Lecture Notes in Pure and Applied Mathematics

Factoring Groups into Subsets

Volume 256

Sándor Szabó

Arthur D. Sands

CRC Press
Taylor & Francis Group

A CHAPMAN & HALL BOOK

Factoring Groups into Subsets

Sándor Szabó
University of Pecs
Pecs, Hungary

Arthur D. Sands
University of Dundee
Dundee, United Kingdom

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group an **informa** business

A CHAPMAN & HALL BOOK

Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Chapman & Hall/CRC is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-9046-8 (Softcover)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

© 2009 by Taylor & Francis Group, LLC

Contents

Symbol Descriptions

Z	The ring of integers.
$Z(n)$	The additive subgroup of the residue classes modulo n.
$Z(p^\infty)$	The Prüfer group, where p is a prime.
$\|G\|$	The order of the group G.
$(G)_p$	The p-component of the group G, where p is a prime.
$\|g\|$	The order of the element g in a group.
$(g)_H$	The H-component of g, where H is a subgroup.
$(g)_p$	The p-component of g, where p is a prime.
$\mathrm{GF}(q)$	The Galois field of order q.
$\langle A\rangle$	The span of the set A in a group.
$\|A\|$	The number of elements of the subset A.
$\mathrm{Ann}(A)$	The annihilator of the subset A.
$(A)_H$	The H-component of the subset A.
$(A)_p$	The p-component of the subset A, where p is a prime.
χ	Character of a finite abelian group.
$\mathrm{Ker}\chi$	The kernel of the character χ.
$F_n(x)$	The nth cyclotomic polynomial.
$\deg F$	The degree of the polynomial F.
$R_m(r)$	A Ramsey number.
$d(u,v)$	The Hamming distance of u and v.
$S_e(u)$	An error sphere of radius e centered at u.
$\nu(n)$	The number of the prime factors of n.
$[g,n]$	Bracket notation for a cyclic subset.
$\chi(\Gamma)$	The chromatic number of the graph Γ.
$\omega(\Gamma)$	The clique number of the graph Γ.
$A+B$	The sum of the subsets A and B.
$A\circ_\varphi B$	The composition of the subsets A and B.

List of Tables

List of Figures

Preface

The factorization theory of abelian groups deals with decomposing an abelian group into a direct sum of its subsets. The nature of these problems are partly algebraic and partly combinatorial. The results have applications in various fields: geometry of tilings, variable length codes, integer codes, error correcting codes, cryptography, graph theory, number theory, Fourier analysis, complex Hadamard matrices, just to mention a few.

This book is about the factorization theory of abelian groups focusing mainly on cyclic groups. The book [157] treats selected topics of the factorization theory with an intention to possibly touch all the main areas. Inevitably overlaps are bound to occur.

The direct sum of isomorphic copies of a cyclic group of prime order, that is, an elementary p-group, behaves in many respects as a finite linear space and must be treated differently than a cyclic group. Some of the results of the factorization theory become trivial when restricted to cyclic groups. On these occasions the exiting part of the problem lies in the non-cyclic case, while at other times the substantial part of the result is in the cyclic case. It is an empirical fact that factoring cyclic groups is still a rich field. For instance, [85] claims that each cryptosystem in use is based on factoring a large cyclic group. Many of the results and applications are available with the mastery of simpler techniques than those required by the general non-cyclic case.

With merciless editing (not including many topics that happened to be our personal favorite) we kept the material to a manageable size. Our hope is that this book will serve as a gentle introduction for practitioners of other fields interested in the applications of the factorization theory of abelian groups.

Chapter 1

Introduction

There are many problems with a combinatorial flavour related to finite abelian groups. The first such result is most likely due to A. L. Cauchy [16] from 1813 and rediscovered by H. Davenport [25] in 1935. Let p be a prime number and let $Z(p)$ be the additive group of residue classes modulo p. For two subsets A, B of $Z(p)$ we define $A+B$ to be $\{a+b : a \in A, b \in B\}$ and we use $|A|$ to denote the number of elements of A. The Cauchy-Davenport theorem now reads as follows.

If A, B are not empty subsets of $Z(p)$, then

$$|A+B| \geq |A| + |B| - 1,$$

provided $p \geq |A| + |B| - 1$.

This result has since been extended and generalized in a number of ways. (See the monograph [91].)

Let A be a set of $Z(n)$ with $|A| = s$. The difference set

$$D = A - A = \{a - a' : a, a' \in Z(n)\}$$

is clearly symmetric in the sense that $d \in D$ implies $-d \in D$. There are at most $s(s-1)/2$ distinct non-zero elements in D. The situation when each non-zero element of $Z(n)$ can be represented uniquely in the way

$$d = a - a', \quad a, a' \in A$$

is particularly interesting. In this case one can use the elements of $Z(n)$ as points of a finite projective plane. The subsets $A+b$, $b \in Z(n)$ will form the straight lines of the plane. In his book [62] F. Kárteszi considered a regular polygon of n sides and coordinatized the vertices by the elements $0, 1, \ldots, n-1$ of $Z(n)$ walking around the polygon, say clockwise. (See also the text [66].) Considering the distances between the vertex 0 and the other vertices $1, \ldots, n-1$ makes clear that the number of non-zero distinct distances occurring between the vertices of the polygon is $(n-1)/2$ when n is odd. Therefore

$$\frac{s(s-1)}{2} \leq \frac{n-1}{2}.$$

We are looking for the cases when equation holds, that is, when $n = s(s-1)+1$. Table 1.1 (on page 2) lists some values of n and s together with a suitable choice of A where the bound is tight.

TABLE 1.1: Some difference sets

s	n	A
3	7	$\{0, 1, 3\}$
4	13	$\{0, 1, 4, 6\}$
5	21	$\{0, 1, 4, 14, 16\}$
6	31	$\{0, 1, 3, 8, 12, 18\}$
7	43	Does not exist.
8	57	$\{0, 1, 3, 13, 32, 36, 43, 52\}$
9	73	$\{0, 1, 3, 7, 15, 31, 36, 54, 63\}$
10	91	$\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\}$

The points coordinatized by the elements of A determine $s(s-1)/2$ distinct non-zero distances. This provides a visualization of the construction. Figure 1.1 (on page 3) illustrates the $n = 21$ special case. Rotating the marked 5-gon one gets 21 subsets of the set $\{0, 1, \ldots, 20\}$, and they form the straight lines of a finite projective plane. The lines are listed in Table 1.2 (on page 4).

Let G be a finite abelian group and let $f : G \to G$ be a one-to-one map. We say that f is a complete map of G if $h : G \to G$, defined by $h(a) = a + f(a)$, is also one-to-one. In 1947 L. J. Paige [103] showed that G has a complete map if and only if G does not have exactly one element of order two. We mention two applications of Paige's theorem. Suppose $a_1, \ldots, a_n$ are the elements of G. The addition or Cayley table of G is an n by n table. The jth entry in the ith row is $a_i + a_j$. Clearly this table is a Latin square. If $f : G \to G$ is a one-to-one map, then the cells with coordinates $[a_i, f(a_i)]$ form a transversal of this Latin square. When all entries in a transversal are distinct the transversal is called a Latin transversal. By Paige's result, the Cayley table of a finite abelian group G admits a Latin transversal if and only if G does not have exactly one element of order two.

Paige's theorem can also be used to prove the following geometric result. A closed polygon that passes through each vertex of a regular polygon of even order consisting of edges and diagonals of the regular polygon always has a pair of parallel segments. A closed polygon in the $n = 8$ case is depicted in Figure 1.2 (on page 3).

To see why let us consider a regular polygon with n vertices, where n is an even number. Coordinatize the vertices with the elements $0, 1, \ldots, n-1$ of $Z(n)$ walking around the regular polygon, say clockwise. Let $f : Z(n) \to Z(n)$ be a one-to-one map. Obviously the elements $f(a)$, $a \in Z(n)$ form a permutation of the elements of $Z(n)$. Suppose that the permutation consists of one single cycle. Then the directed straight line sections $[a, f(a)]$, $a \in Z(n)$ form a closed polygon that passes through each vertex of the regular polygon exactly once. As $Z(n)$ has exactly one element of order two by Paige's theorem, f cannot be a complete map of $Z(n)$. Therefore there are $u, v \in Z(n)$ such that $u + f(u) = v + f(v)$. This gives that the directed edges $[u, f(u)]$ and $[v, f(v)]$ are parallel.

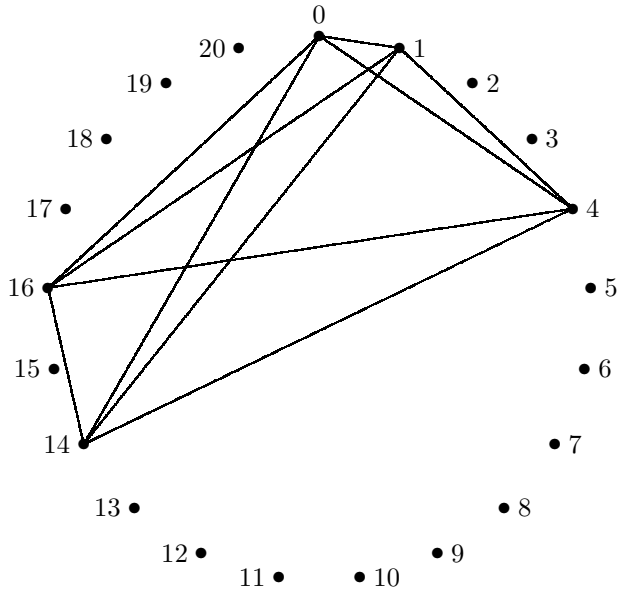

FIGURE 1.1: The vertices of the marked polygon form a difference system in $Z(21)$.

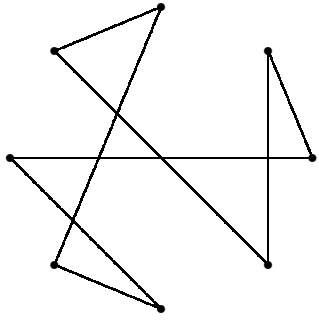

FIGURE 1.2: A closed polygon in the $n = 8$ case with two parallel edges.

TABLE 1.2: The lines of a finite projective plane

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	•	•			•										•		•				
1		•	•			•										•		•			
2			•	•			•										•		•		
3				•	•			•										•		•	
4					•	•			•										•		•
5	•					•	•			•										•	
6		•					•	•			•										•
7	•		•					•	•			•									
8		•		•					•	•			•								
9			•		•					•	•			•							
10				•		•					•	•			•						
11					•		•					•	•			•					
12						•		•					•	•			•				
13							•		•					•	•						
14								•		•					•	•					
15									•		•					•	•				
16										•		•					•	•			•
17	•										•		•					•			
18		•										•		•					•	•	
19			•										•		•					•	•
20	•			•										•		•					•

Another result about regular polygons can be proved with the aid of the above group theoretic argument. We consider n points on a circle that form the vertices of a regular polygon. All the lines passing through two points and all the lines passing through one point but tangent to the circle form the so-called line set of the regular polygon. A permutation of the vertices induces a permutation of the line set. F. Kárteszi [63] showed that if $n \geq 3$ and one permutes the vertices of an n sided regular polygon, then there are two parallel lines in the line set such that they go into parallel lines under the permutation.

Let G be a finite abelian group and let $B, A_1, \ldots, A_n$ be nonempty subsets of G. If for each b in B there are unique elements $a_1, \ldots, a_n$ of G such that

$$b = a_1 + \cdots + a_n, \quad a_1 \in A_1, \ldots, a_n \in A_n,$$

then we say that $B = A_1 + \cdots + A_n$ is a factorization of B. We are accustomed to the situation where $B = G$ and the subsets $A_1, \ldots, A_n$ are cyclic subgroups of G.

In 1938 G. Hajós [47] reformulated a famous unsolved geometry problem of H. Minkowski [88] into a problem of factoring a finite abelian group into certain subsets. Three years later, in 1941, Hajós [48] solved Minkowski's problem using its group theoretical equivalent. With this overture, factoring a finite abelian group into not necessary subgroup factors has entered into the scene.

A nonempty subset A of an abelian group G is defined to be periodic if there is an element g of G such that $A + g = A$ and $g \neq 0$. Periodicity of a subset A is a weakening of A being a subgroup of G. We say that an abelian group G has the Hajós property if in each factorization $G = A + B$ at least one of the factors A and B is periodic. In 1949 G. Hajós [49] called for classifying the finite abelian groups having the above property.

For 1962 the program has been completed and the complete list of finite abelian groups possessing the Hajós property first appeared in [117]. Groups with the Hajós property since then have found several applications. They are used in estimating the Ramsey number of graphs, in Fourier analysis, and in constructing variable length codes.

For a subset A of an abelian group G, the notation $\langle A \rangle$ stands for the smallest subgroup of G that contains A. A subset A of G is called normalized if $0 \in A$. A factorization $G = A_1 + \cdots + A_n$ is termed normalized if each A_i is normalized. We say that a finite abelian group G has the Rédei property if in each normalized factorization $G = A + B$ either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. Let p be a prime. In 1970 L. Rédei [108] asked, if G is of type $Z(p) \oplus Z(p) \oplus Z(p)$ and $G = A + B$ is a normalized factorization of G, then either A or B does not span the whole G. He conjectured that the answer is "yes." In our terminology he conjectured that groups of type $Z(p) \oplus Z(p) \oplus Z(p)$ have the Rédei property. S. Szabó and C. Ward [164] verified Rédei's conjecture for $p \leq 11$.

In 1972 C. B. Swenson [167] raised the question of whether each finite cyclic group has the Rédei property. In 1979 A. D. Sands [125] showed that

groups of type $Z(p^\alpha q^\beta)$, where p, q are distinct primes, do have the Rédei property. At the same time, O. Fraser and B. Gordon [40] constructed a factoring $G = A + B$ such that both A and B span G. In their example G is of type $Z(5) \oplus \cdots \oplus Z(5)$ and $|A| = 5^2$, $|B| = 5^4$. In 1985 S. Szabó [152] constructed a similar factorization for cyclic groups, that is, a normalized factorization in which both factors span the whole group. The question, for which groups G of type $Z(2) \oplus \cdots \oplus Z(2)$ does G have the Rédei property comes from coding theory. It was proved by G. D. Cohen, S. Litsyn, A. Vardy and G. Zémor [19] in 1996 that if the rank of G is at most 7, then G has the Rédei property, and if the rank of G is at least 14, then G does not have the Rédei property. The Rédei property of finite cyclic groups also resurfaced in the works of R. Tijdeman [170] in connection with a problem in Fourier analysis and in the works of C. De Felice [35] studying variable length codes. It is interesting to witness that the Rédei property has occurred in such varied fields of mathematics.

In 1963 A. D. Sands [120] showed that if $G = A_1 + \cdots + A_n$ is a factorization of a finite cyclic group G and each $|A_i|$ is a prime power, then at least one of the factors is periodic. He asked, if $|A_1|$ is a product of two primes and $|A_2|, \ldots, |A_n|$ are primes, then does it follow that one of the factors is periodic? In 1995 K. Corrádi and S. Szabó [21] answered the question in the affirmative. In 2004 A. D. Sands [129] proved the following extension. If each $|A_i|$ is a product of two primes or a prime power, then one of the factors is periodic. Combining this result with constructions due to N. G. de Bruijn [10] provides a way to find the finite cyclic groups with the Hajós property. We can give a transparent proof for the most frequently used result of the factorization theory.

It is a well-known fact that each finite abelian group can be decomposed into a direct sum of cyclic subgroups. This result comes under the name of the fundamental theorem of finite abelian groups in standard group theory books. The point for us is that each finite abelian group admits factorizations in which each factor is a subgroup. Does such a factorization allow a certain amount of perturbation? For instance, we may choose an element h in a subgroup factor H and replace it by $h + d$ to get a perturbed factor A. The subset A differs from the subgroup H in at most one element. For lack of better terminology we call A a simulated subset. It turns out that if $G = A_1 + \cdots + A_n$ is a factorization of the finite abelian group G, where the factors are simulated subsets, then at least one of the factors must be a subgroup. In other words, at least one of the original subgroup factors must remain undisturbed. In Section 6.2 we present a result when a subgroup factor is modified in more than one element.

A subset A of a finite abelian group G is called a cyclic subset if it is in the form

$$A = \{0, a, 2a, \ldots, (r-1)a\},$$

where $a \in G$, r is an integer $r \geq 2$ and the order of a is greater than or equal

to r. G Hajós [48] proved that if a finite abelian group is factored into cyclic subsets, then at least one of the factors is a subgroup. This is the result that provided a solution for Minkowski's geometric problem to which we alluded some paragraphs earlier.

Given an abelian group and a subset A of G, if B is a subset of G for which $G = A + B$ is a factorization of G, then we call B a complementer factor to A. The problems of asking for the existence of a complementer factor, the construction of a complementer factor or finding all possible complementer factors to A are all referred to as the complementer factor problem. The complementer factor problem links the factorization theory of abelian groups to other fields of mathematics and opens up opportunities to employ computers to inspect or construct factorizations.

Let us consider an orthogonal coordinate system in the n-dimensional Euclidean space. Using hyper planes perpendicular to the coordinate axis one can divide the space into n-dimensional unit cubes. These n-dimensional unit cubes tile the n-dimensional space, and we will call this tiling the standard cube tiling. The centers of the cubes in the standard cube tiling form the set Z^n. Plainly Z^n is an abelian group with the operation of addition of vectors. A finite family of the standard cube tiling is called a cubical cluster. A cubical cluster can be given conveniently with a finite subset C of Z^n listing the centers of the cubes making up the cluster. If translated copies of a cubical cluster tile the n-dimensional space, then there is a set L of Z^n such that $Z^n = C + L$ is a factorization of Z^n. The set L, the translation vectors of the clusters, is a complementer factor to C. This observation provides a link between the vast field of tilings and the factorizations of abelian groups. For further details see the survey paper [141]. The case when the cubical cluster consists of 1-dimensional unit cubes, that is, when one tries to tile the number scale by a finite tile, plays an important role in number theory. We have more to say about this in Chapter 7.

The collection of all the $0, 1$ sequences of length n can be identified with the n-dimensional vector space $[\mathrm{GF}(2)]^n$ over the Galois field $\mathrm{GF}(2)$. Clearly the additive part of $[\mathrm{GF}(2)]^n$ is an abelian group. Let A be the Hamming sphere of radius r centered at the point $(0, \ldots, 0)$. If $[\mathrm{GF}(2)]^n = A + C$ is a factorization, then C is a binary r-error correcting perfect code of length n. The code C is simply a complementer factor to the error sphere A. This fact furnishes a connection between the theory of error correcting codes and the factorizations of abelian groups.

Let U be a universal set and let $F = \{S_1, \ldots, S_n\}$ be a family of subsets of U. We say that the sets $A_1, \ldots, A_m \in F$ form an exact cover of U if $A_1 \cup \cdots \cup A_n = U$ and $A_i \cap A_j = \emptyset$ for each i, j, $1 \leq i < j \leq m$. The problem of deciding if there is an exact cover in F is called the exact cover problem in the theory of computations. It is known that the exact cover problem as a decision problem is NP complete. The complementer factor problem can be reduced to the exact cover problem. Note that the fact that $G = A + B$ is a factorization of G is equivalent to the fact that the sets $A + b$, $b \in B$ form

an exact cover of G. In this particular instance of the exact cover problem each member of the family F has the same cardinality. We define a graph Γ. The nodes of Γ are the elements of F and two distinct sets S_i and S_j are connected with an edge if $S_i \cap S_j = \emptyset$. Now the elements of F that form an exact cover of U are all mutually connected, forming a so-called clique in Γ. Therefore the complementer factor problem can also be expressed in terms of finding cliques in a given graph. This connects the theory of computations and the theory of factorizations.

Let G be an abelian group finite or infinite. Let U, V be subsets of G such that the sum $U + V$ is direct, that is, from

$$u_1 + v_1 = u_2 + v_2, \quad u_1, u_2 \in U,\ v_1, v_2 \in V$$

it follows that $u_1 = u_2$, $v_1 = v_2$. The embedding problem asks for the existence of a subgroup H of G and subsets A, B of G for which $G/H = (A + H)/H + (B + H)/H$ is a factorization of the factor group G/H and $U \subseteq A$, $V \subseteq B$. Here

$$(A + H)/H = \{a + H :\ a \in A\},$$
$$(B + H)/H = \{b + H :\ b \in B\}.$$

When G is an infinite group, there may be infinitely many subgroups H of G, and it is not clear a priori that there is an algorithm to decide the existence of an embedding.

The embedding problem originates from the theory of variable length codes. In this setting the group G is Z, the group of integers under addition. U and V are finite sets of integers associated with a finite code C over a finite alphabet. The existence of an embedding is related to the existence of a finite maximal code containing C, the so-called finite closure of the code C. For more details consult with the standard text [4] or the survey paper [14]. In Section 10.1 we will employ factorizations to settle a 16-years-long undecided conjecture from coding theory.

A subset A of a finite abelian group G is termed a Z-subset of G if $kA \subseteq A$ for each integer k. A moment reflection reveals that a Z-subset is a union of cyclic subgroups of G. There are two good reasons to single out the family of Z-subsets and consider factorizations consisting of Z-subsets.

First, it is a basic observation that the sum $A + B$ is direct if

$$(A - A) \cap (B - B) = \{0\}.$$

When A and B are Z-subsets this reduces to checking if

$$(H + K) \cap (L + M) = \{0\}$$

holds for each cyclic subgroup H, K, L, M such that $H, K \subseteq A$, and $L, M \subseteq B$. As this is a less demanding task, one can construct examples of factorings of larger groups.

The second reason lies in the important result that in a factorization $G = A + B$ the factor A can be replaced by kA to get the factorization $G = kA + B$ whenever k is relatively prime to $|A|$. This means that B is not only a complementary factor to A but also is a complementary factor to kA. This further constrains B, which can be exploited in the course of an analysis. However, when A is a Z-subset, $kA = A$ for each integer k and so no extra information can be obtained from B. This indicates that Z-subsets should be treated on their own right.

The Z-subsets were introduced by C. Okuda [95]. He characterized all finite abelian groups that admit only periodic factorizations into two Z-subsets. Section 11.3 is devoted to factoring by Z-subsets. Here we will present Okuda's result in the particular case of cyclic groups since this book focuses mainly on factoring finite cyclic groups.

Let G be a finite abelian group and let A, B be subsets of G. If the sum $A + B$ is direct and $|A||B| = |G| - 1$, then we say that $A + B$ is a near factorization of G. Plainly there is an element $g \in G$ such that $G\backslash\{g\} = A+B$. In order to exclude uninteresting cases, it is customary to require that $|A| \geq 2$, $|B| \geq 2$. Near factorizations are in an intimate connection with perfect graphs and also with certain combinatorial designs.

We present now a factorization definition general enough to include the possibilities occurring in the various applications. We recall from the theory of combinatorial design that a subset D of a finite abelian group G is called a difference set if each $g \in G \setminus \{0\}$ can be represented in exactly k ways in the form

$$g = d - d', \quad d, d' \in A.$$

The numerical parameters of the difference set are $(|G|, |D|, k)$. Note that if D is a difference set of G, then the sum $D + (-D)$ represents each element of $G \setminus \{0\}$ in k ways and represents the zero element in $|D|$ ways. Let f be a function defined on G taking non-negative integer values. Let A, B be subsets of G. We say that the sum $A + B$ is a generalized factorization of G (with respect to the multiplicity function f) if each element $g \in G$ is represented in exactly $f(g)$ ways in the form

$$g = a + b, \quad a \in A, \quad b \in B.$$

If $f(g) = k$ for each $g \in G$, then the sum $A + B$ is a k-fold factorization of G. The $k = 1$ particular case is the most commonly encountered factorization. If

$$f(g) = \begin{cases} 0, & \text{if} \quad g = 0, \\ 1, & \text{if} \quad g \neq 0, \end{cases}$$

then the sum $A + B$ is a near factorization of $G \setminus \{0\}$. When we choose the subset B to be $-A$ and

$$f(g) = \begin{cases} |A|, & \text{if} \quad g = 0, \\ k, & \text{if} \quad g \neq 0, \end{cases}$$

then in the generalized factorization $A + B = A + (-A)$ the factor A is a difference set of G.

Chapter 2

New factorizations from old ones

2.1 Restriction

Let G be a finite abelian group and let A and B be subsets of G. The sum $A+B$ of the subsets A and B is defined to be the set of elements

$$a+b, \quad a \in A,\ b \in B.$$

If the elements on the list $a+b$, $a \in A$, $b \in B$ are distinct, then we say that the sum $A+B$ is *direct*.

LEMMA 2.1
Let G be a finite abelian group and let A, B be non-empty subsets of G. Then the following statements are equivalent to the fact that the sum $A+B$ is direct.

(i) $|A+B| = |A||B|$.

(ii) $a_1 + b_1 = a_2 + b_2$, $a_1, a_2 \in A$, $b_1, b_2 \in B$ *implies* $a_1 = a_2$, $b_1 = b_2$.

(iii) $(A-A) \cap (B-B) \subseteq \{0\}$.

(iv) *The sets $A+b$, $b \in B$ are pair-wise disjoint.*

(v) *The sets $a+B$, $a \in A$ are pair-wise disjoint.*

PROOF (1) We show that (i) implies (ii). Let $a_1, a_2 \in A$, and $b_1, b_2 \in B$ such that $a_1 + b_1 = a_2 + b_2$. We would like to show that $a_1 = a_2$, $b_1 = b_2$.

If $a_1 = a_2$, then by canceling we get $b_1 = b_2$, as required. Thus we may assume that $a_1 \neq a_2$. Now the elements $a+b$, $a \in A$, $b \in B$ are not all distinct and so $|A+B| < |A||B|$. This contradicts $|A+B| = |A||B|$.

(2) We claim that (ii) implies (iii). In order to verify the claim, choose a $g \in (A-A) \cap (B-B)$ and try to show that $g = 0$.

As $g \in A-A$, there are elements $a_1, a_2 \in A$ such that $g = a_1 - a_2$. As $g \in B-B$, there are elements $b_1, b_2 \in B$ such that $g = b_1 - b_2$. Rearranging $a_1 - a_2 = b_1 - b_2$ gives $a_1 + b_2 = a_2 + b_1$. Using (ii) we can draw the conclusion that $a_1 = a_2$, $b_1 = b_2$ and so $g = 0$, as required.

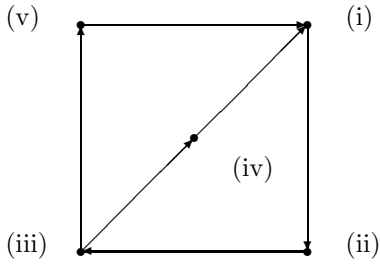

FIGURE 2.1: The implications in the proofs of Lemma 2.1.

(3) We will show that (iii) implies (iv). Choose $b_1, b_2 \in B$ such that $b_1 \neq b_2$ and try to show that $(A + b_1) \cap (A + b_2) = \emptyset$. Assume on the contrary that there is an element $g \in (A + b_1) \cap (A + b_2)$. As $g \in A + b_1$, there is an $a_1 \in A$ such that $g = a_1 + b_1$. As $g \in A + b_2$, there is an $a_2 \in A$ such that $g = a_2 + b_2$. Now $a_1 + b_1 = a_2 + b_2$ and so $a_1 - a_2 = b_2 - b_1$. Using (iii) we can conclude that $a_1 - a_2 = 0$, $b_2 - b_1 = 0$, that is, $a_1 = a_2$, $b_2 = b_1$. But we know that $b_1 \neq b_2$.

(4) The fact that (iii) implies (v) can be checked in a similar way.

(5) We prove that (iv) implies (i). Note that

$$A + B = \bigcup_{b \in B} (A + b).$$

Now

$$|A + B| = \Big| \bigcup_{b \in B} (A + b) \Big| = \sum_{b \in B} |A + b| = |A||B|,$$

as required.

(6) That (v) implies (i) can be settled in a similar way. □

If each element $g \in G$ can be expressed uniquely in the form

$$g = a + b, \quad a \in A,\ b \in B,$$

then the equation $G = A + B$ is called a *factorization* of G.

LEMMA 2.2

Let G be a finite abelian group and let A, B be non-empty subsets of G. The following statements are all equivalent to the fact that the equation $G = A + B$ is a factorization of G.

(i) *The sum $A + B$ is direct and is equal to G.*

(ii) *$G = A + B$ and $|G| = |A||B|$.*

(iii) $|G| = |A||B|$ *and* $(A - A) \cap (B - B) \subseteq \{0\}$.

(iv) $G = A + B$ *and* $(A - A) \cap (B - B) \subseteq \{0\}$.

(v) *The sets* $A + b$, $b \in B$ *form a partition of* G.

(vi) *The sets* $a + B$, $a \in A$ *form a partition of* G.

PROOF (1) We show that (i) implies (ii). As $G = A + B$ is included in both (i) and (ii), it is enough to verify that $|G| = |A||B|$. Since the sum $A+B$ is direct, by Lemma 2.1 (on page 11), $|A + B| = |A||B|$. Using $G = A + B$ we get $|G| = |A + B| = |A||B|$, as required.

(2) We will show that (ii) implies (iii). As $|G| = |A||B|$ is included in both (ii) and (iii), we need to verify only that $(A - A) \cap (B - B) \subseteq \{0\}$. From $|G| = |A||B|$ and $G = A + B$ we get $|A + B| = |A||B|$. By Lemma 2.1 (on page 11), the sum $A + B$ is direct. Again by Lemma 2.1, it follows that $(A - A) \cap (B - B) \subseteq \{0\}$, as required.

(3) We prove that (iii) implies (iv). Since $(A-A)\cap(B-B) \subseteq \{0\}$ is common in (iii) and (iv), it remains to show that $G = A + B$. Plainly $A + B \subseteq G$. So it remains to show that $G \subseteq A + B$. Assume on the contrary that there is a $g \in G$, $g \notin A + B$. Now $|G| < |A||B|$, which contradicts (iii).

(4) We prove that (iv) implies (v). From $(A - A) \cap (B - B) \subseteq \{0\}$, by Lemma 2.1 (on page 11), it follows that the sets $A + b$, $b \in B$ are pair-wise disjoint. From $G = A + B$ it follows that

$$G = \bigcup_{b \in B} (A + b),$$

as required

(5) The fact that (iv) implies (vi) can be verified in an analogous way.

(6) We will prove that (v) implies (i). Since the sets $A + b$, $b \in B$ are pair-wise disjoint, by Lemma 2.1 (on page 11), the sum $A + B$ is direct. Now

$$A + B = \bigcup_{b \in B} (A + b) = G,$$

as required.

(7) It remains to prove that (vi) implies (i). This can be done in a similar manner. ∎

The next lemmas are about constructing a factorization from a known factorization.

LEMMA 2.3

Let G be a finite abelian group. If H is a subgroup of G, and A, B are subsets of G such that $A \subseteq H$, then $(A + B) \cap H = A + (B \cap H)$.

PROOF Choose an element g from $(A+B)\cap H$. Now $g \in A+B$ and $g \in H$. There are $a \in A$, $b \in B$ such that $g = a+b$. From $g \in H$, $a \in H$ it follows that $b \in H$ and so $b \in B \cap H$. Therefore $g \in A+(B\cap H)$, which proves that $(A+B)\cap H \subseteq A+(B\cap H)$.

Next choose an element g from $A+(B\cap H)$. There are elements $a \in A$, $b \in B\cap H$ such that $g = a+b$. Plainly $g \in A+B$ and $g \in H$, and so $g \in (A+B)\cap H$, which shows that $A+(B\cap H) \subseteq (A+B)\cap H$. □

We would like to mention that Lemma 2.3 (on page 13) holds for non-commuta-tive groups and it can be found in standard group theory books under the title Dedekind identity.

COROLLARY 2.1

Let $G = A+B$ be a normalized factorization of the finite abelian group G and let H be a subgroup of G such that $A \subseteq H$. Then $H = A+(B\cap H)$ is a factorization of H.

PROOF Note that since the sum $A+B$ is direct, so is the sum $A+(B\cap H)$. Further,

$$\begin{aligned} H &= G\cap H \\ &= (A+B)\cap H \\ &= A+(B\cap H). \end{aligned}$$

In other words, the sum $A+(B\cap H)$ is direct and is equal to H. □

In the course of our work, when we use Corollary 2.1 we will say that we get the factorization $H = A+(B\cap H)$ by restricting the factorization $G = A+B$ to the subgroup H.

EXERCISE 2.1 Let $G = A+B$ be a normalized factorization of the finite abelian group G and let H be a subgroup of G. Does it follow that $H = (A\cap H)+(B\cap H)$ is a factorization of H? (Hint: Let G be a group of type $Z(3)\oplus Z(3)$ with basis elements x, y and let $A = \langle x\rangle$, $B = \langle y\rangle$, $H = \langle x+y\rangle$.) □

The factorization $G = A+B$ means that the sets $a+B$, $a \in A$ form a partition of G. Intersecting this partition by H gives that the sets $(a+B)\cap H$, $a \in A$ form a partition of H. By Lemma 2.3 (on page 13), $(\{a\}+B)\cap H = \{a\}+(B\cap H)$ and so the sets $a+(B\cap H)$, $a \in A$ form a partition of H. Therefore $A+(B\cap H)$ is a factorization of H. Figure 2.2 (on page 15) illustrates this argument.

We say that a subset A of a finite abelian group G is *full-rank* if $\langle A\rangle = G$. We say that the factorization $G = A+B$ is a *full-rank factorization* if A and

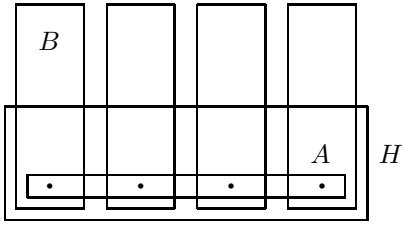

FIGURE 2.2: The subgroup H and the partition $a + B$, $a \in A$.

B are both full-rank subsets of G. The next result shows that if a factor in a factorization is not full-rank, then the factorization must have a certain structure.

LEMMA 2.4

Let $G = A + B$ be a normalized factorization of the finite abelian group G. Suppose that the factorization is not full-rank, say $H = \langle A \rangle \neq G$. Then there are elements $b_1, \ldots, b_s \in B$ and subsets $C_1, \ldots, C_s \subseteq G$ such that $C_1 + b_1, \ldots, C_s + b_s$ form a partition of B and $H = A + C_1, \ldots, H = A + C_s$ are normalized factorizations of H.

PROOF The union of the cosets $H + g$ gives G as g ranges over G. Each $g \in G$ is expressible in the form

$$g = a + b, \quad a \in A,\ b \in B.$$

Now $H+g = H+a+b = H+b$ and so the union of the cosets $H+b$ gives G as b varies over B. There are $b_1, \ldots, b_s \in B$ such that the cosets $H+b_1, \ldots, H+b_s$ form a partition of G. Adding $-b_i$ to both sides of the factorization $G = A + B$ gives the normalized factorization $G = A + (B - b_i)$. Restricting this factorization to H, we get the factorization $H = A + [(B - b_i) \cap H]$. Setting $C_i = (B - b_i) \cap H$, we can see that $H = A + C_i$ is a normalized factorization of H. Note that $C_i + b_i = B \cap (H + b_i)$ and so the sets $C_1 + b_1, \ldots, C_s + b_s$ form a partition of B. □

Lemma 2.4 (on page 15) suggests a way to extend the factorizations of a subgroup to a factorization of the whole group.

LEMMA 2.5

Let H be a subgroup of a finite abelian group G and let $G = D + H$ be a normalized factorization of G, where $D = \{b_1, \ldots, b_s\}$ with $b_1 = 0$. Suppose

that $H = A + C_1, \ldots, H = A + C_s$ are normalized factorizations of H. Set

$$B = (b_1 + C_1) \cup \cdots \cup (b_s + C_s).$$

Then $G = A + B$ is a normalized factorization of G.

PROOF The routine computation

$$\begin{aligned} A + B &= A + [(b_1 + C_1) \cup \cdots \cup (b_s + C_s)] \\ &= (b_1 + A + C_1) \cup \cdots \cup (b_s + A + C_s) \\ &= (b_1 + H) \cup \cdots \cup (b_s + H) \\ &= \{b_1, \ldots, b_s\} + H \\ &= D + H \\ &= G \end{aligned}$$

shows that the sum $A + B$ is equal to G.

Note that the cosets $b_1 + H, \ldots, b_s + H$ are disjoint and

$$b_1 + C_1 \subseteq b_1 + H, \ldots, b_s + C_s \subseteq b_s + H.$$

Therefore the sets $b_1 + C_1, \ldots, b_s + C_s$ are disjoint. From the factorizations $H = A+C_1, \ldots, H = A+C_s$ one can read off that $|C_1| = \cdots = |C_s| = |H|/|A|$. Thus

$$|b_1 + C_1| = \cdots = |b_s + C_s| = |H|/|A|.$$

It follows that

$$|B| = |b_1 + C_1| + \cdots + |b_s + C_s| = s(|H|/|A|).$$

Using this we get

$$\begin{aligned} |A||B| &= |A|s(|H|/|A|) \\ &= s|H| \\ &= |G|, \end{aligned}$$

and so the sum $A + B$ is a factorization of G. ∎

2.2 Factorization

LEMMA 2.6

Let $G = A + B$ be a normalized factorization of the abelian group G. If $A = C + H$ is a factorization of A, where H is a subgroup G, then

$$G/H = (C + H)/H + (B + H)/H$$

is a normalized factorization of the factor group G/H, where

$$(C+H)/H = \{c+H:\ c\in C\},$$
$$(B+H)/H = \{b+H:\ b\in B\}.$$

PROOF Choose a $g\in G$. Since $G=A+B$ is a factorization of G, g can be represented in the form

$$g=a+b,\quad a\in A,\quad b\in B.$$

Since $A=C+H$ is a factorization of A, a can be represented in the form

$$a=c+h,\quad c\in C,\quad h\in H.$$

Consequently, $g=c+h+b$ and so

$$\begin{aligned} g+H &= (c+h+b)+H \\ &= (c+h+H)+(b+H) \\ &= (c+H)+(b+H). \end{aligned}$$

Thus $g+H$ can be represented in the required form. Now assume that

$$(c+H)+(b+H)=(c'+H)+(b'+H),\quad c,c'\in C,\quad b,b'\in B,$$

that is, $(c+b)+H=(c'+b')+H$. There are $h,h'\in H$ such that $c+b+h=c'+b'+h'$. As $G=A+B$ is a factorization of G, from

$$\underbrace{(\ c+h\ )}_{\in A}+\underbrace{(\ b\ )}_{\in B}=\underbrace{(\ c'+h'\ )}_{\in A}+\underbrace{(\ b'\ )}_{\in B}$$

it follows that $c+h=c'+h'$, $b=b'$. Now, using the fact that $A=C+H$ is a factorization we can conclude that $c=c'$, which completes the proof. □

We will refer to the result in Lemma 2.6 (on page 16) by saying that, considering the factor group G/H, the factorization $G=(C+H)+B$ gives the factorization

$$G/H=(C+H)/H+(B+H)/H$$

of the factor group G/H.

LEMMA 2.7

Let $G=A+B$ be a factorization. Suppose that H is a subgroup and C is a subset of G such that the sum $C+H$ is direct and is equal to A. If $G=A+B$ is a full-rank factorization of G, then

$$G/H=(C+H)/H+(B+H)/H$$

is a full-rank factorization of the factor group G/H.

PROOF First let us use the fact that $A = C + H$ is a full-rank subset in G. It follows that for each $g \in G$ there are elements $c_1, \ldots, c_s, \in C$, $h \in H$ and integers $\gamma_1, \ldots, \gamma_s, \gamma$ such that

$$g = \gamma_1 c_1 + \cdots + \gamma_s c_s + \gamma h.$$

Now

$$\begin{aligned} g + H &= (\gamma_1 c_1 + \cdots + \gamma_s c_s + \gamma h) + H \\ &= (\gamma_1 c_1 + H) + \cdots + (\gamma_s c_s + H) + (\gamma h + H) \\ &= \gamma_1 (c_1 + H) + \cdots + \gamma_s (c_s + H). \end{aligned}$$

This means that $(C + H)/H$ is a full-rank subset in G/H.

Next let us use the fact that B is a full-rank subset in G. A similar argument to the one we have just seen gives that $(B + H)/H$ is a full-rank subset in G/H. ∎

We say that a subset A of a finite abelian group G is *periodic* if there is a $g \in G \setminus \{0\}$ such that $g + A = A$. We call the element g a *period* of A.

The periodicity of a subset A of a finite abelian group G can be tested by its translates. Namely, set

$$L = \bigcap_{a \in A} (A - a).$$

It turns out that L is a subgroup of G and, further, that the elements of $L \setminus \{0\}$ are all the periods of A. We will call L the *subgroup of periods* of A.

LEMMA 2.8

Let A be a non-empty subset of a finite abelian group G. Let L be the subset assigned to A.

(i) *If $g \in L$, then $g + A = A$.*

(ii) *If $g + A = A$ for some $g \in G$, then $g \in L$.*

(iii) *L is a subgroup of G.*

(iv) *There is a subset B of A such that the sum $B + L$ is direct and is equal to A.*

PROOF (i) Let $A = \{a_1, \ldots, a_n\}$ and let $g \in L \setminus \{0\}$. For each $a_i \in A$, there is a $b_i \in A$ such that $g = b_i - a_i$, that is, $g = b_1 - a_1 = \cdots = b_n - a_n$. Note

that $b_1, \ldots, b_n$ are pair-wise distinct elements of A. Since A has n elements, $b_1, \ldots, b_n$ are all the elements of A. Consequently,

$$\begin{aligned} g + A &= \{g + a_1, \ldots, g + a_n\} \\ &= \{(b_1 - a_1) + a_1, \ldots, (b_n - a_n) + a_n\} \\ &= \{b_1 + (a_1 - a_1), \ldots, b_n + (a_n - a_n)\} \\ &= \{b_1, \ldots, b_n\} \\ &= A. \end{aligned}$$

(ii) Let g be an element of G for which $g + A = A$. Now the elements $g + a_1, \ldots, g + a_n$ form a permutation of $a_1, \ldots, a_n$. For each $a_i \in A$ there is an $a_j \in A$ such that $g + a_i = a_j$. Now $g = a_j - a_i$ and so

$$g \in \bigcap_{a \in A} (A - a) = L.$$

(iii) Since A is not empty, $0 \in L$. In particular, L is not empty. Let $g, h \in L$. By part (i) of the lemma, $g + A = A$, $h + A = A$. Then $(g + h) + A = g + (h + A) = g + A = A$ shows that $(g + h) + A = A$ and so, by part (ii) of the lemma, $(g + h) \in L$.

(iv) Since G is a union of disjoint cosets modulo L, there are elements $b_1, \ldots, b_s \in A$ such that the cosets $b_1 + L, \ldots, b_s + L$ are distinct and their union contains A. Set $B = \{b_1, \ldots, b_s\}$. Note that $b_i + L \subseteq A$ for each i, $1 \leq i \leq s$. Indeed, each element of $b_i + L$ is in the form $b_i + g$, where $g \in L$ and $(b_i + g) \in A$ as $b_i \in A$. Therefore, the sets $b_1 + L, \ldots, b_s + L$ form a partition of A. This means that the sum $B + L$ is direct and is equal to A.

This completes the proof. ∎

LEMMA 2.9

Let A be a subset of a finite abelian group G. Let C be a subset and let H be a subgroup of G such that the sum $C + H$ is direct and is equal to A. If $g + H$ is a period of $(C + H)/H$ in G/H, then g is a period of A in G.

PROOF Let $C = \{c_1, \ldots, c_s\}$. Since $g + H$ is a period of

$$(C + H)/H = \{c_1 + H, \ldots, c_s + H\}$$

in G/H, it follows that the cosets

$$(g + H) + (c_1 + H), \ldots, (g + H) + (c_s + H)$$

form a permutation of the cosets $c_1 + H, \ldots, c_s + H$. Using this we have

$$\begin{aligned} g + A &= g + (C + H) \\ &= g + [\{c_1, \ldots, c_s\} + H] \\ &= g + [(c_1 + H) \cup \cdots \cup (c_s + H)] \end{aligned}$$

$$
\begin{aligned}
&= (g + c_1 + H) \cup \cdots \cup (g + c_s + H) \\
&= [(g + H) + (c_1 + H)] \cup \cdots \cup [(g + H) + (c_s + H)] \\
&= (c_1 + H) \cup \cdots \cup (c_s + H) \\
&= \{c_1, \ldots, c_s\} + H \\
&= C + H \\
&= A.
\end{aligned}
$$

∎

COROLLARY 2.2

Let H be a subgroup of periods of a subset A of a finite abelian group G. If C is a subset of G such that the sum $C + H$ is direct and is equal to A, then C is not periodic in G and $(C + H)/H$ is not periodic in G/H.

Let G be a finite abelian group and let A, B be subsets of G. Let $\varphi : B \to A$ be a function. We call the set

$$\{\varphi(b) + b : \ b \in B\}$$

the *composition* of A and B with respect to the function φ and we denote it by $A \circ_\varphi B$.

LEMMA 2.10

Let G be a finite abelian group and let H, K be subgroups of G such that $H \subseteq K$. Let D be a complete set of representatives in K modulo H and let $\varphi : D \to H$ be a function.

(i) *The set $E = H \circ_\varphi D$ is a complete set of representatives in K modulo H.*

(ii) *If E is a complete set of representatives in K modulo H, then there is a φ such that $E = H \circ_\varphi D$.*

PROOF (i) Set $E = H \circ_\varphi D$. We will show that each coset in K modulo H contains exactly one element from E. Choose a $d \in D$ and consider the coset $d + H$. Now $\varphi(d) + d \in (H \circ_\varphi D) = E$ and the computation

$$
\begin{aligned}
[\varphi(d) + d] + H &= d + [\varphi(d) + H] \\
&= d + H
\end{aligned}
$$

shows that $\varphi(d) + d \in (d + H)$.

Choose $e_1, e_2 \in E$ and try to show that $e_1 - e_2 \in H$ implies $e_1 = e_2$. Since $e_1 \in E$, there is a $d_1 \in D$ such that $e_1 = \varphi(d_1) + d_1$. Since $e_2 \in E$, there is a $d_2 \in D$ such that $e_2 = \varphi(d_2) + d_2$. Now

$$\underbrace{e_1 - e_2}_{\in H} = \underbrace{\varphi(d_1)}_{\in H} + d_1 - \underbrace{\varphi(d_2)}_{\in H} - d_2$$

gives that $d_1 - d_2 \in H$. Since D is a complete set of representatives in K modulo H, $d_1 - d_2 \in H$ implies $d_1 = d_2$. It follows that $\varphi(d_1) = \varphi(d_2)$ and so

$$e_1 = \varphi(d_1) + d_1 = \varphi(d_2) + d_2 = e_2,$$

as required.

(ii) Choose a $d \in D$. Since E is a complete set of representatives in K modulo H, there is a unique element $e \in E$ for which $e \in (d + H)$. Set $\varphi(d) = e - d$. Now

$$\varphi(d) + d = (e - d) + d = e.$$

Consequently

$$H \circ_\varphi D = \{\varphi(d) + d : \ d \in D\} = E,$$

as required. ∎

LEMMA 2.11

Let G be a finite abelian group. Let A be a subset and let H be a subgroup of G. Let $\varphi : A \to H$ be a function. Then $(H \circ_\varphi A) + H = A + H$.

PROOF Choose an element $g \in (H \circ_\varphi A) + H$. There are elements $a \in A$, $h \in H$ such that $g = [\varphi(a) + a] + h$. Now $g = a + [\varphi(a) + h]$. As $\varphi(a) + h \in H$, it follows that $g \in A + H$.

Choose an element $g \in (A + H)$. There are elements $a \in A$, $h \in H$ such that $g = a + h$. Now $g = [\varphi(a) + a] + [-\varphi(a) + h]$. As $\varphi(a) + a \in H \circ_\varphi A$ and $-\varphi(a) + h \in H$, it follows that $g \in [(H \circ_\varphi A) + H]$. ∎

LEMMA 2.12

Let G be a finite abelian group and let A, B be subsets of G. Let H be the subgroup of periods of B. If the sum $A+B$ is direct, then the sum $(H \circ_\varphi A)+B$ is direct and is equal to $A + B$ for each function $\varphi : A \to H$.

PROOF Since H is the subgroup of periods of B, by Lemma 2.8 (on page 18), there is a subset C of G such that the sum $H + C$ is direct and is equal to B. By Lemma 2.11 (on page 21), $(H \circ_\varphi A) + H = A + H$ and so the computation

$$\begin{aligned}(H \circ_\varphi A) + B &= (H \circ_\varphi A) + (H + C)\\ &= [(H \circ_\varphi A) + H] + C\\ &= (A + H) + C\\ &= A + (H + C)\\ &= A + B\end{aligned}$$

shows that the sum $(H \circ_\varphi A) + B$ is equal to $A + B$.

Choose $g_1, g_2 \in (H \circ_\varphi A)$, $b_1, b_2 \in B$ and show that $g_1 + b_1 = g_2 + b_2$ implies $g_1 = g_2$, $b_1 = b_2$.

There are elements $a_1, a_2 \in A$ such that $g_1 = \varphi(a_1) + a_1$, $g_2 = \varphi(a_2) + a_2$. As $B = H + C$, there are elements $h_1, h_2 \in H$, $c_1, c_2 \in C$ such that $b_1 = h_1 + c_1$, $b_2 = h_2 + c_2$. Now

$$\begin{aligned} g_1 + b_1 &= [\varphi(a_1) + a_1] + [h_1 + c_1] \\ &= a_1 + [\varphi(a_1) + h_1 + c_1], \\ g_2 + b_2 &= [\varphi(a_2) + a_2] + [h_2 + c_2] \\ &= a_2 + [\varphi(a_2) + h_2 + c_2]. \end{aligned}$$

Since the sum $A + B$ is direct, from

$$\underbrace{a_1}_{\in A} + \underbrace{[\varphi(a_1) + h_1 + c_1]}_{\in B} = \underbrace{a_2}_{\in A} + \underbrace{[\varphi(a_2) + h_2 + c_2]}_{\in B}$$

it follows that $a_1 = a_2$ and

$$\varphi(a_1) + h_1 + c_1 = \varphi(a_2) + h_2 + c_2.$$

Plainly $a_1 = a_2$ implies $\varphi(a_1) = \varphi(a_2)$. Since the sum $H + C$ is direct from

$$\underbrace{h_1}_{\in H} + \underbrace{c_1}_{\in C} = \underbrace{h_2}_{\in H} + \underbrace{c_2}_{\in C},$$

it follows that $h_1 = h_2$, $c_1 = c_2$. Therefore

$$g_1 = \varphi(a_1) + a_1 = \varphi(a_2) + a_2 = g_2,$$

$$b_1 = h_1 + c_1 = h_2 + c_2 = b_2,$$

as required. ∎

2.3 Homomorphism

LEMMA 2.13

Let $f : G_1 \to G_2$ be a homomorphism from G_1 onto G_2 and let $G_2 = A_2 + B_2$ be a factorization of G_2. If A_1 is a subset of G_1 such that the restriction of f to A_1 is a bijection from A_1 onto A_2 and $B_1 = f^{-1}(B_2)$, then $G_1 = A_1 + B_1$ is a factorization of G_1.

PROOF Choose a $g_1 \in G_1$ and set $g_2 = f(g_1)$. As $G_2 = A_2 + B_2$ is a factorization of G_2, there are $a_2 \in A_2$, $b_2 \in B_2$ for which $g_2 = a_2 + b_2$. There is an $a_1 \in A_1$ such that $f(a_1) = a_2$. Set $b_1 = g_1 - a_1$. Now the computation

$$\begin{aligned} f(b_1) &= f(g_1 - a_1) \\ &= f(g_1) - f(a_1) \\ &= g_2 - a_2 \\ &= b_2 \end{aligned}$$

shows that $b_1 \in f^{-1}(B_2) = B_1$. Thus each $g_1 \in G_1$ can be represented in the form

$$g_1 = a_1 + b_1, \quad a_1 \in A_1,\ b_1 \in B_1.$$

Suppose now that

$$a_1 + b_1 = a_1' + b_1', \quad a_1, a_1' \in A_1,\ b_1, b_1' \in B_1.$$

Applying f we get $f(a_1) + f(b_1) = f(a_1') + f(b_1')$. As $G_2 = A_2 + B_2$ is a factorization, from

$$\underbrace{(\ f(a_1)\ )}_{\in A_2} + \underbrace{(\ f(b_1)\ )}_{\in B_2} = \underbrace{(\ f(a_1')\ )}_{\in A_2} + \underbrace{(\ f(b_1')\ )}_{\in B_2}$$

it follows that $f(a_1) = f(a_1')$, $f(b_1) = f(b_1')$. Since the restriction of f to A_1 is a bijection, $f(a_1) = f(a_1')$ implies $a_1 = a_1'$. From $a_1 + b_1 = a_1' + b_1'$ it follows that $b_1 = b_1'$, as required. ∎

We refer to the result in Lemma 2.13 (on page 22) as lifting a factorization from G_2 to G_1.

Sometimes we need to consider multiple factorizations. Let G be a finite abelian group and let A, B be subsets of G. If each element $g \in G$ can be represented in exactly k ways in the form

$$g = a + b, \quad a \in A, \quad b \in B,$$

then we say that the sum $A + B$ is a k-fold factorization of G. In other words, for each $g \in G$, there are k distinct pairs

$$(a_1, b_1), \ldots, (a_k, b_k),$$

$a_i \in A$, $b_i \in B$ such that $g = a_1 + b_1 = \cdots = a_k + b_k$. Further,

$$g = a + b, \quad a \in A, \quad b \in B$$

implies that $(a, b) \in \{(a_1, b_1), \ldots, (a_k, b_k)\}$.

LEMMA 2.14
Let $f : G \to H$ be a homomorphism from G onto H such that $k = |\mathrm{Ker} f|$ is finite. Let $G = A + B$ be a factorization of G. Suppose that the restriction of f to A is one-to-one and similarly the restriction of f to B is one-to-one. Then the sum $f(A) + f(B)$ is a k-fold factorization of H.

PROOF Choose an element h of H. There are distinct elements $g_1, \ldots, g_k$ of G with $f(g_1) = \cdots = f(g_r) = h$. Since $G = A + B$ is a factorization of G, there are elements $a_i \in A$, $b_i \in B$ such that $g_i = a_i + b_i$ for each i, $1 \leq i \leq k$. The computation

$$h = f(g_i) = f(a_i + b_i) = f(a_i) + f(b_i)$$

shows that h has k representations in the form $f(a) + f(b)$, $a \in A$, $b \in B$. We claim that the pairs

$$[f(a_1), f(b_1)], \ldots, [f(a_k), f(b_k)]$$

are distinct. In order to verify the claim, suppose that

$$[f(a_i), f(b_i)] = [f(a_j), f(b_j)].$$

As the restriction of f to A is a bijection, from $f(a_i) = f(a_j)$ it follows that $a_i = a_j$. As the restriction of f to B is a bijection, from $f(b_i) = f(b_j)$ it follows that $b_i = b_j$. Therefore $(a_i, b_i) = (a_j, b_j)$. Now

$$g_i = a_i + b_i = a_j + b_j = g_j$$

gives that $i = j$. ∎

COROLLARY 2.3
Let $f : G \to G$ be an automorphism of G and let $G = A+B$ be a factorization of G. Then $G = f(A) + f(B)$ is also a factorization of G.

There are further ways to construct multiple factorizations from a 1-fold factorization.

LEMMA 2.15
Let $G = A+B$ be a factorization of the finite abelian group G. Set $A_1 = G \setminus A$, $B_1 = G \setminus B$. Then the sum

(i) *$A_1 + B$ is a $(|B| - 1)$-fold,*

(ii) *$A + B_1$ is a $(|A| - 1)$-fold,*

(iii) *$A_1 + B_1$ is a $(|A| - 1)(|B| - 1)$-fold*

factorization of G.

PROOF (i) Note that $A_1+B=(G\setminus A)+B=(G+B)\setminus(A+B)$. The sum $G+B$ is a $|B|$-fold factorization of G. The sum $A+B$ is a 1-fold factorization of G. Therefore the sum A_1+B is a $(|B|-1)$-fold factorization of G. The (ii) and (iii) cases can be settled in a similar way. □

We extend the concept of factorization to the case of more than two factors. This step is natural and unavoidable even if one is basically interested in factorizations containing only two factors.

Let G be a finite abelian group and let $A_1,\dots,A_n$ be subsets of G. The sum $A_1+\cdots+A_n$ is defined to be the set of elements

$$a_1+\cdots+a_n,\quad a_1\in A_1,\dots,a_n\in A_n. \tag{2.1}$$

If the elements on the list (2.1) are distinct, then we say that the sum $A_1+\cdots+A_n$ is direct.

LEMMA 2.16

Let G be a finite abelian group and let $A_1,\dots,A_n$ be subsets of G. Set $B_i=A_1+\cdots+A_{i-1}+A_{i+1}+\cdots+A_n$ for each i, $1\le i\le n$. The directness of the sum $A_1+\cdots+A_n$ is equivalent to any of the following statements:

(i) $|A_1+\cdots+A_n|=|A_1|\cdots|A_n|$.

(ii) $a_1+\cdots+a_n=a_1'+\cdots+a_n'$, $a_1,a_1'\in A_1,\dots,a_n,a_n'\in A_n$ *imply* $a_1=a_1',\dots,a_n=a_n'$.

(iii) $(A_i-A_i)\cap(B_i-B_i)\subseteq\{0\}$ *for each* i, $1\le i\le n$.

(iv) *The sets A_i+b_i, $b_i\in B_i$ are pair-wise disjoint for each i, $1\le i\le n$.*

PROOF (1) We show that (i) implies (ii). We choose $a_1,a_1'\in A_1,\dots,a_n$, $a_n'\in A_n$ and we try to show that $a_1=a_1',\dots,a_n=a_n'$. If $a_1=a_1',\dots,a_n=a_n'$, then there is nothing to prove. So we may assume that $(a_1,\dots,a_n)\ne(a_1',\dots,a_n')$. In this case $|A_1+\cdots+A_n|<|A_1|\cdots|A_n|$. By (i), this is not possible.

(2) We will show that (ii) implies (iii). Choose a $g\in(A_i-A_i)\cap(B_i-B_i)$ and try to verify that $g=0$. As $g\in(A_i-A_i)$, there are elements $a_i,a_i'\in A_i$ such that $g=a_i-a_i'$. As $g\in(B_i-B_i)$, there are elements $b_i,b_i'\in B_i$ such that $g=b_i-b_i'$. From $a_i-a_i'=b_i-b_i'$ we get $a_i+b_i'=a_i'+b_i$. Since $b_i,b_i'\in B_i$, b_i,b_i' can be represented in the forms

$$b_i=a_1+\cdots+a_{i-1}+a_{i+1}+\cdots+a_n,$$

$$b_i'=a_1'+\cdots+a_{i-1}'+a_{i+1}'+\cdots+a_n',$$

where

$$a_1, a_1' \in A_1, \ldots, a_{i-1}, a_{i-1}' \in A_{i-1}, a_{i+1}, a_{i+1}' \in A_{i+1}, \ldots, a_n, a_n' \in A_n.$$

From

$$a_1' + \cdots + a_{i-1}' + a_i + a_{i+1}' + \cdots + a_n' = a_1 + \cdots + a_{i-1} + a_i' + a_{i+1} + \cdots + a_n,$$

by (ii), it follows that $a_i = a_i'$ and so $g = 0$.

(3) We claim that (iii) implies (iv). In order to verify the claim, choose $b_i, b_i' \in B_i$ such that $b_i \neq b_i'$ and assume on the contrary that there is an element $g \in (A_i + b_i) \cap (A_i + b_i')$. Since $g \in (A_i + b_i)$, there is an $a_i \in A_i$ such that $g = a_i + b_i$. Since $g \in (A_i + b_i')$, there is an $a_i' \in A_i$ such that $g = a_i' + b_i'$. From $a_i + b_i = a_i' + b_i'$ we get $a_i - b_i' = a_i' - b_i$. By (iii), it follows that $a_i = a_i'$, $b_i' = b_i$. But we know that $b_i \neq b_i'$.

(4) We claim that (iv) implies (i). Set $C_j = A_1 + \cdots + A_{j-1}$ for each j, $2 \leq j \leq n+1$. Clearly $C_j \subseteq B_j$, and so the sets $A_j + c_j$, $c_j \in C_j$ are pair-wise disjoint. Note that

$$\begin{aligned} |C_{j+1}| &= |A_1 + \cdots + A_j| \\ &= \sum_{c_j \in C_j} |A_j + c_j| \\ &= |A_j| + \cdots + |A_j| \\ &= |C_j||A_j|. \end{aligned}$$

Therefore

$$\begin{aligned} |A_1 + \cdots + A_n| &= |C_{n+1}| \\ &= |C_n||A_n| \\ &= |C_{n-1}||A_{n-1}||A_n| \\ &= |C_2||A_2| \cdots |A_n| \\ &= |A_1||A_2| \cdots |A_n|, \end{aligned}$$

as required. ∎

If each $g \in G$ can be expressed uniquely in the form

$$g = a_1 + \cdots + a_n, \quad a_1 \in A_1, \ldots, a_n \in A_n,$$

then we say that the equation $G = A_1 + \cdots + A_n$ is a *factorization* of G.

LEMMA 2.17

Let G be a finite abelian group and let $A_1, \ldots, A_n$ be subsets of G. Set $B_i = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_n$ for each i, $1 \leq i \leq n$. The fact that $G = A_1 + \cdots + A_n$ is a factorization of G is equivalent to any of the following statements:

(i) *The sum* $A_1 + \cdots + A_n$ *is direct and is equal to* G.

(ii) $G = A_1 + \cdots + A_n$ *and* $|G| = |A_1| \cdots |A_n|$.

(iii) $|G| = |A_1| \cdots |A_n|$ *and* $(A_i - A_i) \cap (B_i - B_i) \subseteq \{0\}$ *for each* i, $1 \leq i \leq n$.

(iv) $G = A_1 + \cdots + A_n$ *and* $(A_i - A_i) \cap (B_i - B_i) \subseteq \{0\}$ *for each* i, $1 \leq i \leq n$.

(v) *The sets* $A_i + b_i$, $b_i \in B_i$ *form a partition of* G *for each* i, $1 \leq i \leq n$.

PROOF (1) We show that (i) implies (ii). Since (i) and (ii) both contain $G = A_1 + \cdots + A_n$, it remains to verify that $|G| = |A_1| \cdots |A_n|$. From the directness of the sum $A_1 + \cdots + A_n$, by Lemma 2.16 (on page 25), it follows that $|A_1 + \cdots + A_n| = |A_1| \cdots |A_n|$. Using $G = A_1 + \cdots + A_n$ we get $|G| = |A_1| \cdots |A_n|$, as required.

(2) We will show that (ii) implies (iii). Since (ii) and (iii) both contain $|G| = |A_1| \cdots |A_n|$, it is enough to show that $(A_i - A_i) \cap (B_i - B_i) \subseteq \{0\}$. Combining $G = A_1 + \cdots + A_n$ and $|G| = |A_1| \cdots |A_n|$ in (ii) provides $|A_1 + \cdots + A_n| = |A_1| \cdots |A_n|$. From this, by Lemma 2.16 (on page 25), it follows that $(A_i - A_i) \cap (B_i - B_i) \subseteq \{0\}$.

(3) We will prove that (iii) implies (iv). Since $(A_i - A_i) \cap (B_i - B_i) \subseteq \{0\}$ is common in (iii) and (iv), it remains to show that $G = A_1 + \cdots + A_n$. Plainly $A_1 + \cdots + A_n \subseteq G$. So it remains to show that $G \subseteq (A_1 + \cdots + A_n)$. Assume on the contrary that there is a $g \in G$, $g \notin (A_1 + \cdots + A_n)$. Now, $|G| < |A_1| \cdots |A_n|$ which contradicts (iii).

(4) We show that (iv) implies (v). From $(A_i - A_i) \cap (B_i - B_i) \subseteq \{0\}$, by Lemma 2.16, it follows that the sets $A_i + b_i$, $b_i \in B_i$ are pair-wise disjoint. From $G = A_1 + \cdots + A_n$ it follows that

$$G = \bigcup_{b_i \in B_i} (A_i + b_i),$$

as we wanted.

(5) We claim that (v) implies (i). Since the sets $A_i + b_i$, $b_i \in B_i$ are pair-wise disjoint, by Lemma 2.16 (on page 25), the sum $A_1 + \cdots + A_n$ is direct. Since

$$G = \bigcup_{b_i \in B_i} (A_i + b_i),$$

the sum $A_1 + \cdots + A_n$ is equal to G. ∎

Several times in the book we extended a factorization from a factorization of a subgroup or from a factorization of a factor group to the whole group. The essence of these procedures is summarized in the following lemma.

LEMMA 2.18

Let G *be an abelian group and let* H *be a subgroup of* G. *Let* $H = B_1 + \cdots + B_r$ *be a factorization of* H. *Let* $C_1, \ldots, C_s$ *be subsets of* G *such that*

$G/H = (C_1 + H)/H + \cdots + (C_s + H)/H$ is a factorization of G/H. Then $G = B_1 + \cdots + B_r + C_1 + \cdots + C_s$ is a factorization of G.

PROOF Choose an element g in G. As $G/H = (C_1 + H)/H + \cdots + (C_s + H)/H$ is a factorization of G/H, there are uniquely determined elements $c_1, \ldots, c_s$, such that $c_1 \in C_1, \ldots, c_s \in C_s$ and

$$g + H = (c_1 + H) + \cdots + (c_s + H).$$

Therefore there is a unique $h \in H$ for which

$$g = h + c_1 + \cdots + c_s.$$

Since $H = B_1 + \cdots + B_r$ is a factorization of H, there are uniquely determined elements $b_1, \ldots, b_r$ with $b_1 \in B_1, \ldots, b_r \in B_r$ and

$$h = b_1 + \cdots + b_r.$$

Thus

$$g = b_1 + \cdots + b_r + c_1 + \cdots + c_s,$$

where the elements $b_1, \ldots, b_r$, $c_1, \ldots, c_s$ are uniquely determined. □

2.4 Constructions

The constructions we present here generalize constructions due to N. G. de Bruijn [10].

Let $G = B + H$ be a normalized factorization of the finite abelian group G, where H is a subgroup of G and $B = \{b_1, \ldots, b_r\}$. We will show how simultaneous factorizations of H give rise to new factorizations of G. Suppose H admits simultaneous normalized factorizations in the form $H = A + A_i$, $1 \leq i \leq u$. Set

$$D = (b_1 + D_1) \cup \cdots \cup (b_r + D_r),$$

where $D_i \in \{A_1, \ldots, A_u\}$. By Lemma 2.5 (on page 15), $G = A + D$ is a factorization of G. This result can be generalized. Let $G = B + C + H$ be a normalized factorization where H is a subgroup of G and suppose that H admits normalized simultaneous factorizations $H = A_i + B_j$, $1 \leq i \leq u$, $1 \leq j \leq v$. Let $B = \{b_1, \ldots, b_r\}$, $C = \{c_1, \ldots, c_s\}$. Set

$$\begin{aligned} D &= (b_1 + D_1) \cup \cdots \cup (b_r + D_r), \\ E &= (c_1 + E_1) \cup \cdots \cup (c_s + E_s), \end{aligned} \tag{2.2}$$

where $D_i \in \{A_1, \ldots, A_u\}$, $E_i \in \{B_1, \ldots, B_v\}$.

LEMMA 2.19
$G = D + E$ is a factorization of G.

PROOF We will show that the sum $D+E$ is equal to G and that $|D||E| = |G|$. The following straightforward computation shows that $G = D + E$:

$$\begin{aligned} D + E &= [(b_1 + D_1) \cup \cdots \cup (b_r + D_r)] + [(c_1 + E_1) \cup \cdots \cup (c_s + E_s)] \\ &= (b_1 + c_1 + D_1 + E_1) \cup \cdots \cup (b_r + c_s + D_r + E_s) \\ &= (b_1 + c_1 + H) \cup \cdots \cup (b_r + c_s + H) \\ &= \{b_1 + c_1, \ldots, b_r + c_s\} + H \\ &= (B + C) + H \\ &= G. \end{aligned}$$

From the factorizations $H = A_i + B_1$ it follows that $|A_1| = \cdots = |A_u| = t$ and from the factorizations $H = A_1 + B_j$ it follows that $|B_1| = \cdots = |B_v| = w$. From the computation above we can see that the coset $b_i + H$ contains $b_i + D_i$. Consequently, $b_1 + D_1, \ldots, b_r + D_r$ are disjoint subsets. Therefore $|D| = rt$. Similarly, the coset $c_j + H$ contains $c_j + E_j$ and so $c_1 + E_1, \ldots, c_s + E_s$ are disjoint subsets. Hence $|E| = sw$. Now

$$\begin{aligned} |D||E| &= (rt)(sw) \\ &= r|A_1|s|B_1| \\ &= rs|A_1||B_1| \\ &= rs|H| \\ &= |B||C||H| \\ &= |G|, \end{aligned}$$

as required. ∎

The periodicity of a subset D defined in (2.2) can be tested relatively easily.

LEMMA 2.20
If the subset D defined in (2.2) is periodic, then at least one of the following must hold:

(i) *Each D_i has a common period.*

(ii) *Each D_i is a translated copy of some D_j.*

PROOF Let g be a period of D. First consider the case when $g \in H$. Note that $D_i = (D - b_i) \cap H$. Further, as $g \in H$, by Lemma 2.3 (on page 13),

$$(\{g\} + F) \cap H = \{g\} + (F \cap H)$$

holds for every subset F of G. Now

$$\begin{aligned} D_i &= (D - b_i) \cap H \\ &= (g + D - b_i) \cap H \\ &= g + [(D - b_i) \cap H] \\ &= g + D_i, \end{aligned}$$

and so g is a common period of each D_i.

Let us turn to the case when $g \notin H$. Note that the cosets

$$g + b_1 + H, \ldots, g + b_s + H$$

form a permutation of the cosets

$$b_1 + H, \ldots, b_s + H.$$

Consequently, the sets

$$g + b_1 + D_1, \ldots, g + b_s + D_s$$

form a permutation of the sets

$$b_1 + D_1, \ldots, b_s + D_s.$$

Therefore, for each i, $1 \le i \le s$ there is a j, $1 \le j \le s$ such that $g + b_i + D_i = b_i + D_j$. In other words, D_i is a translated copy of D_j. □

Let H, K, L be subgroups of a finite abelian group G such that $|K| = |L|$ and $G = D + H$, $H = K + L$ are factorizations. Here $D = \{d_1, \ldots, d_s\}$ is a subset of G. Let $\varphi : L \to K$ be a one-to-one function. Set

$$\begin{aligned} A &= K \circ_\varphi L, \\ B &= (d_1 + C_1) \cup \cdots \cup (d_s + C_s), \end{aligned}$$

where $C_i \in \{K, L\}$.

