever $C < G$ is nonnormal cyclic, then any abelian subgroup of G containing C has order at most $p|C|$.

2209. Classify the p-groups G such that whenever $C < G$ is maximal cyclic (maximal nonnormal cyclic), then $|\mathrm{N}_G(C) : C| = p$.

2210. Classify the p-groups all of whose nonnormal maximal cyclic subgroups are conjugate.

2211. Classify the p-groups containing exactly $p^2 + p$ nonnormal subgroups of index p^2.

2212. Classify the p-groups G such that the normalizer of any maximal cyclic subgroup of G is metacyclic.

2213. Study the p-groups G such that $\mathrm{N}_G(A)/A$ is cyclic for all minimal nonabelian (nonnormal abelian) $A < G$.

2214. Let G be a p-group such that all subgroups of $\Phi(G)$ are characteristic in G. Describe the structures of $\Phi(G)$ and G.

2215. Study the p-groups in which any two distinct maximal elementary abelian subgroups have intersection of order p.

2216. Describe the derived subgroups of maximal subgroups of a p-groups G such that G' is abelian of type (p^2, p).

2217 (Z. Janko). Suppose that G' is noncyclic but all maximal subgroups of a p-group G have cyclic derived subgroups. Is it true that the derived subgroups of all maximal subgroups of G have orders $\leq p$? (This is solved in §139.)

2218. Classify the 2-groups G containing a subgroup $H \cong \mathrm{Q}_8$ such that for all such H the subgroup $\mathrm{N}_G(H)$ is Dedekindian.

2219. Classify the 2-groups G containing a maximal subgroup H such that the set $G - H$ contains exactly four involutions.

2220. Let G be a nonabelian group of minimal order p^n and exponent p such that $p^2 \mid \exp(\mathrm{Aut}(G))_p$. Find n.

2221. Study the p-groups all of whose maximal absolutely regular subgroups are nonnormal.

2222. Classify the p-groups G all of whose nonnormal maximal cyclic subgroups are maximal abelian.

2223. Classify the nonabelian p-groups G such that whenever A is maximal nonnormal abelian subgroup of G, then any abelian subgroup of G containing A has order $\leq p|A|$.

2224. Describe the structure of a Sylow p-subgroup of the holomorph of a nonabelian metacyclic p-group.

2225. Classify the p-groups all of whose maximal nonnormal subgroups are conjugate.

2226. Classify the p-groups G all of whose maximal cyclic subgroups are quasinormal (= permutable with all subgroups of G).

2227. Study the p-groups G such that $\mathrm{C}_G(\mathrm{Z}(A)) = A$ for all $A \in \Gamma_1$.

2228. Classify the E_p-groups containing a proper subgroup $\cong \mathrm{M}_{p^n}$. (See §110.)

2229. Study the p-groups in which the intersection of any two nonincident metacyclic subgroups is cyclic.

2230. Given two p-groups F and H, is it true that there exists a p-group G containing H as a nonnormal subgroup and such that $G/H^G \cong F$?

2231. Classify the p-groups all of whose two noncommuting and conjugate (nonconjugate) elements generate a group of maximal class.

2232. Study the p-groups G all of whose nonnormal subgroups have cyclic Frattini subgroups but $\Phi(G)$ is nonabelian.

2233. Classify the p-groups all of whose nonnormal subgroups have cyclic subgroups of index p. (Compare with §16.)

2234. Study the p-groups all of whose $\mathcal{A}_2$-subgroups are metacyclic of class 2.

2235. Classify the p-groups G all of whose cyclic subgroups not contained in $\Phi(G)$ are complemented in G.

2236. Study the nonabelian p-groups G provided that all elements $x \in G - \Phi(G)$ ($x \in G - \mathrm{Z}(G)$) have abelian centralizers.

2237. Given a p-group H, give a low estimate of $|G|$, where G is a p-group whose Frattini subgroup has a subgroup $\cong H$.

2238. Study the p-groups satisfying one of the following three conditions: (i) G has only one normal subgroup of order p^{p-1} and exponent p, (ii) G is generated by normal subgroups of order p^p and exponent p, (iii) G has no normal subgroup of order p^{p+1} and exponent p.

2239. Let $p > 2$ and let H be a group of maximal class and order p^{p+1} containing exactly p maximal subgroups of exponent p. Does there exist a p-group G of maximal class such that $G/\mathrm{Z}(G) \cong H$?

2240. Let $p > 2$ and let H be a group of maximal class and order $> p^{p+1}$ such that all elements of the set $H - H_1$ have order p (here H_1 is the fundamental subgroup of H). Does there exist a p-group G of maximal class such that $G/\mathrm{Z}(G) \cong H$?

2241. Given $n > 1$, does there exist a group (a nonabelian group) of exponent p admitting a nontrivial partition by subgroups of order p^n?

2242. Given $n > 1$, present two lattice isomorphic groups of exponent p and class n that are nonisomorphic.

2243. Describe the set of n such that there is no p-group G of exponent p with $\mathrm{k}(G) = n$. (See Theorem 2.1.)

2244. Describe all possibilities for numbers of generators of all seven maximal subgroups of a 2-group of rank 3.

2245. Study the structure of a p-group G with $|G : G'| = p^2$ containing exactly p maximal subgroups of exponent p.

2246. Study the structure of a two-generator p-group G with elementary abelian maximal subgroup and such that G/G' is abelian of type (p^2, p).

2247. Given $n > 2$, construct the p-group G of exponent $< p^n$ and such that the series

$$G > \mho^1(G) > \mho^2(G) > \cdots > \mho^k(G) > \cdots > \mho^n(G) = \{1\}$$

has length n. Here $\mho^1(G) = \mho_1(G)$, $\mho^{i+1}(G) = \mho_1(\mho^i(G))$ for all $i \geq 1$.

2248. Classify the p-groups all of whose maximal subgroups, except one, have cyclic derived subgroups. (See #39.)

2249. Study the p-groups all of whose maximal subgroups, except one, are special.

2250. Study the metabelian p-groups G with $\exp(G') > p$ all of whose maximal subgroups (nonabelian maximal subgroups) have derived subgroups of exponent p.

2251. Study the p-groups G satisfying $\mathrm{d}(G) < \mathrm{d}(H)$ for all $H \in \Gamma_1$.

2252. Given $e > 2$, does the exist a p-group $G = \Omega_1(G)$ of exponent p^e such that the subgroups G, $\Omega_2^*(G)$, $\ldots$, $\Omega_e^*(G)$ are pairwise distinct.

2253. Let R be a maximal nonnormal elementary abelian subgroup of order p^2 of a p-group G. Study the structure of the normal closure R^G. Consider in detail the case where R^G is of maximal class. (See §134.)

2254. Study the groups of exponent p all of whose special subgroups have the same order p^3.

2255. Let α be an automorphism of a p-group G such that $M^\alpha = M$ for all minimal nonabelian $M < G$. Describe the set $\pi(o(\alpha))$.

2256. Classify the special p-groups G such that $|G| = |\mathrm{Aut}(G)|$.

2257. Given $m > p$, estimate the number of groups G of maximal class and order p^m such that $\mathrm{H}_p(G) < G$.

2258. Find the number of p-groups of maximal class and order p^m possessing an abelian subgroup of index p.

2259. Study the p-groups G possessing a maximal subgroup M with $\mathrm{N}_G(A) \not\leq M$ for all $A < M$.

2260. Study the irregular p-groups, $p > 2$, all of whose subgroups of order p^p and exponent p, except one, are of maximal class (elementary abelian).

2261. Study the p-groups, $p > 2$, all of whose maximal subgroups, except one, are irregular.

2262. Study the p-groups all of whose maximal subgroups, except one, are of class 2 (metabelian).

2263. Study the p-groups G all of whose maximal subgroups have elementary abelian derived subgroups but G' is not elementary abelian (is nonabelian).

2264. Study the p-groups G all of whose minimal nonabelian subgroups are isomorphic (of same order). (For a partial case, see #1717.)

2265. Classify the p-groups G such that whenever $N \lhd M \in \Gamma_1$, then $N \lhd G$.

2266. Study the p-groups G such that whenever $R < G$ is nonnormal of exponent p, then $\exp(\mathrm{N}_G(R)) = p$.

2267. Study the p-groups G containing a nonabelian subgroup E of order p^3 such that $\mathrm{N}_G(E)$ is extraspecial (special).

2268. Classify the p-groups containing exactly p nonnormal maximal abelian subgroups.

2269. Study the p-groups G such that whenever $A < G$ is nonnormal abelian, then $\mathrm{N}_G(A)$ is abelian.

2270. Describe the normal structure of the 2-groups with a cyclic subgroup of index 8. (See §50 and subsection 26^o of Appendix 40.)

2271. Study the p-groups G such that all elements of H' are commutators for any $H \leq G$.

2272. Classify the special p-groups G such that all elements of G' are commutators.

2273. Estimate $|G'|$, where G is a special p-group of rank d with $|G : \mathrm{C}_G(x)| \leq p^k$ for all $x \in G - G'$ (k is fixed).

2274. Study the p-groups G such that $\mathrm{Aut}(G)$ is a p-group of class $\mathrm{cl}(G) - 1$.

2275. Study the p-groups G such that the Sylow p-subgroups of $\mathrm{Aut}(G)$ are special.

2276. Classify the p-groups without nonabelian sections of order p^3.

2277. Classify the p-groups containing two distinct maximal subgroups with derived subgroups of order $\leq p$.

2278. Classify the groups G with abelian subgroup of index p and $|G'| = p^2$.

2279. Classify the groups all of whose nonnormal subgroups have orders $\leq p^3$.

2280. Study the p-groups G all of whose subgroups of order $\geq |G'|$ are normal.

2281. Study the p-groups G with $\mathrm{d}(G) > 2$ containing a subgroup L of order p such that whenever $L < H \in \Gamma_1$, then (i) H is metacyclic, (ii) $|H'| = p$, (iii) H' is cyclic, (iv) H has an abelian subgroup of index p.

2282. Study the p-groups G such that whenever $A < H \in \Gamma_1$ and A is not normal in G, then $\mathrm{N}_G(A) \not\leq H$.

2283. Given $d > 2$, let G be a special p-group of rank d with center of order p^z, where $z < \frac{1}{2}d(d-1)$. Is it true that the Schur multiplier of G is nontrivial?

2284. Describe all representation groups of a given abelian p-group of rank 2.

2285. Describe all extensions having cyclic center of a group of order p by an extraspecial p-group.

2286. Describe the number of subgroups of given order in $\mathrm{Hol}(\mathrm{C}_{2^n})$, the holomorph of the cyclic group C_{2^n} of order 2^n.

2287. Study the p-groups G with $\mathrm{d}(G) > 3$ containing a minimal nonabelian subgroup A such that whenever $A < H \in \Gamma_1$, then (i) $|H'| = p$, (ii) H' is cyclic.

2288. Let $\epsilon_2 = 4$ and $\epsilon_p = 3$ provided $p > 2$. Study the p-groups G with $\mathrm{d}(G) > 3$ containing a metacyclic minimal nonabelian subgroup $A \cong \mathrm{M}_{p^{\epsilon_p}}$ such that whenever $A < H \in \Gamma_1$, then H is metacyclic.

2289. Study the p-groups all whose $\mathcal{A}_2$-subgroups have derived subgroups of order p. (See §§65, 71.)

2290. Study the p-groups G all whose $\mathcal{A}_2$-subgroups are contained in $\Phi(G)$.

2291. Study the p-groups G such that $\Phi(G)$ is an $\mathcal{A}_2$-group.

Bibliography

A

[A-B] E. Adan-Bante, Induction of characters and finite p-groups, *Glasg. Math. J.* **48** (2006), no. 3, 491–502.

[AB-B] M. J. Alejandro and A. Ballester-Bolinches, On a theorem of Berkovich, *Israel J. Math.* **131** (2002), 149–156.

[Alp1] J. L. Alperin, On a special class of regular p-groups, *Trans. Amer. Math. Soc.* **106** (1963), 77–99.

[Alp2] J. L. Alperin, Large abelian subgroups of p-groups, *Trans. Amer. Math. Soc.* **117** (1965), 10–20.

[Alp3] J. L. Alperin, Centralizers of abelian normal subgroups of p-groups, *J. Algebra* **1** (1964), 110–113.

[AlpG] J. L. Alperin and G. Glauberman, Limits of abelian subgroups of finite p-groups, *J. Algebra* **203** (1998), 533–566.

[AlpK] J. L. Alperin and Kuo Tzee-Nan, The exponent and the projective representations of a finite group, *Illinois J. Math.* **11** (1967), 410–414.

[AK1] B. Amberg and L. Kazarin, On the rank of a finite product of two p-groups, in: *Groups–Korea 94*, pp. 1–8, edited by A. C. Kim and D. L. Johnson, Walter de Gruyter, Berlin,1995.

[AK2] B. Amberg and L. Kazarin, On the rank of a product of two finite p-groups and nilpotent p-algebras, *Comm. Algebra* **27** (1999), no. 8, 3895–3907.

[Arg] D. E. Arganbright, The power-commutator structure of finite p-groups, *Pacific J. Math.* **29** (1969), 11–17.

[AS] M. Aschbacher and S. D. Smith, *The Classification of Quasithin Groups 1*, Mathematical Surveys and Monographs 111, American Mathematical Society, Providence, RI, 2004.

B

[BW] A. H. Baartman and J. J. Woeppel, The automorphism group of a p-group of maximal class with abelian maximal subgroup, *Fund. Math.* **93** (1976), no. 1, 41–46.

[Bae1] R. Baer, Groups with abelian central quotient groups, *Trans. Amer. Math. Soc.* **44** (1938), 357–386.

[Bae2] R. Baer, Partitionen endlicher Gruppen, *Math. Z.* **75** (1961), 333–372.

[Bae3] R. Baer, Gruppen mit Hamiltonschem Kern, *Comp. Math.* **2** (1935), 241–246.

[Bae4] R. Baer, Group elements of prime power index, *Trans. Amer. Math. Soc.* **75** (1953), 20–47.

[Bae5] R. Baer, Norm and hypernorm, *Publ. Math. Debrecen* **4** (1956), 347–350.

[Bae6] R. Baer, Supersoluble immersion, *Canad. J. Math.* **11** (1959), 353–399.

[Bae7] R. Baer, Groups with preassigned central and central quotient group, *Trans. Amer. Math. Soc.* **44** (1938), no. 3, 387–412.

[Bae8] R. Baer, Crossed isomorphisms, *Amer. J. Math.* **66** (1944), no. 3, 341–404.

[Bae9] R. Baer, Theory of crossed characters, *Trans. Amer. Math. Soc.* **54** (1943), no. 1, 103–170.

[Bae10] R. Baer, Groups with abelian norm quotient group, *Amer. J. Math.* **61** (1939), no. 3, 700–708.

[Bae11] R. Baer, Group elements of prime power index, *Trans. Amer. Math. Soc.* **75** (1953), no. 1, 20–47.

[BM1] C. Baginski and I. Malinowska, On groups of order p^n with automorphism of order p^{n-2}, *Demonstratio Math.* **23** (1996), no. 3, 565–575.

[BM2] C. Baginski and I. Malinowska, On finite 2-groups with many involutions, *Arch. Math.* **81** (2003), 241–244.

[BBERR] A. Ballester-Bolinches, R. Esteban-Romero and D. J. S. Robinson, On finite minimal nonnilpotent groups, *Proc. Amer. Math. Soc.* **133** (2005), 3455–3462.

[Bal] F. Balogh, Finite groups in which different conjugacy classes have different cardinalities, *J. Algebra* **181** (1996), 286–287.

[Ban] W. Bannusher, Über Gruppen mit genau zwei irreduziblen Charaktergraden I, II, *Math. Nachr.* **154** (1991), 253–563.

[BarI] Y. Barnea and I. M. Isaacs, Lie algebras with few centralizer dimensions, *J. Algebra* **259** (2003), 284–299.

[BauBl] G. Baumslag and N. Blackburn, Groups with cyclic upper central factors, *Proc. Lond. Math. Soc. (3)* **10** (1960), 531–544.

[Bec] H. Bechtell, Frattini subgroups and Φ-central groups, *Pacific J. Math.* **18** (1966), 15–23.

[Bei1] B. Beisigel, Semi-extraspezielle p-Gruppen, *Math. Z.* **156** (1976), 247–254.

[Bei2] B. Beisigel, Die Automorphismengruppen homozyklisher p-Gruppen, *Arch. Math.* **29** (1977), no. 4, 363–366.

[Ben1] H. A. Bender, A determination of the groups of order p^5, *Ann. of Math. (2)* **29** (1927), 61–72.

[Ben2] H. A. Bender, Determination of all prime power groups containing only one invariant subgroup of every index which exceeds this prime number, *Trans. Amer. Math. Soc.* **26** (1924), no. 4, 427–434.

[BenG] H. Bender and G. Glauberman, *Local Analysis for the Odd Order Theorem*, London Mathematical Society Lecture Note Series 188, Cambridge University Press, Cambridge, 1994.

[BeM] R. Bercov and L. Moser, On abelian permutation groups, *Canad. Math. Bull.* **8** (1965), 627–630.

[BKN] T. R. Berger, L. G. Kovacs and M. F. Newman, Groups of prime power order with cyclic Frattini subgroup, *Nederl. Akad. Wetensch. Indag. Math.* **42** (1980), no. 1, 13–18.

[Ber0] V. G. Berkovich, Groups of order p^n possessing an automorphism of order p^{n-1}, *Algebra Logika* **9** (1970), no. 1, 4–8 (Russian).

[Ber1] Y. Berkovich, On p-groups of finite order, *Siberian Math. Zh.* **9** (1968), 1284–1306 (Russian).

[Ber2] Y. Berkovich, Subgroups, normal divisors and epimorphic images of a finite p-group, *Soviet Math. Dokl.* **10** (1969), 878–881.

[Ber3] Y. Berkovich, A generalization of theorems of Ph. Hall and Blackburn and an application to non-regular p-groups, *Math. USSR Izv.* **35** (1971), 815–844.

[Ber4] Y. Berkovich, Some consequences of Maschke's theorem, *Algebra Colloq.* **5** (1998), no. 2, 143–158.

[Ber5] Y. Berkovich, Alternate proofs of some basic theorems of finite group theory, *Glas. Mat.* **40** (2005), no. 2, 207–233.

[Ber6] Y. Berkovich, Finite metacyclic groups, *Soobsch. Akad. Nauk Gruzin. SSR* **68** (1972), 539–542 (Russian).

[Ber7] Y. Berkovich, On finite metacyclic groups, in: *Structural Properties of Algebraic Systems*, pp. 12–19, Nalchik, 1985 (Russian).

[Ber8] Y. Berkovich, Relations between some invariants of finite solvable groups, *Soobsch. Akad. Nauk Gruzin. SSR* **123** (1986), no. 3, 469–472 (Russian).

[Ber9] Y. Berkovich, On subgroups of finite p-groups, *J. Algebra* **224** (2000), 198–240.

[Ber10] Y. Berkovich, Alternate proofs of two theorems of Philip Hall on finite p-groups, and related results, *J. Algebra* **294** (2005), no. 2, 463–477.

[Ber11] Y. Berkovich, On abelian subgroups of p-groups, *J. Algebra* **199** (1998), 262–280.