LEMMA 2.21

With the notations above $G = A + B$ is a factorization of G.

PROOF By Lemma 2.11 (on page 21),

$$\begin{aligned} A + K &= (K \circ_\varphi L) + K \\ &= L + K \\ &= H. \end{aligned}$$

Note that setting $\beta = \varphi^{-1}$ we get $A = L \circ_\beta K$. Indeed, for each $l \in L$, there is a unique $k \in K$ such that $\varphi^{-1}(k) = l$, that is, $\beta(k) = l$. Now

$$\begin{aligned}\varphi(l) + l &= \varphi[\varphi^{-1}(k)] + \varphi^{-1}(k) \\ &= k + \varphi^{-1}(k) \\ &= \beta(k) + k,\end{aligned}$$

and so $A = L \circ_\beta K$ as we claimed.

By Lemma 2.11 (on page 21),

$$\begin{aligned}A + L &= (L \circ_\beta K) + L \\ &= K + L \\ &= H.\end{aligned}$$

In other words, $H = A + K$, $H = A + L$ are simultaneous factorizations of H. By Lemma 2.5 (on page 15), $G = A + B$ is a factorization of G. □

EXAMPLE 2.1 Let G be a group of type $Z(m) \oplus Z(n) \oplus Z(n)$ with basis elements x, y, z, where $|x| = m$, $|y| = |z| = n$. Suppose that $f(0), f(1), \ldots, f(n-1)$ is a permutation of the elements $0, 1, \ldots, n-1$. Set

$$\begin{aligned}H &= \langle x, y \rangle, \\ K &= \langle y \rangle, \\ L &= \langle z \rangle, \\ A &= \{iy + [f(i)]z : \ 0 \le i \le n-1\}.\end{aligned}$$

Note that $A = L \circ_\varphi K$, where $\varphi : K \to L$ is a function defined by $\varphi(iy) = f(i)z$. The sums $A + K$, $A + L$ are factorizations of H. Therefore, by Lemma 2.5 (on page 15), $G = A + B$ is a factorization of G. In fact there is an astronomical number of these factorizations. □

Let H, K, L, M be subgroups of a finite abelian group G such that $|K| = |L| = |M|$ and $G = D + H$, $H = K + L + M$ are factorizations. Here $D = \{d_1, \ldots, d_s\}$ is a subset of G. Let

$$[k, l, f(k, l)], \quad k \in K, \quad l \in L, \quad f(k, l) \in M \tag{2.3}$$

be a Latin square. (The rows are labeled by the elements of K. The columns are labeled by the elements of L. The entries in the cells are the elements of M.) Set $A = M \circ_\alpha (K + L)$, where $\alpha : K + L \to M$ is a map defined by $\alpha(k + l) = f(k, l)$. Set

$$B = (d_1 + C_1) \cup \cdots \cup (d_s + C_s),$$

where $C_i \in \{K, L, M\}$.

LEMMA 2.22
With the notations above, $G = A + B$ is a factorization of G.

PROOF By Lemma 2.11 (on page 21),

$$\begin{aligned} A + M &= [M \circ_\alpha (K + L)] + M \\ &= (K + L) + M \\ &= H. \end{aligned}$$

The Latin square (2.3) can be described by the triples

$$[k, g(k, m), m], \quad k \in K, \quad m \in M, \quad g(k, m) \in L.$$

In this case A can be written in the form $A = L \circ_\beta (K + M)$, where $\beta : K + M \to L$ is a map defined by $\beta(k + m) = g(k, m)$. By Lemma 2.11 (on page 21),

$$\begin{aligned} A + L &= [L \circ_\beta (K + M)] + L \\ &= (K + M) + L \\ &= H. \end{aligned}$$

Finally, the Latin square (2.3) can be described by the triples

$$[h(l, m), l, m], \quad l \in L, \quad m \in M, \quad h(l, m) \in K.$$

Now A can be written in the form $A = K \circ_\gamma (L + M)$, where $\gamma : L + M \to K$ is a map defined by $\gamma(l + m) = h(l, m)$. By Lemma 2.11 (on page 21),

$$\begin{aligned} A + K &= [K \circ_\gamma (L + M)] + K \\ &= (L + M) + K \\ &= H. \end{aligned}$$

In other words, $H = A + K$, $H = A + L$, $H = A + M$ are simultaneous factorizations of H. By Lemma 2.5 (on page 15), $G = A + B$ is a factorization of G. ∎

EXAMPLE 2.2 Let G be a group of type $Z(m) \oplus Z(n) \oplus Z(n) \oplus Z(n)$ with basis elements x, y, z, w, where $|x| = m$, $|y| = |z| = |w| = n$. An n by n Latin square can be described by the n^2 triples $[i, j, f(i, j)]$, $0 \le i, j \le n - 1$, where $f(i, j)$ is the symbol in the jth position in the ith row. Set

$$\begin{aligned} H &= \langle y, z, w \rangle, \\ K &= \langle y \rangle, \\ L &= \langle z \rangle, \\ M &= \langle w \rangle, \\ A &= \{iy + jz + [f(i, j)]w : \ 0 \le i, j \le n - 1\}. \end{aligned}$$

Let us observe that the sums $A+K$, $A+L$, $A+M$ form normalized simultaneous factorizations of H. Let $D = \langle x \rangle$. Now $G = D + H$ is a factorization of G. Consequently, by Lemma 2.5 (on page 15), there is a factorization $G = A + B$ of G. □

Let H, K, L be subgroups of a finite abelian group G such that $|K| = |L|$ and $G = B + C + H$, $H = K + L$ are factorizations. Here

$$B = \{b_1, \ldots, b_r\},$$
$$C = \{c_1, \ldots, c_s\}$$

are subsets of G. Suppose that φ, ψ are one-to-one functions from L to K. Set

$$A_1 = K, \quad B_1 = K \circ_\varphi L,$$
$$A_2 = L, \quad B_2 = K \circ_\psi L,$$

$$D = (b_1 + D_1) \cup \cdots \cup (b_r + D_r),$$
$$E = (c_1 + E_1) \cup \cdots \cup (c_s + E_s),$$

where $D_i \in \{A_1, A_2\}$, $E_i \in \{B_1, B_2\}$.

LEMMA 2.23
With the notations above, $G = D + E$ is a factorization of G.

PROOF Using the ideas of the proof of Lemma 2.21 (on page 30) one can verify that the sums

$$A_1 + B_1, \quad A_1 + B_2, \quad A_2 + B_1, \quad A_2 + B_2$$

are factorizations of H. By Lemma 2.19 (on page 29), it follows that $G = D + E$ is a factorization of G. □

EXAMPLE 2.3 Let G be a group of type $Z(kn) \oplus Z(mn)$ with basis elements x, y, where $|x| = kn$, $|y| = mn$. Assume that $f(0), f(1), \ldots, f(n-1)$ and $g(0), g(1), \ldots, g(n-1)$ are permutations of $0, 1, \ldots, n-1$. Set

$$A_1 = \langle kx \rangle,$$
$$A_2 = \langle my \rangle,$$
$$B_1 = \{(ki)x + [mf(i)]y : \ 0 \le i \le n-1\},$$
$$B_2 = \{(ki)x + [mg(i)]y : \ 0 \le i \le n-1\}.$$

One can verify that the sums

$$A_1 + B_1, \ A_1 + B_2, \ A_2 + B_1, \ A_2 + B_2$$

TABLE 2.1: The factors D and E

D	E
$(0,0,0,0,0,0)$	$(0,0,0,0,0,0)$
$(1,0,0,0,0,0)$	$(1,0,0,1,0,0)$
$(0,1,0,0,0,0)$	$(0,1,0,0,1,0)$
$(1,1,0,0,0,0)$	$(1,1,0,1,1,0)$
$(0,0,1,0,0,0)$	$(0,0,0,0,0,1)$
$(0,0,1,1,0,0)$	$(1,0,0,1,1,1)$
$(0,0,1,0,1,0)$	$(0,1,0,1,0,1)$
$(0,0,1,1,1,0)$	$(1,1,0,0,1,1)$

are normalized simultaneous factorizations of the subgroup $H = \langle kx, my\rangle$ of G. We choose B and C to be the cyclic subsets $B = \{0, x, 2x, \ldots, (k-1)x\}$, $C = \{0, y, 2y, \ldots, (m-1)y\}$. One can verify that $G = B + C + H$ is a factorization of G. Now Lemma 2.19 (on page 29) is applicable and gives that there is a factorization $G = D + E$ of G. □

EXAMPLE 2.4 Let G be a group of type $Z(2) \oplus \cdots \oplus Z(2)$ with basis elements x, y, z, u, v, w. Set

$$\begin{aligned}
A_1 &= \{0, x, y, x+y\} = \langle x, y\rangle = K,\\
A_2 &= \{0, u, v, u+v\} = \langle u, v\rangle = L,\\
B_1 &= \{(0)+(0), (x)+(u), (y)+(v), (x+y)+(u+v)\} = L \circ_\alpha K,\\
B_2 &= \{(0)+(0), (x)+(u+v), (y)+(u), (x+y)+(v)\} = L \circ_\beta K.
\end{aligned}$$

The sums

$$A_1 + B_1, \quad A_1 + B_2, \quad A_2 + B_1, \quad A_2 + B_2$$

form simultaneous factorizations of $H = \langle x, y, u, v\rangle$. If $B = \{0, z\}$, $C = \{0, w\}$, then $G = B + C + H$ is a factorization of G. Setting

$$\begin{aligned}
D &= (0 + A_1) \cup (z + A_2),\\
E &= (0 + B_1) \cup (w + B_2)
\end{aligned}$$

we get that $G = D + E$ is a factorization of G. Lemma 2.20 (on page 29) is applicable and provides that neither D nor E is periodic. The elements of D and E are listed in Table 2.1 (on page 34). □

Let H, K, L, M be subgroups of a finite abelian group G such that $|K| = |L| = |M|$ and $G = B + C + H$, $H = K + L$ are factorizations. Here

$$\begin{aligned}
B &= \{b_1, \ldots, b_r\},\\
C &= \{c_1, \ldots, c_s\}
\end{aligned}$$

are subsets of G. Suppose that

$$[k, l, f(k, l)], \quad [k, l, g(k, l)]$$

are Latin squares, where

$$k \in K, \quad l \in L, \quad f(k, l), g(k, l) \in M.$$

Set $A_1 = K$, $A_2 = L$, $A_3 = M$, $B_1 = M \circ_\alpha (K + L)$, $B_2 = M \circ_\beta (K + L)$, where α, β are functions from $K + L$ to M defined by $\alpha(k + l) = f(k, l)$, $\beta(k, l) = g(k, l)$, respectively. Let

$$D = (b_1 + D_1) \cup \cdots \cup (b_r + D_r),$$
$$E = (c_1 + E_1) \cup \cdots \cup (c_s + E_s),$$

where $D_i \in \{A_1, A_2, A_3\}$, $E_i \in \{B_1, B_2\}$.

LEMMA 2.24
With the notations above, $G = D + E$ is a factorization of G.

PROOF Using the ideas of the proof of Lemma 2.22 (on page 32), one can verify that the sums

$$A_1 + B_1, \quad A_1 + B_2, \quad A_2 + B_1, \quad A_2 + B_2, \quad A_3 + B_1, \quad A_3 + B_2$$

are simultaneous factorizations of H. Then, by Lemma 2.19 (on page 29), it follows that $G = D + E$ is a factorization of G. □

EXAMPLE 2.5 Consider two Latin squares given in the forms

$$[i, j, f(i, j)], \ [i, j, g(i, j)], \quad 0 \le i, j \le n - 1,$$

Let G be a group of type $Z(kn) \oplus Z(mn) \oplus Z(n)$ with basis elements x, y, z, where $|x| = kn$, $|y| = mn$, $|z| = n$. Set

$$\begin{aligned}
A_1 &= \langle kx \rangle, \\
A_2 &= \langle my \rangle, \\
A_3 &= \langle z \rangle, \\
B_1 &= \{(ki)x + (jm)y + [f(i, j)]z : \ 0 \le i, j \le n - 1\}, \\
B_2 &= \{(ki)x + (jm)y + [g(i, j)]z : \ 0 \le i, j \le n - 1\}.
\end{aligned}$$

One can verify that the sums

$$A_1 + B_1, \ A_1 + B_2, \ A_2 + B_1, \ A_2 + B_2, \ A_3 + B_1, \ A_3 + B_2$$

are normalized simultaneous factorizations of the subgroup $H = \langle kx, my \rangle$. If $B = \{0, x, 2x, \ldots, (k-1)x\}$, $C = \{0, y, 2y, \ldots, (m-1)y\}$, then $G = B + C + H$ is a factorization of G. By Lemma 2.19 (on page 29), there is a factorization $G = D + E$ of G. □

Notes

(1) The construction described in Lemma 2.5 and its extension in Lemma 2.19 are due to N. G. de Bruijn [10].

(2) Example 2.4 exhibits a normalized factorization $G = D + E$, where G is an elementary 2-group of rank 6 and neither D nor E is periodic. It can be shown that if $G = D + E$ is a normalized factorization of G with non-periodic factors, then $\langle D \rangle \neq G$ and $\langle E \rangle \neq G$ must hold.

Chapter 3

Non-periodic factorizations

A factorization of an abelian group is said to be *bad* if no factor is periodic. In Section 3.1 we show how to construct bad factorizations for certain finite cyclic groups. We also show how to extend bad factorizations of a subgroup H to bad factorizations of the group G. We shall use the terminology k-bad if there are k factors in the bad factorization.

In Section 3.2 we show how representations of a finite abelian group relate to the factorizations. In the case of finite cyclic groups, we show how the use of cyclotomic polynomials is equivalent to the use of representations.

In Section 3.3 we show how representation theory can be used to show that one factor in a factorization may be replaced by another. The idea is to replace a bad, that is, non-periodic, factor by a less bad factor that can then be studied more easily. We should like to emphasize that Theorem 3.17 (on page 58) is one of the key results of the subject.

3.1 Bad factorizations

In this section we show how to construct bad factorizations for certain cyclic groups. We will show how to construct bad factorizations of larger groups if a bad factorization of a subgroup is known. The results are then used to show that many groups are k-bad.

Let G be an abelian group and let A, B be subsets of G. If A is periodic with period g, then $C = A + B$ is periodic with period g, as shown by the computation

$$\begin{aligned} g + C &= g + (A + B) \\ &= (g + A) + B \\ &= A + B \\ &= C. \end{aligned}$$

If C is periodic, then it does not follow that either A or B is periodic.

EXAMPLE 3.1 Let $A, C_1, \ldots, C_n$ be subsets of an abelian group G such

that the sums $A + C_1, \ldots, A + C_n$ are periodic with a common period g. Set $B = (d_1 + C_1) \cup \cdots \cup (d_n + C_n)$, where $d_1, \ldots, d_n \in G$. Then the sum $A + B$ is periodic with period g. Indeed,

$$\begin{aligned} g + (A + B) &= (g + A) + B \\ &= (g + A) + [(d_1 + C_1) \cup \cdots \cup (d_n + C_n)] \\ &= (d_1 + g + A + C_1) \cup \cdots \cup (d_n + g + A + C_n) \\ &= [d_1 + g + (A + C_1)] \cup \cdots \cup [d_n + g + (A + C_n)] \\ &= (d_1 + A + C_1) \cup \cdots \cup (d_n + A + C_n) \\ &= A + [(d_1 + C_1) \cup \cdots \cup (d_n + C_n)] \\ &= A + B. \end{aligned}$$

Let us choose G to be a group of type $Z(3) \oplus Z(2) \oplus Z(2)$ with basis elements x, y, z such that $|x| = 3$, $|y| = |z| = 2$. Set

$$\begin{aligned} A &= \{0, x + y\}, \\ C_1 &= \langle x \rangle, \\ C_2 &= \langle y \rangle, \\ B &= (0 + C_1) \cup (z + C_2). \end{aligned}$$

Note that the sums $A + C_1$, $A + C_2$ are periodic with period y. Therefore the sum $A + B$ is periodic with period y. Here A, B are normalized subsets and $|A| = 2$, $|B| = 5$. If A were periodic, then, by Lemma 2.8 (on page 18), the periods must belong to A and each of them must have order two. But the order of $x + y$ is three. If B were periodic, then, by Lemma 2.8 (on page 18), its periods must have order 5. But G does not have any element of order 5. □

The next result shows that with suitable extra conditions, if A and B are not periodic, then neither is their sum $A + B$.

THEOREM 3.1

If A, B are normalized non-periodic sets of an abelian group and the sum $\langle A \rangle + B$ is direct, then $A + B$ is a non-periodic set.

PROOF Set $H = \langle A \rangle$. Let $b \in B$. We claim that $(H + b) \cap (A + B) \subseteq A + b$. In order to verify the claim, choose an $x \in (H + b) \cap (A + B)$. As $x \in H + b$, x can be represented in the form

$$x = h + b, \quad h \in H.$$

As $x \in A + B$, x can be written in the form

$$x = a_1 + b_1, \quad a_1 \in A_1, \quad b_1 \in B.$$

Since the sum $H + B$ is direct, from

$$\underbrace{(\ h\ )}_{\in H} + \underbrace{(\ b\ )}_{\in B} = \underbrace{(\ a_1\ )}_{\in H} + \underbrace{(\ b_1\ )}_{\in B}$$

it follows that $h = a_1$, $b = b_1$. Therefore $x = a_1 + b_1 = a_1 + b$ and so $x \in A + b$, as required.

Assume on the contrary that $A + B$ is periodic and let g be a period of $A + B$. Since the sum $H + B$ is direct, so is the sum $A + B$. The sets $A + b$, $b \in B$ form a partition of $A + B$. The situation is depicted in Figure 3.1 (on page 40). Let $b \in B$. Using $(A + b) + g \subseteq (A + B) + g = A + B$ and $0 \in A$ we get that $b + g \in A + B$ and so $b + g$ can be represented in the form

$$b + g = a_1 + b_1, \quad a_1 \in A, \quad b_1 \in B.$$

Now

$$\begin{aligned} A + b + g &= A + a_1 + b_1 \\ &\subseteq H + a_1 + b_1 \\ &= H + b_1. \end{aligned}$$

From $A + b + g \subseteq A + B$, $A + b + g \subseteq H + b_1$ one can see that

$$A + b + g \subseteq (H + b_1) \cap (A + B) \subseteq A + b_1.$$

We intend to show that in fact $A + b + g = A + b_1$. To this end, note that as g is a period of $A + B$, so is $-g$. Starting with $(A + b_1) - g$ and repeating the argument above gives that there is a $b_2 \in B$ such that $(A + b_1) - g \subseteq A + b_2$. Thus

$$A + b + g \subseteq A + b_1 \subseteq A + b_2 + g,$$

that is, $A + b \subseteq A + b_2$. Choose an $a \in A$. From $a + b \in A + b$ it follows that there is an $a_3 \in A$ such that $a + b = a_3 + b_2$. Since the sum $H + B$ is direct, from

$$\underbrace{(\ a\ )}_{\in H} + \underbrace{(\ b\ )}_{\in B} = \underbrace{(\ a_3\ )}_{\in H} + \underbrace{(\ b_2\ )}_{\in B}$$

it follows that $a = a_3$, $b = b_2$. This means that

$$A + b_1 \subseteq A + b_2 + g = A + b + g.$$

Thus $A + b + g = A + b_1$, as required. Since A is not periodic, it follows that $b + g = b_1$. This holds for each $b \in B$ and consequently $B + g \subseteq B$.

Using the fact that $-g$ is a period of $A + B$, and repeating the argument with $-g$ in place of g, we can conclude that $B - g \subseteq B$. Therefore $B \subseteq B + g$ and so $B + g = B$. Since B is not periodic, $g = 0$ must hold. This is a contradiction. ∎

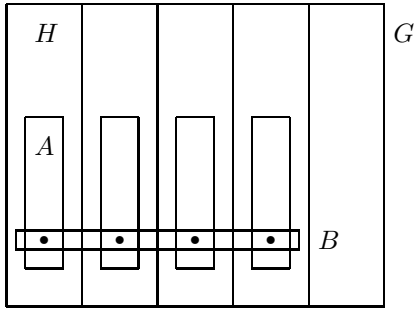

FIGURE 3.1: Cosets modulo H and the sets $A + b$, $b \in B$.

THEOREM 3.2

If H is a proper non-zero subgroup of a cyclic group G, then there exists a normalized non-periodic subset C such that C is a complete set of coset representatives for G modulo H.

PROOF Suppose first that H has prime index in G. Let A be any normalized complete set of coset representatives for G modulo H. If A is periodic, then, since A has a prime order, A is a subgroup. Choose $a \in A$ and $h \in H$ with $a \neq 0$, $h \neq 0$. Replace $a \in A$ by $a + h$ to form a new complete set of coset representatives for G modulo H. As G is cyclic, the order of a cannot be the same as the order of h. Then A is non-periodic.

We now proceed by induction on the index of H in G. Let this index be pm, where p is a prime. From the above we may assume that $m > 1$ and are assuming that the result holds for subgroups of index less than pm and, in particular, for subgroups of index m. Now G contains a subgroup K of index m and H is contained in K, and H has index p in K. By the above there is a non-periodic subset A with $K = H + A$. By the inductive assumption there is a non-periodic subset B with $G = K + B$. Then $G = H + A + B$. Now $\langle A \rangle \subseteq K$ and the sum $K + B$ is direct. By Theorem 3.1 (on page 38), it follows that $A + B$ is non-periodic, as required. □

We are able to extend a bad factorization to a larger group from a subgroup.

THEOREM 3.3

If a proper subgroup H of a group G is k-bad, then G is both k-bad and $(k + 1)$-bad.

PROOF There exists a factorization $H = A_1 + \cdots + A_k$, where each subset A_i is non-periodic. By Theorem 3.1 (on page 38), there exists a non-periodic subset C such that $G = H + C$. Then $G = A_1 + \cdots + A_k + C$ and so G is

$(k+1)$-bad. Also, $\langle A_k \rangle \subseteq H$ and $H + C$ is a direct sum. By Theorem 3.2 (on page 40), $A_k + C$ is non-periodic. By regarding $A_k + C$ as a single factor, we see that G is also k-bad. ∎

If an integer $a \geq 2$ is a product of n not necessarily distinct primes, then we set $\nu(a) = n$. For instance, $\nu(32) = 5$ and $\nu(1000) = 6$. As a consequence of Theorem 3.3 (on page 40) we can construct bad factorizations once one such factorization has been found. To start this process we need to construct some bad factorizations. This we do as follows.

THEOREM 3.4

If G contains a proper subgroup that is a direct sum of two subgroups of composite order and $\nu\big(|G|\big) = 5$, then G is both 2-bad and 3-bad.

PROOF Let a group G contain a proper subgroup H that is the direct sum of subgroups K, L of composite orders. We note that in order that the subgroup H should be cyclic, we require that $|K|$ and $|L|$ are relatively prime.

Now K, L contain non-zero proper subgroups M, N, respectively. By Theorem 3.2 (on page 40), there exist non-periodic subsets A, B such that $K = M + A$, $L = N + B$. Since the sum $K + L$ is direct, it follows that the sum $\langle A \rangle + B$ is direct and so that $A + B$ is non-periodic. Let D be a complete set of coset representatives for G modulo H. Now

$$\begin{aligned} H &= K + L \\ &= (M + A) + (N + B) \\ &= (A + B) + M + N). \end{aligned}$$

We may choose non-zero elements $a \in A$, $b \in B$, $m \in M$, $n \in N$. We form M_1 from M by replacing m by $m + b$ and we form N_1 from N by replacing n by $n + a$. In other words, let

$$\begin{aligned} M_1 &= (M \setminus \{m\}) \cup \{m + b\}, \\ N_1 &= (N \setminus \{n\}) \cup \{n + a\}. \end{aligned}$$

Then, since $b \in L$,

$$\begin{aligned} A + M_1 + L &= A + [(M \setminus \{m\}) \cup \{m + b\}] + L \\ &= A + \big\{[(M + L) \setminus (m + L)] \cup (m + b + L)\big\} \\ &= A + \big\{[(M + L) \setminus (m + L)] \cup (m + L)\big\} \\ &= A + (M + L) \\ &= (A + M) + L \\ &= K + L \\ &= H \end{aligned}$$

and as $a \in K$,

$$\begin{aligned} K + B + N_1 &= K + B + [(N \setminus \{n\}) \cup \{n + a\}] \\ &= B + \big\{[(N + K) \setminus (n + K)] \cup (n + a + K)\big\} \\ &= B + \big\{[(N + K) \setminus (n + K)] \cup (n + K)\big\} \\ &= B + (N + K) \\ &= (B + N) + K \\ &= L + K \\ &= H. \end{aligned}$$

Let $D_1 = D \setminus \{0\}$. Let $C = (M_1 + N) \cup (M + N_1 + D_1)$. Then

$$\begin{aligned} A + B + C &= (A + B) + [(M_1 + N) \cup (M + N_1 + D_1)] \\ &= [(A + B) + (M_1 + N)] \cup [(A + B) + (M + N_1 + D_1)] \\ &= (A + M_1 + L) \cup (K + B + N_1 + D_1) \\ &= H \cup (H + D_1) \\ &= H \cup [D_1 + (H + 0)] \\ &= H + (D_1 \cup \{0\}) \\ &= H + D \\ &= G. \end{aligned}$$

We already know that A, B and $A + B$ are non-periodic. Suppose that g is a period of C. If $g \in H$, then g must be a period of both $M_1 + N$ and $M + N_1$. Now M_1, N_1 are non-periodic. If $g = k + l$, $k \in K$, $l \in L$, then, since the sum $K + L$ is direct, it follows that k is a period of M_1 and l is a period of N. Thus $k = 0$ and $l = g \in N$. Similarly, g being a period of $M + N_1$ implies that $g \in M$. Since $M \cap N = \{0\}$, it follows that $g = 0$. Now suppose that $g \notin H$, that is, $g = h + d$, where $h \in H$, $d \in D_1$. Then $g + M_1 + N$ must equal $M + N_1 + d$ and so $h + M_1 + N = M + N_1$. Now, as above, $M_1 + N$ and $M + N_1$ are periodic but have no common period. Thus $h + M_1 + N = M + N_1$ is impossible. It follows that C is non-periodic. ∎

We have shown that

$$Z(p^3q^2), \quad Z(p^2q^2r), \quad Z(p^2qrs), \quad Z(pqrst)$$

are k-bad for $k = 2, 3$. Here the numbers p, q, r, s, t are assumed to be distinct primes. Note that $\nu\big(|C|\big) = 3$ in the above factorizations and $|C|$ is not a prime power, that is, $|C|$ involves at least two distinct primes.

EXAMPLE 3.2 Let G be a group of type $Z(9) \oplus Z(8)$ with basis elements x, y, where $|x| = 9$, $|y| = 8$. Let $H = \langle x, 2y\rangle$, $D = \{0, y\}$. Clearly $G = D + H$ is a factorization of D. Further, H is a direct sum of the subgroups $K = \langle x\rangle$ and $L = \langle 2y\rangle$. Here $|K| = 9$, $|L| = 4$ are composite numbers. Let

$$M = \langle 3x\rangle, \quad N = \langle 4y\rangle, \quad A = \{0, x, 2x\}, \quad B = \{0, 2y\}.$$

Note that $K = A + M$, $N = B + N$ are factorizations. Next choose the non-zero elements

$$a \in A, \quad b \in B, \quad m \in M, \quad n \in N.$$

Namely let

$$a = x, \quad b = 2y, \quad m = 6x, \quad n = 4y.$$

Form $M_1 = \{0, 3x, 6x + 2y\}$ from $M = \{0, 3x, 6x\}$ by replacing $m = 6x$ by $m+b = 6x+2y$. Form $N_1 = \{0, 4y+x\}$ from $N = \{0, 4y\}$ by replacing $n = 4y$ by $n + a = 4y + x$. Let

$$\begin{aligned} D_1 &= D \setminus \{0\} = \{y\}, \\ C &= (M_1 + N) \cup (M + N_1 + D_1). \end{aligned}$$

Then $G = A + B + C$ is a factorization of G. ∎

EXAMPLE 3.3 The element $ax + by$ of G in Example 3.2 (on page 42) can be identified by the coefficients (a, b). So the elements of G are all the pairs (a, b), $0 \le a \le 8$, $0 \le b \le 7$. The first components are added up modulo 9 and the second components are added up modulo 8. With this notation

$$\begin{aligned} A &= \{00, 10, 20\}, \\ B &= \{00, 02\}, \\ M &= \{00, 30, 60\}, \\ N &= \{00, 04\}, \\ M_1 &= \{00, 30, 62\}, \\ N_1 &= \{00, 14\}, \\ D_1 &= \{10\}. \end{aligned}$$

Using these,

$$C = [\{00, 30, 62\} + \{00, 04\}] \cup [\{00, 30, 60\} + \{00, 14\} + \{10\}].$$

Thus

$$C = \{00, 30, 62, 04, 34, 66, 10, 40, 70, 24, 54, 74\}.$$

∎

EXAMPLE 3.4 The group G in Example 3.2 (on page 42) can be taken

to be $Z(72)$. In this case $x = 8$, $y = 9$ must hold. Now

$$\begin{aligned} A &= \{0, 8, 16\}, \\ B &= \{0, 18\}, \\ M &= \{0, 24, 48\}, \\ N &= \{0, 36\}, \\ M_1 &= \{0, 24, 48 + 18\}, \\ N_1 &= \{0, 36 + 8\}, \\ D_1 &= \{1\}. \end{aligned}$$

Then

$$C = \big(\{0, 24, 66\} + \{0, 36\}\big) \cup \big(\{0, 24, 48\} + \{0, 44\} + \{1\}\big),$$

that is,

$$C = \{0, 24, 66, 36, 60, 30, 1, 25, 49, 45, 69, 21\}.$$

□

THEOREM 3.5

If G contains a proper subgroup that is a direct sum of two subgroups of composite order and $\nu\big(|G|\big) = m \geq 5$, then G is k-bad for each $2 \leq k \leq m-2$.

PROOF The $\nu\big(|G|\big) = m = 5$ case is covered by Theorem 3.4 (on page 41), so we may assume that $\nu\big(|G|\big) = m \geq 6$ and proceed by induction on m. As G contains a proper subgroup that is a direct sum of two subgroups of composite order, it follows that the type of G cannot be $Z(p^m)$ or $Z(p^{m-1}q)$. There is a subgroup H of G with a prime index in G such that the type of H is not $Z(p^\alpha)$ or $Z(p^{\alpha-1}q)$. Now $\nu\big(|H|\big) = m - 1 \geq 5$ and H contains a proper subgroup that is a direct sum of two subgroups of composite order. By the inductive assumption, H is k-bad for each $2 \leq k \leq m - 3$. Now, by Theorem 3.3 (on page 40), G is both k-bad and $(k + 1)$-bad. □

We shall see later that the groups not covered here are k-good. We also note that $\nu\big(|C|\big) \geq 3$ and that $|C|$ must involve at least two distinct prime factors.

EXERCISE 3.1 Let A be a subset of the finite abelian group G.

(a) Show that if A is periodic, then it is periodic with a period of prime order.

(b) Use (a) to show that the sets A, C in Example 3.2 (on page 42) are not periodic.

□

EXERCISE 3.2 Carry out the construction in the proof of Theorem 3.4 (on page 41) when the cyclic group has order 180. □

3.2 Characters

In order to show that groups are good, certain techniques are needed. We present these in this section.

A character χ of a finite abelian group G is a mapping from G to the multiplicative group of roots of unity such that $\chi(a+b) = \chi(a)\chi(b)$ for all $a, b \in G$. So χ is a homomorphism from an additive abelian group to a multiplicative abelian group. The equations $\chi(0) = \chi(0+0) = \chi(0)\chi(0)$ give that $\chi(0) = 1$. The kernel of χ is defined by

$$\mathrm{Ker}\chi = \{a \in G : \chi(a) = 1\}$$

and is a subgroup of G. The unity character maps every element in G to 1.

If A is a subset of G, we define the image under χ of A by

$$\chi(A) = \sum_{a \in A} \chi(a).$$

If A is the empty set, then define $\chi(A)$ to be 0. Of course, if χ is the unity character, then $\chi(A) = |A|$. We define the annihilator of A by

$$\mathrm{Ann}(A) = \{\chi : \chi(A) = 0\}.$$

If there is a g in G for which $\chi(g) \neq 1$, then from $\chi(G+g) - \chi(G) = 0$ one obtains that $\big(\chi(g) - 1\big)\chi(G) = 0$ and thus that $\chi(G) = 0$ for all non-unity characters χ of G. If A, B are subsets of G such that $A + B$ is a direct sum, then $\chi(A+B) = \chi(A)\chi(B)$ for all characters χ of G.

If g is a generator element of G and $|g| = n$, then

$$\big(\chi(g)\big)^n = \chi(ng) = \chi(0) = 1$$

and so $\chi(g)$ is an (n)th root of unity. Conversely, if ρ is an (n)th root of unity, then we may define a character χ of G by setting $\chi(kg) = \rho^k$. Thus the number of distinct characters of G is equal to $|G| = n$. If χ_1 and χ_2 are characters of G, then their point-wise product given by $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$ for all $a \in G$ is also a character of G. Characters of G form a group $\mathcal{G}$ with respect to this operation. Because $\chi(a)$ is a complex number of modulus 1, the inverse of χ is the conjugate of χ, that is, $\chi^{-1} = \overline{\chi}$, where $\overline{\chi}(a) = \overline{\chi(a)}$ for all $a \in G$.

If χ_1 and χ_2 are distinct characters of G, then $\chi_1\overline{\chi}_2$ is not the unity character and so

$$\begin{aligned} 0 &= \sum_{a\in G} \chi_1\overline{\chi}_2(a) \\ &= \sum_{a\in G} \chi_1(a)\overline{\chi_2(a)}. \end{aligned}$$

Thus the $n \times n$ matrix $\big[\chi(a)\big]$, where the rows are indexed by the characters χ of G and the columns by the elements a of G, has linearly independent rows and so is non-singular. (The linear independence is meant over the field of complex numbers.)

A is a multiset from G if, for each $g \in G$, g occurs in A with multiplicity $\lambda_A(g)$. Of course, if A is a subset of G, then $\lambda_A(g) = 1$ for $g \in A$ and $\lambda_A(g) = 0$ for $g \notin A$. Clearly λ_A is a function from G to the set of non-negative integers. For a multiset A of G we define

$$\chi(A) = \sum_{g\in G} \lambda_A(g)\chi(g).$$

THEOREM 3.6

If A and B are multisets from a group G, then $A = B$ if and only if $\chi(A) = \chi(B)$ for all characters χ of G.

PROOF If $A = B$, then $\lambda_A(g) = \lambda_B(g)$ for each $g \in G$ and so $\chi(A) = \chi(B)$ for all characters χ of G. Conversely, let $\chi(A) = \chi(B)$ for all characters χ of G. Then

$$\sum_{g\in G} \lambda_A(g)\chi(g) = \sum_{g\in G} \lambda_B(g)\chi(g),$$

that is,

$$\sum_{g\in G} \chi(g)[\lambda_A(g) - \lambda_B(g)] = 0.$$

Hence $[\lambda_A(g) - \lambda_B(g)]$, $g \in G$ is a solution of a homogeneous system of linear equations. Since the matrix $\big[\chi(g)\big]$ is non-singular, it follows that $\lambda_A(g) = \lambda_B(g)$ for all $g \in G$ and so that $A = B$. (Here linear independence means linear independence over the field of complex numbers.) ∎

Let $\mathcal{G}$ be the group of characters of G and let ε be the unity character of G, that is, the identity element of $\mathcal{G}$.

THEOREM 3.7

Let $A_1, \ldots, A_k$ be subsets of the finite abelian group G. Then $A_1 + \cdots + A_k$ is a factorization of G if and only if the following two conditions hold:

(i) $|A_1|\cdots|A_k| = |G|$.

(ii) $\mathrm{Ann}(A_1) \cup \cdots \cup \mathrm{Ann}(A_k) = \mathcal{G} \setminus \{\varepsilon\}$.

PROOF Let $A_1 + \cdots + A_k = G$ be a factorization of G. Then, for each character χ,

$$\begin{aligned}\chi(A_1 + \cdots + A_k) &= \chi(A_1)\cdots\chi(A_k)\\ &= \chi(G).\end{aligned}$$

The unity character here implies that $|A_1|\cdots|A_k| = |G|$. Each non-unity character leads to $\chi(A_1)\cdots\chi(A_k) = 0$ and so to $\chi(A_i) = 0$ for some i. Thus $\mathrm{Ann}(A_1) \cup \cdots \cup \mathrm{Ann}(A_k)$ is equal to the set of all non-unity characters of G.

Conversely, if $|A_1|\cdots|A_k| = |G|$ and $\mathrm{Ann}(A_1) \cup \cdots \cup \mathrm{Ann}(A_k) = \mathcal{G} \setminus \{\varepsilon\}$, then $\chi(A_1 + \cdots + A_k) = \chi(G)$ for all characters χ of G. It follows from Theorem 3.6 (on page 46) that $A_1 + \cdots + A_k = G$, as required. □

THEOREM 3.8

Let A be a subset and let h be an element of the finite abelian group G. The following two statements are equivalent:

(i) *h is a period of A.*

(ii) *$\chi(h) \neq 1$ implies $\chi(A) = 0$ for each character χ of G.*

PROOF Suppose h is a period of A. This means that $h \neq 0$ and $A+h = A$. Choose a character χ of G. Applying χ to the equation $A + h = A$ gives that $\chi(A)\chi(h) = \chi(A)$, which is equivalent to $\chi(A)\big[1-\chi(h)\big] = 0$. Plainly $\chi(h) \neq 1$ implies $\chi(A) = 0$.

Next suppose that $\chi(h) \neq 1$ implies $\chi(A) = 0$ for each character χ of G. We will show that $A + h = A$ holds by verifying that $\chi(A)\chi(h) = \chi(A)$ holds for each character χ of G. If $\chi(h) = 1$, then this equation holds. If $\chi(h) \neq 1$, then $\chi(A) = 0$ and again the equation holds. □

EXERCISE 3.3 Use Theorem 3.8 (on page 47) to show that $A = \{0, 8, 16\}$, $B = \{0, 18\}$ are not periodic subsets of $Z(72)$. □

THEOREM 3.9

Let H be a subgroup and let A be a non-empty subset of a finite abelian group G. The following are equivalent:

(i) $\mathrm{Ann}(H) \subseteq \mathrm{Ann}(A)$.

(ii) *There is a subset B of G such that $A = H + B$, where the sum is direct.*

PROOF Suppose $A = H + B$, where the sum $H + B$ is direct. Let $\chi \in \mathrm{Ann}(H)$. Then $\chi(A) = \chi(H)\chi(B) = 0$ and so $\chi \in \mathrm{Ann}(A)$.

Conversely, let $\mathrm{Ann}(H)$ be contained in $\mathrm{Ann}(A)$. Let $h \in H$. Let χ be any character of G. Then $\chi(h+A) = \chi(h)\chi(A)$. If $\chi(h) = 1$, then $\chi(h+A) = \chi(A)$. If $\chi(h) \neq 1$, then, since H is a group and the restriction of χ to H is not the unity mapping, it follows that $\chi(H) = 0$. Therefore $\chi(A) = 0$ and so

$$\begin{aligned}\chi(h + A) &= \chi(h)\chi(A)\\ &= \chi(A).\end{aligned}$$

By Theorem 3.6 (on page 46), it follows that $h + A = A$. Choose an element $a \in A$. Then $h + (A - a) = A - a$. As $0 \in (A - a)$, it follows that $h \in (A - a)$ and so $H \subseteq (A - a)$ and then $H + a \subseteq A$. Let $A_1 = A \setminus (H + a)$. Then $\chi(H) = 0$ implies that $\chi(A_1) = 0$. If $A_1 = \emptyset$, then $A = H + a$ and the result holds with $B = \{a\}$. We assume that $A_1 \neq \emptyset$ and proceed by induction on $|A|$. Choose $a_1 \in A_1$ and let $A_2 = A_1 - a_1$. As $|A_2| = |A_1| < |A|$ by the inductive assumption, the result holds for A_2 and so there is a B_2 such that $A_2 = H + B_2$. Then

$$[A \setminus (H + a)] - a_1 = H + B_2$$

or, equivalently,

$$A = [(H + B_2) + a_1] \cup (H + a).$$

Now

$$\begin{aligned}A &= [(H + B_2) + a_1] \cup (H + a)\\ &= [H + (B_2 + a_1)] \cup (H + a)\\ &= H + [(B_2 + a_1) \cup \{a\}],\end{aligned}$$

as required. ∎

THEOREM 3.10

Let H, K be subgroups of G and let A be a non-empty subset of G. The next two statements are equivalent:

(i) $\mathrm{Ann}(H) \cap \mathrm{Ann}(K) \subseteq \mathrm{Ann}(A)$.

(ii) *There exist subsets B, C of G such that $A = (H + B) \cup (K + C)$, where the sums $H + B$ and $K + C$ are direct and the union is disjoint.*

PROOF If $A = (H + B) \cup (K + C)$, as in the statement of the theorem, then $\chi(A) = \chi(H)\chi(B) + \chi(K)\chi(C)$. Therefore, for all such characters χ, $\chi(H) = \chi(K) = 0$ implies that $\chi(A) = 0$.

Suppose now that $\mathrm{Ann}(H) \cap \mathrm{Ann}(K) \subseteq \mathrm{Ann}(A)$. Let $h \in H$, $k \in K$. Consider the multisets $A \cup (A - h - k)$ and $(A - h) \cup (A - k)$. Let χ be a character of G. Then

$$\chi\big(A \cup (A - h - k)\big) = \chi(A)\big(1 + \overline{\chi(h)\chi(k)}\big)$$

and

$$\chi\big((A - h) \cup (A - k)\big) = \chi(A)\big(\overline{\chi(h)} + \overline{\chi(k)}\big).$$

If either $\chi(h) = 1$ or $\chi(k) = 1$, then the two expressions are equal. If $\chi(h) \neq 1$ and $\chi(k) \neq 1$, then $\chi(H) = \chi(K) = 0$ and so $\chi(A) = 0$. Once again the two expressions are equal. By Theorem 3.6 (on page 46), it follows that

$$A \cup (A - h - k) = (A - h) \cup (A - k).$$

Let $a \in A$. Then

$$(A - a) \cup \big[(A - a) - h - k\big] = \big[(A - a) - h\big] \cup \big[(A - a) - k\big].$$

Now $0 \in (A - a)$. Therefore $0 \in \big[(A - a) - h\big]$ or $0 \in \big[(A - a) - k\big]$, that is, $h \in (A - a)$ or $k \in (A - a)$. So if $K \not\subseteq (A - a)$, it follows that $H \subseteq (A - a)$. Similarly, if $H \not\subseteq (A - a)$, it follows that $K \subseteq (A - a)$. By symmetry we may assume that H is contained in $(A-a)$, that is, $H+a \subseteq A$. Let $A_1 = A\backslash(H+a)$. Then $\chi(H) = \chi(K) = 0$ implies that $\chi(A_1) = 0$. If $A_1 = \emptyset$, then $A = H + a$ and the result holds with $B = \{a\}$ and $C = \emptyset$. We assume that $A_1 \neq \emptyset$ and proceed by induction on $|A|$. Choose $a_1 \in A_1$ and let $A_2 = A_1 - a_1$. As $|A_2| = |A_1| < |A|$ by the induction assumption, the result holds for A_2 and so there exist B_2, C_2 such that $A_2 = (H + B_2) \cup (K + C_2)$, with direct sums and a disjoint union, as required. Then

$$\big[A \setminus (H + a)\big] - a_1 = (H + B_2) \cup (K + C_2)$$

or, equivalently,

$$A = \{[(H + B_2) \cup (K + C_2)] + a_1\} \cup (H + a).$$

Now

$$\begin{aligned}
A &= \{[(H + B_2) \cup (K + C_2)] + a_1\} \cup (H + a) \\
&= \{[(H + B_2) + a_1] \cup [(K + C_2) + a_1]\} \cup (H + a) \\
&= [(H + B_2) + a_1] \cup [(K + C_2) + a_1] \cup (H + a) \\
&= [(H + B_2) + a_1] \cup (H + a) \cup [(K + C_2) + a_1] \\
&= [H + (B_2 + a_1)] \cup (H + a) \cup [K + (C_2 + a_1)] \\
&= \{H + [(B_2 + a_1) \cup \{a\}]\} \cup [K + (C_2 + a_1)],
\end{aligned}$$

as required, since $A_1 \cap (H + a) = \emptyset$. ∎

We illustrate by an example that this result does not extend to the three subgroup case.

EXAMPLE 3.5 Let G be the modulo 30 additive group. Let

$$H = \langle 15 \rangle, \quad K = \langle 10 \rangle, \quad L = \langle 6 \rangle.$$

Set

$$A = \big((L+1) \cup K\big) \setminus (H+10).$$

Then $A = \{0, 1, 7, 13, 19, 20\}$. Clearly

$$\mathrm{Ann}(H) \cap \mathrm{Ann}(K) \cap \mathrm{Ann}(L) \subseteq \mathrm{Ann}(A).$$

Suppose that A can be represented in the form

$$A = (H+B) \cup (K+C) \cup (L+D),$$

where the unions are disjoint and the sums are direct. Considering the cardinalities we have

$$|A| = |H||B| + |K||C| + |L||D|.$$

Now, as

$$|A| = 6, \quad |H| = 2, \quad |K| = 3, \quad |L| = 5,$$

this reduces to

$$6 = 2|B| + 3|C| + 5|D|.$$

It follows that $0 \le |B| \le 3$, $0 \le |C| \le 2$, $0 \le |D| \le 1$ and so there are at most $(4)(3)(2) = 24$ choices for $|B|$, $|C|$, $|D|$. An inspection reveals that the only possible choices for $(|B|, |C|, |D|)$ are $(0, 2, 0)$ and $(3, 0, 0)$. Therefore either $A = K + C$ or $A = H + B$. Neither of these is true as neither 10 nor 15 is a period of A. ∎

We see that, for a subset A and characters χ of a group G, the question of when $\chi(A) = 0$ will be important. We should note that this depends only on the kernel of χ.

THEOREM 3.11

Let A be a subset of a group G. Let χ_1, χ_2 be characters of G with $\mathrm{Ker}\chi_1 = \mathrm{Ker}\chi_2$. *Then $\chi_1(A) = 0$ if and only if $\chi_2(A) = 0$.*

PROOF Let $\mathrm{Ker}\chi_1 = \mathrm{Ker}\chi_2 = K$. Now G/K is a cyclic group. Let it have order m and generator $g + K$. Let $\chi_1(g) = \rho$, $\chi_2(g) = \sigma$. Since $mg \in K$, then $\chi_1(mg) = \rho^m = 1$, $\chi_2(mg) = \sigma^m = 1$. Since $rg \notin K$ for $1 \le r \le m-1$,

it follows that $\rho^r \neq 1$, $\sigma^r \neq 1$ and so ρ and σ are (m)th primitive roots of unity. Let

$$A = \bigcup_{j=1}^{s} \{\underbrace{k_j + r(j)g}_{a_j}\},$$

where $k_j \in K$ and $0 \leq r(j) \leq m-1$. Then

$$\chi_1(A) = \sum_{j=0}^{m-1} \rho^{r(j)} \quad \text{and} \quad \chi_2(A) = \sum_{j=0}^{m-1} \sigma^{r(j)}.$$

Since ρ and σ are primitive roots of unity of the same order, it follows that $\chi_1(A) = 0$ if and only if $\chi_2(A) = 0$. ∎

Here we are essentially using the fact that the (m)th cyclotomic polynomial is irreducible over the field Q of rationals. The (m)th cyclotomic polynomial $F_m(x)$ is the monic polynomial of degree $\phi(n)$, where $\phi(n)$ denotes Euler's totient function, whose zeros are the (m)th primitive roots of unity. It is a result of Kronecker that, if m and n are relatively prime positive integers, then $F_m(x)$ is irreducible over the field Q_n generated over Q by the (n)th roots of unity.

THEOREM 3.12

Let m and n be relatively prime positive integers. Then the (m)th cyclotomic polynomial $F_m(x)$ is irreducible over the field Q_n of (n)th roots of unity.

PROOF Let ρ be an (m)th primitive root of unity and σ an (n)th primitive root of unity. Let $G(x)$ be a polynomial with coefficients in Q_n such that $G(\rho) = 0$. In order to prove the result, it suffices to show that $G(\rho^d) = 0$ for all integers d relatively prime to m.

Let

$$G(x) = \sum_r a_r x^r,$$

where $a_r \in Q_n$ and so

$$a_r = \sum_s b_{r,s} \sigma^s,$$

where $b_{r,s} \in Q$. Then

$$0 = G(\rho) = \sum_r \sum_s b_{r,s} \sigma^s \rho^r.$$

Now there exists, since m and n are relatively prime, an integer $t(r,s)$ such that

$$t(r,s) \equiv s \pmod{n},$$
$$t(r,s) \equiv r \pmod{m}.$$

Then

$$\sum_r \sum_s b_{r,s}(\sigma\rho)^{t(r,s)} = 0.$$

Now $\rho\sigma$ is an (mn)th primitive root of unity. By the irreducibility of $F_{mn}(x)$ over Q it follows, for all integers d relatively prime to mn, that $(\rho\sigma)^d$ is a zero of

$$H(x) = \sum_r \sum_s b_{r,s} x^{t(r,s)}.$$

There exists c such that $1 + cn \equiv d \pmod{m}$. Then $\sigma^{1+cn} = \sigma$, $\rho^{1+cn} = \rho^d$ and $1 + cn$ is relatively prime to mn. Hence

$$\begin{aligned} 0 &= H\big((\rho\sigma)^{1+cn}\big) \\ &= \sum_r \sum_s b_{r,s}\big((\rho\sigma)^{1+cn}\big)^{t(r,s)} \\ &= \sum_r \sum_s b_{r,s}\sigma^{t(r,s)}(\rho^d)^{t(r,s)} \\ &= \sum_r \sum_s b_{r,s}\sigma^{s}(\rho^d)^{r} \\ &= G(\rho^d), \end{aligned}$$

which is the desired result. ∎

If A is a subset of a group $G = \langle g \rangle$ with $|g| = n$, then

$$A = \bigcup_{j=1}^{r} \{k(j)g\},$$

where $0 \le k(j) \le n - 1$. We associate with A the polynomial

$$A(x) = \sum_{j=1}^{r} x^{k(j)}.$$

Let χ be a character of G with $\chi(g) = \rho$. Then

$$\chi(A) = \sum_{j=1}^{r} \rho^{k(j)} = A(\rho).$$

If ρ is an (m)th primitive root of unity, then $\chi(A) = 0$ if and only if $A(\rho) = 0$, and this is so if and only if $F_m(x)$ divides $A(x)$ over the rationals. Thus the method involving group characters and the method involving cyclotomic polynomials are equivalent.

If p is a prime, then the (p^e)th primitive roots of unity are the complex numbers σ satisfying $\sigma^{p^e} = 1$ but for which $\sigma^{p^{e-1}} \ne 1$. It follows that

$$F_{p^e}(x) = \frac{(x^{p^e} - 1)}{(x^{p^{e-1}} - 1)}$$

$$= 1 + x^{p^{e-1}} + \cdots + x^{(p-1)p^{e-1}}.$$

Let $m = p^e n$, where p is a prime not dividing n. Then, if ρ is an (m)th primitive root of unity, we may write $\rho = \sigma\tau$, where σ is a (p^e)th primitive root of unity and τ a (n)th primitive root of unity. Then, as above, $A(\rho) = 0$ implies $\sum \rho^{k(j)} = 0$. Let

$$k(j) \equiv s(j) \pmod{p^e},$$
$$k(j) \equiv t(j) \pmod{n},$$

with $0 \leq s(j) \leq p^e - 1$, $0 \leq k(j) \leq n - 1$. Then

$$0 = \sum \rho^{k(j)} = \sum \sigma^{s(j)} \tau^{t(j)}.$$

By Theorem 3.11 (on page 50), it follows that $F_{p^e}(x)$ divides

$$P(x) = \sum \tau^{t(j)} x^{s(j)}$$

over Q_n. Since the degree of $P(x)$ is less than p^e, there exists $B(x)$ of degree less than p^{e-1} with $P(x) = F_{p^e}(x)B(x)$. From the form of $F_{p^e}(x)$ given above it follows that in $P(x)$ the coefficients of

$$x^s, x^{s+p^{e-1}}, \ldots, x^{s+(p-1)p^{e-1}}$$

in $P(x)$ are equal. This will turn out to be a useful result.

Let G be a finite abelian group. To a subset A of G we assign the subset

$$K = \bigcap_{\chi \in \mathrm{Ann}(A)} \mathrm{Ker}\chi.$$

Here the intersection is taken over all characters χ of G that annihilate A. Note that $\mathrm{Ker}\chi$ is a subgroup of G and consequently K is a subgroup of G. We call K the *Corrádi subgroup* of A.

LEMMA 3.1

Let G be a finite abelian group and let $G = A + B$ be a factorization. If the Corrádi subgroup of A is not equal to $\{0\}$, then B is periodic.

PROOF Let K be the Corrádi subgroup of A and assume that $K \neq \{0\}$. Choose a $g \in K \setminus \{0\}$. We will show that $B + g = B$. It is enough to show that $\chi(B + g) = \chi(B)$ holds for each character χ of G. The equation $\chi(B)\chi(g) = \chi(B)$ plainly holds when $\chi(B) = 0$ or $\chi(g) = 1$. So let us suppose that $\chi(B) \neq 0$ and $\chi(g) \neq 1$. Now χ is not the principal character of G. Applying χ to the factorization $G = A + B$ gives that $0 = \chi(A)\chi(B)$. As $\chi(B) \neq 0$, it follows that $\chi(A) = 0$, that is, $\chi \in \mathrm{Ann}(A)$, and so we get the contradiction that $\chi(g) = 1$. □

Let p be a prime and let G be a group of type $Z(p^{\alpha(1)}) \oplus \cdots \oplus Z(p^{\alpha(n)})$, where $\alpha(1) \geq \cdots \geq \alpha(n) \geq 1$. The p power $p^{\alpha(1)}$ is called the *exponent* of G. The order of each element of G divides the exponent.

LEMMA 3.2

Let p be a prime and let G be a finite abelian p-group whose exponent is q. Let A be a normalized subset of G such that $|A|$ is a divisor of $|G|$ and $|A| > 2$. Set

$$g = (q/p)\Big[\sum_{a\in A} a\Big].$$

Then g is an element of the Corrádi subgroup of A.

PROOF We would like to show that $\chi(A) = 0$ implies $\chi(g) = 1$ for each character χ of G. Let χ be a character of G for which

$$0 = \chi(A) = \sum_{a\in A} \chi(a).$$

There is a (p^β)th primitive root of unity ρ such that each $\chi(a)$ is a power of ρ. Say $\chi(a) = \rho^{\gamma(a)}$ for each $a \in A$. Obviously, p^β is a divisor of q and consequently $\rho^q = 1$. By the remark after the proof of Theorem 3.12 (on page 51),

$$\begin{aligned}\{\chi(a) \ : \ a \in A\} &= \bigcup_{i=1}^{t} \rho^{\delta(i)}\{1, \rho^{p^{\beta-1}}, \rho^{2p^{\beta-1}}, \ldots, \rho^{(p-1)p^{\beta-1}}\} \\ &= \{\rho^{\delta(i)}\rho^{jp^{\beta-1}} \ : \ 1 \leq i \leq t, \ 0 \leq j \leq p-1\}.\end{aligned}$$

Using this we compute $\chi(g)$. First we deal with the case when p is odd:

$$\begin{aligned}\chi(g) &= \prod_{i=1}^{t}\prod_{j=0}^{p-1}\Big[\rho^{\delta(i)}\rho^{jp^{\beta-1}}\Big]^{q/p} \\ &= \prod_{i=1}^{t}\Big[\big(\rho^{\delta(i)}\big)^{(q/p)p}\prod_{j=0}^{p-1}\big(\rho^{jp^{\beta-1}}\big)^{q/p}\Big] \\ &= \prod_{i=1}^{t}\big(\rho^q\big)^{\delta(i)}\big(\rho^{p^{\beta-1}(p-1)p/2}\big)^{q/p} \\ &= \prod_{i=1}^{t}\big(\rho^q\big)^{p^{\beta-1}(p-1)/2} \\ &= 1,\end{aligned}$$

as required.

Let us turn to the $p = 2$ case. Note that now $\rho^{p^{\beta-1}} = -1$. Further note that as $2t = |A|$ divides $|G|$, it follows that $2t$ is a power of 2. As $2t > 2$, t must be even:

$$\begin{aligned}\chi(g) &= \prod_{i=1}^{t}\left[\rho^{\delta(i)}(+1)\rho^{\delta(i)}(-1)\right]^{q/2} \\ &= \prod_{i=1}^{t}\left(\rho^{2\delta(i)}\right)^{q/2}\prod_{i=1}^{t}(-1)^{q/2} \\ &= \prod_{i=1}^{t}\left(\rho^{q}\right)^{\delta(i)} \\ &= 1.\end{aligned}$$

This completes the proof. ∎

COROLLARY 3.1

Let p be a prime and let G be a finite abelian p-group whose exponent is q. Let $G = A + B$ be a normalized factorization of G, where $|A| > 2$. Set

$$d = \sum_{a\in A} a.$$

If $|d| = q$, then B is periodic.

PROOF Let $g = (q/p)d$. As $|d| = q$, it follows that $g \neq 0$. By Lemma 3.2 (on page 54), B is periodic. ∎

3.3 Replacement

It is often useful to be able to replace one factor by another in a factorization. A subset A of a group G is said to be *replaceable* by a subset B of G if, whenever $A + C = G$ is a factorization of G, so also is $B + C = G$.

THEOREM 3.13

If A is a direct factor of a finite abelian group G and B is a subset of G such that $|A| = |B|$ and $\mathrm{Ann}(A) \subseteq \mathrm{Ann}(B)$, then A is replaceable by B.

PROOF Let $G = A + C$ be a factorization of G. Consider the set or possible multiset, $B + C$. We will show that $\chi(A + C) = \chi(B + C)$ for

each character χ of G. Then, by Theorem 3.7 (on page 46), it follows that $A + C = B + C$, that is, $B + C$ is a set of not just a multiset from G. Let χ be a non-unity character of G. Applying χ to the factorization $G = A + C$ we get

$$\begin{aligned} 0 &= \chi(G) \\ &= \chi(A + C) \\ &= \chi(A)\chi(C). \end{aligned}$$

It follows that either $\chi(A) = 0$ or $\chi(C) = 0$. As $\chi(A) = 0$ implies $\chi(B) = 0$, we get $\chi(B+C) = \chi(B)\chi(C) = 0$ and so $\chi(A+C) = \chi(B+C)$. Let χ be the unity character of G. Applying χ to the factorization $G = A + C$ gives that

$$\begin{aligned} |G| &= \chi(G) \\ &= \chi(A + C) \\ &= \chi(A)\chi(C) \\ &= |A||C|. \end{aligned}$$

As $|A| = |B|$ it follows that

$$\begin{aligned} |A||C| &= |B||C| \\ &= \chi(B)\chi(C) \\ &= \chi(B + C). \end{aligned}$$

This shows that $\chi(A + C) = \chi(B + C)$. □

We give one application of this result.

THEOREM 3.14

Let A be a subset and H a subgroup of a finite abelian group G such that $|A| = |H| < |A \cap H| + (1/2)|H|$. Then A is replaceable by H.

PROOF Let $\chi(A) = 0$, where χ is a character of G. If $\chi(H) \neq 0$, then, since H is a subgroup, $\chi(h) = 1$ for all $h \in H$. Now, as $|A| = |H|$, $|A \cap H| > (1/2)|A|$. Let $|A \cap H| = k$, $|A| = l$. Then $k > l - k$. Then

$$\begin{aligned} 0 &= \chi(A) \\ &= \sum_{a \in A \cap H} \chi(a) + \sum_{a \in A \setminus H} \chi(a) \\ &= k + \sum_{i=1}^{l-k} \chi(a_i), \end{aligned}$$

where $A \setminus H = \{a_1, \ldots, a_{l-k}\}$. However, this is impossible since $\chi(a_i)$ is a root of unity and so

$$k = \left| \sum_{i=1}^{l-k} \chi(a_i) \right|$$

$$\begin{aligned} &\leq \sum_{i=1}^{l-k} |\chi(a_i)| \\ &< l-k. \end{aligned}$$

Hence $\chi(A) = 0$ implies that $\chi(H) = 0$ and so A is replaceable by H. □

Let $G = A + B$ be a factorization of G. Then each $g \in G$ may be expressed as

$$g = a + b, \quad a \in A, \quad b \in B.$$

We call a the *A-component* of g and we denote it by $(g)_A$. Similarly, we call b the B-component of g and we denote it by $(g)_B$. We should note here that we are working with a fixed factorization of G, that is, each of $(g)_A$, $(g)_B$ depends on both A and B. If G is a direct sum of its subgroups H and K such that $|H|$ is a power of the prime p and $|K|$ is relatively prime to p, then H is called the *p-component* of G.

THEOREM 3.15

Let $G = A + B$ be a factorization of the abelian group G. Then, for each $g \in G$, we have that $\{(g + a)_A : a \in A\} = A$.

PROOF Let $a_1, a_2 \in A$ be such that $(g + a_1)_A = (g + a_2)_A$. Then, from

$$\begin{aligned} g + a_1 &= (g + a_1)_A + (g + a_1)_B, \\ g + a_2 &= (g + a_2)_A + (g + a_2)_B, \end{aligned}$$

we deduce that $a_1 + (g + a_2)_B = a_2 + (g + a_1)_B$. It follows that $a_1 = a_2$. Hence $\{(g + a)_A : a \in A\} = A$. □

If A is a subset of an abelian group G and k is an integer, then we denote the set $\{ka : a \in A\}$ by kA.

THEOREM 3.16

If $G = A + B$ is a factorization of the finite abelian group G, then so is $G = (-A) + B$.

PROOF Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$ be such that $-a_1 + b_1 = -a_2 + b_2$. Then $a_2 + b_1 = a_1 + b_2$. Then $a_1 = a_2$ and $b_1 = b_2$. Therefore the sum $(-A) + B$ is direct. Then

$$\begin{aligned} \big|(-A) + B\big| &= \big|(-A)\big||B| \\ &= |A||B| \\ &= |G|. \end{aligned}$$

It follows that $G = (-A) + B$ is a factorization. ∎

The next exercise is related to alternative proofs of Theorem 3.16 (on page 57).

EXERCISE 3.4 Let A, B be subsets of a finite abelian group G.

(a) Show that the sum $A+B$ is direct if and only if $(A-A)\cap(B-B) = \{0\}$. Show that if $|G| \leq |A+B|$, then $G \subseteq (A+B)$.

(b) Use (a) to show that A can be replaced by $-A$.

(c) Use Theorem 3.13 (on page 55) to show that A can be replaced by $-A$.

∎

THEOREM 3.17
If A is a direct factor of a finite abelian group G and k is an integer relatively prime to $|A|$, then A is replaceable by kA.

PROOF Let $|A| = n$ and let p be a prime that does not divide n. We claim that, for each $g \in G$, the subset

$$\{(g + pa)_A : a \in A\}$$

is equal to A. Let $a' \in A$ and consider the number of solutions of

$$(g + x_1 + \cdots + x_p)_A = a' \tag{3.1}$$

with all $x_i \in A$. Let us choose $x_1, \ldots, x_{p-1}$ arbitrarily and set $h = g + x_1 + \cdots + x_{p-1}$. By Theorem 3.15 (on page 57), $(h + x_p)_A = a'$ can be solved for x_p uniquely. Thus there are n^{p-1} solutions of (3.1). Now, from any given solution we may obtain other solutions by permuting the list $x_1, \ldots, x_p$. Let $y_1, \ldots, y_s$ be all the distinct elements among $x_1, \ldots, x_p$ and let $r_1, \ldots, r_s$ denote the number of occurrences of $y_1, \ldots, y_s$ among $x_1, \ldots, x_p$. The number of such permutations of $x_1, \ldots, x_p$ is

$$\frac{p!}{(r_1!)\cdots(r_s!)}.$$

This number is divisible by p, unless $x_1 = \cdots = x_p$, in which case $s = 1$, $r_1 = p$. Now p does not divide n^{p-1}. Hence at least one solution with $x_1 = \cdots = x_p = a$, say, occurs. Then $(g + pa)_A = a'$.

Next we would like to establish that in the equation $(g + pa)_A = a'$ the element a is uniquely determined by g and a'. To do so let $C(a')$ be the set of all a for which $(g + pa)_A = a'$. We have already seen that $C(a') \neq \emptyset$. Note

that $a' \neq a''$ implies that $C(a') \cap C(a'') = \emptyset$. Indeed, if $a \in C(a') \cap C(a'')$, then $a' = (g + pa)_A$ and $a'' = (g + pa)_A$. This leads to the contradiction that $a' = a''$.

Hence $pa_1 = pa_2$ with $a_1, a_2 \in A$ implies that $a_1 = a_2$. Suppose that $pa_1 + b_1 = pa_2 + b_2$ with $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Then there exists $a \in A$, $b \in B$ such that $pa_1 - b_2 = pa_2 - b_1 = a + b$. Hence $a = (-b + pa_1)_A$, $a = (-b + pa_2)_A$. It follows that $a_1 = a_2$ and so that $pa_1 = pa_2$, $b_1 = b_2$. Thus the sum $pA + B$ is direct and $|pA| = |A|$. Therefore $pA + B = G$, and this is a factorization.

By repeating this argument, the desired result holds for any positive integer k relatively prime to n. The result for negative integers k then follows from Theorem 3.16 (on page 57). ∎

Let a group G be the direct sum of two subgroups H, K of relatively prime orders. Then, for each subset A of G, we define

$$(A)_H = \{(a)_H : a \in A\},$$
$$(A)_K = \{(a)_K : a \in A\}.$$

We note that if $|G| = nm$, where n, m are relatively prime, then there are unique subgroups of order n and m, respectively, and G is their direct sum.

THEOREM 3.18

If a finite abelian group G is a direct sum of subgroups H, K of relatively prime orders and a direct factor A of G is such that $|A|$ divides $|H|$, then A is replaceable by $(A)_H$.

PROOF Let $|H| = m$, $|K| = n$. Since m and n are relatively prime, there exists k such that $kn \equiv 1 \pmod{m}$. Then, since $|A|$ divides m, kn is relatively prime to $|A|$. By Theorem 3.17 (on page 58), A may be replaced by knA. Let $a \in A$. Then

$$\begin{aligned} kna &= kn[(a)_H + (a)_K] \\ &= kn[(a)_H] + kn[(a)_K] \\ &= (a)_H. \end{aligned}$$

Therefore A is replaceable by $(A)_H$. ∎

We note that Theorem 3.18 (on page 59) implies that the H-components of the elements of A are distinct.

THEOREM 3.19

If a finite abelian group G is a direct sum of subgroups H, K of relatively

prime orders and $G = A + B$ is a factorization where $|A| = |H|$, $|B| = |K|$, then $G = H + B = A + K$.

PROOF Since $(A)_H \subseteq H$ and $|(A)_H| = |A| = |H|$, it follows that $(A)_H = H$. Similarly we have that $(B)_K = K$. The result then follows by Theorem 3.18 (on page 59). □

Notes

(1) We make some remarks on the non-cyclic case. Theorem 3.1 (on page 38) and its proof do not depend on the group being cyclic. Theorem 3.2 (on page 40) fails if H has index 2 in G and all elements of H have order 2. In all the other cases the proof still holds, but in the index 2 case we must choose h to be not of order 2 when replacing $a \in A$ by $a + h$. Of course if H has index 2 in an elementary 2-group, all subsets A of order 2 and with $0 \in A$ are subgroups. For this reason Theorem 3.3 (on page 40) holds except for elementary 2-groups. The construction of non-periodic subsets A, B, $A + B$, C with $G = A + B + C$ still works except in the cases where K or L is an elementary group of order 4. Again Theorems 3.4 (on page 41) and 3.5 (on page 44) fail if either of the subgroups of composite order is elementary of order 4. For this reason we cannot give best possible results for general k or for types of orders of factors in the non-cyclic case.

(2) The constructions used here are due to N. G. de Bruijn [10]. G. Hajós [50] described how certain 3-dimensional cube tilings helped him to find bad factorings for cyclic groups. The groups are required to have three generators, two of which have to have composite order. The smallest such cyclic group has order $(4)(9)(5) = 180$. N. G. de Bruijn improved on and extended these ideas. In fact, his constructions cover all but one bad factoring of finite abelian groups. The one missing bad factorization was provided by A. D. Sands [116].

(3) Almost all the results in Section 3.3 hold in the non-cyclic case. Only when the polynomial $A(x)$ is introduced are we specifically using the fact that G is cyclic. The group character methods apply in general, but the cyclotomic polynomial methods do not always apply.

(4) The irreducibility of the cyclotomic polynomials has a long history. C. F. Gauss [45] showed that $F_{17}(x)$ is irreducible over the field or rational numbers. This result was extended by his students to the $F_p(x)$ and $F_n(x)$ cases where p is a prime and n is any integer. Theorem 3.12 (on page 51) goes back to L. Kronecker [70].

(5) It was G. Hajós [49] who used cyclotomic polynomials to study factorizations of cyclic groups of prime power order. The idea of applying characters is developed in L. Rédei [107]. In connection with multiple factorization R.

M. Robinson [110] used characters systematically.

(6) The fact that tactically replacing factors in a factorization is a powerful tool to investigate factorizations was first recognized and exploited by L. Rédei [107].

Chapter 4

Periodic factorizations

4.1 Good factorizations

In this chapter we consider finite cyclic groups. In Chapter 3 we showed that for certain orders of factors bad factorizations arise and claimed in Section 3.1 that these results were best possible. In order to justify this claim, the cases where we must show that one factor is necessarily periodic are as follows:

(i) Each factor has either prime power order or order equal to the product of two primes.

(ii) One factor has arbitrary order but all the other factors have orders which are powers of the same prime.

Later in the chapter we shall obtain formulae involving chains of subgroups and of coset representatives that give rise to all factorizations satisfying these conditions. We shall also deduce for each positive integer k the family of all cyclic groups that possess the Hajós k-property.

We recall that we may use equivalently for a factor A that a character χ is in $\mathrm{Ann}(A)$ or that a cyclotomic polynomial $F_m(x)$ divides a polynomial $A(x)$ associated with A. If g is a generator of G, then here $\chi(g)$ must have order m. The polynomial $A(x)$ is obtained from

$$A = \bigcup_{i=1}^{k} \{r(i)g\}$$

as

$$A(x) = \sum_{i=1}^{k} x^{r(i)}.$$

We choose $r(i)$ with $0 \leq r(i) \leq |G| - 1$. By Theorem 3.11 (on page 50), it does not matter which generator we use for G nor which particular (m)th primitive root of unity we use for $\chi(g)$. In the case $m = |G|$, also equivalent is the condition that $\mathrm{Ker}\chi = \{0\}$.

THEOREM 4.1

Let a subset A of G be a direct factor of G and have prime power order. If $|G| = n$ and $F_n(x)$ divides $A(x)$, then A is periodic.

PROOF Let $|A| = p^f$, where p is prime. Since $|A|$ divides $|G|$, $|G| = p^e m$, where $e \geq f$ and p does not divide m. Let g be a generator of G. Now there exist subgroups H, K of G with $|H| = p^e$, $|K| = m$ and G is the direct sum of these subgroups. Then $g = h+k$, where $h \in H$, $k \in K$ and $H = \langle h \rangle$, $K = \langle k \rangle$. Let χ be a character such that $\chi(g)$ has order n. Then $F_n(x)$ divides $A(x)$ implies that $\chi(A) = 0$. Since $\chi(g)$ has order n, it follows that $\chi(h)$ has order p^e and $\chi(k)$ has order m. Let $\chi(h) = \rho$, $\chi(k) = \sigma$. Let

$$A = \bigcup_{i=1}^{p^f} \{r(i)h + s(i)k\},$$

where $0 \leq r(i) \leq p^e - 1$, $0 \leq s(i) \leq m - 1$.

Then

$$0 = \chi(A) = \sum_{i=1}^{p^f} \rho^{r(i)} \sigma^{s(i)}.$$

Now, by Theorem 3.18 (on page 59), the H-components of the elements of A are distinct. Now

$$(A)_H = \bigcup_{i=1}^{p^f} \{r(i)h\}$$

and so the integers $r(i)$ are distinct. Since $F_{p^e}(x)$ is irreducible over the field generated by the (m)th roots of unity, it follows that $F_{p^e}(x)$ divides

$$\sum_{i=1}^{p^e} x^{r(i)} \sigma^{s(i)}. \tag{4.1}$$

Since $0 \leq r(i) \leq p^e - 1$, it follows that the other factors have degree less than p^{e-1}. Hence the coefficients of x^r and $x^{r+p^{e-1}}$ in (4.1) are equal. Since x^r, for given r, can occur once only, it follows that if $rh + sk$ occurs in A, so does $(r + p^{e-1})h + sk$. It follows that $p^{e-1}h$ is a period of A. ∎

We should note that the conditions that $F_n(x)$ divides $A(x)$ and that A has prime power order dividing $|G|$ are not, on their own, sufficient to show that A is periodic. (The division of polynomials is meant over the field of rationals.)

EXAMPLE 4.1 Let $G = Z(30)$. Let

$$A = \{0, 1, 11, 15, 21\}.$$

Then $|A| = 5$ and

$$A(x) = 1 + x + x^{11} + x^{15} + x^{21}$$

$$= 1 + x^{15} + x(1 + x^{10} + x^{20}).$$

Since $F_{30}(x)$ divides both

$$1 + x^{15} = \frac{1 - x^{30}}{1 - x^{15}}$$

and

$$1 + x^{10} + x^{20} = \frac{1 - x^{30}}{1 - x^{10}},$$

it follows that $F_{30}(x)$ divides $A(x)$. (The division of polynomials is meant over the field of rationals.) Clearly A is not periodic. In this case we may take $H = \langle h \rangle = \langle 6 \rangle$ and $K = \langle k \rangle = \langle 5 \rangle$. Then

$$A = \{0h + 0k, h + 5k, h + k, 0h + 3k, h + 3k\},$$

$$\chi(A) = (1 + \sigma^3) + \rho(\sigma^5 + \sigma + \sigma^3) = 0.$$

In this case the integers $r(i)$ are not distinct and so zero coefficients can arise as sums of powers of σ. Here $\rho = \chi(h)$ and $\sigma = \chi(k)$ are primitive (5)th and (6)th roots of unity, respectively. □

COROLLARY 4.1

In any factorization of a cyclic group of prime power order one factor is always periodic.

We should note that exactly one factor is periodic. The unique subgroup of prime order must be a subgroup of the group of periods of any periodic factor. This cannot happen for two factors, as then their sum could not be direct.

THEOREM 4.2

Let G be cyclic group of order $p^e q^f$, where p and q are distinct primes. Let B be a subset of order pq such that $\chi(B) = 0$, where χ is a character of G with $\mathrm{Ker}\chi = \{0\}$. *Then B is periodic.*

PROOF G has subgroups H, K of orders p^e, q^f, respectively, and $G = H + K$. Let $H = \langle h \rangle$, $K = \langle k \rangle$. Let $P = \langle p^{e-1}h \rangle$ and $Q = \langle q^{f-1}k \rangle$. The condition for a character χ of G that $\mathrm{Ker}\chi = \{0\}$ is equivalent to the conditions that $\chi(h)$ has order p^e and $\chi(k)$ has order q^f. In turn, these conditions are equivalent to

$$\chi(p^{e-1}h) \neq 1, \quad \chi(q^{f-1}k) \neq 1$$

and so to the conditions that

$$\chi(P) = 0, \quad \chi(Q) = 0.$$

Thus $\chi(P) = \chi(Q) = 0$ implies that $\chi(B) = 0$. So we may apply Theorem 3.10 (on page 48) to conclude that there exist subsets E, F such that

$$B = (P + E) \cup (Q + F),$$

where the sums are direct and the union is disjoint. Now from $|B| = pq$, $|P| = p$, $|Q| = q$ it follows that $pq = p|E| + q|F|$. Note that p divides $|F|$ and q divides $|E|$, and so $1 = |E|/q + |F|/p$. From this it follows that either $|E| = q$, $|F| = 0$ or $|E| = 0$, $|F| = p$. Hence either $B = P + E$ or $B = Q + F$. In each case B is periodic. □

We note that we do not need any condition here stating that B is a direct factor of G. However, we have a strong restriction on the order of G. Example 4.4 (on page 73) will show that some such restriction is needed even if B is a direct factor of G.

EXERCISE 4.1 Without the restriction that B is a direct factor of G the reader may like to give an example in $Z(30)$ such that $|B| = 10$, $F_{30}(x)$ divides $B(x)$ and B is not periodic. (Hint: Choose B to be the following set.)

$$B = \{0, 1, 2, 3, 12, 13, 15, 16, 22, 23\}.$$

□

COROLLARY 4.2

If G is a cyclic group of order $p^e q^f$, where p and q are distinct primes, then, in any factorization of G in which each factor has either order a prime power or order pq, one factor must be periodic.

PROOF This follows immediately from Theorems 4.1 (on page 63) and 4.2 (on page 65). □

This is the special case of (i) (on page 63) for groups of this order. Before proceeding to the general case, we present an elementary result that is used in its proof.

LEMMA 4.1

If $\alpha, \beta, \gamma, \delta$ are complex numbers of the same modulus and $\alpha + \beta = \gamma + \delta$, then one of the following must hold true:

$$\begin{array}{lllll} \text{(i)} & \alpha = -\beta, & \gamma = -\delta, \\ \text{(ii)} & \alpha = \gamma, & \beta = \delta, \\ \text{(iii)} & \alpha = \delta, & \beta = \gamma. \end{array}$$

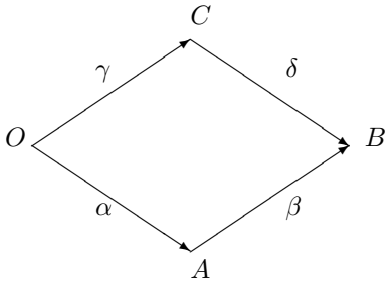

FIGURE 4.1: The Argand diagram of a vector rhombus.

PROOF Suppose that (i) and (ii) do not hold true. In an Argand diagram let $\overrightarrow{OA}$ represent α and $\overrightarrow{AB}$ represent β. Since $\alpha + \beta \neq 0$, B is not at O. Let $\overrightarrow{OC}$ represent γ. Since $\alpha \neq \gamma$, C is not at A. Since $\alpha + \beta = \gamma + \delta$, $\overrightarrow{CB}$ must represent δ. (See Figure 4.1 on page 67.) Since $|\alpha| = |\beta| = |\gamma| = |\delta|$, we have that $|\overrightarrow{OA}| = |\overrightarrow{AB}| = |\overrightarrow{OC}| = |\overrightarrow{CB}|$. Hence O, A, B, C is a rhombus and so $\alpha = \delta$, $\beta = \gamma$. Thus, as required, (iii) holds true. ∎

THEOREM 4.3

Let G be a finite cyclic group. If in a factorization of a group G each factor has either prime power order or order that is the product of two distinct primes, then one factor is periodic.

PROOF Let $A_1 + \cdots + A_l = G$ be the factorization. We may assume that the factorization is normalized. Then, if χ is a character of G such that $\mathrm{Ker}\chi = \{0\}$ and $\chi(A_i) = 0$, where A_i has prime power order, it follows by Theorem 4.1 (on page 63), that this factor is periodic. Thus we may assume that all such factors A_i have order $p(i)q(i)$, where $p(i)$, $q(i)$ are distinct primes. By reordering the factors, if necessary, we may assume that $\chi(A_i) = 0$ for $1 \leq i \leq u$ and that this does not hold for $i > u$.

Let $(G)_p$ denote the p-component of G for each p dividing $|G|$. By Theorem 3.18 (on page 59), A_i may be replaced by B_i, where B_i consists of the $((G)_{p(i)} + (G)_{q(i)})$-components of elements of A_i, $1 \leq i \leq l$. This gives the factorization

$$B_1 + \cdots + B_u + A_{u+1} + \cdots + A_l = G.$$

Since $\chi(A_i) \neq 0$, $i > u$, it follows that $\chi(B_j) = 0$ for at least one value of j, $1 \leq j \leq u$. We may assume that $\chi(B_1) = 0$. For convenience we write $|B_1| = pq$.

Let η be the restriction of χ to $(G)_p + (G)_q$. Then $\mathrm{Ker}\chi = \{0\}$ implies that $\mathrm{Ker}\eta = \{0\}$ and $B_1 \subseteq (G)_p + (G)_q$ implies that $\eta(B_1) = \chi(B_1) = 0$. By Theorem 4.2 (on page 65), it follows that B_1 is periodic.

Let $|G| = p^e q^f m$, where m is not divisible by p or by q. Then G has a generating set $\{a, b, c\}$, where a, b, c have orders p^e, q^f, m, respectively. Since $\mathrm{Ker}\chi = \{0\}$, it follows that $\chi(a) = \alpha$, $\chi(b) = \beta$, $\chi(c) = \gamma$ are primitive roots of unity of orders p^e, q^f, m, respectively. Now B_1 has a period of order p or q. We assume that B_1 has a period of order p and so that $B_1 = P + D$, where $P = \langle p^{e-1}a \rangle$. Then D is a subset of $(G)_p + (G)_q$ of order q. Let

$$D = \bigcup_{j=0}^{q-1} \{r(j)a + s(j)b\}.$$

From the form of P we may assume that $0 \le r(j) \le p^{e-1} - 1$. By Theorem 3.18 (on page 59), the elements of B_1 and so also of D are distinct. From $B_1 = P + D$ it follows that

$$A_1 = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{q-1} \{(ip^{e-1} + r(i))a + s(j)b + e(i,j)c\},$$

where $0 \le s(j) \le q^f - 1$, $0 \le e(i,j) \le m - 1$. When performing arithmetical operations we shall treat the coefficients $e(i,j)$ as integers modulo m. Then $\chi(A_1) = 0$ implies that

$$\sum_{i=0}^{p-1} \sum_{j=0}^{q-1} \alpha^{ip^{e-1}+r(j)} \beta^{s(j)} \gamma^{e(i,j)} = 0.$$

It follows that the polynomial

$$\sum_{i=0}^{p-1} \sum_{j=0}^{q-1} x^{ip^{e-1}+r(j)} \beta^{s(j)} \gamma^{e(i,j)} = 0,$$

obtained by replacing α by x, is divisible by $F_{p^e}(x)$. Thus, as before, the coefficients of

$$x^r, x^{r+p^{e-1}}, \ldots, x^{r+(p-1)p^{e-1}}$$

in the polynomial are equal for each r, $0 \le r \le p^{e-1} - 1$. Hence

$$\begin{aligned} \sum_{r(j)=0} \beta^{s(j)} \gamma^{e(0,j)} &= \sum_{r(j)=1} \beta^{s(j)} \gamma^{e(1,j)} \\ &\vdots \\ &= \sum_{r(j)=p-1} \beta^{s(j)} \gamma^{e(p-1,j)}. \end{aligned}$$

Let

$$G_{i,i'}^{(r)}(x) = \sum_{r(j)=i} x^{s(j)}\gamma^{e(i,j)} - \sum_{r(j)=i'} x^{s(j)}\gamma^{e(i',j)}.$$

Then, since β is a zero of this polynomial, it follows that $F_{q^f}(x)$ divides $G_{i,i'}^{(r)}(x)$. As usual, this implies that the coefficients of

$$x^s, x^{s+q^{f-1}}, \ldots, x^{s+(q-1)q^{f-1}}$$

are equal, where $0 \le s \le q^{f-1}-1$. Now, since the elements in D are distinct, the pairs $\big(r(j), s(j)\big)$ are also distinct, $0 \le j \le q-1$. Thus, for a given pair $(r, s+tq^{f-1})$, there either exists a unique j with $\big(r(j), s(j)\big) = (r, s+tq^{f-1})$ or else no such pair $\big(r(j), s(j)\big)$ exists at all. In the second case the coefficient in $G_{i,i'}^{(r)}(x)$ of $x^{s+(q-1)q^{f-1}}$ is equal to zero. In the first case this coefficient is $\gamma^{e(i,j)} - \gamma^{e(i',j)}$, where j is the value obtained above.

Suppose for given values of r, s that both situations arise. Then all coefficients of $x^{s+(q-1)q^{f-1}}$ must be zero for $0 \le t \le q-1$. Thus, for that t for which a solution j exists with $r(j) = r$, $s(j) = s + tq^{f-1}$, we must have that $\gamma^{e(i,j)} = \gamma^{e(i',j)}$ holds for all i, i'. So we have, for this j, that

$$e(0,j) = e(1,j) = \cdots = e(p-1,j).$$

If a solution exists for v values of t, this gives rise to v such values of j and so to vp terms in A_1. Since A_1 has pq terms, it follows that, for all other values r', s', there are also fewer than q values of t where a solution $r(j) = r'$, $s(j) = s' + tq^{f-1}$ occurs. It follows that all coefficients in $G_{i,i'}^{(r')}(x)$ are zero for all r', i, i'. Hence $\gamma^{e(i,j)} - \gamma^{e(i',j)}$ for all i, i', j. It follows that $e(i,j) = e(i',j)$ and so that $p^{e-1}a$ is a period of A_1.

So we may now suppose that a pair (r,s) exists such that all q values of $(r, s+tq^{e-1})$, $0 \le t \le q-1$, do occur as $\big(r(j), s(j)\big)$, $0 \le j \le q-1$. This gives rise to all pq elements in A_1. Since $0 \in A_1$, we may choose $(r,s) = (0,0)$. It follows that B_1 is the subgroup of order pq. So we may rewrite A_1 as

$$A_1 = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{q-1} \{ip^{e-1}a + jq^{f-1}b + e(i,j)c\}.$$

$B_1 = P + D$ now gives that $D = \langle q^{f-1}b \rangle$ is the subgroup of order q. So the pairs $\big(r(j), s(j)\big)$ that arise are $(0, jq^{f-1})$, $0 \le j \le q-1$. Thus

$$G_{i,i'}^{(0)}(x) = \sum_{j=0}^{q-1} x^{jq^{f-1}}\gamma^{e(i,j)} - \sum_{j=0}^{q-1} x^{jq^{f-1}}\gamma^{e(i',j)}.$$

It follows that

$$\gamma^{e(i,j)} - \gamma^{e(i',j)} = \gamma^{e(i,j')} - \gamma^{e(i',j')}$$

for all i, i', j, j', where $0 \le i, i' \le p-1$, $0 \le j, j' \le q-1$.

This is an equation involving complex numbers of modulus 1 and so by Lemma 4.1 (on page 66), only the following three possibilities arise for each quadruple i, i', j, j':

$$\begin{array}{lll} e(i,j) = e(i,j') & \text{and} \quad e(i',j) = e(i',j') & \text{(C1)} \\ e(i,j) = e(i',j) & \text{and} \quad e(i,j') = e(i',j') & \text{(C2)} \\ e(i,j) = e(i',j') + m/2 & \text{and} \quad e(i',j) = e(i,j') + m/2. & \text{(C3)} \end{array}$$

This third case (C3), in which

$$\gamma^{e(i,j)} = -\gamma^{e(i',j')},$$

can arise only if m is even.

Firstly let us assume that only the cases (C1) and (C2) occur. If, for a given i, we have that $e(i,j) = e(i,j')$ for all j, j', then it follows from (C1) that $e(i',j) = e(i',j')$ for all i', j, j'. From this it follows that $q^{f-1}b$ is a period of A_1.

Now we may suppose that r, r' and s, s' exist such that neither (C1) nor (C2) holds for these pairs. Then m must be even and, by (C3), $e(r,s) = e(r',s') + m/2$ and $e(r',s) = e(r,s') + m/2$. Let $\gamma^{e(r,s)} = \rho$, $\gamma^{e(r',s)} = \sigma$. Then, as $\gamma^{m/2} = -1$, we have that $\gamma^{e(r',s')} = -\rho$, $\gamma^{e(r,s')} = -\sigma$. Since neither (C1) nor (C2) is satisfied for these pairs, it follows that $\rho \ne \pm\sigma$, that is, $\rho^2 \ne \sigma^2$. Since m is even, it follows that pq is odd. By Theorem 3.17 (on page 58), it follows that A_1 may be replaced by $2A_1$. Suppose that $\chi(2A_1) = 0$. Now this replacement of A_1 by $2A_1$ leads to a replacement of a, b, c by $2a$, $2b$, $2c$ and so of α, β, γ by α^2, β^2, γ^2, respectively. Since p and q are odd, α^2 and β^2 are still primitive roots of unity of orders p^e and q^f, respectively. Thus in the formulae arising from $2A_1$, divisibility by $F_{p^e}(x)$ and $F_{q^f}(x)$ still occurs as for those arising from A_1. Hence for r, r' and s, s' it will follow that

$$\gamma^{2e(r,s)} - \gamma^{2e(r',s)} = \gamma^{2e(r,s')} - \gamma^{2e(r',s')}.$$

This shows that $\rho^2 - \sigma^2 = \sigma^2 - \rho^2$, which implies that $\rho^2 = \sigma^2$. This is false. Therefore $\chi(2A_1) \ne 0$.

We may now proceed by induction on u. We have the factorization

$$G = 2A_1 + A_2 + \cdots + A_u + \cdots + A_l.$$

If $u = 1$, we must have $\chi(2A_1) = 0$ and so, from above, either (C1) or (C2) holds in each case for A_1. Thus A_1 is periodic. So, if A_1 is not periodic, in this factorization we have only $u-1$ factors A_i with $\chi(A_i) = 0$. By the inductive assumption, some of these factors A_i, $2 \le i \le u$ must be periodic. ∎

We now present an example in which condition (C3) does arise. In particular, this will show that $\chi(A_1) = \chi(B_1) = 0$ does not necessarily imply that A_1 is periodic.

EXAMPLE 4.2 Let p, q be distinct odd primes and let m be an even integer greater than 2 and not divisible by p or by q. Let G be generated by elements a, b, c of orders p, q, m, respectively. Let $I = \{i : 0 \le i \le p-1\}$ be a disjoint union of non-empty sets I_1, I_2 with $0 \in I_1$. Let $J = \{j : 0 \le j \le q-1\}$ be a disjoint union of non-empty sets J_1, J_2 with $0 \in J_1$. In the notation used in the proof of Theorem 4.3 (on page 67) we define $e(i,j)$ as follows:

$$e(i,j) = \begin{cases} 0, & \text{if} \quad (i,j) \in I_1 \times J_1, \\ m/2, & \text{if} \quad (i,j) \in I_2 \times J_2, \\ 1, & \text{if} \quad (i,j) \in I_2 \times J_1, \\ 1 + m/2, & \text{if} \quad (i,j) \in I_1 \times J_2. \end{cases}$$

Let

$$A_1 = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{q-1} \{ia + jb + e(i,j)c\}.$$

Then $|A_1| = pq$ and B_1 is the subgroup $\langle a, b\rangle$. Hence $\chi(B_1) = 0$, where χ is defined as above. Now

$$\begin{aligned} \chi(A_1) &= \sum_{i\in I_1} \alpha^i \sum_{j\in J_1} \beta^j - \sum_{i\in I_2} \alpha^i \sum_{j\in J_2} \beta^j + \\ &\quad \gamma\Big(\sum_{i\in I_2} \alpha^i \sum_{j\in J_1} \beta^j - \sum_{i\in I_1} \alpha^i \sum_{j\in J_2} \beta^j\Big) \\ &= \sum_{i\in I} \alpha^i \sum_{j\in J_1} \beta^j - \sum_{i\in I_2} \alpha^i \sum_{j\in J} \beta^j + \\ &\quad \gamma\Big(\sum_{i\in I} \alpha^i \sum_{j\in J_1} \beta^j - \sum_{i\in I_1} \alpha^i \sum_{j\in J} \beta^j\Big). \end{aligned}$$

Now

$$\sum_{i\in I} \alpha^i = \sum_{j\in J} \beta^j = 0.$$

Hence $\chi(A_1) = 0$. Since $|A_1| = pq$ if A_1 is periodic, then either a or b is a period. From the definition of I_1 and I_2 there exists $i \in I_1$ such that $i+1 \in I_2$. Then $e(i,0) = 0$, $e(i+1,0) = 1$. Thus $ia \in A_1$ and $(i+1)a + c \in A_1$. Since the pairs (i,j) each occur only once in B_1, it follows that $(i+1)a \notin A_1$ and so a is not a period of A_1. By a similar argument b is not a period of A_1. Since $B_1 = \langle a, b\rangle$, it is easy to see that $A_1 + \langle c\rangle = G$. We may choose m to be a power of 2 or to be equal to $2r$, where r is an odd prime different from p and q, to obtain a factorization with factors of appropriate orders.

In this example $\chi(2A_1) \neq 0$ follows from the theory given in the proof of Theorem 4.3 (on page 67). It may also be seen directly since in $\chi(2A_1)$ we are replacing $\gamma^{m/2} = -1$ in $\chi(A_1)$ by $\gamma^m = 1$. The smallest example occurs in $Z(60)$ with $p = 3$, $q = 5$, $m = 4$. ∎

EXAMPLE 4.3 Let us choose $p = 3$, $q = 5$, $m = 4$ in Example 4.2 (on page 71). With this choice G is of type $Z(3) \oplus Z(5) \oplus Z(4)$ and

$$I = \{0, 1, 2\}, \quad J = \{0, 1, 2, 3, 4\}.$$

For the sake of definiteness let

$$\begin{aligned} I_1 &= \{0, 1\}, & I_2 &= \{2\}, \\ J_1 &= \{0, 1, 2, 3\}, & J_2 &= \{4\}. \end{aligned}$$

The values of $e(i, j)$ are the entries of the matrix

$$\begin{matrix} 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 \\ 1 & 1 & 1 & 1 & 2. \end{matrix}$$

Then the elements of A_1 are the following:

$$\begin{matrix} 000 & 010 & 020 & 030 & 043 \\ 100 & 110 & 120 & 130 & 143 \\ 201 & 211 & 221 & 231 & 242. \end{matrix}$$

The sum of the roots of unity

$$\begin{matrix} 1 & \beta & \beta^2 & \beta^3 & -\beta^4\gamma \\ \alpha & \alpha\beta & \alpha\beta^2 & \alpha\beta^3 & -\alpha\beta^4\gamma \\ \alpha^2\gamma & \alpha^2\beta\gamma & \alpha^2\beta^2\gamma & \alpha^2\beta^3\gamma & -\alpha^2\beta^4 \end{matrix}$$

is equal to $\chi(A_1)$. Augment this list with

$$\beta^4, -\beta^4, \alpha\beta^4, -\alpha\beta^4, \alpha^2\beta^4\gamma, -\alpha^2\beta^4\gamma.$$

Using the facts that

$$\begin{aligned} 0 &= (1 + \beta + \beta^2 + \beta^3 + \beta^4), \\ 0 &= (1 + \beta + \beta^2 + \beta^3 + \beta^4)\alpha, \\ 0 &= (1 + \beta + \beta^2 + \beta^3 + \beta^4)\alpha^2\gamma, \end{aligned}$$

we get that

$$\begin{aligned} \chi(A_1) &= -\beta^4\gamma - \beta^4 - \alpha\beta^4\gamma - \alpha\beta^4 - \alpha^2\beta^4 - \alpha^2\beta^4\gamma \\ &= -\beta^4(1 + \gamma) - \alpha\beta^4(1 + \gamma) - \alpha^2\beta^4(1 + \gamma) \\ &= -\beta^4(1 + \gamma)(1 + \alpha + \alpha^2) \\ &= 0. \end{aligned}$$

□

EXAMPLE 4.4 We may choose the group G in Example 4.3 (on page 72) to be $Z(60)$. In this case $a = 20$, $b = 12$, $c = 15$. Now the elements of A_1 are the following:

$$\begin{array}{rrrrr} 0 & 12 & 24 & 36 & 33 \\ 20 & 32 & 44 & 56 & 53 \\ 55 & 7 & 19 & 31 & 58. \end{array}$$

We know that A_1 has a complementer factor in G. Namely,

$$B_1 = \{0, 12, 24, 36, 48\}$$

is a direct factor of A_1 in G. From Example 4.2 (on page 71) we know that the polynomial

$$A_1(x) = \sum_{a \in A} x^a$$

is divisible by the cyclotomic polynomial $F_{6)}(x)$ over the field of rational numbers. ∎

We now present the result that covers case (ii) (on page 63).

THEOREM 4.4

Let G be a finite cyclic group. If $G = A_1 + \cdots + A_k + B$ is a factorization in which each factor A_i has order a power of a prime p, then one of the factors is periodic.

PROOF Let G have order $p^e m$, where m is not divisible by p. Then there are subgroups H, K of G of orders p^e, m, respectively, such that G is the direct sum of H and K. Let $H = \langle h \rangle$, where h has order p^e. Let $(A_i)_H = B_i$, $1 \leq i \leq k$. By Theorem 3.18 (on page 59), the subsets A_i may be replaced by B_i to give a factorization $G = B_1 + \cdots + B_k + B$. Let $c \in K$. Then $b_1 + \cdots + b_k + b \in H + c$, where $b_i \in B_i$, $b \in B$ if and only if $b \in H + c$, since $B_i \subseteq H$, $1 \leq i \leq k$. It follows that

$$B_1 + \cdots + B_k + \big(B \cap (H + c)\big) = H + c$$

and so that

$$B_1 + \cdots + B_k + \big((B - c) \cap H\big) = H.$$

It follows by Corollary 4.1 (on page 65) that exactly one of these factors is periodic and that the subgroup $P = \langle p^{e-1} h \rangle$ of order p is a group of periods of this factor.

Suppose first that none of the factors $B_1, \ldots, B_k$ is periodic. Then P is a subgroup of periods $(B - c) \cap H$ and so of $B \cap (H + c)$ for all $c \in K$. Now

$$B = \bigcup_{c \in K} \big[B \cap (H + c)\big],$$

as $H + K = G$. Hence P is a group of periods of B and B is periodic.

So we may now suppose that one of the first k factors, say B_1, is periodic. We note that this implies that $B_2, \ldots, B_k$ are not periodic. By Theorem 3.18 (on page 59), we have a factorization

$$G = A_1 + B_2 + \cdots + B_k + B.$$

Let χ be a character of G such that $\chi(h)$ has order p^e. Now $B_2, \ldots, B_k$ are subsets of H and if $\chi(B_i) = 0$ for any i, $2 \leq i \leq k$, then, by Theorem 4.1 (on page 63), the subset B_i is periodic. This is false. Hence, for all such characters χ of G, either $\chi(A_1) = 0$ or $\chi(B) = 0$. Let $\{\chi_i : i \in I\}$ be the set of all such characters with $\chi_i(A_1) = 0$. Let $L_i = \mathrm{Ker}\chi_i$. Since $\chi_i(h)$ has order p^e, it follows that $L_i \subset K$. Let

$$L = \bigcap_{i \in I} L_i.$$

Let us suppose that $L \neq \{0\}$. We should note that the condition that $\chi(h)$ has order p^e is equivalent to the condition that $\chi(p^{e-1}h) \neq 1$ and so to the condition that $\chi(P) = 0$. Let χ be a character such that $\chi(P) = \chi(L) = 0$. $\chi(P) = 0$ implies, by Theorem 4.1 (on page 63), that $\chi(B_i) \neq 0$, $2 \leq i \leq k$. $\chi(L) = 0$ implies that $\chi(L_i) = 0$ for each subgroup L_i containing L and so that $\chi(A_1) \neq 0$. Hence $\chi(P) = \chi(L) = 0$ implies that $\chi(B) = 0$. By Theorem 3.10 (on page 48), it follows that there exist subsets D, E such that $B = (P + D) \cup (L + E)$, where the sums are direct and the union is disjoint. Now there is a subset F such that $B_1 = P + F$ and the sum $B_1 + B$ is direct. It follows that D is the empty set and so $B = L + E$. Thus B is periodic with L as a group of periods.

Finally we may suppose that $L = \{0\}$. Now, since B_1 has $P = \langle p^{e-1}h \rangle$ as a group of periods, it follows that if rh occurs in B_1, so also does $(r + p^{e-1})h$. Let

$$A_1 = \bigcup \{r(j)h + d_j\},$$

where $0 \leq r(j) \leq p^{e-1} - 1$ and $d_j \in K$. Let $i \in I$. Then $\chi_i(A_1) = 0$ and $\chi_i(h) = \rho$, where ρ is a (p^e)th primitive root of unity. Then

$$\sum \rho^{r(j)} \chi_i(d_j) = 0.$$

Since $\chi_i(d_j)$ is an (m)th root of unity, it follows that $F_{p^e}(x)$ divides

$$\sum x^{r(j)} \chi_i(d_j)$$

over the (m)th cyclotomic field. As before, it follows that the coefficients of x^r and $x^{r+p^{e-1}}$ are equal. Since r and $r + p^{e-1}$ can occur once in the expression for B_1, and so in that for A_1, their coefficients are in the form $\chi_i(d)$ and $\chi_i(d')$ with $d, d' \in K$. Then

$$\chi_i(d - d') = \chi_i(d)\chi_i^{-1}(d') = 1.$$

Hence $d - d' \in L_i$. This is true for each i and so

$$d - d' \in \bigcap_{i \in I} L_i = \{0\}.$$

Hence $d = d'$. It follows that $p^{e-1}h$ is a period of A_1. ∎

We close the section with an open problem.

PROBLEM 4.1 Let G be a finite abelian group and let $G = B + A_1 + \cdots + A_n$ be a factorization of G, where each $|A_i|$ is a prime. Let p, q be distinct primes.

(1) If $|B| = p^2$ and the p-component of G is cyclic, does it follow that at least one of the factors $B, A_1, \ldots, A_n$ is periodic?

(2) If $|B| = pq$ and, further, the p-component and the q-component of G are cyclic, doest it follow that at least one of the factors $B, A_1, \ldots, A_n$ is periodic?

∎

4.2 Good groups

The results from Section 4.1 enable us now to determine for each number of factors k the groups that are k-good. This establishes the claim made earlier in Section 3.1 that all the bad groups had been given. We note that it follows from Theorem 3.3 (on page 40) that if a group G is k-good and a subgroup H admits factorizations with either k or $k-1$ factors occurring, then H is good of that order. Thus we need only consider borderline cases.

THEOREM 4.5

If p, q are distinct primes and G is a cyclic group of order $p^e q$, then G is k-good for all relevant k, that is, for $2 \leq k \leq e + 1$.

PROOF This follows immediately from Theorem 4.4 (on page 73). ∎

For the remaining groups we deal first with the case $k = 2$. By Theorems 3.4 (on page 41) and 4.5 (on page 75), we need only consider the cases where $\nu\big(|B|\big) \leq 4$.

THEOREM 4.6
If G is a finite cyclic group group such that $2 \leq \nu\big(|G|\big) \leq 4$, then G is 2-good.

PROOF By Theorem 3.3 (on page 40) we need only consider the case $\nu\big(|G|\big) = 4$. The groups not already covered are those of orders p^2q^2, p^2qr, $pqrs$, where p, q, r, s are distinct primes. If one factor has prime power order, the result follows by Theorem 4.4 (on page 73). Otherwise, each factor must have order equal to the product of two primes. The desired result then follows by Theorem 4.3 (on page 67). ∎

Thus the list of 2-good groups consists of the groups

$$Z(p^eq), \quad Z(p^2q^2), \quad Z(p^2qr), \quad Z(pqrs)$$

and all subgroups admitting two factors, where p, q, r, s are distinct primes. In other words, $Z(n)$ is a 2-good group if n is a divisor of the following numbers:

$$p^eq, \quad p^2q^2, \quad p^2qr, \quad pqrs$$

and big enough to allow two factors in the factorization of $Z(n)$.

We now turn to the case $k \geq 3$. By Theorem 3.5 (on page 44) we need only consider the cases $Z(p^eq)$, as above, and the cases $\nu(|G|) = k$ or $k + 1$.

THEOREM 4.7
If G is a finite cyclic group such that $k \leq \nu\big(|G|\big) \leq k + 1$, then G is k-good.

PROOF If $\nu\big(|G|\big) = k$, then every factor has prime order and the result follows from Theorem 4.3 (on page 67). If $\nu\big(|G|\big) = k + 1$, then all factors but one must have prime order while the remaining factor has order either the square of a prime or the product of two distinct primes. Again the result follows by Theorem 4.3 (on page 67). ∎

We note that for $k = 2$ the borderline case occurs with $\nu\big(|G|\big) = 4 = k + 2$, but for $k \geq 3$ it occurs with $\nu\big(|G|\big) = k + 1$. Thus the cases $k = 2$ and $k = 3$ have the same result.

One reason for studying which groups are good is that formulae exist for their factorizations. These formulae are given in terms of chains of subgroups and of complete sets of coset representatives for one subgroup modulo the next smaller subgroup in the chain.

The crucial idea is that from a factorization of a good group we obtain a factorization of a smaller group and then this process may be continued. We note that the fact that a group is good followed from Theorems 4.1 (on page 63), 4.3 (on page 67), or 4.4 (on page 73). So the formulae will hold for factorizations involving only factors of these orders.

Let G be a group and let $G = A_1 + \cdots + A_k$ be a factorization where one of these conditions on the orders of the factors is satisfied. Then one of the factors, say A_1, must be periodic and so, by Lemma 2.8 (on page 18), there is a subgroup H_1 and a subset B_1 such that $A_1 = H_1 + B_1$, where the sum is direct. Then $G = (H_1 + B_1) + A_2 + \cdots + A_k$ leads to the factorization

$$G/H_1 = (B_1 + H_1)/H_1 + (A_2 + H_1)/H_1 + \cdots + (A_k + H_1)/H_1.$$

Since $|B_1|$ divides $|A_1|$, the conditions on the orders of the factors are still satisfied. Thus the process may be repeated, obtaining at each stage a factorization of a group of smaller order. If H_1 is chosen to be the maximal possible, then, by Corollary 2.2 (on page 20), B_1 is not periodic and in the factorization of G/H_1 the factor $(B_1 + H_1)/H_1$ is not periodic. Thus one of the other factors must be periodic.

We have defined the composition of two subsets with respect to a function in Section 2.2. We need this concept here, but in a slightly modified form since we work here with normalized subsets. Let A, B be subsets of an abelian group G such that $0 \in A$, $0 \in B$ and let φ be a function from B to A with $\varphi(0) = 0$. We define a subset $A \circ_\varphi B$ by

$$\{\varphi(b) + b : b \in B\}.$$

We refer to $A \circ_\varphi B$ as the *composition* of A and B with respect to the function φ.

THEOREM 4.8

Let $k \geq 2$ be a fixed integer. Let G be a finite cyclic group and let

$$\{0\} \subseteq H_1 \subseteq \cdots \subseteq H_m = G$$

be a strictly ascending chain of subgroups. Let $D_1, \ldots, D_{m-1}$ be subsets, each containing zero, such that D_j is a complete set of coset representatives for H_{j+1} modulo H_j. Let subsets A_i, $1 \leq i \leq k$ satisfy

$$A_i = H_1 \overset{+}{\circ} (D_1 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots)),$$

where at each position where the symbol $\overset{+}{\circ}$ occurs $+$ is selected for one value of i and $\circ$ is selected for the $k-1$ remaining values. Then $G = A_1 + \cdots + A_k$ is a factorization.

In the formulae in the theorem we suppressed the functions φ. Of course, with each $\circ$ a function φ is associated. The statement is that, for each possible choice of the functions, $G = A_1 + \cdots + A_k$ is a factorization of G. Clearly one of the subsets A_i is periodic. So only periodic factorizations can be obtained by these formulae. Example 4.5 (on page 79) will present a particular case, so the reader might prefer to have a look at this before turning to the proof.

PROOF We proceed by induction on $\nu(|G|)$. Let $\nu(|G|) = 2$. Then $\{0\} \subseteq H_1 \subseteq H_2 = G$. Now

$$A_1 = H_1 + (D_1 \circ \{0\}), \quad A_2 = H_1 \circ (D_1 + \{0\}),$$

$$A_3 = H_1 \circ (D_1 \circ \{0\}), \ldots, A_k = H_1 \circ (D_1 \circ \{0\}).$$

Since $D_1 \circ \{0\} = \{0\}$, $A_1 = H_1$, $A_2 = H_1 \circ D_1$ and $A_3 = \{0\}, \ldots, A_k = \{0\}$. So A_2 is a complete set of coset representatives for G modulo H_1 and $G = A_1 + A_2 + A_3 + \cdots + A_k$ is a factorization, as required.

Now let $t = \nu(|G|) \geq 3$ and assume that the result holds for all groups K with $\nu(|K|) < t$. Now clearly $G = H_1 + D_1 + \cdots + D_{m-1}$ is a factorization. We may assume that

$$A_1 = H_1 + B_1, \quad A_2 = H_1 \circ B_2, \ldots, A_k = H_1 \circ B_k,$$

where the subsets $B_1, B_2, \ldots, B_k$ are contained in $D_1 + \cdots + D_{m-1}$ and depend on the choices of $+$ and $\circ$ in

$$D_1 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots)).$$

Let $\overline{g} = g + H_1$ denote the image of g in G under the natural projection from G onto G/H_1. For each subset B of G such that $H_1 + B$ is direct, let

$$\overline{B} = \{\overline{b} : b \in B\}.$$

Then $\overline{D}_1 = H_2/H_1$ and $\overline{D}_j$ is a complete set of coset representatives for H_{j+1}/H_1 modulo H_j/H_1 for $2 \leq j \leq k-1$. Now $\nu(|G/H_1|) < r$. So, by the inductive assumption,

$$G/H_1 = \overline{B}_1 + \cdots + \overline{B}_k$$

is a factorization. We note that if $A_1 = H_1$, then $B_1 = \{0\}$ and so $\overline{B}_1$ may be omitted here. Let $g \in G$. Then there exists $\overline{b}_j \in \overline{B}_j$ such that $\overline{g} = \overline{b}_1 + \cdots + \overline{b}_k$. Since $A_i = H_1 \circ B_i$ for $2 \leq i \leq k$, it follows that there exists $h_i \in H_1$ such that $h_i + b_i = a_i \in A_i$. Then, as $g = h + b_1 + \cdots + b_k$ for some $h \in H_1$, we have that

$$\begin{aligned} g &= h - h_2 - \cdots - h_k + b_1 + a_2 + \cdots + a_k \\ &\in A_1 + A_2 + \cdots + A_k. \end{aligned}$$

Also,

$$\begin{aligned} |G| &= |H_1||G/H_1| \\ &= |H_1||B_1| \cdots |B_k| \\ &= |A_1| \cdots |A_k|. \end{aligned}$$

Hence the sum is direct and $G = A_1 + A_2 + \cdots + A_k$ is a factorization.

The result follows by induction. ∎

EXAMPLE 4.5 We illustrate the $k = 3$, $m = 4$ special case of Theorem 4.8 (on page 77). The chain of subgroups now is

$$\{0\} \subseteq H_1 \subseteq H_2 \subseteq H_3 \subseteq H_4 = G.$$

D_1 is a complete set of representatives in H_2 modulo H_1. D_2 is a complete set of representatives in H_3 modulo H_2. D_3 is a complete set of representatives in H_4 modulo H_3. To get the formulae

$$\begin{aligned} A_1 &= H_1 + (D_1 \circ (D_2 + (D_3 \circ \{0\}))), \\ A_2 &= H_1 \circ (D_1 \circ (D_2 \circ (D_3 + \{0\}))), \\ A_3 &= H_1 \circ (D_1 + (D_2 \circ (D_3 \circ \{0\}))). \end{aligned}$$

we filled a 3 by 5 array writing H_1, D_1, D_2, D_3, $\{0\}$ in each row. We then inserted $+$ and $\circ$ signs into the gaps such that in each column the $+$ sign appears exactly once. There are 3^4 possible choices for the $+$ and $\circ$ signs. □

EXAMPLE 4.6 Let G be a group type $Z(2) \oplus Z(2) \oplus Z(2) \oplus Z(2)$ with basis elements x, y, z, u. Set

$$\begin{aligned} H_1 &= \langle x \rangle, & & \\ H_2 &= \langle x, y \rangle, & D_1 &= \{0, y\}, \\ H_3 &= \langle x, y, z \rangle, & D_2 &= \{0, z\}, \\ H_4 &= \langle x, y, z, u \rangle, & D_3 &= \{0, u\}. \end{aligned}$$

To compute $D_3 \circ \{0\}$ in the formulae in Example 4.5 (on page 79), we should consider a function $\varphi : \{0\} \to D_3$ with $\varphi(0) = 0$. There is only one choice for φ and so $D_3 \circ \{0\} = \{\varphi(0) + 0\} = \{0\}$. The new formulae for A_1, A_2, A_3 are

$$\begin{aligned} A_1 &= H_1 + (D_1 \circ (D_2 + \{0\})), \\ A_2 &= H_1 \circ (D_1 \circ (D_2 \circ D_3)), \\ A_3 &= H_1 \circ (D_1 + (D_2 \circ \{0\})). \end{aligned}$$

To evaluate $D_2 \circ D_3$ we need a function $\varphi : D_3 \to D_2$ with $\varphi(0) = 0$. As $\varphi(u)$ is either 0 or z, there are the following two choices for $D_2 \circ D_3 = \{\varphi(0 + 0, \varphi(u) + u\}$:

$$\{0, u\}, \quad \{0, z + u\}.$$

At this point the procedure forks into two branches. There are two sets of formulae for A_1, A_2, A_3:

$$\begin{aligned} A_1 &= H_1 + (D_1 \circ \{0, z\}), \\ A_2 &= H_1 \circ (D_1 \circ \{0, u\}), \\ A_3 &= H_1 \circ (D_1 + \{0\}), \\ A_1 &= H_1 + (D_1 \circ \{0, z\}), \\ A_2 &= H_1 \circ (D_1 \circ \{0, z + u\}), \\ A_3 &= H_1 \circ (D_1 + \{0\}). \end{aligned}$$

Let us continue to work only with the second set of formulae. To evaluate $D_1 \circ \{0, z\}$ we consider a function $\varphi : \{0, z\} \to D_1$ and get the following two possibilities for $D_1 \circ \{0, z\} = \{\varphi(0) + 0, \varphi(z) + z\}$:

$$\{0, z\}, \quad \{0, y + z\}.$$

Similarly, we have the following two possibilities for $D_1 \circ \{0, z + u\}$:

$$\{0, z + u\}, \quad \{0, y + z + u\}.$$

We end up with four sets of formulae for A_1, A_2, A_3. We continue to work only with the next one:

$$\begin{aligned} A_1 &= H_1 + \{0, y + z\}, \\ A_2 &= H_1 \circ \{0, z + u\}, \\ A_3 &= H_1 \circ D_1. \end{aligned}$$

The possible choices for $H_1 \circ \{0, z + u\}$ are

$$\{0, z + u\}, \quad \{0, x + z + u\}.$$

The possible choices for $H_1 \circ D_1$ are

$$\{0, y\}, \quad \{0, x + z\}.$$

There are four sets of formulae for A_1, A_2, A_3. We again choose only one branch to follow and we get

$$\begin{aligned} A_1 &= \{0, x, y + z, x + y + z\}, \\ A_2 &= \{0, z + u\}, \\ A_3 &= \{0, x + y\}. \end{aligned}$$

∎

EXERCISE 4.2 Let G be $Z(16)$ with generator element x. Set

$$\begin{aligned} H_1 &= \langle 8x \rangle, \\ H_2 &= \langle 4x \rangle, \quad & D_1 &= \{0, 4x\}, \\ H_3 &= \langle 2x \rangle, \quad & D_2 &= \{0, 2x\}, \\ H_4 &= \langle x \rangle, \quad & D_3 &= \{0, x\}. \end{aligned}$$

Carry out a similar computation to the one done in Example 4.6 (on page 79). ∎

EXERCISE 4.3 Let p be a prime and let G be a finite abelian p-group. Suppose $|H_i : H_{i+1}| = p$ holds in the chain of subgroups in Theorem 4.8 (on

page 77). Show that if in the formula for A_i the number of + signs is s, then $|A_i| = p^s$. ∎

We now show that if the conditions on the orders of factors given in Theorems 4.3 (on page 67) and 4.4 (on page 73) hold true then all such factorizations are obtained in this way.

THEOREM 4.9

Let G be a finite cyclic group. Let $G = A_1 + A_2 + \cdots + A_k$ be a factorization of G such that the orders of the factors satisfy at least one of the following:

(i) *Each factor has prime power order or order equal to the product of two distinct primes.*

(ii) *Each factor except possibly one has order equal to the power of a fixed prime p.*

Then there exists a chain of subgroups

$$\{0\} \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_m = G$$

and of complete sets of coset representatives D_j for H_{j+1} modulo H_j, $1 \leq j \leq m-1$, such that the sets A_i are given by the formulae

$$A_i = H_1 \overset{+}{\circ} (D_1 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots))),$$

where, at each position where the symbol $\overset{+}{\circ}$ occurs, + is chosen once and $\circ$ is chosen in the remaining $k-1$ places.

PROOF The proof is by induction on $\nu\big(|G|\big)$. Let $\nu\big(|G|\big) = 2$. Then $G = A_1 + A_2$, where each factor has prime order. It follows that one factor, say A_1, is periodic. Since A_1 has prime order and $0 \in A_1$, $A_1 = H_1$, for some subgroup H_1 of G, then $G = H_1 + A_2$ implies that $A_2 = D_1$ for some set D_1 of coset representatives for H_2 modulo H_1, where $H_2 = G$. Then

$$A_1 = H_1 = H_1 + (D_1 \circ \{0\}),$$
$$A_2 = D_1 = H_1 \circ (D_1 + \{0\}).$$

Thus the result holds in this smallest case.

Let $G = A_1 + A_2 + \cdots + A_k$, where the orders of these factors satisfy (i) or (ii). We make the inductive assumption that the result holds for all groups K with $\nu\big(|K|\big) < \nu\big(|G|\big)$. By Theorem 4.3 (on page 67) or Theorem 4.4 (on page 73) it follows that one factor, say A_1, is periodic. Let H_1 be the subgroup of periods of A_1. Then, by Lemma 2.8 (on page 18), $A_1 = H_1 + B_1$ for some subset B_1. If $A_1 = H_1$, we may omit the set B_1. We have that $G = H_1 + B_1 + A_2 + \cdots + A_k$.

Let the canonical projection from G to G/H_1 send $g \in G$ to $\overline{g} \in G/H_1$. For any subset A of G, let $\overline{A} = \{\overline{a} : a \in A\}$. If $H_1 + A$ is a direct sum, then $|\overline{A}| = |A|$. From above it follows that $G/H_1 = \overline{B}_1 + \overline{A}_2 + \cdots + \overline{A}_k$. Since $|B_1|$ divides $|A_1|$, it follows that the condition on the order of the factors still holds. By the inductive assumption, the result holds for such factorizations of G/H_1. So there is a chain of subgroups

$$\{0\} \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_m = G/H_1$$

and sets of coset representatives E_j, $2 \leq j \leq m$, for K_{j+1} modulo K_j. Then there exist subgroups H_j of G such that $K_j = H_j/H_1$ and there exist subsets D_j of G such that $\overline{D}_j = E_j$. Then D_j is a set of coset representatives for H_{j+1} modulo H_j, $2 \leq j \leq m$.

Now

$$\overline{B}_1 = K_2 \circ (D_2 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (E_{m-1} \overset{+}{\circ} \{0\}) \cdots)))$$

$$\overline{A}_i = K_2 \circ (E_2 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (E_{m-1} \overset{+}{\circ} \{0\}) \cdots)))$$

by the inductive assumption. Let $a_i \in A_i$. Then, from

$$\overline{a}_i \in K_2 \circ (E_2 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (E_{m-1} \overset{+}{\circ} \{0\}) \cdots))),$$

it follows that there exists $h_1 \in H_1$ such that $a_i + h_1$ belongs to

$$H_1 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots)).$$

Let D_1 be a set of coset representatives for H_2 modulo H_1. Then each $h_2 \in H_2$ may be represented as

$$h_2 = h_1' + d_1, \quad h_1' \in H_1, \quad d_1 \in D_1.$$

Hence

$$a_i + h_1 + h_1' \in D_1 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots)).$$

It follows that

$$a_i \in H_1 \circ (D_1 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots))).$$

Similarly we have that any $b_1 \in B_1$ is such that there exists $h_1'' \in H_1$ such that

$$b_1 + h_1'' \in D_1 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots)).$$

Therefore

$$A_1 = H_1 + B_1 = H_1 \circ (D_1 \overset{+}{\circ} (D_2 \overset{+}{\circ} (\cdots \overset{+}{\circ} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots))).$$

The result follows by induction. ∎

We note in these formulae that once the chain of subgroups H_j has been chosen, the choice of the sets D_j of coset representatives does not affect the

sets A_i obtained. This follows since, if C_j is any other such choice, then $H_j \circ C_j$ and $H_j \circ D_j$ give exactly the same subsets.

Also, if $+$ is chosen in the given set A_k at two successive places, then these two places may be put together and so the number of steps in the chain is reduced. This follows because

$$A + (B + C) = (A + B) + C$$

and

$$A \circ (B \circ C) = (A + B) \circ C.$$

So the summation of A and B occurs in every set A_i.

Using the observation above in the $k = 2$ case, one may assume that the $+$ and $\circ$ signs alternate in the formulae for A_1 and A_2. In fact, one may assume that

$$A_1 = H_1 + (D_1 \circ (\cdots \overset{+}{\circ} (D_{m-1} \overset{\circ}{+} \{0\}) \cdots))),$$
$$A_2 = H_1 \circ (D_1 + (\cdots \overset{\circ}{+} (D_{m-1} \overset{+}{\circ} \{0\}) \cdots))).$$

Therefore, in the $k = 2$ special case, one conveniently can use the following recursion:

$$\begin{array}{llll} U_{m-1} = D_{m-1}, & & V_{m-1} = \{0\}, & \\ U_{m-2} = D_{m-2} + V_{m-1}, & & V_{m-2} = D_{m-2} \circ U_{m-1}, & \\ \quad \vdots & & \quad \vdots & \\ U_1 & = D_1 + V_2, & V_1 & = D_1 \circ U_2, \\ A_1 & = H_1 + V_1, & A_2 & = H_1 \circ U_1. \end{array}$$

EXERCISE 4.4 Verify that if

$$A_1 = H_1 + (D_1 \circ (D_2 + (D_3 \circ \{0\}))),$$
$$A_2 = H_1 \circ (D_1 + (D_2 \circ (D_3 + \{0\}))),$$

then

$$\begin{array}{ll} U_3 = D_3, & V_3 = \{0\}, \\ U_2 = D_2 + V_3, & V_2 = D_2 \circ U_3, \\ U_1 = D_1 + V_2, & V_1 = D_1 \circ U_2, \\ A_1 = H_1 + V_1, & A_2 = H_1 \circ U_1. \end{array}$$

∎

EXERCISE 4.5 Verify that if

$$\begin{array}{ll} U_4 = D_4, & V_4 = \{0\}, \\ U_3 = D_3 + V_4, & V_3 = D_3 \circ U_4, \\ U_2 = D_2 + V_3, & V_2 = D_2 \circ U_3, \\ U_1 = D_1 + V_2, & V_1 = D_1 \circ U_2, \\ A_1 = H_1 + V_1, & A_2 = H_1 \circ U_1, \end{array}$$

then

$$A_1 = H_1 + (D_1 \circ (D_2 + (D_3 \circ (D_4 + \{0\})))),$$
$$A_2 = H_1 \circ (D_1 + (D_2 \circ (D_3 + (D_4 \circ \{0\})))).$$

□

THEOREM 4.10

Let G be a finite cyclic group. If G is a k-good group, then every factorization of G into k factors is given by the formulae in Theorem 4.9 (on page 81).

PROOF This follows since the proof that G is k-good depended on every factorization of G into k factors satisfying one of the conditions on the orders of factors used in Theorem 4.9 (on page 81). □

We now present some examples to illustrate the use of these formulae.

EXAMPLE 4.7 Let $G = Z(24)$ be presented as the integers modulo 24. Let

$$A = \{0, 10, 12, 22\},$$
$$B = \{0, 4, 5, 8, 13, 21\}.$$

Then it may be verified directly that $G = A + B$.

It is clear that A is periodic with group of periods $H_1 = \{0, 12\}$, but that B is not periodic. Then $A = H_1 + B_1$, where $B_1 = \{0, 10\}$. In this case, G/H_1 consists just of the integers modulo 12. So $\overline{B} = \{0, 4, 5, 8, 1, 9\}$. Then $\overline{B}$ is periodic with group of periods $\overline{H}_2 = \{0, 4, 8\}$ and $\overline{B} = \overline{H}_2 + \{0, 1\}$. Also $H_2 = \{0, 4, 8\} + \{0, 12\}$ is the required subgroup of G. The factor group G/H_2 is just integers modulo 4 and we have the factorization

$$\begin{aligned} G/H_2 &= \{0, 10\} + \{0, 1\} \\ &= \{0, 2\} + \{0, 1\}. \end{aligned}$$

Here $\{0, 2\}$ is a subgroup and $H_3 = H_2 + \{0, 2\} = \langle 2 \rangle$. Finally, $H_4 = G$. The sets of coset representatives are

$$D_1 = \{0, 4, 8\}, \quad D_2 = \{0, 2\}, \quad D_3 = \{0, 1\}.$$

Then

$$\begin{aligned} A &= \{0,12\} + (\{0,4,8\} \circ (\{0,2\} + (\{0,1\} \circ \{0\}))) \\ &= \{0,12\} + (\{0,4,8\} \circ \{0,2\}) \\ &= \{0,12\} + \{0,2+8\}, \\ B &= \{0,12\} \circ (\{0,4,8\} + (\{0,2\} \circ (\{0,1\} + \{0\}))) \\ &= \{0,12\} \circ (\{0,4,8\} + \{0,1+0\}) \\ &= \{0,12\} \circ \{0,4,8,1,5,9\} \\ &= \{0,4,5,8,1+12,9+12\}. \end{aligned}$$

We should note that $\overline{B}$ factorizes as the sum of subsets of orders 3 and 2 in G/H_1, but that this does not imply that B will factorize in G. Let $B = C+D$ with $|C| = 3$, $|D| = 2$. Since $0 \in B$, we may, as usual, assume that $0 \in C \cap D$. If D were to consist of two even integers, then we could not obtain three even and three odd integers in B. So we need to check only the cases $\{0,5\}$, $\{0,13\}$, $\{0,21\}$ for D. If $4 \notin C$, then one of 23, 9, 17 must be in B, which is false. Thus, though $\overline{B}$ factorizes, B itself does not. ∎

EXAMPLE 4.8 In how many ways may we factorize $Z(12)$ as $A + B$ with $|A| = 4$, $|B| = 3$ and $0 \in A \cap B$?

We may represent $Z(12)$ as the integers modulo 12. First let us suppose that A is a subgroup. Then we have the chain of subgroups

$$\{0\} \subseteq H_1 \subseteq H_2 = G,$$

where $H_1 = \langle 3 \rangle$, $D_1 = \{0,1,2\}$.

Then $B = H_1 \circ (D_1 + \{0\}) = H_1 \circ \{0,1,2\}$. Since $0 \in B$, we have $B = \{0, 1+h_1, 2+h_1'\}$ with $h_1, h_1' \in H_1$. Thus there are 16 choices for B.

Secondly, we may have that B is periodic and so that $B = H_1 = \langle 4 \rangle$. Then we have the chain

$$\{0\} \subseteq H_1 \subseteq H_2 = G,$$

where $D_1 = \{0,1,2,3\}$. We have $A = H_1 \circ D_1$ and so $A = \{0, 1+h_1, 2+h_1', 3+h_1''\}$ with $h_1, h_1', h_1'' \in H_1 = \langle 4 \rangle$. This gives 27 choices for A. However, one of these choices with $h_1 = 8$, $h_1' = 4$, $h_1'' = 0$ gives $A = \{0,9,6,3\} = \langle 3 \rangle$, and this is already covered in the first case. Thus there are 26 new choices for A.

Thirdly, we may have that A_1 is periodic but is not a subgroup. Then we have the chain

$$\{0\} \subseteq H_1 \subseteq H_2 \subseteq H_3 = G,$$

where

$$\begin{aligned} H_1 &= \langle 6 \rangle, & H_2 &= \langle 2 \rangle, \\ D_1 &= \{0,2,4\}, & D_2 &= \{0,1\}. \end{aligned}$$

Then

$$\begin{aligned} A &= \langle 6 \rangle + (\{0,2,4\} \circ (\{0,1\} + \{0\})), \\ B &= \langle 6 \rangle \circ (\{0,2,4\} + (\{0,1\} \circ \{0\})). \end{aligned}$$

Then

$$A = \{0, 6\} + (\{0, 2, 4\} \circ \{0, 1\}).$$

This gives three choices for A as $\{0, 6\}+\{0, 1\}$, $\{0, 6\}+\{0, 3\}$, or $\{0, 6\}+\{0, 5\}$. In the second choice, $A = \langle 3\rangle$ and this is already covered in the first case. So only two new choices arise for A. Also, $B = \{0, 6\} \circ \{0, 2, 4\}$. This gives four choices for B. Again one of these choices is $B = \{0, 2 + 6, 4 + 0\} = \langle 4\rangle$ and this has already been covered in the second case. So only three new choices for B occur. Thus there are six new choices altogether.

So $A + B$ may be found in $16 + 26 + 6 = 48$ ways. □

We say that two factorizations $G = A_1 + \cdots + A_k$ and $G = B_1 + \cdots + B_k$ are equivalent if there exist elements g_i and a reordering $B_{r(i)}$, $1 \le i \le k$ of the subsets B_i such that $A_i + g_i = B_{r(i)}$, $1 \le i \le k$. With the restriction that $0 \in A_i \cap B_i$ for all i, we will have $g_i = -a_i$ for some $a_i \in A_i$. We note that $A - g_1 = A - g_2$ if and only if $g_1 - g_2$ is either 0 or is a period of A. So the number of subsets equivalent to A in this way is equal to $|A|/|H|$, where H is the subgroup of periods of A.

EXAMPLE 4.9 If $G = Z(12)$, find the number of equivalence classes of factorizations of the form $G = A + B$ with $|A| = 4$, $|B| = 3$, and $0 \in A \cap B$.

From Example 4.8 (on page 85) we see that if A is a subgroup, there are 16 choices for B. In one of these B is a subgroup. The other 15 subsets give rise to 5 groups of 3 equivalent subgroups as $|B| = 3$. This gives 6 equivalence classes in all in this case.

In the second case in Example 4.8 (on page 85), B is a subgroup and there are 26 choices for A. From the third case of Example 4.8 (on page 85), we see that in 2 of these cases A is periodic with $\{0, 6\}$ as its subgroup of periods. We may also see these directly with $h_1' = 4$ and $h_1 = h_1'' + 4 \ne 8$. The two sets arising in this way must be equivalent. In the remaining 24 choices for A, A is non-periodic and we have 6 groups of 4 equivalent subsets. This gives 7 equivalence classes.

Finally, in the third case, A is periodic with subgroup of periods of order 2 and B is not periodic. Thus the 2 choices for A are equivalent and the 3 choices for B are equivalent. So only 1 equivalence class arises.

In all we have $6 + 7 + 1 = 14$ equivalence classes of factorizations of this form. □

EXERCISE 4.6 Find all factorizations of $G = Z(12)$ of the form $G = A + B + C$ with $|A| = |B| = 2$, $|C| = 3$, and $0 \in A \cap B \cap C$. Find the number of equivalence classes of these factorizations. □

4.3 Krasner factorizations

In this section $Z(n)$ is represented by the integers $\{0, 1, \ldots, n-1\}$. A Krasner factorization of $Z(n)$ is one in which only the ordinary addition of integers is used, that is, all the relevant sums lie between 0 and $n-1$. We first give an account of the classification of Krasner factorizations and then consider its relationship to factorizations in which $Z(n)$ has suitable Hajós properties.

It is straightforward to construct Krasner factorizations. We use the bracket notation $[a, r]$ for the cyclic subset

$$\{0, a, 2a, \ldots, (r-1)a\}.$$

Let $n = r_1 r_2 \cdots r_k$, where each $r_i > 1$. Let

$$A_1 = [1, r_1],\ A_2 = [r_1, r_2], \ldots, A_k = [r_1 \cdots r_{k-1}, r_k].$$

Then it is easy to see that $Z(n) = A_1 + A_2 + \cdots + A_k$ is a Krasner factorization. So, if $\{1, \ldots, k\}$ is partitioned into m non-empty subsets $I_1, \ldots, I_m$ and

$$B_j = \sum_{i \in I_j} A_i,$$

then $Z(n) = B_1 + \cdots + B_m$ is a Krasner factorization. The classification obtained shows that every Krasner factorization may be obtained in this way. Since $[a, r] + [ra, s] = [a, rs]$, we may assume that no subset I_j contains two consecutive integers.

LEMMA 4.2
Let $Z(n) = A + B$ be a Krasner factorization. Then there exists $r > 1$ such that $[1, r]$ is a direct summand of one factor and r divides every integer in the other factor.

PROOF Since $0, 1 \in Z(n)$, it follows that $0 \in A$, $0 \in B$ and that 1 is in one factor, say A. Then there exists $r > 1$ such that $\{0, 1, \ldots, r-1\} \subseteq A$ and $r \notin A$. Clearly we must have $r \in B$. We make the inductive assumption that

(i) If $tr \in A$ for $t < s$, then $tr + u \in A$ for all $u \in [1, r]$,

(ii) If $d \in B$ and $d \leq sr$, then r divides d.

We already know that these hold for $s = 1$. Let $tr \in A$ for $t < s + 1$ and let $u \in [1, r]$. We need only consider the case $t = s$. Let $sr + u = a + b$ with $a \in A$, $b \in B$. If $b > sr$, then $(s+1)r$ has two representations in $A + B$,

namely, $sr + r$ and $\big((s+1)r - b\big) + b$. Hence $b \leq sr$ and by the inductive assumption $b = vr$, and so $a = (s-v)r + u$. Let $(s-v)r = a_1 + b_1$ with $a_1 \in A$, $b_1 \in B$. Then $b_1 = wr$ for some w and so $a_1 = (s-v-w)r$. By the inductive assumption $a_1 + u \in A$. Hence $a = (a_1 + u) + b_1$. Since the sum $A + B$ is direct, it follows that $b_1 = 0$ and so that $sr + u \in A$.

Now let $b_2 \in B$ with $b_2 \leq (s+1)r$. If $b_2 \leq sr$, then r divides b_2. Let $b_2 = sr + u_1$. Let $sr = a_3 + b_3$ with $a_3 \in A$, $b_3 \in B$. Then $b_3 = xr$ and so $a_3 = (s-x)r$. It follows that $(s-x)r + u_1 \in A$ whenever $u_1 \in [1, r]$. Then $b_2 = \big((s-x)r + u_1\big) + b_3 \in A + B$. This is not possible. Therefore $u_1 = r$ and $b_2 = (s+1)r$. The results (i) and (ii) follow by induction on s.

Now, if $sr + u \in A$, $u \in [1, r]$, then $sr = a + b$, for some $a \in A$, $b \in B$. Then $b = tr$ and so $a = (s-t)r$. Hence $(s-t)r + u \in A$ and so $sr + u = \big((s-t)r + u\big) + b$. It follows that $b = 0$ and so that $sr \in A$. Let $D = \{a \in A : \ r \text{ divides } a\}$. Then, from above, $A = [1, r] + D$, as required. □

THEOREM 4.11

Let $Z(n) = B_1 + \cdots + B_m$ be a Krasner factorization. Then there exist integers $r_1, \ldots, r_k$ such that $n = r_1 \cdots r_k$ and each $r_j > 1$. Also there exists a partition $I_1 \cup \cdots \cup I_m$ of $\{1, 2, \ldots, k\}$ into non-empty subsets such that

$$B_j = \sum_{i \in I_j} A_i,$$

where $A_i = [r_1 \cdots r_{i-1}, r_i]$.

PROOF As before, we have that $0 \in B_j$ for each j and that 1 is in one factor, say B_1. Then there exists r such that $[1, r] \subseteq B_1$ but $r \notin B_1$. Let $B_2 + \cdots + B_m = D$. Then, by Lemma 4.2 (on page 87), r divides each element in D and so, as $0 \in B_j$, it follows that r divides each element in B_j, $2 \leq j \leq m$.

Also, if $E = \{a \in B_1 : \ r \text{ divides } a\}$, then $B_1 = [1, r] + E$. Since the factorization is of the Krasner type, it is clear that $E + B_2 + \cdots + B_m$ is a Krasner sum equal to $[r, (n/r)]$.

The least value of n for which sums can occur is of the form pq, where p, q are primes, not necessarily distinct. In this case $m = 2$ and $|B_1| = p$, $|B_2| = q$. We know that $Z(pq)$ has the Hajós 2-property. Thus one factor, say B_1, is periodic. Hence $B_1 = [q, p]$. Since the sum is of the Krasner type, the only possibility is that $B_2 = [1, q]$. Then B_1 and B_2 are in the required forms.

We may proceed by induction on n. In the above sum $E + B_2 + \cdots + B_m$, we may divide every element by r to obtain a Krasner sum of $[1, (n/r)]$. By the inductive assumption there exist integers $r_2, \ldots, r_k$ whose product is n/r such that this Krasner factorization can be formed as above from the factorization

$$[1, r_2] + [r_2, r_3] + \cdots + [r_2 \cdots r_{k-1}, r_k].$$

When we multiply by r and add on $[1, r_1]$, where $r_1 = r$, this gives the Krasner factorization

$$[1, r_1] + [r_1, r_2] + \cdots + [r_1 \cdots r_{k-1}, r_k]$$

of $[1, n]$. On recalling that $B_1 = [1, r] + E$, this then leads, as required, to the original factorization. ∎

In a Krasner factorization $Z(n) = A_1 + \cdots + A_k$ with $n = r_1 r_2 \cdots r_k$, $A_i = [r_1 \cdots r_{i-1}, r_i]$, the last factor A_k is a subgroup. It is clear that none of the earlier factors A_i, $i < k$, is a subgroup. Furthermore, no sum of these earlier factors is periodic. Let ρ be a primitive (n)th root of unity and $\chi(1) = \rho$, where χ is a character of $Z(n)$. Then $\chi(H) = 0$ for all non-zero subgroups of $Z(n)$. The equation

$$\chi(A_i) = \sum_{i=0}^{r_i - 1} \rho^{r_1 \cdots r_{i-1}} = 0$$

implies upon multiplying by $(1 - \rho^{r_1 \cdots r_{i-1}})$ that $\rho^{r_1 \cdots r_i} = 1$. This is false for $i < k$. Thus $\chi(A_i) \neq 0$ and so H cannot be a subgroup of periods of any sum of factors A_i with all $i < k$. Thus in any Krasner factorization exactly one factor is periodic, namely, the factor that has A_k as a direct summand.

THEOREM 4.12

Let the cyclic group $Z(n)$ have the Hajós k-property. Let $Z(n) = A_1 + \cdots + A_k$ be a factorization. Then there exist subsets $U_1, \ldots, U_k$ of $Z(n)$ such that $Z(n) = U_1 + \cdots + U_k$ is a Krasner factorization. Also, for any partition $\{1, \ldots, k\} = I \cup J$ it follows that

$$Z(n) = \sum_{i \in I} A_i + \sum_{j \in J} U_j$$

is a factorization and so that $|U_i| = |A_i|$.

PROOF The smallest case occurs when $k = 2$ and $n = pq$, where p, q are primes, not necessarily distinct.

Let $Z(pq) = A_1 + A_2$, where $|A_1| = p$, $|A_2| = q$. Then either A_1 or A_2 is periodic and so is a subgroup. We may assume that A_1 is a subgroup and so that $A_1 = [q, p]$. Let $U_1 = A_1$ and $U_2 = [1, q]$. Then clearly $Z(pq) = U_1 + U_2 = A_1 + U_2$ is a Krasner factorization and $Z(pq) = A_1 + A_2 = U_1 + A_2$ is a factorization.