[Ber12] Y. Berkovich, On the order of the commutator subgroup and the Schur multiplier of a finite p-group, *J. Algebra* 144 (1991), no. 2, 269–272.

[Ber13] Y. Berkovich, On the number of subgroups of given order in a finite p-group of exponent p, *Proc. Amer. Math. Soc.* **109** (1990), no. 4, 875–879.

[Ber14] Y. Berkovich, On the number of elements of given order in a finite p-group, *Israel J. Math.* **73** (1991), 107–112.

[Ber15] Y. Berkovich, On the number of subgroups of given order and exponent p in a finite irregular p-group, *Bull. Lond. Math. Soc.* **24** (1992), 259–266.

[Ber16] Y. Berkovich, Counting theorems for finite p-groups, *Arch. Math.* **59** (1992), 215–222.

[Ber17] Y. Berkovich, On the number of solutions of equation $x^{p^k} = a$ in a finite p-group, *Proc. Amer. Math. Soc.* **16** (1992), no. 3, 585–590.

[Ber18] Y. Berkovich, On p-subgroups of finite symmetric and alternating groups, *Contemp. Math.* **93** (1989), 67–76.

[Ber19] Y. Berkovich, On the number of solutions of equation $x^{p^k} = 1$ in a finite group, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **6** (1995), 5–12.

[Ber20] Y. Berkovich, On the number of subgroups of a given structure in a finite p-group, *Arch. Math.* **63** (1994), 111–118.

[Ber21] Y. Berkovich, Normal subgroups in a finite group, *Soviet Math. Dokl.* **9** (1968), 1117–1120.

[Ber22] Y. Berkovich, Short proofs of some basic characterization theorems of finite p-group theory, *Glas. Mat.* **41(61)** (2006), 239–258.

[Ber23] Y. Berkovich, On an irregular p-group, Siberian J. Math. **12, 4** (1971), 907–911.

[Ber24] Y. Berkovich, On subgroups and epimorphic images of finite p-groups, *J. Algebra* **248** (2002), 472–553.

[Ber25] Y. Berkovich, Finite Group. Selected Topics, Parts I, II, in preparation.

[Ber26] Y. Berkovich, Nonnormal and minimal nonabelian subgroups of a finite group, *Israel J. Math.*, to appear.

[Ber27] Y. Berkovich, Hall chains in finite p-groups, *Israel J. Math.* **168** (2008), 29–51.

[Ber28] Y. Berkovich, Alternate proofs of characterization theorems of Miller and Janko on p-groups, and some related results, *Glas. Math.* **42(62)** (2007), 319–343.

[Ber29] Y. Berkovich, On the metacyclic epimorphic images of a finite p-group, *Glas. Mat.* **42(62)** (2007), 259–269.

[Ber30] Y. Berkovich, Finite p-groups with few minimal nonabelian subgroups. With an appendix by Z. Janko, *J. Algebra* **297** (2006), no. 1, 62–100.

[Ber31] Y. Berkovich, Alternate proofs of some basic theorems of finite group theory, *Glas. Mat.* **40** (2005), 207–233.

[Ber32] Y. Berkovich, A property of p-groups of order $p^{p(e+1)}$ and exponent p^e, *Glas. Mat.* **40(60)** (2005), 51–58.

[Ber33] Y. Berkovich, Finite p-groups in which some subgroups are generated by elements of order p, *Glas. Mat.* **44(64)** (2009), 167–175.

[Ber34] Y. Berkovich, Minimal nonabelian and maximal subgroups of a finite p-group, *Glas. Mat.* **43(63)** (2008), 97–109.

[Ber35] Y. Berkovich, Nonnormal and minimal nonabelian subgroups of a finite group, submitted.

[Ber36] Y. Berkovich, A generalization of Burnside's second theorem on $\{p, q\}$-groups, *Izv. Severo-Kavkaz. Tzentra Vyssh. Skoly, Estestv. Nauki* **4** (1985), 18–22 (Russian); English translation in *Amer. Math. Soc. Transl. (2)* **149** (1991), 31–39.

[Ber37] Y. Berkovich, A corollary of Frobenius' normal p-complement theorem, *Proc. Amer. Math. Soc.* **127, 9** (1999), 2505–2509.

[Ber38] Y. Berkovich, On a lemma of Thompson, *Glas. Mat.* **39(59)** (2004), no. 2, 213–220.

[Ber39] Y. Berkovich, A necessary and sufficient condition for the simplicity of a finite group, in: *Algebra and Number Theory*, pp. 17–21 Nalchik, 1979 (Russian).

[Ber40] Y. Berkovich, On π-separable groups, *J. Algebra* **186** (1996), 120–131.

[Ber41] Y. Berkovich, The subgroup and normal structure of a finite p-group, *Soviet Math. Dokl.* **106** (1971), 71–75.

[Ber42] Y. Berkovich, On automorphisms of order p of metacyclic p-groups without cyclic subgroups of index p, *Glas. Mat.* **44(64)** (2009), no. 2, 343–348.

[Ber43] Y. Berkovich, *Groups of Prime Power Order*, Volume 1, Walter de Gruyter, Berlin, 2008.

[Ber44] Y. Berkovich, Finite groups covered by few proper subgroups, *Glas. Mat.* **45(65)** (2010), 415–429.

[Ber45] Y. Berkovich, A generalization of theorems of Carter and Wielandt, *Soviet Math. Dokl.* **7** (1966), 1525–1529 (Russian).

[Ber46] Y. Berkovich, Finite non-Dedekindian p-groups all of whose nonnormal cyclic subgroups of minimal order have index p in their normalizers, in preparation.

[Ber47] Y. Berkovich, On finite p-groups containing a maximal elementary abelian subgroup of order p^2, to appear in *Glas. Mat.*

[Ber48] Y. Berkovich, Finite p-groups generated by certain minimal nonabelian subgroups, manuscript.

[Ber49] Y. Berkovich, The number of subgroups of given order in a metacyclic p-group, to appear in *Glas. Mat.*

[Ber50] Y. Berkovich, Alternate proofs of two classical theorems on finite solvable groups and some related results for p-groups, *Glas. Mat.* **45(65)** (2010), 431–439.

[Ber51] Y. Berkovich, On the number of subgroups of given type in a finite p-group, *Glas. Mat.* **43(63)** (2008), 59–95.

[Ber52] Y. Berkovich, Characterizations of abelian and minimal nonabelian groups, *Glas. Mat.* **45(65)** (2010), 55–62.

[BFP] Y. Berkovich, G. Freiman and C. E. Praeger, Small squaring and cubing properties for finite groups, *Bull. Aust. Math. Soc.* **44** (1991), no. 3, 429–450.

[BG] Y. G. Berkovich and S. L. Gramm, On finite Γ-quasi-nilpotent groups, in: *Mathematical Analysis and Its Applications*, pp. 34–39, Rostov Gos. Univ., Rostov-Don, 1969 (Russian).

[BIK] Y. Berkovich, I. M. Isaacs and L. S. Kazarin, Distinct monolithic character degrees, *J. Algebra* **216** (1999), 448–480.

[BJ1] Y. Berkovich and Z. Janko, *Groups of Prime Power Order*, Volume 2, Walter de Gruyter, Berlin, 2008.

[BJ2] Y. Berkovich and Z. Janko, Structure of finite p-groups with given subgroups, *Contemp. Math.* **402** (2006), 13–93.

[BJ3] Y. Berkovich and Z. Janko, On subgroups of finite p-groups, *Israel J. Math.* **171** (2009), 39–40.

[BK] Y. Berkovich and L. Kazarin, Indices of elements and the normal structure of finite groups, *J. Algebra* **283, 2** (2005), 564–583.

[BerM] Y. Berkovich and A. Mann, On sums of degrees of irreducible characters, *J. Algebra* **199** (1998), 646–665.

[BZ] Y. Berkovich and E. Zhmud, *Characters of Finite Groups*, Parts 1 and 2, Translations of Mathematical Monographs 172 and 181, American Mathematical Society, Providence, RI, 1998, 1999.

[Bert1] E. A. Bertram, On large cyclic subgroups of finite groups, *Proc. Amer. Math. Soc.* **56** (1976), 63–66.

[Bert2] E. A. Bertram, Large centralizers in finite solvable groups, *Israel J. Math.* **47** (1984), 335–344.

[BEOB1] H. U. Besche, B. Eick and E. A. O'Brien, The groups of order at most 2000, *Electron. Res. Announc. Amer. Math. Soc.* **7** (2001), 1–4.

[BEOB2] H. U. Besche, B. Eick and E. A. O'Brien, A millennium project: constructing small groups, *Internat. J. Algebra Comput.* **12** (2002), 623–644.

[Bey] F. R. Beyl, The Schur multiplicator of metacyclic groups, *Proc. Amer. Math. Soc.* **40** (1973), 413–418.

[BeyFS] F. R. Beyl, U. Felgner and P. Schmid, On groups occurring as center factor groups, *J. Algebra* **61** (1979), 161–177.

[BeyT] F. R. Beyl and J. Tappe, *Group Extensions, Representations and the Schur Multiplicator*, Lecture Notes in Mathematics 958, Springer-Verlag, Berlin, 1982.

[Bla1] N. Blackburn, On prime-power groups in which the derived group has two generators, *Proc. Cambridge Philos. Soc.* **53** (1957), 19–27.

[Bla2] N. Blackburn, On prime power groups with two generators, *Proc. Cambridge Philos. Soc.* **54** (1958), 327–337.

[Bla3] N. Blackburn, On a special class of p-groups, *Acta Math.* **100** (1958), 45–92.

[Bla4] N. Blackburn, Über das Produkt von zwei zyklischen Gruppen, *Math. Z.* **68** (1958), 422–427.

[Bla5] N. Blackburn, Generalizations of certain elementary theorems on p-groups, *Proc. Lond. Math. Soc.* **11** (1961), 1–22.

[Bla6] N. Blackburn, Automorphisms of finite p-groups, *J. Algebra* **3** (1966), 28–29.

[Bla7] N. Blackburn, Finite groups in which the nonnormal subgroups have nontrivial intersection, *J. Algebra* **3** (1966), 30–37.

[Bla8] N. Blackburn, Note on a paper of Berkovich, *J. Algebra* **24** (1973), 323–334.

[Bla9] N. Blackburn, Some homology groups of wreath products, *Illinois J. Math.* **16** (1972), 116–129.

[Bla10] N. Blackburn, Über Involutionen in 2-Gruppen, *Arch. Math.* **35** (1980), 75–78.

[Bla11] N. Blackburn, The derived group of a 2-group, *Math. Proc. Cambridge Philos. Soc.* **101** (1987), 193–196.

[Bla12] N. Blackburn, On centralizers in p-groups, *J. Lond. Math. Soc. (2)* **9** (1975), 478–482.

[Bla13] N. Blackburn, Groups of prime-power order having an abelian centralizer of type $(r, 1)$, *Monatsh. Math.* **99** (1985), 1–18.

[Bla14] N. Blackburn, Conjugacy in nilpotent groups, *Proc. Amer. Math. Soc.* **16** (1965), 143–148.

[Bla15] N. Blackburn, Nilpotent groups in which the derived group has two generators, *J. Lond. Math. Soc.* **35** (1960), 33–35.

[Bla16] N. Blackburn, *Problems on the Theory of Finite Groups of Prime Power Order*, PhD Thesis, University of Cambridge, 1956, 184 pp.

[BDM] N. Blackburn, M. Deaconescu and A. Mann, Equilibrated groups, *Math. Proc. Cambridge Philos. Soc.* **120** (1996), no. 2, 579–588.

[BlaEs] N. Blackburn and A. Espuelas, The power structure of metabelian p-groups, *Proc. Amer. Math. Soc.* **92** (1984), 478–484.

[BlaEv] N. Blackburn and L. Evens, Schur multipliers of p-groups, *J. Reine Angew. Math.* **309** (1979), 100–113.

[BlaH] N. Blackburn and L. Hethelyi, Some further properties of soft subgroups, *Arch. Math.* **65** (1997), no. 5, 365–371.

[Blac1] S. R. Blackburn, Enumeration within isoclinism classes of groups of prime power order, *J. Lond. Math. Soc. (2)* **50** (1994), 293–304.

[Blac2] S. R. Blackburn, Groups of prime power order with derived subgroup of prime order, *J. Algebra* **219** (1999), 625–657.

[BlDM] H. F. Blichfeldt, L. E. Dickson and G. A. Miller, *Theory and Applications of Finite Groups*, Stechert, New York, 1938.

[Boh] J. Bohanon, Finite groups with maximal normalizers I, arXiv: 09053790v2 math.GR 2 June 2009.

[BosI] N. Boston and I. M. Isaacs, Class numbers of p-groups of given order, *J. Algebra* **279** (2004), 810–819.

[BosW] N. Boston and J. L. Walker, 2-groups with few conjugacy classes, *Proc. Edinb. Math. Soc. (2)* **43** (2000), no. 1, 211–217.

[Bou] S. Bouc, The Dade group of a p-group, *Invent. Math.* **64** (2006), 189–231.

[Boz] Z. Bozikov, Finite 2-groups with a nonabelian Frattini subgroup of order 16, *Arch. Math.* **166** (2008), 11–15.

[BozJ1] Z. Bozikov and Z. Janko, Finite 2-groups G with $|\Omega_3^*(G)| = 2^5$, *J. Group Theory* **7** (2004), 65–73.

[BozJ2] Z. Bozikov and Z. Janko, On a question of N. Blackburn about finite 2-groups, *Israel J. Math.* 147 (2005), 329–331.

[BozJ3] Z. Bozikov and Z. Janko, On finite p-groups in which the centralizer of each element is a normal subgroup, manuscript.

[BozJ4] Z. Bozikov and Z. Janko, Finite p-groups all of whose nonmetacyclic subgroups are generated by involutions, *Arch. Math.* **90** (2008), 14–17.

[BozJ5] Z. Bozikov and Z. Janko, A complete classification of finite p-groups all of whose noncyclic subgroups are normal, *Glas. Mat.* **44(64)** (2009), 177–185.

[BozJ6] Z. Bozikov and Z. Janko, 2-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian, *Glas. Mat.* **45(65)** (2010), 63–83.

[Bran] A. Brandis, Beweis eines Satzes von Alperin und Kuo Tzee-Nan, *Illinois J. Math.* **13** (1969), 275.

[BCS] R. Brandl, A. Caranti and C. M. Scoppola, Metabelian thin p-groups, *Quart. J. Math. Oxford (2)* **43** (1992), 157–173.

[Br] R. Brown, Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements, *J. Combin. Theory Ser. A* **49** (1988), no. 2, 294–307; II, *ibid.* **56** (1991), no. 2, 285–289.

[Bro] J. Brodkey, A note on finite groups with an abelian Sylow group, *Proc. Amer. Math. Soc.* **14** (1963), 132–133.

[Bur1] W. Burnside, *The Theory of Groups of Finite Order*, Dover Publications, NY, 1955.

[Bur2] W. Burnside, On some properties of groups whose orders are powers of primes I, *Proc. Lond. Math. Soc. (2)* **11** (1912), 225–245; II, *ibid* **13** (1913), 6–12.

[Bur3] W. Burnside, On the outer automorphisms of a group, *Proc. Lond. Math. Soc. (2)* **11** (1913), 40–42.

[Bur4] W. Burnside, On an unsettled question in the theory of discontinuous groups, *Quart. J. Math.* **33** (1902), 230–238.

[Buz] K. Buzasi, On the structure of the wreath product of a finite number of cyclic groups of prime order, *Publ. Math. Debrecen* **15** (1968), 107–129.

C

[Ca] A. Caranti, Projectivity of p-groups of maximal class, *Rend. Semin. Mat. Univ. Padova* **61** (1979), 393–404 (Italian).

[Carl] J. Carlson, Maximal elementary abelian subgroups of rank 2, *J. Group Theory* **10** (2007), 5–13.

[Car] R. W. Carter, Nilpotent self-normalizing subgroups of soluble groups, *Math. Z.* **75** (1961), 136–139.

[CarF] R. W. Carter and P. Fong, The Sylow 2-subgroups of the finite classical groups, *J. Algebra* **1** (1964), 139–151.

[CP] V. Cepulic and O. Pyliavska, A class of nonabelian nonmetacyclic finite 2-groups, *Glas. Mat.* **41(61)** (2006), 65–70.

[CIS] V. Cepulic, M. Ivankovic and E. Kovac-Strico, Second-metacyclic finite 2-groups, *Glas. Mat.* **40(60)** (2005), no. 1, 59–69.

[Cha] E. I. Chankov, p-groups with five nonlinear irreducible characters, manuscript.

[Che] Y. Cheng, On finite p-groups with cyclic commutator subgroups, *Arch. Math.* **39** (1982), 295–298.

[CD] A. Chermak and A. L. Delgado, A measuring argument for finite permutation groups, *Proc. Amer. Math. Soc.* **107** (1989), 907–914.

[CH] D. Chillag and M. Herzog, Finite groups with almost distinct character degrees, *J. Algebra* **319** (2008), 716–729.

[CI] M. D. E. Conder and I. M. Isaacs, Derived subgroups of products of an abelian and a cyclic subgroup, *J. Lond. Math. Soc. (2)* **69** (2004), 333–348.

[Con] S. B. Conlon, p-groups with an abelian maximal subgroup and cyclic centre, *J. Aust. Math. Soc. Ser. A* **25** (1976), no. 2, 221–233.

[CorH] K. Corradi and L. Hethelyi, On a class of p-groups, *Ann. Univ. Sci. Budapest Eótvós Sect. Math.* **27** (1985), 235–240.

[CT] G. Corsi Tani, Automorphisms fixing every normal subgroup of a p-group, *Bull. Un. Mat. Ital. A* **64** (1985), 245–252.

[CosH] J. Cossey and T. Hawkes, Sets of p-powers as conjugacy classes sizes, *Proc. Amer. Math. Soc.* **128** (2000), 49–51.

[CHM] J. Cossey, T. Hawkes and A. Mann, A criterion for a group to be nilpotent, *Bull. Lond. Math. Soc.* **24** (1992), 267–270.

[Cur1] M. J. Curran, The automorphism group of a split metacyclic 2-group, *Arch. Math.* **89** (2007), no. 1, 10–23.

[Cur2] M. J. Curran, The automorphism group of a nonsplit metacyclic 2-group, *Arch. Math.* **90** (2008), no. 6, 483–489.

[Curz] M. Curzio, Classification of finite minimal non-metacyclic groups, *Acta Sci. Math. Szeged* **47** (1984), 289–295.

[Cut] G. Cutolo, On a question about automorphisms of finite p-groups, *J. Group Theory* **9** (2006), 231–250.

D

[Dad] E. C. Dade, Products of orders of centralizers, *Math. Z.* **96** (1967), 223–225.

[DS] R. Dark and C. Scoppola, On Camina groups of prime power order, *J. Algebra* **181** (1996), 787–802.

[Dav1] R. M. Davitt, The automorphism group of finite p-abelian p-groups, *Illinois J. Math.* **16** (1972), 76–85.

[Dav2] R. M. Davitt, The automorphism group of a finite metacyclic p-group, *Proc. Amer. Math. Soc.* **25** (1970), 876–879.