So we may proceed by induction on n. Let $Z(n) = A_1 + \cdots + A_k$. Then some factor, say A_1, is periodic. Let $A_1 = Z(r) + B_1$. Then, from $Z(n) = Z(r) + B_1 + A_2 + \cdots + A_k$ we obtain, as usual, that

$$Z(n)/Z(r) = \overline{B}_1 + \overline{A}_2 + \cdots + \overline{A}_k,$$

where $\overline{B}_1 = \big(B_1 + Z(r)\big)/Z(r)$ and $\overline{A}_i = \big(A_i + Z(r)\big)/Z(r)$. We note that $Z(r)$ as a subgroup of $Z(n)$ is equal to $[(a/r), r]$. So $Z(n)/Z(r)$ may be regarded as being equal to $\{0, 1, \ldots, (n/r)-1\}$ with addition being made modulo $m = n/r$. Thus for any subset X of $Z(n)$ we may define $\overline{X}$ by setting $x \equiv \overline{x} \pmod{m}$, where $0 \leq x \leq n-1$ and $0 \leq \overline{x} \leq m-1$. Since we have a factorization of $Z(n)$, it follows that $|\overline{B}_1| = |B_1|$, $|\overline{A}_1| = |A_1|$ for $2 \leq i \leq k$.

We may now use the inductive hypotheses. Thus there exist subsets $V_1, V_2, \ldots, V_k$ of $Z(m)$ such that $Z(m) = V_1 + V_2 + \cdots + V_k$ is a Krasner factorization. If $A_1 = Z(r)$ and $B_1 = \{0\}$, we have that $V_1 = \{0\}$ and so, in this case, it should be omitted. For any partition $\{1, \ldots, k\} = I \cup J$ we have that

$$Z(n) = \sum_{i \in I} A_i + \sum_{j \in J} V_j$$

is a factorization if $1 \notin I$. If $1 \in I$, then

$$Z(n) = B_1 + \sum_{i \in I} A_i + \sum_{j \in J} V_j$$

is a factorization. Now we may set $U_1 = [m, r] + V_1$, $U_j = V_j$ for $2 \leq j \leq k$. Then it is clear that the desired result holds. ∎

When we were giving all factorizations of groups with the Hajós k-property we pointed out that the formulae would hold if at any stage of the argument the group G having the desired property implies that the quotient group G/H which arose at the next stage also had the desired property. We shall show next that this happens when this property is the existence of suitable Krasner factorizations. We shall refer to a factorization which is given by these formulae as a factorization arising from the Hajós-Sands construction.

THEOREM 4.13

Let $Z(n) = D_1 + \cdots + D_m$ be a factorization such that there exist subsets $U_1, \ldots, U_m$ with the properties that $Z(n) = U_1 + \cdots + U_m$ is a Krasner factorization and, for each partition $I \cup J$ of $\{1, \ldots, m\}$,

$$Z(n) = \sum_{i \in I} D_i + \sum_{j \in J} U_j$$

is a factorization. Then the given factorization of $Z(n)$ arises by the Hajós-Sands construction.

PROOF Again the smallest case occurs with $m = 2$ and $n = pq$, where p, q are primes. Since $Z(pq)$ has the Hajós 2-property, we already know that all its factorizations arise in this way.

So we may proceed by induction on n. We know that exactly one of the Krasner factors, say U_1, is periodic. Let A_k be its group of periods. Let χ

be a character of $Z(n)$ such that $\chi(A_k) = 0$. Then $\chi(r_1 \cdots r_{k-1}) \neq 1$ and so $\chi(A_j) \neq 0$ for $j < k$. Then in this factorization $Z(n) = D_1 + U_2 + \cdots + U_m$ we have that $\chi(D_1) = 0$, since $\chi(U_j) \neq 0$ for $2 \leq j \leq m$. Therefore A_k is a group of period of D_1. Let $D_1 = A_k + B_1$ and let $n = r_k s$. Then, as before, we have a factorization $Z(s) = \overline{B}_1 + \overline{D}_2 + \cdots + \overline{D}_m$ satisfying the given properties. By the inductive assumption this arises from the Hajós-Sands construction. Now, for $2 \leq j \leq m$, we have that $D_j = \overline{D}_j \circ A_k$. Also $B_1 = \overline{B}_1$ and $D_1 = B_1 + A_k$. It now follows that the original factorization arises from the Hajós-Sands construction, as required. ∎

Theorems 4.12 (on page 89) and 4.13 (on page 90) imply the following result. The $k = 2$ special case of the result is due to C. De Felice [37]. She used the result in connection with variable length codes.

THEOREM 4.14

A group $Z(n)$ possesses the Hajós k-property if and only if, given any factorization $Z(n) = A_1 + \cdots + A_k$, there exist subsets $U_1, \ldots, U_k$ such that $Z(n) = U_1 + \cdots + U_k$ is a Krasner factorization and

$$Z(n) = \sum_{i \in I} D_i + \sum_{j \in J} U_j$$

is a factorization for all partitions $I \cup J$ of $\{1, \ldots, k\}$.

Notes

(1) It is clear that Section 4.1 is almost entirely restricted to consideration of cyclic groups. However, an examination of the proof of Theorem 4.4 (on page 73) will show that while the subgroup H of order p^e must be cyclic, there is no use made anywhere of the subgroup K being cyclic. Thus the result holds for groups with cyclic p-components.

(2) In 1963 A. D. Sands [120] asked, if $G = B + A_1 + \cdots + A_k$ is a factorization of the finite abelian group G such that each $|A_i|$ is a prime and $|B|$ is a product of two primes, then does it follow that one of the factors is periodic? After 31 years K. Corrádi and S. Szabó [22] showed that the answer is "yes." In 2005 A. D. Sands [129] proved the generalization presented in Theorem 4.3 (on page 67).

(3) The formulae describing all possible factorizations of finite good groups are due to G. Hajós [49]. However, A. D. Sands had to correct a point later in [115].

(4) The phrase Krasner factorization was coined by C. De Felice [36]. A Krasner factorization $A + B$ of $Z(n)$ can be interpreted as a factorization

$A + B + H$ of Z, where H is the subgroup spanned by n.

(5) For non-cyclic finite abelian groups, the question of which groups satisfy the Hajós k-property has been solved for $k = 2$ but not for general k. In the $k = 2$ case a complete list is given in [117]. Unlike the cyclic case, however, general theorems leading to the result have not been found. There is little improvement known to the original solutions, which treated each case separately. So all we wish to do is refer the reader to [117], where references covering these groups are given. For general k, the case of p-groups, where p is a prime, is not completely solved. For $p = 2$ it is soved in [1]. For $p > 3$ it is solved in the work of Wittmann [172] and of Rédei [107]. For $p = 3$, the case when one factor has order 9 and the other factors have order 3 remains undecided in general.

Chapter 5

Various factorizations

In Section 5.1 here we consider the Rédei property. If in a normalized factorization of an abelian group $G = A + B$ we have that $\langle A\rangle = H$ is a proper subgroup of G, then it is clear that $A + (B \cap H) = H$. Thus we have a factorization of a smaller group. We consider situations where this is useful, but we also give examples of factorizations which do not have this property, that is, where $\langle A\rangle = \langle B\rangle = G$.

In Section 5.2 we consider quasi-periodic factorizations, which is a generalization of the concept of periodic factorizations. When Hajós first found examples of non-periodic factorizations, he asked whether the factorizations must satisfy this weaker condition. We give examples to show that this need not be the case but also show that under certain conditions it will be so.

5.1 The Rédei property

Let $G = A + B$ be a normalized factorization of the finite abelian group G. If $\langle A\rangle = G$, then we say that A is a *full-rank factor*. If in the normalized factorization $G = A + B$ both factors are full-rank, then we say that the factorization is a *full-rank factorization*. If a finite abelian group does not admit normalized full-rank factorization, then we will say that G has the *Rédei property*. In other words, G has the Rédei property if, whenever $G = A+B$ is a normalized factorization of G, then one of the factors A and B is contained by a subgroup that is smaller than G. When $G = \{0\}$, from a factorization $G = A + B$ it follows that $A = B = \{0\}$. Now $\langle A\rangle = \langle B\rangle = G$ and by our definition G does not have the Rédei property. However it looks more sensible to modify the definition such that $G = \{0\}$ has the Rédei property by definition.

EXERCISE 5.1 Let G be a finite cyclic group with basis element x. Let $G = A+B$ be a normalized factorization of G. Verify that $G = (A+x)+(B+x)$ is a (not necessarily normalized) factorization of G. Then show that $\langle A+x\rangle = \langle B + x\rangle = G$. This shows why, in the definition of the Rédei property, the factorizations are restricted to be normalized. ∎

We know that if $G = A + B$ is a normalized factorization of G, then $G = (A - a) + B$ is also a normalized factorization of G for each $a \in A$. Note that $\langle A \rangle = \langle A - a \rangle$. Thus, when we deal with the Rédei property of groups, a factor A can be replaced by $A - a$ for each $a \in A$.

The next two lemmata are about extending factorizations from subgroups to a group. We state the first lemma without proof only for the sake of easy reference.

LEMMA 5.1

If two groups do not have the Rédei property, then neither does their direct sum.

LEMMA 5.2

Let the finite abelian group G be the internal direct sum of its subgroups H and K, where K is cyclic. If $H = A + B$ is a normalized factorization of H with $\langle A \rangle = \langle B \rangle = H$, and if there is an element $a \in A \setminus \{0\}$ such that $\langle A \setminus \{a\} \rangle = H$, then there is a normalized factorization $G = A_1 + B_1$ of G with $\langle A_1 \rangle = \langle B_1 \rangle = G$.

PROOF Let $K = \langle k \rangle$ and define the subsets A_1, B_1 of G by

$$\begin{aligned} A_1 &= [A \setminus \{a\}] \cup \{a + k\}, \\ B_1 &= B + K. \end{aligned}$$

The computation

$$\begin{aligned} G &= H + K \\ &= (A + B) + K \\ &= A + (B + K) \\ &= A + B_1 \end{aligned}$$

shows that $G = A + B_1$ is a factorization of G. Define a function $\varphi : A \to K$ by

$$\varphi(a_1) = \begin{cases} 0, & \text{if} \quad a_1 \neq a, \\ k, & \text{if} \quad a_1 = a. \end{cases}$$

One can verify that $A_1 = K \circ_\varphi A$ and that K is a subgroup of the subgroup of periods of B_1. By Lemma 2.12 (on page 21), the sum $A_1 + B_1$ is direct and is equal to $A + B_1$. Thus $G = A_1 + B_1$ is a factorization of G and obviously the factorization is normalized.

We claim that $\langle A_1 \rangle = \langle B_1 \rangle = G$. From $a \in H = \langle A \setminus \{a\} \rangle \subseteq \langle A_1 \rangle$ and $a + k \in \langle A_1 \rangle$ it follows that $k \in \langle A_1 \rangle$. Now $H = \langle A \setminus \{a\} \rangle \subseteq \langle A_1 \rangle$ and $k \in \langle A_1 \rangle$ imply that $G = \langle H, k \rangle \subseteq \langle A_1 \rangle$ and so $\langle A_1 \rangle = G$. From $B_1 = B + K$ it is clear

that $B \subseteq B_1$ and $k \in B_1$. Hence $H = \langle B \rangle \subseteq \langle B_1 \rangle$ and $k \in \langle B_1 \rangle$. From this it follows that $G = \langle H, k \rangle \subseteq \langle B_1 \rangle$ and so $\langle B_1 \rangle = G$. ∎

We say that a finite abelian group G is *not qualifying* if G is a direct sum of three cyclic groups L_1, L_2, L_3 that have composite orders that are pair-wise relatively prime.

THEOREM 5.1

Let G be a non-qualifying group. Then G does not have the Rédei property.

PROOF Let $|L_i| = u_i v_i$, $2 \leq u_i \leq v_i$ and let x_i be a basis element of L_i. Set

$$\begin{aligned} A_i &= \{0, x_i, 2x_i, \ldots, (u_i - 1)x_i\}, \\ H_i &= \langle u_i x_i \rangle, \quad 1 \leq i \leq 3, \\ H &= H_1 + H_2 + H_3, \\ A &= A_1 + A_2 + A_3. \end{aligned}$$

We claim that the sum $A + H$ is a factorization of G. Since $|A||H| = |G|$ holds, it is enough to verify that the sum $A + H$ is equal to G. The next computation show that this holds:

$$\begin{aligned} A + H &= (A_1 + A_2 + A_3) + (H_1 + H_2 + H_3) \\ &= (A_1 + H_1) + (A_2 + H_2) + (A_3 + H_3) \\ &= \langle x_1 \rangle + \langle x_2 \rangle + \langle x_3 \rangle \\ &= G. \end{aligned}$$

Next we construct a subset B from H by adding and removing certain subsets. Remove

$$\begin{aligned} &H_2 + [(v_1 - 1)u_1]x_1, \\ &H_3 + [(v_2 - 1)u_2]x_2, \\ &H_1 + [(v_3 - 1)u_3]x_3 \end{aligned}$$

from H and add

$$\begin{aligned} &H_2 + [(v_1 - 1)u_1]x_1 + x_2, \\ &H_3 + [(v_2 - 1)u_2]x_2 + x_3, \\ &H_1 + [(v_3 - 1)u_3]x_3 + x_1 \end{aligned}$$

to H to get B. We claim that

$$A + H_2 + [(v_1 - 1)u_1]x_1 = A + H_2 + [(v_1 - 1)u_1]x_1 + x_2, \tag{5.1}$$

$$A + H_3 + [(v_2 - 1)u_2]x_2 = A + H_3 + [(v_2 - 1)u_2]x_2 + x_3, \tag{5.2}$$

$$A + H_1 + [(v_3 - 1)u_3]x_3 = A + H_1 + [(v_3 - 1)u_3]x_3 + x_1. \tag{5.3}$$

Note that (5.1) is equivalent to the fact that x_2 is a period of $A + H_2$. The computation

$$A + H_2 = (A_1 + A_2 + A_3) + H_2$$

$$\begin{aligned} &= (A_1 + A_3) + (A_2 + H_2) \\ &= (A_1 + A_3) + \langle x_2 \rangle \end{aligned}$$

makes visible that $\langle x_2 \rangle$ is a subgroup of the subgroup of periods of $A + H_2$. We leave the verification of equations (5.2) and (5.3) to the reader as an exercise. Next we claim that the sets

$$\begin{aligned} &A + H_2 + [(v_1 - 1)u_1]x_1, \\ &A + H_3 + [(v_2 - 1)u_2]x_2, \\ &A + H_1 + [(v_3 - 1)u_3]x_3 \end{aligned}$$

are disjoint. To prove the claim assume the contrary, that

$$\{A + H_2 + [(v_1 - 1)u_1]x_1\}$$

and

$$\{A + H_3 + [(v_2 - 1)u_2]x_2\}$$

are not disjoint. This is equivalent to stating that

$$\{A_1 + \langle x_2 \rangle + A_3 + [(v_1 - 1)u_1]x_1\}$$

and

$$\{A_1 + A_2 + \langle x_3 \rangle + [(v_2 - 1)u_2]x_2\}$$

are not disjoint. The coefficient of x_1 in any element in the first set is bigger than $v_1 - 1$. The coefficient of x_1 in any element in the second set is at most $v_1 - 1$. This contradiction proves our claim. We leave the remaining cases for the reader as an exercise. It follows that $G = A + B$ is a factorization of G.

Finally we claim that in the $G = A + B$ factorization $\langle A \rangle = G$ and $\langle B \rangle = G$. To verify the claim note that $x_1 \in A_1$, $x_2 \in A_2$, $x_3 \in A_3$ and $A_1, A_2, A_3 \subseteq A$. Hence $x_1, x_2, x_3 \in A$. This gives $\langle A \rangle = G$. To prove that $\langle B \rangle = G$, note that each of

$$\begin{aligned} &H_2 + [(v_1 - 1)u_1]x_1 + x_2, \\ &H_3 + [(v_2 - 1)u_2]x_2 + x_3, \\ &H_1 + [(v_3 - 1)u_3]x_3 + x_1 \end{aligned}$$

is a subset of B. When $v_i \geq 3$, then $u_i x_i \in B$. Then $[(v_i - 1)u_i]x_i \in \langle B \rangle$ and so $x_1, x_2, x_3 \in \langle B \rangle$. This argument in the $u_1 = v_1 = 2$ case should be modified slightly since in this case $u_1 x_1 \notin B$. If $u_1 = v_1 = 2$, then $v_2 \geq 3$, $v_3 \geq 3$. Now we can complete the argument using $u_1 x_1 + u_3 x_3 \in B$ and $u_2 x_2, u_3 x_3 \in B$. □

We illustrate the construction in the previous proof.

TABLE 5.1: The factors A, H, and B

A		H		B	
0, 0, 0	1, 0, 0	0, 0, 0	[2]2, 0, 0	0, 0, 0	[2]2, 1, 0
0, 0, 1	1, 0, 1	0, 0, 5	2, 0, 5	0, 0, 5	2, 0, 5
0, 0, 2	1, 0, 2	0, 0, 10	2, 0, 10	0, 0, 10	2, 0, 10
0, 0, 3	1, 0, 3	0, 0, 15	2, 0, 15	0, 0, 15	2, 0, 15
0, 0, 4	1, 0, 4	[1]0, 0, 20	[1]2, 0, 20	[1]1, 0, 20	[1]3, 0, 20
0, 1, 0	1, 1, 0	0, 3, 0	[2]2, 3, 0	0, 3, 0	[2]2, 4, 0
0, 1, 1	1, 1, 1	0, 3, 5	2, 3, 5	0, 3, 5	2, 3, 5
0, 1, 2	1, 1, 2	0, 3, 10	2, 3, 10	0, 3, 10	2, 3, 10
0, 1, 3	1, 1, 3	0, 3, 15	2, 3, 15	0, 3, 15	2, 3, 15
0, 1, 4	1, 1, 4	0, 3, 20	2, 3, 20	0, 3, 20	2, 3, 20
0, 2, 0	1, 2, 0	[3]0, 6, 0	[2]2, 6, 0	[3]0, 6, 1	[2]2, 7, 0
0, 2, 1	1, 2, 1	[3]0, 6, 5	2, 6, 5	[3]0, 6, 6	2, 6, 5
0, 2, 2	1, 2, 2	[3]0, 6, 10	2, 6, 10	[3]0, 6, 11	2, 6, 10
0, 2, 3	1, 2, 3	[3]0, 6, 15	2, 6, 15	[3]0, 6, 16	2, 6, 15
0, 2, 4	1, 2, 4	[3]0, 6, 20	2, 6, 20	[3]0, 6, 21	2, 6, 20

EXAMPLE 5.1 Let G be a group of type $Z(4) \oplus Z(9) \oplus Z(25)$ with basis elements x_1, x_2, x_3, where $|x_1| = 4$, $|x_2| = 9$, and $|x_3| = 25$. Let

$$\begin{aligned}
A_1 &= \{0, x_1\},\\
A_2 &= \{0, x_2, 2x_2\},\\
A_3 &= \{0, x_3, 2x_3, 3x_3, 4x_3\},\\
H_1 &= \{0, 2x_2\},\\
H_2 &= \{0, 3x_2, 6x_2\},\\
H_3 &= \{0, 5x_3, 10x_3, 15x_3, 20x_3\},\\
A &= A_1 + A_2 + A_3,\\
H &= H_1 + H_2 + H_3.
\end{aligned}$$

To construct B we replace the cosets

$$\begin{aligned}
&H_2 + 1 \cdot (2x_1),\\
&H_3 + 2 \cdot (3x_2),\\
&H_1 + 4 \cdot (5x_3)
\end{aligned}$$

in H by the cosets

$$\begin{aligned}
&H_2 + 1 \cdot (2x_1) + x_2,\\
&H_3 + 2 \cdot (3x_2) + x_3,\\
&H_1 + 4 \cdot (5x_3) + x_1,
\end{aligned}$$

respectively. □

EXAMPLE 5.2 The element $a_1x_1 + a_2x_2 + a_3x_3$ of the group G in Example 5.1 (on page 97) can be represented by the coefficients (a_1, a_2, a_3). In this way the elements of G are all (a_1, a_2, a_3), where $0 \le a_1 \le 3$, $0 \le a_2 \le 8$, $0 \le a_3 \le 24$. The first components are added modulo 4. The second components are added modulo 9. The third components are added modulo 25. Now

$$\begin{aligned}
A_1 &= \{(0,0,0),(1,0,0)\},\\
A_2 &= \{(0,0,0),(0,1,0),(0,2,0)\},\\
A_3 &= \{(0,0,0),(0,0,1),(0,0,2),(0,0,3),(0,0,4)\},\\
H_1 &= \{(0,0,0),(2,0,0)\},\\
H_2 &= \{(0,0,0),(0,3,0),(0,6,0)\},\\
H_3 &= \{(0,0,0),(0,0,5),(0,0,10),(0,0,15),(0,0,20)\}.
\end{aligned}$$

The elements of $A = A_1 + A_2 + A_3$, $H = H_1 + H_2 + H_3$ are listed in Table 5.1 (on page 97). Then we replace the cosets

$$\begin{aligned}
&\{(0,0,0),(0,3,0),(0,6,0)\} + (2,0,0),\\
&\{(0,0,0),(0,0,5),(0,0,10),(0,0,15),(0,0,20)\} + (0,6,0),\\
&\{(0,0,0),(2,0,0)\} + (0,0,20).
\end{aligned}$$

Then we replace the cosets in H by the cosets

$$\begin{aligned}
&\{(0,0,0),(0,3,0),(0,6,0)\} + (2,1,0),\\
&\{(0,0,0),(0,0,5),(0,0,10),(0,0,15),(0,0,20)\} + (0,6,1),\\
&\{(0,0,0),(2,0,0)\} + (1,0,20),
\end{aligned}$$

respectively, to get B. In order to keep track of the changes, we marked the replaced elements by [2], [3], [1], respectively. ∎

EXAMPLE 5.3 The group G in Example 5.1 (on page 97) can be identified by $Z(900)$. In this case $x_1 = 225$, $x_2 = 100$, $x_3 = 36$. Now

$$\begin{aligned}
A_1 &= \{0, 225\},\\
A_2 &= \{0, 100, 200\},\\
A_3 &= \{0, 36, 72, 108, 144\},\\
H_1 &= \{0, 450\},\\
H_2 &= \{0, 300, 600\},\\
H_3 &= \{0, 180, 360, 540, 720\}.
\end{aligned}$$

The elements of $A = A_1 + A_2 + A_3$, $H = H_1 + H_2 + H_3$ are listed in Table 5.2 (on page 99). Then we replace the cosets

$$\{0, 300, 600\} + 450,$$

TABLE 5.2: The factors A, H, and B

		A		
0	36	72	108	144
100	136	172	208	244
200	236	272	308	344
225	261	297	333	369
325	361	397	433	469
425	461	497	533	569
		H		
0	180	360	540	[1]720
[2]150	330	510	690	870
300	480	660	840	120
[2]450	630	810	90	[1]270
[3]600	[3]780	[3] 60	[3]240	[3]420
[2]750	30	210	390	570
		B		
0	180	360	540	[1] 45
[2]250	330	510	690	870
300	480	660	840	120
[2]550	630	810	90	[1]495
[3]636	[3]816	[3] 96	[3]276	[3]456
[2]850	30	210	390	570

$$\{0, 180, 360, 540, 720\} + 600,$$
$$\{0, 450\} + 720$$

in H by the cosets

$$\{0, 300, 600\} + 550,$$
$$\{0, 180, 360, 540, 720\} + 636,$$
$$\{0, 450\} + 45,$$

respectively, to get B. In order to keep track of the changes, we marked the replaced elements by [2], [3], [1], respectively. □

Let F be the family of groups $Z(n)$ such that n is a divisor of one of the following numbers:

$$p^\alpha q^\beta r, \quad p^\alpha qrs, \quad pqrst, \tag{5.4}$$

where p, q, r, s, t are distinct primes and $\alpha \geq 2$, $\beta \geq 2$ are integers.

THEOREM 5.2

Let G be a finite cyclic group. If G has the Rédei property, then G must belong to the F family.

PROOF Let G be of type

$$Z(p_1^{\alpha(1)} \cdots p_m^{\alpha(m)} q_1 \cdots q_n),$$

where $p_1, \ldots, p_m$, $q_1, \ldots, q_n$ are distinct primes and

$$\alpha(1) \geq 2, \ldots, \alpha(m) \geq 2$$

are integers. Subgroups of G of types

$$Z(p_1^{\alpha(1)} p_2^{\alpha(2)} p_3^{\alpha(3)}),\ Z(p_1^{\alpha(1)} p_2^{\alpha(2)} q_1 q_2),$$
$$Z(p_1^{\alpha(1)} q_1 \cdots q_4), \quad Z(q_1 \cdots q_6)$$

are not qualifying. The family F is constructed such that its members do not have any non-qualifying subgroup. Group cyclic direct factors of G together to form non-qualifying groups, as many as possible. As a result G can be expressed as a direct sum of two subgroups L and M such that L is a direct sum of qualifying subgroups $H_1, \ldots, H_u$ and M belongs to the F family. We claim that if G has the Rédei property, then $u = 0$. To prove the claim we assume that $u \geq 1$. From the proof of Theorem 5.1 (on page 95) we can read off that there is an element $a \in A \setminus \{0\}$ such that $\langle A \setminus \{a\} \rangle = G$. In fact, there are

$$|A| - 3 = u_1 u_2 u_3 - 3 \geq 2 \cdot 3 \cdot 5 - 3 = 27$$

obvious choices for a. Using Lemma 5.2 (on page 94) several times, if this is necessary, we can see that $H_u + M$ does not have the Rédei property. Then, by Lemma 5.1 (on page 94), $(H_1 + \cdots + H_{u-1}) + (H_u + M)$ does not have the Rédei property. ∎

THEOREM 5.3

Let p and q be distinct primes. A cyclic group of order $p^e q^f$ has the Rédei property.

PROOF Let G be a cyclic group of order $p^e q^f$. Let $G = A + B$ be a factorization of G with $0 \in A$, $0 \in B$. In order to show that either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$, we assume the contrary, that $\langle A \rangle = G$ and $\langle B \rangle = G$. Let x and y be basis elements of G with $|x| = p^e$, $|y| = q^f$. Let $H = \langle px, y \rangle$, $K = \langle x, qy \rangle$. As $\langle A \rangle = G$ we cannot have $A \subseteq H$, and so there is an element $a_1 \in A$ whose order is $p^e q^\beta$. As $\langle A \rangle = G$ we cannot have $A \subseteq K$, and so there is an element $a_2 \in A$ whose order is $p^\alpha q^f$. If $a_1 = a_2$, then A contains an element of order $p^e q^f$. If $a_1 \neq a_2$, $A - a_2$ contains an element of order $p^e q^f$. Since A can be replaced by $A - a_2$, we may assume that there is a factorization $G = A + B$ such that $\langle A \rangle = \langle B \rangle = G$ and both A and B contain an element of order $p^e q^f$. Let $a \in A$ be such that $|a| = p^e q^f$ and let $b \in B$ be such that $|b| = p^e q^f$. Obviously a is a basis element of G. There is an integer k such that $b = ka$.

As $|b| = p^e q^f$, it follows that k is relatively prime to $p^e q^f$. By Theorem 3.17 (on page 58), in the factorization $G = A + B$, the factor A can be replaced by kA to get the factorization $G = kA + B$. From

$$\underbrace{(\quad ka \quad)}_{\in kA} + \underbrace{(\quad 0 \quad)}_{\in B} = \underbrace{(\quad 0 \quad)}_{\in kA} + \underbrace{(\quad b \quad)}_{\in B},$$

it follows the contradiction $b = 0$. □

THEOREM 5.4

Finite cyclic groups that are 2*-good have the Rédei property.*

PROOF Let G be a finite cyclic group that has the 2-good property. Let $G = A + B$ be a factorization of G, where $0 \in A$, $0 \in B$. Let $n = \nu\big(|G|\big)$ be the number of not necessarily distinct prime factors of $|G|$. If $n = 1$, then $|G|$ is a prime and from the factorization $G = A + B$ it follows that $A = \{0\}$ or $B = \{0\}$. Thus $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$. We assume that $n \geq 2$ and proceed by induction on n.

As G is 2-good in the factorization $G = A + B$, one of the factors, say A, is periodic. By Lemma 2.8 (on page 18), there is a subgroup H of G and there is a subset C of G such that the sum $C + H$ is direct and is equal to A. Considering the factor group G/H from the factorization $G = (C + H) + B$, we get the factorization

$$G/H = [(C + H)/H] + [(B + H)/H]$$

of the factor group G/H. Here

$$(C + H)/H = \{c + H : c \in C\},$$
$$(B + H)/H = \{b + H : b \in B\}.$$

Now $|G/H| < |G|$ and G/H is 2-good as it is guaranteed by its type. By the inductive assumption it follows that $(C + H)/H$ or $(B + H)/H$ is contained in a subgroup of G/H that is not equal to G/H. If $\langle A\rangle = \langle B\rangle = G$, then, by Lemma 2.7 (on page 17), $(C + H)/H$ and $(B + H)/H$ are full-rank subsets in G/H. Therefore A or B is contained by a subgroup of G that is not equal to G. □

THEOREM 5.5

Let p, q be distinct primes. Let G be a finite abelian group whose p-component and q-component are cyclic. If $G = A + B$ is a factorization of G and $|A| = p^\alpha q^\beta$, then either $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$.

PROOF Assume that there is a counter-example, that is, there is a factorization $G = A + B$ such that $|A| = p^\alpha q^\beta$ and $\langle A\rangle = \langle B\rangle = G$. Let H be

the p-component of G with $|H| = p^\gamma$. Let K be the q-component of G with $|K| = q^\delta$. Set $M = H + K$.

We claim that in a counter-example $G = A + B$ we can replace A by A' such that there is an $a \in A'$ with $|(a)_M| = p^\gamma q^\delta$.

To prove the claim we can argue in the following way. If $(a)_M \in pH + K$ for each $a \in A$, then $\langle A \rangle \neq G$. This is not the case. It follows that there is an $a_1 \in A$ such that $(a_1)_M \notin pH + K$. This means $|(a_1)_M| = p^\gamma q^\mu$. If $\mu = \delta$, then we are done. We assume that $\mu < \delta$. If $(a)_M \in H + qK$ for each $a \in A$, then $\langle A \rangle \neq G$. It follows that there is an $a_2 \in A$ such that $(a_2)_M \notin H + qK$. This means that $|(a_2)_M| = p^\nu q^\delta$. If $\nu = \gamma$, then we are done. We assume that $\nu < \gamma$.

Adding $-a_2$ to the factorization $G = A + B$, we get the factorization

$$\begin{aligned} G &= G - a_2 \\ &= (A - a_2) + B \\ &= A' + B. \end{aligned}$$

Set $a = a_1 - a_2$. Plainly, $a \in A'$. Let $|(a)_M| = p^e q^f$. From $a + a_2 = a_1$ we get $(a)_H + (a_2)_H = (a_1)_H$. If $e < \gamma$, then the order of $(a)_H + (a_2)_H$ is less than p^γ and the order of $(a_1)_H$ is p^γ. This is an outright contradiction. Therefore $e = \gamma$. From $a_2 = a_1 - a$ we get $(a_2)_K = (a_1)_K - (a)_K$. If $f < \delta$, then the order of $(a_1)_K - (a)_K$ is less than q^δ and the order of $(a_2)_K$ is q^δ. This contradiction shows that $f = \delta$. Thus $|(a)_M| = p^\gamma q^\delta$ and $a \in A'$, as we claimed.

Next we claim that in a counter-example $G = A' + B$ we may replace B by B' such that there is a $b \in B'$ with $|(b)_M| = p^\gamma q^\delta$. This claim can be verified in the same way as we have just seen.

Let us suppose that $G = A + B$ is a counter-example such that there are $a \in A$, $b \in B$ with $|(a)_M| = |(b)_M| = p^\gamma q^\delta$. Let N be the complementary direct summand of M in G and let $|N| = n$. By Theorem 3.17 (on page 58), in the factorization $G = A + B$, the factor A can be replaced by nA to get the factorization $G = nA + B = A' + B$. Clearly, N is a complete set of coset representatives of G modulo M. The sets $B \cap (M + c)$, $c \in N$ form a partition of B. There is a $c \in N$ such that $b \in B \cap (M + c)$.

Adding $-c$ to the factorization $G = A' + B$, we get the factorization

$$\begin{aligned} G &= G - c \\ &= A' + (B - c). \end{aligned}$$

Note that $M = \langle A' \rangle$. Restricting the factorization $G = A' + (B - c)$ to M, we get the factorization

$$\begin{aligned} M &= G \cap M \\ &= A' + \big[(B - c) \cap M\big]. \end{aligned}$$

(For restricting a factorization to a subgroup see Corollary 2.1 on page 14.) Obviously, M is a cyclic group of order $p^\gamma q^\delta$. In the factorization

$$\begin{aligned} M &= A' + \big[(B-c) \cap M\big] \\ &= A' + B', \end{aligned}$$

$\langle A' \rangle = M$. From $b \in B \cap (M + c)$ we get $b - c \in (B - c) \cap M = B'$. Then $|(b)_M| = p^\gamma q^\delta$ and $(b-c)_M = (b)_M - (c)_M = (b)_M$ show that $\langle B' \rangle = M$. Now $\langle A' \rangle = \langle B' \rangle = M$ contradicts Theorem 5.3 (on page 100). □

COROLLARY 5.1

The cyclic group $Z(n)$ has the Rédei property if and only if n is a divisor of one of the numbers in the list (5.4).

PROOF By Theorem 5.2 (on page 99), $Z(n)$ does not have the Rédei property if n is a proper multiple of a number from the list (5.4). On the other hand, if n is a divisor of a number in this list, then in the factorization $Z(n) = A + B$ at least one of $|A|$, $|B|$ has at most two distinct prime divisors. Therefore Theorem 5.5 (on page 101) is applicable and gives that $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. □

In the remaining part of this section we describe how cube tilings can help to construct certain factorizations. It is quite common that geometrical problems can be solved by reformulating them into algebraic problems. It is less common that the geometric reinterpretation of an algebraic problem suggests useful hints to solve the algebraic problem.

Consider the 3-dimensional Euclidean space with coordinate unit vectors e_1, e_2, e_3 filled with rectangular boxes of dimensions v_1, v_2, v_3 such that the boxes are abutting face-to-face and the edges are parallel to the coordinate axis. Divide the boxes into $v_1v_2v_3$ unit cubes and then cut each unit cube into smaller cells of dimensions $1/u_1, 1/u_2, 1/u_3$. Here u_1, u_2, u_3, v_1, v_2, v_3 are given positive integers. Figure 5.1 (on page 104) illustrates the tiling in the $v_1 = 5$, $v_2 = 3$, $v_3 = 4$, $u_1 = 2$, $u_2 = 4$, $u_3 = 3$ particular case. The corners of the small cells form a lattice L_1. The corners of the unit cubes form a lattice L_2. The corners of the large cells form a lattice L_3. The lattice L_3 is spanned by v_1e_1, v_2e_2, v_3e_3. The lattice L_2 is spanned by e_1, e_2, e_3. The lattice L_1 is spanned by $(1/u_1)e_1, (1/u_2)e_2, (1/u_3)e_3$. Clearly L_i is an abelian group with operation of addition of vectors and L_2, L_3 are subgroups of L_1. The factor group $G = L_1/L_3$ is a direct sum of cyclic groups of orders u_1v_1, u_2v_2, u_3v_3, respectively. Let x_i denote the coset $(1/u_i)e_i + L_3$, $1 \leq i \leq 3$. Then x_1, x_2, x_3 are basis elements of G. The collection of $u_1v_1u_2v_2u_3v_3$ small cells filling a large cell can be identified with the elements of G. Rearranging these cells

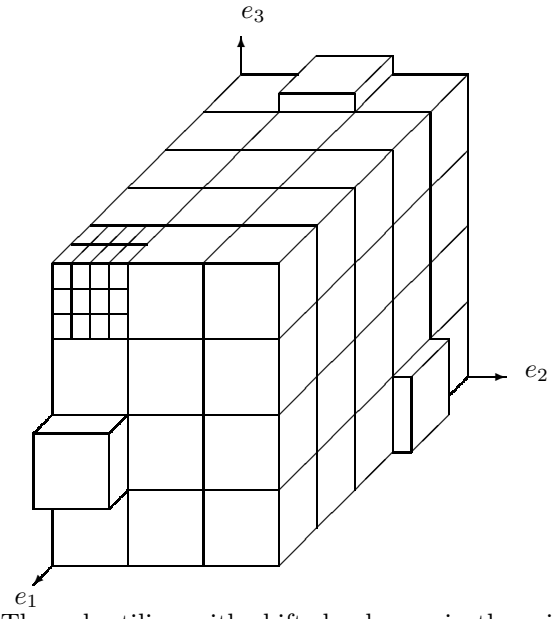

FIGURE 5.1: The cube tiling with shifted columns in three independent directions.

leads to new decompositions of G. Let

$$A_i = \{0, x_i, 2x_i, \ldots, (u_i - 1)x_i\},$$
$$H_i = \langle u_i x_i \rangle, \quad 1 \le i \le 3.$$

Then $A = A_1 + A_2 + A_3$ corresponds to $u_1u_2u_3$ small cells that form a unit cube and $H = H_1 + H_2 + H_3$ corresponds to the $v_1v_2v_3$ unit cubes that form a large cell. The factorization

$$G = (H_1 + H_2 + H_3) + A_1 + A_2 + A_3$$

corresponds to the fact that the cubes form a tiling. We construct a new set B from H by removing

$$H_2 + (v_1 - 1)u_1x_1,$$
$$H_3 + (v_2 - 1)u_2x_2,$$
$$H_1 + (v_3 - 1)u_3x_3$$

from H and adding

$$H_2 + (v_1 - 1)u_1x_1 + x_2,$$
$$H_3 + (v_2 - 1)u_2x_2 + x_3,$$
$$H_1 + (v_3 - 1)u_3x_3 + x_1$$

to H. Replacing $H_2+(v_1-1)u_1x_1$ by $H_2+(v_1-1)u_1x_1+x_2$ corresponds to the fact that an infinite column of unit cubes parallel to the e_2 is shifted parallel

to e_2. Replacing $H_3 + (v_2 - 1)u_2x_2$ by $H_3 + (v_2 - 1)u_2x_2 + x_3$ corresponds to the fact that an infinite column of unit cubes parallel to the e_3 is shifted parallel to e_3. Finally, replacing $H_1 + (v_3 - 1)u_3x_3$ by $H_1 + (v_3 - 1)u_3x_3 + x_1$ corresponds to the fact that an infinite column of unit cubes parallel to the e_1 is shifted parallel to e_1. The infinite columns we are shifting are not blocking each other's movements as they are disjoint and the resulting cube system is a tiling. The new cube tiling corresponds to a new factorization of G in the form

$$G = B + (A_1 + A_2 + A_3).$$

Of course we can carry out the described factorization construction without any reference to cube tilings and can check if the factorization has the desired properties in a purely algebraic manner.

Note that if the numbers u_1v_1, u_2v_2, u_3v_3 are pair-wise relatively primes, then the group G is cyclic. Thus the procedure above can be used to construct factorizations for finite cyclic groups. Two instances of this factorization procedure appeared in the book. At the first occasion, the first 5 of the numbers

$$u_1,\ v_1,\ u_2,\ v_2,\ u_3,\ v_3 \tag{5.5}$$

were chosen to be at least 2 and v_3 was set to be 1. In this case $A_3 = \{0\}$. This setting lead to a factorization $G = B + A_1 + A_2$, where none of the sets B, A_1, A_2, $A_1 + A_2$ is periodic. This construction is described in detail in the proof of Theorem 3.4 (on page 41).

In the second case, we chose all the numbers (5.5) to be at least 2. This setting lead to a factorization $G = B + A_1 + A_2 + A_3$, where both B and $A = A_1 + A_2 + A_3$ span the whole G. This construction is used in the proof of Theorem 5.1 (on page 95).

PROBLEM 5.1 Is it true that if each maximal subgroup of a finite abelian group has the Hajós 2-property, then it has the Rédei property? □

5.2 Quasi-periodicity

Let $G = A + B$ be a normalized factorization of G. We say that the partition $B = B_1 \cup \cdots \cup B_n$ of the factor B is *regular* if there is a periodic subset $C = \{c_1, \ldots, c_n\}$ of G such that $c_1 = 0$, $|C| \geq 2$ and $A + B_i = A + B_1 + c_i$ for each i, $1 \leq i \leq n$. We will call the normalized factorization $G = A + B$ *quasi-periodic* if one of the factors has a regular partition.

An example can help to illustrate the definition.

EXAMPLE 5.4 Let G be a group of type $Z(6)\oplus Z(6)$ with basis elements x, y. Set

$$\begin{aligned} A &= (0x + \langle 2x + 2y\rangle) \cup (1x + \langle 2x\rangle) \\ &= \{0, x, 2x + 2y, 3x, 4x + 4y, 5x\}, \\ B &= (0y + \langle 2x + 4y\rangle) \cup (1y + \langle 2y\rangle) \\ &= \{0, y, 4x + 2y, 3y, 2x + 4y, 5y\}. \end{aligned}$$

A routine computation shows that each of the sums

$$\begin{aligned} &\langle 2x + 2y\rangle + \langle 2x + 4y\rangle, \quad \langle 2x + 2y\rangle + \langle 2y\rangle, \\ &\langle 2x\rangle + \langle 2x + 4y\rangle, \quad \langle 2x\rangle + \langle 2y\rangle \end{aligned}$$

forms a factorization of $\langle 2x, 2y\rangle$ and $\{0, x\} + \{0, y\}$ is a complete set of representatives of G modulo $\langle 2x, 2y\rangle$. By Lemma 2.19 (on page 29), $G = A + B$ is a factorization of G. Let

$$\begin{aligned} B_1 &= \{0, y, 5y\}, \\ B_2 &= \{4x + 2y, 3y, 2x + 4y\}, \end{aligned}$$

$$C = \{c_1, c_2\}, \quad c_1 = 0, \quad c_2 = 3y.$$

Another routine computation gives that C is periodic, $B = B_1 \cup B_2$ is a partition of B such that $A + B_1 = A + B_1 + c_1$, and $A + B_2 = A + B_1 + c_2$, that is, the factorization $G = A + B$ is quasi-periodic. □

THEOREM 5.6

If in the normalized factorization $G = A + B$ the factor B is periodic, then B has a regular partition and the factorization is quasi-periodic.

PROOF Let H be the subgroup of periods of B. Clearly $|H| \geq 2$. Let D be a subset of B such that $B = D + H$ is a factorization of B and let $H = \{h_1, \ldots, h_n\}$ with $h_1 = 0$. Set $B_i = D + h_i$, $1 \leq i \leq n$. Now $B_1 \cup \cdots \cup B_n$ is a partition of B and $A + B_i = A + B_1 + h_i$ holds. □

In 1950, G. Hajós [50], after constructing factorizations $G = A + B$, where none of A and B are periodic and G is cyclic, advanced the question if each factorization of a finite abelian group is quasi-periodic. In connection with such seemingly unrelated topics as coding theory and Fourier analysis, the question recently has resurfaced where the case when G is a cyclic group is relevant. (See [36] and [74], respectively.) In the meantime, in 1974 A. D. Sands [123] showed that if $p \geq 5$ is a prime, then groups of type $Z(p^2) \oplus Z(p)$ admit non-quasi-periodic factorizations.

In Fuchs [41] an alternative definition of quasi-periodicity is used. Let $G = A + B$ be a normalized factorization of G. We say that the partition $B = B_1 \cup \cdots \cup B_n$ of the factor B is regular if there is a subgroup $H = \{h_1, \ldots, h_n\}$

of G such that $h_1 = 0$, $|H| \geq 2$ and $A + B_i = A + B_1 + h_i$ for each i, $1 \leq i \leq n$. We will call the normalized factorization $G = A + B$ quasi-periodic if one of the factors has a regular partition.

A subgroup H of G with $|H| \geq 2$ is a periodic subset, so the second definition of the quasi-periodicity is seemingly more restrictive than the first version. It turns out that the two definitions are equivalent.

THEOREM 5.7

The two definitions of quasi-periodicity are equivalent.

PROOF Suppose that $B_1 \cup \cdots \cup B_n$ is a regular partition of B by the first definition, that is, there is a periodic subset $C = \{c_1, \ldots, c_n\}$ of G such that $c_1 = 0$, $|C| \geq 2$ and $A + B_i = A + B_1 + c_i$ for each i, $1 \leq i \leq n$. There is a subgroup $H = \{h_1, \ldots, h_r\}$ and a subset $D = \{d_1, \ldots, d_s\}$ such that $h_1 = 0$, $|H| \geq 2$ and $C = H + D$ is a factorization. Now $h_i + d_j$ is equal to an element $c_{f(i,j)}$ of C. Clearly the indices $f(i, j)$, $1 \leq i \leq r$, $1 \leq j \leq s$ form a permutation of $1, \ldots, n$. Set

$$E_i = B_{f(i,1)} \cup \cdots \cup B_{f(i,s)}, \quad 1 \leq i \leq r.$$

Then $E_1 \cup \cdots \cup E_r$ is a partition of B. The computation

$$\begin{aligned}
A + E_1 + h_i &= A + (B_{f(1,1)} \cup \cdots \cup B_{f(1,s)}) + h_i \\
&= (A + B_{f(1,1)} + h_i) \cup \cdots \cup (A + B_{f(1,s)} + h_i) \\
&= (A + B_1 + c_{f(1,1)} + h_i) \cup \cdots \cup (A + B_1 + c_{f(1,s)} + h_i) \\
&= (A + B_1 + h_1 + d_1 + h_i) \cup \cdots \cup (A + B_1 + h_1 + d_s + h_i) \\
&= (A + B_1 + d_1 + h_i) \cup \cdots \cup (A + B_1 + d_s + h_i) \\
&= (A + B_1 + h_i + d_1) \cup \cdots \cup (A + B_1 + h_i + d_s) \\
&= (A + B_1 + c_{f(i,1)}) \cup \cdots \cup (A + B_1 + c_{f(i,s)}) \\
&= (A + B_{f(i,1)}) \cup \cdots \cup (A + B_{f(i,s)}) \\
&= A + (B_{f(i,1)} \cup \cdots \cup B_{f(i,s)}) \\
&= A + E_i
\end{aligned}$$

shows that $A + E_i = A + E_1 + h_i$ for each i, $1 \leq i \leq r$. Therefore the partition $E_1 \cup \cdots \cup E_r$ is regular by the second definition. Thus the two definitions of quasi-periodicity are equivalent. □

From the above argument one can read off that in the second definition it may be assumed that the order of H is a prime.

The next theorem can be used in certain cases to extend a factorization from a subgroup to the whole group.

THEOREM 5.8

Let G be a finite abelian group and let H be a subgroup of G such that the

index $|G : H|$ is a prime and H is not a direct factor of G. If H has a factorization that is not quasi-periodic, then so also has G.

PROOF Let $H = A + B$ be a factorization that is not quasi-periodic. Let C be a complete set of representatives in G modulo H such that $0 \in C$. Then $G = H + C$ is a normalized factorization and plainly $G = A + (B + C)$ is a factorization. We claim that the factorization $G = A + (B + C)$ is not quasi-periodic.

To prove the claim assume first that A admits a regular partition. This means that there are subsets $A_1, \ldots, A_n$ and a subgroup K of G with the following properties. The subsets $A_1, \ldots, A_n$ form a partition of A,

$$A_1 + (B + C) + k_i = A_i + (B + C), \quad 1 \le i \le n,$$

$K = \{k_1, \ldots, k_n\}$ with $k_1 = 0$. By the remark before the theorem, we may assume that $|K|$ is a prime.

From $K \cap H = \{0\}$ it follows that $G = H \oplus K$. This is not the case. So $K \cap H \neq \{0\}$ and hence $K \subseteq H$. From $A, B \subseteq H$ it follows that

$$\begin{aligned} A_1 + B + k_i &= (A_1 + B + C + k_i) \cap H \\ &= (A_i + B + C) \cap H \\ &= A_i + B, \end{aligned}$$

which contradicts the definitions of A, B.

Next assume that $(B + C)$ has a regular partition. This means that there are subsets $D_1, \ldots, D_n$ and a subgroup K of G such that the sets $D_1, \ldots, D_n$ form a partition of $(B + C)$,

$$A + D_1 + k_i = A + D_i, \quad 1 \le i \le n,$$

$K = \{k_1, \ldots, k_n\}$, $k_1 = 0$. As before, we may assume that $|K|$ is a prime and we get that $K \subseteq H$. Let $E_i = D_i \cap H$. Since $A \subseteq H$,

$$\begin{aligned} A + E_i &= A + (D_i \cap H) \\ &= (A + D_i) \cap (A + H) \\ &= (A + D_i) \cap H \\ &= (A + k_i + D_1) \cap H \\ &= (A + k_i + D_1) \cap (A + k_i + H) \\ &= (A + k_i) + (D_1 \cap H) \\ &= A + E_1 + k_i, \\ B &= B + \{0\} \\ &= B + (C \cap H) \\ &= (B + C) \cap H \\ &= (D_1 \cup \cdots \cup D_n) \cap H \\ &= (D_1 \cap H) \cup \cdots \cup (D_n \cap H) \\ &= E_1 \cup \cdots \cup E_n. \end{aligned}$$

Therefore B has a regular partition in the factorization $H = A + B$. This contradiction completes the proof. ∎

THEOREM 5.9

Let p be a prime. If $p \geq 5$, then a group of type $Z(p^2) \oplus Z(p)$ has a non-quasi-periodic factorization.

PROOF Let G be a group of type $Z(p^2) \oplus Z(p)$ with basis elements x, y such that $|y| = p^2$, $|x| = p$. Let f be a permutation of $0, 1, \ldots, p-1$. Set $b_i = iy$, $0 \leq i \leq p-1$, $K_1 = \langle py \rangle$, $K_2 = \langle x \rangle$,

$$A = \{ix + f(i)py : \ 0 \leq i \leq p-1\},$$
$$B = [b_0 + K_1] \cup [b_1 + K_2] \cup \cdots \cup [b_{p-1} + K_2].$$

We choose f to be the transposition $(p-2, p-1)$. One can verify that the sums $A + K_1$, $A + K_2$ are factorizations of $\langle x, py \rangle$ and that $b_0, \ldots, b_{p-1}$ is a complete set of representatives of G modulo $\langle x, py \rangle$. By Lemma 2.19 (on page 29), $G = A + B$ is a normalized factorization of G. If A is periodic, then as $|A| = p$, A must be a subgroup. Since A is not a subgroup of G, A cannot be periodic. Using Lemma 2.20 (on page 29) one can establish that B is not periodic either.

We claim that the factorization $G = A + B$ is not quasi-periodic. To prove the claim, assume the contrary, that the factorization is quasi-periodic. Assume that A has a regular partition $A_1 \cup \cdots \cup A_n$. There is a subgroup $H = \{h_1, \ldots, h_n\}$ of G such that $h_1 = 0$, $|H| \geq 2$, and $B + A_i = B + A_1 + h_i$ for each i, $1 \leq i \leq n$. We may assume that $|H|$ is a prime, that is, $n = |H| = p$. From $|A_1| = \cdots = |A_n|$ it follows that $p = |A| = p|A_1|$ and so $|A_1| = 1$. Let $A_i = \{a_i\}$. Now $B + A_i = B + A_1 + h_i$ is equivalent to $B + a_i = B + a_1 + h_i$. Since B is not periodic, we get that $a_i = a_1 + h_i$. This means that

$$\begin{aligned} A &= \{a_1, \ldots, a_n\} \\ &= \{a_1 + h_1, \ldots, a_1 + h_n\} \\ &= a_1 + \{h_1, \ldots, h_n\} \\ &= a_1 + H. \end{aligned}$$

In particular, A is periodic which, is not the case.

Assume next that B has a regular partition $B_1 \cup \cdots \cup B_n$. There is a subgroup $H = \{h_1, \ldots, h_n\}$ such that $h_1 = 0$, $|H| \geq 2$ and $A + B_i = A + B_1 + h_i$ for each i, $1 \leq i \leq n$. We may assume that $|H|$ is a prime, that is, $n = |H| = p$. From $|B_1| = \cdots = |B_n|$ it follows that $p^2 = |B| = p|B_1|$. Hence $|B_1| = p$. The computation

$$\begin{aligned} G &= A + B \\ &= A + (B_1 \cup \cdots \cup B_n) \\ &= (A + B_1) \cup \cdots \cup (A + B_n) \end{aligned}$$

$$\begin{aligned}
&= (A + B_1 + h_1) \cup \cdots \cup (A + B_1 + h_n) \\
&= (A + B_1) + \{h_1, \ldots, h_n\} \\
&= A + B_1 + H \\
&= (A + B_i - h_i) + H \\
&= A + B_i + (-h_i + H) \\
&= A + B_i + H
\end{aligned}$$

shows that the sum $A + B_i + H$ is equal to G. Using $|G| = p^3$, $|A| = p$, $|B_i| = p$, and $|H| = p$, we can see that $|G| = |A||B_i||H|$ and so the equation $G = A + B_i + H$ is a factorization of G. In particular, the sum $A + H$ is direct. Therefore $|A + H| = p^2$. Set $L = \langle x, py \rangle$. Note that $A \subseteq L$, $H \subseteq L$ and so $A + H \subseteq L$. It follows that $L = A + H$ is a factorization of L. Finally, $G = B_i + L$ is a factorization of G.

Note that the elements of B are distributed over the residue classes modulo L in the following way:

$$\begin{aligned}
0y + \langle py \rangle &\subseteq 0y + L, \\
1y + \langle x \rangle &\subseteq 1y + L, \\
&\vdots \\
(p-1)y + \langle x \rangle &\subseteq (p-1)y + L.
\end{aligned}$$

We claim that B_i contains exactly one element from each of the following sets:

$$0y + \langle py \rangle, \quad 1y + \langle x \rangle, \ldots, (p-1)y + \langle x \rangle.$$

In order to prove the claim, assume the contrary, that B_i contains distinct elements u, v such that $u, v \in \langle py \rangle$ or $u, v \in jy + \langle x \rangle$. Let us deal with the $u, v \in \langle py \rangle$ case first. Since the sum $B_i + L$ is direct, it follows that the cosets $u + L$ and $v + L$ are distinct. On the other hand, $u, v \in \langle py \rangle \subseteq L$ gives the contradiction that the cosets $u + L$ and $v + L$ are equal.

Let us turn to the case when $u, v \in jy + \langle x \rangle$. Again, since the sum $B_i + L$ is direct, it follows that the cosets $u + L$ and $v + L$ are distinct. Then the cosets $(u - jy) + L$ and $(v - jy) + L$ are distinct. On the other hand, $u - jy, v - jy \in \langle x \rangle \subseteq L$ gives the contradiction that the cosets $(u - jy) + L$ and $(v - jy) + L$ are equal.

Since B_1 contains exactly one element from the set $0y + \langle py \rangle$ and exactly one element from the set $1y + \langle x \rangle$, there are integers α_1, β_1 such that $1 \leq \alpha_1, \beta_1 \leq p - 1$ and

$$0y + \alpha_1 py, \quad 1y + \beta_1 x \in B_1.$$

Similarly, since B_2 contains exactly one element from $0y + \langle py \rangle$ and exactly one element from $1y + \langle x \rangle$, there are integers α_2, β_2 such that $1 \leq \alpha_2, \beta_2 \leq p - 1$ and

$$0y + \alpha_2 py, \quad 1y + \beta_2 x \in B_2.$$

Consider the equation $A + B_2 = A + B_1 + h_2$ and write it in the form $A + B_1 = A + B_2 + k$, where $k = -h_2$. Using this and $A \subseteq L$ we get

$$A + (B_1 \cap L) = (A + B_1) \cap (A + L)$$

$$\begin{aligned}
&= (A + B_1) \cap L \\
&= (A + B_2 + k) \cap L \\
&= (A + k + B_2) \cap L \\
&= (A + k + B_2) \cap (A + k + L) \\
&= A + k + (B_2 \cap L).
\end{aligned}$$

Therefore

$$A + \alpha_1 py = A + k + \alpha_2 py.$$

As A is not periodic it follows that

$$\begin{aligned}
\alpha_1 py &= k + \alpha_2 py, \\
k &= (\alpha_1 - \alpha_2) py.
\end{aligned}$$

Similarly, from the equation $A + B_1 - y = A + k + B_2 - y$, it follows that

$$A + [(B_1 - y) \cap L] = A + k + [(B_2 - y) \cap L].$$

Then adding y we get that

$$\begin{aligned}
A + [B_1 \cap (L + y)] &= A + k + [B_2 \cap (L + y)], \\
A + y + \beta_1 x &= A + k + y + \beta_2 x, \\
A + \beta_1 x &= A + k + \beta_2 x.
\end{aligned}$$

As A is not periodic it follows that

$$\begin{aligned}
\beta_1 x &= k + \beta_2 x, \\
k &= (\beta_1 - \beta_2) x.
\end{aligned}$$

Comparing the two expressions we have for k gives that

$$(\beta_1 - \beta_2) x = (\alpha_1 - \alpha_2) py.$$

Since x, y is a basis for G, it follows that $\beta_1 = \beta_2$. This is a contradiction since $B_1 \cap B_2 = \emptyset$. Thus B does not have a regular partition in the factorization $G = A + B$. ∎

THEOREM 5.10

Let p be a prime. If $p \geq 3$, then a group of type $Z(p^2) \oplus Z(p^2)$ has a non-quasi-periodic factorization.

PROOF Let G be a group of type $Z(p^2) \oplus Z(p^2)$ with basis elements x, y. Set $a_i = ix$, $b_i = iy$, $0 \leq i \leq p - 1$,

$$\begin{aligned}
K_1 &= \langle px + py \rangle, \quad K_2 = \langle px \rangle, \\
K_3 &= \langle px + 2py \rangle, \; K_4 = \langle py \rangle,
\end{aligned}$$

$$A = [a_0 + K_1] \cup [a_1 + K_2] \cup \cdots \cup [a_{p-1} + K_2],$$
$$B = [b_0 + K_3] \cup [b_1 + K_4] \cup \cdots \cup [b_{p-1} + K_4].$$

Let $L = \langle px, py \rangle$. One can verify that $K_i + K_j = L$ is a factorization of L for $1 \le i < j \le 4$ and $a_i + b_j$, $0 \le i, j \le p-1$ is a complete set of representatives of G modulo L. By Lemma 2.19 (on page 29), $G = A + B$ is a normalized factorization of G. Using Lemma 2.20 (on page 29) it can be checked that A and B are not periodic.

We claim that the factorization $G = A + B$ is not quasi-periodic. To prove the claim assume the contrary, that the factorization is quasi-periodic. Assume first that B has a regular partition $B_1 \cup \cdots \cup B_n$. This means that there is a subgroup $H = \{h_1, \ldots, h_n\}$ of G such that $h_1 = 0$, $|H| \ge 2$ and $A + B_i = A + B_1 + h_i$ for each i, $1 \le i \le n$. We may assume that $|H|$ is a prime, that is, $n = |H| = p$. It follows that $|B_1| = \cdots = |B_n|$ and so $p|B_1| = p^2$. We get that $|B_1| = p$. Note that G has the following $p + 1$ subgroups of order p:

$$\langle px \rangle,$$
$$\langle ipx + py \rangle, \quad 0 \le i \le p-1.$$

It follows that H is one of these subgroups.

As in the proof of Theorem 5.9 (on page 109), we can see that $G = A + B_i + H$ is a factorization of G. It follows that the sum $A + H$ is direct. If $H \in \{K_1, K_2\}$, then the sum $A + H$ is certainly not direct and so $H \notin \{K_1, K_2\}$. Now $H + K_1 = H + K_2 = L$ are factorizations of L. Set $C = \{a_0, a_1, \ldots, a_{p-1}\}$. The computation

$$\begin{aligned} A + H &= [(a_0 + K_1) \cup (a_1 + K_2) \cup \cdots \cup (a_{p-1} + K_2)] + H \\ &= (a_0 + K_1 + H) \cup (a_1 + K_2 + H) \cup \cdots \cup (a_{p-1} + K_2 + H) \\ &= (a_0 + L) \cup (a_1 + L) \cup \cdots \cup (a_{p-1} + L) \\ &= \{a_0, a_1, \ldots, a_{p-1}\} + L \\ &= C + L. \end{aligned}$$

shows that the sum $C + L$ is equal to $A + H$. The cardinalities give that the equation $A + H = C + L$ is a factorization of $A + H$. Clearly, $G = B_i + C + L$ is a factorization of G.

Note that the elements of B are distributed over the residue classes modulo L in the following way:

$$\begin{aligned} 0y + \langle px + 2py \rangle &\subseteq 0y + L, \\ 1y + \langle py \rangle &\subseteq 1y + L, \\ &\vdots \\ (p-1)y + \langle py \rangle &\subseteq (p-1)y + L. \end{aligned}$$

Since the sum $B_i + L$ is direct, it follows that B_i contains exactly one element from each of

$$0y + \langle px + 2py \rangle, \quad 1y + \langle py \rangle, \ldots, (p-1)y + \langle py \rangle.$$

There are integers α_1, β_1 such that $1 \leq \alpha_1, \beta_1 \leq p-1$ and

$$0y + \alpha_1(px + 2py), \quad 1y + \beta_1 py \in B_1.$$

Similarly, there are integers α_2, β_2 such that $1 \leq \alpha_2, \beta_2 \leq p-1$ and

$$0y + \alpha_2(px + 2py), \quad 1y + \beta_2 py \in B_2.$$

Consider the equation $A + B_2 = A + B_1 + h_2$ and write it in the form $A + B_1 = A + B_2 + k$, where $k = -h_2$. Restricting both sides of the equation $A + B_1 = A + B_2 + k$ to L, we get

$$\begin{aligned} A + (B_1 \cap L) &= A + k + (B_2 \cap L), \\ A + \alpha_1(px + 2py) &= A + k + \alpha_2(px + 2py). \end{aligned}$$

As A is not periodic it follows that

$$\begin{aligned} \alpha_1(px + 2py) &= k + \alpha_2(px + 2py), \\ k &= (\alpha_1 - \alpha_2)(px + 2py). \end{aligned}$$

Restricting both sides of the equation $A + B_1 - y = A + k + B_2 - y$ to L gives that

$$A + [(B_1 - y) \cap L] = A + k + [(B_2 - y) \cap L].$$

Then, adding y we get that

$$\begin{aligned} A + [B_1 \cap (L + y)] &= A + k + [B_2 \cap (L + y)] \\ A + y + \beta_1 py &= A + k + y + \beta_2 py, \\ A + \beta_1 py &= A + k + \beta_2 py. \end{aligned}$$

As A is not periodic it follows that

$$\begin{aligned} \beta_1 py &= k + \beta_2 py, \\ k &= (\beta_1 - \beta_2)py. \end{aligned}$$

Comparing the two expressions we have for k gives that

$$(\alpha_1 - \alpha_2)(px + 2py) = (\beta_1 - \beta_2)py.$$

Since x, y is a basis for G, it follows that $\alpha_1 = \alpha_2$. This is a contradiction since $B_1 \cap B_2 = \emptyset$. Thus B does not have a regular partition in the factorization $G = A + B$. In an analogous way we can verify that A does not have a regular partition either. ∎

THEOREM 5.11

Let p be an odd prime. A group of type $Z(p^3) \oplus Z(p)$ has a non-quasi-periodic factorization.

PROOF Let G be a group of type $Z(p^3) \oplus Z(p)$ with basis elements x, y, where $|x| = p^3$, $|y| = p$. Set $a_i = ix$, $b_i = ipx$, $0 \le i \le p-1$,

$$\begin{aligned} K_1 &= \langle p^2 x \rangle, \qquad K_2 = \langle y \rangle, \\ K_3 &= \langle p^2 x + y \rangle, \; K_4 = \langle 2p^2 x + y \rangle, \end{aligned}$$

$$\begin{aligned} A &= [a_0 + K_1] \cup [a_1 + K_2] \cup \cdots \cup [a_{p-1} + K_2], \\ B &= [b_0 + K_3] \cup [b_1 + K_4] \cup \cdots \cup [b_{p-1} + K_4]. \end{aligned}$$

One can verify that each of the sums

$$K_1 + K_3, \quad K_1 + K_4, \quad K_2 + K_3, \quad K_2 + K_4$$

is a factorization of $\langle p^2 x, y \rangle$ and that the elements $a_i + b_j$, $0 \le i, j \le p-1$ form a complete set of representatives of G modulo $\langle p^2 x, y \rangle$. By Lemma 2.19 (on page 29), $G = A + B$ is a normalized factorization of G. Lemma 2.20 (on page 29) can be used to show that neither A nor B is periodic.

We want to prove that the factorization $G = A+B$ is not quasi-periodic. To prove the claim assume the contrary, that the factorization is quasi-periodic. Assume first that A has a regular partition. This means that there is a partition $A_1 \cup \cdots \cup A_n$ of A and there is a subgroup $H = \{h_1, \ldots, h_n\}$ of G such that $h_1 = 0$, $|H| \ge 2$ and $A_i + B = A_1 + B + h_i$ for each i, $1 \le i \le n$. We may assume that $|H|$ is a prime, that is, $n = |H| = p$. It follows that $|B_1| = \cdots = |B_n|$ and so $p|B_1| = p^2$. We get that $|B_1| = p$. Note that G has the following $p+1$ subgroups of order p:

$$\begin{aligned} &\langle p^2 x \rangle, \\ &\langle ip^2 x + y \rangle, \quad 0 \le i \le p-1. \end{aligned}$$

It follows that H is one of these subgroups.

As in the proof of Theorem 5.9 (on page 109), we can see that $G = A_i + B + H$ is a factorization of G. It follows that the sum $B + H$ is direct. If $H \in \{K_3, K_4\}$, then the sum $B+H$ is plainly not direct and so $H \notin \{K_3, K_4\}$. Set $L = \langle p^2 x, y \rangle$, $C = \{b_0, b_1, \ldots, b_{p-1}\}$ and note that $H + K_3 = H + K_4 = L$ are factorizations of L. The computation

$$\begin{aligned} B + H &= [(b_0 + K_3) \cup (b_1 + K_4) \cup \cdots \cup (b_{p-1} + K_4)] + H \\ &= (b_0 + K_3 + H) \cup (b_1 + K_4 + H) \cup \cdots \cup (b_{p-1} + K_4 + H) \\ &= (b_0 + L) \cup (b_1 + L) \cup \cdots \cup (b_{p-1} + L) \\ &= \{b_0, b_1, \ldots, b_{p-1}\} + L \\ &= C + L \end{aligned}$$

shows that the sum $C + L$ is equal to $B + H$. The cardinalities imply that the equation $B + H = C + L$ is a factorization of $B + H$. Clearly, $G = A_i + C + L$ is a factorization of G.

Note that the elements of A are distributed over the residue classes modulo L in the following way:

$$\begin{aligned} 0y + \langle px + 2py \rangle &\subseteq 0y + L, \\ 1y + \langle py \rangle &\subseteq 1y + L, \\ &\vdots \\ (p-1)y + \langle py \rangle &\subseteq (p-1)y + L. \end{aligned}$$

Since the sum $A_i + L$ is direct, it follows that A_i contains exactly one element from each of

$$0x + \langle p^2 x \rangle, \quad 1x + \langle y \rangle, \ldots, (p-1)x + \langle y \rangle.$$

Since A_1 has exactly one element from $\langle p^2 x \rangle$ and exactly one element from $\langle y \rangle$, it follows that there are integers α_1, β_1 such that $1 \leq \alpha_1, \beta_1 \leq p-1$, and

$$0x + \alpha_1(p^2 x), \quad 1x + \beta_1 y \in A_1.$$

Similarly, there are integers α_2, β_2 such that $1 \leq \alpha_2, \beta_2 \leq p-1$, and

$$0x + \alpha_2(p^2 x), \quad 1x + \beta_2 y \in A_2.$$

Considering the equation $A_2 + B = A_1 + B + h_2$, we can derive the contradiction that $A_1 \cap A_2 \neq \emptyset$ in the same way as in the proof of Theorem 5.10 (on page 111).

The case when B admits a regular partition can be settled in a similar way. □

We spell out a consequence of Theorems 5.8–5.11.

COROLLARY 5.2

Let p be a prime and let $G = Z(p^\alpha) \oplus Z(p^\beta)$. In the following cases there is a factorization $G = A + B$ that is not quasi-periodic:

$$\begin{aligned} &p \geq 5, \quad \alpha \geq 2, \quad \beta \geq 1, \\ &p = 3, \quad \alpha \geq 2, \quad \beta \geq 2, \\ &p = 3, \quad \alpha \geq 3, \quad \beta \geq 1. \end{aligned}$$

The next result indicates a connection between the Rédei property and quasi-periodicity.

THEOREM 5.12

Let $G = A + B$ be a normalized factorization of the finite abelian group G. If $\langle A \rangle$ has a periodic set C of coset representatives, then the factorization is quasi-periodic.

PROOF Let $H = \langle A \rangle$. Then $G = H + C$ is a factorization. Let $C = \{c_1, \ldots, c_n\}$, where $c_1 = 0$. Let us define B_i by

$$B_i = B \cap (H + c_i), \quad 1 \leq i \leq n.$$

Now the sets $B_1, \ldots, B_n$ form a partition of B. From the factorization $G = A + B$ by adding $-c_i$ to both sides we get the factorization $G = A + (B - c_i)$. Since $A \subseteq H$, restricting the factorization $G = A + (B - c_i)$ to H, we get the factorization

$$H = A + \big[(B - c_i) \cap H\big].$$

Adding c_i to both sides gives

$$H + c_i = A + \big[B \cap (H + c_i)\big],$$

that is, $H + c_i = A + B_i$. In particular, $H = A + B_1$. Therefore $A + B_1 + c_i = A + B_i$, as required. □

COROLLARY 5.3

Let p be a prime. Each normalized factorization of an elementary p-group with the Rédei property is quasi-periodic.

THEOREM 5.13

Let p be a prime. Let G be a finite abelian group that is the direct sum of its subgroups H and K. If p does not divide $|H|$ and $|K| = p$, then each normalized factorization of G is quasi-periodic.

PROOF Let $G = A + B$ be a normalized factorization of G. Since the order of G is equal to the product of the orders of A and B, we may assume that $p \nmid |A|$ and $p \mid |B|$. Let $K = \langle f \rangle$. The factor A can be written in the form

$$A = A_0 \cup \cdots \cup A_{p-1},$$

where $A_i = A \cap (H + if)$. Further, there are subsets $D_0, \ldots, D_{p-1} \subseteq H$ such that $A_i = D_i + if$. Thus

$$A = [D_0 + 0f] \cup \cdots \cup [D_{p-1} + (p-1)f].$$

Similarly, B can be written in the form

$$B = B_0 \cup \cdots \cup B_{p-1},$$

where $B_i = B \cap (H + if)$. There are subsets $C_0, \ldots, C_{p-1} \subseteq H$ such that $B_i = C_i + if$. Therefore

$$B = [C_0 + 0f] \cup \cdots \cup [C_{p-1} + (p-1)f].$$

We claim that $A+B_v = A+B_0+vf$ holds for each v, $1 \le v \le p-1$. Using the above notations, the claim is equivalent to

$$\begin{aligned}&([D_0+0f] \cup \cdots \cup [D_{p-1}+(p-1)f]) + [C_v+vf]\\ &= ([D_0+0f] \cup \cdots \cup [D_{p-1}+(p-1)f]) + [C_0+0f] + vf,\end{aligned}$$

that is, it is equivalent to

$$\begin{aligned}&[D_0+C_v+0f] \cup \cdots \cup [D_{p-1}+C_v+(p-1)f]\\ &= [D_0+C_0+0f] \cup \cdots \cup [D_{p-1}+C_0+(p-1)f].\end{aligned}$$

In fact we will verify that $D_u+C_v = D_u+C_0$ holds for each u, v, $0 \le u \le p-1$, $1 \le v \le p-1$.

Choose an integer $t(i)$ such that

$$\begin{aligned}t(i) &\equiv 1 \pmod{|H|},\\ t(i) &\equiv i \pmod{|K|}.\end{aligned}$$

Such a $t(i)$ exists for each i, $0 \le i \le p-1$. In the factorization $G = A+B$, the factor A can be replaced by $t(i)A$ to get the normalized factorization $G = t(i)A+B$. Note that

$$\begin{aligned}t(i)A &= [t(i)D_0 + t(i)0f] \cup \cdots \cup [t(i)D_{p-1} + (p-1)t(i)f]\\ &= [D_0+0f] \cup \cdots \cup [D_{p-1}+(p-1)if].\end{aligned}$$

The factorization

$$G = ([D_0+0f] \cup \cdots \cup [D_{p-1}+(p-1)f]) + B$$

provides that the sets

$$D_0+B+0f, \ldots, D_{p-1}+B+(p-1)f \tag{5.6}$$

form a partition of G. The $i=0$ and $i=1$ special cases of (5.6) give that

$$\begin{aligned}&[D_1+B] \cup \cdots \cup [D_{p-1}+B]\\ &= [D_1+B+f] \cup \cdots \cup [D_{p-1}+(p-1)f+B].\end{aligned} \tag{5.7}$$

Choose an integer u, $1 \le u \le p-1$. Note that

$$[D_u+B] \cap [D_w+B+wf] = \emptyset$$

for each w, $1 \le w \le p-1$, $w \ne u$. In order to verify the claim, assume on the contrary that

$$[D_u+B] \cap [D_w+B+wf] \ne \emptyset$$

for some u and w. Adding uif to both sides, we get

$$[D_u + B + uif] \cap [D_w + B + (w + iu)f] \neq \emptyset. \tag{5.8}$$

The congruence

$$wi \equiv w + iu \pmod{p}$$

is solvable for i and so (5.8) contradicts (5.6). This contradiction proves our claim.

From (5.7) it follows that $[D_u + B] = [D_u + B + uf]$. Using this equation repeatedly we get that

$$D_u + B = D_u + B + f = D_u + B + 2f = \cdots = D_u + B + (p-1)f.$$

Choose an integer v, $1 \leq v \leq p-1$. The equation $D_u + B = D_u + B + (p-v)f$ can be written in the form

$$\begin{aligned} &D_u + ([C_0 + 0f] \cup \cdots \cup [C_{p-1} + (p-1)f]) \\ &= D_u + ([C_0 + (p-v)f] \cup \cdots \cup [C_{p-1} + (p-v+p-1)f]), \end{aligned}$$

that is, in the form

$$\begin{aligned} &[D_u + C_0] \cup \cdots \cup [D_u + C_{p-1} + (p-1)f] \\ &= [D_u + C_0 + (p-v)f] \cup \cdots \cup [D_u + C_{p-1} + (p-v+p-1)f]. \end{aligned}$$

Intersecting by H we get $D_u + C_0 = D_u + C_v$. This holds for each u, v, $1 \leq u \leq p-1$, $1 \leq v \leq p-1$. (The $u = 0$ case is not covered.)

It remains to verify that $D_0 + C_v = D_0 + C_0$ holds for each v, $1 \leq v \leq p-1$. In fact we will show that $D_u + C_0 = D_u + C_v$ holds for each u, v, $0 \leq u \leq p-2$, $1 \leq v \leq p-1$. Adding f to the factorization $G = A + B$, we get the normalized factorization $G = (A + f) + B$. Here

$$A + f = [D_0 + 1f] \cup [D_1 + 2f] \cup \cdots \cup [D_{p-2} + (p-1)f] \cup D_{p-1}.$$

(Now D_{p-1} will play the earlier role of D_0.) Repeating the whole argument in this setting, we get the required result. ∎

COROLLARY 5.4

If n is a square-free integer, then each normalized factorization $Z(n) = A + B$ is quasi-periodic.

One might wonder, if each normalized factorization of a finite abelian group G is quasi-periodic, then does this hold for each subgroup of G? Using Theorem 5.13 (on page 116) and Theorem 5.9 (on page 109), we can see that for this question the answer is "no."

TABLE 5.3: The factors A and B

A			B		
0000			0000	2012	4031
1000	0010	0013	0141	2103	4122
2000	0020	0021	0223	2230	4204
3000	0030	0034	0332	2344	4313
4000	0040	0042	0414	2421	4440
0100	0001	0011	1024	3043	
0200	0002	0022	1110	3134	
0300	0003	0033	1242	3211	
0400	0004	0044	1301	3320	
			1433	3402	

EXAMPLE 5.5 Let G be a group of type $Z(2)\oplus Z(25)\oplus Z(5)$. Now G is a direct sum of its subgroups H and K, whose types are $Z(2)$ and $Z(25)\oplus Z(5)$, respectively. By Theorem 5.13 (on page 116), each normalized factorization of G is quasi-periodic. By Theorem 5.9 (on page 109), the subgroup K of G admits non-quasi-periodic factorizations. □

The factorizations of finite abelian groups have applications in cryptography. For instance, Minghua Qu and S. A. Venstone [105] used a classical result of L. Rédei [107] in cryptography. Since checking if a given factorization is quasi-periodic or not seems computationally expensive, we think that quasi-periodicity can be used in cryptography too.

EXAMPLE 5.6 To illustrate the difficulties in checking quasi-periodicity, let G be a group of type $Z(5) \oplus \cdots \oplus Z(5)$ with basis elements x, y, u, v. The element $ax + by + cu + dv$ is encoded simply by the coefficients $[a, b, c, d]$. Consider the subsets A and B of G given in Table 5.3 (on page 119). One can check that $G = A + B$ is a factorization of G. We may notice that $\langle A\rangle = \langle B\rangle = G$. If it were the case that $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$, then for sure the factorization would be quasi-periodic. We do not know if this factorization is quasi-periodic or not. If fact, to decide if the factorization is quasi-periodic looks difficult. The group G has $(5^4 - 1)/4 = 156$ subgroups of order 5. Further, the factor A can be partitioned in the form $A = A_1 \cup \cdots \cup A_5$ in $(24!)/((4!)(5!)(5!)(5!)(5!))$ ways, assuming that $0 \in A_1$. □

We close the chapter with some open problems. Let $G = A + B$ be a normalized factorization of G and suppose that $B_1 \cup \cdots \cup B_n$ is a regular partition of B, that is, there is a subsgroup $H = \{h_1, \ldots, h_n\}$ of G such that $|H| \geq 2$, $h_1 = 0$ and $A + B_i = A_1 + B_1 + h_i$ for each i, $1 \leq i \leq n$. In the proof of Theorem 5.9 (on page 109), we saw that from these it follows that $G = A + B_i + H$. In other words, in the factorization $G = A + B$, factor B can be replaced by a periodic subset.

PROBLEM 5.2 (See [123].) Is it true that in each factorization $G = A+B$ of a finite abelian group G at least one of the factors can be replaced by a periodic subset? □

From Corollary 5.4 (on page 118) it is clear that if n is a square-free integer, then in each factorization $Z(n) = A + B$ one of the factors can be replaced by a periodic subset.

PROBLEM 5.3 Is it true that in each normalized factorization $G = A+B$ of a finite abelian group G at least one of the factors can be replaced by a subset that does not span the whole G? □

PROBLEM 5.4 Are there finite cyclic groups that have non-quasi-periodic factorizations? Are there finite elementary p-groups with non-quasi-periodic factorizations, where p is a prime? Are there finite abelian 2-groups admitting non-quasi-periodic factorizations? □

Notes

(1) By Corollary 5.3 (on page 116) if an elementary p-group G has the Rédei property, then G admits only quasi-periodic factorizations. We would like to mention the following results on characterizing elementary p-groups with the Rédei property. Let p be a prime and let $f(p)$ be the largest integer such that each elementary p-group of rank $f(p)$ has the Rédei property. From [107], it follows that $f(p) \geq 2$ for each p. By [101], $f(2) = 9$ and by [100], $f(3) = 5$. A construction of [26] shows that $f(p) \leq 4$ for $p \geq 5$ and in [164] it was verified that $f(p) = 3$ for $p = 5, 7, 11$.

(2) In 1953 N. G. de Bruijn [11] nearly proved that each factorization of a cyclic group of square-free order is always quasi-periodic. After more than fifty years, Theorem 5.13 (on page 116) settles this problem.

(3) Quasi-periodicity can be defined in connection with multiple factorization, too. J. P. Steinberger [146] deals with k-fold quasi-periodic factorizations. In fact, his investigations were motivated by [11].

Chapter 6

Factoring by many factors

6.1 Factoring periodic subsets

In this section we consider factorization of a periodic subset instead of a group. Plainly, a group distinct from $\{0\}$ is always periodic, so we deal with an extension of factoring groups.

Let G be a finite abelian group and let A be a subset of G. We say that A is *weakly periodic* if there is an element $g \in G \setminus \{0\}$ such that A and $g + A$ mutually differ in at most one element. In other words, either $A = g + A$ and so A is periodic or A contains one element that is not in $g + A$ and conversely $g + A$ contains one element that is not in A. The element g is called a *weak period* of A. Note that if g is a weak period of A, then so is $-g$. It is clear that a periodic subset is weakly periodic. Also, a cyclic subset is weakly periodic.

Let G be a finite abelian group. We single out a family of subsets of G and call them hereditary periodicity forcing subsets of G, in short, HPF subsets of G. In fact, this way of talking is too loose and we have to exercise a little more care.

A subset A of G is said to be periodicity forcing if each factorization $G = A + B$ implies that either A or B is periodic. In short we say that A is a PF subset.

Let F be a family of finite abelian groups that is closed with respect to taking subgroups and quotient groups. With each group G in F, let there be associated a family of subsets $S(G)$. We assume that the subsets in $S(G)$ are PF subsets. Let A be a subset in $S(G)$. If A is periodic and P is the group of periods of A, then we require that $(A + P)/P$ belong to $S(G/P)$. Let $G = A + B$ be a factorization of G and let Q be the group of periods of B. Then we require that $(A + Q)/Q$ belong to $S(G/Q)$. If these families of subsets $S(G)$ of groups G in F satisfy these additional properties, we shall say that this family has the HPF property.

We now give examples of such families. Firstly, let F consist of all finite abelian groups and let $S(G)$, for each G in F, consist of all weakly periodic subsets of G.

LEMMA 6.1
The family $S(G)$, $G \in F$ has the HPF property.

PROOF Let A be a weakly periodic subset with weak period g. We claim that A is in one of the following forms:

$$D + \langle g \rangle,$$
$$h + \{0, g, 2g, \ldots, (r-1)g\},$$
$$[D + \langle g \rangle] \cup [h + \{0, g, 2g, \ldots, (r-1)g\}.$$

Here $D \subseteq G$, $h \in G$, r is an integer and the union is disjoint. The subset $D + \langle g \rangle$ is periodic with period g. The subset $h + \{0, g, 2g, \ldots, (r-1)g\}$ is a translated copy of the cyclic subset $\{0, g, 2g, \ldots, (r-1)g\}$.

In order to prove the claim suppose that A is weakly periodic but not periodic. Let h be in A but not in $g + A$. Then $h + g \in g + A$ and, as A contains only one element not in $g + A$, $h + g \in A$. Suppose that $h + sg \in A$, $0 \leq s \leq r - 1$ but that $a + rg \notin A$. Let $C = \{0, g, 2g, \ldots, (r-1)g\}$. Then $h + C \subseteq A$. Suppose that $g + C \neq Q$. Let $A = (g + C) \cup B$, where $(g + C) \cap B = \emptyset$. Then $g + B = B$ since A and $g + A$ differ in one element only. So A is the disjoint union of a periodic subset B with period g and a translate of the cyclic subset C.

Consider a factorization $G = A + B$. The factorization is equivalent to the fact that the sets

$$a + B, \quad a \in A$$

form a partition of G. Adding g to the factorization $G = A + B$, we get the factorization $G = g + G = (g + A) + B$. This means that the sets

$$g + a + B, \quad a \in A$$

form a partition of G. Comparing the two partitions gives that $h + B = h + rg + B$ or, equivalently, $B = rg + B$. If $rg = 0$, then A is periodic with period g. If $rg \neq 0$, then B is periodic with period rg. So A is a PF subset.

It remains to prove that any homomorphic image of a weakly periodic subset is weakly periodic. To prove this let H be a subgroup of G. The homomorphic image of A in the factor group G/H under the natural homomorphism is

$$(A + H)/H = \{(a + H) : \ a \in A\}.$$

It is plain that $(g + H)$ is a weak period of $(A + H)/H$. Therefore A is an HPF subset. ∎

For the second example we restrict our attention to the family F of all finite abelian groups G whose p-component is cyclic, where p is a given prime. This family is closed under the formation of subgroups and of quotient groups. For each G in F we define $S(G)$ to be the family of subsets of order p^α, $\alpha \geq 0$.

LEMMA 6.2
Let p be a prime. The families $S(G)$ satisfy the HPF property.

PROOF Let A be an element of $S(G)$ and let $G = A+B$ be a factorization of G. By Theorem 4.3 (on page 67), either A or B is periodic. This means that A is a PF subset.

If H is any subgroup of G, then it is clear that $(A+H)/H$ has order which divides $|A|$ and so it is a power of p. Hence $(A+H)/H$ is an element of $S(G/H)$. It follows that $S(G)$, $G \in F$ has the HPF property. □

LEMMA 6.3
Let G be a finite cyclic group and let $G = A+B$ be a normalized factorization of G. If A is an HPF subset of G and A is not periodic, then there are cyclic subsets $C_1, \ldots, C_s$ such that $G = C_1 + \cdots + C_s + B$ is a factorization of G, each $|C_i|$ is a prime, and each C_i is not periodic.

PROOF We divide the proof into two parts. First we prove that there are cyclic subsets $C_1, \ldots, C_s$ such that $G = C_1 + \cdots + C_s + B$ is a factorization of G and each $|C_i|$ is a prime. Here we do not mind if some of the factors happen to be a subgroup of G.

If $|B| = 1$, that is, $B = \{0\}$, then A is periodic. By the hypotheses of the lemma, A is not periodic so $|B| \geq 2$. Assume that $|B|$ is a prime, say $|B| = p$. Let $|G| = np$ and let g be a generator element of G. From the factorization $G = A + B$, since A is an HPF subset of G, it follows that either A or B is periodic. By the assumption of the lemma, B is periodic. In fact B is a subgroup of G and so $B = \langle ng \rangle$. Let

$$C = \{0, g, 2g, \ldots, (n-1)g\}.$$

It is easy to check that $G = C + \langle ng \rangle$ is a factorization of G. Using the identity

$$\begin{aligned}\{0, a, 2a, \ldots, (uv-1)a\} = {} & \{0, a, 2a, \ldots, (u-1)a\} + \\ & \{0, ua, 2ua, \ldots, (v-1)ua\}\end{aligned}$$

we can decompose C into a sum of the cyclic subset $C_1, \ldots, C_s$ such that each $|C_i|$ is a prime.

Let $\nu\big(|B|\big)$ be the number of the not necessarily distinct prime factors of $|B|$. The $\nu\big(|B|\big) = 1$ case is settled so we assume that $\nu\big(|B|\big) \geq 2$ and proceed by an induction on $\nu\big(|B|\big)$. Consider the factorization $G = A + B$. As A is an HPF subset of G, we get that B is periodic. By Lemma 2.8 (on page 18), there is a subgroup H of G and a subset D of B such that B is a direct sum of H and D and $|H|$ is a prime. From the factorization $G = A + (H + D)$, by considering the factor group G/H, we get the factorization

$$G/H = [(A+H)/H] + [(D+H)/H]$$

of G/H. Clearly G/H is a finite cyclic group and the factor $(A+H)/H$ is an HPF subset of G/H. The induction assumption gives that there are cyclic subsets $C_1, \ldots, C_s$ of G such that

$$G/H = [(C_1 + H)/H] + \cdots + [(C_s + H)/H] + [(D + H)/H]$$

is a factorization of G/H and each $|C_i|$ is a prime. It follows that $C_1 + \cdots + C_s + D$ is a complete set of representatives modulo H. Now

$$\begin{aligned} G &= (C_1 + \cdots + C_s + D) + H \\ &= C_1 + \cdots + C_s + (D + H) \\ &= C_1 + \cdots + C_s + B \end{aligned}$$

are factorizations of G.

If there is no subgroup among $C_1, \ldots, C_s$, then we are done. Suppose there is a subgroup among $C_1, \ldots, C_s$, say C_1. Now both H and C_1 are subgroups of G and both have a prime number of elements. It follows that $|H| \neq |C_1|$. Let $C_1 = \langle c \rangle$ and let $H = \langle h \rangle$. In the direct sum $H + C_1$, C_1 can be replaced by

$$C_1' = \{0, c + h, 2(c + h), \ldots, (p-1)(c + h)\},$$

that is, $H + C_1 = H + C_1'$. Obviously C_1' is not a subgroup. Therefore

$$\begin{aligned} G &= C_1 + \cdots + C_s + B \\ &= C_1 + \cdots + C_s + (D + H) \\ &= H + C_1 + \cdots + C_s + D \\ &= H + C_1' + C_2 + \cdots + C_s + D \\ &= C_1' + C_2 + \cdots + C_s + (D + H) \\ &= C_1' + C_2 + \cdots + C_s + B \end{aligned}$$

are factorizations of G. In this way we can get rid of all the subgroups among $C_1, \ldots, C_s$. □

THEOREM 6.1

Let G be a finite cyclic group and let $G = A_1 + \cdots + A_k + B$ be a normalized factorization of G such that $A = A_1 + \cdots + A_k$ is periodic and each A_i is an HPF subset of G. Then one of the factors $A_1, \ldots, A_k$ is periodic.

PROOF Assume the contrary, that there is a counter-example for the theorem. If $k = 1$, then, by the assumptions of the theorem, A_1 is periodic. Thus in a counter-example $k \geq 2$. If $B = \{0\}$, then $G = A_1 + \cdots + A_k$ is a factorization of G. By Lemma 6.3 (on page 123), there are non-subgroup cyclic subsets of prime cardinality $C_1, \ldots, C_s$ such that $G = C_1 + \cdots + C_s$ is a factorization of G. By Theorem 4.3 (on page 67), one of the factors $C_1, \ldots, C_s$ is periodic. This is a contradiction. Thus in a counter-example $B \neq \{0\}$.

Let g be a period of $A = A_1 + \cdots + A_k$. Choose a $b \in B \setminus \{0\}$ and set $C = \big(B \setminus \{0\}\big) \cup \{b + g\}$. Define a function $\varphi : B \to H$ by

$$\varphi(b_1) = \begin{cases} 0, & \text{if} \quad b_1 \neq b, \\ g, & \text{if} \quad b_1 = b, \end{cases}$$

and note that $C = H \circ_\varphi B$. By Lemma 2.12 (on page 21), it follows that the sum $A + C$ is direct and is equal to $A + B$. Therefore $G = A + C$ is a factorization of G, that is,

$$G = A_1 + \cdots + A_k + C \tag{6.1}$$

is a normalized factorization of G. In the factorization $G = A_1 + \cdots + A_k + B$ by Lemma 6.3 (on page 123), each A_i can be replaced by a sum of non-subgroup cyclic subsets to get the normalized factorization

$$G = C_1 + \cdots + C_u + B. \tag{6.2}$$

Similarly, in (6.1), each A_i can be replaced by a sum of non-subgroup cyclic subsets to get the normalized factorization

$$G = D_1 + \cdots + D_v + C. \tag{6.3}$$

Let χ be a faithful character of G. Applying χ to (6.2) we get that

$$0 = \chi(C_1) \cdots \chi(C_u)\chi(B).$$

If $\chi(C_i) = 0$ for some i, $1 \leq i \leq u$, then C_i is a subgroup of G. This is not the case and so $\chi(B) = 0$. A similar argument in connection with (6.3) gives that $\chi(C) = 0$. Now

$$\begin{aligned} 0 &= \chi(B) - \chi(C) \\ &= \chi(b) - \chi(b + g) \\ &= \chi(b) - \chi(b)\chi(g) \\ &= \chi(b)[1 - \chi(g)]. \end{aligned}$$

It follows that $\chi(g) = 1$ and then $g = 0$. This contradiction completes the proof. ∎

THEOREM 6.2

Let G be a finite cyclic group and let $A_1, \ldots, A_k$ be cyclic subsets or simulated subsets of G. Assume that $A = A_1 + \cdots + A_k$ is periodic. Then one of the factors $A_1, \ldots, A_k$ is a subgroup of G.

PROOF Let g be a period of A and let χ be a faithful character of G. Applying χ to the equation $A = A + g$ we get that $\chi(A) = \chi(A + g) =$

$\chi(A)\chi(g)$ and then $\chi(A)[1-\chi(g)]=0$. As $g\neq 0$ we get $\chi(g)\neq 1$. Thus $0=\chi(A)=\chi(A_1)\cdots\chi(A_k)$ and so $\chi(A_i)=0$ for some i, $1\leq i\leq k$. Suppose first that A_i is a cyclic subset, say

$$A_i=\{0,a,2a,\ldots,(q-1)a\}.$$

Now

$$\chi(A_i)=1+\chi(a)+[\chi(a)]^2+\cdots+[\chi(a)]^{q-1}.$$

Note that $\chi(a)\neq 1$ as $a\neq 0$. Therefore

$$0=\chi(A_i)=\frac{1-[\chi(a)]^q}{1-\chi(a)}.$$

It follows that $[\chi(a)]^q=1$, that is, $qa=0$, and so A_i is a subgroup of G.

Secondly, suppose that A_i is a simulated subset, say

$$A_i=\big(H\setminus\{l\}\big)\cup\{l+d\},$$

where H is a subgroup of G, $l\in H$, $d\in G$. Now

$$\chi(A_i)=\Big[\sum_{h\in H}\chi(h)\Big]-\chi(l)+\chi(l+d).$$

Note that

$$\Big[\sum_{h\in H}\chi(h)\Big]=0.$$

Therefore $0=\chi(A_i)=\chi(l)[\chi(d)-1]$. It follows that $\chi(d)=1$. Then $d=0$ and so A_i is a subgroup of G. ∎

Let $A_1,\ldots,A_k$ be subsets of a finite cyclic group G. If each element g of G can be expressed exactly n ways in the form

$$g=a_1+\cdots+a_k,\quad a_1\in A_1,\ldots,a_k\in A_k,$$

then we say that the sum $A_1+\cdots+A_k$ is an n-fold factorization of G. Using the ideas in the proof of Theorem 6.2 (on page 125), one can prove the following result.

THEOREM 6.3

Let G be a finite cyclic group, and let $A_1,\ldots,A_k$ be cyclic or simulated subsets of G. If $A_1+\cdots+A_k$ is an n-fold factorization of G, then at least one of the factors $A_1,\ldots,A_k$ is a subgroup of G.

The next two examples show that the conditions that the group is cyclic or the factors are cyclic cannot be dropped from Theorem 6.2 (on page 125), respectively.

EXAMPLE 6.1 Let $G = Z(2) \oplus Z(3) \oplus Z(3)$ and let x, y, z be a system of generators of G such that $|x| = 2$, $|y| = |z| = 3$. Set

$$\begin{aligned} A &= G \setminus \{x + 2z, 2z\}, \\ A_1 &= \{0, x + z\}, \\ A_2 &= \{0, x + y\}, \\ A_3 &= \{0, x + y + z\}, \\ A_4 &= \{0, x + y + 2z\}. \end{aligned}$$

One can verify that the sum $A_1 + \cdots + A_4$ is direct and is equal to A. Further, A is periodic with period x and none of the factors $A_1, \ldots, A_4$ is a subgroup of G. □

EXAMPLE 6.2 Let $G = Z(p) \oplus Z(q) \oplus Z(r)$ and let x, y, z be a system of generators of G with $|x| = p$, $|y| = q$, $|z| = r$. Here p, q, r are distinct primes. Set

$$\begin{aligned} A &= \big(\langle y \rangle \cup (z + \{0, y, 2y, \ldots, (p-1)y\})\big) + \langle x \rangle, \\ A_1 &= \langle y \rangle \cup (z + \langle x \rangle), \\ A_2 &= \{0, x + y, 2(x + y), \ldots, (p-1)(x + y)\}. \end{aligned}$$

It is clear that A is periodic with period x. We claim that the sum $A_1 + A_2$ is direct and is equal to A. We show that

$$\begin{aligned} \chi(A) &= \chi(A_1 + A_2) \\ &= \chi(A_1)\chi(A_2) \end{aligned}$$

holds for each character χ of G. For the principal character this obviously holds. Choose a non-principal character χ of G. Suppose that $\chi(x) \neq 1$. Now $\chi(A) = 0$. If $\chi(y) = 1$, then $\chi(A_2) = 0$. If $\chi(y) \neq 1$, then $\chi(A_1) = 0$. Thus we may assume that $\chi(x) = 1$. Now

$$\begin{aligned} \chi(A) &= \big[\chi(\langle y \rangle) + \chi(z)(1 + \chi(y) + [\chi(y)]^2 + \cdots + [\chi(y)]^{p-1})\big]p, \\ \chi(A_1) &= \chi(\langle y \rangle) + \chi(z)p, \\ \chi(A_2) &= 1 + \chi(y) + [\chi(y)]^2 + \cdots + [\chi(y)]^{p-1}. \end{aligned}$$

We can see that $\chi(A) = \chi(A_1)\chi(A_2)$ holds. □

The following examples illustrate that the condition that the factors are cyclic or simulated subsets cannot be relaxed in Theorem 6.3 (on page 126).

EXAMPLE 6.3 Let $G = Z(p_1) \oplus Z(p_2) \oplus Z(q)$, where p_1, p_2, q are distinct primes. Let x_1, x_2, y be a system of generators of G such that $|x_1| = p_1$, $|x_2| = p_2$, $|y| = q$. Set

$$\begin{aligned} A_1 &= \{0, x_1, 2x_1, \ldots, (p_1 - 2)x_1, (p_1 - 1)x_1 + y\}, \\ A_2 &= \{0, x_2, 2x_2, \ldots, (p_2 - 2)x_2, (p_2 - 1)x_2 + y\}, \\ B &= \{0, y, 2y, \ldots, (q-2)y, x_1 + (q-1)y\}, \\ C &= \langle x_1 \rangle \cup x_2 + \langle y \rangle. \end{aligned}$$

We claim that the sum $A_1 + A_2 + B + C$ is a $(p_1 + q)$-fold factorization of G. It is enough to show that $\chi(A_1 + A_2 + B + C) = 0$ for each non-principal character χ of G. To prove the claim, let χ be a non-principal character of G. If $\chi(y) = 1$, then $\chi(x_i) \neq 1$ for some i, $1 \leq i \leq 2$. In this case $\chi(A_i) = 0$. Thus we may focus our attention on the $\chi(y) \neq 1$ case. If $\chi(x_1) = 1$, then $\chi(B) = 0$. If $\chi(x_1) \neq 1$, then $\chi(C) = 0$. □

EXAMPLE 6.4 Let $G = Z(p^3) \oplus Z(q)$, where p, q are distinct primes, and x, y is a generating system of G with $|x| = p^3$, $|y| = q$. Set

$$\begin{aligned} A_1 &= \{0, x, 2x, \ldots, (p-1)x\}, \\ A_2 &= \{0, px, 2px, \ldots, (p-1)px\}, \\ A_3 &= \{0, p^2x, 2p^2x, \ldots, (p-1)p^2x + y\}, \\ B &= \{0, y, 2y, \ldots, (q-2)y, p^2x + (q-1)y\}, \\ C &= \langle p^2x \rangle \cup x + \langle y \rangle. \end{aligned}$$

We claim that the sum $A_1 + A_2 + A_3 + B + C$ is a $(p+q)$-fold factorization of G. To prove the claim, pick a non-principal character χ of G. Suppose first that $\chi(y) = 1$. Since $\chi(x) \neq 1$ and $\chi(p^3x) = 1$, we get that $\chi(p^{i-1}x) \neq 1$ and $\chi(p^ix) = 1$ for some i, $1 \leq i \leq 3$. Now $\chi(A_i) = 0$. In the remaining part we may assume that $\chi(y) \neq 1$. If $\chi(p^2x) = 1$, then $\chi(B) = 0$. If $\chi(p^2x) \neq 1$, then $\chi(C) = 0$. □

The factorization $A = A_1 + A_2$ in Example 6.2 (on page 127) helps to clarify a point in connection with replacing a factor in a factorization. Let $G = A + B$ be a factorization of the finite abelian group G. If k is an integer relatively prime to $|A|$, then, by Theorem 3.17 (on page 58), in the factorization $G = A + B$ the factor A can be replaced by kA to get a factorization $G = kA + B$. Is it possible to replace the group G by a periodic subset A in the result above? The factorization $A = A_1 + A_2$ shows that the answer to this question is "no". Indeed, note that q is relatively prime to $|A_2| = p$ and

$$qA_2 = \{0, x, 2x, \ldots, (p-1)x\}.$$

Now the sum $A_1 + qA_2$ is not direct. Therefore, in the factorization $A = A_1 + A_2$, the factor A_2 cannot be replaced by qA_2 to get a factorization.

6.2 Simulated subsets

Let A be a normalized subset of a finite abelian group G and let λ be a positive integer. We say that A is a *λ-simulated subset* of G if there is a subgroup H of G such that $|A| = |H|$ and $|A \setminus H| \leq \lambda$. In words, A differs

from H in at most λ elements. We say that H is an associated subgroup of A. When $|A| = p$ is a prime and $\lambda = p - 1$, then A may have several associated subgroups. If $\lambda < |A|/2$, then from $|A \cap H| > |H|/2$ it follows that $\langle A \cap H \rangle = H$. However, the subgroup H is not determined uniquely, as shown by the next examples.

EXAMPLE 6.5 Let $G = Z(2) \oplus Z(2) \oplus Z(2)$ with basis elements x, y, z such that $|x| = |y| = |z| = 2$. Set

$$\begin{aligned} A &= \{0, x, y, y + z\}, \\ H &= \{0, x, y, x + y\} = \langle x, y \rangle, \\ K &= \{0, y, z, y + z\} = \langle y, z \rangle. \end{aligned}$$

In this case $|H| = |K| = |A|$ and $|A \cap H| = |A \cap K| = |A| - 1$, that is, A differs from both H and K only in one element. □

EXAMPLE 6.6 Let G be a group of type $Z(3) \oplus Z(3)$ with basis elements x, y, where $|x| = |y| = 3$. Set

$$\begin{aligned} A &= \{0, x, 2x + y\}, \\ H &= \{0, x, 2x\} = \langle x \rangle, \\ K &= \{0, 2x + y, x + 2y\} = \langle 2x + y \rangle. \end{aligned}$$

In this case $|H| = |K| = |A|$ and $|A \cap H| = |A \cap K| = |A| - 1$. Thus A is a 1-simulated subset with two distinct associated subgroups H and K. □

EXAMPLE 6.7 Let $G = Z(4) \oplus Z(2)$ with basis elements x, y such that $|x| = 4$, $|y| = 2$. Set

$$\begin{aligned} A &= \{0, x, 2x, y\}, \\ H &= \{0, x, 2x, 3x\} = \langle x \rangle, \\ K &= \{0, 2x, y, 2x + y\} = \langle 2x, y \rangle. \end{aligned}$$

Here $|H| = |K| = |A|$ and $|A \cap H| = |A \cap K| = |A| - 1$. Further, $H \neq K$. This means that A is a 1-simulated subset with two associated subgroups. □

The next exercise points out that the λ-simulated subsets can be expressed in terms of the composition of subsets defined in Section 2.2.

EXERCISE 6.1 Let H be a subgroup of a finite abelian group G and let $\varphi : H \to (G \setminus H) \cup \{0\}$ be a function such that $\varphi(0) = 0$. The set $G \circ_\varphi H$, the composition of G and H with respect to φ, is defined by

$$G \circ_\varphi H = \{\varphi(h) + h : \ h \in H\}.$$

Show that if $\varphi(h) \neq 0$ holds at most λ times, then $G \circ_\varphi H$ is a λ-simulated subset of G. ∎

In this section we will consider factorizations $G = A_1 + \cdots + A_k$, where each A_i is a λ_i-simulated subsets of G. Let p_i be the least prime divisor of $|A_i|$. We will show that if G is a finite cyclic group and $\lambda_i = p_i - 1$, then at least one of the factors $A_1, \ldots, A_k$ must be a subgroup of G.

First we prove a series of propositions about roots of unity.

LEMMA 6.4

Let ρ be a primitive (n)th root of unity and let p be the least prime divisor of n. Let $a(1), \ldots, a(u)$ be non-negative integers. If

$$\rho^{a(1)} + \cdots + \rho^{a(u)} = 0, \tag{6.4}$$

then $u \geq p$.

PROOF We may assume that $0 \leq a(i) \leq n-1$. Assume first that $n = p^e$. Replace ρ by x in (6.4) to get the polynomial

$$P(x) = x^{a(1)} + \cdots + \rho^{a(u)}.$$

The coefficients of $P(x)$ are integers and the degree of $P(x)$ is at most $p^e - 1$. As $P(1) = u$ it follows that $P(x)$ is not the zero polynomial. Consider the (p^e)th cyclotomic polynomial

$$F_{p^e}(x) = 1 + x^{p^{e-1}} + x^{2p^{e-1}} + \cdots + x^{(p-1)p^{e-1}}.$$

We will use the fact that $F_{p^e}(x)$ is irreducible over the field of rational numbers. Note that ρ is a common root of $P(x)$ and $F_{p^e}(x)$. This implies that $F_{p^e}(x)$ divides $P(x)$ over the rationals. There is a polynomial $Q(x)$ with rational coefficients such that $P(x) = F_{p^e}(x)Q(x)$. Now

$$\begin{aligned} \deg Q(x) &= \deg P(x) - \deg F_{p^e}(x) \\ &\leq (p^e - 1) - (p-1)p^{e-1} \\ &= p^{e-1} - 1. \end{aligned}$$

When we multiply $F_{p^e}(x)$ and $Q(x)$ in the way we learned in school, we can see that the non-zero terms of $Q(x)$ all appear among the terms of $P(x)$. If the coefficient of x^a is non-zero in $Q(x)$, then the coefficients of

$$x^a,\ x^{a+p^{e-1}},\ x^{a+2p^{e-1}}, \ldots, x^{a+(p-1)p^{e-1}} \tag{6.5}$$

are equal and non-zero. It follows that p divides u and consequently $u \geq p$.

Next assume that $n = p^e r$, where r is relatively prime to p, $r \geq 2$. We use induction on the number of distinct prime divisors of n. There is a primitive

(p^e)th root of unity σ and a primitive (r)th root of unity τ such that: $\rho = \sigma\tau$. Let us consider the following congruences.

$$\begin{aligned} a(i) &\equiv b(i) \pmod{p^e}, \\ a(i) &\equiv c(i) \pmod{r}. \end{aligned}$$

If $a(i)$ is given, then $b(i)$, $c(i)$ can be computed. Conversely, if $b(i)$, $c(i)$ are given, then by the Chinese remainder theorem $a(i)$ can be computed. We assume that

$$0 \le b(i) \le p^e - 1, \quad 0 \le c(i) \le r - 1.$$

Let $d(1), \ldots, d(v)$ be all the distinct numbers among $b(1), \ldots, b(u)$. Now

$$\begin{aligned} 0 &= \sum_{i=1}^{u} \rho^{a(i)} \\ &= \sum_{i=1}^{u} (\sigma\tau)^{a(i)} \\ &= \sum_{i=1}^{u} \sigma^{b(i)} \tau^{c(i)} \\ &= \sum_{i=1}^{v} \alpha_i \sigma^{d(i)}, \end{aligned}$$

where α_i is a non-empty sum of powers of τ.

Let q be the least prime divisor of r. Plainly we have that $p < q$. If $\alpha_i = 0$ for some i, $1 \le i \le v$, then by the inductive assumption α_i has at least q terms and we are done. We assume that $\alpha_i \ne 0$ for each i, $1 \le i \le v$. Replacing σ by x we get the polynomial

$$P(x) = \sum_{i=1}^{v} \alpha_i x^{d(i)}.$$

The coefficients of $P(x)$ are from the (r)th cyclotomic field and $P(x)$ is not the zero polynomial. By Theorem 3.12 (on page 51), the (p^e)th cyclotomic polynomial is irreducible over the (r)th cyclotomic field. The argument we have used in the first part of the proof provides that if the coefficient of x^a is not zero in $P(x)$, then the coefficients of the x powers in (6.5) are all equal and non-zero. There are again at least p terms in (6.4). ∎

LEMMA 6.5

Let ρ be a primitive (n)th root of unity and let p be the least prime divisor of n. Let $a(1), \ldots, a(u)$, $b(1), \ldots, b(v)$ be non-negative integers. If

$$\rho^{a(1)} + \cdots + \rho^{a(u)} = \rho^{b(1)} + \cdots + \rho^{b(v)} \tag{6.6}$$

and no $\rho^{a(i)}$ is equal to a $\rho^{b(j)}$, then $u \ge p$ or $v \ge p$.

PROOF We may assume that $0 \le a(i), b(j) \le n-1$. Assume first that $n = p^e$. Replacing ρ by x in (6.6) results in the polynomial

$$P(x) = \sum_{i=1}^{u} x^{a(i)} - \sum_{j=1}^{v} x^{b(j)}.$$

The coefficients of $P(x)$ are integers and the degree of $P(x)$ is at most $p^e - 1$. As $x^{a(1)}$ is not equal to any $x^{b(j)}$, the coefficient of $x^{a(1)}$ is not zero in $P(x)$ and $P(x)$ is not the zero polynomial. Note that $P(\rho) = 0$ and the argument involving the (p^e)th cyclotomic polynomial gives that p divides both u and v.

Next assume that $n = p^e r$, where r is relatively prime to p and $r \ge 2$. We use induction on the number of distinct prime divisors of n. Let q be the least prime divisor of r. Clearly $p < q$. There is a primitive (p^e)th root of unity σ and there is a primitive (r)th root of unity τ such that $\rho = \sigma\tau$. Let us consider the next congruences:

$$\begin{aligned} a(i) &\equiv c(i) \pmod{p^e}, \\ a(i) &\equiv d(i) \pmod{r}, \\ b(j) &\equiv f(j) \pmod{p^e}, \\ b(j) &\equiv g(j) \pmod{r}. \end{aligned}$$

If $a(i)$, $b(j)$ are given, then $c(i)$, $d(i)$, $f(j)$, $g(j)$ of course can be computed. If $c(i)$, $d(i)$, $f(j)$, $g(j)$ are given, then by the Chinese remainder theorem $a(i)$, $b(j)$ can be computed. We assume that

$$0 \le c(i), f(j) \le p^e - 1, \quad 0 \le d(i), g(j) \le r - 1.$$

Let $h(1), \ldots, h(w)$ be all the distinct numbers among $c(1), \ldots, c(u)$, $f(1), \ldots, f(v)$. Now

$$\begin{aligned} 0 &= \sum_{i=1}^{u} \rho^{a(i)} - \sum_{j=1}^{v} \rho^{b(j)} \\ &= \sum_{i=1}^{u} (\sigma\tau)^{a(i)} - \sum_{j=1}^{v} (\sigma\tau)^{b(j)} \\ &= \sum_{i=1}^{u} \sigma^{c(i)} \tau^{d(i)} - \sum_{j=1}^{v} \sigma^{f(j)} \tau^{g(j)} \\ &= \sum_{i=1}^{w} \alpha_i \sigma^{h(i)}. \end{aligned}$$

Here α_i is a sum of powers of τ. We distinguish three cases:

(i) Each power of τ in α_i has + sign.

(ii) Each power of τ in α_i has − sign.

(iii) The powers of τ in α_i have both + and − signs.

If $\alpha_i = 0$ and (i) holds, then, by Lemma 6.4 (on page 130), α_i has at least q terms and so $u \geq q > p$. If $\alpha_i = 0$ and (ii) holds, then, by Lemma 6.4 (on page 130), α_i has at least q terms and so $v \geq q > p$. If $\alpha_i = 0$ and (iii) holds, then we have an equation $\beta = \gamma$, where both sides are sums of powers of τ. We claim that no term $\tau^{d(s)}$ in β is equal to a term $\tau^{g(t)}$ in γ. Indeed, $\tau^{d(s)} = \tau^{g(t)}$ leads to $\sigma^{h(i)}\tau^{d(s)} = \sigma^{h(i)}\tau^{g(t)}$. This means that $h(i) = c(s) = f(t)$ and we get the contradiction that $\rho^{a(s)} = \rho^{b(t)}$. Let u' be the number of terms in β and let v' be the number of terms in γ. From $\beta = \gamma$ by the inductive assumption we get that $u' \geq q$ or $v' \geq q$. It follows that $u \geq u' \geq q > p$ or $v \geq v' \geq q > p$. We may assume that $\alpha_i \neq 0$ for each i, $1 \leq i \leq w$.

Consider the polynomial

$$P(x) = \sum_{i=1}^{w} \alpha_i x^{h(i)}.$$

The coefficients of $P(x)$ are from the (r)th cyclotomic field. The degree of $P(x)$ is at most $p^e - 1$ and $P(x)$ is not the zero polynomial. Note that σ is a common root of $P(x)$ and the (p^e)th cyclotomic polynomial. The divisibility argument we have seen gives that if the coefficient of x^a is not zero in $P(x)$, then the coefficients of the x powers in (6.5) are all equal and non-zero. Let us fix an x^a and consider the p equal coefficients. Let these be $\alpha_1, \ldots, \alpha_p$.

If (i) holds for α_1 and (ii) holds for α_2, then Lemma 6.4 (on page 130) is applicable to $\alpha_1 - \alpha_2 = 0$ and gives that $u \geq q > p$. Thus we may assume that there are no i, j such that (i) holds for α_i and (ii) holds for α_j. If (i) holds for one α_i, then (i) or (iii) holds for each α_j. Counting the terms with + sign in each α_j gives that $u \geq p$. If (ii) holds for some α_i, then (ii) or (iii) holds for each α_j. Counting the terms with − signs in each α_j establishes that $v \geq p$. If (iii) holds for each α_i, then counting the terms with + signs gives $u \geq p$ and counting the terms with − signs gives $v \geq p$. ∎

The next example illustrates that in general the hypotheses of Lemma 6.5 (on page 131) cannot be weakened.

EXAMPLE 6.8 If ρ is a primitive 6th root of unity, then ρ^2 has order 3 and so

$$1 + \rho^2 + \rho^4 = 0.$$

Note that $\rho^4 = -\rho$. Using this we get

$$1 + \rho^2 = \rho.$$

With the $n = 6$, $p = 2$, $u = 2$, $v = 1$ choices, the conditions of Lemma 6.5 (on page 131) are met and the conclusion that $\max\{u, v\} \geq p$ holds with equality. ∎

LEMMA 6.6

Let ρ be a primitive (n)th root of unity and let p be the least prime divisor of n. Let $a(1), \ldots, a(u)$ be non-negative integers. If

$$\rho^{a(1)} + \cdots + \rho^{a(u)} = 0$$

and $1 \leq u \leq 2p-1$, then u divides n.

PROOF If $n = p^e$, then, as we have seen in the proof of Lemma 6.4 (on page 130), it follows that p divides u. From $1 \leq u \leq 2p-1$ we get that $u = p$ and so u divides n.

We use induction on the number of distinct prime divisors of n. Let $n = p^e r$, where p does not divide r, $r \geq 2$. Let q be the least prime divisor of r. Note that $p < q$. Write ρ in the form $\rho = \sigma\tau$, where σ, τ are primitive (p^e)th, (r)th roots of unity. Define the numbers $b(i)$, $c(i)$ by

$$\begin{aligned} a(i) &\equiv b(i) \pmod{p^e}, \\ a(i) &\equiv c(i) \pmod{r} \end{aligned}$$

with

$$0 \leq b(i) \leq p^e - 1, \quad 0 \leq c(i) \leq r-1.$$

Let $d(1), \ldots, d(v)$ be all the distinct numbers among $b(1), \ldots, b(u)$. Now

$$\begin{aligned} 0 &= \sum_{i=1}^{u} \rho^{a(i)} \\ &= \sum_{i=1}^{u} (\sigma\tau)^{a(i)} \\ &= \sum_{i=1}^{u} \sigma^{b(i)} \tau^{c(i)} \\ &= \sum_{i=1}^{v} \alpha_i \sigma^{d(i)}, \end{aligned}$$

where α_i is a sum of powers of τ. Let t_i be the number of terms in α_i.

If $\alpha_i = 0$ for each i, $1 \leq i \leq v$, then, by Lemma 6.4 (on page 130), $t_i \geq q$ for each i. From

$$vq \leq t_1 + \cdots + t_v = u \leq 2p - 1 < 2q - 1$$

it follows that $v = 1$. Then $u = t_1 < 2q - 1$. The inductive assumption is applicable to $\alpha_1 = 0$ and we can conclude that u divides r. Then u divides $n = p^e r$. We assume that $\alpha_i \neq 0$ for some i.

Consider the polynomial

$$P(x) = \sum_{i=1}^{v} \alpha_i x^{d(i)}.$$

The coefficients of $P(x)$ are from the (r)th cyclotomic field. The degree of $P(x)$ is at most $p^e - 1$ and $P(x)$ is not the zero polynomial. Note that σ is a common root of $P(x)$ and the (p^e)th cyclotomic polynomial. The divisibility argument gives that the coefficients of the x powers in (6.5) are all equal. From this it follows that p divides v and then $p \le v$. From $p \le v \le u \le 2p-1$ it follows that $v = p$. We can see that

$$P(x) = \sum_{i=1}^{p} \alpha_i x^{d(i)}$$

and $\alpha_1 = \cdots = \alpha_p$. As $t_1 + \cdots + t_p = u \le 2p - 1$, we can see that $1 \le t_i \le p$ holds for each i, $1 \le i \le p$. Note that the equation $t_1 + \cdots + t_p = 2p-1$ allows one $t_i = p$ and the rest to be 1. From $\alpha_1 = \cdots = \alpha_p$ it follows that $t_i \ge q$ for some i unless the sums are identical. Now $t_i \ge q$ and $t_j \ge 1$ for all $j \ne i$ is not possible as $q > p$. Therefore $1 \le t_i < q$ for each i. If no cancellation is possible in the equation $\alpha_1 = \alpha_i$, then, by Lemma 6.5 (on page 131), we get that $t_1 \ge q$ or $t_i \ge q$. This is not the case, so cancellations are possible and $t_1 = \cdots = t_p$. Let t be this common value. Now $pt = u \le 2p - 1$ implies that $t = 1$ and then $u = p$. Therefore u divides n. □

Perhaps it is worthwhile to present an example to point out that the conditions of Lemma 6.6 (on page 134) are tight.

EXAMPLE 6.9 If ρ is a primitive (15)th root of unity, then plainly

$$1 + \rho^3 + \rho^6 + \rho^9 + \rho^{12} = 0.$$

This means that with the $n = 15$, $p = 3$, $u = 5$ choices, $u \le 2p - 1$ holds with equality. □

LEMMA 6.7

Let ρ, σ be primitive (n)th and (q)th roots of unity such that q is a prime, q does not divide n. Let p be the least prime divisor of n and let $a(i)$, $b(i)$, $c(i)$ be non-negative integers. If

$$\rho^{a(1)}\sigma^{b(1)} + \cdots + \rho^{a(u)}\sigma^{b(u)} = \rho^{c(1)} + \cdots + \rho^{c(u)} \tag{6.7}$$

and no $\sigma^{b(i)}$ is equal to 1, then $u \ge p$.

PROOF We may assume that $0 \le a(i), c(i) \le n - 1$, $1 \le b(i) \le q - 1$. If $u = 1$, then (6.7) reduces to $\rho^{a(1)}\sigma^{b(1)} = \rho^{c(1)}$, which is clearly impossible. We assume that $u \ge 2$. Replace σ by x in (6.7) to get the polynomial

$$P(x) = \sum_{i=1}^{u} \rho^{a(i)} x^{b(i)} - \sum_{i=1}^{u} \rho^{c(i)}.$$

The coefficients of $P(x)$ are from the (n)th cyclotomic field and the degree of $P(x)$ is at most $q-1$. The coefficient of x^0 in $P(x)$ is $\alpha_0 = -\rho^{c(1)} - \cdots - \rho^{c(u)}$. If $P(x)$ is the zero polynomial, then $\alpha_0 = 0$. By Lemma 6.4 (on page 130), $u \geq p$. Thus we may assume that $P(x)$ is not the zero polynomial.

Note that σ is a common root of $P(x)$ and the (q)th cyclotomic polynomial. It follows by the divisibility argument that the coefficients of

$$x^0,\ x^1,\ x^2, \ldots, x^{q-1}$$

in $P(x)$ are all equal. Let $\alpha_0, \ldots, \alpha_{q-1}$ be these coefficients, that is,

$$\alpha_0 = -\sum_{i=1}^{u} \rho^{c(i)},$$
$$\alpha_i = \sum_{\{j:b(j)=i\}} \rho^{a(j)}, \quad 1 \leq i \leq q-1.$$

Suppose $q \geq 3$ and consider $\alpha_1 = \alpha_i$ for $2 \leq i \leq q-1$.

If total cancellation does not occur, then some of the terms are left on one side and by Lemma 6.5 (on page 131) $u \geq p$ follows, as required. Otherwise, the terms in $\alpha_1, \ldots, \alpha_{q-1}$ are identical. Consequently, each $\alpha_1, \ldots, \alpha_{q-1}$ has the same number of terms, say t. It follows that $t(q-1) = u$.

Let $\alpha_1 = \rho^{d(1)} + \cdots + \rho^{d(t)}$. From $\alpha_1 = \alpha_0$ we get

$$\rho^{d(1)} + \cdots + \rho^{d(t)} + \rho^{c(1)} + \cdots + \rho^{c(u)} = 0.$$

If $t + u \leq 2p - 1$, then Lemma 6.6 (on page 134) gives that $t + u = tq$ divides n and so t divides n and q divides n. From q divides n it follows that $q \geq p$. By the hypotheses of the lemma, $q \neq p$ and so $q > p$. If $t = 1$, then from $(q-1)t = u$ we get $u = q - 1 > p - 1$; then $u \geq p$, as required. If $t \neq 1$, then from t divides n and it follows that $t \geq p$ and then $u = t(q-1) \geq p$. We may assume that $t + u \geq 2p$. Note that $u \geq t$ and so $2u \geq t + u \geq 2p$ implies $u \geq p$.

Finally we are left with the case $q = 2$. Now each $\sigma^{b(i)}$ is equal to -1 and (6.7) is equivalent to

$$\rho^{a(1)} + \cdots + \rho^{a(u)} + \rho^{c(1)} + \cdots + \rho^{c(u)} = 0.$$

If $2u \leq 2p - 1$, then Lemma 6.6 (on page 134) is applicable and implies that $2u$ divides n. In particular, u divides n and, as $u \geq 2$, it follows that $u \geq p$. As the $2u \leq 2p - 1$ case is settled, we are left with the $2u \geq 2p$ case. But now $u \geq p$. ∎

LEMMA 6.8

Let G be a finite abelian group and let A be a $(p-1)$-simulated subset of G, where p is the least prime divisor of $|A|$. If A is periodic, then A is equal to an associated subgroup H of G.

PROOF If $|A|$ is a prime, then the result is trivial. Assume that $|A|$ is not a prime. Now the associated subgroup H of A is uniquely determined. Let g be a period of A. We may suppose that $|g| = r$ is a prime. Clearly $p \leq r$. The map $a \to a + g$, $a \in A$ permutes the elements of A. The permutation consists of cycles of length r and there are at least two cycles. One of the cycles contains two distinct elements a, b that are also contained by H. As $a + tg = b$ with $1 \leq t \leq r - 1$, we get $g \in H$. Note that each cycle contains at least one element from H. Consider the cycle that contains an element c from H and let d be another element from this cycle. Now $c + tg = d$ gives that $d \in H$. Therefore $A = H$. □

LEMMA 6.9

Let G be a finite cyclic group and let $G = A_1 + \cdots + A_k$ be a normalized factorization of G. If each A_i is a $(p_i - 1)$-simulated subset, where p_i is the least prime divisor of $|A_i|$, then A_i can be replaced by an associated subgroup H_i of A_i.

PROOF In the case $|A_i| \geq 2p_i$, Theorem 3.14 (on page 56) gives that A_i can be replaced by H_i. Suppose that $|A_i| \leq 2p_i - 1$. Since p_i is the least prime divisor of $|A_i|$, it follows that $|A_i| = p_i$. Now Theorem 4.4 (on page 73) is applicable and gives that A_i or

$$B = A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k$$

is periodic. If A_i is periodic, then we get $A_i = H_i$ as $|A_i|$ is a prime. We may assume that B is periodic. There is a subgroup H of G and a subset C of G such that $B = C + H$, where the sum is direct. We choose H to be the largest possible. Consequently C is not periodic. From the factorization $G = A_i + C + H$, by considering the factor group G/H, we get the factorization

$$G/H = (A_i + H)/H + (C + H)/H.$$

Theorem 4.4 (on page 73) is applicable and gives that $(A_i + H)/H$ or $(C + H)/H$ is periodic. By the maximality of H, $(C+H)/H$ cannot be periodic and so $(A_i+H)/H$ is periodic. Since $|A_i|$ is a prime, it follows that $(A_i+H)/H = (H_i + H)/H$ and then $A_i + H = H_i + H$. Using this we get

$$\begin{aligned} G &= A_i + C + H \\ &= A_i + H + C \\ &= H_i + H + C \\ &= H_i + B. \end{aligned}$$

This shows that A_i can be replaced by H_i in the factorization $G = A_1 + \cdots + A_k$. □

THEOREM 6.4

Let G be a finite cyclic group and let $G = A_1 + \cdots + A_k$ be a normalized factorization of G. If each A_i is a $(p_i - 1)$-simulated subset, where p_i is the least prime divisor of $|A_i|$, then some A_i is equal to an associated subgroup H_i of A_i.

PROOF By Lemma 6.9 (on page 137), each A_i may be replaced by one of its associated subgroups H_i in any factorization involving A_i as a factor. Therefore $G = H_1 + \cdots + H_k$. Since G is cyclic, it follows that for each pair i, j, $i \neq j$, the integers $|H_i|$ and $|H_j|$ are relatively prime. Each element in $A_i \setminus H_i$ may be expressed as $h_{i,j} + d_{i,j}$, where $h_{i,j} \in H_i$ and

$$d_{i,j} \in H_1 + \cdots + H_{i-1} + H_{i+1} + \cdots + H_k.$$

Here we have that $1 \leq j \leq m_i \leq p_i - 1$. It follows that $|d_{i,j}|$ is relatively prime to $|H_i|$. Let k_i be the lowest common multiple of $|d_{i,j}|$, $1 \leq j \leq m_i$ and let q_i be a prime factor of k_i. Then we may replace A_i by $(k_i/q_i)A_i$ and we note that $(k_i/q_i)H_i = H_i$. When this replacement is carried out certain $d_{i,j}$ may satisfy $(k_i/q_i)d_{i,j} = 0$ and the remaining $d_{i,j}$, of which at least one must exist, satisfy $|d_{i,j}| = q_i$. We shall assume, for each i, that this replacement has been carried out. By renumbering the elements, we still have that $1 \leq m_i \leq p_i - 1$.

Let χ be a character of G with $\mathrm{Ker}\chi = \{0\}$. As before, we can deduce that $G = A_1 + \cdots + A_k$ implies that $\chi(A_i) = 0$, for some i. We may assume that $\chi(A_1) = 0$. Since $d_{1,j}$ has order q_1, we have $\chi(d_{1,j}) = \sigma^{b(j)}$ and that $\chi(d_{1,j}) \neq 1$, where σ is a primitive (q_1)th root of unity. We also have that $\chi(H_1) = 0$ and so that $\chi(h_{1,j}) = \rho^{a(j)}$, where ρ is a primitive (n_1)th root of unity and $n_1 = |H_1|$. From above it follows that q_1 does not divide n_1.

From $\chi(A_1) = \chi(H_1)$ it follows that

$$\rho^{a(1)}\sigma^{b(1)} + \cdots + \rho^{a(u)}\sigma^{b(u)} = \rho^{c(1)} + \cdots + \rho^{c(u)}.$$

Here we replaced m_1 by u. It follows by Lemma 6.7 (on page 135) that $m_1 \geq p_1$. This is false.

Hence $A_1 = H_1$ and the result holds. ∎

We exhibit examples to show that the condition $\lambda \leq p_i - 1$ cannot be replaced by the weaker condition $\lambda \leq p_i$ in Theorem 6.4 (on page 138).

EXAMPLE 6.10 Let p, q, r be primes such that $p < q < r$. Let $G = Z(p) \oplus Z(q) \oplus Z(r)$ with basis elements x, y, z, where $|x| = p$, $|y| = q$, $|z| = r$. Take

$$A = \{0, x, \ldots, (p-1)x\} + \{0, y, \ldots, (q-2)y, (q-1)y + z\},$$
$$B = \{0, z, \ldots, (r-2)z, (r-1)z + x\}.$$

One should verify that $G = A + B$ is a factorization of G. Note that A is periodic. The non-zero elements of the subgroup $\langle x \rangle$ are periods of A. But A is not a subgroup. It differs from $\langle x, y \rangle$ in p elements. Further, B differs from $\langle z \rangle$ in one element. □

EXAMPLE 6.11 Choose distinct primes q, r, s, t such that $q < r$ and $s < t$. Let G be a cyclic group generated by the elements x, y, u, v with $|x| = q$, $|y| = r$, $|u| = s$, $|v| = t$. Set $H = \langle x \rangle$, $K = \langle u \rangle$, and

$$A = H \cup (y + H) \cup \cdots \cup [(r-2)y + H] \cup [(r-1)y + u + H],$$
$$B = K \cup (v + K) \cup \cdots \cup [(t-2)v + K] \cup [(t-1)v + x + K].$$

Let $L = \langle x, y \rangle$, $M = \langle u, v \rangle$. Now $|A| = |L|$, $|B| = |M|$. One can verify that $G = A + B$ and consequently $G = A + B$ is a factorization of G. Plainly, A is periodic. The non-zero elements of H are periods of A. However, A is not a subgroup of G. It differs from the subgroup L in q elements and q is the least prime divisor of $|A|$. Similarly, B differs from the subgroup M in s elements and s is the least prime factor of $|B|$. □

Notes

(1) L. Fuchs [41] asked, if a direct sum of cyclic subsets forms a periodic subset of a finite abelian group, then does it follow that one of the factors is periodic? Most likely he hoped to get a simplified proof for Hajós's classical theorem in this way. Fuchs's question was the starting point of studying factorizations of periodic subsets. We have to point out that Fuchs was considering the direct sum of more general subsets than cyclic subsets.

(2) The idea of using vanishing sums of roots of unity to analyze factorizations goes back to [126].

Chapter 7

Group of integers

7.1 Sum sets of integers

A cyclic group of order n may be realized as the additive group Z/nZ, that is, as the integers modulo n. When we interpret Theorem 3.19 (on page 59) in this way we obtain the following result.

THEOREM 7.1

Let m and n be relatively prime positive integers. If $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$ are sets of integers such that their sum set

$$A + B = \{a_i + b_j : \ 1 \leq i \leq m, \ 1 \leq j \leq n\}$$

is a complete set of representatives modulo mn, then A is a complete set of residues modulo m and B is a complete set of residues modulo n.

PROOF We may interpret A and B as subsets of Z/mnZ. Then the statement that $A + B$ is a complete set of residues modulo mn is equivalent to the statement that $A + B = Z/mnZ$ is a factorization. Now the subgroups H, K of orders m, n are

$$H = nZ/mnZ \quad \text{and} \quad K = mZ/mnZ.$$

By Theorem 3.19 (on page 59), we have that

$$Z/mnZ = (nZ/mnZ) + B.$$

Now if any two elements of B were congruent modulo n, this sum would not be direct. Hence B is a complete set of residues modulo n. Similarly, from

$$Z/mnZ = A + (mZ/mnZ),$$

it follows that A is a complete set of residues modulo m. ∎

It is natural to ask what happens if the sum of these sets of integers is a complete set of residues but m and n are no longer assumed to be relatively

prime. We shall see that there is one positive result where one of the two sets is a complete set of residues. In all the other cases examples will be given where neither set is a complete set of residues.

In order to prove the positive result we need the following result on the factorization of the group of order p^2, p prime, which is a very special case of Theorem 4.3 (on page 67).

If p is a prime, the group G has order p^2 and $G = A + B$ is a factorization such that $0 \in A$, $0 \in B$, then either A or B is a subgroup of G.

We note that if $G = Z/p^2Z$ and A is a subgroup, that is, $A = pZ/p^2Z$, then B must be a complete set of residues modulo p.

THEOREM 7.2

Let m, n be relatively prime positive integers and let p be a prime not dividing mn. If A is a set of pm integers and B is a set of pn integers such that $A+B$ is a complete set of residues modulo p^2mn, then either A is a complete set of residues modulo pm or B is a complete set of residues modulo pn.

PROOF Let $G = Z/p^2mnZ$. Then G is a direct sum of subgroups H, K, L of orders p^2, m, n, respectively. From the above information we have that $G = A + B$ is a factorization. By Theorem 3.17 (on page 58), it follows that

$$\begin{aligned} G &= nA + B \\ &= A + mB \\ &= nA + mB \end{aligned}$$

are all factorizations. We note that $nA \subseteq H + K$ and that $mB \subseteq H + L$. Let $k \in K$, $l \in L$. Then for $a \in nA$, $b \in mB$ we have that $a + b \in H + k + l$ if and only if $a \in H + k$, $b \in H + l$. Hence

$$\big(nA \cap (H + k)\big) + \big(mB \cap (H + l)\big) = H + k + l$$

and so

$$\big((nA - k) \cap H\big) + \big(mB - l) \cap H\big) = H.$$

If one subset, say $(nA-k)\cap H$, has order p^2 for any such k, then $(mB-l)\cap H$ has order 1 for all $l \in L$. Now from $mB \subseteq H + L$ it follows that

$$mB = \bigcup_{l \in L} \big(mB \cap (H + l)\big).$$

Hence

$$|mB| = \sum_{l \in L} \big|mB \cap (H + l)\big| = |L| = n,$$

which is false as $|mB| = |B| = pn$. Hence

$$\big|(nA - k) \cap H\big| = p = \big|(mA - l) \cap H\big|$$

for all $k \in K$, $l \in L$.

Now H has a unique subgroup M of order p. From

$$(nA \cap H) + (mB \cap H) = H$$

it follows that either $nA \cap H = M$ or that $mB \cap H = M$. We may suppose that $nA \cap H = M$. Then

$$M + \big(mB \cap (H + l)\big) = H + l$$

for each $l \in L$. As above, it follows that $M + mB = H + L$ and so that

$$\begin{aligned} M + K + mB &= H + K + L \\ &= G. \end{aligned}$$

If $M + K + B$ is not a direct sum, then there exist $b_1, b_2 \in B$ with $b_1 \neq b_2$ such that $b_1 - b_2 \in M + K$. Then $mb_1 - mb_2 \in M + K$. Since the sum $M + K + mB$ is direct, it follows that $mb_1 = mb_2$. Since $|mB| = |B|$ it follows that $b_1 = b_2$. Therefore the sum $M + K + B$ is direct and so $M + K + B = G$.

Now $|M + K| = pm$ and so $M + K = pnZ/p^2mnZ$. As before, it follows that B is a complete set of residues modulo pn. ∎

We should note that, in this case, we cannot have that both A and B are complete sets of residues. If this were so, then A would be replaceable by $M + K$ to give that $M + K + mB = G$ and B would be replaceable by $M + L$ to give that $nA + M + L = G$. Now, we have seen that either $nA \cap H = M$ or $mB \cap H = M$. Now $M \subseteq nA$ contradicts that $nA + M + L$ is direct and, similarly, $M \subseteq mB$ contradicts that $M + K + mB$ is direct.

We shall now give examples to show that in all other cases there exist sets of integers A, B neither of which is a complete set of residues modulo $|A|$ or modulo $|B|$, respectively, but which are such that $A + B$ is a complete set of residues modulo $|A||B|$.

THEOREM 7.3

Let there exist sets of integers C, D of order r, s, respectively, such that C, D are not complete sets of residues modulo r, s, respectively, but such that $C + D$ is a complete set of residues modulo rs. Let u, v be integers relatively prime to rs, then there exists a set A of order ru and a set B of order sv such that $A + B$ is a complete set of residues modulo $rsuv$ but A, B are not complete sets of residues modulo ru, sv, respectively.

PROOF Let E, F be any sets of integers containing 0 of orders u, v, respectively, such that $E + F$ is a completes set of residues modulo uv. For example, we may take

$$\begin{aligned} E &= \{0, 1, 2, \ldots, u - 1\}, \\ F &= \{0, u, 2u, \ldots, (v - 1)u\}. \end{aligned}$$

Let

$$A = uvC + rsE, \quad B = uvD + rsF.$$

Then

$$A + B = uv(C + D) + rs(E + F).$$

Now uv and rs are relatively prime, therefore there exist k, l with $kuv + lrs = 1$. For any integer m there exist $c \in C$, $d \in D$, $e \in E$, $f \in F$ such that $km \equiv c + d \pmod{rs}$ and $lm \equiv e + f \pmod{uv}$. Then

$$m = kuvm + lrsm \equiv uv(c + d) + rs(e + f) \pmod{rsuv}.$$

It follows that $A + B$ is a complete set of residues modulo $rsuv$. Now there exist $c_1, c_2 \in C$ such that $c_1 \equiv c_2 \pmod{r}$ and so such that $uvc_1 \equiv uvc_2 \pmod{ru}$. It follows that A is not a complete set of residues modulo ru. Similarly, it follows that B is not a complete set of residues modulo sv. □

EXAMPLE 7.1 Let $r = p^e$, $e \geq 2$ and $s = p^f$, $f \geq 1$. Let

$$A_1 = \{0, 1, \ldots, p - 1\}, \quad A_k = p^{k-1}A_1, \quad k \geq 2.$$

Then $A_1 + \cdots + A_{e+f}$ is easily seen to be a complete set of residues modulo p^{e+f}. Let A be a sum of e of these sets, which includes A_{e+f} but not A_{e+f-1}. Let B be the sum of the remaining f sets. Then $A + B$ is a complete set of residues modulo p^{e+f}. The elements of A_{e+f} are in A and are congruent modulo p^{e+f-1}. Since $f \geq 1$, they are congruent modulo p^e and so A is not a complete set of residues modulo p^e. The elements of A_{e+f-1} are in B and are congruent modulo p^{e+f-2}. Since $e \geq 2$, they are congruent modulo p^f and so B is not a complete set of residues modulo p^f. □

EXAMPLE 7.2 Let $p = 2$, $e = 2$, $f = 1$ in Example 7.1 (on page 144). These are the smallest possible choices for p, e, f. Now

$$A = \{0, 1\} + \{0, 4\} = \{0, 1, 4, 5\}, \quad B = \{0, 2\}.$$

It is clear that $A + B$ is a complete set of residues modulo 8 while A is not a complete set of residues modulo 4 nor is B a complete set of residues modulo 2. □

From Theorem 7.3 (on page 143) and Example 7.1 (on page 144), it follows that if p^2 divides m and p divides n, then sets of integers exist with m, n elements, respectively, which are not complete sets of residues but such that their sum is a complete set of residues modulo mn.

EXAMPLE 7.3 Let p, q be distinct primes. Let

$$A = \{0, pq^2, 2pq^2, \ldots, (p - 1)pq^2\} +$$

$$B = \begin{array}{l}\{0, p^2, 2p^2, \ldots, (q-1)p^2\},\\ \{0, q^2, 2q^2, \ldots, (p-1)q^2\}+\\ \{0, p^2q, 2p^2q, \ldots, (q-1)p^2q\}.\end{array}$$

Then $|A| = |B| = pq$ and

$$A + B = \begin{array}{l}\{0, q^2, 2q^2, \ldots, (p^2-1)q^2\}+\\ \{0, p^2, 2p^2, \ldots, (q^2-1)p^2\}\end{array}$$

is a complete set of residues modulo p^2q^2. Since A contains 0 and pq^2 it is not a complete set of residues modulo pq. Similarly, B is not a complete set of residues modulo pq. □

EXAMPLE 7.4 The smallest values for p, q occur with $p = 2$, $q = 3$ in Example 7.3 (on page 144). In this case

$$A = \{0, 18\} + \{0, 4, 8\}, \quad B = \{0, 9\} + \{0, 12, 24\}$$

and

$$A + B = \{0, 9, 18, 27\} + \{0, 4, 8, 12, 16, 20, 24, 28, 32\},$$

that is, $A + B = \langle 9\rangle + \langle 4\rangle$ in the group $Z(36)$ of integers modulo 36, which gives the required factorization. □

It follows from Examples 7.1 (on page 144) and 7.3 (on page 144) and Theorem 7.3 (on page 143) that if pq divides both m and n, then the required type of example exists. If p^2 or q^2 divides either m or n, it follows from the previous example. If not, then $m = pqu$, $n = pqv$, where u and v are relatively prime to pq. The result then follows from this example.

We have now justified the claim that Theorems 7.1 (on page 141) and 7.2 (on page 142) provide all the positive results of this type.