[Dav3] R. M. Davitt, On the automorphism group of a finite p-group with a small central quotient, *Canad. J. Math.* **32** (1980), 1168–1176.

[DO1] R. M. Davitt and A. D. Otto, On the automorphism group of a finite p-group with the central quotient metacyclic, *Proc. Amer. Math. Soc.* **30** (1971), 467–472.

[DO2] R. M. Davitt and A. D. Otto, On the automorphism group of a finite modular p-group, *Proc. Amer. Math. Soc.* **35** (1972), 399–404.

[Ded] R. Dedekind, Über Gruppen, deren sämtliche Teiler Normalteiler sind, *Math. Ann.* **48** (1897), 548–561.

[Del] P. Deligne, Congruences sur le nombre de sous-groupes d'ordre p^k dans un groupe fini, *Bull. Belg. Math. Soc. Simon Stevin* **18** (1966), 129–132.

[DemW] U. Dempwolff and S. K. Wong, On cyclic subgroups of finite groups, *Proc. Edinb. Math. Soc. (2)* **25** (1982), no. 1, 19–20.

[Die] J. Dietz, Automorphisms of p-groups given as cyclic-by-elementary abelian extensions, *J. Algebra* **242** (2001), 417–432.

[DdSMS] J. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p-Groups*, London Mathematical Society Lecture Notes Series 157, Cambridge University Press, Cambridge, 1991.

[Dol] S. Dolfi, Arithmetical conditions on the length of the conjugacy classes of a finite group, *J. Algebra* **174** (1995), 753–771.

[Dra] S. V. Draganyuk, On the structure of finite primary groups all 2-maximal subgroups of which are abelian, in: *Complex Analysis, Algebra and Topology*, pp. 42–51, Kiev, 1990 (Russian).

E

[Eas] T. E. Easterfield, The orders of products and commutators in prime-power groups, *Proc. Cambridge Philos. Soc.* **36** (1940), 14–26.

[Eic1] B. Eick, Schur multiplicators of finite p-groups with fixed coclass, *Israel J. Math.* **166** (2008), 157–166.

[Eic2] B. Eick, The converse of a theorem of W. Gaschütz on Frattini subgroups, *Math. Z.* **224** (1997), 103–111.

[EOB] B. Eick and E. A. O'Brien, Enumerating p-groups, *J. Aust. Math. Soc.* **67** (1999), 191–205.

[ELG] B. Eick and C. R. Leedham-Green, On the classification of prime-power groups by coclass, *Bull. Lond. Math. Soc.* **40** (2008), 274–288.

[ENOB] B. Eick, M. F. Newman and E. A. O'Brien. The class-breadth conjecture revisited, *J. Algebra* **300** (2006), 384–393.

[ELGOB] B. Eick, C. R. Leedham-Green and E. A. O'Brien, Constructing automorphism groups of p-groups, *Comm. Algebra* **30** (2002), no. 5, 2271–2295.

[ERNS] S. Evans-Riley, M. F. Newman and C. Schneider, On the soluble length of groups with prime-power order, *Bull. Aust. Math. Soc.* **59** (1999) 343–346.

[Exa] T. Exarchakos, On the number of automorphisms of a finite p-group, *Canad. Math. J.* **32** (1980), 1448–1458.

F

[Fal] K. Faltings, Automorphismengruppen endlicher abelscher p-Gruppen, in: *Studies on Abelian Groups (Symposium, Montpellier, 1967)*, pp. 101–119, Springer-Verlag, Berlin, 1968.

[Fan] Y. Fan, A characterization of elementary abelian p-groups by counting subgroups, *Math. Pract. Theory* **1** (1988), 63–65 (Chinese); MR 89h: 20030.

[Fau1] R. Faudree, A note on the automorphism group of a p-group, *Proc. Amer. Math. Soc.* **19** (1968), 1379–1382.

[Fau2] R. Faudree, Regular metabelian groups of prime-power order, *Bull. Aust. Math. Soc.* **3** (1970), 49–54.

[FKS] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups, II, *J. Reine Angew. Math.* **328** (1981), 39–57.

[Fei] W. Feit, Theory of finite groups in the twentieth century, *Amer. Math. Heritage: Algebra and Applied Math.* **13** (1981), 37–60.

[FT] W. Feit and J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.

[F-A1] G. A. Fernandez-Alcober, An introduction to finite p-groups: regular p-groups and groups of maximal class, *Mat. Contemp.* **20** (2001), 155–226.

[F-A2] G. A. Fernandez-Alcober, Omega subgroups of powerful p-groups, *Israel J. Math.* **16** (2007), no. 2, 75–79.

[F-AL] G. A. Fernandez-Alcober and L. Legaretta, Conjugacy classes of nonnormal subgroups of finite nilpotent p-groups, *J. Group Theory* **11** (2008), no. 3, 381–397.

[F-AM1] G. A. Fernandez-Alcober and A. Moreto, Groups with two extreme character degrees and their normal subgroups, *Trans. Amer. Math. Soc.* **353** (2001), 2271–2292.

[F-AM2] G. A. Fernandez-Alcober and A. Moreto, On the number of conjugacy class sizes and character degrees in finite p-groups, *Proc. Amer. Math. Soc.* **129** (2001), 3201–3204.

[F-AS] G. A. Fernandez-Alcober and R. T. Shepherd, On the order of p-groups of abundance zero, *J. Algebra* **201** (1998), 392–400.

[Fit] W. B. Fite, On metabelian groups, *Trans. Amer. Math. Soc.* **3** (1902), 331–353.

[Fitt] H. Fitting, Die Gruppe der zentralen Automorphismen einer Gruppe mit Hauptreihe, *Math. Ann.* **114** (1937), 355–372.

[FlyMH] J. Flynn and D. MacHale, Determining all finite groups whose automorphism group is a p-group, *Math. Proc. R. Ir. Acad.* **91A** (1991), no. 2, 259–264.

[FMHOBS] J. Flynn, D. MacHale, E. A. O'Brien and R. Sheely, Finite groups whose automorphism groups are 2-groups, *Math. Proc. R. Ir. Acad.* **94A** (1994), no. 2, 137–145.

[Fom] A. N. Fomin, Finite 2-groups in which the centralizer of a certain involution is of order 8, *Ural Gos. Univ. Mat. Zap.* **8** 1972), no. 3, 122–132 (Russian).

[For] C. E. Ford, Characters of p-groups, *Proc. Amer. Math. Soc.* **101** (1987), 595–601.

[FJO] S. Fouladi, A. R. Jamali and R. Orfi, On the automorphism group of a finite p-group with cyclic Frattini subgroup, *Math. Proc. R. Ir. Acad.* **108** (2008), no. 2, 165–174.

[FO] R. Fouladi and R. Orfi, Automorphisms of metabelian prime power order groups, *Bull. Aust. Math. Soc.* **77** (2008), 261–276.

[FrT] J. S. Frame und O. Tamaschke, Über die Ordnungen der Zentralisatoren der Elemente in endlichen Gruppen, *Math. Z.* **83** (1964), 41–45.

[Fro] G. Frobenius, Verallgemeinerung des Sylowschen Satzes, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1895), 981–993.

[FS] G. Frobenius and L. Stickelberger, Über Gruppen von vertauschbaren Elementen, *J. Reine Angew. Math.* **86** (1879), 217–262.

G

[Gag] S. M. Gagola, Jr., A character theoretic condition for $\mathrm{F}(G) > 1$, *Comm. Algebra* **33** (2005), 1369–1382.

[GL] S. M. Gagola and M. L. Lewis, A character theoretic condition characterizing nilpotent groups, *Comm. Algebra* **27** (1999), no. 3, 1053–1056.

[Gal] J. A. Gallian, Finite p-groups with homocyclic central factors, *Canad. J. Math.* **26** (1974), 636–643.

[Gas1] W. Gaschütz, Über die Φ-Untergruppe endlicher Gruppen, *Math. Z.* **58** (1953), 160–170.

[Gas2] W. Gaschütz, Kohomologische Trivialitäten und äußere Automorphismen von p-Gruppen, *Math. Z.* **88** (1965), 432–433.

[Gas3] W. Gaschütz, Nichtabelsche p-Gruppen besitzen äußere p-Automorphismen, *J. Algebra* **4** (1966), 1–2.

[Gas4] W. Gaschütz, *Lectures on Subgroups of Sylow Type in Finite Solvable Groups*, Australian National University, Canberra, 1979.

[GNY] W. Gaschütz, J. Neubüser and Ti Yen, Über den Multiplikator von p-Gruppen, *Math. Z.* **100** (1970), 93–96.

[GMMPS] N. Gavioli, A. Mann, V. Monti, A. Previtali and C. Scoppola, Groups of prime power order with many conjugacy classes, *J. Algebra* **202** (1998), 129–141.

[GMS] N. Gavioli, A. Mann and C. Scoppola, Two applications of the Hughes subgroup of finite groups, in: *Ischia Group Theory 2006*, pp. 138–146, World Scientific, Singapore, 2007.

[Gil] J. D. Gillam, A note on finite metabelian p-groups, *Proc. Amer. Math. Soc.* **25** (1970), 189–190.

[Gil2] J. D. Gillam, A finite p-group $G = AB$ with $\mathrm{Core}(A) = \mathrm{Core}(B) = 1$, *Rocky Mountain J. Math.* **3** (1973), 15–17.

[Glas] S. P. Glasby, 2-groups with every automorphism central, *J. Aust. Math. Soc. Ser. A* **41** (1986), 233–236.

[Gla1] G. Glauberman, Large abelian subgroups of finite p-groups, *J. Algebra* **196** (1997), 301–338.

[Gla2] G. Glauberman, Large abelian subgroups of groups of prime exponent, *J. Algebra* **237** (2001), 735–768.

[Gla3] G. Glauberman, On Burnside's other $p^a g^b$ theorem, *Pacific J. Math.* **56** (1975), 469–476.

[Gla4] G. Glauberman, Isomorphic subgroups of finite p-groups, I, II, *Canad. J. Math.* **23** (1971), 983–1022, 1023–1039.

[Gla5] G. Glauberman, Large subgroups of small class in finite p-groups, *J. Algebra* **272** (2004), 128–153.

[Gla6] G. Glauberman, Centrally large subgroups of finite p-groups, *J. Algebra* **300** (2006), 480–508.

[Gla7] G. Glauberman, Existence of normal subgroups in finite p-groups, *J. Algebra* **319** (2008), 800–805.

[Gla8] G. Glauberman, A p-group with no normal large abelian subgroup, manuscript.

[GM] G. Glauberman and N. Mazza, p-groups with maximal elementary abelian subgroup of rank 2, *J. Algebra* **323** (2010), 1729–1737.

[God] C. Godino, Outer automorphisms of certain p-groups, *Proc. Amer. Math. Soc.* **17** (1966), 922–329.

[Gol] Y. A. Golfand, On groups all of whose subgroups are nilpotent, *Dokl. Akad. Nauk SSSR* **125** (1948), 1313–1315.

[G-SJ-Z] J. Gonsalez-Sanchez and A. Jaikin-Zapirain, On the structure of normal subgroups of potent p-groups, *J. Algebra* **276** (2004), 193–209.

[Gore1] A. Goren, A measuring argument for finite permutation groups, *Israel J. Math.* **145** (2005), 333–339.

[Gore2] A. Goren, Another measuring argument for finite permutation groups, *J. Group Theory* **10** (2007), 829–840.

[GH1] A. Goren and M. Herzog, A general measuring argument for finite permutation groups, *Proc. Amer. Math. Soc.* **137** (2009), 3197–3205.

[GH2] A. Goren and M. Herzog, General measuring arguments for finite permutation groups, *Contemp. Math.* **524** (2010), 67–78.

[Gor1] D. Gorenstein, On a theorem of Philip Hall, *Pacific J. Math.* **19** (1966), 77–80.

[Gor2] D. Gorenstein, *Finite Groups*, Harper and Row, NY, 1968.

[Gor3] D. Gorenstein (editor), *Reviews on Finite Groups*, American Mathematical Society, Providence, RI, 1974.

[GLS] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number 1, Chapter G: General Group Theory*, American Mathematical Society, Providence, RI, 1995.

[GLS$_5$] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number 5*, American Mathematical Society, Providence, RI, 2002.

[Gre] J. A. Green, On the number of automorphisms of a finite group, *Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.* **237** (1956), 574–580.

[Gre2] J. A. Green, On groups with odd prime-power exponent, *J. Lond. Math. Soc.* **37** (1952), 476–485.

[Gro] F. Gross, 2-automorphic 2-groups, *J. Algebra* **40** (1976), 348–353.

[Gro2] F. Gross, Automorphisms of permutational wreath products, *J. Algebra* **117** (1988), 472–493.

[Grov] L. C. Grove, *Groups and Characters*, Pure and Applied Mathematics, Wiley-Interscience, New York, 1997.

[Grov1] J. R. J. Groves, On minimal irregular p-groups, *J. Aust. Math. Soc.* **16** (1973), 78–89.

[Grov2] J. R. J. Groves, On direct products of regular p-groups, *Proc. Amer. Math. Soc.* **37** (1973), 377–379.

[Grov3] J. R. J. Groves, Some criteria for the regularity of a direct product of regular p-groups, *J. Aust. Math. Soc. Ser. A* **24** (1977), 35–49.

[Grn1] O. Grün, Beiträge zur Gruppentheorie. V, Über endliche p-Gruppen, *Osaka Math. J.* **5** (1953), 117–146.

[Grn2] O. Grün, Über das direkte Produkt regulärer p-Gruppen, *Arch. Math.* **5** (1954), 241–243.

[Grn3] O. Grün, Eine obere Grenze für die Klasse einer h-stufigen p-Gruppe, *Abh. Math. Semin. Univ. Hambg.* **21** (1957), 90–91.

[Grn4] O. Grün, Einige Sätze über Automorphismen abelschen p-Gruppen, *Abh. Math. Semin. Univ. Hambg.* **24** (1960), 54–58.

[GS] M. Grüninger and P. Schmidt, Groups of central type and Schur multipliers with large exponent, *Illinois J. Math.* **47** (2003), no. 1–2, 265–272.

[GR] R. Guralnick and G. Robinson, On the commuting probability in finite groups, *J. Algebra* **300** (2006), no. 2, 509–528.

H

[HalM1] M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.

[HalM2] M. Hall, *Combinatorial Theory*, Wiley-Interscience, New York, 1986.

[HS] M. Hall and J. K. Senior, *On Groups of Order 2^n ($n \leq 6$)*, Macmillan, New York, 1964.

[Hal1] P. Hall, A contribution to the theory of groups of prime power order, *Proc. Lond. Math. Soc.* **36** (1933), 29–95.

[Hal2] P. Hall, On a theorem of Frobenius, *Proc. Lond. Math. Soc.* **40** (1936), 468–501.

[Hal3] P. Hall, The classification of prime power groups, *J. Reine Angew. Math.* **182** (1940), 130–141.

[Hal4] P. Hall, *Nilpotent Groups*, Canadian Mathematical Congress, University of Alberta, 1957.

[Hal5] P. Hall, On groups of automorphisms, *J. Math.* **182** (1940), 194–204.

[Hal6] P. Hall, Some sufficient conditions for a group to be nilpotent, *Illinois J. Math.* **2** (1958), 787–801.

[Hal7] P. Hall. Verbal and marginal subgroups, *J. Reine Angew. Math.* **182** (1940), 156–167.

[Hal8] P. Hall, The Eulerian functions of a group, *Quart. J. Math.* **7** (1936), 134–151.

[Hal9] P. Hall, Complemented groups, *J. Lond. Math. Soc.* **12** (1937), 201–204.

[HH] P. Hall and G. Higman, On the p-length of p-solvable groups and the reduction theorems for Burnside's problem, *Proc. Lond. Math. Soc.* **(3)** (1956), 1–42.

[Han] A. Hanaki, A condition on lengths of conjugacy classes and character degrees, *Osaka J. Math.* **33** (1996), 207–216.

[Har] K. Harada, On some 2-groups of normal 2-rank 2, *J. Algebra* **20** (1972), no. 1, 90–93.

[Harr] M. E. Harris, On decomposing an abelian p-group under a p'-operator group, *Algebra Colloq.* **7** (2000), 291–294.

[Haw] T. O. Hawkes, On the automorphism group of a 2-group, *Proc. Lond. Math. Soc.* **26** (1973), 207–225.

[HIO] T. O. Hawkes, I. M. Isaacs and M. Özaydin, On the Möbius function of a finite group, *Rocky Mountain J. Math.* **19** (1989), 1003–1034.

[HMH] P. Hegarty and D. MacHale, Two-groups in which an automorphism inverts precisely half of elements, *Bull. Lond. Math. Soc.* **30** (1998), 129–135.

[Hei1] H. Heineken, Gruppen mit kleinen abelschen Untergruppen, *Arch. Math.* **29** (1977), 20–31.

[Hei2] H. Heineken, Über ein Levisches Nilpotenzkriterium, *Arch. Math.* **12** (1961), 176–178.

[Hei3] H. Heineken, Nilpotente Gruppen, deren sämtliche Normalteiler charakteristisch sind, *Arch. Math.* **33** (1979/80), 497–503.

[Hei4] H. Heineken, Bounds for the nilpotency class of a group, *J. Lond. Math. Soc.* **37** (1962), 456–458.

[HL1] H. Heineken and H. Liebeck, On p-groups with odd order automorphism groups, *Arch. Math.* **24** (1973), 465–471.

[HL2] H. Heineken and H. Liebeck, The occurrence of finite groups in the automorphism group of nilpotent groups of class 2, *Arch. Math.* **25** (1974), 8–16.

[Hel1] G. T. Helleloid, A survey of automorphism groups of finite p-groups, arXiv.mathGR/0610294 v2 25 Oct 2006, 1–20.

[Hel2] G. T. Helleloid, *Automorphism Groups of Finite p-Groups: Structure and Applications*, PhD Thesis, Stanford University, 2007.

[HelM] G. T. Helleloid and U. Martin, The automorphism group of a finite p-group is almost always is a p-group, *J. Algebra* **312** (2007), 294–329.

[Herz] M. Herzog, Counting group elements of order p modulo p^2, *Proc. Amer. Math. Soc.* **66** (1977), 247–250.

[HK] M. Herzog and G. Kaplan, Large cyclic subgroups contain non-trivial normal subgroups, *J. Group Theory* **4** (2001), 247–253.

[HKL1] M. Herzog, G. Kaplan and A. Lev, On the commutator and the center of finite groups, *J. Algebra* **278** (2004), 494–501.

[HKL2] M. Herzog, G. Kaplan and A. Lucchini. On subgroups containing non-trivial normal subgroups, *Israel J. Math.* **137** (2003), 183–188.

[HL] M. Herzog and A. Lev, Characters and representations of p-groups of class 2, *Algebra Colloq.* **13** (2006), no. 1, 89–98.

[HLMM] M. Herzog, P. Longobardi, M. Maj and A. Mann, On generalized Dedekind groups and Tarski super monsters, *J. Algebra* **226** (2000), 690–613.

[Het1] L. Hethelyi, On powerful normal subgroups of a p-group, *Monatsh. Math.* **130** (2000), 201–209.