In his book *Abelian Groups* [41], page 331, Fuchs in Problem 77 asks, "If $G = S + T$ where G is finite (cyclic), can then one of the subsets S, T be replaced by a subgroup of G?" He attributes the question to G. Hajós. There are easy counter-examples. The smallest occurs in the cyclic group of order 8.

EXAMPLE 7.5 Let $Z(8) = \langle g\rangle$ and let

$$A = \{0, g\} + \{0, 4g\}, \quad B = \{0, 2g\}.$$

Then $Z(8) = A + B$ is a factorization of $Z(8)$ and A cannot be replaced by $\langle 2g\rangle$ nor B by $\langle 4g\rangle$. (The astute reader is not going to fail to detect that this example and Example 7.4 share a common origin.) □

The results given in this section are sufficient to determine exactly the finite cyclic groups for which a positive answer holds.

THEOREM 7.4

For every factorization into two factors of a finite cyclic group G, one factor is replaceable by a subgroup if and only if G has order pm, where p is a prime and m is square-free.

PROOF Let G have order pm, as above. If p does not divide m, then pm is square-free. So the orders of any two factors are relatively prime. By Theorem 3.19 (on page 59), each factor may be replaced by a subgroup.

If p divides m, then the orders of the factors need not be relatively prime. In this case the orders are pu and pv, where u and v are relatively prime and not divisible by p. Then, by Theorem 7.2 (on page 142) one of the factors gives rise to a complete set of residues. This implies that the other factor is replaceable by a subgroup.

Now suppose that the order of G is not of this form. Then either there is a prime p whose cube divides the order of G or there are two primes p and q whose squares divide the order of G. In both cases we have seen examples of factorizations where neither factor is a complete set of residues. Equivalently, this means that neither factor is replaceable by a subgroup. ∎

7.2 Direct factor subsets

There is one problem to which we should like to have a solution. This is to find an internal characterization as to when a given subset A of a group G is a direct factor of G. We present two conditions which are together sufficient for this to happen. One of these conditions is also necessary. We show that the second condition is also necessary if $|A|$ has at most two distinct prime factors. The question as to whether this condition is necessary in the general case remain open.

We observe the following results on cyclotomic polynomials.

THEOREM 7.5

Let m, m_1, m_2, n be non-negative integers.

(i) *If n and m are relatively prime, then*

$$F_n(x^m) = \prod_{d|m} F_{nd}(x).$$

(ii) *If every prime divisor of m is also a divisor of n, then $F_n(x^m) = F_{nm}(x)$.*

(iii) *If $m = m_1 m_2$ where every prime divisor of m_1 is also a divisor of n and m_2 is relatively prime to n, then*

$$F_n(x^m) = \prod_{d|m_2} F_{nm_1d}(x).$$

PROOF (i) This follows from the observation that ρ^m is a primitive (n)th root of unity if and only if ρ is a primitive (nd)th root of unity for some divisor d of n, whenever m and n are relatively prime. There are no other zeros of these polynomials and there are no repeated zeros since cyclotomic polynomials has no repeated zeros and cyclotomic polynomials corresponding to different parameters are relatively prime.

(ii) This follows in a similar way. From the given conditions it follows that ρ^m is a primitive (mn)th root of unity.

(iii) This follows by successive applications of (i) and (ii). ∎

Let G be a finite cyclic group with generator element g. Let A be a subset of G such that

$$A = \{k(1)g, \ldots, k(m)g\},$$

where $0 \leq k(1), \ldots, k(m) \leq |G| - 1$. Exactly in the same way as in Section 3.2 with a subset A of G we associate a polynomial

$$A(x) = x^{k(1)} + \cdots + x^{k(m)}.$$

Clearly $A(x)$ depends on the choice of the generator element g. In the course of our work we will fix a g and so a uniquely determined $A(x)$ will be associated with A.

We now state the two conditions referred to in the introduction. Let A be a subset of a group G.

C1. $|A| = \prod F_d(1)$, where d runs through all divisors of $|G|$ such that $F_d(x)$ divides $A(x)$.

C2. If $s(1), \ldots, s(k)$ are powers of distinct primes and $F_{s(i)}(x)$ divides $A(x)$, $1 \leq i \leq k$, then $F_{s(1)\cdots s(k)}(x)$ divides $A(x)$.

We should observe that

$$F_s(1) = \begin{cases} p, & \text{if } s = p^e, \ p \text{ is a prime,} \\ 1, & \text{otherwise,} \end{cases}$$

whenever $s > 1$. So in condition C1 we may restrict our attention to prime powers.

Note that the polynomial $A(x)$ has 0, 1 coefficients. It is a well-known fact that the polynomial $F_n(x)$ has integer coefficients. When we talk about the divisibility of polynomials we understand divisibility over the field of rational numbers.

We show first that C1 is a necessary condition.

THEOREM 7.6

Let $G = A + B$ be a factorization of the group G. Then A satisfies condition C1.

PROOF Let p be a prime dividing $n = |G|$. Let $n = p^e m$, where p does not divide m. Let $|A| = p^f m_1$, where $m_1 \mid m$. Then $|B| = p^{e-f} m_2$, where $m_1 m_2 = m$. For each r, $1 \leq r \leq e$, $F_{p^r}(x)$ divides either $A(x)$ or $B(x)$. Since these polynomials are monic, it follows that for each r such that $F_{p^r}(x)$ divides $A(x)$. Then p divides $|A|$ and the same result holds for B. Hence exactly f such cyclotomic polynomials divide $A(x)$ and exactly $e - f$ of them divides $B(x)$. By (7.2), $F_s(1) = 1$ whenever s is not a prime power and $s > 1$, hence it follows that $|A| = \prod F_d(1)$, where d runs through all divisors of n such that $F_d(x)$ divides $A(x)$. Thus condition C1 is satisfied. ∎

We now show that conditions C1 and C2 together are sufficient to show that A is a factor of a factorization.

THEOREM 7.7

Let A be a subset of a finite cyclic group G such that conditions C1 and C2 both hold. Then A is a direct factor of G.

PROOF Let $|G| = n = p_1^{e(1)} \cdots p_k^{e(k)}$, where $p_1, \ldots, p_k$ are the distinct prime factors of n. Let S denote the set of prime powers s such that $s \in S$ if and only if $F_s(x)$ divides $A(x)$. (The divisibility is meant over the field of rationals.) For each i, let $n = p_i^{e(i)} m_i$. For each prime power t not in S such that t divides n, let $m(t) = m_i$, where $t = p_i^{f(i)}$. We define a polynomial $B(x)$ by

$$B(x) = \prod F_t(x^{m(t)}),$$

where the product is taken over all prime powers t dividing n such that $t \notin S$. Since t is a prime power, the polynomial $F_t(x^{m(t)})$ has non-negative integer coefficients and so $B(x)$ has non-negative integer coefficients.

Let d be a divisor of n, $d > 1$. Let $d = p_1^{g(1)} \cdots p_k^{g(k)}$. If, for each i, either $g(i) = 0$ or $p_i^{g(i)} \in S$, then, by condition C2, $F_d(x)$ divides $A(x)$. Otherwise, there exists i such that $p_i^{g(i)} = t$, where $t > 1$, $t \notin S$. Let $d = p_i^{g(i)} c$. Then c divides $m_i = m(t)$. Now, by part (i) of Theorem 7.5 (on page 146),

$$F_t(x^{m(t)}) = \prod_{e \mid m(t)} F_{te}(x).$$

Since the case $c = e$ will arise, it follows that $F_d(x)$ divides $B(x)$.

It follows that

$$\prod_{\substack{d|n \\ d>1}} F_d(x) = 1 + x + x^2 + \cdots + x^{n-1}$$

divides $A(x)B(x)$. Let

$$A(x)B(x) = U(x)(1 + x + x^2 + \cdots + x^{n-1}).$$

Then $A(1)B(1) = U(1)n$. Now $A(1) = \prod F_d(1)$, where $F_d(x)$ divides $A(x)$, $d \mid n$, $d > 1$ and so $A(1) = \prod p_i^{g(i)}$, where $s \in S$ occurs exactly $g(i)$ times with s being a power of p_i. $B(1) = \prod F_t(1) = \prod p_i^{e(i)-g(i)}$, since t occurs in the remaining $e(i) - g(i)$ times as a power of p_i. Hence $A(1)B(1) = \prod p_i^{e(i)} = n$. Therefore $U(1) = 1$. Hence $x - 1$ divides $U(x) - 1$. Now $r \equiv s \pmod{n}$ if and only if $x^r \equiv x^s \pmod{(x^n - 1)}$:

$$\begin{aligned} A(x)B(x) - (1 + x + \cdots + x^{n-1}) &= (U(x) - 1)(1 + x + \cdots + x^{n-1}) \\ &\equiv 0 \pmod{(x^n - 1)}. \end{aligned}$$

Now, since $A(x)$ and $B(x)$ have non-negative integer coefficients, if $B(x)$ had a coefficient greater than 1, then so would $A(x)B(x)$. This is not so. Hence $B(x)$ has coefficients only in $\{0, 1\}$. Therefore there is a subset, which we may call B, giving rise to $B(x)$. Then

$$A(x)B(x) \equiv 1 + x + \cdots + x^{n-1} \pmod{(x^n - 1)}$$

implies that $A + B = G$ is a factorization, as required. □

We note that if we set $B_t(x) = F_t(x^{m(t)})$, then $B_t(x)$ has coefficients only in $\{0, 1\}$ and so corresponds to a subset, which we may call B_t, of order p_i where t is a power of p_i. Then, since $B(x) = \prod B_t(x)$, it follows that B is a direct product of the subsets B_t. If $t = p_i^{e(i)}$, then

$$F_t(x^{m(i)}) = \frac{(x^q - 1)}{(x^{n/p_i} - 1)}.$$

Thus, in this case, B_t is the unique subgroup of order p_i and B is periodic.

It is an open question whether every direct factor of a group satisfies C2. We shall show that this is so if at most two distinct primes divide the order of A.

THEOREM 7.8

If G is a finite cyclic group whose order is divisible by at most two distinct primes, then each direct factor A of G satisfies condition C2.

PROOF If G has a prime power order, there is nothing to prove. So we may proceed by induction on the order of G. Let G have order $p^e q^f$, where p and q are distinct primes. Let $G = A + B$ be a factorization of G. By Theorem 5.3 (on page 100), either $\langle A\rangle \neq G$ or $\langle B\rangle \neq G$.

Consider first the case when $\langle A\rangle = H$ and H is a proper subgroup of G. Then $A \subseteq H$ and $A + B = G$ implies that $A + (B \cap H) = H$ is a factorization of H. By the inductive assumption it follows that A satisfies condition C2.

Now let us consider the case where $\langle B\rangle \neq G$. By interchanging p and q, if necessary, we may assume that $B \subseteq pG$. Let g be a generator of G. We recall that $F_d(x)$ divides $A(x)$ if and only if $\chi(A) = 0$, where χ is a character of G such that $\chi(g)$ is a primitive (d)th root of unity. Now $\{0, g, 2g, \ldots, (p-1)g\}$ is a complete set of representatives for G modulo pG. Then $A + B = G$, $B \subseteq pG$ implies that

$$\big(A \cap (pG + rg)\big) - rg + B = pG, \tag{7.1}$$

for $0 \leq r \leq p-1$. Let $F_{p^s}(x)$ and $F_{q^t}(x)$ divide $A(x)$, where $s > 1$. Then $F_{p^s}(x)$ and $F_{q^t}(x)$ do not divide $B(x)$. It follows from (7.1) then that $F_{p^s}(x)$ and $F_{q^t}(x)$ divide

$$A_r(x) = \big(A \cap (pG + rg)\big)(x).$$

By the inductive assumption it follows that $F_{p^s q^t}(x)$ divides $A_r(x)$. Now

$$A = \bigcup_{r=0}^{p-1} \big[A \cap (pG + rg)\big]$$

and so

$$A(x) = \sum_{r=0}^{p-1} A_r(x).$$

Hence $F_{p^s q^t}(x)$ divides $A_r(x)$, as required.

Now we consider the case $s = 1$, that is, where $F_p(x)$ and $F_{q^t}(x)$ divide $A(x)$. Then $\chi(A) = 0$, where χ is a character of G such that $\chi(g)$ has order p. This implies that χ restricted to pG is the identity character. So we can make no deduction from (7.1). Let η be a character of G such that $\eta(g)$ has order pq^t. Then $\eta(pg)$ has order q^t. Now $B \subseteq pG$. Let λ be a character of G such that $\lambda(q^f g) = 1$ and $\lambda(p^e g) = \eta(p^e g)$. Then since $\eta(q^f g) = 1$, λ and η agree on pG. Then $F_{pq^t}(x)$ divides $B(x)$ if and only if $\eta(B) = 0$. $\eta(B) = 0$ if and only if $\lambda(B) = 0$, as $B \subseteq pG$, $\lambda(B) = 0$. $\lambda(B) = 0$ if and only if $F_{q^t}(x)$ divides $B(x)$, since $\lambda(g)$ has order q^t. $F_{q^t}(x)$ divides $A(x)$ and so cannot divide $B(x)$. Therefore $F_{pq^t}(x)$ does not divide $B(x)$ and so divides $A(x)$.

It follows that A satisfies condition C2. ∎

THEOREM 7.9

If G is a finite cyclic group and A is a direct factor of G whose order has at most two distinct prime factors, then A satisfies condition C2.

PROOF If A has a prime power order, there is nothing to prove. So let the distinct primes p and q divide $|A|$. Let $|G| = p^e q^f m$, where m is relatively prime to pq. Let $A + B = G$ be a factorization of G. Let G be a direct sum of subgroups H, K, where $|H| = p^e q^f$, $|K| = m$. By Theorem 3.18 (on page 59) we may replace A by $(A)_H$ to obtain the factorization $G = (A)_H + B$. Then $(A)_H \subseteq H$ implies that $(A)_H + (B \cap H) = H$. By Theorem 7.8 (on page 101), it follows that $(A)_H$ satisfies condition C2. Let g be a generator of G. Let χ, η be characters of G such that $\chi(g)$, $\eta(g)$ have orders p^s, q^t, respectively. Then χ and η restricted to K are the identity characters. Thus

$$\chi(A) = \chi((A)_H), \qquad \eta(A) = \eta((A)_H).$$

Thus $\chi(A) = 0$, $\eta(A) = 0$ imply that $\chi((A)_H) = 0$, $\eta((A)_H) = 0$. By condition C2 it follows that $(\chi\eta)((A)_H) = 0$ and so that $(\chi\eta)(A) = 0$, where $(\chi\eta)(g) = \chi(g)\eta(g)$. This is equivalent to condition C2 holding for A, as required. ∎

In Section 5.2, Problem 5.2 (on page 120) asks if, in a factorization of a group G, can one factor always be replaced by a periodic factor? We now show that a special case of this does hold.

THEOREM 7.10

Let G be a finite cyclic group and let $G = A + B$ be a factorization in which each factor has order divisible by at most two distinct primes. Then one factor is replaceable by a periodic subset.

PROOF If the orders of A and B are relatively prime, then G is a direct sum of subgroups H, K with $|H| = |A|$ and $|K| = |B|$. By Theorem 3.19 (on page 59), we have that

$$G = A + B = H + B = A + K.$$

So each of A and B may be replaced by a subgroup.

Now we may suppose that there is a prime p dividing both $|A|$ and $|B|$. Let $|G| = p^e m$, where m is not divisible by p. Then $F_{p^e}(x)$ divides $A(x)$ or $B(x)$. We may assume that $F_{p^e}(x)$ divides $B(x)$. By Theorems 7.6 (on page 148) and 7.9 (on page 150), A satisfies conditions C1 and C2. By using the construction in the proof of Theorem 7.7 (on page 148), we obtain a subset C such that $G = A + C$ is a factorization. Now $F_{p^e}(x)$ does not divide $A(x)$ and so $C(x)$ contains a factor $F_{p^e}(x^m)$. As remarked after the proof of Theorem 7.7 (on page 148), this implies that C is periodic. So B has been replaced by a periodic factor, as required. ∎

7.3 Tiling the integers

We have dealt, so far, with finite cyclic groups. We now consider the infinite cyclic group. We shall always represent it as the additive group Z of integers. We should extend the concept of factorization to the infinite case. Let G be an infinite abelian group. Let I be an index set and let A_i, $i \in I$ be a family of subsets of G. We will assume that each A_i is normalized, that is, contains the zero element. If each element g of G can be expressed uniquely in the form

$$g = \sum_{i \in I} a_i, \qquad a_i \in A_i$$

such that only finitely many of the a_i's are distinct from 0, then we say that

$$G = \sum_{i \in I} A_i$$

is a factorization of G.

EXAMPLE 7.6 We consider the following well-known factorization of Z into an infinite sum of finite sets. Let $A_r = \{0, (-2)^r\}$, $r \geq 0$. Then

$$Z = \sum_{i=0}^{\infty} A_i.$$

This is the standard dyadic representation. Since no finite subset of Z can be periodic, we have a factorization with no periodic factor. □

By choosing infinite sets of factors we can obtain factorizations into two or more infinite sets, none of which is periodic.

EXAMPLE 7.7 One such choice occurs with

$$A = \sum_{r \text{ odd}} A_r, \qquad B = \sum_{r \text{ even}} A_r.$$

In this choice each $a \in A$ satisfies $a \leq 0$ and each $b \in B$ satisfies $b \geq 0$. This shows that Theorem 3.16 (on page 57) does not hold here. If we replace A by $-A$, then all factors in $-A$ and B are non-negative. The sum is still direct, but $(-A) + B$ simply leads to the binary representation of the set of non-negative integers. □

We should note that Theorem 3.15 (on page 57) also fails to hold.

EXAMPLE 7.8 Choose $g < 0$. Then

$$(g + a)_A = (g + a) - (g + a)_B \leq g + a \leq g.$$

Hence the set $\{(g + a)_A : a \in A\}$ cannot contain the elements of A that are greater than g. ∎

The elements $(g + a)_A$ in Example 7.8 (on page 153) are still distinct, that is, $(g + a_1)_A = (g + a_2)_A$ still implies, exactly as in the proof of Theorem 3.15 (on page 57), that $a_1 = a_2$. Hence the result still holds for finite subsets A of Z. The same is true for Theorem 3.16 (on page 57) but requires some additional proof, which we now present.

THEOREM 7.11

Let $Z = A + B$ be a factorization in which A is finite. Then $Z = (-A) + B$ is also a factorization.

PROOF There is no change needed in the proof that the sum $(-A) + B$ is direct. Let $g \in Z$. Since A is finite, the set $\{(g+a)_A : a \in A\}$ is equal to A. Since $0 \in A$, there exists $a \in A$ such that $(g + a)_A = 0$. So there exists $b \in B$ with $g + a = b$. Hence $g = (-a) + b \in (-A) + B$. Therefore $Z = (-A) + B$, as required. ∎

Theorem 3.17 (on page 58) deals only with finite subsets A and the result still holds for Z.

THEOREM 7.12

If the finite subset A of Z is a direct factor of Z and k is an integer relatively prime to $|A|$, then A is replaceable by kA.

PROOF There is no change in the proof as far as the statements that the sum $pA + B$ is direct and that $|pA| = |A|$, where p is a prime not dividing $|A|$. We need to show that if $A + B = Z$ is a factorization, then so also is $pA + B = Z$. Let $g \in Z$. We use the factorization $Z = (-A) + B$, obtained in Theorem 7.11 (on page 153). Hence

$$\big\{(g + p(-a))_{(-A)} : (-a) \in (-A)\big\} = -A.$$

Therefore there exists $a \in A$ such that $(g - pa)_{(-A)} = 0$. Then $g - pa \in B$ and so $g \in pA + B$.

It follows that $Z = pA + B$ is a factorization. As in Theorem 3.17 (on page 58), the general result follows by repeated use of this result. ∎

There is a more general result here.

THEOREM 7.13
If $Z = A+B$, where A is finite, and there exists a subset C such that $|C| = |A|$ and the sum $C + B$ is direct, then $Z = C + B$.

PROOF Let $g \in Z$. Then $Z = Z + g = (A + g) + B$. Therefore, by Theorem 7.11 (on page 153), $Z = -(A+g)+B$. Let $c \in C$. Then there exist $a \in A$, $b \in B$ with $-c = -(a+g)+b$. Hence $a+g = c+b$. Let $c' \in C$, $c' \neq c$. Then $a' + g = c' + b'$ for some $a' \in A$, $b' \in B$. If $a = a'$, then $c + b = c' + b'$. This contradicts the fact that the sum $C + B$ is direct. Since $|A| = |C|$, it follows that every element of A occurs. Since $0 \in A$, it follows that $g \in C+B$. Hence $C + B = G$. ∎

Because of the examples given earlier, we restrict our attention to the case $Z = A + B$, where A is finite. The subsets $A + b$, $b \in B$ are translates of A. The set A is said to tile Z when every integer belongs to exactly one such translate, that is, whenever $A + B$ gives a factorization of Z.

A subgroup of Z is of the form kZ, $k \geq 0$. For $k = 0$ the index $|Z : kZ| = \infty$. For $k > 0$ the index $|Z : kZ| = k$. Let $Z = A + B$ be a factorization of Z, where B is periodic. There is a subgroup H of Z and a normalized subset C of Z such that $B = C + H$. From the factorization $Z = A + (C + H)$ we get the factorization

$$Z/H = (A + H)/H + (C + H)/H$$

of the factor group Z/H. The index $|Z : H|$ is finite and we have a factorization of a finite cyclic group $Z/(kZ)$ for some integer k.

We now show that in any tiling of Z the set B of translations is a periodic set. We may translate the tile A and assume not only that $0 \in B$ but also that 0 is the least element in A. Let d be the largest element of A; that is, using geometrical terminology, let d be the diameter of A.

THEOREM 7.14
Let $Z = A + B$, where $|A|$ is finite, then the set B is periodic. The subgroup of periods kZ of B is such that $|A|$ divides k and $k \leq 2^d$.

PROOF For each $m \in Z$ let $B_m = \{b \in B : b \leq m\}$. (Therefore, in this proof, subscripts are reserved solely for this purpose.) Let $A = \{a(1), a(2), \ldots, a(n)\}$ with

$$0 = a(1) < a(2) < \cdots < a(n) = d.$$

Then from $Z = A + B$ it follows that $A + B_m$ consists of all integers less than or equal to m and a set C_m of Z satisfying $m < c \leq m + d$ for all $c \in C_m$. The smallest integer in $B \setminus B_m$ is determined by this set. It must be the least integer b with $b > m$, $b \notin C_m$, that is, the smallest integer b with

$b \notin A + B_m$. Let $D_m = C_m - m$. Then D_m is a subset of $[1, d]$. There are only a finite number of such subsets. Now at each stage the next element of B is determined by C_m, and this in turn determines the next set $A + B_{m+1}$. This process then repeats itself to determine B. Now if $D_m = D_{m'}$, where $m < m'$, the process is the same from $A + B_m$ and from $A + B_{m'}$. Hence $m' - m$ is a period of all elements in B from this stage onwards. We may start with any m. Since there are only a finite number of such periods, as each is less than or equal to 2^d, it follows that B is periodic. If the group of periods of B is kZ, then $B = B' + kZ$ for some finite subset B' and $Z = A + B' + kZ$ implies that $A + B'$ gives the integers modulo k. Hence $|A||B'| = k$ and so $|A|$ divides k. We have already noted that $k \leq 2^d$. □

This problem is often looked at from the opposite viewpoint. Given a finite subset A of Z, can we find conditions that imply that A tiles Z? Can we find necessary and sufficient conditions for this that depend only on the structure of A?

If the elements of a set A with $0 \in A$ have a common divisor d, we define $(1/d)A = \{(1/d)a : a \in A\}$.

THEOREM 7.15

Let A be a finite subset of Z with $0 \in A$ and let d be a common factor of the integers in A. Then A tiles Z if and only if $(1/d)A$ tiles Z.

PROOF Let A tile Z. Then there exists a subset B such that $Z = A + B$. Now $A \subseteq dZ$. Hence $A + (B \cap dZ) = dZ$. We may divide each subset here by d and so we obtain that $(1/d)A + (1/d)(B \cap dZ) = Z$. Hence $(1/d)A$ tiles Z.

Let $(1/d)A$ tile Z. Then there exists a subset C such that $(1/d)A + C = Z$. On multiplying by d we obtain that $A + dC = dZ$. Now let $E = \{0, 1, \ldots, d - 1\}$. Then $A + dC + E = dZ + E = Z$. Therefore A tiles Z. □

From this result it follows that we may assume that the greatest common divisor of the numbers in A is 1 without loss of generality.

We deal first with the case where $|A|$ is a prime power. If A consists of the elements

$$0 = a_1 < a_2 < \cdots < a_n,$$

then we may associate with it the polynomial

$$A(x) = \sum_{a \in A} x^a.$$

THEOREM 7.16

Let A be a subset of Z with its least element equal to 0 and order equal to p^e, where p is a prime. Then A tiles Z if and only if there exists e cyclotomic

polynomials

$$F_{p^{r(1)}}(x), \ldots, F_{p^{r(e)}}(x) \tag{7.2}$$

dividing $A(x)$, *where* $1 = r(1) < r(2) < \cdots < r(e)$.

PROOF Suppose first that A tiles Z. Then there is a subset B such that $Z = A + B$. By Theorem 7.14 (on page 154), there is an integer k divisible by p^e such that $B = B_1 + kZ$. Then $A + B_1$ is a complete set of residues modulo k, that is, it gives a factorization of $Z(k) \approx Z/(kZ)$. (Here $\approx$ stands for "is isomorphic to.") Now, using $1 + kZ$ as a generator, the polynomial $A(x)$ corresponds to the factor A when reduced modulo $x^k - 1$. Hence

$$A(x)B_1(x) \equiv 1 + x + x^2 + \cdots + x^{k-1} \pmod{(x^k - 1)}.$$

As in the proof of Theorem 7.6 (on page 148), exactly e cyclotomic polynomials in the list (7.2) divide $A(x)$. If $r(1) > 1$, then p divides every exponent in $A(x)$ and so the p divides every entry in A. So the assumption that the numbers in A have a greatest common divisor equal to 1 implies that $r(1) = 1$.

Conversely, if the cyclotomic polynomials (7.2) divide $A(x)$, then, by Theorem 7.7 (on page 148), there is an integer k and a subset B_1 such that $A + B_1$ is a complete set of residues modulo k. Setting $B = B_1 + kZ$, it follows that $A + B = Z$ and so that A tiles Z. □

We should note that the construction used in Theorem 7.7 (on page 148) leads to a factorization with $k = r(e)$, where $r(i) \le r(e)$, $1 \le i \le e$. In this case A is periodic modulo k with period equal to k/p. In the case $e = 1$, $A(x)$ is divisible by $F_p(x)$. Since $|A| = p$, it follows that A is a complete set of residues modulo p.

THEOREM 7.17

If A tiles Z, then there exists a set $B_1 + kZ$ such that $A + B_1 + kZ = Z$ and the only prime factors of k are the prime factors of $|A|$.

PROOF There exist sets B, C such that $B = C + mZ$ and $A + C + mZ = Z$. Let $m = kl$, where the primes dividing k divide $|A|$ and the primes dividing l do not divide $|A|$. By Theorem 7.12 (on page 153), we may replace A by lA and so obtain $lA + C + mZ = Z$. Since $lA \subseteq lZ$, it follows that $lA + \big((C + mZ) \cap lZ\big) = lZ$. As in the proof of Theorem 7.15 (on page 155), it follows that $A + (1/l)\big((C + mz) \cap lZ\big) = Z$. Since $m = lk$, it follows that $mZ \subseteq lZ$. So for $c \in C$, $c + md$, $d \in Z$ belongs to lZ if and only if l divides c. Therefore $(1/l)\big((C + mZ) \cap lZ\big) = B_1 + kZ$, where $b \in B_1$ if and only if $lb \in C$. Hence $A + B_1 + kZ = Z$, as required.

Let A be a subset of Z with least element 0. Let $A(x)$ satisfy conditions C1 and C2 of Section 7.2. For each prime p_i dividing $|A|$, let $e(i)$ be the

greatest integer among the integers $r(i)$ such that $F_{p_i^{r(i)}}(x)$ divides $A(x)$. Let $m = \prod p_i^{e(i)}$, where the product is taken over all prime divisors p_i of $|A|$. Then A corresponds to a subgroup A_1 of $Z/(mZ)$, where $a \in A$ corresponds to $a + mZ$ in A_1. Then $1 + mZ$ is a generator of $Z/(mZ)$ and $A(x) = A_1(x)$. By Theorem 7.7 (on page 148), A_1 is a direct factor of $Z/(mZ)$ and so there is a subset B_1 of $Z/(mZ)$ such that $A_1 + B_1 = Z/(mZ)$. Then B_1 corresponds, as above, to a subset B of Z and $A + B$ is a complete set of residues modulo m. Hence $A + B + mZ = Z$. So A tiles Z and this value of m satisfies the conditions of Theorem 7.17 (on page 156). It is also the least possible value of m. Suppose that $A + C + kZ = Z$ and that $p_i^{e(i)}$ does not divide k. Let $|A| = \prod p_i^{s(i)}$. Then, from $A_1 + C_1 = Z/(kZ)$, as above, it follows that there are $s(i)$ powers of p_i, each dividing k, such that the corresponding cyclotomic polynomials divide $A_1(x) = A(x)$. Then, since $p_i^{e(i)}$ also has this property, it follows that $p_i^{s(i)+1}$ divides $|A|$, which is false. Therefore $p_i^{e(i)}$ divides k and so m divides k, as required. ∎

Consider a factorization $Z = A+B$, where A is finite. By Theorem 7.14 (on page 154), B is periodic. The next result shows that there are factorizations $Z = A + B$ such that the length of the smallest positive period of B is large in comparison to the diameter of A.

THEOREM 7.18

There are infinitely many factorizations $Z = A + B$ and a fixed positive constant c such that $k > cd^2$, where k is the smallest positive period of B and d is the diameter of the finite set A.

PROOF Let p, q be primes such that $5 < p < q$. By a known result in number theory we can choose q such that $p < q < 2p$. Set $k = (3p)(5q)(2)$, $x = 10q$, $y = 6p$, $z = 15pq$. The cyclic group $Z(k)$ is a direct sum of the subgroups $\langle x\rangle$, $\langle y\rangle$, $\langle z\rangle$. The orders of the elements x, y, z are $3p$, $5q$, 2, respectively. By the construction in the proof of Theorem 3.4 (on page 41), there is a factorization $Z(k) = A+B_1$ such that none of the factors is periodic and A is in the form

$$A = \{0, x, 2x\} + \{0, y, 2y, 3y, 4y\}.$$

The diameter of A is

$$d = 20p + 24q < 20p + 24 \cdot 2p = 68p.$$

It follows that

$$k = 30pq > 30p^2 \geq 30\Big(\frac{d}{68}\Big)^2 = cd^2.$$

From the factorization $Z(k) = A + B_1$ we get a factorization $Z = A + (B_1 + kZ)$. □

From the proof of Theorem 7.14 (on page 154), we can see that $k \leq 2^d$ holds for each factorization $Z = A + B$, where d is the diameter of the finite A and k is the smallest period of B. The next theorem improves on this estimate asymptotically.

THEOREM 7.19

Let $Z = A + B$ be a factorization of Z, where d is the diameter of the finite A and k is the least positive period of B. There exist d_1, c_1, c_2 such that d_1 is an integer; c_1, c_2 are positive constants; and

$$k < c_1 \exp(c_2 \sqrt{d} \ln d \sqrt{\ln \ln d})$$

holds for $d > d_1$.

PROOF Consider a factorization $Z = A + B$ such that d is the diameter of the finite A and k is the smallest positive period of B. We may assume that 0 is the smallest and d is the largest element of A. There is a subset B_1 of Z such that $B = B_1 + kZ$. Now $Z = A + B_1 + kZ$ implies that $A + B_1$ is a complete set of residues modulo k. We can say that $A + B_1$ is a factorization of $Z(k)$.

For each divisor d of k, $d > 1$, the cyclotomic polynomial $F_d(x)$ divides $A(x)B_1(x)$. Let $F_{s(1)}(x), \ldots, F_{s(m)}(x)$ be all the cyclotomic polynomials among these that divide $A(x)$. The distinct divisors $s(1), \ldots, s(m)$ of k can be arranged such that

$$1 < s(1) < s(2) < \cdots < s(m).$$

As $F_{s(i)}(x)$ divides $A(x)$ and $\deg F_{s(i)}(x) = \phi(s(i))$, it follows that

$$\phi(s(1)) + \cdots + \phi(s(m)) \leq \deg A_1(x) \leq d. \tag{7.3}$$

A result from analytic number theory (see [54]) tells us that the lower limit of

$$\frac{\phi(n) \ln \ln n}{n}$$

is equal to $e^{-\gamma}$; that is, for each $\varepsilon > 0$, there is an integer n_0 such that

$$(e^{-\gamma} - \varepsilon) \frac{n}{\ln \ln n} \leq \phi(n) \tag{7.4}$$

for $n > n_0$. Here $\gamma = 0.57721\ldots$ is the Euler constant. Let us fix an ε, n_0 and set $c_3 = e^{-\gamma} - \varepsilon$. From (7.4) we get

$$\ln c_3 + \ln n \leq \ln \phi(n) + \ln \ln \ln n.$$

There is an $n_1 > n_0$ such that

$$\ln \phi(n) \le \ln n \le 2 \ln \phi(n) \tag{7.5}$$

for each $n > n_1$.

We claim that there is an integer d_2 such that

$$s(1) + \cdots + s(m) \le (e^{-\gamma} + 2\varepsilon) d \ln \ln d \tag{7.6}$$

for $d > d_2$. To prove the claim we estimate the sum $s(1) + \cdots + s(m)$:

$$\begin{aligned}
\sum_{i=1}^{m} s(i) &= \sum_{s(i) \le n_1} s(i) + \sum_{s(i) > n_1} s(i) \\
&\le n_1^2 + \sum_{s(i) > n_1} (e^{-\gamma} + \varepsilon) \phi(s(i)) \ln \ln(s(i)) && \text{(see (7.4))} \\
&\le n_1^2 + (e^{-\gamma} + \varepsilon) d \ln \ln(s(m)) && \text{(see (7.3))} \\
&\le n_1^2 + (e^{-\gamma} + \varepsilon) d (\ln 2 + \ln \ln d) && \text{(see (7.5))} \\
&\le (e^{-\gamma} + 2\varepsilon) d \ln \ln d. && \text{(for } d > d_2\text{)}
\end{aligned}$$

This proves the claim.

From (7.6) it follows that there is a positive constant c_4 such that $m \le c_4 \sqrt{d \ln \ln d}$ for $d > d_2$.

Let χ be a character of $Z(k)$. Note that if $\chi(A) = 0$, then $\chi(1)$ is a root of $A(x)$. If the order of $\chi(1)$ is s, then $F_s(x)$ divides $A(x)$. Conversely, if $F_s(x)$ divides $A(x)$, then $\chi(A) = 0$ for each character χ of $Z(k)$ with $|\chi(1)| = s$. (We have to admit that the notation $|\chi(1)|$ is rather confusing. As $\chi(1)$ is a complex number, some readers may think that $|\chi(1)|$ means the length of the number. The intended meaning of $|\chi(1)|$ here is the order of $\chi(1)$ in the multiplicative group of the non-zero complex numbers.)

Set $t = s(1) \cdots s(m)$. We claim that if $t < k$, then t is an element of the Corrádi subgroup of A and consequently, by Lemma 3.1 (on page 53), t is a period of B_1.

In order to prove the claim, assume that $t < k$ and note that $|\chi(1)|$ is one of $s(1), \ldots, s(k)$, say $|\chi(1)| = s(i)$. This implies that

$$\chi(t) = [\chi(1)]^t = [[\chi(1)]^{s(i)}]^{[t/s(i)]} = 1$$

as required.

As B_1 is not periodic, $k \le t$ holds. Finally there is an integer d_1 such that

$$\begin{aligned}
k \le t \le \prod_{i=1}^{m} s(i) &\le [(e^{-\gamma} + 2\varepsilon) d \ln \ln d]^m \\
&\le c_1 \exp(c_2 \sqrt{d} \ln d \sqrt{\ln \ln d})
\end{aligned}$$

for $d > d_1$. ∎

Notes

(1) The proof of Theorem 7.14 (on page 154) first appeared in Hajós [49] with the following introduction. "In a letter N. G. de Bruijn writes that if $G = A + B$ is a factorization of an infinite cyclic group and A is finite, then B must be periodic. Without knowing his proof I give a proof here."

(2) Theorems 7.18 and 7.19 (on page 158) are due to M. N. Kolountzakis [67]. A similar result is proved by L. Z. Ruzsa [112]. Improved estimates can be found in J. P. Steinberger [147] and A. Biró [5].

(3) Theorems 7.11, 7.12, and 7.13 are about factorizations of Z. In Chapter 8 we will see that, in fact, these results hold in full generality for each abelian group.

Chapter 8

Infinite groups

8.1 Groups with cyclic subgroups

We now turn our attention to infinite abelian groups with the property that every finitely generated subgroup is cyclic. We first give a description of these groups. We then consider factorizations of them, but restrict our attention to the cases where at most one factor is infinite.

THEOREM 8.1

Let G be a subgroup of a quotient group of the additive group Q of rationals. Then every finitely generated subgroup of G is cyclic.

PROOF Let $m_1/n_1, m_2/n_2, \ldots, m_k/n_k$ be a finite set of rational numbers with $m_i, n_i \in Z$, $n_i > 0$. Let n be the lowest common multiple of $n_1, \ldots, n_k$. Then $\langle m_1/n_1, \ldots, m_k/n_k \rangle \subseteq \langle 1/n \rangle$. Since subgroups of cyclic groups are cyclic, it follows that every finitely generated subgroup of Q is cyclic.

Since homomorphic images of cyclic groups are also cyclic, it follows that the same result holds for these groups and for their subgroups. ∎

We shall now show in a series of results that the converse of Theorem 8.1 (on page 161) also holds. We observe first that a mixed group G cannot have this property. If $a \in G$ has infinite order and $b \in G$ has non-zero finite order, then it is clear that $\langle a, b \rangle$ cannot be cyclic. So we need to consider only the torsion-free and torsion cases. We deal first with the torsion-free case.

THEOREM 8.2

Let G be a torsion-free group such that every finitely generated subgroup of G is cyclic. Then G is isomorphic to a subgroup of Q.

PROOF Let $a \in G$, $a \neq 0$. Let $b \in G$. Then $\langle a, b \rangle$ is cyclic and so there exists $c \in G$ with $\langle a, b \rangle = \langle c \rangle$. So for some integers m, n, we have that $a = mc$, $b = nc$, and $m \neq 0$. Suppose also that $\langle a, b \rangle \subseteq \langle d \rangle$. Then, for some integers u, v, we have that $a = ud$, $b = vd$, and $v \neq 0$. Hence $mc = vd$, $nc = vd$,

and so $vmc = vud = unc$. Since $c \neq 0$ and G is torsion-free, it follows that $vm = un$. Thus $v/u = n/m$.

Therefore there is a well-defined mapping from G to Q given by $f(b) = n/m$. Let $g \in G$ and let $f(g) = r/s$. Then there exists $h \in G$ with $\langle a, g\rangle \subseteq \langle h\rangle$ and $a = sh$, $g = rh$. Since $\langle c, h\rangle$ is cyclic, we may choose h with $\langle c\rangle \subseteq \langle h\rangle$ and so $c = kh$ for some integer k. Then $b + g = nc + rh = (nk + r)h$. It follows that $f(b + g) = (nk + r)/s$. Now $a = mc = mkh = sh$. Hence $mk = s$. Thus

$$f(b + g) = nk/mk + r/s = n/m + r/s = f(b) + f(g).$$

It is clear that $\mathrm{Ker} f = \{0\}$. Hence G is isomorphic to a subgroup of Q. ∎

We consider now the group Q/Z. This is a torsion group and so it is the direct sum of its primary components. Let p be a prime. Then the p-component of Q/Z is generated by the elements

$$a_1 = (1/p) + Z,\ a_2 = (1/p^2) + Z, \ldots, a_n = (1/p^n) + Z, \ldots.$$

These elements satisfy the relations $pa_1 = 0$, $pa_n = a_{n-1}$, $n \geq 2$. This group is known as a Prüfer group and is denoted by $Z(p^\infty)$. Let $g \in Z(p^\infty)$, $g \neq 0$. Then there exist integers m_r such that

$$g = \sum_{r=1}^{k} m_r a_r, \quad 0 \leq m_r < p, \quad m_k \neq 0.$$

Since $a_r = p^{k-r} a_k$, $1 \leq r \leq k$. It follows that $g = ma_k$, where p does not divide m. Then there exists s such that $ms \equiv 1 \pmod{p^k}$ and so $sg = a_k$. Hence $\langle g\rangle = \langle a_k\rangle$. Since this Prüfer group is a subgroup of an image of Q, it follows by Theorem 8.1 (on page 161) that every finitely generated subgroup is cyclic. Thus

$$\{0\} \subseteq \langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots \subseteq \langle a_k\rangle \subseteq \cdots$$

is an ascending chain containing every finitely generated subgroup of $Z(p^\infty)$. If $\langle g_1, \ldots, g_j, \ldots\rangle$ is an infinitely generated subgroup, then there exist integers n_j such that $\langle g_j\rangle = \langle a_{n_j}\rangle$. The set of integers n_j must be unbounded. It follows that $Z(p^\infty)$ itself is the only infinite subgroup.

THEOREM 8.3

Let G be a torsion group such that every finitely generated subgroup is cyclic. Then G is isomorphic to a subgroup of G/Z.

PROOF Since G is the direct sum of its primary components, it suffices to prove the result for these. So we may suppose that G is a p-group for some prime p. If G is finite, then G itself must be cyclic. Thus G is isomorphic to the subgroup $\langle a_k\rangle$ of $Z(p^\infty)$ for some integer k.

Suppose now that G is infinite. Let $b, c \in G$. Then $\langle b, c\rangle$ is isomorphic to $Z(p^k)$ for some integer k. Since the subgroups of $Z(p^k)$ form a chain, it follows that either $\langle b\rangle \subseteq \langle c\rangle$ or that $\langle c\rangle \subseteq \langle b\rangle$. Let $b_1 \in G$, $b_1 \neq 0$, be such that $pb_1 = 0$. Suppose that $b_2, \ldots, b_m$ exist in G such that $pb_r = b_{r-1}$ for $2 \leq r \leq m$. Then $\langle b_m\rangle$ is isomorphic to $Z(p^m)$. If G has no element of order greater than p^m, then, by the above, each $g \in G$ satisfies $\langle g\rangle \subseteq \langle a_m\rangle$. This is not possible as G is infinite. It follows that G contains an element b of order p^{m+1}. Then, by the above, $\langle b_m\rangle \subseteq \langle b\rangle$. From consideration of the orders it follows that $pub = b + m$ for some integer u not divisible by p.

Let $ub = b_m$. Then $pb_{m+1} = b_m$. Thus we may construct an infinite ascending chain of subgroups,

$$\{0\} \subseteq \langle b_1\rangle \subseteq \cdots \subseteq \langle b_m\rangle \subseteq \cdots \subseteq G.$$

If $g \in G$ and g has order p^m, then $\langle g\rangle \subseteq \langle b_m\rangle$. It follows that $\bigcup\langle b_m\rangle = G$. Hence G is isomorphic to $Z(p^\infty)$.

If we now return to the general case we see that

$$G = \bigoplus_{p\in P}(G)_p = \Big[\bigoplus_{p\in P_1} Z(p^\infty)\Big] \oplus \Big[\bigoplus_{p\in P_2} Z(p^{m_p})\Big],$$

where P is the set of all primes and P_1, P_2 are disjoint sets of primes. It follows that G is isomorphic to a subgroup of Q/Z.

It follows from the remark about mixed groups and Theorems 8.2 (on page 161) and 8.3 (on page 162) that the converse of Theorem 8.1 (on page 161) holds. ∎

When we are considering factorizations of infinite groups, we shall always assume that each factor contains the zero element. If A_i, $i \in I$, is a set of subsets of a group G, then $\sum_{i\in I} A_i$ is the set of each $g \in G$ for which there exists a finite subset I_1 of I such that

$$g = \sum_{i\in I_1} a_i$$

for some elements $a_i \in A_i$. Equivalently, we can use the convention that

$$g = \sum_{i\in I} a_i,$$

where $a_i \in A_i$ and only a finite number of elements a_i are non-zero. As usual, the sum of subsets $\sum_{i\in I} A_i$ is direct if

$$\sum_{i\in I} a_i = \sum_{i\in I} a_i',$$

where a_i and a_i' are in A_i, implies that $a_i = a_i'$ for all $i \in I$. A direct sum gives a factorization of G if each element $g \in G$ is expressible in this form.

We consider first torsion-free groups.

THEOREM 8.4

Let G be a non-zero subgroup of Q and let $G = A_1 + \cdots + A_k + B$ be a factorization of G in which each subset A_i is finite. Then the subset B is periodic.

PROOF Let $A_1 + \cdots + A_k = A$. Then A is a finite subset of G and so $H = \langle A \rangle$ is a cyclic group. Let h be a generator of H. Then there is a finite set of integers m_j, $j \in J$ with $A = \{m_j h : j \in J\}$. Let $m = \max\{|m_i - m_j| : i, j \in J\}$. Let C be a set of coset representatives for G modulo H. Since $A \subseteq H$ it follows, for each $c \in C$, that $A + \big((B \cap (H + c)) - c\big) = H$. Then, by Theorem 7.14 (on page 154), $B \cap (H + c)$ is periodic with period m_c satisfying $0 < m_c \leq 2^m$. Let n be the lowest common multiple of the numbers $1, 2, \ldots, 2^m$. Then m_c divides n for each $c \in C$. Hence n is a period of $B \cap (H + c)$ and so n is a period of B as

$$B = \bigcup_{c \in C} \big[B \cap (H + c)\big].$$

∎

As noted in Exercises 7.6 (on page 152) and 7.7 (on page 152), there are bad (non-periodic) factorizations of Z involving infinitely many finite sets or two or more infinite sets. These examples may also be extended to non-zero subgroups of Q. As we have seen above, such a group G contains a cyclic subgroup $H = \langle h \rangle$ and

$$G/H \approx \Big[\bigoplus_{p \in P_1} Z(p^\infty)\Big] \oplus \Big[\bigoplus_{p \in P_2} Z(p^{n_p})\Big].$$

Now we may write the corresponding subgroup of G/H as

$$\{0, h/p, 2h/p, \ldots, (p-1)h/p\}$$
$$+\{0, h/p^2, 2h/p^2, \ldots, (p-1)h/p^2\} + \cdots.$$

This process will terminate if $p \in P_2$ and continue indefinitely if $p \in P_1$. In G, none of these sets is periodic and so the desired examples may be constructed starting with examples for H and then using these subsets to extend them to G.

We now turn to the case of infinite torsion groups. If such a group G contains a finite cyclic group which admits bad factorizations, then, in a similar way, we may extend these to bad factorizations of G. Since the cyclic groups

$$Z(p^3q^2), \quad Z(p^3qr)$$

admit bad factorizations, the only groups left to consider are the infinite subgroups of $Z(p^\infty) \oplus Z(q)$. Here we are assuming that p, q, r are distinct primes. We present first one general result which is a generalization of Theorem 4.4 (on page 73). We then turn to specific groups.

THEOREM 8.5

Let G be an infinite torsion group such that every finitely generated subgroup is cyclic. Let p be a prime and let $G = A_1 + \cdots + A_k + B$ be a factorization of G in which each A_i is a finite set and $|A_i|$ is a power of p. Then one of the factors is periodic.

PROOF Let $H = \langle A_1, A_2, \ldots, A_k \rangle$. Then H is a finite cyclic group. Let C be a set of coset representatives for G modulo H. Then, as in the proof of Theorem 8.4 (on page 164), it follows that

$$A_1 + \cdots + A_k + \big((B \cap (H + c)) - c\big) = H,$$

for each $c \in C$. Let B_c be a translation of $\big((B \cap (H + c)) - c\big)$ such that $0 \in B_c$. Then $A_1 + \cdots + A_k + B_c = H$.

It follows from Theorem 4.4 (on page 73) that, for each $c \in C$, one of these factors is periodic. If some factor A_i is periodic, then the desired result holds. So we may assume that B_c is periodic for each $c \in C$. In order to complete the proof we need to examine more closely the proof of Theorem 4.4 (on page 73).

In the factorization of H we may replace each subset A_i by its p-component B_i. If none of these components is periodic, it follows that the unique subgroup P of H of order p is a subgroup of periods of B_c for each $c \in C$. It follows, as above, that B is periodic. If some subset, say B_1, is periodic, then there is a unique subgroup L determined by A_1 and H. If $L = \{0\}$, then A_1 is periodic. If $L \neq \{0\}$, then L is a subgroup of periods of B_c for each $c \in C$. Again it follows that B is periodic. ∎

THEOREM 8.6

If p, q are distinct primes; $G = Z(p^\infty) \oplus Z(q)$; and

$$G = A_1 + \cdots + A_k + B,$$

where all the subsets A_i are finite, then one of the factors of G is periodic.

PROOF Let $H = \langle A_1, A_2, \ldots, A_k \rangle$. Then H is a finite cyclic subgroup of G and $|H|$ divides $p^n q$ for some integer n. Let C be a set of coset representatives for G modulo H. As in the proof of Theorem 8.4 (on page 164), it follows that

$$A_1 + \cdots + A_k + \big((B \cap (H + c)) - c\big) = H$$

for all $c \in C$. Since $Z(p^n q)$ and its subgroups have the Hajós m-property for all relevant m, it follows that one of these factors is periodic. If $A_1, \ldots, A_k$ have order a power of p, it follows by Theorem 8.5 (on page 165) that one factor from $A_1, \ldots, A_k, B$ must be periodic. If not all $|A_i|$ are powers of p, then q divides $|A_i|$ for one value of i and $B \cap (H + c)$ has order a power of p for all $c \in C$. Hence, if no factor A_i is periodic, the unique subgroup P of order p is a subgroup of periods of $B \cap (H + c)$ for all $c \in C$. As before, it follows that B is periodic. □

The same result holds for $K = Z(p^\infty)$. This follows from Theorem 8.5 (on page 165). It also follows from Theorem 8.6 (on page 165) since if $b \in G = Z(p^\infty) \oplus Z(q)$ has order q and $a \in K$, $a \neq 0$, then

$$D = \{0, b, \ldots, (q-2)b, (q-1)b + a\}$$

is a non-periodic set of coset representatives for G modulo K.

We now consider factorizations involving infinitely many factors.

THEOREM 8.7

Let p, q be distinct primes $G = Z(p^\infty) \oplus Z(q)$ and let

$$G = \sum_{i \in I} A_i$$

be a factorization in which all the factors A_i are finite. Then one of these factors is periodic.

PROOF Let H be the subgroup of G of order pq. Then each element of H belongs to a finite sum of factors A_i. Since H is finite, it follows that H belongs to a finite sum of factors, say

$$H \subseteq \sum_{i \in J} A_i,$$

where J is a finite subset of I. Let

$$B = \sum_{i \in I \setminus J} A_i.$$

For convenience we may suppose that $J = \{1, \ldots, k\}$. Then $G = A_1 + \cdots + A_k + B$. By Theorem 8.6 (on page 165), either one of the factors $A_1, \ldots, A_k$ is periodic or B is periodic. If B is periodic, then one of its periods has order either p or q. However, these elements belong to H and $H + B$ is a direct sum. This is not possible. Hence one of the factors $A_1, \ldots, A_k$ is periodic. □

As before, the result also holds for $K = Z(p^\infty)$ since $G = K + D$ and D is finite but is not periodic.

THEOREM 8.8
Let p, q be distinct primes $G = Z(p^\infty) \oplus Z(q)$ and

$$G = B + \sum_{i \in I} A_i$$

be a factorization in which all the factors A_i are finite. Then some factor of G is periodic.

PROOF If I is a finite set, the result follows by Theorem 8.6 (on page 165). So we may assume that I is infinite. Since G is countable, it follows that I is countable and we may assume that $I = \{1, 2, 3, \ldots\}$. For each $k \in I$ let

$$H_k = \langle A_1, A_2, \ldots, A_k \rangle, \quad B_{k+1} = B + \sum_{i>k} A_i.$$

Let C_k be a set of coset representatives for G modulo H_k. Then

$$A_1 + \cdots + A_k + \big((B_{k+1} \cap (H_k + c)) - c\big) = H_k$$

for all $c \in C_k$. As in the proofs of Theorems 4.4 (on page 73) and 8.5 (on page 165), it follows either that one of the factors $A_1, \ldots, A_k$ is periodic or that there is a period of $B_{k+1} \cap (H_k + c)$ which depends only on $A_1, \ldots, A_k$ and not on c. As above, it follows that B_{k+1} is periodic and that an element a of order p or an element d of order q is a period. Since G has only one subgroup of order p and only one subgroup of order q, either all elements of order p or all elements of order q are periods of B_{k+1}. It follows that either a or d is a period of B_{k+1} for infinitely many k.

Suppose that this holds for a, say. Let $g \in B$. Then $g \in B_{k+1}$ and so $g + a \in B_{k+1}$ for infinitely many k. Let $k = r$ be such a value. Then $g + a = a_{r+1} + \cdots + a_{r+s} + b$ with $a_i \in A_i$, $b \in B$. Let $k = t > r + s$ be such a value. Then $g + a = a_{r+1} + \cdots + a_{r+s} + b'$ with $a_i \in A_i$, $b' \in B$. Now the sum $B + \sum A_i$ is assumed to be direct. It follows that

$$a_{r+1} + \cdots + a_{r+s} = a_{t+1} + \cdots + a_{t+u} = 0$$

and that $b = b'$. Hence $B + a \subseteq B$. Now

$$\Big(\sum A_i\Big) + B + a = G + a = G.$$

This could not hold if $B + a \neq B$. Hence $B + a = B$. It follows that B is periodic. ∎

It is natural to consider whether the formulae given in Section 4.2 for good finite groups still apply in these infinite cases.

It is clear that this is not the case for the groups considered in Theorem 8.4 (on page 164). In a factorization of Z, after one step we obtain a factorization

of an image of Z. This can be any finite cyclic group. So it need not be good and the process cannot be continued.

In the case of the groups covered in Theorems 8.5 (on page 165) and 8.6 (on page 165), the process can be continued. If a subset A_i has prime power order so also will any image of it. Also, the images of the groups $Z(p^\infty) \oplus Z(q)$ and $Z(p^\infty)$ are either of these type or are isomorphic to $Z(q)$. It follows that the process will continue at each stage. Furthermore, since $A_1, \ldots, A_k$ are finite subsets, the process will terminate after a finite number of steps.

We give one short example to illustrate this for a factorization of the type considered in Theorem 8.5 (on page 165).

EXAMPLE 8.1 Let $G = Z(p^\infty) \oplus Z(q)$, where p, q are distinct primes. Let $G = A_1 + A_2 + B$, where $|A_1| = |A_2| = p$. Then one of the these factors is periodic. Let us suppose that B is periodic with group of periods H_1. Then $B = H_1 + B_1$ for some subset B_1. As before, this leads to the factorization

$$G/H_1 = (A_1 + H_1)/H_1 + (A_2 + H_1)/H_1 + (B_1 + H_1)/H_1.$$

Since $A_1 + A_2 + H_1$ is direct, it follows that

$$\big|(A_1 + H_1)/H_1 + (A_2 + H_1)/H_1\big| = p^2.$$

Now it follows that one of these two subsets is periodic and, as it has prime order, it must be a subgroup. We may assume that $(A_1 + H_1)/H_1 = H_2/H_1$, that is, $A_1 + H_1 = H_2$, where H_2 is a subgroup and H_1 has index p in H_2. Now we have a factorization,

$$G/H_2 = (A_2 + H_2)/H_2 + (B_1 + H_2)/H_2.$$

Again we have that $\big|(A_2+H_2)/H_2\big| = p$ since $A_2+H_2 = A_1+A_2+H_1$ is a direct sum. Again it follows that one of the two factors of G/H_2 is periodic. Let us suppose that $(A_2+H_2)/H_2$ is periodic. (We should note that if $(B_1+H_2)/H_2$ is periodic, then the image of $(A_2 + H_2)/H_2$ would be periodic at the next stage.) As for A_1, it follows that $A_2 + H_2 = H_3$, where H_3 is a subgroup and H_2 has index p in H_3. This now leads to $G/H_3 = (B_1 + H_3)/H_3$, that is, to $G = B_1 + H_3$.

So we have a chain of subgroups,

$$\{0\} \subseteq H_1 \subseteq H_2 \subseteq H_3 = G$$

and

$$\begin{aligned} H_2 &= H_1 + A_1, \\ H_3 &= H_2 + A_2, \\ G &= H_3 + B_1, \\ B &= H_1 + B_1. \end{aligned}$$

So once again it is a question of finding sets of coset representatives for H_2 modulo H_1 to find A_1, for H_3 modulo H_2 to find A_2, and for G modulo H_3 to

find B_1. So once again the formulae of Section 4.2 arise. The only difference is that H_1 may be an infinite subgroup and that H_3 may have infinite index in G. One of these must hold and both may hold. □

8.2 Groups with special p-components

It has been shown that if in the factorization of a finite abelian group, which has a cyclic p-component for one prime p, every factor except perhaps one has order a power of p, then one factor must be periodic. In this section this result is extended to certain infinite abelian groups. It is assumed that the group is a torsion group and that for some prime p the p-component is either cyclic or quasi-cyclic. The result is proved first in the case where the number of factors is finite and then for an infinite number of factors, assuming, as above, that every factor except perhaps one has order a power of p.

Let p be a prime. It was shown in Theorem 4.4 (on page 73) that if G is a finite abelian group with cyclic p-component and there is a factorization of G such that every factor except perhaps one has order a power of p, then one factor must be periodic. Here we consider the generalization of this result to certain infinite groups. We assume that the group G is a torsion group. We assume that the p-component of G is either cyclic or quasi-cyclic. It is then shown that the corresponding result holds.

In order to avoid trivial cases, it is assumed that each factor A_i has order greater than 1.

Even for finite groups these results do not generalize further. Let p and q be distinct primes. A special case of a result of N. G. De Bruijn [10] shows that the group $Z(p^3q^2)$ has a factorization involving three non-periodic factors of orders p, q, and p^2q. So we cannot allow two factors whose order is not a power of p, nor allow two factors of different prime orders. For non-cyclic groups there are again examples due to N. G. de Bruijn [10] with two factors each non-periodic for such groups of order p^3, $p > 3$, and similar but more complicated examples for $p = 2$ and $p = 3$. An example will be given here of a factorization of Z in which each factor has order p, for any prime p and, since non-zero subgroups of Z are infinite, no factor can be periodic. This will be used to show that Theorem 8.10 (on page 171) does not hold for any torsion-free or mixed group.

We consider first the case in which the number of factors is finite.

THEOREM 8.9

Let p be a prime and let G be a torsion abelian group whose p-component $(G)_p$ is either cyclic or quasi-cyclic. If $G = A_1 + \cdots + A_k + B$ is a factorization of G in which each factor A_i is finite and has order a power of p, then one of

the factors of G is periodic.

PROOF This result is a generalization to the infinite case of Theorem 4.4 (on page 73). There the corresponding result for finite abelian groups is shown to hold. In order to prove the present result, we shall need not just the result but some details of the proof given there.

By Theorem 3.17 (on page 58), we may replace A_i by kA_i for any integer k not divisible by p. Since G is a torsion group, the subgroup $(G)_p$ has as its complement in G the subgroup H which is the direct sum of the other primary components of G. Since A_i is finite, there exists an integer n, not divisible by p, such that the order of the H-component of each element in A_i divides n. Similarly, there exists an integer p^e such that the order of the p-component of each element of A_i divides p^e. Let $mn \equiv 1 \pmod{p^e}$. Let $mnA_i = B_i$. Then B_i is the subset consisting of the p-components of the elements of A_i and so $B_i \subseteq (G)_p$. By Theorem 3.17 (on page 58) it follows that $|B_i| = |A_i|$ and that $G = B_1 + \cdots + B_k + B$ is a factorization of G. It follows that for each $h \in H$

$$B_1 + \cdots + B_k + \big((B \cap ((G)_p + h)) - h\big) = (G)_p.$$

If $(G)_p$ is cyclic, it follows by a result of G. Hajós (or by Theorem 4.3 on page 67) that one of these factors is periodic. So the unique subgroup M of order p is a group of periods of the periodic factor. If no factor B_i is periodic, it follows that, for each $h \in H$, $B \cap ((G)_p + h)$ has M as a group of periods. Since B is the union of these subsets, B is periodic with M as a group of periods. So, in this case, we may assume that one of the other factors here, say B_1, has M as a group of periods.

Now we consider the case in which $(G)_p = Z(p^\infty)$. Since $B_1 + \cdots + B_k$ is a finite set, the subgroup N generated by it is a finite subgroup of $(G)_p$ and so is cyclic of order a power of p. Let $(B \cap ((G)_p + h)) - h$ be denoted by B_h for each $h \in H$. Let C be a complete set of coset representatives for N modulo $(G)_p$. Then, for each $c \in C$,

$$B_1 + \cdots + B_k + \big((B_h \cap (N + c)) - c\big) = N.$$

As before, it follows that M is a group of periods of some factor. If no factor B_i is periodic, then M is a group of periods of $B_h \cap (N + c)$, for each $c \in C$, and so is a group of periods of B_h for each $h \in H$. As above, it follows that B is periodic. Again we may assume that M is a group of periods of B_1.

Now let us consider the factorization $G = A_1 + B_2 + \cdots + B_k + B$. Let F be the subgroup generated by $A_1 + B_2 + \cdots + B_k$. Since this set is finite, the subgroup F is finite. Let D be a complete set of coset representatives for G modulo F. Then, for each $d \in D$, it follows that

$$F = A_1 + B_2 + \cdots + B_k + \big((B \cap (F + d)) - d\big)$$

is a factorization. As stated earlier, we now need to make use of the proof of Theorem 4.4 (on page 73). There a subgroup K is defined which depends

only on A_1 and F. It is shown there that if $K = \{0\}$, then A_1 is periodic. If $K \neq \{0\}$, then it is shown that K is a group of periods of $B \cap (F + d)$. Since the definition of K does not depend on d, it follows as above that K is a group of periods of B. ∎

We now turn to the general case where the number of factors is infinite.

THEOREM 8.10

Let p be a prime and let G be a torsion abelian group whose p-component is either cyclic or quasi-cyclic. If $G = B + \sum_{i\in I} A_i$ is a factorization of G in which each factor A_i has order a power of p, then one of the factors of G is periodic.

PROOF We may assume that the set I is infinite. As above, each factor A_i may be replaced by its p-component B_i. Hence any finite sum of these factors may be replaced in this way. Since each element of the sum $\sum B_i$ is contained in a finite sum, it follows that the infinite sum is still direct. Since I is infinite and each B_i is contained in $(G)_p$, it follows that $(G)_p = Z(p^\infty)$. Since $\sum B_i$ is direct and $(G)_p$ is countable, it follows that I is a countable set. We may assume that I is the set of positive integers.

Let

$$C_k = B + \sum_{i>k} A_i.$$

Then $G = B_1 + \cdots + B_k + C_k$ is a factorization. Then $(G)_p = B_1 + \cdots + B_k + (C_k \cap (G)_p)$ is a factorization. If no factor B_i, $i \in I$, is periodic, it follows as in the proof of Theorem 8.9 (on page 169) that the subgroup M of order p of $(G)_p$ is a group of periods of C_k for every k. Since the sum $B + \sum A_i$ is direct, it is easy to see that

$$\bigcap_{k\in I} C_k = B.$$

It follows that M is a group of periods of B.

Thus we may assume that some factor B_i, say B_1, is periodic. Let F_k be the subgroup generated by $A_1 + B_2 + \cdots + B_k$ for each $k \in I$. Since each subset here is finite and G is a torsion group, it follows that F_k is a finite abelian group. We have the factorizations $A_1 + B_2 + \cdots + B_k + (C_k \cap F_k) = F_k$. As in the proof of Theorem 4.4 (on page 73) there is a subgroup K_k whose definition depends only on A_1 and F_k such that A_1 is periodic if $K_k = \{0\}$ and, if $K_k \neq \{0\}$, then K_k is a group of periods of C_k. We need to examine the definition of K_k as given in the proof of Theorem 4.4 (on page 73). There the characters χ of F_k are considered such that the restriction of χ to the p-component of F_k is injective. Equivalently, these are the characters χ of F_k such that $\chi(M) = 0$. The subgroup K_k is then defined to be the intersection of the kernels of all such characters which have the additional property that $\chi(A_1) = 0$. The

subgroups F_k, $k \in I$, form an ascending chain. Since $B_1 = mA_1$ for some m, it follows from $M \subseteq \langle B_1 \rangle$ that $M \subseteq \langle A_1 \rangle = F_1$. Hence, if the character χ has the desired property for F_k, then the restriction of χ to F_1 also has this property. It is clear that $\mathrm{Ker}(\chi|_{F_1}) \subseteq \mathrm{Ker}(\chi)$. It follows that $K_1 \subseteq K_k$.

If A_1 is not periodic, it follows that $K_1 \neq \{0\}$. Then K_1 is a group of periods of C_k for all k. As above, it follows that K_1 is a group of periods of B. ∎

We have assumed in these two theorems that the group involved is a torsion abelian group. If we consider the group Z of integers, then there exist factorizations in which each factor has prime order.

EXAMPLE 8.2 Let p be a prime and define the subsets A_r by

$$A_r = (-p)^{r-1}\{0, 1, \ldots, p-1\}.$$

Then $Z = \sum A_r$. This is not a new result since it is simply a rephrasing of the fact that each integer n may be expressed uniquely as

$$n = \sum a_r(-p)^{r-1}$$

with each $a_r \in \{0, 1, \ldots, p-1\}$. ∎

We may use the factorization in Example 8.2 (on page 172) in two ways. For the first of these we need the following result.

LEMMA 8.1

Let H be a proper non-zero subgroup of an abelian group G. Then there exists a non-periodic complete set of coset representatives for G modulo H except in the case where H is a subgroup of index 2 in an elementary 2-group.

PROOF Since any subset of order 2 in an elementary 2-group is periodic, it is clear that the result cannot hold in the exceptional case. Otherwise, if H has index 2 and the set $\{0, c\}$ is a periodic set of coset representatives, we may choose $a \in H$ with $2a \neq 0$ and use the non-periodic set $\{0, a+c\}$ instead. Now assume that H has index greater than 2. Let C be a complete set of coset representatives for G modulo H with $0 \in H$. If C is periodic, let d be a period. Let h be any non-zero element of H. Then the set B formed from C by replacing d by $h + d$ is also a complete set of coset representatives and $0 \in B$. Let g be a period of B and let b be a non-zero element of $B \cap C$. If $g = h + d$, then $h + d + b = c$, where $c \in C$. Since the sum $H + C$ is direct and normalized from

$$\underbrace{(\ h\ )}_{\in H} + \underbrace{(\ d+b\ )}_{\in C} = \underbrace{(\ 0\ )}_{\in H} + \underbrace{(\ c\ )}_{\in C},$$

it follows that $h = 0$, $d + b = c$. But $h = 0$ is a contradiction.

Then, for $g \neq h + d$, we have that $g + h + d = b_1$, where $b_1 \in B \cap C$. Since the sum $H + B$ is direct and normalized from

$$\underbrace{(\ h\ )}_{\in H} + \underbrace{(\ g + d\ )}_{\in B} = \underbrace{(\ 0\ )}_{\in H} + \underbrace{(\ b_1\ )}_{\in B},$$

it follows that $h = 0$, $g + d = b_1$. But $h = 0$ is a contradiction. Therefore B is a non-periodic set, as required. □

EXAMPLE 8.3 If the abelian group G is not a torsion group, then it contains a subgroup H isomorphic to Z. We may factorize H, as above, into a sum of non-periodic subsets of prime order p. By Lemma 8.1 (on page 172), we may factorize G as $H + B$, where B is non-periodic. Thus we have a factorization of G into a sum of subsets all of which, except one, have order p and such that no factor is periodic. Thus Theorem 8.10 (on page 171) does not hold for any torsion-free or mixed abelian group. □

We can use this example involving Z to demonstrate another result.

EXAMPLE 8.4 In the proofs we have replaced a finite number of factors by other factors and have also mentioned that the replacement of infinitely many factors still results in a direct sum. It need not, however, still give a factorization. Let us consider the factorization given above of Z taking $p = 2$ to give a specific example. We may replace A_1 by $5A_1$ and replace A_r by $3A_r$ for all $r > 1$. This gives a sum equal to $\{0, 5\} + 6Z$, which is not even a subgroup of Z. □

Let $G = A + B$ be a normalized factorization of the infinite abelian group G, where A is infinite. Now the sum $A + B$ is direct. Let us construct the subset C from A by removing one element from $A \setminus \{0\}$. Clearly, $|C| = |A|$ and the sum $C + B$ is direct. However, the sum $C + B$ is not equal to G and so it is not a factorization of G. A. D. Sands [128] asked the following: Let $G = A + B$ be a factorization, where A is finite. Let C be a subset of G such that $|C| = |A|$ and the sum $C + B$ is direct. Does it follow that $G = C + B$ is a factorization of G?

S. J. Eigen and V. S. Prasad [27] have shown that the answer is in the affirmative. We present their result since this is the key to extending certain factorization results from finite abelian groups to infinite ones. We need two lemmata.

LEMMA 8.2

Let G be an abelian group and let A, B, C be normalized subsets of G such that A and C are finite. If $G \subseteq A + B$ and the sum $C + B$ is direct, then

$|C| \leq |A|$.

PROOF As $G \subseteq A + B$, the union of the subsets $A + b$, $b \in B$ is equal to G. It follows that

$$\begin{aligned} C &= C \cap G \\ &= C \cap (A + B) \\ &= C \cap \Big[\bigcup_{b \in B} (A + b)\Big] \\ &= \bigcup_{b \in B} \Big[C \cap (A + b)\Big]. \end{aligned}$$

Considering the cardinalities we get

$$|C| = \sum_{b \in B} \big|C \cap (A + b)\big|. \tag{8.1}$$

Note that the directness of the sum $C + B$ implies the directness of the sum $C + (-B)$. Indeed, let $c_1, c_2 \in C$, $b_1, b_2 \in B$ such that

$$c_1 + (-b_1) = c_2 + (-b_2).$$

Rearranging this equation we get

$$c_1 + b_2 = c_2 + b_1.$$

Since the sum $C + B$ is direct, it follows that $c_1 = c_2$ and $b_2 = b_1$, as required.