[Het2] L. Hethelyi, On subgroups of p-groups having soft subgroups, *J. Lond. Math. Soc. (2)* 41 (1990), 425–427.

[Het3] L. Hethelyi, Some additional properties of subgroups of p-groups having soft subgroups, *Studia Sci. Math. Hungar.* **29** (1994), 317–320.

[Het4] L. Hethelyi, Some remarks on 2-groups having soft subgroups, *Studia Sci. Math. Hungar.* **27** (1992), 295–299.

[Het5] L. Hethelyi, Soft subgroups of p-groups, *Ann. Univ. Sci. Budapest Eötvós Sect. Math.* **27** (1984), 81–85.

[Het6] L. Hethelyi, On linear p-groups of degree p, *Studia Sci. Math. Hungar.* **23** (1988), 369–373.

[HetL] L. Hethelyi and L. Levai, On elements of order p in powerful p-groups, *J. Algebra* **270** (2003), 1–6.

[Hig1] G. Higman, Suzuki 2-groups, *Illinois J. Math.* **7** (1963), 79–96.

[Hig2] G. Higman, Enumerating p-groups, I. Inequalities, *Proc. Lond. Math. Soc.* **10** (1960), 24–30.

[Hig3] G. Higman, Enumerating p-groups, II. Problems whose solution is PORC, *Proc. Lond. Math. Soc.* **10** (1960), 566–582.

[Hob1] C. Hobby, The Frattini subgroup of a p-group, *Pacific J. Math.* **10** (1960), 209–211.

[Hob2] C. Hobby, A characteristic subgroup of a p-group, *Pacific J. Math.* **10** (1960), 853–858.

[Hob3] C. Hobby, Generalizations of a theorem of N. Blackburn on p-groups, *Illinois J. Math.* **5** (1961), 225–227.

[Hob4] C. Hobby, The derived series of a finite p-group, *Illinois J. Math.* **5** (1961), 228–233.

[Hob5] C. Hobby, Abelian subgroups of p-groups, *Pacific J. Math.* **12** (1962), 1343–1345.

[Hob6] C. Hobby, Nearly regular p-groups, *Canad. J. Math.* **19** (1967), 520–522.

[Hob7] C. Hobby, Finite groups with normal normalizers, *Canad. J. Math.* **20** (1968), 1256–1260.

[HW] C. Hobby and C. R. B. Wright, A generalization of a theorem of N. Ito on p-groups, *Proc. Amer. Math. Soc.* **1** (1960), 707–709.

[HogK] G. T. Hogan and W. P. Kappe, On the H_p-problem for finite p-groups, *Proc. Amer. Math. Soc.* **20** (1969), 450–454.

[HEOB] D. F. Holt, B. Eick and E. A. O'Brien, *Handbook of Computational Group Theory*, CRC Press, Boca Raton, FL, 2005.

[Hop1] C. Hopkins, Metabelian groups of order p^m, $p > 2$, *Trans. Amer. Math. Soc.* **37** (1935), 161–195.

[Hop2] C. Hopkins, Non-abelian groups whose groups of automorphisms are abelian, *Ann. of Math.* **29** (1927/28), 508–520.

[HI] R. B. Howlett and I. M. Isaacs, On groups of central type, *Math. Z.* **179** (1982), 555–569.

[Hua] L. K. Hua, Some "Anzahl" theorems for groups of prime power order, *Sci. Rep. Nat. Tsing Hua Univ. A* **4** (1947), 313–327.

[HT1] L. K. Hua and H. F. Tuan, Determination of the groups of odd-prime-power order p^n which contain a cyclic subgroup of index p^2, *Sci. Rep. Nat. Tsing. Hua Univ. A* **4** (1940), 145–154.

[HT2] L. K. Hua and H. F. Tuan, Some "Anzahl" theorems for groups of prime-power orders, *J. Chinese Math.* **2** (1940), 313–319.

[HTh] D. R. Hughes and J. G. Thompson, The H_p-problem and the structure of H_p-groups, *Pacific J. Math.* **9** (1959), 1097–1101.

[Hug] N. J. S. Hughes, The structure and order of the group of central automorphisms of a finite group, *Proc. Lond. Math. Soc.* **53** (1951), 377–385.

[Hum] K. Hummel, The order of the automorphism group of a central product, *Proc. Amer. Math. Soc.* **47** (1975), 37–40.

[Hup1] B. Huppert, *Endliche Gruppen*, Band 1, Springer-Verlag, Berlin, 1967.

[Hup2] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Z.* **58** (1953), 243–264.

[Hup3] B. Huppert, *Character Theory of Finite Groups*, Walter de Gruyter, Berlin, 1999.

[HupB] B. Huppert and N. Blackburn, *Finite Groups II*, Springer-Verlag, Berlin, 1982.

[HupM] B. Huppert and O. Manz, Orbit sizes of p-groups, *Arch. Math.* **54** (1990), 105–110.

I

[IY] N. Iivory and H. Yamaki, On a conjecture of Frobenius, *Bull. Amer. Math. Soc.* **25** (1991), 413–416.

[Ila] I. Ilani, Counting finite index subgroups and P. Hall enumeration principle, *Israel J. Math.* **68** (1989), no. 1, 18–26.

[Isa1] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, NY, 1976.

[Isa2] I. M. Isaacs, An alternate proof of the Thompson replacement theorem, *J. Algebra* **15** (1970), 149–150.

[Isa3] I. M. Isaacs, The number of generators of a linear p-group, *Canad. J. Math.* **24** (1972), 852–858.

[Isa4] I. M. Isaacs, Sets of p-powers as irreducible character degrees, *Proc. Amer. Math. Soc.* **96** (1986), 551–552.

[Isa5] I. M. Isaacs, *Algebra: A Graduate Course*, Brooks/Cole, Pacific Grove, 1994.

[Isa6] I. M. Isaacs, Commutators and commutator subgroup, *Amer. Math. Monthly* **84** (1977), 720–722.

[Isa7] I. M. Isaacs, Automorphisms fixing elements of prime order in finite groups, *Arch. Math.* **68** (1997), 359–366.

[Isa8] I. M. Isaacs, Equally partitioned groups, *Pacific J. Math.* **49** (1973), 109–116.

[Isa9] I. M. Isaacs, Normal subgroups and nonabelian quotients in p-groups, *J. Algebra* **247** (2002), 231–243.

[Isa10] I. M. Isaacs, Recovering information about a group from its complex group algebra, *Arch. Math.* **47** (1986), 293–295.

[Isa11] I. M. Isaacs, Characters of groups associated with finite algebras, *J. Algebra* **177** (1995), 708–730.

[Isa12] I. M. Isaacs, Groups with many equal classes, *Duke Math. J.* **37** (1970), 501–506.

[Isa13] I. M. Isaacs, Coprime group actions fixing all nonlinear irreducible characters, *Canad. J. Math.* **41** (1989), 68–82.

[Isa14] I. M. Isaacs, Large orbits in nilpotent action, *Proc. Amer. Math. Soc.* **127** (1999), 45–50.

[Isa15] I. M. Isaacs, Solvable groups contain large centralizers, *Israel J. Math.* **55** (1986), 58–64.

[Isa16] I. M. Isaacs, Subgroups close to all their conjugates, *Arch. Math.* **55** (1990), 1–4.

[Isa17] I. M. Isaacs, Derived subgroups and centers of capable groups, *Proc. Amer. Math. Soc.* **129** (2001), 2853–2859.

[Isa18] I. M. Isaacs, Abelian point stabilizers in transitive permutation groups, *Proc. Amer. Math. Soc.* **130** (2002), 1923–1925.

[Isa19] I. M. Isaacs, *Finite Group Theory*, American Mathematical Society, New York, 2008.

[IsM] I. M. Isaacs and A. Moreto, The character degrees and nilpotence class of a p-group, *J. Algebra* **238** (2001), 827–842.

[INW] I. M. Isaacs, G. Navarro and T. R. Wolf, Finite group elements where no irreducible character vanishes, *J. Algebra* **222** (1999), 413–423.

[IsP1] I. M. Isaacs and D. S. Passman, A characterization of groups in terms of the degrees of their characters I, *Pacific J. Math.* **15** (1965), 877–903; II, *ibid.* **24** (1968), 467–510.

[IsP2] I. M. Isaacs and D. S. Passman, Half-transitive automorphism groups, *Canad. J. Math.* **18** (1966), 1243–1250.

[IsR] I. M. Isaacs and G. R. Robinson, On a theorem of Frobenius: solutions of $x^n = 1$ in finite groups, *Amer. Math. Monthly* **99** (1992), 352–354.

[IsS] I. M. Isaacs and M. C. Slattery, Character degree sets that do not bound the class of a p-group, *Proc. Amer. Math. Soc.* **129** (2002), 119–123.

[Ish] K. Ishikawa, On finite p-groups which have only two conjugacy lengths, *Israel J. Math.* **129** (2002), 119–123.

[Ito1] N. Ito, On the degrees of irreducible representations of a finite group, *Nagoya Math. J.* **3** (1951), 5–6.

[Ito2] N. Ito, On finite groups with given conjugate types, I, *Nagoya Math. J.* **6** (1953), 17–28.

[Ito3] N. Ito, *Lectures on Frobenius and Zassenhaus Groups*, Chicago, 1969.

[Ito4] N. Ito, On a theorem of L. Redei and J. Szep concerning p-groups, *Acta Sci. Math. Szeged* **14** (1952), 186–187.

[Ito5] N. Ito, Note on p-groups, *Nagoya Math. J.* **1** (1950), 113–116.

[Ito6] N. Ito, Über das Produkt von zwei zyklischen 2-Gruppen, *Publ. Math. Debrecen* **4** (1956), 517–520.

[Ito7] N. Ito, Über das Produkt von zwei abelschen Gruppen, *Math. Z.* **62** (1955), 400–401.

[Ito8] N. Ito, A conjecture on p-groups, manuscript.

[Ito9] N. Ito, On Hadamard 2-groups, manuscript.

[Ito10] N. Ito, Über eine Frattini-Gruppe duale Bildung, *Nagoya Math. J.* **9** (1955), 123–127.

[Ito11] N. Ito, Macdonald p-groups, manuscript.

[IM] N. Ito and A. Mann, Counting classes and characters of groups of prime exponent, *Israel J. Math.* **156** (2006), 205–220.

[IO] N. Ito and A. Ohara, Sur les groupes factorisables par deux 2-groupes cycliques, I, II, *Proc. Japan Acad. Ser. A Math. Sci.* **32** (1956), 736–743.

[Iwa] K. Iwasawa, Über die endlichen Gruppen und die Verbände ihrer Untergruppen, *J. Univ. Tokyo* **4** (1941), 171–199.

J

[Jai1] A. Jaikin-Zapirain, On the abundance of finite p-groups, *J. Group Theory* **2** (2000), no. 3, 225–231.

[Jai2] A. Jaikin-Zapirain, On almost regular automorphisms of finite p-groups, *Adv. Math.* **153** (2000), 391–402.

[JNOB] R. James, M. F. Newman and E. A. O'Brien, The groups of order 128, *J. Algebra* **129** (1990), 136–158.

[Jam] R. James, 2-groups of almost maximal class, *J. Aust. Math. Soc. Ser. A* **19** (1975), 343–357; corrigendum, *ibid* **35** (1983), 307.

[Jan1] Z. Janko, Finite 2-groups with small centralizer of an involution, *J. Algebra* **241** (2001), 818–826.

[Jan2] Z. Janko, Finite 2-groups with small centralizer of an involution, 2, *J. Algebra* **245** (2001), 413–429.

[Jan3] Z. Janko, Bemerkung über eine Arbeit von N. Ito, *Glasnik Mat.-Fiz. Astronom. Drustvo Mat. Fiz. Hroatske Ser. II* **11** (1961), 75–77.

[Jan4] Z. Janko, A theorem on nilpotent groups, *Glasnik Mat.-Fiz. Astronom. Drustvo Mat. Fiz. Hroatske Ser. II* **115** (1960), 247–249.

[Jan5] Z. Janko, Finite 2-groups with no normal elementary abelian subgroups of order 8, *J. Algebra* **246** (2001), 951–961.

[Jan6] Z. Janko, Finite 2-groups with a self-centralizing elementary abelian subgroup of order 8, *J. Algebra* **269** (2003), 189–214.

[Jan7] Z. Janko, Finite 2-groups G with $|\Omega_2(G)| = 16$, *Glas. Mat.* **40(60)** (2005), 71–86.

[Jan8] Z. Janko, Finite 2-groups with exactly four cyclic subgroups of order 2^n, *J. Reine Angew. Math.* **566** (2004), 135–181.

[Jan9] Z. Janko, Minimal nonmodular p-groups, *Glas. Mat.* **39** (2004), 221–233.

[Jan10] Z. Janko, 2-groups with self-centralizing subgroup of type $(4, 2)$, *Glas. Mat.* **39** (2004), 235–243.

[Jan11] Z. Janko, Elements of order at most 4 in finite 2-groups, *J. Group Theory* **7** (2004), 431–436.

[Jan12] Z. Janko, The structure of the Burnside group of order 2^{12}, manuscript.

[Jan13] Z. Janko, Nonmodular quaternion-free 2-groups, *Israel J. Math.* **154** (2006), 157–184.

[Jan14] Z. Janko, On maximal cyclic subgroups in finite p-groups, *Math. Z.* **254** (2006), 29–31.

[Jan15] Z. Janko, Minimal non-quaternion-free finite 2-groups, *Israel J. Math.* **154** (2006), 185–189.

[Jan16] Z. Janko, A classification of finite 2-groups with exactly three involutions, *J. Algebra* **291** (2005), 505–533.

[Jan17] Z. Janko, Elements of order at most 4 in finite 2-groups 2, *J. Group Theory* **8** (2005), 683–686.

[Jan18] Z. Janko, Finite p-groups with a uniqueness condition for non-normal subgroups, *Glas. Mat.* **40(60)** (2005), 235–240.

[Jan19] Z. Janko, Finite 2-groups all of whose nonabelian subgroups are generated by involutions, *Math. Z.* **252** (2006), 419–420.

[Jan20] Z. Janko, On finite 2-groups generated with three involutions, manuscript.

[Jan21] Z. Janko, Finite p-groups with $\Omega_2^*(G)$ is metacyclic, *Glas. Mat.* **41(61)** (2006), 71–76.

[Jan22] Z. Janko, New results in the theory of finite p-groups, *Contemp. Math.* **402** (2006), 193–195.

[Jan23] Z. Janko, Nonabelian 2-groups in which any two noncommuting elements generate a group of maximal class, *Glas. Mat.* **41(61)** (2006), 271–274.

[Jan24] Z. Janko, On maximal abelian subgroups in finite p-groups, *Math. Z.* **258** (2008), 629–635.

[Jan25] Z. Janko, Finite nonabelian 2-groups all of whose minimal nonabelian subgroups are of exponent 4, *J. Algebra* **315** (2007), 801–808.

[Jan26] Z. Janko, Finite 2-groups with exactly one nonmetacyclic maximal subgroup, *Israel J. Math.* **16** (2008), 313–347.

[Jan27] Z. Janko, Finite 2-groups all of whose maximal cyclic subgroups of composite order are self-centralizing, *J. Group Theory* **10** (2007), 1–4.

[Jan28] Z. Janko, Cyclic subgroups of order 4 in finite 2-groups, *Glas. Mat.* **42(62)** (2007), 345–355.

[Jan29] Z. Janko, Some peculiar minimal situations by finite p-groups, *Glas. Mat.* **43(63)** (2008), 111–120.

[Jan30] Z. Janko, On minimal nonabelian subgroups of p-groups, *J. Group Theory* **12** (2009), 289–303.

[Jan31] Z. Janko, Some exceptional minimal situations by finite p-groups, in: *Ischia Group Theory 2008*, Proceedings of the Conference in Group Theory (Naples, Italy, April 1–4, 2008), pp. 116–119, World Scientific Publishing, Singapore, 2009.

[Jan32] Z. Janko, Finite nonabelian 2-groups such that any two distinct minimal nonabelian subgroups have cyclic intersection, *J. Group Theory* **13** (2010), 549–554.

[Jan33] Z. Janko, Finite p-groups G with $p > 2$ and $\mathrm{d}(G) = 2$ having exactly one maximal subgroup which is neither abelian nor minimal nonabelian, *Glas. Mat.*, to appear.

[Jan34] Z. Janko, Finite p-groups G with $p > 2$ and $\mathrm{d}(G) > 2$ having exactly one maximal subgroup which is neither abelian not minimal nonabelian, *Glas. Mat.*, to appear.

[Jan35] Z. Janko, Finite p-groups all of whose subgroups have normalizers of index at most p, *J. Algebra*, to appear.

[Jan36] Z. Janko, Finite nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic to $\mathrm{M}_{2^{n+1}} = \langle a, t \mid a^{2^n} = t^2 = 1,\ a^t = a^{1+2^{n-1}} \rangle$, $n \geq 3$ fixed, manuscript.

[Jan37] Z. Janko, Finite nonabelian 2-groups all of whose minimal nonabelian subgroups are metacyclic and have exponent 4, *J. Algebra*, to appear.

[John] D. L. Johnson, A property of finite p-groups with trivial multiplicator, *Amer. J. Math.* **98** (1976), 105–108.

[JonK1] D. Jonah and M. Konvisser, Abelian subgroups p-groups, an algebraic approach, *J. Algebra* **34** (1975), 386–402.

[JKon2] D. Jonah and M. W. Konvisser, Some nonabelian p-groups with abelian automorphism groups, *Arch. Math.* **26** (1975), 131–133.

[Jon1] M. R. Jones, Multiplicators of p-groups, *Math. Z.* **127** (1972), 165–166.

[Jon2] M. R. Jones, A property of finite p-groups with trivial multiplicators, *Trans. Amer. Math. Soc.* **210** (1975), 179–183.

[Juh] A. Juhasz, The group of automorphisms of a class of finite groups, *Trans. Amer. Math. Soc.* **270** (1982), no. 2, 467–481.

K

[Kal1] L. Kaloujnine, La structure des p-groupes de Sylow des groupes symetriques finis, *Ann. Sci Éc. Norm. Supér.* **65** (1968), 239–276.

[Kal2] L. Kaloujnine, Zum Problem der Klassifikation der endlichen metabelschen p-Gruppen, *Wiss. Z. Humboldt-Univ. Berlin, Math.-Nat. Reihe* **4** (1955), 1–7.

[Kan] M. Kanazawa, On a class of p-groups, *Kumamoto J. Sci. (Math.)* **10** (1973), 1–24.

[KaS] I. L. Kantor and A. S. Solodovnikov, *Hypercomplex Numbers. An Elementary Introduction to Algebras*, Springer-Verlag, New York, 1989.

[Kap] L.-G. Kappe, On power margins, *J. Algebra* **122** (1989), 337–344.

[KapY] L.-G. Kappe and J. Ying, On exact power margin groups, *Rend. Semin. Mat. Univ. Padova* **87** (1992), 246–265.

[Kar1] G. Karpilovsky, *The Schur Multiplier*, Clarendon Press, Oxford, 1986.

[Kar2] G. Karpilovsky, *Group Representations*, Volume 2, North-Holland, Amsterdam, 1993.