As the sum $C + (-B)$ is direct, the sets $C - b$, $b \in B$ are pair-wise disjoint. It follows that

$$\begin{aligned} A &= A \cap G \\ &\supseteq A \cap [C + (-B)] \\ &= A \cap \Big[\bigcup_{b \in B} (C - b)\Big] \\ &= \bigcup_{b \in B} \Big[A \cap (C - b)\Big]. \end{aligned}$$

Considering the cardinalities we get

$$\sum_{b \in B} \big|A \cap (C - b)\big| \leq |A|. \tag{8.2}$$

Using

$$\big|C \cap (A + b)\big| = \big|A \cap (C - b)\big|$$

from (8.1) and (8.2) we get $|C| \leq |A|$, as required. ∎

LEMMA 8.3

Let G be an abelian group and let A, B be normalized subsets of G. If $G = A + B$ is a factorization of G and A is finite, then $G = A + (-B)$ is a factorization of G.

PROOF As the sum $A+B$ is direct, so is the sum $A+(-B)$. Consequently, the sets $A - b$, $b \in B$ are pair-wise disjoint. We would like to show that the sets $A - b$, $b \in B$ in fact form a partition of G. Assume on the contrary that there is a $g \in G$ such that

$$g \notin \bigcup_{b\in B} (A - b).$$

Now

$$\begin{aligned} A + g &= (A + g) \cap G \\ &\supseteq (A + g) \cap [A + (-B)] \\ &= (A + g) \cap \Big[\bigcup_{b\in B} (A - b)\Big] \\ &= \bigcup_{b\in B} \Big[(A + g) \cap (A - b)\Big]. \end{aligned}$$

Considering the cardinalities we get

$$\sum_{b\in B} \big|(A + g) \cap (A - b)\big| < |A + g|. \tag{8.3}$$

Adding g to both sides of the factorization $G = A + B$, we get the factorization $G = (A + g) + B$. The union of the sets $(A + g) + b$, $b \in B$ is equal to G. It follows that

$$\begin{aligned} A &= A \cap G \\ &= A \cap [(A + g) + B] \\ &= A \cap \Big\{\bigcup_{b\in B} [(A + g) + b]\Big\} \\ &= \bigcup_{b\in B} \Big\{A \cap [(A + g) + b]\Big\}. \end{aligned}$$

Considering the cardinalities we get

$$|A| = \sum_{b\in B} \big|A \cap [(A + g) + b]\big|. \tag{8.4}$$

Using

$$\big|A \cap [(A + g) + b]\big| = \big|(A - b) \cap (A + g)\big|$$

from (8.3) and (8.4) we get the $|A| < |A + g| = |A|$ contradiction. ∎

THEOREM 8.11

Let G be an abelian group and let A, B, C be normalized subsets of G such that A is finite. If $G = A + B$ is a factorization, $|C| = |A|$ and the sum $C + B$ is direct, then $G = C + B$ is a factorization.

PROOF We need to prove only $G \subseteq C + B$. Since the sum $C + B$ is direct, the sets $C + b$, $b \in B$ are pair-wise disjoint. We would like to show that the sets $C + b$, $b \in B$ form a partition of G:

$$\begin{aligned} A + g &= (A + g) \cap G \\ &\supseteq (A + g) \cap (C + B) \\ &= (A + g) \cap \Big[\bigcup_{b \in B} (C + b)\Big] \\ &= \bigcup_{b \in B} \Big[(A + g) \cap (C + b)\Big]. \end{aligned}$$

For the cardinalities this gives

$$\sum_{b \in B} \big|(A + g) \cap (C + b)\big| < |A + g|. \tag{8.5}$$

In the factorization $G = A + B$, by Lemma 8.3 (on page 175), the factor B can be replaced by $(-B)$ to get the factorization $G = A + (-B)$. Adding g to both sides of the factorization $G = A + (-B)$, we get the factorization $G = (A + g) + (-B)$. The union of the sets $(A + g) - b$, $b \in B$ is equal to G. It follows that

$$\begin{aligned} C &= C \cap G \\ &= C \cap [(A + g) + (-B)] \\ &= C \cap \Big\{\bigcup_{b \in B} [(A + g) - b]\Big\} \\ &= \bigcup_{b \in B} \Big\{C \cap [(A + g) - b]\Big\}. \end{aligned}$$

Counting the elements we get

$$|C| = \sum_{b \in B} \big|(C \cap [(A + g) - b]\big|. \tag{8.6}$$

Using

$$\big|C \cap [(A + g) - b]\big| = \big|(C + b) \cap (A + g)\big|$$

from (8.5) and (8.6) we get $|C| < |A + g| = |A|$. By Lemma 8.2, this is a contradiction. ∎

Next we extend Theorem 4.3 (on page 67) to infinite groups. We need a lemma about replacing subsets by a cyclic subset.

LEMMA 8.4
Let $G = A + B$ be a normalized factorization of the abelian group G such that $|A| = p$ is a prime. Choose an $a \in A \setminus \{0\}$ and set

$$C = \{0, a, 2a, \ldots, (p-1)a\}.$$

Then $G = C + B$ is a factorization of G.

PROOF By Theorem 3.17 (on page 58), in the factorization $G = A + B$, the factor A can be replaced by tA to get the factorization $G = tA + B$ for each integer t that is relatively prime to p. Suppose that

$$A = \{0, a_1, a_2, \ldots, a_{p-1}\}.$$

The factorization $G = tA + B$ is equivalent to the fact that the sets

$$t0 + B,\ ta_1 + B,\ ta_2 + B, \ldots, ta_{p-1} + B \tag{8.7}$$

form a partition of G. We will show that the sets

$$0a_1 + B,\ 1a_1 + B,\ 2a_1 + B, \ldots, (p-1)a_1 + B \tag{8.8}$$

form a partition of G. This will give that $G = C + B$ is a factorization of G, where

$$C = \{0, a_1, 2a_1, \ldots, (p-1)a_1\}.$$

First we claim that the sets in the list (8.8) are disjoint. To prove the claim, assume the contrary, that $(ia_1 + B) \cap (ja_1 + B) \neq \emptyset$, where $0 \leq i < j \leq p-1$. It follows that $(0a_1 + B) \cap (ta_1 + B) \neq \emptyset$, where $t = j - i$. This is a contradiction.

Choose a $g \in G$. Then we claim that $g \in ia_1 + B$ for some i, $0 \leq i \leq p-1$. To prove the claim consider the sets (8.7) for $1 \leq t \leq p-1$. If $g \in t0 + B$ or $g \in ta_1 + B$ for some t, $1 \leq t \leq p-1$, then we are done. So we may assume that $g \notin t0 + B$ and $g \notin ta_1 + B$ for each t, $1 \leq t \leq p-1$. By the pigeon-hole principle, there are i, j, s such that $1 \leq i < j \leq p-1$, $2 \leq s \leq p-1$ and $g \in ia_s + B$, $g \in ja_s + B$. Now $(ia_s + B) \cap (ja_s + B) \neq \emptyset$, from which we get the contradiction $(0 + B) \cap (ta_s + B) \neq \emptyset$, where $t = j - i$. ∎

THEOREM 8.12
Let $p_1, \ldots, p_s$ be distinct primes and let G be a group in the form

$$G = \sum_{i=1}^{s} Z(p_i^\infty).$$

Suppose that

$$G = \sum_{i \in I} A_i$$

is a normalized factorization of G, where $|A_i|$ is a product of two distinct primes or a power of a prime for finitely many i and $|A_i|$ is a prime for the remaining i. Then at least one of the factors is periodic.

PROOF Assume the contrary, that

$$G = \sum_{i \in I} A_i \tag{8.9}$$

is a counter-example.

(1) Choose a factor A in (8.9) for which $|A| = q$ is a prime. We claim that q is equal to one of $p_1, \ldots, p_s$. In order to prove the claim, assume the contrary, that q is not equal to any of $p_1, \ldots, p_s$. Write the factorization (8.9) in the form $G = A + B$, where

$$B = \sum_{\substack{i \in I \\ A_i \neq A}} A_i. \tag{8.10}$$

Set

$$t = \prod_{a \in A} |a|.$$

Since G is a torsion group, such a t does exist. Plainly t is relatively prime to q. By Theorem 3.17 (on page 58), in the factorization $G = A + B$, the factor A can be replaced by tA to get the factorization $G = tA + B$. As tA is a member of a factorization, it follows that the elements ta, $a \in A$ are distinct. But $ta = 0$ for each $a \in A$. This contradiction shows that q is equal to one of $p_1, \ldots, p_s$.

(2) Let A be a factor in (8.9) for which $|A| = q$ is a prime. Write the factorization (8.9) in the form $G = A + B$, where B is defined by (8.10). Set

$$(A)_q = \{(a)_q : \ a \in A\}.$$

We claim that in the factorization $G = A + B$ the factor A can be replaced by $(A)_q$ to get the factorization $G = (A)_q + B$. In particular, the q-parts of the elements of A are distinct. To verify the claim let

$$u = \prod_{a \in A} |(a)_{q'}|,$$
$$v = \prod_{a \in A} |(a)_q|.$$

The congruence $ut \equiv 1 \pmod{v}$ is solvable for t as u is relatively prime to v. Clearly ut is relatively prime to q and so, by Theorem 3.17 (on page 58), in the factorization $G = A + B$ the factor A can be replaced by utA to get the factorization $G = utA + B$. Let w be the order of $(a)_q$. Computing uta we get

$$\begin{aligned} uta &= ut[(a)_q] + ut[(a)_{q'}] \\ &= ut[(a)_q] \\ &= (a)_q, \end{aligned}$$

since $ut \equiv 1 \pmod{w}$ also holds. Therefore $(A)_q = utA$, and this proves the claim.

(3) Choose a factor A in the factorization (8.9) for which $|A| = q$ is a prime. By Lemma 8.4 (on page 177), in the factorization $G = A + B$ the factor A can be replaced by the cyclic subset

$$C = \{0, c, 2c, \ldots, (q-1)c\}, \tag{8.11}$$

where $c \in A \setminus \{0\}$, to get the factorization $G = C + B$. We distinguish two cases. If there is an $a \in A$ such that $|(a)_q| = q^\alpha$, $\alpha \geq 2$, then A can be replaced by $(A)_q$, then $(A)_q$ can be replaced by a cyclic subset in the form (8.11), where $|c| = q^\alpha$. Clearly this C is not periodic. We replace A by C in the factorization (8.9). In order to keep the notational difficulties to a minimum, we will denote C again by A. In other words, we keep the old names for the new factors.

If $|(a)_q| = q$ for each $a \in A \setminus \{0\}$ and $q > 2$, then $(A)_q$ is the unique subgroup of $Z(q^\infty)$ of order q. Since A is not a subgroup of G, it follows that there is an $a \in A \setminus \{0\}$ such that $(a)_{q'} \neq 0$. In this case A can be replaced by a cyclic subset C in the form (8.11), where $|(c)_q| = q$ and $|(c)_{q'}|$ is a prime, and so it is one of $p_1, \ldots, p_s$. Clearly C is not periodic. We replace A by C in the factorization (8.9) but then change the name C back to A.

(4) We partition the index set I into three sets I_1, I_2, I_3 in the following manner. If $i \in I_1 \cup I_2$, then

$$A_i = \{0, a_i, 2a_i, \ldots, (q_i - 1)a_i\},$$

where q_i is a prime. In the $i \in I_1$ case $|a_i| = q_i^{\alpha(i)}$, $\alpha(i) \geq 2$. In the $i \in I_2$ case $|a_i|$ is a product of two distinct primes. If $i \in I_3$, then $|A_i|$ is either a product of two distinct primes or a power of a prime. In this case we do not modify A_i.

(5) Let A, B be factors of the factorization (8.9) such that $|A| = |B| = q$ is an odd prime. We claim that if $a \in A \setminus \{0\}$, $b \in B \setminus \{0\}$, then $|(a)_q| \neq |(b)_q|$. In particular, I_2 cannot have more than s elements. To prove the claim assume the contrary, that $a \in A \setminus \{0\}$, $b \in B \setminus \{0\}$, $|(a)_q| = |(b)_q|$ and write the factorization (8.9) in the form $G = A + B + C$, where

$$C = \sum_{\substack{i \in I \\ A_i \neq A, B}} A_i.$$

Using step (2) from the factorization $G = A + B + C$ we get the factorization $G = (A)_q + (B)_q + C$. Since $|(a)_q| = |(b)_q|$, it follows that $(a)_q$ and $(b)_q$ span the same cyclic subgroup of $Z(q^\infty)$. There is an integer t such that $t[(a)_q] = (b)_q$. Clearly t is relatively prime to q. By Theorem 3.17 (on page 58), in the factorization $G = (A)_q + (B)_q + C$, the factor $(A)_q$ can be replaced by $t[(A)_q]$ to get the factorization $G = t[(A)_q] + (B)_q + C = A' + B' + C$.

From

$$\underbrace{(\ t[(a)_q]\ )}_{\in A'} + \underbrace{(\ 0\ )}_{\in B'} + \underbrace{(\ 0\ )}_{\in C} = \underbrace{(\ 0\ )}_{\in A'} + \underbrace{(\ (b)_q\ )}_{\in B'} + \underbrace{(\ 0\ )}_{\in C}$$

it follows the contradiction that $t[(a)_q] = (b)_q = 0$.

(6) Let q be one of the primes $p_1, \ldots, p_s$. Note that the sum

$$\sum_{|A_i|=q} (A_i)_q$$

is direct and is equal to $Z(q^\infty)$. If $i \in I_2$, then A_i is in the form

$$A_i = \{0, c_i + d_i, 2(c_i + d_i), \ldots, (q_i - 1)(c_i + d_i)\},$$

where $|c_i| = q_i$ and $|d_i|$ are from the primes $p_1, \ldots, p_s$.

Because of the structure of G, for each positive integer f there is a unique cyclic subgroup H_i of $Z(p_i^\infty)$ of order p_i^f. Since $I_2 \cup I_3$ is a finite set, there is a positive integer f such that

$$A_i \subseteq H_1 \oplus \cdots \oplus H_s = H$$

for each $i \in I_2 \cup I_3$. Set $J = \{i :\ A_i \subseteq H\}$ We claim that

$$H = \sum_{i \in J} A_i$$

is a factorization. We have already seen that $A_i \subseteq H$ for each $i \in J$. Set

$$B = \sum_{i \in J} A_i.$$

We will show that $H \subseteq B$. There is a finite subset J' of I such that

$$H \subseteq \sum_{i \in J'} A_i.$$

For the sake of notational convenience we assume that $J' = \{1, \ldots, n\}$, where n is a positive integer. Clearly $J \subseteq J'$.

Choose an $h \in H$. Since $h \in G$ and since (8.9) is a factorization of G, h can be represented in the form

$$h = a_1 + \cdots + a_n, \quad a_1 \in A_1, \ldots, a_n \in A_n.$$

If $J' \subseteq J$, then we are done. Thus we may assume that $n \notin J$, $a_n \neq 0$ since this is only a matter of rearranging finitely many factors in the factorization (8.9). As $n \notin J$, it follows that $n \in I_1$. The order of a_n is a multiple of q^{f+1}, where q is one of $p_1, \ldots, p_s$. The order of the q-part of h is at most q^f. This leads to the

$$\begin{aligned} q^f &\geq |(h)_q| \\ &= \max\{|(a_1)_q|, \ldots, |(a_n)_q|\} \\ &\geq q^{f+1} \end{aligned}$$

contradiction. Therefore

$$H = \sum_{i \in J} A_i$$

is a factorization. Here H is a finite cyclic group. By Theorem 4.3 (on page 67), one of the factors is periodic. This contradiction completes the proof. □

In [140] S. K. Stein advances the following problem.

PROBLEM 8.1 Let $Z^n = A + B$ be a normalized factorization. Suppose A is finite and has n independent elements. Is there a subset C such that $Z^n = A + C$ is a normalized factorization and C has n independent periods? □

If the answer for Problem 8.1 is affirmative, then there is a subset D and a subgroup H of Z^n such that the index $|Z^n : H|$ is finite and the sum $D + H$ is direct and is equal to C. So $Z^n = A + C = A + D + H$ is a factorization. From this we get the normalized factorization

$$Z^n/H = (A + H)/H + (D + H)/H.$$

Note that the factor group Z^n/H is finite. As a side result, the problem if a given subset A tiles Z^n can be reduced to a finite problem and consequently can be decided in finitely many steps.

Stein's problem is unsolved. However, in the special case when the cardinality of A is a prime, a stronger result holds. Namely, not only the factor B can be replaced by a periodic subset but in fact B itself has n independent periods. This result is a consequence of Lemma 8.4 (on page 177).

THEOREM 8.13

Let $Z^n = A + B$ be a normalized factorization of Z^n. If $|A|$ is a prime and A has n independent elements, then B has n independent periods.

PROOF Let $|A| = p$, where p is a prime. Let $a_1, \ldots, a_n$ be independent elements of A. Set

$$A_i = \{0, a_i, 2a_i, \ldots, (p-1)a_i\}.$$

In the factorization $Z^n = A + B$, by Lemma 8.4 (on page 177), the factor A can be replaced by A_i to get the normalized factorization $Z^n = A_i + B$. From this, by the proof of Lemma 6.1 (on page 122), it follows that $B = pa_i + B$, that is, pa_i is a period of B. □

Notes

(1) The results of the factorization theory of finite cyclic groups are motivated by the applications from other fields of mathematics. The situation with infinite groups is different. These results are not answers for the need of applications. Here we wanted to contrast the infinite case with the purely finite factorizations.

(2) The fact that the infinite groups $Z(p^\infty) \oplus Z_q$, $Z(2^\infty) \oplus Z_2$, $Q \oplus Z_p$ have the Hajós 2-property was proved first in [118]. Here it was also shown that these are the only infinite groups having the Hajós 2-property.

(3) M. Szegedy [166] solves the $|A| \leq 4$ particular case of Problem 8.1 (on page 181). He also solves the special case when $|A|$ is a prime.

Chapter 9

Combinatorics

9.1 Complete maps

For a positive integer n, an n by n *Latin square* is an n by n array that consists of n^2 cells arranged in n rows and n columns. Each cell contains one of the n symbols and each symbol appears in each row and in each column. A *transversal* of the array consists of n cells, one from each row and no two from the same column. If the symbols in a transversal are all distinct, then it is called a *Latin transversal*.

Let $a_1, \ldots, a_n$ be all the elements of G. A permutation $b_1, \ldots, b_n$ of the elements of G is called a *complete permutation* of G if $a_1 + b_1, \ldots, a_n + b_n$ is also a permutation of the elements of G. In other words, a function $f : G \to G$ is called a *complete map* of G if f is one-to-one and if the function $g : G \to G$ defined by $g(a) = a + f(a)$, $a \in G$ is also one-to-one.

Let G be a finite abelian group of order n with Cayley table C. Clearly C is a Latin square. Each transversal of C can be associated with a one-to-one function $f : G \to G$ such that, for each $a_i \in G$, the transversal contains the element $a_i + f(a_i)$ in the row in C corresponding to a_i. If the elements $a_i + f(a_i)$, $1 \leq i \leq n$ form a permutation of the elements of G, then the n cells of the transversal contain n distinct elements and the transversal is a Latin transversal. It is clear that in the case of a Latin transversal both the set of elements $f(a_i)$, $1 \leq i \leq n$ and the set of elements $a_i + f(a_i)$, $1 \leq i \leq n$ are equal to G. Conversely, if a permutation f of the elements of G exists such that the elements $a_i + f(a_i)$, $1 \leq i \leq n$ also form a permutation of the elements of G, then these sets give rise, as above, to a Latin transversal in C. If f is such a permutation and $b_1 \in G$, then clearly the mapping $g_1 : G \to G$ defined by $g_1(a_i) = b_1 + f(a_i)$ is also such a permutation. We can construct n complete maps in this way. If $b_1 \neq b_2$, then clearly $g_1(a_i) \neq g_2(a_i)$ and so these n Latin transversals do not intersect in pairs. Thus if one Latin transversal exists in C, then C is a disjoint union of n Latin transversals. If such a permutation f of G exists, then

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} f(a_i)$$

$$= \sum_{i=1}^{n} \big(a_i + f(a_i)\big)$$
$$= \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} f(a_i)$$
$$= 2\sum_{i=1}^{n} a_i.$$

Hence

$$\sum_{i=1}^{n} a_i = 0.$$

We now describe the groups which satisfy this condition.

THEOREM 9.1

The sum of the elements of a finite abelian group G is equal to zero if and only if the 2-component $(G)_2$ of G is not a non-zero cyclic group.

PROOF The elements g of G such that $2g \neq 0$ occur in pairs as $\{g, -g\}$ and hence sum to zero. Let $H = \{g \in G : \ 2g = 0\}$. If $H = \{0\}$, then the sum of elements of G is zero, as required. Otherwise, H is a direct sum of s subgroups and each is isomorphic to $Z(2)$. Let $b_1, \ldots, b_s$ be a basis for H. Then in

$$\sum_{h \in H} h,$$

each element b_i occurs 2^{s-1} times in terms of the sum. If $s > 1$, then, since $2^{s-1}b_i = 0$, it follows that the sum is zero. If $s = 1$, then the sum is equal to b_1 and so in this case it is not zero. □

Thus the equivalent conditions of this theorem are necessary conditions for the existence of a transversal in the Cayley table.

In 1947 L. J. Paige [103] showed that they are also sufficient. We present now a proof of this result using ideas from the factorization theory.

EXERCISE 9.1

(a) Let the 2-component of a finite abelian group G be the direct sum of s cyclic groups (distinct from $\{0\}$). Show that G has $2^s - 1$ elements of order two.

(b) Suppose that a finite abelian group G has exactly one element of order two. Show that the 2-component of G is cyclic.

□

TABLE 9.1: Complete maps for the groups $Z(2) \oplus Z(2) \oplus Z(2)$ and $Z(2n) \oplus Z(2)$

a	$f(a)$	$a + f(a)$
0	0	0
x	z	$x + z$
y	$x + z$	$x + y + z$
$x + y$	x	y
z	$x + y + z$	$x + y$
$x + z$	$x + y$	$y + z$
$y + z$	y	z
$x + y + z$	$y + z$	x
a	$f(a)$	$a + f(a)$
$(2k)x$	$(n - k)x$	$(n + k)x$
$(2k)x + y$	$(2n - k)x + y$	$(k)x$
$(2k + 1)x$	$(n - k)x + y$	$(n + k + 1)x + y$
$(2k + 1)x + y$	$(2n - k)x$	$(k + 1)x + y$

In view of Exercise 9.1, Paige's theorem can be reformulated equivalently in the following form.

THEOREM 9.2

A finite abelian group G possesses a complete map if and only if the 2-component of G is either $\{0\}$ or the direct sum of at least two cyclic groups (distinct from $\{0\}$).

PROOF We divide the proof into smaller steps.

(1) A group of type $Z(2) \oplus Z(2) \oplus Z(2)$ has a complete map.

In order to prove this claim, let G be a group of type $Z(2) \oplus Z(2) \oplus Z(2)$ with basis elements x, y, z, where $|x| = |y| = |z| = 2$. Table 9.1 (on page 185) shows that G has a complete map.

(2) A group of type $Z(2n) \oplus Z(2)$, where $n \geq 1$ has a complete map.

In order to prove the claim, let G be a group of type $Z(2n) \oplus Z(2)$, $n \geq 1$. Let x, y be basis elements of G such that $|x| = 2n$, $|y| = 2$. Set

$$H = \langle x \rangle, \quad K = \langle y \rangle, \quad M = \langle 2x \rangle, \quad N = \langle nx \rangle,$$

$$C = \{0, x, 2x, \ldots, (n-1)x\}.$$

We use Table 9.1 (on page 185) to show that G has a complete map. As k runs from 0 to $n - 1$, the elements in the first column run over the elements of the sets M, $M + y$, $M + x$, $M + x + y$, respectively. Note that

$$\begin{aligned} G &= H + K \\ &= (M + \{0, x\}) + \{0, y\} \\ &= M + (\{0, x\} + \{0, y\}) \end{aligned}$$

$$= M + \{0, x, y, x + y\}$$

are factorizations of G. It follows that the sets M, $M + y$, $M + x$, $M + x + y$ form a partition of G. Thus a runs over the elements of G. Similarly, the factorizations

$$\begin{aligned} G &= H + K \\ &= x + (H + K) \\ &= x + H + K \\ &= x + (C + N) + K \\ &= x + C + \{0, nx\} + \{0, y\} \end{aligned}$$

give that the sets $C + x$, $C + (n + 1)x + y$, $C + x + y$, $C + (n + 1)x$ form a partition of G. Therefore $f(a)$ runs over the elements of G. Finally, the equations

$$\begin{aligned} G &= H + K \\ &= H + \{0, y\} \\ &= H \cup (H + y) \\ &= H \cup (H + x + y) \\ &= H + \{0, x + y\} \\ &= C + N + \{0, x + y\} \\ &= C + \{0, nx\} + \{0, x + y\} \end{aligned}$$

show that the sets $C + nx$, C, $C + (n + 1)x + y$, $C + x + y$ form a partition of G. It follows that $a + f(a)$ runs over the elements of G. Therefore G has a complete map.

(3) Let G be a finite abelian group and let H be a subgroup of G. If both H and the factor group G/H have a complete map, then so does G. In particular, if G is the direct sum of the groups H and K such that both H and K have complete maps, then so does G.

To prove the claim, assume that $h_1, \ldots, h_r$ are all the elements of H and $k_1, \ldots, k_r$ is a complete permutation of H, that is, $h_1 + k_1, \ldots, h_r + k_r$ are all the elements of H. Then assume that $a_1 + H, \ldots, a_s + H$ are all the elements of G/H and $b_1 + H, \ldots, b_s + H$ is a complete permutation of G/H. This means that $a_1 + b_1 + H, \ldots, a_s + b_s + H$ is a rearrangement of the elements of G/H. It follows that these cosets are disjoint and their union is equal to G, that is, $G = \{a_1 + b_1, \ldots, a_s + b_s\} + H$ is a factorization of G. In other words,

$$\begin{matrix} (a_1 + b_1) + (h_1 + k_1), \ldots, (a_1 + b_1) + (h_r + k_r) \\ \vdots \qquad\qquad \ddots \qquad\qquad \vdots \\ (a_s + b_s) + (h_1 + k_1), \ldots, (a_s + b_s) + (h_r + k_r) \end{matrix}$$

are all the elements of G. Therefore G has a complete map.

(4) A group of type $Z(2^{\alpha(1)}) \oplus Z(2^{\alpha(2)})$, where $\alpha(1) \geq \alpha(2) \geq 1$ has a complete map.

To prove the claim, let G be a group of type $Z(2^{\alpha(1)}) \oplus Z(2^{\alpha(2)})$, with $\alpha(1) \geq \alpha(2) \geq 1$. If $\alpha(2) = 1$, then by step (2), G has a complete map. So we may assume that $\alpha(2) \geq 2$ and start an induction on $\alpha(2)$. Now G has a subgroup H of type $Z(2) \oplus Z(2)$ such that the factor group G/H is of type $Z(2^{\alpha(1)-1}) \oplus Z(2^{\alpha(2)-1})$. By step (2), H has a complete map. By the inductive assumption, G/H has a complete map. Therefore, by step (3), G has a complete map.

(5) A non-cyclic group of type $Z(2) \oplus \cdots \oplus Z(2)$ has a complete map.

In order to prove this assertion, let G be a group of type $Z(2) \oplus \cdots \oplus Z(2)$, where the number of the direct summands is n and $n \geq 2$. First let us deal with the case when n is even. The $n = 2$ case has already been settled in step (2). So we may assume that $n \geq 4$. As G is a direct sum of subgroups of types

$$Z(2) \oplus Z(2), \ldots, Z(2) \oplus Z(2),$$

one can use step (3) repeatedly to show that G has a complete map. Let us turn to the case when n is odd. The $n = 3$ case has already been settled in step (1). We may assume that $n \geq 5$. Now G is a direct sum of groups of types

$$Z(2) \oplus Z(2) \oplus Z(2),\ \ Z(2) \oplus Z(2), \ldots, Z(2) \oplus Z(2)$$

and we can use step (3) to show that G has a complete map.

(6) A group of type $Z(2^{\alpha(1)}) \oplus \cdots \oplus Z(2^{\alpha(n)})$, where $n \geq 3$ and $\alpha(1) \geq \cdots \geq \alpha(n) \geq 1$, has a complete map.

In order to verify the claim, consider a group G of type $Z(2^{\alpha(1)}) \oplus \cdots \oplus Z(2^{\alpha(n)})$, where $n \geq 3$ and $\alpha(1) \geq \cdots \geq \alpha(n) \geq 1$. Set $t = \alpha(1) + \cdots + \alpha(n)$. If $\alpha(1) = 1$, that is, if $t = n$, then by step (5) we are done. We may assume that $\alpha(1) \geq 2$, that is, $t \geq n + 1$, and start an induction on t. Clearly G has a subgroup H of type $Z(2) \oplus Z(2)$ such that the factor group G/H is of type

$$Z(2^{\alpha(1)-1}) \oplus Z(2^{\alpha(2)-1}) \oplus Z(2^{\alpha(3)}) \oplus \cdots \oplus Z(2^{\alpha(n)})$$

or

$$Z(2^{\alpha(1)-1}) \oplus Z(2^{\alpha(3)}) \oplus \cdots \oplus Z(2^{\alpha(n)}),$$

depending on whether $\alpha(2) \geq 2$ or $\alpha(2) = 1$. By step (2), H has a complete map. By the inductive assumption, G/H has a complete map. Finally, by step (3), G has a complete map.

(7) A finite abelian group of odd order has a complete map.

Indeed, the map $f : G \to G$ defined by $f(a) = a$, $a \in G$ is suitable.

(8) We are ready to finish the proof. Let G be a finite abelian group such that G does not have exactly one element of order two. The group G can be written uniquely as a direct sum of the groups H and K such that the order of H is odd and the order of K is a power of 2. Since G does not have exactly one element of order two, K is not a cyclic group, that is, K is not of type $Z(2^{\alpha})$. Therefore, by steps (4), (5), and (6), K has a complete map. By step (7), H has a complete map. Hence, by step (3), G has a complete map.

This completes the proof. ∎

L. Euler observed that if a Latin square does not have a Latin transversal, then it cannot have an orthogonal mate. He also observed that the addition table of a cyclic group of even order has no Latin transversal.

THEOREM 9.3

Let G be an abelian group of order n and let M be its addition table. We know that M is an n by n Latin square.

(i) *If M has a Latin transversal, then it does not have a transversal with exactly $n-1$ distinct symbols.*

(ii) *If M has a transversal with exactly $n-1$ distinct symbols, then it does not have a Latin transversal.*

(iii) *If n is an odd prime, then M does not have a transversal with exactly two distinct symbols.*

PROOF Let $a_1, \ldots, a_n$ be all the elements of G. The addition table M of G can be described by listing the triples $[a_i, a_j, a_i + a_j]$, $1 \leq i, j \leq n$. Here $a_i + a_j$ is the symbol in the row labeled by a_i and in the column labeled by a_j.

If $f : G \to G$ is a one-to-one map, then $f(a_1), \ldots, f(a_n)$ is a permutation of the elements $a_1, \ldots, a_n$ and the triples $[a_i, f(a_i), a_i + f(a_i)]$, $1 \leq i \leq n$ form a transversal of M.

The elements of order two in G together with the zero element 0 form a subgroup H of G, which is a direct sum of s cyclic groups of order two. To prove (i), assume that M has a Latin transversal. By Paige's theorem, $s \neq 1$, that is, either $s = 0$ or $s \geq 2$. Assume also that the table has a transversal containing exactly $n-1$ distinct symbols. Let the triples $[a_i, f(a_i), a_i + f(a_i)]$, $1 \leq i \leq n$ form this transversal and its entries. The list $a_1 + f(a_1), \ldots, a_n + f(a_n)$ contains exactly $n-1$ distinct elements of G. Thus one element of G is missing from the list, say u, and one element of G appears twice, say v. Clearly $u \neq v$. The sum $a_1 + f(a_1) + \cdots + a_n + f(a_n) + u - v$ is equal to the sum $a_1 + \cdots + a_n$. This gives $f(a_1) + \cdots + f(a_n) = v - u$. We know that $f(a_1), \ldots, f(a_n)$ is a permutation of $a_1, \ldots, a_n$. Every non-zero element whose order is not two can be paired with its negative. So $f(a_1) + \cdots + f(a_n) = h_1 + \cdots + h_t$, where $h_1, \ldots, h_t$ are all the elements of H. In the case $s = 0$, $H = \{0\}$ and we get the contradiction $u = v$. In the case $s \geq 2$, again $h_1 + \cdots + h_t = 0$ and we get the contradiction $u = v$. In order to see that $h_1 + \cdots + h_t = 0$, list 2^s sequences of 0's and 1's of length s. Each sequence forms a row of a 2^s by s table. Notice that each column contains 2^{s-1} 0's and 2^{s-1} 1's. Since the latter number is even, $h_1 + \cdots + h_t = 0$.

The case (ii) is the contrapositive of case (i).

Let us turn to the proof of (iii). Suppose that n is an odd prime and M has a transversal with exactly two distinct elements. Suppose that the triples $[a_i, f(a_i), a_i + f(a_i)]$, $1 \leq i \leq n$ form this transversal. There are exactly two distinct elements in the list $a_1 + f(a_1), \ldots, a_n + f(a_n)$, say u and v. The sum $a_1 + f(a_1) + \cdots + a_n + f(a_n)$ is equal 0, as is shown by pairing each element with its negative. The sum is also equal to $ku + (n-k)v$, where $1 \leq k \leq n-1$. Thus $0 = ku + (n-k)v$. This implies $ku = kv$, which, since k is relatively prime to the order of G, leads to the contradiction, $u = v$. ∎

9.2 Ramsey numbers

Let K_n be the complete graph on n vertices. The number of edges of K_n is $\binom{n}{2}$. We color all of these edges of K_n using m colors. A subgraph K_r of K_n is called monochrome if all edges of K_r have the same color. If K_n does not contain a monochrome K_r, then we say that K_n is monochrome K_r-free. It is an exercise to show that no matter how the edges of K_6 are colored with two colors, there is always a monochrome K_3 in K_6. It is a classical result of F. P. Ramsey [106] that, for each m and r, there is a number $R_m(r)$ such that if $n \geq R_m(r)$, then K_n always contains a monochrome K_r, no matter how the edges of K_n are colored with m colors. The numbers $R_m(r)$ are called *Ramsey numbers.*

Factorizations of finite cyclic groups can be used to establish lower bounds for Ramsey numbers. Let H be a finite abelian group. A subset S of $H \setminus \{0\}$ is called *symmetric* if $x \in S$ implies $-x \in S$. A subset S of $H \setminus \{0\}$ is called *r-free* if S is symmetric and there are no distinct elements $x_1, \ldots, x_r \in S$ such that $x_i - x_j$ belongs to S for each i, j, $1 \leq i, j \leq r$, $i \neq j$. In other words, S is r-free if S is symmetric and for each distinct $x_1, \ldots, x_r \in S$ there are distinct x_i, x_j such that $x_i - x_j \notin S$.

EXERCISE 9.2 Let H be the group of integers modulo 13 and set $S = \{-2, -1, 1, 2\}$. The set S plainly has one subset of order 4. Check by inspection that S is a 4-free subset of H. The set S has 4 subsets of order 3. After inspecting them, show that S is 3-free. The set S has 6 subsets of order 2. Verify that S is not 2-free. ∎

LEMMA 9.1

Let H be a finite abelian group. Suppose that the sets $A_1, \ldots, A_m$ form a partition of $H \setminus \{0\}$. If each A_i is r-free, then $R_m(r+1) \geq |H| + 1$.

PROOF Let $n = |H|$ and let K_n be the complete graph whose nodes are

the elements of H. Choose an edge (x, y) of K_n. Compute $x - y$. Note that $x - y \neq 0$ since $x \neq y$. As the sets $A_1, \ldots, A_m$ form a partition of $H \setminus \{0\}$, $x - y$ belongs to one of $A_1, \ldots, A_m$, say $x - y \in A_i$. We color the edge (x, y) with the color A_i. We claim that with this coloring K_n does not have a monochrome subgraph K_{r+1}. To prove the claim, assume the contrary, that there is a monochrome K_{r+1} in K_n. Let $y_1, \ldots, y_{r+1}$ be the vertices of K_{r+1} and let all the edges of K_{r+1} be colored with the same color, say A_u. Set $x_i = y_1 - y_i$ for each i, $2 \leq i \leq r + 1$. Now $x_i = y_1 - y_i \in A_u$ for each i, $2 \leq i \leq r + 1$. As

$$\begin{aligned} x_i - x_j &= (y_1 - y_i) - (y_1 - y_j) \\ &= y_j - y_i, \end{aligned}$$

it follows that $x_i - x_j$ are distinct elements and all belong to A_u for each i, j, $2 \leq i < j \leq r + 1$. This is impossible because A_u is r-free. ∎

EXERCISE 9.3 Let H be the group of integers modulo 13. Verify that the sets

$$\begin{aligned} A_1 &= \{-2, -1, 1, 2\}, \\ A_2 &= \{-8, -4, 4, 8\}, \\ A_3 &= \{-6, -3, 3, 6\} \end{aligned}$$

form a partition of $H \setminus \{0\}$. Compute the colors of some of the edges of the graph K_{13} whose nodes are the elements of H. Figure 9.1 (on page 191) shows the edges colored by A_2. Table 9.2 (on page 191) contains the incidence matrix of K_{13}. The k in the ith row and jth columns means that the (i, j) edge is colored with A_k. ∎

Let F denote the Galois field of p^h elements, that is, $F = \mathrm{GF}(p^h)$. It is known that F is a h-dimensional vector field over $\mathrm{GF}(p)$ and the elements of F can be represented uniquely in the form

$$x_0 + x_1\beta + \cdots + x_{h-1}\beta^{h-1},$$

where $x_0, x_1, \ldots, x_{h-1}$ are integers between 0 and $p - 1$. The additive part of F is an abelian group of type $Z(p) \oplus \cdots \oplus Z(p)$. The set $F \setminus \{0\}$ is a cyclic group under multiplication. There is an $\alpha \in F$ such that

$$F \setminus \{0\} = \{\alpha^i : \ 0 \leq i \leq p^h - 2\}.$$

LEMMA 9.2

Let $n = (p^h - 1)/(2m)$ and let $Z(mn) = A + B$ be a factorization with $|A| = m$, $|B| = n$. If

$$X = \{\alpha^b, -\alpha^b : b \in B\}$$

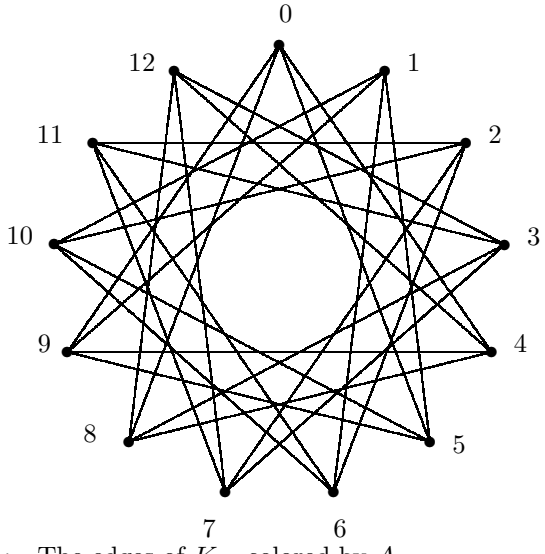

FIGURE 9.1: The edges of K_{13} colored by A_2.

TABLE 9.2: The incidence matrix of K_{13}

	0	1	2	3	4	5	6	7	8	9	10	11	12
0		1	1	3	2	2	3	3	2	2	3	1	1
1	1		1	1	3	2	2	3	3	2	2	3	1
2	1	1		1	1	3	2	2	3	3	2	2	3
3	3	1	1		1	1	3	2	2	3	3	2	2
4	2	3	1	1		1	1	3	2	2	3	3	2
5	2	2	3	1	1		1	1	3	2	2	3	3
6	3	2	2	3	1	1		1	1	3	2	2	3
7	3	3	2	2	3	1	1		1	1	3	2	2
8	2	3	3	2	2	3	1	1		1	1	3	2
9	2	2	3	3	2	2	3	1	1		1	1	3
10	3	2	2	3	3	2	2	3	1	1		1	1
11	1	3	2	2	3	3	2	2	3	1	1		1
12	1	1	3	2	2	3	3	2	2	3	1	1	

TABLE 9.3: The incidence matrix of the Keller graph K_2

	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
00	×						●			●	●	●			●	
01		×						●	●		●	●				●
02			×		●				●	●		●	●			
03				×		●			●	●	●			●		
10			●		×						●			●	●	●
11				●		×						●	●		●	●
12	●						×		●					●	●	●
13		●						×		●				●	●	●
20		●	●	●			●		×						●	
21	●		●	●				●		×						●
22	●	●		●	●						×		●			
23	●	●	●			●						×		●		
30			●			●	●	●			●		×			
31				●	●		●	●				●		×		
32	●				●	●		●	●						×	
33		●			●	●	●			●						×

is an r-free subset of $F \setminus \{0\}$, then $R_m(r+1) \geq |F| + 1$.

PROOF Set $A = \{a(1), \ldots, a(m)\}$ and $B = \{b(1), \ldots, b(n)\}$. Since $\alpha^{(p^h-1)/2} = -1$, we have

$$\begin{aligned} F \setminus \{0\} &= \bigcup_{i=0}^{p^h-2} \{\alpha^i\} \\ &= \bigcup_{i=0}^{(p^h-3)/2} \{\alpha^i, -\alpha^i\} \\ &= \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} \{\alpha^{a(i)+b(j)}, -\alpha^{a(i)+b(j)}\} \\ &= \bigcup_{i=1}^{m} \Big[\bigcup_{j=1}^{n} \{\alpha^{b(j)}, -\alpha^{b(j)}\} \Big] \alpha^{a(i)} \\ &= \bigcup_{i=1}^{m} X\alpha^{a(i)}. \end{aligned}$$

The set X is plainly symmetric. It follows that $X\alpha^{a(i)}$ is also symmetric. By the assumption of the lemma, X is r-free. It follows that $X\alpha^{a(i)}$ is also r-free for each i, $1 \leq i \leq m$. By Lemma 9.1 (on page 189), $R_m(r+1) \geq |F| + 1$. □

As an illustration we show that $42 \leq R_2(5)$.

EXAMPLE 9.1 Let us note that

$$\mathrm{GF}(41) \setminus \{0\} = \{1, \alpha, \ldots, \alpha^{39}\},$$

where $\alpha = 6$. In other words, 6 is a primitive root modulo 41:

$$\begin{array}{llll} \alpha^0 = 1, & \alpha^5 = 27, & \alpha^{10} = 32, & \alpha^{15} = 3, \\ \alpha^1 = 6, & \alpha^6 = 39, & \alpha^{11} = 28, & \alpha^{16} = 18, \\ \alpha^2 = 36, & \alpha^7 = 29, & \alpha^{12} = 4, & \alpha^{17} = 26, \\ \alpha^3 = 11, & \alpha^8 = 10, & \alpha^{13} = 24, & \alpha^{18} = 33, \\ \alpha^4 = 25, & \alpha^9 = 19, & \alpha^{14} = 21, & \alpha^{19} = 34. \end{array}$$

Setting $n = (41-1)/(2 \cdot 2) = 10$, one can verify that

$$\begin{aligned} Z(2 \cdot 10) &= \{0, 10\} + \{0, 1,\ 2, 3,\ 4, 5,\ 6, 7,\ 8, 9\} \\ &= \{0, 10\} + \{0, 1, 12, 3, 14, 5, 16, 7, 18, 9\} \\ &= A + B \end{aligned}$$

is a factorization of $Z(2 \cdot 10)$. Here $K = \{0, 10\}$ is a subgroup of $Z(2 \cdot 10)$ and $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ is a complete set of representatives modulo K. Note that $B = K \circ_\varphi D$, where the function $\varphi : D \to K$ is defined by

$$\varphi(2) = \varphi(4) = \varphi(6) = \varphi(8) = 10$$

and $\varphi(d) = 0$ otherwise. The particular choice of B is the result of checking all the possible $2^9 = 512$ choices for φ. A computer assisted inspection carried out by R. Hill and R. W. Irving [59] in 1982 shows that

$$\begin{aligned} X &= \{\alpha^b, -\alpha^b : b \in B\} \\ &= \{\alpha^b :\ b \in B\} \cup \{-\alpha^b :\ b \in B\} \\ &= \{1, 6, 4, 11, 21, 27, 18, 29, 33, 19\} \cup \{40, 35, 37, 30, 20, 14, 23, 12, 8, 22\} \end{aligned}$$

is a 4-free set. By Lemma 9.2 (on page 190), $R_2(5) \geq 42$. Verifying that X is a 4-free set by brute force simply amounts to going through all the $\binom{20}{4} = 4845$ subsets of X with 4 elements. □

9.3 Near factorizations

Let Γ be a finite undirected graph without loops and double edges. A coloring of the nodes of Γ is called a *well-coloring* or a proper coloring if each vertex of Γ is colored and if adjacent vertices never receive the same color. There is a minimal number of colors with which Γ can be well-colored. This number is called the chromatic number of Γ and is denoted by $\chi(\Gamma)$. There

is a maximum among the sizes of the cliques of Γ. This is the clique number of Γ and is denoted by $\omega(\Gamma)$.

Note that if Γ contains Δ, a clique of size k, then in a well-coloring of Γ the nodes of Δ require at least k colors and so $\omega(\Gamma) \leq \chi(\Gamma)$. If one is looking for the clique number of Γ, then any ad hoc well-coloring of Γ provides an upper bound for the chromatic number of Γ and so for the clique number of Γ. Or, conversely, if one is looking for the chromatic number of Γ, then any casually picked clique of Γ can be used to establish a lower bound for the chromatic number of Γ.

However, the gap between the quantities $\omega(\Gamma)$ and $\chi(\Gamma)$ can be arbitrarily large. In 1949 A. Zykov [174] proved that for any given integer $k \geq 1$ there is a graph Γ for which $\chi(\Gamma) > k$ and $\omega(\Gamma) = 3$. In 1959 P. Erdős [29] gave a probabilistic proof for Zykov's result and using the same technique later extended it.

In 1960 C. Berge introduced the notion of perfect graph. A graph Γ is perfect if $\omega(\Delta) = \chi(\Delta)$ holds for each induced subgraph Δ of Γ. The fundamental open problem concerning perfect graphs is the following conjecture, the so-called strong perfect graph conjecture of Berge. A graph is perfect if and only if it contains no induced subgraph isomorphic to an odd cycle of at least five vertices or the complement of such a cycle.

A graph Γ is called *partitionable* if it has $pq+1$ vertices and for each vertex v of Γ the induced subgraph $\Gamma \setminus \{v\}$ admits a partition into p cliques of size q and also admits a partition into q stable sets of size p.

L. Lovász [82] and M. W. Padberg [102] proved that every minimally imperfect graph is partitionable. Thus, for a counter-example for the strong perfect graph conjecture, one should search in the family of partitionable graphs. It turns out that one can use factorizations of finite abelian groups to construct certain partitionable graphs.

Let G be a finite abelian group and let A, B be subsets of G. If

(1) $|A| \geq 2$, $|B| \geq 2$,

(2) the sum $A + B$ is direct,

(3) $|A||B| = |G| - 1$,

then we say that $A + B$ is a *near factorization* of G. One element of G is not in the sum $A+B$, that is, $A+B$ is a factorization of $G \setminus \{g\}$ for some element g of G.

We consider the following question. Given a finite abelian group G, are there subsets A, B of G forming a near factorization of G? If there are, then plainly $|G| - 1$ cannot be a prime. On the other hand, if $|G| - 1$ is not a prime and G is a cyclic group, then G admits a near factorization. Indeed, let $|G| - 1 = uv$, where $u \geq 2$, $v \geq 2$. Let $G = \langle g \rangle = \{0, g, 2g, \ldots, uvg\}$. Set

$$A = \{0, g, 2g, \ldots, (u-1)g\},$$
$$B = \{0, ug, 2ug, \ldots, (v-1)ug\}.$$

Now the sum $A + B$ is direct and $|A| = u$, $|B| = v$, as required. Our question has to be restated. Are there subsets A, B of a non-cyclic finite abelian G forming a near factorization of G?

LEMMA 9.3

Let g be an element of the finite abelian group G and let A, B be subsets of G. If the sum $A + B$ is direct, then so is the sum $(A + g) + B$.

PROOF Suppose that the sum $A + B$ is direct. Then, by Lemma 2.2 (on page 12), $(A - A) \cap (B - B) = \{0\}$. Note that $(A - A) = (A + g) - (A + g)$. Therefore $[(A + g) - (A + g)] \cap (B - B) = \{0\}$ and so, by Lemma 2.2 (on page 12), the sum $(A + g) + B$ is direct. □

COROLLARY 9.1

If the sum $A + B$ is a near factorization of the finite abelian group G, then so is the sum $(A - g) + (B - h)$ for each $g, h \in G$. In particular, one may assume that the sum $A + B$ is normalized.

Let G be a finite abelian group and let X be a subset of G such that $0 \notin X$ and $X = -X$. We define a graph Γ. The nodes of Γ are the elements of G and two distinct nodes $g, h \in G$ are joined by an undirected edge if $g - h \in X$. We call Γ the *Cayley graph* of G relative to the set X. We intended to work with graph with undirected edges without loops and without double edges. The condition $0 \notin X$ implies $g - g \notin X$, and therefore loops cannot occur in Γ. The condition $X = -X$ ensures that if there is an edge from g to h, then there is an edge from h to g, that is, the edges of Γ are undirected.

Let A, B be subsets of G such that $A + B$ is a factorization of $G \setminus \{y\}$. Setting $X = (A - A) \setminus \{0\}$, this near factorization gives rise to a Cayley graph Γ of G relative to X. It is plain that the sets $A + b$, $b \in B$ form a partition of $G \setminus \{y\}$ and each set $A + b$, $b \in B$ spans a clique of Γ of size $|A|$. Further, the sets $a + B$, $a \in A$ form a partition of $G \setminus \{y\}$ and each set $a + B$, $a \in A$ spans an independent set in Γ of size $|B|$. Replacing the sets A, B by $A + g$, $B + h$, the uncovered element y of the near factorization $A + B$ will change to $y + g + h$. The subset $X = (A - A) \setminus \{0\}$ will not change. This means that each element of G can play the role of the uncovered element and so Γ is a partitionable graph.

EXAMPLE 9.2 Let G be $Z(13)$ and set $A = \{0, 1, 2\}$, $B = \{0, 3, 6, 9\}$. A routine computation shows that the sum $A + B$ is direct and is equal to $Z(13) \setminus \{12\}$. The Cayley graph Γ of G relative to the set $X = (A - A) \setminus \{0\} = \{1, 2, 11, 12\}$ is depicted in Figure 9.2 (on page 196). □

One can put the factorization theory to use to show that in certain cases

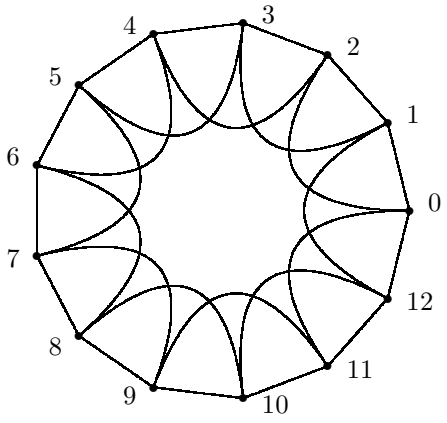

FIGURE 9.2: The Cayley graph Γ relative to X.

near factorizations do not exist.

THEOREM 9.4

The subsets A, B of a finite abelian group G cannot form a near factorization of G if G is not cyclic and $\min\big(|A|, |B|\big) \leq 3$.

PROOF Let G be a finite abelian group and let A, B be subsets of G such that the sum $A + B$ is a near factorization of G. We may assume that $2 \leq |A| \leq |B|$ since this is only a matter of swapping A and B. By Lemma 9.3 (on page 195), we may assume that $A + B = G \setminus \{0\}$ and $0 \in A$. Set $H = \langle A \rangle$. We claim that $H = G$. In order to prove the claim, assume on the contrary that $H \neq G$. There is an element $g \in G \setminus \{0\}$ such that the sets $A + b$, $b \in B \cap (g + H)$, form a partition of the coset $g + H$. It follows that $|A|$ divides $|H|$ and so $|A|$ divides $|G|$. Then $|A||B| = |G| - 1$ implies the contradiction that $|A|$ divides 1.

In the $|A| = 2$ case, A can be put to the $A = \{0, a\}$ form. As $\langle A \rangle = G$, it follows that G is cyclic.

Let us turn to the $|A| = 3$ case. We may assume that A and B are normalized subsets. Set $A = \{0, a, b\}$. There is an element d of G such that $b = 2a + d$. Thus $A = \{0, a, 2a + d\}$. The equation $G = (A + B) \cup \{g\}$ means that the sets

$$B,\ a + B,\ 2a + d + B,\ \{g\}$$

form a partition of G. Adding a to the equation $G = (A + B) \cup \{g\}$ yields that $G = G + a = [(A + a) + B] \cup \{g + a\}$. This means that the sets

$$a + B,\ 2a + B,\ 3a + d + B,\ \{g + a\}$$

form a partition of G. Comparing the two partitions we get

$$B \cup (2a + d + B) \cup \{g\} = (2a + B) \cup (3a + d + B) \cup \{g + a\}.$$

Note that $(2a + d + B) \cap (3a + d + B) = \emptyset$ since $B \cap (a + B) = \emptyset$. Thus

$$2a + d + B \subseteq (2a + B) \cup \{g + a\}, \tag{9.1}$$

$$B \subseteq (3a + d + B) \cup \{g + a\}. \tag{9.2}$$

By (9.1), d is a weak period of B. Consequently, $-d$ is also a weak period of B.

If $g + a \notin 2a + d + b$, then, by (9.1), $2a + d + B = 2a + B$ and so $d + B = B$. Then, by (9.2), $3a$ is a weak period of B.

If $g+a \notin B$, then, by (9.2), $B = 3a+d+B$ or, equivalently, $-d+B = 3a+B$. But $-d + B$ and B differ mutually in at most one element. Therefore $3a + B$ and B differ mutually in at most one element. Thus $3a$ is a weak period of B.

The summary of our analysis is that B is weakly periodic and $3a$ is a weak period of B.

By the proof of Lemma 6.1 (on page 122), B is in one of the following forms:

$$\langle 3a \rangle + C, \tag{9.3}$$

$$\{0, 3a, 6a, \ldots, (r-1)3a\}, \tag{9.4}$$

$$[\langle 3a \rangle + C] \cup [h + \{0, 3a, 6a, \ldots, (r-1)3a\}], \tag{9.5}$$

where C is a normalized subset of G, $h \in G$ and r is an integer $0 \leq r \leq |3a|-1$.

The equation $|G| - 1 = |A||B| = 3|B|$ shows that $|G|$ is relatively prime to 3. Consequently, $\langle 3a \rangle = \langle a \rangle$. If B is in form (9.3) or (9.5), then $a \in B$. Now $a \in A$, $a \in B$ contradict the fact that the sum $A + B$ is direct. Thus B is in the form (9.4). As $\langle B \rangle = G$, it follows that G is cyclic.

This completes the proof. ∎

We usually represent the elements of $Z(n)$ by $0, 1, \ldots, n-1$ and the group operation is the addition of integers modulo n. The near factorization $Z(n + 1) \setminus \{g\} = A + B$ is called a *Krasner near factorization* if $0 \leq a + b \leq n$ for each $a \in A$, $b \in B$. We call this near factorization a CGPW near factorization if $g = n$. V. Chvatal, R. L. Graham, A. F. Perold, and S. H. Whitesides [18] used it in connection with perfect graphs.

It is easy to find CGPW near factorizations. Let

$$A = \{0, 1, \ldots, a-1\} = [1, a],$$
$$B = \{0, a, \ldots, (b-1)a\} = [a, b]$$

and $n = ab$. (Here we use the bracket notation for cyclic subsets.) Then $Z(n + 1) \setminus \{n\} = A + B$ is a near factorization. From a given CGPW near factorization one can construct a new CGPW near factorization. Let $Z(n_1 +$

$1) \setminus \{n_1\} = A_1 + B_1$ be a CGPW near factorization and let $k \geq 2$ be an integer. Set $A_2 = A_1 + [n_1, k]$, $B_2 = B_1 + [n_1, k]$, $n_2 = n_1 k$.

LEMMA 9.4
$Z(n_2+1) \setminus \{n_2\} = A_2 + B_1$ and $Z(n_2+1) \setminus \{n_2\} = A_1 + B_2$ are CGPW near factorizations.

PROOF The computation

$$\begin{aligned} A_2 + B_1 &= (A_1 + [n_1, k]) + B_1 \\ &= A_1 + B_1 + [n_1, k] \\ &= (A_1 + B_1) + [n_1, k] \\ &= [1, n_1] + [n_1, k] \\ &= [1, n_1 k] \\ &= [1, n_2] \\ &= Z(n_2 + 1) \setminus \{n_2\} \end{aligned}$$

shows that $Z(n_2 + 1) \setminus \{n_2\} = A_2 + B_1$ is a Krasner near factorization. A similar computation shows that $Z(n_2+1) \setminus \{n_2\} = A_1 + B_2$ is a Krasner near factorization. □

LEMMA 9.5
Each CGPW near factorization is constructed from a near factorization $[1, a] + [a, b]$ using the construction described above.

PROOF Let us note that the CGPW near factorization $Z(n+1) \setminus \{n\} = A + B$ is identical to the Krasner factorization $Z(n) = A + B$. By Lemma 4.2 (on page 87), there exists an integer $a > 1$ such that $[1, a]$ is a direct summand of A or B, say A, and each element of B is a multiple of a. □

Of course, in a typical Krasner near factorization $Z(n + 1) \setminus \{g\} = A + B$, the element g need not to be zero.

EXAMPLE 9.3 Let $A = \{0, 1, 2\}$, $B = \{1, 4, 7\}$. Now $Z(10) \setminus \{3\} = A + B$ is a Krasner near factorization but not a CGPW near factorization. □

PROBLEM 9.1 Are there non-cyclic finite abelian groups admitting near factorizations? □

PROBLEM 9.2 Describe all Krasner near factorizations of $Z(n + 1)$. □

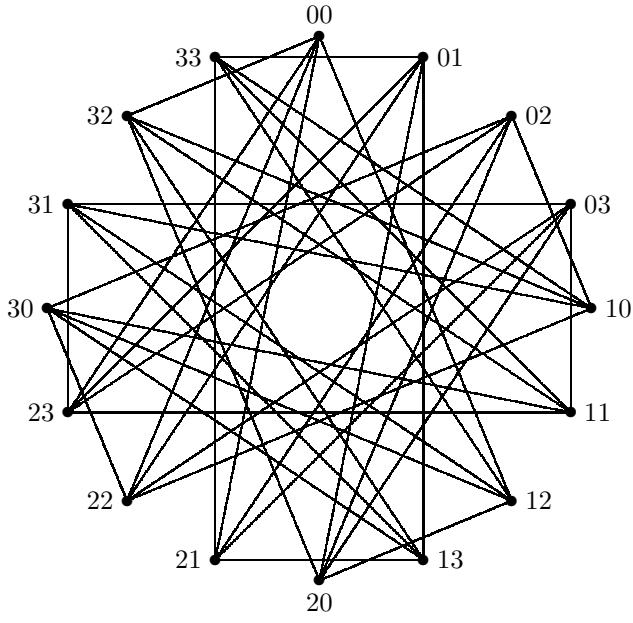

FIGURE 9.3: The Keller graph K_2.

9.4 A family of random graphs

The Keller graph K_n is defined in the following way. The nodes of K_n are

$$\big\{(a_1, \ldots, a_n) : a_i \in \{0, 1, 2, 3\}\big\}.$$

Two distinct vertices $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are connected if there is an i such that $b_i - a_i \equiv 2 \pmod 4$ and further there is a j for which $b_j - a_j \not\equiv 0 \pmod 4$ and $i \neq j$. The incidence matrix of the Keller graph K_2 is given in Table 9.3 (on page 192) and the graph itself is given by Figure 9.3 (on page 199).

The maximal clique problem of a graph is NP hard. However, the theory does not give any hint on which instances of graphs the problem is intractable. An empirical investigation of J. Marconi and J. A. Foster [86] indicates that finding a maximal clique in Keller graphs is an example of a family of problems that are inherently difficult for genetic algorithms. Therefore, Keller graphs can be used for testing maximal clique algorithms. To provide a larger battery of tests, we suggest a family of random graphs for testing maximal clique algorithms that shares many characteristics of the Keller graphs.

Let G be a finite abelian group; let A, B be subsets of G; and let $\varphi : B \to A$ be a function. We define $A \circ_\varphi B$, the composition of the subsets A and B, to

be $\{\varphi(b) + b : b \in B\}$. As an example let

$$A = \{a_1, a_2, a_3\}, \quad B = \{b_1, b_2, b_3, b_4\}$$

and let φ be defined by

$$\varphi(b_1) = a_1, \quad \varphi(b_2) = a_1, \quad \varphi(b_3) = a_3, \quad \varphi(b_4) = a_2.$$

Then $A \circ_\varphi B = \{a_1 + b_1, a_1 + b_2, a_3 + b_3, a_2 + b_4\}$. In our application, φ will be picked randomly so that each φ has the same probability, $1/(|A|^{|B|})$.

Let G be a finite abelian group and let

$$\{0\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

be an ascending chain of subgroups of G. Let $D_1, \ldots, D_{n-1}$ be subsets of G such that D_i is a complete set of representatives for H_{i+1} modulo H_i. (For the sake of a uniform notation, we introduce $D_0 = H_1$.) Then use the following recursion:

$$\begin{array}{ll} U_{n-1} = D_{n-1}, & V_{n-1} = \{0\}, \\ U_{n-2} = D_{n-2} + V_{n-1}, & V_{n-2} = D_{n-2} \circ U_{n-1}, \\ \quad \vdots & \quad \vdots \\ U_1 \quad = D_1 + V_2, & V_1 \quad = D_1 \circ U_2, \\ U_0 \quad = H_1 + V_1, & V_0 \quad = D_0 \circ U_1. \end{array}$$

Set $A = V_0$, $B = U_0$. The functions

$$\varphi_{n-1} : U_{n-1} \to D_{n-2}, \ldots, \varphi_1 : U_{n-1} \to D_0$$

are chosen randomly and are suppressed in the formulae above. Then, by Theorem 4.8 (on page 77), $G = A + B$ is a factorization. We discard B and ask if A has a complementer factor. Finding a complementer factor to A can be reduced to finding a clique of size $|B|$ in a graph Γ. The nodes of Γ are the elements of G, and two distinct nodes $g, h \in G$ are joined with an edge if $g - h \notin (A - A)$. Finding a chain of subgroups is easy. The construction works equally well with each choice of the system of representatives $D_1, \ldots, D_{n-1}$, so the most obvious choice is suitable.

EXAMPLE 9.4 Let G be a cyclic group of order 81. Let $n = 4$ and

$$\begin{array}{ll} H_0 = \langle 0 \rangle & = \{0\}, \\ H_1 = \langle 27 \rangle & = \{0, 27, 54\}, \\ H_2 = \langle 9 \rangle & = \{0, 9, 18, \ldots, 72\}, \\ H_3 = \langle 3 \rangle & = \{0, 3, 6, \ldots, 78\}, \\ H_4 = \langle 1 \rangle & = \{0, 1, 2, \ldots, 80\}. \end{array}$$

An obvious choice for $D_0, \ldots, D_3$ is

$$\begin{array}{l} D_0 = \{0, 27, 54\}, \\ D_1 = \{0, 9, 18\}, \\ D_2 = \{0, 3, 6\}, \\ D_3 = \{0, 1, 2\}. \end{array}$$

One can go on to compute an $A = V_0$. Then $A - A$ and construct a graph with 81 nodes and maximal cliques of size 9. □

Of course many of the factorization constructions we presented in Section 2.4 can be used for constructing families of random graphs.

When $|G|$ is large in the construction above, then so is $|A - A|$. Therefore, checking $b - a \in (A - A)$ can use up a considerable portion of the available resources. To overcome this problem we should settle for a moderate size $|G|$, and then form an s-fold direct sum $G_1 = G \oplus \cdots \oplus G$. Now $G = A_1 + B_1$ is a factorization of G_1, where A_1 is a direct sum of isomorphic copies of A and B_1 is a direct sum of isomorphic copies of B. As usual, we discard B_1 and ask if A_1 has a complementer factor. In the complementer factor graph two elements $(a_1, \ldots, a_s)$ and $(b_1, \ldots, b_s)$ of G_1 are connected by an edge if there is an i for which $b_i - a_i \notin (A - A)$. We may introduce the extra requirement that there is a j such that $b_j - a_j \neq 0$ and $i \neq j$ if we want to avoid recovering the original complementer factor B_1.

As a result we get a graph of size $|G|^s$ instead of $|G|$ and the work of checking incidence of vertices increases only s-fold. This last graph is a direct generalization of the Keller graph.

9.5 Complex Hadamard matrices

Let H be an n by n matrix whose entries are complex mth roots of unity. If $HH^* = nI$, then we say that H is a *complex Hadamard matrix*. Here I is the n by n identity matrix and H^* is the Hermite transpose of H. In the $m = 2$ particular case, the entries of H are $+1$ or -1 and we get back the Hadamard matrices in the ordinary sense. Ordinary Hadamard matrices have important applications in combinatorics. For instance, they can be used to construct error correcting codes and certain block designs. For more details consult [2].

The columns of a complex Hadamard matrix can be considered as a finite set of orthogonal functions defined on a finite set. Let G be a finite abelian group with elements $g_1, \ldots, g_n$ and let $\chi_1, \ldots, \chi_n$ be the characters of G. By the standard orthogonality relations, the columns of the matrix

$$\begin{bmatrix} \chi_1(g_1) & \cdots & \chi_1(g_n) \\ \vdots & \ddots & \vdots \\ \chi_n(g_1) & \cdots & \chi_n(g_n) \end{bmatrix}$$

are orthogonal and the rows of the matrix are orthogonal. In other words, the character table of a finite abelian group forms a set of orthogonal functions. In Fourier analysis, these orthogonal functions are called *Vilenkin systems*.

The character table of a subgroup of G is clearly a Vilenkin system too. Restricting the characters of G to a subset of G in a typical case does not lead to an orthogonal system. As it turns out, complex Hadamard matrices are related to certain multiple factorizations of finite abelian groups. Exploiting this connection, we will be able to construct complex Hadamard matrices. We will see that there is a large collection of subsets of G such that restricting the characters of G to these subsets does yield an orthogonal system of functions.

Let G be a finite abelian group and let $A_1, \ldots, A_n$ be subsets of G. If each element g of G can be expressed in the form

$$g = a_1 + \cdots + a_n, \quad a_1 \in A_1, \ldots, a_n \in A_n$$

in exactly k ways, then we say that the sum $A_1 + \cdots + A_n$ is a k-fold factorization of G. We speak about *multiple factorizations* of G when we do not wish to refer to the value of k.

Using the ideas of Section 3.2, it can be checked that the sum $A_1 + \cdots + A_n$ forms a multiple factorization of G if and only if $\chi(A_1 + \cdots + A_n) = \chi(A_1) \cdots \chi(A_n) = 0$ for each non-principal character χ of G.

Let the group G be a group of type $Z(q_1) \oplus \cdots \oplus Z(q_n)$, where $q_i = u(i)v(i)$, $u(i), v(i) \geq 2$ for each i, $1 \leq i \leq n$. Let $x_1, \ldots, x_n$ be basis elements of G. Let ρ be a root of unity whose order is the least common multiple of $q_1, \ldots, q_n$. For each i, $1 \leq i \leq n$, there is a positive integer $w(i)$ such that the order of $\rho^{w(i)}$ is equal to q_i. Each character χ of G can be represented in the form

$$\chi(x_1) = \rho^{w(1)\nu(1)}, \ldots, \chi(x_n) = \rho^{w(n)\nu(n)}, \tag{9.6}$$

where

$$0 \leq \nu(1) \leq q_1 - 1, \ldots, 0 \leq \nu(n) \leq q_n - 1.$$

For the sake of clarity we single out two special cases. When $q_1 = \cdots = q_n = q$, then G is a homocyclic abelian group. In this case, the least common multiple of $q_1, \ldots, q_n$ is q and the $w(1), \ldots, w(n)$ numbers are all equal to one. When $q_1, \ldots, q_n$ are pair-wise relatively primes, then G is a cyclic group. Now the least common multiple of $q_1, \ldots, q_n$ is the product $q_1 \cdots q_n$ and $w(i) = (q_1 \cdots q_n)/q_i$ for each i, $1 \leq i \leq n$.

Set $C_i = \{0, x_i, 2x_i, \ldots, (u(i) - 1)x_i\}$. Suppose that $A + C_1 + \cdots + C_n$ is a multiple factorization of G. Let $a_1, \ldots, a_\alpha$ be the elements of A. Each a_i can be written uniquely in the form

$$a_i = \lambda(i, 1)x_1 + \cdots + \lambda(i, n)x_n,$$

where

$$0 \leq \lambda(i, 1) \leq q_1 - 1, \ldots, 0 \leq \lambda(i, n) \leq q_n - 1.$$

For the sake of brevity we introduce the notation

$$s(i) = [\lambda(i, 1), \ldots, \lambda(i, n)].$$

Pick a non-principal character χ of G defined by (9.6). Let $d = [\nu(1), \ldots, \nu(n)]$.

LEMMA 9.6
Suppose that

$$\chi(C_1) \neq 0, \ldots, \chi(C_n) \neq 0. \tag{9.7}$$

Then

$$0 = \rho^{\langle d, s(1)\rangle} + \cdots + \rho^{\langle d, s(\alpha)\rangle}. \tag{9.8}$$

(Here $\langle d, s(i)\rangle$ stands for the weighted scalar product

$$w(1)\nu(1)\lambda(i,1) + \cdots + w(n)\nu(n)\lambda(i,n)$$

and not for the span of a subset as usual.)