[Kar3] G. Karpilovsky, *Projective Representations of Finite Groups*, Monographs and Textbooks in Pure and Applied Mathematics 94, Marcel Dekker, Inc., New York, Basel, 1985.

[Kaz1] L. S. Kazarin, Groups with certain conditions for normalizers of subgroups, *Uchen. zapiski Perm Univ.* **218** (1969), 268–279 (Russian).

[Kaz2] L. S. Kazarin, On some classes of finite groups, *Soviet Math. Dokl.* **12** (1971), no. 2, 549–553.

[Kaz3] L. S. Kazarin, Groups with restrictions on normalizers of subgroups, *Izv. vuzov (mathematics)* **2** (1973), 41–50 (Russian).

[Kaz4] L. S. Kazarin, On the product of two nilpotent groups, in: *Problems in Group Theory and Homological Algebra*, pp. 62–66, Yaroslavl, 1981; II, *ibid*, pp. 47–49, Yaroslavl, 1982 (Russian).

[Kaz5] L. S. Kazarin, On groups with factorization, *Soviet Math. Dokl.* **23** (1981), no. 1, 19–22 (Russian).

[Kaz6] L. S. Kazarin, On Burnside's p^α-lemma, *Mat. Zametki* **48** (1990), 45–48; English translation in *Math. Notes* **48** (1990), 749–751.

[Keg1] O. H. Kegel, Produkte nilpotenter Gruppen, *Arch. Math.* **12** (1961), 90–93.

[Keg2] O. H. Kegel, Die Nilpotenz der H_p-Gruppen, *Math. Z.* **75** (1960), 373–376.

[Khu1] E. I. Khukhro, *Nilpotent Groups and Their Automorphisms*, Walter de Gruyter, Berlin, 1993.

[Khu2] E. I. Khukhro, *p-Automorphisms of Finite p-Groups*, CUP, Cambridge, 1998.

[Kim1] I. Kiming, Some remarks on a certain class of finite p-groups, *Math. Scand.* **76** (1995), 35–49.

[Kim2] I. Kiming, Structure and derived length of finite p-groups possessing an automorphism of p-power order having exactly p fixed points, *Math. Scand.* **62** (1988), 153–172.

[Kin1] B. W. King, Normal subgroups of groups of prime-power order, in: *Proceedings of the 2nd International Conference on the Theory of Groups*, pp. 401–408, Lecture Notes in Mathematics 372, Springer-Verlag, Berlin, 1973.

[Kin2] B. W. King, Normal structure of p-groups, *Bull. Aust. Math. Soc.* **10** (1974), 317–318.

[Kino] Y. Kinosita, On an enumeration of certain subgroups of a p-group, *J. Osaka Inst. Sci. Tech., Part I* **1** (1949), 13–20.

[Klu] F. L. Kluempen, The power structure of 2-generator 2-groups of class two, *Algebra Colloq.* **9** (2002), no. 3, 287–302.

[Kno] H. G. Knoche, Über den Frobeniusschen Klassenbegriff in nilpotenten Gruppen, I, II, *Math. Z.* **55** (1951), 71–83; *ibid* **59** (1953), 8–16.

[Kon1] M. Konvisser, Embedding of abelian subgroups in p-groups, *Trans. Amer. Math. Soc.* **153** (1971), 469–481.

[Kon2] M. Konvisser, 2-groups which contain exactly three involutions, *Math. Z.* **130** (1973), 19–30.

[Kon3] M. Konvisser, Metabelian p-groups which contain a self-centralizing element, *Illinois J. Math.* **14** (1970), 650–657.

[Kon4] M. Konvisser, 2-groups of normal rank 2 for which the Frattini subgroup has rank 3, *Trans. Amer. Math. Soc.* **165** (1972), 451–469.

[KonJ] M. Konvisser and D. Jonah, Counting abelian subgroups of p-groups. A projective approach, *J. Algebra* **34** (1975), 309–330.

[KovN] L. G. Kovacs and M. F. Newman, Direct complementation in groups with operators, *Arch. Math.* **13** (1962), 427–433.

[KLG] L. G. Kovacs and C. R. Leedham-Green, Some normally monomial p-groups of maximal class and large derived length, *Quart. J. Math. Oxford Ser. (2)* **37** (1986), 49–54.

[KM] J. Krempa and I. Malinowska, Groups of p-automorphisms for finite p-groups, *Publ. Math. Debrecen* **61** (3–4) (2002), 495–509.

[Kul] A. Kulakoff, Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p-Gruppen, *Math. Ann.* **104** (1931), 779–793.

[KS] H. Kurzweil und B. Stellmacher, *Theorie der endlichen Gruppen. Eine Einführung*, Springer-Verlag, Berlin, 1998.

L

[Laf1] T. J. Laffey, The minimum number of generators of a finite p-group, *Bull. Lond. Math. Soc.* **5** (1973), 288–290.

[Laf2] T. J. Laffey, Bounding the order of a finite p-group, *Proc. R. Ir. Acad.* **80a** (1980), no. 2, 131–134.

[Laf3] T. J. Laffey, A lemma on finite p-groups and some consequences, *Proc. Cambridge Philos. Soc.* **75** (1974), 133–137.

[Laf4] T. J. Laffey, Centralizers of elementary abelian subgroups in finite p-groups, *J. Algebra* **51** (1978), 88–96.

[Laf5] T. J. Laffey, The number of solutions of $x^3 = 1$ in a 3-group, *Math. Z.* **149** (1976), no. 1, 43–45.

[Lam1] T.-Y. Lam, Artin exponent of finite groups, *J. Algebra* **9** (1968), 94–119.

[Lam2] T.-Y. Lam, On the number of solutions of $x^{p^k} = a$ in a p-group, *Illinois J. Math.* **32** (1988), 575–583.

[Lang] S. Lang, *Algebra*, Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2002.

[Lan] G. L. Lange, Two-generator Frattini subgroups of finite groups, *Israel J. Math.* **29** (1978), 357–360.

[LGMK1] C. R. Leedham-Green and S. McKay, *The Structure of Groups of Prime Power Order*, London Mathematical Monographs, New Series, Oxford Science Publications, Oxford University Press, Oxford, 2002.

[LGMK2] C. R. Leedham-Green and S. McKay, On p-groups of maximal class, I, *Quart. J. Math. Oxford Ser. (2)* **27** (1976), 297–311; II, *ibid.* **29** (1978), 175–186; III, *ibid* **29** (1978), 281–299.

[LGN] C. R. Leedham-Green and P. M. Neumann, Space groups and groups of prime power order I, *Arch. Math.* **35** (1980), 193–202.

[LGNW] C. R. Leedham-Green, P. M. Neumann and J. Wiegold, The breadth and the class of a finite p-group, *J. London Math. Soc. (2)* **1** (1969), 409–420.

[Leo] A. Leone, Finite minimal non-KC-groups, *Matematiche* **38** (1987), 191–200.

[Leon1] Y. K. Leong, Finite 2-groups of class two with cyclic centre, *J. Aust. Math. Soc. Ser. A* **27** (1979), 125–140.

[Leon2] Y. K. Leong, Odd order nilpotent groups of class two with cyclic centre, *J. Aust. Math. Soc.* **17** (1974), 142–153.

[Lem] S. Lemiex, Finite exceptional p-groups of small order, *Comm. Algebra* **35** (2007), no. 6, 1890–1894.

[Lev1] F. W. Levi, Groups in which the commutator operations satisfy certain algebraic conditions, *J. Indian Math. Soc. (N.S.)* **6** (1942), 87–97.

[Lev2] F. W. Levi, Notes on group theory. I, II, *J. Indian Math. Soc. (N.S.)* **8** (1944), 1–9.

[LC] Heng Li and G. Y. Chen, On Cernikov p-groups, *Discrete Math.* **308** (2008), no. 21, 4992–4997.

[Li1] Shirong Li, The structure of NC-groups, *J. Algebra* **241** (2001), 611–619.

[Li2] Shirong Li, Finite 2-groups with large centralizers of abelian subgroups, *Math. Proc. R. Ir. Acad.* **104A** (2004), no. 2, 191–197.

[Li3] Shirong Li, The number of conjugacy classes of nonnormal cyclic subgroups in nilpotent groups of odd order, *J. Group Theory* **1** (1998), 165–171.

[Li4] Tianze Li, A simple example of two groups with the same automorphism group, *Arch. Math.* **92** (2009), 287–290.

[Lie1] H. Liebeck, A note an prime-power groups with symmetrical generating relations, *Proc. Cambridge Philos. Soc.* **51** (1955), 594–595.

[Lie2] H. Liebeck, The automorphism group of a finite p-group, *J. Algebra* **4** (1966), 426–432.

[Lie3] H. Liebeck, Outer automorphisms in nilpotent groups of class 2, *J. Lond. Math. Soc.* **40** (1965), 268–275.

[LM] P. Longobardi and M. Maj, On p-groups of breadth two, *Algebra Colloq.* **6** (1999), 121–124.

[LMM] P. Longobardi, M. Maj and A. Mann, Minimal classes and maximal class in p-groups, *Israel J. Math.* **110** (1999), 93–102.

[LubM] A. Lubotzky and A. Mann, Powerful p-groups 1, *J. Algebra* **105** (1987), 484–505.

[Luc] A. Luccini, On the order of transitive permutation groups with cyclic point-stabilizer, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **9** (1998), no. 4, 241–243.

[LZY] Heng Lv, Wei Zhou and Dapeng Yu, Some finite p-groups with bounded index of every normal subgroup in its normal closure, *J. Algebra* (to appear).

M

[Macd1] I. D. Macdonald, Generalizations of a classical theorem on nilpotent groups, *Illinois J. Math.* **8** (1964), 556–570.

[Macd2] I. D. Macdonald, A question of C. R. Hobby on regular p-groups, *Proc. Edinb. Math. Soc. (2)* **18** (1973), 207–208.

[Macd3] I. D. Macdonald, Commutators and their products, *Amer. Math. Monthly* **93** (1986), 440–444.

[Macd4] I. D. Macdonald, Finite p-groups with unique maximal classes, *Proc. Edinb. Math. Soc. (2)* **26** (1983), 233–239.

[Macd5] I. D. Macdonald, The breadth of finite p-groups, *Proc. Roy. Soc. Edinburgh Sect. A* **78** (1977/78), 1–39.

[Macd6] I. D. Macdonald, Groups of breadth four have class five, *Glasg. Math. J.* **19** (1978), 141–148.

[Macd7] I. D. Macdonald, Computer results on Burnside groups, *Bull. Aust. Math. Soc.* **9** (1973), 433–438.

[Macd8] I. D. Macdonald, Solution of the Hudges problem for finite groups of class $2p - 2$, *Proc. Amer. Math. Soc.* **27** (1971), 39–42.

[Macd9] I. D. Macdonald, Some examples in the theory of groups, in: *Mathematical Essays Dedicated to A. J. Macintyre*, pp. 263–269, Ohio University Press, Athens, Ohio, 1970.

[Macd10] I. D. Macdonald, On cyclic commutator subgroups, *J. Lond. Math. Soc.* **38** (1963), 419–422.

[Macd11] I. D. Macdonald, On central series, *Proc. Edinb. Math. Soc. (2)* **3** (1962/63), 175–178.

[Macd12] I. D. Macdonald, Some p-groups of Frobenius and extraspecial types, *Israel J. Math.* **40** (1981), 350–364.

[Macd13] I. D. Macdonald, More on p-groups of Frobenius type, *Israel J. Math.* **56** (1986), 335–344.

[Macd14] I. D. Macdonald, A computer application to finite p-groups, *J. Aust. Math. Soc. Ser. A* **17** (1974), 102–112.

[Macd15] I. D. Macdonald, On Hughes problem and others, *J. Aust. Math. Soc.* **10** (1969), 475–479.

[Macd16] I. D. Macdonald, Some explicit bounds in groups with finite derived groups, *Proc. Lond. Math. Soc. (3)* **11** (1981), 23–56.

[MacW] A. R. MacWilliams, On 2-groups with no normal abelian subgroup of rank 3 and their occurrence as Sylow 2-subgroups of finite simple groups, *Trans. Amer. Math. Soc.* **150** (1970), 345–408.

[Mal1] I. Malinowska, Finite p-groups with few automorphisms, *J. Group Theory* **4** (2001), 395–400.

[Mal2] I. Malinowska, p-automorphisms of finite p-groups: problems and questions, in: *Advances in Group Theory*, pp. 111–127, Aracne Editrice, Rome, 2002.

[Mal3] I. Malinowska, On quasi-inner automorphisms of a finite p-group, *Publ. Math. Debrecen* **41** (1992), 73–77.

[Mal4] I. Malinowska, On automorphism groups of finite p-groups, *Rend. Semin. Mat. Univ. Padova* **91** (1994), 265–271.

[Mal5] I. Malinowska, On finite nearly uniform groups, *Publ. Math. Debrecen* **69** (2006), no. 1–2, 155–169.

[Man1] A. Mann, Generators of 2-groups, *Israel J. Math.* **10** (1971), 158–159.

[Man2] A. Mann, Regular p-groups, *Israel J. Math.* **10** (1971), 471–477.

[Man3] A. Mann, Regular p-groups, II, *Israel J. Math.* **14** (1973), 294–303.

[Man4] A. Mann, Regular p-groups, III, *J. Algebra* **70** (1981), 89–101.

[Man5] A. Mann, The power structure of p-groups I, *J. Algebra* **42** (1976), 121–135; II, *ibid* **318** (2007), 953–956.

[Man6] A. Mann, Regular p-groups and groups of maximal class, *J. Algebra* **42** (1976), 136–141.

[Man7] A. Mann, Conjugacy classes in finite groups, *Israel J. Math.* **31** (1978), 78–84.

[Man8] A. Mann, Groups with small abelian subgroups, *Arch. Math.* **50** (1988), 210–213.

[Man9] A. Mann, Extreme elements of finite p-groups, *Rend. Semin. Mat. Univ. Padova* **83** (1990), 45–54.

[Man10] A. Mann, On p-groups whose maximal subgroups are isomorphic, *J. Aust. Math. Soc. Ser. A* **59** (1995), 143–147.

[Man11] A. Mann, The number of generators of finite p-groups, *J. Group Theory* **8** (2005), 317–337.

[Man12] A. Mann, Minimal characters of p-groups, *J. Group Theory* **2** (1999), 225–250.

[Man13] A. Mann, On the splitting of extensions by a group of prime order, *Arch. Math.* **56** (1991), 105–106.

[Man14] A. Mann, Some finite groups with large conjugacy classes, *Israel J. Math.* **71** (1990), 55–63.

[Man15] A. Mann, Generators of p-groups, in: *Proceedings of the St. Andrews Conference on Groups 1985*, pp. 273–281, London Mathematical Society Lecture Notes 121, Cambridge University Press, Cambridge, 1986.

[Man16] A. Mann, Some applications of powerful p-groups, in: *Proceedings of the St. Andrews Conference on Groups 1989*, pp. 370–385, London Mathematical Society Lecture Notes Series 159, Cambridge University Press, Cambridge, 1991.

[Man17] A. Mann, A transfer result for powerful Sylow subgroups, *J. Algebra* **178** (1995), 299–301.

[Man18] A. Mann, Finite groups with maximal normalizers, *Illinois J. Math.* **12** (1968), 67–75.

[Man19] A. Mann, Enumerating finite groups and their defining relations, *J. Group Theory* **1** (1998), 59–64.

[Man20] A. Mann, Some questions about p-groups, *J. Aust. Math. Soc. Ser. A* **67** (1999), 356–379.

[Man21] A. Mann, The derived length of p-groups, *J. Algebra* **224** (2000), 263–267.

[Man22] A. Mann, Finite p-Groups, in preparation.

[Man23] A. Mann, Groups generated by elements of small breadth, *J. Group Theory* **4** (2001), 241–246.

[Man24] A. Mann, On the power structure of some p-groups, *Circ. Mat. Palermo II* **23** (1990), 227–235.

[Man25] A. Mann, Groups with few class sizes and the centralizer equality subgroup, *Israel J. Math.* **142** (2004), 367–380.

[Man26] A. Mann, Philip Hall's 'rather curious' formula for abelian p-groups, *Israel J. Math.* **96B** (1996), 445–448.

[Man27] A. Mann, An inequality for group presentations, *Bull. Aust. Math. Soc.* **62** (2000), 467–469.

[Man28] A. Mann, Conjugacy class sizes in finite p-groups, *J. Aust. Math. Soc.* **85** (2008), 251–255; correction, *ibid.* **87** (2009), 429–431.

[Man29] A. Mann, On characters-classes duality and orders of centralizers, *Contemp. Math.* **402** (2006), 215–217.

[Man30] A. Mann, Normally monomial p-groups, *J. Algebra* **300** (2006), 2–9.

[Man31] A. Mann, On the exponent of the product of two groups, *Rend. Semin. Mat. Univ. Padova* **115** (2006), 205–207.

[Man32] A. Mann, Elements of minimal breadth in finite p-groups and Lie algebras, *J. Aust. Math. Soc.* **81** (2006), 209–214.

[Man33] A. Mann, The number of subgroups of metacyclic groups, *Contemp. Math.* **524** (2010), 93–95.

[Man34] A. Mann, The power structure of p-groups, II., *J. Algebra* **318** (2007), 953–956.

[Man35] A. Mann, On skew p-groups, *Publ. Math. Debrecen* **69** (2006), 353–360.

[MM] A. Mann and C. Martinez, The exponent of finite groups, *Arch. Math.* **67** (1996), 8–10.

[ManS] A. Mann and C. Scoppola, On p-groups of Frobenius type, *Arch. Math.* **56** (1991), 320–332.

[Mas] D. Mason, On finite simple groups G in which every element of $L(G)$ is of Bender type, *J. Algebra* **40** (2002), 125–202.

[Mat] H. Matsuyama, Solvability of groups of order $2^a p^b$, *Osaka J. Math.* **10** (1973), 375–378.

[Mat1] S. Mattarei, An example of p-groups with identical character tables and different derived lengths, *Arch. Math.* **62** (1994), 12–20.

[Mat2] S. Mattarei, On character tables of wreath products, *J. Algebra* **175** (1995), 157–178.

[Mar] S. Martin, Almost all p-groups have automorphism group a p-group, *Bull. Amer. Math. Soc.* **15** (1986), 78–82.

[Maz1] M. Mazur, On powers in powerful p-groups, *J. Group Theory* **10** (2007), no. 4, 431–433.

[Maz2] V. D. Mazurov, 2-groups with an automorphism of odd order fixing all involutions, *Algebra Logika* **8** (1969), no. 6, 874–885 (Russian).

[Mazz1] N. Mazza, The Dade group of a metacyclic p-group, *J. Algebra* **266** (2003), no. 1, 102–111.

[Mazz2] N. Mazza, Connected components of the category of elementary abelian subgroups, *J. Algebra* **320** (2008), no. 12, 4242–4248.

[McK1] S. McKay, *Finite p-Groups*, Queen Mary Mathematical Notes 18, Queen Mary & Westfield College, University of London, London, 2000.

[McK2] S. McKay, On the structure of a special class of p-groups, *Quart. J. Math. Oxford Ser. (2)* **38** (1987), 489–502.

[McKel] A. M. McKelven, Groups of order 2^m that contain cyclic subgroups of order 2^{m-3}, *Amer. Math. Monthly* **13** (1906), 121–136.

[MS] U. Meierfrankenfeld and B. Stellmacher, The generic groups of p-type, preprint, Michigan State University, 1997.

[Men] F. Menegazzo, Automorphisms of p-groups with cyclic commutator subgroup, *Rend. Semin. Mat. Univ. Padova* **90** (1993), 81–101.

[Mie1] R. J. Miech, Metabelian p-groups of maximal class, *Trans. Amer. Math. Soc.* **152** (1970), 331–373.

[Mie2] R. J. Miech, Some p-groups of maximal class, *Trans. Amer. Math. Soc.* **189** (1974), 1–47.

[Mie3] R. J. Miech, On p-groups with a cyclic commutator subgroup, *J. Aust. Math. Soc.* **20** (1975), 178–198.

[Mie4] R. J. Miech, The metabelian p-groups of maximal class, *Trans. Amer. Math. Soc.* **236** (1978), 93–119.

[Mie5] R. J. Miech, The metabelian p-groups of maximal class, II, *Trans. Amer. Math. Soc.* **272** (1982), 465–484.

[Mil1] G. A. Miller, An extension of Sylow's theorem, *Proc. Lond. Math. Soc. (2)* **2** (1904), 142–143.

[Mil2] G. A. Miller, Number of abelian subgroups in every prime power group, *Amer. J. Math.* **51** (1929), 31–34.

[Mil3] G. A. Miller, A nonabelian group whose group of isomorphisms is abelian, *Messenger Math.* **43** (1913), 124–125 (or G. A. Miller, *Collected Works, Volume 5*, pp. 415–417, University of Illinois Press, Urbana, 1959).

[Mil4] G. A. Miller, On the groups of order p^m which contain operators of order p^{m-2}, *Trans. Amer. Math. Soc.* **26** (1902), 383–387.

[Mil5] G. A. Miller, Isomorphisms of a group whose order is a power of a prime, *Trans. Amer. Math. Soc.* October (1911), 387–402.

[Mil6] G. A. Miller, The groups of order p^m which contain exactly p cyclic subgroups of order p^α, *Trans. Amer. Math. Soc.* **7** (1906), 228–232.

[Mil7] G. A. Miller, Determination of all the groups of order 2^m which contain an odd number of cyclic subgroups of composite order, *Trans. Amer. Math. Soc.* **6** (1905), 58–62.

[Mil8] G. A. Miller, On the holomorph of the cyclic group of order p^m, *Trans. Amer. Math. Soc.* **9** (1908), 232–236.

[Mil9] G. A. Miller, The groups in which every subgroup is either abelian or Hamiltonian, *Trans. Amer. Math. Soc.* **8** (1907), 25–29.

[MilM] G. Miller and H. Moreno, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.* **4** (1903), 398–404.

[Mill] W. H. Mills, The automorphisms of the holomorph of a finite abelian group, *Trans. Amer. Math. Soc.* **85** (1956), 1–34.

[Miy] K. Miyake, The application of the principal ideal theorem to p-groups, *Nagoya Math. J.* **99** (1985), 73–88.

[MLC] E. Morgado Morales and M. Lazo Cortis, On the Sylow p-groups of the automorphism group of a finite homocyclic p-group, *Rev. Cienc. Mat.* **6** (1985), 35–44 (Spanish).

[Mori1] M. Morigi, A note on factorized (finite) p-groups, *Rend. Semin. Mat. Univ. Padova* **98** (1997), 101–105.

[Mori2] M. Morigi, Power automorphisms of finite p-groups, *Comm. Algebra* **70** (1999), 4853–4877.

[Mori3] M. Morigi, On the minimal number of generators of finite non-abelian p-groups having an abelian automorphism group, *Comm. Algebra* **23** (1995), 2045–2064.

[Mori4] M. Morigi, On p-groups with abelian automorphism group, *Rend. Semin. Mat. Univ. Padova* **92** (1994), 47–58.

[Mul] O. Müller, On p-automorphisms of finite p-groups, *Arch. Math.* **32** (1979), 533–538.

N

[Nak1] K. Nakamura, Über den Quasinormalteiler der regulären p-Gruppe von der Klasse 2, *Nagoya Math. J.* **26** (1966), 61–67.

[Nak2] K. Nakamura, Über einige Beispiele der Quasinormalteiler einer p-Gruppe, *Nagoya Math. J.* **31** (1968), 97–103.

[Nap1] F. Napolitani, Sui p-gruppi modulari finiti, *Rend. Semin. Mat. Univ. Padova* **39** (1967), 296–303.

[Nap2] F. Napolitani, Gruppi finite minimal non modulari, *Rend. Semin. Mat. Univ. Padova* **45** (1971), 229–248.

[Nei] L. I. Neikirk, Groups of order p^m which contain cyclic subgroups of order p^{m-3}, *Trans. Amer. Math. Soc.* **6** (1905), 316–325.

[Nek1] K. G. Nekrasov, On finite 2-groups with small Frattini subgroup, in: *Logical-Algebraic Constructions*, pp. 75–82, Tver, 1992 (Russian).

[Nek2] K. G. Nekrasov, On some 2-groups with a small noncyclic Frattini subgroup, in: *Algebraic and logical constructions*, pp. 53–65, Tver, 1994 (Russian).

[Nek3] K. G. Nekrasov, *Elementary Proof of Wall's Result on the Structure of Finite Groups with a Great Number of Involutions*, Kalinin. Gos. Univ., Kalinin, 1983, Dep. VINITI 6/2/1984, N 789-84 (Russian).

[Nek4] K. G. Nekrasov, Structure of finite groups with a great number of involutions, in: *Questions of Group Theory and Homological Algebra*, pp. 23–25, Yaroslavl, 1985 (Russian).

[NekB] K. G. Nekrasov and Y. Berkovich, Necessary and sufficient condition for cyclicity of the Frattini subgroup of a finite p-group, in: *Questions of Group Theory and Homological Algebra*, pp. 35–37, Yaroslavl, 1985 (Russian).

[Neu1] B. H. Neumann, Groups covered by finitely many cosets, *Publ. Math. Debrecen* **3** (1954), 227–242

[Neu2] B. H. Neumann, On some finite groups with trivial multiplicator, *Publ. Math. Debrecen* **4** (1955), 190–194.

[Neu3] B. H. Neumann, On a conjecture of Hanna Neumann, *Proc. Glasg. Math. Assoc.* **1** (1956), 13–17.

[Neu4] B. H. Neumann, Some finite groups with few defining relations, *J. Aust. Math. Soc. Ser. A* **38** (1985), 230–240.

[Neu5] B. H. Neumann, Yet more on finite groups with few defining relations, in: *Proceedings of the Singapore Group Theory Conference 1987*, pp. 183–193, Walter de Gruyter, Berlin, 1989.

[Neu6] P. M. Neumann, Two combinatorial problems in group theory, *Bull. Lond. Math. Soc.* **21** (1989), 456–458.

[NO] M. F. Newman and E. A. O'Brien, Classifying 2-groups by coclass, *Trans. Amer. Math. Soc.* **351** (1999), 131–169.

[Nin] Y. Ninomiya, Finite p-groups with cyclic subgroups of index p^2, *Math. J. Okayama Univ.* **36** (1994), 1–21.

[Nori] T. Noritzsch, A note on character degrees of p-groups and their normal subgroups, *Arch. Math.* **59** (1992), 319–321.

O

[O'B1] E. A. O'Brien, The groups of order 256, *J. Algebra* **143** (1991), 219–235.

[O'BV-L] E. A. O'Brien and M. R. Vaughan-Lee, The groups of order p^7 for odd prime p, *J. Algebra* **292** (2005), no. 1, 243–258.

[O'BSV-L] E. A. O'Brien, C. M. Scoppola and M. R. Vaughan-Lee, Not every p-group can be generated by elements of the same order, *Proc. Amer. Math. Soc.* **134** (2006), no. 12, 3457–3464.

[Ols] A. Y. Olshanski, The number of generators and orders of abelian subgroups of finite p-groups, *Math. Notes* **23** (1978), 183–185

[OP] E. A. Ormerod and G. Parmeggiani, Finite p-groups with normal normalizers, *Bull. Aust. Math. Soc.* **69** (2004), 141–140.

[Ore] O. Ore, Contributions to the theory of groups of finite order, *Duke Math. J.* **5** (1938), 431–460.

[Ott] A. D. Otto, Central automorphisms of a finite p-group, *Trans. Amer. Math. Soc.* **125** (1966), 280–287.

P

[PS] P. P. Palfy and M. Szalay, The distribution of the character degrees of the symmetric p-groups, *Acta Math. Hungar.* **41** (1983), 137–150.

[PR] C. Parker and P. Rowley, *Symplectic Amalgams*, Springer-Verlag, Berlin, 2002.

[PS1] G. Parmeggiani and B. Stellmacher, p-groups of small breadth, *J. Algebra* **213** (1999), 52–68.

[Pas] D. S. Passman, Nonnormal subgroups of p-groups, *J. Algebra* **15** (1970), no. 3, 352–370.

[Pat1] A. R. Patterson (= MacWilliams), On Sylow 2-subgroups with no normal Abelian subgroups of rank 3, in finite fusion-simple groups, *Trans. Amer. Math. Soc.* **187** (1974), 1–67.

[Pat2] A. R. Patterson (= MacWilliams), The minimal number of generators for p-subgroups of $\mathrm{GL}(n, p)$, *J. Algebra* **32** (1974), 132–140.

[Paz] G. Pazdersky, Prime power groups which are cyclic extensions of elementary Abelian groups, *Math. Nachr.* **97** (1980), 57–68.

[Pen] E. A. Pennington, On products of finite nilpotent groups, *Math. Z.* **134** (1973), 81–83.

[Pet] J. Petrescu, Sur les commutateurs, *Math. Z.* **61** (1954), 348–356.

[Pil] O. S. Pilavskaya, Classification of groups of exponent p with an abelian normal subgroup of index p^2, in: *Infinite Groups and Related Algebraic Structures*, pp. 210–226, Kiev, 1993 (Russian).

[Pol] J. Poland, Two problems on finite groups with k conjugate classes, *J. Aust. Math. Soc.* **8** (1968), 49–55.

Q

[QT] G. H. Qian and F. Tang, Finite groups all of whose abelian subgroups are QTI-groups, *J. Algebra* **320** (2008), 3605–3611.

[QW] G. H. Qian and Y. M. Wang, A note on character kernels in finite groups of prime power order, *Arch. Math.* **90** (2008), no. 3, 193–199.

R

[Red1] L. Redei, Das schiefe Produkt in der Gruppentheorie, *Comment. Math. Helvet.* **20** (1947), 225–267.

[Red2] L. Redei, Die endlichen einstufig nichtnilpotenten Gruppe, *Publ. Math. Debrecen* **4** (1956), 303–324.

[Red3] L. Redei, *Endliche p-Gruppen*, Akademiai Kiado, Budapest, 1989.

[Rie] J. M. Riedl, Character degrees, class sizes and normal subgroups of a certain class of p-groups, *J. Algebra* **218** (1999), 190–215.

[Rocc] N. R. Rocco, On week commutativity between finite p-groups, *J. Algebra* **76** (1982), 471–488.

[Rock] D. M. Rocke, p-groups with abelian centralizers, *Proc. Lond. Math. Soc. (3)* **30** (1975), 55–75.

[Rod] E. Rodemich, The groups of order 128, *J. Algebra* **67** (1980), 129–142.

[Ron] C. Ronse, On centralizers of involutions in 2-groups, *Math. Proc. Cambridge Philos. Soc.* **86** (1979), 199–204.

[Roi1] M. Roitman, On Zsigmondy primes, *Proc. Amer. Math. Soc.* **125** (1997), 1913–1919.

[Roi2] M. Roitman, Relative indices of elements of finite p-groups, manuscript.

[Roq] P. Roquette, Realisierungen von Darstellungen endlicher nilpotenter Gruppen, *Arch. Math.* **9** (1958), 241–250.

[Rus1] D. J. Rusin, What is the probability that two elements of a finite group commute, *Pacific J. Math.* **82** (1979), 237–247.

[Rus2] D. J. Rusin, The 2-groups of rank 2, *J. Algebra* **149** (1992), 1–31.

S

[Sag1] I. A. Sagirov, Degrees of irreducible characters of 2-groups of Suzuki, *Math. Notes* **66** (1999), 258–263.

[Sag2] I. A. Sagirov, Degrees of irreducible characters of p-groups of Suzuki $\mathrm{A}_p(m, \theta)$, $p > 2$, to appear.

[Sag3] I. A. Sagirov, Finite groups having exactly two degrees of monolithic characters, in: *Questions of Group Theory and Homological Algebra*, pp. 1–8, University of Yaroslavl, Yaroslavl, 1998.

[Sak] A. I. Saksonov, Answer on a Brauer question, *Izv. Akad. Nauk BSSR, fiz.-mat. nauki* **1** (1967), 129–130.

[SMDS] A. R. Salemkar, M. R. R. Moghaddam, M. Davarpanah and F. Saeedi, A remark on the Schur multiplier of p-groups, *Comm. Algebra* **35** (2007), no. 4, 1215–1221.

[SMS] A. R. Salemkar, M. R. R. Moghaddam and F. Saeedi, The commutator subgroup Schur multiplier of a pair of finite groups, *J. Aust. Math. Soc.* **81** (2006), no. 1, 1–9.

[San] P. J. Sanders, The coexponent of a regular p-group, *Comm. Algebra* **28** (2000), 1309–1333.

[SanW] P. J. Sanders and T. S. Wilde, The class and coexponent of a finite p-group, manuscript.

[Sand] P. R. Sanders, The central automorphisms of a finite group, *J. Lond. Math. Soc.* **44** (1969), 225–228.

[Sano] I. N. Sanov, Solution of Burnside's problem for exponent four, *Leningrad State Univ. Ann. Math. Ser.* **10** (1940), 166–170.

[Sau] M. du Sautoy, Counting p-groups and nilpotent groups, *Publ. Math. Inst. Hautes Études Sci.* **92** (2000), 63–112.

[Sc] E. Schenkman, On the norm of a group, *Illinois J. Math.* **4** (1960), 150–152.

[Schm1] P. Schmid, Normal p-subgroups in the group of outer automorphisms of a finite p-group, *Math. Z.* **147** (1976), 271–277.

[Schm2] P. Schmid, Frattinian p-groups, *Geom. Dedicata* **6**, (1990), 359–364.

[Schm3] P. Schmid, On the automorphism group of extraspecial 2-groups, *J. Algebra* **234** (2000), 492–506.

[Schm4] P. Schmid, Über den grössten nilpotenten Normalteiler der Automorphismengruppe einer endlichen Gruppe, *J. Algebra* **25** (1973), 165–171.

[Sch1] O. Y. Schmidt, A new proof of the theorem of A. Kulakoff in group theory, *Mat. Sb.* **39** (1932), 66–71 (Russian).

[Sch2] O. Y. Schmidt, Groups all whose subgroups are nilpotent, *Mat. Sb.* **31** (1924), 366–372 (Russian).

[Sch3] O. Y. Schmidt, Groups having only one class of nonnormal subgroups, *Mat. Sb.* **33** (1926), 161–172 (Russian).

[Sch4] O. Y. Schmidt, Groups with two classes of nonnormal subgroups, *Proc. Seminar on Group Theory* (1938), 7–26 (Russian).

[Schn1] C. Schneider, On the derived subgroup of a finite p-group, *Austral. Math. Soc. Gaz.* **26** (1999), 232–237.

[Schn2] C. Schneider, Groups of prime-power order with a small second derived quotient, *J. Algebra* **286** (2003), 539–551.

[Schn3] C. Schneider, On derived series of a finite p-group, arXiv.math.GR/0510220v2 25 Oct 2005, 1–20.

[Schr] O. Schreier, Über die Erweiterung von Gruppen, I, *Monatsh. Math. Physik* **34** (1926), 165–180; II, *Abh. Math. Semin. Univ. Hambg.* **4** (1926), 321–346.

[Sco] C. M. Scoppola, Groups of prime power order as Frobenius–Wielandt complements, *Trans. Amer. Math. Soc.* **325** (1991), 855–874.

[ScS] C. M. Scoppola and A. Shalev, Applications of dimension subgroups to the power structure of p-groups, *Israel J. Math.* **73** (1991), 45–56.

[Scot] W. R. Scott, *Group Theory*, Prentice Hall, Englewood Cliffs, 1964.

[Sei1] G. Seitz, Finite groups having only one irreducible representation of degree greater than one, *Proc. Amer. Math. Soc.* **19** (1968), 459–461.

[Sha1] A. Shalev, The structure of finite p-groups: effective proof of coclass conjectures, *Invent. Math.* **115** (1994), 315–345.

[Sha2] A. Shalev, Finite p-groups, in: *Finite and Locally Finite Groups*, pp. 401–450, Kluwer Academic Publications, Dodrecht, 1995.

[She] V. A. Sheriev, A description of the class of finite p-groups whose 2-maximal subgroups are abelian, in: *Proceedings of a Seminar on Algebraic Systems 2*, pp. 25–76, Krasnoyarsk, 1970 (Russian).

[Shul] E. E. Shult, On finite automorphic algebras, *Illinois J. Math.* **13** (1969), 625–653.

[Shum] P. Shumyatsky, Involutory automorphisms of finite groups and their centralizers, *Arch. Math.* **71** (1998), 425–432.

[Sil] G. Silberberg, Finite equilibrated 2-generated 2-groups, *Acta Math. Hungar.* **110** (2006) 23–35.

[Sim] C. C. Sims, Enumerating p-groups, *Proc. Lond. Math. Soc.* **15** (1965), 151–166.

[SU] V. M. Sitnikov and A. D. Ustjuzaninov, Finite groups with three classes of non-invariant subgroups, *Ural Gos. Univ. Mat. Zap.* **6** (1967), no. 1, 94–102 (Russian).

[Sla1] M. C. Slattery, Character degrees of finite p-groups, in: *The Arcata Conference on Representations of Finite Groups*, pp. 89–92, Proceedings of Symposia in Pure Mathematics 47, Part 2, American Mathematical Society, Providence, RI, 1987.

[Sla2] M. C. Slattery, Character degrees and nilpotent class in p-groups, *J. Aust. Math. Soc. Ser. A* **57** (1994), 76–80.

[Sla3] M. C. Slattery, Character degrees and derived length in p-groups, *Glasg. Math. J.* **30** (1988), 221–230.

[Sla4] M. C. Slattery, Computing character degrees in p-groups, *J. Symbolic Comput.* **2** (1986), 51–58

[Spe] W. Specht, Isomorphic subgroups of finite p-groups revisited, *Canad. J. Math.* **26** (1974), 574–579.

[Sto] S. E. Stonehewer, Permutable subgroups of some finite p-groups, *J. Aust. Math. Soc.* **16** (1973), 90–97.

[SS] E. G. Straus and G. Szekeres, On a problem of D. R. Hughes, *Proc. Amer. Math. Soc.* **9** (1958), 157–158.

[Str] R. R. Struik, Some nonabelian 2-groups with abelian automorphism groups, *Arch. Math.* **39** (1982), 299–302.

[Suz1] M. Suzuki, *Group Theory*, Volume I and II, Springer-Verlag, Berlin, 1982 and 1986.

[Suz2] M. Suzuki, *Structure of a Group and the Structure of Its Lattice of Subgroups*, Ergebnisse der Mathematik und ihrer Grenzgebiete 10, Springer-Verlag, Berlin, 1956.

[Sze] G. Szekeres, On finite metabelian p-groups with two generators, *Acta Sci. Math. Szeged* **21** (1960), 270–291.

T

[Tau] O. Taussky, Remark on the class field tower, *J. Lond. Math. Soc.* **12** (1937), 82–85.

[TY] Y. Takegahara and T. Yoshida, Character theoretical aspects of nilpotency class, *Comm. Algebra* **36** (2008), no. 7, 2625–2637.

[Tes] L. Teschke, Über die Normalteiler der p-Sylowgruppe der symmetrische Gruppe vom Grade p^m, *Math. Nachr.* **87** (1979), 197–212.

[Tho1] J. G. Thompson, A replacement theorem for p-groups and a conjecture, *J. Algebra* **13** (1969), 149–151.

[Tho2] J. G. Thompson, Finite groups with fixed-point-free automorphisms of prime order, *Proc. Nat. Acad. Sci. USA* **45** (1959), 578–581.

[Tho3] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, 1, *Bull. Amer. Math. Soc.* **74** (1968), 383–437.

[Tho4] J. G. Thompson, Fixed points of p-groups acting on p-groups, *Math. Z.* **86** (1964), 12–13.

[Tho5] J. G. Thompson, Centralizers of elements in p-groups, *Math. Z.* **96** (1967), 292–293.

[Tow] M. J. Towers, *Modular Representations of p-Groups*, PhD Thesis, Hertford College, University of Oxford, 2005.

[Tim] F. Timmesfeld, A remark on Thompson's replacement theorem and a consequence, *Arch. Math.* **38** (1982), 491–492.

[Tis] T. Tisch, 2-Gruppen mit kleinen selbstzentralisierenden Untergruppen, *Comm. Algebra* **7** (1979), 833–844.

[Tit] G. N. Titov, Groups containing a cyclic subgroup of index p^3, *Mat. Zametki* **28** (1980), 17–24.

[Tua1] H. F. Tuan, A theorem about p-groups with abelian subgroup of index p, *Acad. Sin. Sci. Rec.* **3** (1950), 17–23.

[Tua2] H. F. Tuan, An Anzahl theorem of Kulakoff's type for p-groups, *Sci. Rep. Nat. Tsing-Hua Univ. A* **5** (1948), 182–189.

U

[Ust1] A. D. Ustjuzaninov, Finite 2-groups in which the set of self-centralizing abelian normal subgroups of rank ≥ 3 is empty ($\mathrm{SCN}_3(2) = \varnothing$), *Izv. Akad. Nauk SSSR* **37** (1973), 251–283 (Russian).

[Ust2] A. D. Ustjuzaninov, Finite 2-groups with three involutions, *Sibirsk. Mat. Z.* **13** (1972), 182–197.

V

[VL] M. R. Vaughan-Lee, Breadth and commutator subgroups of p-groups, *J. Algebra* **32** (1976), 278–285.

[VLW1] M. R. Vaughan-Lee and J. Wiegold, Breadth, class and commutator subgroups of p-groups, *J. Algebra* **32** (1974), 268–277.

[VLW2] M. R. Vaughan-Lee and J. Wiegold, Generation of p-groups by elements of bounded breadth, *Proc. Roy. Soc. Edinburgh Sec. A* **95** (1983), 215–221.

[V-L] A. Vera-Lopez, On the number of conjugacy classes in a finite p-group, *Hokkaido Math. J.* **18** (1989), 477–485.

[V-LA] A. Vera-Lopez and J. M. Arregi, Conjugacy classes of Sylow subgroups of GL(n, q), *J. Algebra* **152** (1992), 1–19.

[V-LF1] A. Vera-Lopez and G. A. Fernandez-Alcober, Centralizers of small order in p-groups of maximal class, *Comm. Algebra* **20** (1992), 1051–1059.

[V-LF2] A. Vera-Lopez and G. A. Fernandez-Alcober, The conjugacy vector of a p-group of maximal class, *Israel J. Math.* **86** (1994), 233–255.

[V-LL] A. Vera-Lopez and C. Larrea, On the number of conjugacy classes in a finite p-group, *Arch. Math.* **53** (1989), 126–133.

[V-LLO] A. Vera-Lopez and L. Ortiz de Elguea, The conjugacy-vectors of all relative holomorphs of an elementary abelian group of order 16, *Port. Math.* **47** (1990), no. 3, 243–257.

[V-LS] A. Vera-Lopez and J. Sangroniz, Classification of all relative holomorphs of an abelian group of type $C_4 \times C_4$, *Rev. R. Acad. Cienc. Exactas Fís. Quím. Nat. Zaragoza (2)* **43** (1988), 7–12 (Spanish).

[Ver1] L. Verardi, On groups whose non-central elements have the same finite number of conjugates, *Boll. Unione Mat. Ital. A (7)* 2 (1988), 391–400.

[Ver2] L. Verardi, A class of finite groups of exponent p in which every normal subgroup is characteristic, *Boll. Unione Mat. Ital. A (7)* **4** (1988), 307–317.

W

[Waa] R. W. van der Waall, On finite p-groups whose commutator subgroups are cyclic, *Indag. Math.* **35** (1973), 342–345.

[Wal] G. E. Wall, On Hughes' H_p-problem, in: *Proceeding of the International Conference on the Theory of Groups* (Canberra, 1965), pp. 357–362, Gordon and Breach, New York 1967.

[Wal2] G. E. Wall, Finite groups with class-preserving outer automorphisms, *J. Lond. Math. Soc.* **22** (1947), 315–320.

[Wal3] G. E. Wall, Secretive prime-power groups of large rank, *Bull. Aust. Math. Soc.* **12** (1975), 963–969.

[War] H. N. Ward, Automorphisms of quaternion-free 2-groups, *Math. Z.* **112** (1969), 52–58.

[Ward] B. L. van der Warden, *Algebra*, Volume I, Springer-Verlag, Berlin, 1971.

[WW] C. Warren and J. Wiegold, Generation of p-groups by elements of bounded breadth, *J. Group Theory* **2** (1999), 373–376.

[Web1] U. H. M. Webb, An elementary proof of Gaschütz' theorem, *Arch. Math.* **35** (1980), 23–26.

[Web2] U. H. M. Webb, The number of stem covers of an elementary abelian p-group, *Math. Z.* **182** (1983), no. 3, 327–337.

[Web3] U. H. M. Webb, The occurrence of groups as automorphisms of nilpotent p-groups, *Arch. Math.* **37** (1981), no. 6, 481–498.

[Web4] U. H. M. Webb, On the rank of a p-group of class 2, *Canad. Math. Bull.* **26** (1983), 101–105.

[Web5] U. H. M. Webb, The Schur multiplier of a nilpotent group, *Trans. Amer. Math. Soc.* **291** (1985), 755–763.

[Web6] U. H. M. Webb, The using graphs to investigate the automorphism groups of nilpotent groups, in: *Graphs and Applications*, pp. 223–247, Wiley-Interscience, New York, 1985.

[Weh] B. A. F. Wehrfritz, *Finite Groups*, World Scientific, Singapore, 1999.

[Wei1] P. M. Weichsel, On isoclinism, *J. Lond. Math. Soc.* **38** (1963), 63–65.

[Wei2] P. M. Weichsel, On critical p-groups, *Proc. Lond. Math. Soc. (3)* **14** (1964), 83–100.

[Wei3] P. M. Weichsel, On p-abelian groups, *Proc. Amer. Math. Soc.* **18** (1967), 736–737.

[Weir1] A. Weir, Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p, *Proc. Amer. Math. Soc.* **6** (1955), 529–533.

[Weir2] A. Weir, The Sylow subgroups of the symmetric groups, *Proc. Amer. Math. Soc.* **6** (1955), 534–541.

[Wer] J. Wergieluk, 3-*erzeugende* 2-*Gruppen, deren maximale Untergruppen alle* 2-*erzeugt sind*, Diplomarbeit, Technische Universität Wien, Wien, 2007.

[Wie1] J. Wiegold, Multiplicators and groups with finite central factor-groups, *Math. Z.* **89** (1965), 245–247.

[Wie2] J. Wiegold, The Schur multiplier: an elementary approach, *Proceedings of the St. Andrews Conference on Groups 1981*, pp. 137–154, London Mathematical Society Lecture Notes 71, Cambridge University Press, Cambridge, 1982.

[Wie3] J. Wiegold, The multiplicator of direct product, *Quart. J. Math. Oxford Ser. (2)* **22** (1971), 103–105.

[Wie4] J. Wiegold, Commutator subgroups of finite p-groups, *J. Aust. Math. Soc.* **10** (1969), 480–484.

[Wiel1] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

[Wiel2] H. Wielandt, Über Produkte von nilpotenten Gruppen, *Illinois J. Math.* **2** (1958), 611–618.

[Wiel3] H. Wielandt, Sylowgruppen and Kompositionsstruktur, *Abh. Math. Semin. Univ. Hambg.* **22** (1958), 215–228.

[Wild] M. Wild, The groups of order sixteen made easy, *Amer. Math. Monthly* **112** (2005), 20–30.

[Wil1] B. Wilkens, On quaternion-free 2-groups, *J. Algebra* **258** (2002), 477–492.

[Wil2] B. Wilkens, On the upper exponent of a finite p-group, *J. Algebra* **277** (2004), 249–263.

[Wil3] B. Wilkens, 2-groups of breadth 3, *J. Algebra* **318** (2007), 202–224.

[Wil4] B. Wilkens, A note on 2-automorphic 2-groups, *J. Algebra* **184** (1996), no. 1, 199–206.

[Wil5] B. Wilkens, Finite p-groups not characteristic in any p-group in which they are properly contained, *Israel J. Math.* **166** (2008), 97–112.

[Wil6] B. Wilkens, p-groups without noncharacteristic normal subgroups, *Israel J. Math.* **172**, 357–369.

[Wilk] D. F. Wilkinson, The groups of order p^7 (p any prime), *J. Algebra* **118** (1988), 109–119.

[Wils] L. Wilson, On the power structure of powerful p-groups, *J. Group Theory* **5** (2002), no. 2. 129–144.

[Wim1] A. Wiman, Über p-Gruppen von maximaler Klasse, *Acta Math.* **88** (1952), 417–446.

[Wim2] A. Wiman, Über mit Diedergruppen verwandte p-Gruppen, *Ark. Mat. Astr. Fys.* **33A** (1946), no. 6, 1–12.

[Wol] B. Wolf, A note on p'-automorphisms of p-groups P of maximal class centralizing the center of P, *J. Algebra* **190** (1997), no. 1, 163–171.

[Won] W. J. Wong, Bilinear and quadratic maps, and some p-groups of class 2, *J. Algebra* **163** (1994), no. 2, 516–537.

[Wri] D. Wright, Degree of minimal permutation representation of covering groups of abelian groups, *Amer. J. Math.* **96** (1974), 578–592.

X

[Xia] C. Xiao, A conjecture on the automorphism group of a finite p-group, *Rend. Circ. Mat. Palermo (2)* **23** (1990), 347–351.

[Xu1] M. Y. Xu, The power structure of finite p-groups, *Bull. Aust. Math. Soc.* **36** (1987), no. 1, 1–10.

[Xu2] M. Y. Xu, P. Hall's basis theorem for regular p-groups and its application to some classification problems, *Comm. Algebra* **19** (1991), no. 4, 1271–1280.

[Xu3] M. Y. Xu, A theorem on metabelian p-groups and some consequences, *Chin. Ann. Math. Ser. B* **5** (1984), 1–6.

[Xu4] M. Y. Xu, Regular p-groups and their generalizations, manuscript.

[XZA] M. Y. Xu, Q. Zhang and L.-J. An, Finite p-groups all of whose nonabelian subgroups are generated by two elements, *J. Algebra* **319** (2008), no. 9, 3603–3620.

Y

[Yad1] M. K. Yadav, On automorphisms of some finite p-groups, *Proc. Indian Acad. Sci. Math. Sci.* **118** (2008), 1–11.

[Yad2] M. K. Yadav, Class preserving automorphisms of finite p-groups, *J. Lond. Math. Soc. (2)* **75** (2007), 755–772.

[Yor] I. O. York, The exponent of certain finite p-groups, *Proc. Edinb. Math. Soc. (2)* **33** (1990), 483–490.

Z

[Zap] G. Zappa, Finite groups in which all nonnormal subgroups have the same order II, *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **14** (2003), no. 1, 13–21 (Italian).

[Zas] H. Zassenhaus, *The Theory of Groups*, Chelsea, New York, 1958.

[Zen1] V. I. Zenkov, Intersections of abelian subgroups in finite groups, *Math. Notes* **56** (1994), 869–871.

[Zen2] V. I. Zenkov, A uniqueness theorem and intersections of nilpotent subgroups in finite groups, *Mat. Sb.* **184** (1993), 151–159.

[Zha] J. P. Zhang, Finite groups with many conjugate elements, *J. Algebra* **170** (1994), 608–624.

[ZAX1] Q. H. Zhang, L.-J. An and M. Y. Xu, Finite p-groups all of whose non-abelian proper subgroups are metacyclic, *Arch. Math.* **87** (2006), 1–5.

[ZAX2] Q. H. Zhang, L.-J. An and M. Y. Xu, Finite p-groups all of whose subgroups of index p^2 are abelian, *Algebra Colloq.* **15** (2008), no. 1, 167–180.

[ZG] Q. H. Zhang and J. Gao, Normalizers of nonnormal subgroups of finite p-groups, manuscript.

[ZL] J. Q. Zhang and X. H. Li, Finite p-groups all of whose proper subgroups have small derived subgroups, *Sci. China Ser. A* **53** (2010), no. 5 1357–1362.

[ZP] Q. H. Zhang and H. P. Peng, On Hua-Tuan's conjecture, *Sci. China Ser. A* **52** (2009), no. 2, 389–393.

[ZSQX] Q. H. Zhang, C. J. Sun, H. P. Qu and M. Y. Xu, Finite two-generator equilibrated p-groups, *Sci. China Ser. A* **50** (2007), 8114–820.

[Zhm1] E. M. Zhmud, Finite groups with uniquely generated normal subgroups, *Mat. Sb.* **72** (1967), 135–147 (Russian).

[Zhm2] E. M. Zhmud, On the multiplier of a finite group with nontrivial center, *Ukrainian Math. J.* **47** (1995), 546–550 (Russian).

[Zhm3] E. M. Zhmud, Symplectic geometries and projective representations of finite abelian groups, *Mat. Sb.* **87** (1972) 3–17 (Russian).

[Zhm4] E. M. Zhmud, Symplectic geometries over finite abelian groups, *Mat. Sb.* **86** (1971), 9–33 (Russian).

[Zhm5] E. M. Zhmud, The isomorphisms of the lattice of normal subgroups of a finite nilpotent group, *Vestnik Kharkov Univ.* **26** (1967), 3–17 (Russian).

[Zho] X. Zhou, On the order of Schur multipliers of finite p-groups, *Comm. Algebra* **22** (1994), 1–8.

Author index

A
Alperin J. L., §103, Appendices 29, 32

B
Baer R., §§140, 143, Appendix 29
Berkovich Y., §§96, 97, 106–108, 110–112, 116, 119, 124, 134–136, 137, 138, 143, Appendices 27–29, 31, 32, 39, 40, 43
Blackburn N., §§97, 101, 110, 114, 119, 131, 132, 134, Appendix 38
Bohanon J., §122, Appendix 40, Research problems and themes

C
Caranti A., Appendix 42
Carter R., Appendix 28
Cartwright M., §133
Cepulic V., §137
Chunikhin S. A., Appendix 28
Crestani E., §113

D
Dapeng Yu., §144
Deaconescu M., §110
Dempwolff U., Appendix 29

E
Eckman B., Appendix 36

F
Fomin A. N., Appendix 28
Freiman G., Appendix 44
Frobenius G., Appendices 39, 43

G
Gao J., §138
Glauberman G., §§127, 134, Appendices 31, 40
Golfand Y. A., Appendix 40
Gorenstein D., Appendix 40, Research problems and themes

H
Hall M., Appendix 43
Hall P., Appendices 28, 43
Harada K., §99
Herstein I., Appendix 30
Herzog M., Appendices 29, 37
Hethelyi L., §§130, 131, Appendix 40
Higman G., Appendix 35
Hurwitz A., Appendix 36

I
Isaacs I. M., §§104, 105, 123, Appendices 29, 34, Research problems and themes
Ito N., Appendices 33, 39, Research problems and themes

J
Janko Z., §§93–95, 98–102, 106, 107, 113, 115, 117, 118, 120–123, 125, 127, 129, 131–133, 137, 138, 139–142, 144, Appendices 28, 39, 40, 41, Research problems and themes
Jonah D., §103

K
Kaplan G., Appendix 29
Kazarin L., §105
Kegel O., Appendices 28, 39
Knoche H. G., §121
Konvisser M., §103
Kostrikin A., Research problems and themes

L
Leedham-Green C. R., §133
Li Tianze, §126
Li X. H., §137
Leone A., §139
Longobardi P., Appendix 37
Luccini A., Appendix 29
Lv Heng, §144
Lyons R., Appendices 29, 40

M
Macdonald I., Appendices 38, 40
Maj M., Appendix 37
Mann A., §§110, 123, 124, Appendices 35, 37, 40, Research problems and themes
Mazza N., §§127, 134, Appendix 40, Research problems and themes
Meierfrankenfeld U., §109
Miller G. A., Research problems and themes

N
Neumann P. M., §133
Newman M. F., Appendix 35

O
Ore O., Appendix 28

P
Parmeggiani G., §121
Passman D., §112, Appendix 34
Pennington E., Appendix 29
Piljavska O. C., §137

Q
Qian G. H., Appendix 40

R
Redei L., §§93–95, 100–102, 118, 134, 135.
Roitman M., Appendix 44

S
Sambale B., §126, Appendix 40
Schenkman E., §§140, 143
Schmidt O., §§96, 112
Seeley C., Appendix 35
Shareshian J., §122
Shult E., Appendix 30
Shumyatsky P., Appendix 31
Silberberg G., §110
Sims C., Appendix 35
Solomon R., Appendix 40
Stellmacher B., §§109, 121
Suzuki M., §105, Appendix 29
Sylow L., Appendix 28

T
Tang F., Appendix 40
Thompson J., §104, Appendix 30

W
Wiegold J., §133
Wielandt H., Appendices 28, 39, 40
Wilkens B., Research problems and themes
Wong S. K., Appendix 29

Y
Yu Dapeng, §144

Z
Zappa G., §112
Zelmanov E., Research problems and themes
Zenkov V., Appendix 29
Zhang J. Q., §137
Zhang Q. H., §138
Zhou Wei, §144
Zhmud E., Research problems and themes

Subject index

A

abelian subgroups, §§99, 100–103, 111, 116, Appendix 32
abelian subgroups of given exponent and small index, Appendix 32
all on minimal nonabelian p-groups, §118
all on p-groups of maximal class, §119
$A_p(s, \theta)$, the Suzuki p-group, §105
automorphisms, §§105, 140
automorphisms of order p of a metacyclic p-group, $p > 2$, without cyclic subgroup of index p, §109

B

Baer's characterization of $O_p(G)$, Appendix 28
Baer's theorem on 2-groups with nonabelian norm, §§140, 143
Baer–Suzuki theorem, Appendix 29
Berkovich's factorization theorem, Appendix 28
B-group, Appendix 39
$\mathcal{B}(G)$, Appendix 39
$BI(p^k)$-group, §144
$\mathcal{B}_p(G)$, Appendix 39
$\mathcal{B}_\varphi(G)$, Appendix 39
$\mathcal{B}_<(G)$, Appendix 39
Blackburn's counting theorems, §114
Blackburn's theorems, §§110, 114, 132, Appendix 38
Bozikov–Janko's theorem on 2-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian, §100
breadth of a p-group §121
Brodkey's theorem, §28

C

Carter subgroup, Appendix 28
Carter's theorem, additional property, Appendix 28
center, its index in a p-group of subgroup breadth 1, Bohanon's theorem, Janko's proof of, §122
central automorphism, §§105, 140
centralizers of elements in p-groups, Blackburn's theorems, §132
character degrees of p-groups associated with finite algebras, Isaacs' theorem, §104
characterization of metacyclic p-groups with abelian subgroup of index p, §124
characterization of the last member of the lower central series of a group, Appendix 39
characterization of simple groups, Appendix 28
characterizations of abelian groups, §111
characterizations of minimal nonabelian groups, §111
characterizations of p-groups of maximal class, §97, 136, Appendix 40
Chunikhin–Hall characterization of solvable groups, Appendix 28
$c_k(G)$, the number of cyclic subgroups of order p^k in a p-group G, §124
class and breadth of p-groups, theorems of Leedham-Green–Newman–Wiegold, §133
classification of p-groups possessing a maximal set of noncommuting elements of cardinality $p + 1$, §116
commutator subgroup of a p-group having subgroup breadth 1, §128

consequences of Frobenius' normal p-complement theorem, Appendix 39
counting theorems, §§103, 114, 124
covering of groups by proper subgroups, §116
cyclic subgroups, §§117, 124, 137–139
CZ-groups, §102

D
degrees of irreducible characters of p-groups associated with finite algebras, Isaacs' theorem, §104
Dempwolff–Wong's theorem, Isaacs' generalization of, Appendix 29
derived subgroup, §§128, 137, 139
Dirichlet's principle, Appendix 44
distinct Carter subgroups are not permutable, Appendix 28
doubling coefficient, Appendix 44

E
element breadth, §133
elementary abelian subgroups, §§127, 134
equilibrated p-groups, §110
equilibrated p-groups containing a proper subgroup of maximal class, §110
equilibrated p-groups of maximal class, §110
E_p-groups, §110
E_p-groups containing a proper nonabelian subgroup of order p^3 and exponent p, §110
E_p-groups containing a proper subgroup of maximal class and order p^4, $p > 2$, §110
E_3-groups containing a proper subgroup of maximal class and order $> 3^4$, §110
existence of L_p-subgroups, §97
existence of 2-groups $G_1 < G$ such that $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G)$, Sambale's example, §126
extraspecial p-groups, §115, Appendix 36

F
factorized groups, §110, Appendix 29
Freiman's theorem on a finite group subsets with small doubling, Appendix 44
Frobenius' normal p-complement theorem and its consequences, Appendix 39

G
$\gamma(G)$, maximal number of pairwise noncommuting elements in G, §116
generalized Dedekindian groups, Appendix 37
generalized soft subgroups, §134
Glauberman's theorem on nilpotent p'-subgroups of $\mathrm{GL}(n, p)$, Appendix 31
Glauberman–Mazza's theorem on p-groups, $p > 2$, with maximal elementary abelian subgroup of order p^2, additional properties of such groups, §134
groups all of whose nonabelian maximal subgroups are two-generator, §136
groups all of whose nonnormal subgroups have the same order, §112
groups containing a finite subset with small doubling coefficient, Freiman's theorem, Appendix 44
groups containing exactly one maximal subgroup which is neither abelian nor minimal nonabelian, §§100–102
groups covered by few proper subgroups, §116
groups G satisfying $\Phi(G)' = G'$, §111
groups G satisfying $\Phi(G)' = H'$ for all maximal $H < G$, §111
groups G satisfying $\Phi(G)' = H'$ for all nonabelian maximal $H < G$, §111
groups G with $\alpha_1(G) - \alpha_1(H) = p - 1$ for some nonabelian $H \in \Gamma_1$, Appendix 40

groups G with small $\gamma(G)$, §116
groups in which any two elements of distinct orders are permutable, Appendix 40
groups in which the number of solutions of $x^n = 1$ equals n, two alternate proofs, §135
groups not generated by some minimal nonabelian subgroups, §135
groups of central automorphisms of Suzuki's p-groups, Appendix 105
groups of exponent p, Appendix 40
groups of exponent p all of whose nonabelian maximal subgroups are two-generator, §136
groups of exponent p all of whose nonabelian maximal subgroups have centers of order p, §136
groups of exponent p^e without minimal nonabelian subgroups of exponent p, §95
groups of Frattini class 2, G. Higman's theorems, Appendix 35
group subsets with small doubling, Appendix 44
groups with at most two conjugate classes of nonnormal subgroups, §96
groups with few classes of minimal nonabelian subgroups, §108
groups with few pairwise noncommuting elements, §116

H

Hadamard's 2-groups, Ito's theorems, Appendix 33
Hall's theorem on solvable groups, alternate proof of, Appendix 43
Hall–Chunikhin's characterization of solvable groups, Appendix 28
Harada's theorem on 2-groups with self-centralizing abelian subgroup of order 8, Janko's proof, §99
Hethelyi' theorems on soft subgroups, §130
H(G) or $Z_\infty(G)$, the hypercenter of G (= the last member of the upper central series of G), Appendix 39
hypercenter, Appendix 39
Hurwitz' theorem on composition of quadratic forms, Eckmann's proof, Appendix 36

I

infinitude of 2-groups of rank 3 all of whose maximal subgroups have rank 2, §113
irredundant coverings, §116
irredundant coverings by few subgroups, §116
irredundant coverings of p-groups by $p + 2$ subgroups, §116
irredundant coverings of p-groups by k subgroups, $k < p + 2 \leq 2p$, §116
irredundant coverings of p-groups of maximal class with abelian subgroup of index p by abelian subgroups, §116
Isaacs example, §105
Isaacs–Passman's theorem of p-groups G all of whose nonlinear irreducible characters have degree p, Appendix 34
Isaacs' theorem on exponent of abelian point stabilizer in transitive group, Appendix 29
Ito's theorems on Hadamard 2-groups, Appendix 33

J

Janko's theorems, §§93–95, 98, 101, 102
Janko–Kegel's theorem on normal closure, Appendix 28
J-group, Appendix 37
Jonah–Konvisser's counting theorems, §103

K

Kegel's theorems, Appendices 28, 39
Kegel–Wielandt's theorem on products of nilpotent subgroups, Appendix 28

$K_\infty(G)$ (last member of the lower central series of G), Appendix 30

L

large cyclic subgroups, Appendix 29
last member of the lower central series of a nonnilpotent group and its generation, Appendix 39
lattice isomorphism of p-groups of maximal class, Caranti's theorem, Appendix 42
$\leq$-dispersive groups, Appendix 39
lemmas of Ore, Appendix 28
Leone's theorem on p-groups all of whose subgroups have cyclic derived subgroups, §139

M

Macdonald's p-groups, Appendix 40
Macdonald's theorems, Appendices 38, 40
Mann's theorem on the number of subgroups of given order in a metacyclic p-group, $p > 2$, §124
$\mathcal{MA}_k(G)$, the set of minimal nonabelian subgroups of exponent $\leq p^k$, is a p-group, §135
maximal chain, Appendix 40
maximal set of noncommuting elements, §116
maximal subgroups, §100–102, 106, 107, 109–111, 113, 115, 116, 119, 125, 129, 135–139, Appendices 27, 38, 40
maximal subgroups of two-generator 2-groups, §106
metacyclic equilibrated p-groups, their class, §110
metacyclic minimal nonabelian subgroups of exponent 4, §93
metacyclic p-group, number of subgroups of given order of, §124
metacyclic p-group, number of cyclic subgroups of given order of, §124
metacyclic p-groups with nonabelian section of order p^4 and exponent p^2, §124
metacyclic p-groups without minimal nonabelian subgroups that have no cyclic subgroups of index p, §124
metacyclic subgroups of index p in a p-group, §§106, 107, 109
metacyclic 2-groups with a nonabelian section of order 8, §124
minimal nonabelian equilibrated p-groups, §110
minimal nonabelian subgroups, §§93–95, 100–102, 108, 111, 116, 118, 132, 134–138, Appendix 41
minimal nonabelian subgroups of metacyclic p-groups, §124
minimal nonnilpotent subgroups, §116, Appendix 39

N

$\mathcal{N}(G)$, the norm of a group G, §§140, 143
nilpotence class of 2-groups all of whose subgroups are two-generator, §113
nilpotent p'-subgroups of class 2 in $\mathrm{GL}(n, p)$, Appendix 31
nonabelian p-groups $G = \Omega_1(G)$, $p > 2$, that are not generated by nonabelian subgroups of order p^3 and exponent p, §135
nonabelian p-groups $G = \Omega_k(G)$, $k > 1$, that are not generated by minimal nonabelian subgroups of exponent $\leq p^k$, §135
nonabelian 2-groups G all of whose minimal nonabelian subgroups are isomorphic to M_{2^n}, n fixed, §98
nonabelian 2-groups G all of whose minimal nonabelian subgroups have cyclic centralizers, Appendix 41
nonabelian 2-groups G all of whose minimal nonabelian subgroups have exponent $< \exp(G)$, §95
nonabelian 2-groups $G = \Omega_1(G)$ are generated by dihedral subgroups of order 8, §135

non-Dedekindian p-groups all of whose nonnormal subgroups have the same order, §112
nonmetacyclic minimal nonabelian subgroups of exponent 4, §94
nonnilpotent groups covered by few proper subgroups, §116
nonnormal cyclic subgroups of minimal order, §138
norm of a group, §140
normal closure, §138, Appendices 28, 39
normalizer, §§121, 128, 138
$\nu(G)$, §138
number of generators of maximal subgroups of two-generator 2-groups, §129
number of involutions in 2-groups, §114
number of subgroups of given order in a metacyclic p-group, Mann's theorem, §124
number of subgroups of given order in a metacyclic 2-group, Berkovich's theorems, §124
number of solutions of $x^p = 1$ in a p-group G, §101
number of two-generator maximal subgroups in a two-generator 2-group, §106

O

order of the central automorphism group of the Suzuki p-group, §105
Ore's lemmas, Appendix 28
Ore's theorem on maximal subgroups of solvable groups with equal cores, Appendix 28

P

p-closed groups, Appendices 29, 39
Pennington's theorem, Isaacs' proof of, Appendix 29
permutable subgroups, Appendix 39
p-groups all of whose maximal abelian subgroups containing a nonnormal cyclic subgroup of minimal order, say, p^ν have order p^ν or $p^{\nu+1}$, §138
p-groups all of whose maximal subgroups except one are extraspecial, §115
p-groups all of whose maximal subgroups, except a few, are CZ-groups, §115
p-groups all of whose maximal subgroups have derived subgroups of orders $\leq p$, §137
p-groups all of whose minimal nonabelian subgroups have cyclic centralizers, Appendix 41
p-groups all of whose nonabelian maximal subgroups are either metacyclic or minimal nonabelian, §142
p-groups all of whose nonnormal cyclic subgroups of minimal order have index p in their normalizers, §138
p-groups all of whose nonnormal subgroups are cyclic, Appendix 40
p-groups all of whose nonnormal subgroups have the same order, §112
p-groups all of of whose proper subgroups have cyclic derived subgroups, §139
p-groups all of whose proper subgroups have derived subgroups of order $\leq p$, §137
p-groups all of whose proper subgroups have subgroup breadth 1, §128
p-groups containing a maximal subset of pairwise noncommuting elements of cardinality $p + 1$, §116
p-groups G containing a maximal subgroup H all of whose subgroups are G-invariant, §125
p-groups G satisfying $\mathrm{C}_G(x) \leq \mathrm{N}_G(H)$ for all abelian $H < G$ and $x \in H^\#$, Appendix 40
p-groups G with $\gamma(G) = p + 1$, §116
p-groups G with $\gamma(G) = p + 2$, §116

p-groups G with $\gamma(G) \leq 2p$, §116
p-groups G with $p > 2$ and $\mathrm{d}(G) = 2$ having exactly one maximal subgroup which is neither abelian nor minimal nonabelian, §102
p-groups having exactly one maximal subgroup with cyclic center, §141
p-groups in which normalizers of all subgroups have index $\leq p$ (= groups of subgroup breadth 1), §122
p-groups in which some subgroups are generated by elements of order p, §97
p-groups of element breadth 2, Janko's proof of the Parmeggiani–Stellmacher theorem, §121
p-groups of Frattini class 2, §35
p-groups of maximal class, §§109, 110, Appendix 40
p-groups of subgroup breadth 1, §128
p-groups, $p > 2$, with exactly one maximal subgroup which is neither abelian nor minimal nonabelian, §§101, 102
p-groups some of whose subgroups are generated by elements of order p, §97
p-groups that are not generated by minimal nonabelian subgroups of given exponent, §135
p-groups with a maximal subset of pairwise noncommuting elements of cardinality $p + 1$, §116
p-groups with a 2-uniserial subgroup of order p, §131
p-groups with at most two conjugacy classes of nonnormal subgroups, §96
p-groups with bounded index of cyclic subgroups in their normal closures, §144
p-groups with cyclic subgroup of index p^3, power structure of, Appendix 40
p-groups with exactly one maximal subgroup which is neither abelian or minimal nonabelian, §§100–102
p-groups with few conjugate classes of minimal nonabelian subgroups, §108
p-groups with maximal elementary abelian subgroup of order p^2, its centralizer, properties of these groups, §134
p-groups with large normalizers, §122
p-groups with maximal metacyclic subgroup without cyclic subgroup of index p, their automorphisms of order p, §109
p-groups with small normalizers of nonnormal subgroups (cyclic subgroups), §138
p-groups with small number of solutions of $x^{p^k} = 1$, Appendix 44
p-groups with some subgroups generated by elements of order p, §97
p-groups with strong normalizer conditions for nonnormal cyclic subgroups of minimal order, §138
p-groups with 2-uniserial subgroup of order p, §131
p-groups with uniserial subgroup of order p, Appendix 40
p-groups with uniserial subgroup of order p^2, Appendix 40
p-groups with $|\mathrm{Z}_n(G)| = p^n$, Appendix 40
p-groups without $p + 2$ pairwise noncommuting elements, §116
p-groups without subgroup of order p^{p+1} and exponent p, Appendix 40
p-nilpotent groups, Appendix 39
ϕ-dispersive groups, Appendix 39
power automorphism, §140

Q

quasi-regular metacyclic p-groups, §124

R

ranks of maximal subgroups of two-generator 2-groups, §107
review of characterizations by minimal nonabelian subgroups, §118
review of characterizations of p-groups of maximal class, §119
$R(G)$, §124

S

S_1-groups, §138
Schenkman's theorem about the norm, §140
Shult's theorem, Appendix 30
$s_k(G)$, the number of subgroups of order p^k in a p-group G, §124
soft subgroups of p-groups, properties of, Hethelyi's theorems, §§130, 134, Appendix 40
solvable groups, theorems of Carter, Chunikhin–Hall, Hall, Appendix 43
solvable groups with exactly n solutions of the equation $x^n = 1$, two alternate proofs of, Appendix 43
special p-groups, §§105, 112
square of the set, Appendix 44
structure of the groups C_{2^n} wr C_2 and M wr C_2, Appendix 27
subgroup breadth, §§121, 128
subgroups of exponent p, Appendix 40
subgroups of finite groups generated by all elements in two shortest conjugacy classes, §123
subsets with small doubling, Appendix 44
supersolvable group, Appendix 39
supersolvably immersed subgroup, Appendix 39
Sylow's theorem, alternate group of, Appendix 28

T

theorem of Baer on 2-groups with nonabelian norm, §143
theorem of Baer–Suzuki, Appendix 29
theorems of Blackburn and Macdonald, §38
theorem of Dempwolff–Wong, Appendix 29
theorem of Glauberman, Shumyatsky's proof, Appendix 31
theorem of Herstein, Appendix 30
theorems of Isaacs, Appendix 29
theorems of Jonah and Konvisser, §103
theorem of Pennington, Isaacs' proof, Appendix 29
theorem of Schult, Appendix 30
theorem of Zenkov, Isaacs' proof of, Appendix 29
theorem on groups in which the number of solutions of $x^n = 1$ is equal to n, two new proofs of, §43
theorems and lemmas of Sylow, Ore, Hall on solvable groups, Carter, Gaschütz and so on, Appendix 28
theorems of Herzog, Kaplan and Luccini on groups with large cyclic subgroup, Appendix theorems of Isaacs, Appendix 29
theorems of Wielandt–Kegel on solvability of groups $G = AB$, where A and B are nilpotent, Appendix 28
Thompson's lemmas, Appendix 30
two-generator equilibrated p-groups, $p > 2$, §116
two-generator nonmetacyclic $\mathcal{A}_2$-group, §106
two-generator p-groups, §§106, 107, 110, 129
two-generator 2-groups all of whose nonabelian maximal subgroups are two-generator, §106
two-generator 2-groups containing exactly one maximal subgroup which is not two-generator, §129
two-generator WE_p-groups, $p > 2$, §110
2-groups all of whose minimal nonabelian subgroups are isomorphic to $M_{2^{n+1}}$ for a fixed n, §98

2-groups all of whose minimal nonabelian subgroups are metacyclic of exponent 4, §93
2-groups all of whose minimal nonabelian subgroups are nonmetacyclic and have exponent 4, §94
2-groups all of whose nonnormal subgroups are either cyclic or generalized quaternion, Appendix 40
2-groups all of whose nonnormal subgroups are either cyclic or of maximal class, §117
2-groups containing a maximal elementary abelian subgroup of order 4, §127
2-groups G all of whose minimal nonabelian subgroups have exponent $< \exp(G)$, §95
2-groups in which any two distinct minimal nonabelian subgroups have cyclic intersection, §120
2-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian, §100
2-groups with maximal elementary abelian subgroup of order 4, §127
2-groups with sectional rank ≤ 4, §99
two-uniserial subgroup of order p, §131

W

WE_p-groups, examples of WE_p-groups, §110
Wielandt's lemmas on factorizable groups, Appendix 28
Wielandt's theorem on groups with cyclic Sylow p-subgroup, Appendix 28
Wielandt's theorems on normal closures, Appendix 39
Wielandt–Kegel's factorization theorem, Appendix 28
wreathed 2-groups, description of elements and maximal subgroups, Appendix 27

Z

Zenkov's theorem on intersection, Isaacs' proof of, Appendix 29
$\mathrm{Z}_\infty(G)$ or $\mathrm{H}(G)$ (= hypercenter of G), Appendix 39