PROOF Let us watch the multiple factorization $A+C_1+\cdots+C_n = A+B$ of G. As χ is a non-principal character of G, by the result we quoted, it follows that $0 = \chi(A)\chi(C_1)\cdots\chi(C_n)$. Using (9.7) we get that $\chi(A) = 0$. Therefore

$$\begin{aligned} 0 &= \chi(A) \\ &= \sum_{i=1}^{\alpha} \chi(a_i) \\ &= \sum_{i=1}^{\alpha} \rho^{w(1)\nu(1)\lambda(i,1)} \cdots \rho^{w(n)\nu(n)\lambda(i,n)} \\ &= \sum_{i=1}^{\alpha} \rho^{w(1)\nu(1)\lambda(i,1)+\cdots+w(n)\nu(n)\lambda(i,n)} \\ &= \sum_{i=1}^{\alpha} \rho^{\langle d, s(i)\rangle}, \end{aligned}$$

as required. ∎

Using equation (9.8), we can construct complex Hadamard matrices. Let us start with a multiple factorization $A+C_1+\cdots+C_n = A+B$ of G. Suppose that $|A| \leq |B|$. Choose a subset B_1 of B such that $|B_1| = |A|$. Let $b_1, \ldots, b_\alpha$ be the elements of B_1 and write the element b_j in the form

$$b_j = \mu(j,1)x_1 + \cdots + \mu(j,n)x_n.$$

Set

$$t(j) = [\mu(j,1), \ldots, \mu(j,n)].$$

Finally, let $h_{i,j} = \rho^{\langle t(i), s(j)\rangle}$ and

$$H = \begin{bmatrix} h_{1,1} & \ldots & h_{1,\alpha} \\ \vdots & \ddots & \vdots \\ h_{\alpha,1} & \ldots & h_{\alpha,\alpha} \end{bmatrix}.$$

TABLE 9.4: The values of $s(i), t(i)$

i	$s(i)$	$t(i)$
1	$(0,0,0)$	$(0,0,0)$
2	$(1,0,2)$	$(0,0,1)$
3	$(0,2,1)$	$(0,1,0)$
4	$(0,2,3)$	$(0,1,1)$
5	$(2,1,0)$	$(1,0,0)$
6	$(3,0,2)$	$(1,0,1)$
7	$(2,3,0)$	$(1,1,0)$
8	$(2,2,2)$	$(1,1,1)$

LEMMA 9.7
The H defined above is a complex Hadamard matrix.

PROOF Multiplying the ith row of H by the jth column of H^* gives that

$$\sum_{k=1}^{\alpha} \rho^{\langle t(i),s(k)\rangle - \langle t(j),s(k)\rangle} = \sum_{k=1}^{\alpha} \rho^{\langle t(i)-t(j),s(k)\rangle}.$$

If $i = j$, then this sum is equal to α, as required. It remains to show that it is zero if $i \neq j$. If (9.7) holds, then Lemma 9.6 (on page 203) is applicable with the $d = t(i) - t(j)$ choice. Note that $\chi(C_k) = 0$ if and only if $\chi(x_k) \neq 1$ and $\chi(u(k)x_k) = 1$. We assume that $\chi(u(k)x_k) = 1$, and we show that in this case $\chi(x_k) = 1$ holds. $\chi(u(k)x_k) = 1$ means that $\rho^{u(k)w(k)[\mu(i,k)-\mu(j,k)]} = 1$. This in turns means that

$$u(k)[\mu(i,k) - \mu(j,k)] \equiv 0 \pmod{u(k)v(k)}.$$

Hence

$$\mu(i,k) - \mu(j,k) \equiv 0 \pmod{v(k)}.$$

The kth component of $t(i)$ is running from 0 to $v(k) - 1$, and so it follows that $\mu(i,k) = \mu(j,k)$. Using this we get that $\chi(x_k) = 1$. This completes the proof. □

In order to illustrate the procedure of constructing complex Hadamard matrices, we work out a toy example.

EXAMPLE 9.5 Let the group G be a group of type $Z(4) \oplus Z(4) \oplus Z(4)$ and let x_1, x_2, x_3 be a basis of G. Let $C_i = \{0, x_i\}$ and let $B = C_1 + C_2 + C_3$. Choosing A to be

$$\{0, x_1 + 2x_3, 2x_2 + x_3, 2x_2 + 3x_3, 2x_1 + x_2, 3x_1 + 2x_3,$$
$$2x_1 + 3x_2, 2x_1 + 2x_2 + 2x_3\},$$

the reader can verify that the sum $A+C_1+C_2+C_3$ is a multiple factorization of G. In fact it is a 1-fold factorization of G. The values of $s(i)$ and $t(j)$ are listed in Table 9.4 (on page 204). Let ρ be a 4th primitive root of unity. Computing the scalar products $\langle s(i), t(i)\rangle$, we get the following 8 by 8 complex Hadamard matrix:

$$H = \begin{bmatrix} \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 & \rho^0 \\ \rho^0 & \rho^2 & \rho^1 & \rho^3 & \rho^0 & \rho^2 & \rho^0 & \rho^2 \\ \rho^0 & \rho^0 & \rho^2 & \rho^2 & \rho^1 & \rho^0 & \rho^3 & \rho^2 \\ \rho^0 & \rho^2 & \rho^3 & \rho^1 & \rho^1 & \rho^2 & \rho^3 & \rho^0 \\ \rho^0 & \rho^1 & \rho^0 & \rho^0 & \rho^2 & \rho^3 & \rho^2 & \rho^2 \\ \rho^0 & \rho^3 & \rho^1 & \rho^3 & \rho^2 & \rho^1 & \rho^2 & \rho^0 \\ \rho^0 & \rho^1 & \rho^2 & \rho^2 & \rho^3 & \rho^3 & \rho^1 & \rho^0 \\ \rho^0 & \rho^3 & \rho^3 & \rho^1 & \rho^3 & \rho^1 & \rho^1 & \rho^2 \end{bmatrix}.$$

□

Plainly there is another way to arrive at the matrix H in Example 9.5 (on page 204). First, write up the 64 by 64 character table of G. Then, restrict the characters of G to the set A. Finally, cancel the rows of the character table that do not correspond to elements of A. In short, we can get H by restricting the character table of G to the subset A. We claim that H is not a character table of any finite abelian group. In other words, H is not a Vilenkin system. In order to verify the claim, let G_1 be an abelian group of order 8. We know that G_1 must be isomorphic to one of the groups $Z(8)$, $Z(4)\oplus Z(2)$, $Z(2)\oplus Z(2)\oplus Z(2)$.

Suppose first that the columns of H are the values of the characters of G_1 taken on the elements of G_1. The elements of the first column of H are the values of the characters of G_1 on the zero element 0. The elements of the last column of H are the values of the characters of G_1 on a second order element of G_1 and we get that G_1 cannot have more elements of order two. Consequently, G_1 is a cyclic group of order 8. But in H each complex number has multiplicative order at most four.

Next suppose that the rows of H are the values of the characters of G_1 on the elements of G_1. Since G_1 must have an element of order two, H must contain two rows in which the entries are $+1$ or -1. (One corresponds to the zero element of G_1 and one corresponds to a second order element of G_1.) But H does not have two such rows. Therefore H is not a Vilenkin system.

Chapter 10

Codes

10.1 Variable length codes

If A is a non-empty finite alphabet, then A^* stands for the set of all the possible finite words which can be formed using letters from A. With the operation of the concatenation of words A^* is a free semi-group generated by the elements of A. The neutral element is the empty word. A non-empty subset C of A^* is called a *code* if for each $c_1, \ldots, c_u, d_1, \ldots, d_v \in C$ from

$$c_1 \cdots c_u = d_1 \cdots d_v$$

it follows that $u = v$, then $c_1 \cdots c_u = d_1 \cdots d_u$ implies that $c_1 = d_1, \ldots, c_u = d_u$. For further details on variables codes the reader is advised to consult the classical monograph of J. Berstel and D. Perrin [4]. For a crash course on variable length codes we suggest the survey paper of V. Bruyère and M. Latteux [14].

In order not to be in short supply of examples of codes, we describe a way to construct codes over a binary alphabet $\{x, y\}$. Once a code C is constructed by deleting elements from C we get new codes. There are various ways to construct codes; we choose one related to factorizations. Let $B = \{b(1), \ldots, b(s)\}$ be a set of integers. Suppose $A_1, \ldots, A_s$ are subsets of integers such that the sum $A_i + B$ is direct for each i, $1 \leq i \leq s$. This simply means that

$$a + b = a' + b', \quad a, a' \in A_i, \quad b, b' \in B$$

imply that $a = a'$, $b = b'$. Set

$$C_i = \{x^{b(i)} y x^a : \ a \in A_i\}, \quad 1 \leq i \leq s.$$

LEMMA 10.1
The set $C = C_1 \cup \cdots \cup C_s$ is a code over the binary alphabet $\{x, y\}$.

PROOF It is enough to verify that, given a word w that is a product of elements of C, we are able to decompose w into a product of elements of C without any ambiguity.

If the letter y does not appear in w, then w cannot be a product of elements of C. If y appears in w once, then w must be a single code word in C. By counting we can find the number of x's in front of y in w. Let this number be β. If β is equal to one of $b(1), \ldots, b(s)$, say $\beta = b(i)$, then w must belong to C_i. By scanning w we can find the number of x's following y. Let this number be α. If $\alpha \in A_i$, then w must be the code word $x^{b(i)}yx^{\alpha}$ in C.

Consider next the case when y appears in w at least twice. We can find the number of x's in front of the first y and the number of x's between the first and second y's. Let these numbers be β and α, respectively. There is a $b(i)$ such that $\beta = b(i)$; otherwise w cannot be a product of elements of C. Then α can be represented in the form

$$\alpha = a + b, \quad a \in A_i, \quad b \in B;$$

otherwise w is not a product of elements of C. We can chop off the code word $x^{b(i)}yx^{a}$ from the front of w and repeat the procedure with a shorter word. □

EXAMPLE 10.1 In case of the code exhibited in Table 10.2 (on page 212)

$$\begin{aligned} B &= \{0, 3, 8, 11\}, \\ A_1 &= \{0, 1, 7, 13, 14\}, \\ A_2 &= \{0, 2, 4, 6\}, \\ A_3 &= \{0, 2, 4, 6\}, \\ A_4 &= \{0, 1, 2\}. \end{aligned}$$

The reader is invited to verify that the sum $A_i + B$ is direct for each i, $1 \leq i \leq 4$. □

In the construction above, direct sums of subsets of the set of integers were used. Next we use direct sums of subsets of a finite cyclic group. Choose a positive integer n. Let $B = \{b(1), \ldots, b(s)\}$ be a subset of $Z(n)$. Here we think of $Z(n)$ as the set of elements $0, 1, \ldots, n-1$ with the operation of addition modulo n. Suppose that $A_1, \ldots, A_s$ are subsets of $Z(n)$ such that the sum $A_i + B$ is direct in $Z(n)$ for each i, $1 \leq i \leq s$. Set

$$C_i = \{x^{b(i)}yx^{a} : \ a \in A_i\}, \quad 1 \leq i \leq s.$$

LEMMA 10.2
The set $C = \{x^n\} \cup C_1 \cup \cdots \cup C_s$ is a code over the alphabet $\{x, y\}$.

PROOF The proof parallels the proof of Lemma 10.1 (on page 207). The only difference is that when we count the number of appearances of x's we should do so modulo n. □

We say that a code C over the alphabet A is *maximal* if for each code C' over A from $C \subseteq C'$ it follows that $C = C'$. Every code C over A is contained

by a maximal code C' over A. A code C is called *complete* if each word of A^* is a factor of some word of C^*. Any complete code C' that contains C is called a *completion* of C. If C is a finite code and it has a finite completion, then C is finitely completable. We would like to point out that the notions of maximal and of complete code are in general not equivalent. For finite codes, however, it is true that a code is maximal if and only if it is complete. We will restrict our attention exclusively to finite codes.

In 1989, A. Restivo, S. Salemi, and T. Sportelli [109] found a remarkable necessary condition for a code being finitely completable in terms of factorizations of finite cyclic groups.

THEOREM 10.1

Let C be a finitely completable code over the binary alphabet $\{x, y\}$ such that $y \in C$. Define the sets

$$R = \{r : \ x^r y^i \in C, \quad i \geq 1\},$$
$$S = \{s : \ y^i x^s \in C, \quad i \geq 1\}.$$

If C' is a finite completion of C, then there is a positive integer n with $x^n \in C'$. In addition, there are $A, B \subseteq Z(n)$ such that $R \subseteq A$, $S \subseteq B$ and $Z(n) = A+B$ is a factorization.

By means of Theorem 10.1 (on page 209) it is possible to exhibit finite codes which cannot be embedded into a finite maximal code. In fact, almost all known non-completable codes are constructed in this way.

THEOREM 10.2

Let

$$C = \{x^n\} \cup \{x^r y, \ yx^s : \quad r \in R, \ s \in S\}$$

be a finite code over the alphabet $\{x, y\}$ with $y \in C$. If n is a prime and $|R| \geq 2$, $|S| \geq 2$, then C cannot have a finite completion.

PROOF Assume the contrary, that C has a finite completion C'. From $x^n \in C$ it follows that $x^n \in C'$. By Theorem 10.1 (on page 209), there are $A, B \subseteq Z(n)$ such that $R \subseteq A$, $S \subseteq B$ and $Z(n) = A + B$ is a factorization. From this it follows that $n = |Z(n)| = |A||B|$. This is obviously impossible. □

The next result illustrates that the Rédei property can be used to construct finite codes over a binary alphabet without the possibility of a finite completion. Let us consider the following list of integers:

$$p^\alpha q^\beta r, \quad p^\alpha qrs, \quad pqrst, \tag{10.1}$$

where p, q, r, s, t are distinct primes and α, β are positive integers.

THEOREM 10.3
Let n be a positive divisor of one of the numbers on the list (10.1). Let

$$C = \{x^n\} \cup \{x^r y,\ yx^s :\quad r \in R,\ s \in S\}$$

be a finite code over the alphabet $\{x, y\}$. If $0 \in R \cap S$, R contains relatively prime integers, and similarly S contains relatively prime integers, then C has no finite completion.

PROOF Suppose C has a finite completion C'. Note that $x^n \in C$ and $y \in C$ as $0 \in R \cap S$. By Theorem 10.2 (on page 209), there are $A, B \subseteq Z(n)$ such that $R \subseteq A$, $S \subseteq B$ and $Z(n) = A + B$ is a factorization. Let $u, v \in R$ such that $0 \le u, v \le n-1$ and u, v are relatively prime. There are integers r, s for which $ur + vs = 1$. Then $ur + vs \equiv 1 \pmod{n}$. This means $\langle A \rangle = Z(n)$. Similarly, $\langle B \rangle = Z(n)$. On the other hand, by Corollary 5.1 (on page 103), $Z(n)$ possesses the Rédei property and consequently either $\langle A \rangle \ne Z(n)$ or $\langle B \rangle \ne Z(n)$. This contradiction completes the proof. □

A. Restivo, S. Salemi, and T. Sportelli have advanced the following conjecture.

CONJECTURE 10.1 Let k, n, p be positive integers such that $p, k < n$, and p is a prime, $p \nmid k$. Let A, B be subsets of $Z(n)$, where $0, 1 \in A$ and $0, p, k \in B$. Then $Z(n) = A + B$ cannot be a factorization. □

In 2007, A. D. Sands [131] showed that the conjecture is incorrect.

EXAMPLE 10.2 To exhibit a counter-example, let us start with the normalized factorization $G = A + B$ described in Example 5.3 (on page 98). Here G is a cyclic group of order 900, $|A| = |B| = 30$, and the elements of A, B are listed in Table 5.2 (on page 99). Note that $361 \in A$. Since 361 is relatively prime to 900, the congruence $361l \equiv 1 \pmod{900}$ is solvable. One can check that $l = 541$ is a solution. As $l = 541$ is relatively prime to $|A| = 30$, in the factorization $G = A + B$ the factor A can be replaced by lA to get the normalized factorization $G = lA + B$. Next we consider the elements $b = 45$, $c = 96$ of B. In the factorization $G = lA + B$, the factor B can be replaced by $B - b$ to get the normalized factorization $G = lA + (B - b)$. Here $c - b = 51 = 3 \cdot 17$ is an element of $B - b$. As 17 is relatively prime to 900, the congruence $17m \equiv 1 \pmod{900}$ is solvable. It can be verified that $m = 53$ is a solution. Since $m = 53$ is relatively prime to $|B - b| = 30$, in the factorization $G = lA + (B - b)$ the factor $B - b$ can be replaced by $m(B - b)$ to get the normalized factorization $G = lA + m(B - b)$. Setting $A_1 = lA$, $B_1 = m(B - b)$ leads to the normalized factorization $G = A_1 + B_1$. The elements of A_1, B_1 are listed in Table 10.1 (on page 211). One can see that

TABLE 10.1: The factors A_1 and B_1

		A_1		
0	576	252	828	504
100	676	352	28	604
200	776	452	128	704
225	801	477	153	729
325	1	577	253	829
425	101	677	353	29
		B_1		
315	855	495	135	0
65	705	345	885	525
15	555	195	735	375
665	405	45	585	450
723	363	3	543	183
365	105	645	285	825

$0, 1 \in A_1$, $0, 3, 65 \in B_1$. We choose the prime p to be 3 and we choose k to be 65. Here $p \nmid k$ and consequently the factorization is a counter-example to Conjecture 10.1 (on page 210). ∎

The next theorem is motivated by Conjecture 10.1 (on page 210).

THEOREM 10.4

Let k, n, p be positive integers such that $p, k < n$, p is a prime, and $p \nmid k$. Let A, B be subsets of Z_n with $0, 1 \in A$, $0, p, k \in B$. If $Z(n) = A + B$ is a factorization, then there are primes $p_1, \ldots, p_6$ such that p_1, p_2, p_3 are distinct; p_4, p_5, p_6 are distinct; and $(p_1 \cdots p_6) \mid n$.

Note that in a counter-example to Conjecture 10.1 (on page 210), n must be at least $(2 \cdot 3 \cdot 5)^2 = 900$.

PROOF Consider the factorization $Z(n) = A + B$. The assumptions of the theorem give that $\langle A \rangle = \langle B \rangle = Z(n)$. If $|A|$ has at most two distinct prime divisors, then, by Theorem 5.5 (on page 101), either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. This is not the case and so $|A|$ must have at least three distinct prime divisors. A similar argument gives that $|B|$ must have at least three distinct prime divisors. ∎

In 1985, to refute the triangle conjecture, P. W. Shor [138] constructed the code listed in Table 10.2 (on page 212).

It is undecided if Shor's code has a finite completion. Suppose that Shor's code has a finite completion, say C'. It is known that there is a positive

TABLE 10.2: Shor's code

y	x^3y	x^8y	$x^{11}y$
yx	x^3yx^2	x^8yx^2	$x^{11}yx$
yx^7	x^3yx^4	x^8yx^4	$x^{11}yx^2$
yx^{13}	x^3yx^6	x^8yx^6	
yx^{14}			

integer n such that $x^n \in C'$.

THEOREM 10.5

Suppose that C' is a finite completion of Shor's code and $x^n \in C'$. Then there are distinct primes p_1, p_2, p_3 such that $(330p_1p_2p_3) \mid n$.

Note that in particular $n \geq 9900$.

PROOF The sets R and S associated with Shor's code are

$$R = \{0, 3, 8, 11\}, \quad S = \{0, 1, 7, 13, 14\}.$$

Note that y is a code word in Shor's code and so $y \in C'$. By Theorem 10.1 (on page 209), there is an integer n and subsets A, B of $Z(n)$ such that $R \subseteq A$, $S \subseteq B$ and $Z(n) = A + B$ is a factorization.

If $2 \nmid |B|$, then, by Theorem 3.17 (on page 58), in the factorization $Z(n) = A + B$ the factor B can be replaced by $8B$ to get the factorization $Z(n) = A + 8B$. Then

$$\underbrace{(\ 0\ )}_{\in A} + \underbrace{(\ 8\ )}_{\in 8B} = \underbrace{(\ 8\ )}_{\in A} + \underbrace{(\ 0\ )}_{\in 8B}$$

contradicts the factorization. Thus $2 \mid |B|$. A similar argument gives that $3 \mid |B|$ and $11 \mid |B|$.

If $5 \nmid |B|$, then B can be replaced by $5B$ to get the factorization $Z(n) = A + 5B$. Now

$$\underbrace{(\ 3\ )}_{\in A} + \underbrace{(\ 5\ )}_{\in 5B} = \underbrace{(\ 8\ )}_{\in A} + \underbrace{(\ 0\ )}_{\in 5B}$$

is a contradiction. Thus $5 \mid |B|$ and so $(2 \cdot 3 \cdot 5 \cdot 11) \mid |B|$.

Note that $\langle A \rangle = \langle B \rangle = Z(n)$. By Theorem 5.5 (on page 101), $|A|$ must have at least three distinct prime divisors p_1, p_2, p_3. Hence n is a multiple of $330p_1p_2p_3$. ∎

Cyclic groups having the Hajós 2-property can be used to construct codes that have finite completions. Suppose that $Z(n)$ has the Hajós 2-property and $Z(n) = A + B$ a normalized factorization. C. De Felice [36] has shown

that

$$\{x^n\} \cup \{yx^a : \ a \in A\} \cup \{x^b y : \ b \in B\}$$

is a code over the alphabet $\{x, y\}$ and the code has a finite completion. N. H. Lam [77] has proved that

$$\{x^n\} \cup \{x^a y x^b : \ a \in A, \ b \in B\}$$

is a code and it has a finite completion.

10.2 Error correcting codes

If A is a finite set, then A^n denotes the Descartes product of n copies of A, that is, the set of n-tuples with entries from A. We can make A an abelian group and then consider A^n as a direct sum of n copies of A. If $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ are elements of A^n, then the Hamming distance $d(u, v)$ is equal to the number of i's for which $u_i \neq v_i$. It is a routine exercise to check that d is a distance and so A^n is a metric space with this distance function. The sphere of center u and radius e is the set $S_e(u) = \{v \in A^n : d(u, v) \leq e\}$. A perfect e-error correcting code is a subset of C of A^n such that A^n is a disjoint union of spheres $S_e(u)$, $u \in C$. This means that the sum $S_e(0) + C$ is direct and gives A^n, that is, $A^n = S_e(0) + C$ is a factorization of A^n. A code is called a *subgroup code* if C is a subgroup of A^n. B. Lindström [79] asked if every perfect code is periodic. It is a well-known fact for coding theorists that the perfect 1-error correcting binary codes are periodic. The next proof of A. D. Sands is included since it uses techniques from the factorization theory of abelian groups. Then we construct perfect 1-error correcting non-binary codes that are not periodic.

THEOREM 10.6

Let C be a 1-error correcting perfect binary code of length n. If $n \geq 3$, then C is periodic.

PROOF Let G be an elementary 2-group of rank n. Let $x_1, \ldots, x_n$ be a basis for G. Each element a of G can be written uniquely in the form

$$a = a_1 x_1 + \cdots + a_n x_n, \quad 0 \leq a_1, \ldots, a_n \leq 1.$$

We identify a with the n-tuple $(a_1, \ldots, a_n)$ and so we can identify G with $\{0, 1\}^n$. If C is a perfect 1-error correcting binary code of length n, then $G = B + C$ is a factorization of G, where $B = \{0, x_1, \ldots, x_n\}$. Clearly

B corresponds to the Hamming sphere of radius 1 in $\{0,1\}^n$ centered at $(0,\ldots,0)$. The factorization $G = B + C$ implies that

$$2^n = |G| = |B||C| = (n+1)|C|,$$

that is, $n+1$ divides 2^n. There is an integer m such that $n+1 = 2^m$, and so $n = 2^m - 1$. Set $g = x_1 + \cdots + x_n$. We claim that g is an element of the Corrádi subgroup of B and so, by Lemma 3.1 (on page 53), g is a period of C.

In order to verify the claim, let k be the number of i's for which $\chi(x_i) = 1$. Consequently, $n-k$ is the number of i's with $\chi(x_i) = -1$ Note that

$$B = \bigcup_{i=1}^{n} \{0, x_i\}.$$

From this we get

$$\begin{aligned} 0 &= \chi(B) \\ &= \Big[\sum_{i=1}^{n} \big(\chi(0) + \chi(x_i)\big)\Big] - (n-1)\chi(0) \\ &= \Big[\sum_{i=1}^{n} \big(1 + \chi(x_i)\big)\Big] - (n-1) \\ &= k \cdot 2 - (n-1) \end{aligned}$$

and so $k = (n-1)/2$. Hence

$$k = \frac{n-1}{2} = \frac{2^m - 2}{2} = 2^{m-1} - 1.$$

Note that $n = 2^m - 1$ is odd since $n = 0$ is not possible. Further, if $n \geq 3$, then $m \geq 2$ and so $k = 2^{m-1} - 1$ is odd. Consequently, $n - k$ is even. Then

$$\chi(g) = (1)^k(-1)^{n-k} = 1,$$

as required. ∎

Let F be the field of $q = p^h$ elements, where p is a prime, that is, $F = \mathrm{GF}(q)$. Let F^n be the vector space of all ordered n-tuples of elements of F. The additive structure of F^n is an abelian group G of type $Z(p) \oplus \cdots \oplus Z(p)$. A perfect e-error correcting code is a subset of C of F^n such that F^n is a disjoint union of spheres $S_e(u)$, $u \in C$. This means that $G = S_e(0) + C$ is a factorization of G. The code C is called *linear* when it is a subspace of F^n. There is an $\alpha \in F$ such that

$$F \setminus \{0\} = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}.$$

Set $n = q + 1$ and define the linear map $\phi : F^n \to F^2$ by

$$\begin{aligned} \phi(e_i) &= e'_1 + \alpha^{i-1} e'_2, \quad 1 \le i \le q-1, \\ \phi(e_q) &= e'_1, \\ \phi(e_{q+1}) &= e'_2. \end{aligned}$$

Here e_i is the vector of F^n whose ith component is 1 and the others are 0. Similarly, e'_i is the vector of F^2 whose ith component is 1 and the other is 0. Set

$$c_i = -e_i + e_q + \alpha^{i-1} e_{q+1}, \quad 1 \le i \le q-1.$$

Let C be the kernel of ϕ. The computation

$$\begin{aligned} \phi(c_i) &= \phi(-e_i + e_q + \alpha^{i-1} e_{q+1}) \\ &= \phi(-e_i) + \phi(e_q) + \alpha^{i-1}\phi(e_{q+1}) \\ &= -e'_1 - \alpha^{i-1} e'_2 + e'_1 + \alpha^{i-1} e'_2 \\ &= 0 \end{aligned}$$

shows that $c_i \in C$. On the other hand, $c_1, \ldots, c_{q-1}$ are linearly independent vectors and so they form a basis for C. The $(q-1)$-dimensional subspace C of F^n spanned by the vectors $c_1, \ldots, c_{q-1}$ is a perfect 1-error correcting code of length n over the alphabet $\{0, 1, \alpha, \ldots, \alpha^{q-2}\}$. This C can also be used to construct a perfect 1-error correcting code that is not periodic.

A typical element x of C can be written in the form

$$x = x_1 c_1 + \cdots + x_{q-1} e_{q-1}, \quad x_1, \ldots, x_{q-1} \in F.$$

Using components, x can be represented as

$$x = (x_1, \ldots, x_n),$$

where

$$\begin{aligned} x_q &= -x_1 - x_2 - \cdots - x_{q-1}, \\ x_{q+1} &= -x_1 - \alpha x_2 - \cdots - \alpha^{q-2} x_{q-1}. \end{aligned}$$

Let π be a permutation of the elements of F. For $x = (x_1, \ldots, x_n) \in F^n$ we define $\pi(x)$ to be

$$(\pi(x_1), \ldots, \pi(x_{q-1}), x_q, x_{q+1}).$$

One can verify that $d(x, y) = d\big(\pi(x), \pi(y)\big)$ and so

$$D = \pi(C) = \{\pi(c) : \ c \in C\}$$

is also a perfect 1-error correcting code. We choose π to be the transposition $(1, \alpha)$. Further, we choose q to be the prime p, $p \ge 5$.

LEMMA 10.3

With these choices D is not periodic.

PROOF In order to prove the claim, assume the contrary, that D is periodic with period $g = (g_1, \ldots, g_n)$. Since $p \geq 5$, we can choose a y_i such that $y_i \notin \{1, \alpha\}$ and $y_i + g_i \notin \{1, \alpha\}$. Set $y = y_1 c_1 + \cdots + y_{q-1} c_{q-1}$. Plainly $y \in C$. Computing $\pi(y)$ shows that $\pi(y) = y$ and consequently $y \in D$. As g is a period of D, it follows that $y + g \in D$. Computing $\pi^{-1}(y + g)$ shows that $\pi^{-1}(y + g) = y + g$ and so $y + g \in C$. Since C is a subspace, it follows that $g \in C$. Therefore $mg \in C$ for each integer m. If $g_1 = \cdots = g_{q-1} = 0$, then, as

$$\begin{aligned} g_q &= -g_1 - g_2 - \cdots - g_{q-1}, \\ g_{q+1} &= -g_1 - \alpha g_2 - \cdots - \alpha^{q-2} g_{q-1}, \end{aligned}$$

we get $g_q = g_{q+1} = 0$, that is, g is the zero element of F^n. This is not the case. So one of $g_1, \ldots, g_{q-1}$ is not zero. Say $g_1 \neq 0$. As $g, \alpha g, \ldots, \alpha^{q-2} g$ are all periods of D, we may assume that $g_1 = 1$. Suppose α^i occurs among $g_1, \ldots, g_{q-1}$ exactly n_i times. The qth components of g and $\pi(g)$ are equal. This gives that

$$n_0 \cdot 1 + n_1 \cdot \alpha \equiv n_1 \cdot 1 + n_0 \cdot \alpha \pmod{q}$$

and so $n_0 = n_1$. Working with $\alpha g, \ldots, \alpha^{q-2} g$ we get $n_0 = n_1 = \cdots = n_{q-2} = 1$. We know that $g_1 = 1$. We may assume that $g_2 = \alpha$. Watching the $(q+1)$th components of g and $\pi(g)$, we can conclude that

$$1 + \alpha \cdot \alpha \equiv \alpha + 1 \cdot \alpha \pmod{q}.$$

This means that α is a root of the polynomial $1 - 2x + x^2 = (1 - x)^2$ over GF(q). From this it follows that $\alpha = 1$. This is a contradiction. Thus D is not periodic. ∎

10.3 Tilings

Let M be a set of integers and let S be a subset of a finite abelian group G. If each element g in $G \setminus \{0\}$ can be represented uniquely in the form

$$g = ms, \quad m \in M, \quad s \in S, \tag{10.2}$$

then we say that $G \setminus \{0\} = MS$ is a *splitting* of G. We call M the *multiplier set* of the splitting and we call S the *splitting set* of the splitting. We will be interested in the special case when $M = \{1, 2, \ldots, k\}$ and $G = Z(p)$, where k is a positive integer and p is a prime.

EXAMPLE 10.3 Let G be $Z(13)$ and set

$$M = \{1, 2\}, \quad S = \{1, 4, 3, 12, 9, 10\}.$$

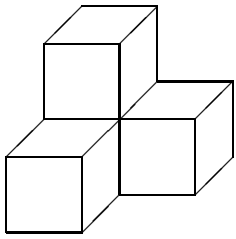

FIGURE 10.1: A $(3,1)$-semicross.

One can verify that each element of $G \setminus \{0\}$ can be represented uniquely in the form (10.2). Let

$$M' = \{-2,-1,1,2\}, \quad S' = \{1,4,3\}.$$

Again it can be checked that each element of $G \setminus \{0\}$ is uniquely expressible in the form (10.2). □

Let $e_1, \ldots, e_n$ be an orthonormal basis in the n-dimensional Euclidean space. Let k be a positive integer. The union of the n-dimensional cubes whose centers are

$$je_i, \quad 1 \le i \le n, \quad 0 \le j \le k$$

is called an (n,k)-*semicross*. Figure 10.1 (on page 217) depicts a $(3,1)$-semicross. The semicross is a union of $nk+1$ unit cubes, one center cube and n joining arms of length k. The problem we consider is for which values of n and k do translated copies of an (n,k)-semicross tile the n-dimensional space? Let $M = \{1,2,\ldots,k\}$. It turns out that the following is true.

LEMMA 10.4

If there is an abelian group G such that $|G| = nk+1$ and $G \setminus \{0\} = MS$ is a splitting, then translated copies of the (n,k)-semicross tile the n-dimensional space.

PROOF Assume that there is an abelian group G such that $|G| = nk+1$ and $G \setminus \{0\} = MS$ is a splitting. Let $S = \{s-1, \ldots, s_n\}$. Each $g \in G \setminus \{0\}$ can be represented uniquely in the form

$$g = js_j, \quad 1 \le i \le n, \quad 1 \le j \le k.$$

Choose an orthonormal basis $e_1, \ldots, e_n$ for the n-dimensional Euclidean space. Clearly the n-dimensional Euclidean space is an abelian group under the operation of addition of vectors. Choose an orthonormal basis $e_1, \ldots, e_n$ for this space. Let L be the subgroup spanned by the vectors $e_1, \ldots, e_n$. Let

$$C = \{je_i : \ 1 \le i \le n, \ 0 \le j \le k\}.$$

Let us define a map $f : L \to G$ by

$$f(a_1e_1 + \cdots + a_ne_n) = a_1s_1 + \cdots + a_ns_n.$$

Plainly f is a homomorphism and the restriction of f to C is a one-to-one map between C and G. Set $L_1 = f^{-1}(0)$. One can show that $L = C + L_1$ is a factorization of L_1. (In fact, we are lifting the trivial factorization $G = G+\{0\}$ up to the factorization $L = C+L_1$. Lemma 2.13 (on page 22) dealt with lifting factorizations when the groups were finite.)

Now the sets $C + l_1$, $l_1 \in L_1$ form a partition of L or, in other words, translated copies of C tile L. □

Factorizations of finite cyclic groups play an essential role in studying splittings when G is a cyclic group of prime order.

Let p be a prime and let $M = \{1, 2, \ldots, k\}$. Suppose that $Z(p) \setminus \{0\} = MS$ is a splitting. We may view $Z(p)$ as consisting of the integers $0, 1, \ldots, p-1$ that are added modulo p. Now both M and S are subsets of the integers. The set $Z(p) \setminus \{0\}$ is a cyclic group with multiplying $1, 2, \ldots, p-1$ modulo p. Thus the splitting $Z(p) \setminus \{0\} = MS$ is a multiplicative factorization of the cyclic group $Z(p) \setminus \{0\}$. Choosing a primitive root modulo p, one can convert this multiplicative factorization into an additive factorization. Let g be a primitive root modulo p. Now

$$Z(p) \setminus \{0\} = \{g^i : \ 0 \le i \le p-2\}$$

is a cyclic group of order $p-1$ with the multiplication modulo p. On the other hand,

$$Z(p-1) = \{i : \ 0 \le i \le p-2\}$$

is a cyclic group of order $p-1$ with addition modulo $p-1$. The map $\gamma : Z(p) \setminus \{0\} \to Z(p-1)$ defined by $\gamma(g^i) = i$ sets up the isomorphism between the two groups. Consider the splitting $Z(p) = \{0\} \cup MS$, where

$$M = \{1, 2, \ldots, k\}, \quad S = \{s_1, \ldots, s_n\}.$$

Setting

$$A = \{a(i) : \ g^{a(i)} = i, \ 1 \le i \le k\},$$
$$B = \{b(i) : \ g^{b(i)} = s_i, \ 1 \le i \le n\},$$

the splitting (the multiplicative factorization) $Z(p) \setminus \{0\} = MS$ corresponds to the additive factorization $Z(p-1) = A + B$.

EXAMPLE 10.4 Let $p = 37$. We can choose the primitive root g of p to

be 2. We compute the following powers of the 2 modulo 37:

$$\begin{array}{llll} 2^0 = 1, & 2^9 = 31, & 2^{18} = 36, & 2^{27} = 6, \\ 2^1 = 2, & 2^{10} = 25, & 2^{19} = 35, & 2^{28} = 12, \\ 2^2 = 4, & 2^{11} = 13, & 2^{20} = 33, & 2^{29} = 24, \\ 2^3 = 8, & 2^{12} = 26, & 2^{21} = 29, & 2^{30} = 11, \\ 2^4 = 16, & 2^{13} = 15, & 2^{22} = 21, & 2^{31} = 22, \\ 2^5 = 32, & 2^{14} = 30, & 2^{23} = 5, & 2^{32} = 7, \\ 2^6 = 27, & 2^{15} = 23, & 2^{24} = 10, & 2^{33} = 14, \\ 2^7 = 17, & 2^{16} = 9, & 2^{25} = 20, & 2^{34} = 28, \\ 2^8 = 34, & 2^{17} = 18, & 2^{26} = 3, & 2^{35} = 19. \end{array}$$

One can check that with the choices

$$\begin{aligned} M &= \{1, 2, 3\}, \\ S &= \{1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36\}, \end{aligned}$$

$Z(37) = \{0\} \cup MS$ is a splitting. Using the list of powers above, we can see that the sets corresponding to M and S are

$$\begin{aligned} A &= \{0, 1, 26\}, \\ B &= \{0, 27, 3, 24, 30, 33, 15, 12, 6, 21, 9, 18\}, \end{aligned}$$

respectively. It is another straightforward computation to establish that $Z(36) = A + B$ is a factorization. □

Consider an (n, k)-semicross and assume that $nk + 1 = p$ is a prime. If $M = \{1, 2, \ldots, k\}$ splits $Z(p)$, then translated copies of the semicross tile the n-dimensional space. This condition is equivalent to the fact that the set A corresponding to M has a complementer factor in $Z(p-1)$. Putting it differently, given A (constructed from M), there must exist a B such that $Z(p-1) = A + B$ is a factorization. In general, the complementer factor problem is rather intractable since it is equivalent to finding a maximal clique in an associated graph. We will discuss the special case when $|M| = k$ is a prime. If $|M| = k$ is a prime, then, by Theorem 4.4 (on page 73), in the factorization $G = Z(p-1) = A+B$ one of A or B is periodic. If A is periodic, then as $|A| = k$ is a prime it follows that A is equal to the unique subgroup $H = \langle (p-1)/k \rangle$ of G. In this case A clearly has a complementer factor. A complete set of representatives modulo H can be chosen to be B. If in the factorization $G = A + B$ the factor B is periodic, then, by Lemma 2.14 (on page 24), there is a subgroup K and a normalized subset C of G such that $|K|$ is a prime and the sum $C+K$ is direct and is equal to B. Thus $G = A+C+K$ is a factorization. Considering the factor group G/K, we get the factorization

$$G/K = [(A + K)/K] + [(C + K)/K].$$

Here

$$\begin{aligned} (A + K)/K &= \{a + K : \ a \in A\}, \\ (C + K)/K &= \{c + K : \ c \in C\}, \end{aligned}$$

and G/K is a cyclic group of order $(p-1)/|K|$. Therefore, in the case when B is periodic, we end up with a factorization $G' = A' + B'$, where $G' = Z((p-1)/|K|)$. This reduces the problem to a smaller group.

From the argument above one can extract the following test for the existence of a complementary factor B provided $|A| = k$ is a prime.

LEMMA 10.5

The set A has a complementer factor B in $Z(p-1)$ if and only if A is equal to one of

$$K = \langle d \rangle \quad \text{in} \quad Z(dk),$$

where d runs over the positive divisors of $(p-1)/k$.

In order to illustrate how to apply the test, we work out two examples.

EXAMPLE 10.5 Let us decide if $M = \{1, 2, 3\}$ splits $Z(103)$. Note that 5 is a primitive root modulo 103 and

$$1 = 5^0, \quad 2 = 5^{44}, \quad 3 = 5^{39}.$$

We face the question if $A = \{0, 44, 39\}$ has a complementer factor B in $Z(102)$. The decomposition of $102/3$ into primes is $2 \cdot 17$ and so the divisors of $102/3$ are $34, 17, 2, 1$. We should check if $A = \{0, 44, 39\}$ is equal to one of

$$\begin{array}{lll} \langle 34 \rangle = \{0, 34, 68\} & \text{in} & Z(102), \\ \langle 17 \rangle = \{0, 17, 34\} & \text{in} & Z(51), \\ \langle 2 \rangle = \{0, 2, 4\} & \text{in} & Z(6), \\ \langle 1 \rangle = \{0, 1, 2\} & \text{in} & Z(3). \end{array}$$

The reduced versions of A modulo $102, 51, 6, 3$, respectively, are

$$\begin{array}{ll} \{0, 44, 39\}, & \{0, 44, 39\}, \\ \{0, 2, 3\}, & \{0, 2, 0\}. \end{array}$$

Therefore A has no complementer factor in $Z(102)$ and $M = \{1, 2, 3\}$ does not split $Z(103)$. ∎

EXAMPLE 10.6 Let us investigate if $M = \{1, 2, 3, 4, 5\}$ splits $Z(421)$. Using the facts that 2 is a primitive root of modulo 421 and

$$1 = 2^0, \quad 2 = 2^1, \quad 3 = 2^{404}, \quad 4 = 2^2, \quad 5 = 2^{278},$$

we are left with the problem of whether $A = \{0, 1, 404, 2, 278\}$ has a complementer factor in $Z(420)$. The prime factorization of 420 is $2^2 \cdot 3 \cdot 5 \cdot 7$. The positive divisors of $420/5 = 2^2 \cdot 3^1 \cdot 7^1$ are in the form $2^{\beta(1)}3^{\beta(2)}7^{\beta(3)}$, where

$$0 \le \beta(1) \le 2, \quad 0 \le \beta(2) \le 1, \quad 0 \le \beta(3) \le 1.$$

TABLE 10.3: The divisors of 84

$\beta(1)$	$\beta(2)$	$\beta(3)$	d
0	0	0	1
0	0	1	7
0	1	0	3
0	1	1	21
1	0	0	2
1	0	1	14
1	1	0	6
1	1	1	42
2	0	0	4
2	0	1	28
2	1	0	12
2	1	1	84

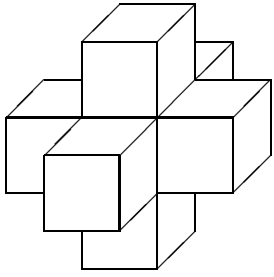

FIGURE 10.2: A $(3, 1)$-cross.

Table 10.3 (on page 221) contains the 12 positive divisors of 420/5. We can notice that 1 will belong to any reduced version of A modulo d and only $\langle 1\rangle$ in $Z(5)$ contains 1. So it is enough to check if A is equal to $\langle 1\rangle = \{0, 1, 2, 3, 4\}$ in $Z(5)$. This holds. Therefore A has a complementer factor in $Z(420)$. Translated copies of an $(84, 5)$-semicross tile the 84-dimensional Euclidean space. ∎

Let $e_1, \ldots, e_n$ be an orthonormal basis of the n-dimensional Euclidean space and let k be a positive integer. The union of the n-dimensional unit cubes whose centers are

$$je_i, \quad 1 \leq i \leq n, \quad -k \leq j \leq k$$

is called an (n, k)-*cross*. An (n, k)-cross is a union of $2kn + 1$ unit cubes, $2n$ arms of length k are joining a central cube. A $(3, 1)$-cross can be seen in Figure 10.2 (on page 221). Let $l_1, \ldots, l_n$ be independent vectors in the n-dimensional space. The set L of all linear combinations of $l_1, \ldots, l_n$ with integer coefficients is a called a *lattice*. We also say that L is spanned by $l_1, \ldots, l_n$. Clearly L is an abelian group with the operation of the addition

of vectors. Let us fix the coordinate unit vectors $e_1, \ldots, e_n$. A lattice L spanned by the vectors $l_1, \ldots, l_n$ is termed an *integer lattice* or a Z-lattice if each coordinate of each l_i is an integer. Similarly, L is defined to be a *rational lattice* or Q-lattice if each coordinate of each l_i is a rational number. A tiling consisting of translated copies of an (n, k)-cross will be called a Z-lattice tiling if the translation vectors of the crosses form a Z-lattice. Analogously we talk about Q-lattice tilings.

LEMMA 10.6

Let $M = \{-k, \ldots, -1, 1, \ldots, k\}$. There exists a Z-lattice tiling by translates of an (n, k)-cross if and only if there is an abelian group G such that $|G| = 2kn + 1$ and $G \setminus \{0\} = MS$ is a splitting.

PROOF Let $e_1, \ldots, e_n$ be an orthonormal basis for the n-dimensional Euclidean space. Let L be the lattice spanned by $e_1, \ldots, e_n$. Clearly L is an abelian group under the addition of vectors and each Z-lattice is a sublattice of L. Let

$$C = \{je_i : \ 1 \le i \le n, \ -k \le j \le k\}.$$

The elements of C are the centers of the n-dimensional cubes forming an (n, k)-cross.

Assume that there is a Z-lattice tiling by translates of an (n, k)-cross. This means that there is a lattice L_1 such that $L_1 \subseteq L$ and the sets $C + l + 1$, $l_1 \in L_1$ form a partition of L. In other words, each $l \in L$ can be represented uniquely in the form

$$l = c + l_1, \quad c \in C, \quad l_1 \in L_1.$$

Let $G = L/L_1$ and set $s_i = e_i + L_1$ for each i, $1 \le i \le n$. Now each $g \in G \setminus \{0\}$ can be represented uniquely in the form

$$g = js_i, \quad 1 \le i \le n, \quad 1 \le |j| \le k.$$

Therefore $G \setminus \{0\} = MS$ is a splitting, where $S = \{s_1, \ldots, s_n\}$.

Next assume that there is an abelian group G such that $|G| = 2kn + 1$ and $G \setminus \{0\} = MS$ is a splitting. Suppose $S = \{s_1, \ldots, s_n\}$. Let us define a map $f : L \to G$ by

$$f(a_1e_1 + \cdots + a_ne_n) = a_1s_1 + \cdots + a_n.$$

As in the proof of Lemma 10.4 (on page 217), we can see that the trivial factorization $G = G + \{0\}$ can be lifted to the factorization $L = C + f^{-1}(0)$. Therefore, translated copies of an (n, k)-cross form a Z-lattice tiling of the n-dimensional Euclidean space. ∎

In the $k = 1$ special case, $M = \{-1, 1\}$. If G is an abelian group of order $2n + 1$, then G does not have element of order two. Therefore $g \in G \setminus \{0\}$

implies $g \neq -g$ and so $G \setminus \{0\}$ can be represented in the form

$$G \setminus \{0\} = \{-g_n, \ldots, -g_1, g_1, \ldots, g_n\}.$$

In short, $M = \{-1, 1\}$ splits G with the splitting set

$$S = \{g_1, \ldots, g_n\}.$$

We summarize the geometrical content of the above argument in the following lemma.

LEMMA 10.7

For each positive n, the n-dimensional space can be tiled with translated copies of an $(n, 1)$-cross, where the translation vectors form a Z-lattice.

We work out the details in the $n = 4$ special case.

EXAMPLE 10.7 Let G be a cyclic group of order $2n + 1 = 9$ with generator element x. Plainly $G \setminus \{0\} = \{-1, 1\}S$ is a splitting, where

$$\begin{aligned} S &= \{g_1, g_2, g_3, g_4\} \\ &= \{x, 2x, 3x, 4x\}. \end{aligned}$$

To prove the claim that translates of a $(4, 1)$-cross tile the 4-dimensional space, let N be the lattice spanned by $e_1, \ldots, e_4$ and let $f : N \to G$ be a map defined by

$$\begin{aligned} f(a_1e_1 + \cdots + a_4e_4) &= a_1g_1 + \cdots + a_4g_4 \\ &= a_1(x) + a_2(2x) + a_3(3x) + a_4(4x). \end{aligned}$$

It can be verified that f is a homomorphism. Let L be the kernel of f. The factor group N/L is isomorphic to G. The cosets

$$-e_4 + L, \ldots, -e_1 + L, 0 + L, e_1 + L, \ldots, e_4 + L$$

correspond to the elements

$$-g_4, \ldots, -g_1, 0, g_1, \ldots, g_4,$$

respectively. Therefore the cosets form a partition of N. The equation

$$N = \{-e_4, \ldots, -e_1, 0, e_1, \ldots, e_4\} + L$$

is a factorization of N and so translated copies of a $(4, 1)$-cross tile the 4-dimensional space. The translation vectors belong to L. Next we describe L more explicitly. Set

$$\begin{aligned} l'_1 &= 9e_1 \\ l'_2 &= 2e_1 - e_2 \\ l'_3 &= 3e_1 \qquad - e_3 \\ l'_4 &= 4e_1 \qquad\qquad - e_4 \end{aligned}$$

and let L' be the lattice spanned by $l'_1, \ldots, l'_4$. We claim that $L = L'$. Computing $f(l'_1), \ldots, f(l'_4)$ shows that $L' \subseteq L$. Indeed,

$$\begin{aligned} f(l'_1) &= f(9e_1) &&= 9x &&= 0, \\ f(l'_2) &= f(2e_1 - e_2) &&= 2x - 2x &&= 0, \\ f(l'_3) &= f(3e_1 - e_3) &&= 3x - 3x &&= 0, \\ f(l'_4) &= f(4e_1 - e_4) &&= 4x - 4x &&= 0. \end{aligned}$$

On the other hand, let $l = b_1e_1 + \cdots + b_4e_4$ be an element of L. Adding integer multiples of $l'_2, \ldots, l'_4$ to l we get $l + l' = be_1$, where $l' \in L'$ and $0 \leq b \leq 8$. From

$$0 = f(l + l') = f(be_1) = bx$$

it follows that $b = 0$ and so $L \subseteq L'$. Therefore $L = L'$. ∎

LEMMA 10.8
Let $q_1, \ldots, q_n$ be positive integers, let

$$M = \{-k, \ldots, -1, 1, \ldots, k\},$$

and let N be the lattice spanned by $(1/q_1)e_1, \ldots, (1/q_n)e_n$. If there is an abelian group G of order $(2kn+1)q_1 \cdots q_n$ and elements $g_1, \ldots, g_n$ of G such that $G = \big(\{0\} \cup MS\big) + A_1 + \cdots + A_n$ is a factorization, where

$$\begin{aligned} S &= \{q_1g_1, \ldots, q_ng_n\}, \\ A_i &= \{0, g_i, 2g_i, \ldots, (q_i - 1)g_i\}, \quad 1 \leq i \leq n, \end{aligned}$$

then there is a tiling of translates of an (n, k)-cross in which the translation vectors form a sublattice L of N. In addition, if the set $\big(\{0\} \cup MS\big)$ is not a subgroup of G, then L is not a Z-lattice.

EXAMPLE 10.8 For $n = 4$, $2n+1 = 9$ is not a prime. To apply Lemma 10.8 (on page 224) in the $n = 4$, $k = 1$ special case, choose $q_1, \ldots, q_4$ to be $1, 1, 1, 2$, respectively, and let G be a cyclic group of order $(2n+1)q_1 \cdots q_4 = 18$ with generator element x. The factorizations

$$\begin{aligned} G &= \{0, x, 2x\} + \langle 3x \rangle \\ &= \{0, x, 2x - 3x\} + \langle 3x \rangle \\ &= \{-x, 0, x\} + \langle 3x \rangle \\ &= \{-x, 0, x\} + \{0, 3x\} + \{0, 6x, 12x\} \\ &= \{-x, 0, x\} + \{0, 6x, 12x\} + \{0, 3x\} \\ &= \{-x, 0, x\} + \{0, 6x, 12x - 18x\} + \{0, 3x\} \\ &= \{-x, 0, x\} + \{-6x, 0, 6x\} + \{0, 3x\} \\ &= \{-6x, -7x, -5x, -x, 0, x, 5x, 7x, 6x\} + \{0, 3x\} \\ &= \big(\{0\} \cup \{-1, 1\}\{x, 5x, 7x, 2 \cdot 3x\}\big) + \{0, 3x\} \end{aligned}$$

show that with the

$$g_1 = x, \quad g_2 = 5x, \quad g_3 = 7x, \quad g_4 = 3x$$

choices G has a factorization in the form $G = \big(\{0\} \cup MS\big) + A_1 + \cdots + A_4$. The set $\big(\{0\} \cup MS\big)$ is not a subgroup of G. By the above criterion there is a tiling consisting of translated copies of a $(4,1)$-cross, where the translation vectors form a lattice L which is not a Z-lattice.

In order to see the details let $f : N \to G$ be a map defined by

$$\begin{aligned} f\big[a_1(1/q_1)e_1 + \cdots + a_4(1/q_4)e_4\big] &= a_1g_1 + \cdots + a_4g_4 \\ &= a_1(x) + a_2(5x) + a_3(7x) + a_4(3x). \end{aligned}$$

We check that f is a homomorphism and set $L = \mathrm{Ker}(f)$. The factor group N/L is isomorphic to G. It follows that each element n of N can be represented uniquely in the form

$$n = c + a_1 + \cdots + a_4 + l,$$

where

$$\begin{aligned} c &\in \{-e_4, \ldots, -e_1, 0, e_1, \ldots, e_4\}, \\ a_i &\in \big\{0, (1/q_i)e_i, 2(1/q_i)e_i, \ldots, (q_i - 1)(1/q_i)e_i\big\}, \\ l &\in L. \end{aligned}$$

This means that, translating a $(4,1)$-cross by elements of L, the crosses tile the 4-dimensional space. We can describe L in terms of its basis vectors. Set

$$\begin{aligned} l'_1 &= 18e_1 \\ l'_2 &= 5e_1 - e_2 \\ l'_3 &= 7e_1 \qquad - e_3 \\ l'_4 &= 3e_1 \qquad\qquad -(1/2)e_4 \end{aligned}$$

and let L' be the lattice spanned by $l'_1, \ldots, l'_4$. One can verify that $L = L'$. Now l'_4 makes it obvious that L is not a Z-lattice. □

The construction in Example 10.8 (on page 224) can be carried out in larger generality and one can proof the following result.

LEMMA 10.9

When $2n + 1$ is not a prime, there are tilings by translates of an $(n,1)$-cross such that the translation vectors form a Q-lattice that is not a Z-lattice.

10.4 Integer codes

In this section we describe single error correcting codes over the alphabet $\{0, 1, \ldots, m-1\}$ and their connection with splitting and factoring abelian groups.

Let $f : A \to B$ be an injective function. The set $C = \mathrm{Im}f$ is called a code. Intuitively, the element $a \in A$ is coded by the element $f(a) \in B$. In the most commonly encountered situation, A, B are chosen to be F^k, F^n, respectively, where F is the Galois field of order 2. In this case a 0, 1 sequence of length k is coded by a 0, 1 sequence of length n. When f is a linear map it is customary to associate the exact sequence

$$\{0\} \longrightarrow F^k \xrightarrow{f} F^n \xrightarrow{g} F^{n-k} \longrightarrow \{0\}$$

with the code. For us a similar exact sequence,

$$\{0\} \longrightarrow [Z(m)]^k \xrightarrow{f} [Z(m)]^n \xrightarrow{g} [Z(m)]^{n-k} \longrightarrow \{0\}$$

will be relevant, where $Z(m)$ is the ring of integers modulo m. The code $C = \mathrm{Im}f$ can be described equivalently as $C = \mathrm{Ker}g$. In other words, an $a \in [Z(m)]^n$ is a code word if $g(a) = 0$. In general, $g(a)$ is not equal to 0 and it is called the *syndrome* of a. In order to further particularize the construction, let $k = n - 1$ and let us fix the sequence of elements $s_1, \ldots, s_n$ of $Z(m) \setminus \{0\}$ and define the function g by

$$g(a) = \sum_{i=1}^{n} s_i a_i,$$

where $a = (a_1, \ldots, a_n)$. The sequence $s_1, \ldots, s_n$ is called a *weight sequence*. The choice of the weights leads to various codes.

Suppose that a single substitution error occurs, say the letter a_i is replaced by a letter $a_i' = a_i + e_i$ in the code word

$$a = (a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n),$$

where e_i is coming from a fixed error set E. One then receives the new word,

$$a' = (a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n),$$

instead of a. The set of elements

$$(a_1, \ldots, a_{i-1}, a_i + e_i, a_{i+1}, \ldots, a_n),$$

where i runs over $1, \ldots, n$ and e_i varies over the elements of $E \cup \{0\}$, is called a *substitution error sphere* centered at a. We denote it by $S(a, E)$. One can check that $S(a, E)$ has $n|E| + 1$ elements. Table 10.4 (on page 227) depicts the elements of $S(a, E)$ in the particular case when $a = (0, 0, 0)$ and $E = \{1, 2, 4, 8\}$. A subset C of $[Z(m)]^n$ is called a perfect single t-substitution error correcting code if the substitution error spheres

$$S(c, E), \quad c \in C$$

TABLE 10.4: A substitution error sphere

000			
100	200	400	800
010	020	040	080
001	002	004	008

form a partition of $[Z(m)]^n$. We will show that perfect substitution error correcting codes are related to splittings of $Z(m)$.

The syndrome of the word a' is

$$\begin{aligned} g(a') &= \Big[\sum_{j=1}^{i-1} s_j a_j\Big] + s_i a_i' + \Big[\sum_{j=i+1}^{n} s_j a_j\Big] \\ &= \Big[\sum_{j=1}^{i-1} s_j a_j\Big] + s_i a_i + \Big[\sum_{j=i+1}^{n} s_j a_j\Big] + s_i a_i' - s_i a_i \\ &= \Big[\sum_{j=1}^{n} s_j a_j\Big] + s_i(a_i' - a_i) \\ &= g(a) + s_i e_i \\ &= s_i e_i. \end{aligned}$$

If all the possible non-zero syndromes are pair-wise distinct, then the distortion can be corrected. In other words, a single substitution error can be corrected if

$$s_i e_i = s_j e_j, \quad e_i, e_j \in E$$

imply that $s_i = s_j$ and $e_i = e_j$.

Let us consider the case when the error set E is equal to

$$\{\pm 1, \pm 2, \ldots, \pm t\}.$$

We may sum up our consideration in the following way. If there is a subset S of $Z(m)$ such that $Z(m) \setminus \{0\} = ES$ is a splitting of $Z(m)$, then there is a 1-error correcting t-substitution perfect code of word length $|S|$ over the alphabet $Z(m)$.

Let d, n, k be nonnegative integers such that $d \leq k$. The sequence $a = (a_1, \ldots, a_n)$ is called an (n, d, k)-sequence if $d \leq a_i \leq k$ holds for each i, $1 \leq i \leq n$. Plainly, if $a = (a_1, \ldots, a_n)$ is an (n, d, k)-sequence, then $b = (a_1 - d, \ldots, a_n - d)$ is an $(n, 0, k - d)$-sequence, that is, b can be viewed as a word of length n over the alphabet $\{0, 1, \ldots, k - d\} = Z(m)$, where $m = k - d + 1$. The set of all (n, d, k)-sequences is denoted by $T(n, d, k)$. It can be checked that $T(n, d, k)$ has $(k - d + 1)^n$ elements.

To an (n, d, k)-sequence $a = (a_1, \ldots, a_n)$ we assign the 0, 1 sequence

$$h(a) = (\underbrace{0, \ldots, 0}_{a_1}, 1, \underbrace{0, \ldots, 0}_{a_2}, 1, \ldots, \underbrace{0, \ldots, 0}_{a_n}, 1).$$

The sequence $h(a)$ has

$$(a_1 + 1) + \cdots + (a_n + 1) = n + a_1 + \cdots + a_n$$

components. The 1's in $h(a)$ are called *peaks* and consecutive 0's are called *runs*. If the first peak is shifted to the right by j digits, then we get the sequence

$$(\underbrace{0, \ldots, 0}_{a_1+j}, 1, \underbrace{0, \ldots, 0}_{a_2-j}, 1, \ldots, \underbrace{0, \ldots, 0}_{a_n}, 1)$$

from $h(a)$, provided, of course, that $a_2 - j \geq 0$ holds. If the first peak is shifted to the left by j digits, then we get the sequence

$$(\underbrace{0, \ldots, 0}_{a_1-j}, 1, \underbrace{0, \ldots, 0}_{a_2+j}, 1, \ldots, \underbrace{0, \ldots, 0}_{a_n}, 1)$$

from $h(a)$. Naturally, we must assume that $a_1 - j \geq 0$. Similarly, we can speak of shifting the ith peak to the left or to the right by j digits in $h(a)$ for each i, $1 \leq i \leq n - 1$.

Let $a = (a_1, \ldots, a_n)$ be an (n, d, k)-sequence and let the error set E be $\{\pm 1, \pm 2, \ldots, \pm t\}$. Suppose that a single shift error occurs in $h(a)$, say the letter a_i is replaced by $a'_i = a_i - j$ and a_{i+1} is replaced by $a'_{i+1} = a_{i+1} + j$, where $j \in E$ and $1 \leq i \leq n - 1$. We get the new sequence

$$a' = (a_1, \ldots, a_{i-1}, a'_i, a'_{i+1}, a_{i+2}, \ldots, a_n).$$

The set of elements

$$(a_1, \ldots, a_{i-1}, a_i - e, a_{i+1} + e, a_{i+2}, \ldots, a_n),$$

where e ranges over $E \cup \{0\}$ and i varies over $1, \ldots, n - 1$, is called, a *single shift error sphere* centered at a with radius t. We denote it by $S(a, t)$. In Table 10.5 (on page 229) we list the elements of $S(a, t)$ in the special case when $a = (2, 2, 2, 2)$, $t = 2$. It is a routine exercise to verify that if a is of length n, then $S(a, t)$ has $2nt + 1$ elements. Note that if a is an (n, d, k)-sequence, then the elements of $S(a, t)$ are $(n, d - t, k + t)$-sequences. A subset C of $T(n, d - t, k + t)$ is called a perfect single t-shift error correcting code if the shift error spheres

$$S(c, t), \quad a \in C$$

form a partition of $T(n, d - t, k + t)$.

Next we show that the existence of shift error correcting codes is related to splittings of abelian groups.

TABLE 10.5: A single shift error sphere

2222	001001001001		
0422	100001001001	4022	000011001001
1322	010001001001	3122	000101001001
2042	001100001001	2402	001000011001
2132	001010001001	2312	001000101001
2204	001001100001	2240	001001000011
2213	001001010001	2231	001001000101

The syndrome of a' is

$$\begin{aligned} g(a') &= \Big[\sum_{j=1}^{i-1} s_j a_j\Big] + s_i a'_i + s_{i+1} a'_{i+1} + \Big[\sum_{j=i+2}^{n} s_j a_j\Big] \\ &= \Big[\sum_{j=1}^{i-1} s_j a_j\Big] + s_i a_i + s_{i+1} a_{i+1} + \Big[\sum_{j=i+2}^{n} s_j a_j\Big] + \\ &\quad s_i a'_i + s_{i+1} a'_{i+1} - s_i a_i - s_{i+1} a_{i+1} \\ &= \Big[\sum_{j=1}^{n} s_j a_j\Big] + s_i(a'_i - a_i) + s_{i+1}(a'_{i+1} - a_{i+1}) \\ &= g(a) + s_i(-j) + s_{i+1} j \\ &= j(s_{i+1} - s_i). \end{aligned}$$

If all the possible non-zero syndromes are pair-wise distinct, then the distortion can be corrected. Let $W = \{w_1, \ldots, w_{n-1}\}$ be a subset of $Z(m)$. If each element of $Z(m) \setminus \{0\}$ is uniquely expressible in the form

$$jw_i, \quad 1 \le |j| \le t, \quad 1 \le i \le n-1,$$

that is, if $Z(m) \setminus \{0\} = EW$ is a splitting, then there is a 1-error correcting perfect t-shift code. We just have to choose

$$s_2 - s_1, s_3 - s_2, \ldots, s_n - s_{n-1}$$

to be $w_1, \ldots, w_{n-1}$, respectively.

The code constructions described above can be generalized, namely, specify an alphabet of t letters $X = \{0, 1, \ldots, t-1\}$. Then use the subset $C = X^n \cap \mathrm{Ker} g$ of $[Z(m)]^n$ as a code. As an example, we consider the so-called Varshamov-Tenengolts code. (See [171].) Let $t = 2$ and so $X = \{0, 1\}$ is a binary alphabet. Further, let $m = n+1$. The weight sequence $(s_1, s_2, \ldots, s_n)$ is chosen to be $= (1, 2, \ldots, n)$. The function $g : [Z(m)]^n \to Z(m)$ as usual is defined by

$$g(a) = \sum_{i=1}^{n} i a_i.$$

Here the components of the word $a = (a_1, \ldots, a_n)$ are the elements of the alphabet X. The Varshamov-Tenengolts code is capable of correcting one asymmetric error.

Suppose one asymmetric error occurs; say the letter a_i is accidentally changed to a_i' in the code word

$$a = (a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n)$$

during the transition and we actually receive the distorted word

$$a' = (a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n).$$

The syndrome of a' is

$$\begin{aligned} g(a') &= \Big[\sum_{j=1}^{i-1} j a_j\Big] + i a_i' + \Big[\sum_{j=i+1}^{n} j a_j\Big] \\ &= \Big[\sum_{j=1}^{n} j a_j\Big] + i a_i' - i a_i \\ &= g(a) + i(a_i' - a_i) \\ &= i(a_i' - a_i). \end{aligned}$$

Note that $g(a') = 0$ if $a_i = a_i' = 0$ and $g(a') = -i$ if $a_i = 1$ and $a_i' = 0$. Therefore, all the possible non-zero syndromes are pair-wise distinct and the error in the word a' can be corrected to recover the word a.

V. I. Levenshtein [78] observed that the Varshamov-Tenengolts code could be used for correcting single deletion errors. Suppose that the code word

$$a = (a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n)$$

is transmitted, the letter a_i is deleted, and

$$a' = (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$$

has arrived. Let L_0, L_1 be the number of 0's, 1's to the left of a_i in a, respectively. Similarly, let R_0, R_1 be the number of 0's, 1's to the right of a_i in a, respectively. By counting the 0's and 1's in a' we can find $L_0 + R_0$ and $L_1 + R_1$. Plainly $L_0 + L_1 = i - 1$ and $R_0 + R_1 = n - i$. The syndrome of

a' is

$$\begin{aligned} g(a') &= \Big[\sum_{j=1}^{i-1} ja_j\Big] + \Big[\sum_{j=i+1}^{n} (j-1)a_j\Big] \\ &= \Big[\sum_{j=1}^{i-1} ja_j\Big] + ia_i + \Big[\sum_{j=i+1}^{n} ja_j\Big] + \\ &\quad \Big[\sum_{j=i+1}^{n} (j-1)a_j\Big] - ia_i - \Big[\sum_{j=i+1}^{n} ja_j\Big] \\ &= \Big[\sum_{j=1}^{i-1} ja_j\Big] - ia_i - \Big[\sum_{j=i+1}^{n} a_j\Big] \\ &= g(a) - ia_i - R_1 \\ &= -R_1 - ia_i. \end{aligned}$$

If $a_i = 0$, then $g(a') = -R_1$ and $|g(a')| \leq L_1 + R_1$. If $a_i = 1$, then $g(a') = -R_1 - i$ and $|g(a')| > L_1 + R_1$.

The error correction procedure is the following. If $|g(a')| \leq L_1 + R_1$, then we can draw the conclusion that $a_i = 0$ and $|g(a')| = R_1$. Using $L_1 + R_1$, we can compute L_1. We cannot compute i, but we may insert the missing 0 anywhere between the (L_1)th and the $(L_1 + 1)$th 1's in the word a' to recover the word a. If $|g(a')| > L_1 + R_1$, then we can draw the conclusion that $a_i = 1$ and $|g(a')| = R_1 + i$. From $R_0 + R_1 = n - i$, R_0 can be computed and then i can be computed.

The *complementer subgroup problem* is the following. Given a finite abelian group G and a subset A of G such that $|A|$ divides $|G|$, decide if there is a subgroup H of G such that $G = A + H$ is a factorization of G. The complementer subgroup problem is computationally less demanding than the complementer factor problem. But it still can be hard if G has too many subgroups. However, for cyclic groups it is definitely easy since there is only one subgroup for each given order. For a given subgroup H of G it is straightforward to check if $G = A + H$ is a factorization of G. Say one checks if the elements of A are pair-wise incongruent modulo H.

Let p be a prime. S. K. Stein calls a splitting $Z(p) \setminus \{0\} = MS$ a *coset splitting* if S is a multiplicative subgroup of the multiplicative group $Z(p) \setminus \{0\}$ and consequently M is a complete set of representatives modulo S, which explains the name. We have just seen that deciding if a given M coset splits $Z(p) \setminus \{0\}$ is computationally simpler than deciding if M splits $Z(p) \setminus \{0\}$.

We will prove that if $G = A + B$ is a normalized factorization of the finite cyclic group G, where $|A| = q$ is a prime, $\langle A \rangle = G$, then B is a subgroup of G.

This result greatly simplifies the search for the 1-error correcting t-substitution and t-shift codes in the case when t is a prime. To see why, let $M =$

$\{\pm 1, \pm 2, \ldots, \pm t\}$ and let $Z(p) \setminus \{0\} = MS$ be a splitting. The splitting corresponds to the multiplicative factorization $Z(p) \setminus \{0\} = MS$. Note that $L = \{-1, 1\}$ is a subgroup of $Z(p) \setminus \{0\}$. Set $A = \{1, 2, \ldots, t\}$. Plainly, $M = AL$ is a multiplicative factorization of M. Considering the factor group $G = [Z(p)\setminus\{0\}]/L$ from $Z(p)\setminus\{0\} = (AL)S$, we get the factorization $G = AB$, where $B = \{sL : \ s \in S\}$. By our assumption, $|A| = t$ is a prime. Choose $a \in A$, $b \in B$. Multiplying the factorization $G = AB$ by $a^{-1}b^{-1}$, we get the normalized factorization

$$G = Ga^{-1}b^{-1} = (Aa^{-1})(Bb^{-1}).$$

By renaming we may assume that the original factorization $G = AB$ is normalized. Set $H = \langle A\rangle$. If $H \neq G$, then restricting the factorization $G = AB$ to H we get the factorization $H = G \cap H = A(B \cap H)$. Choose a complete set of representatives $c_1, \ldots, c_s$ in G modulo H. Set $C = \{c_1, \ldots, c_s\}$. It is clear that $G = HC$ is a factorization of G. Then

$$G = [A(B \cap H)]C = A[(B \cap H)C]$$

is a factorization of G. Therefore, if A has a complementer factor in H, then A has a complementer factor in G. In other words, the problem of deciding if A has a complementer factor in G can be reduced to the problem of deciding if A has a complementer factor in $H = \langle A\rangle$.

By the mentioned result, from the normalized factorization $H = AD$ it follows that D is a subgroup of H. This means that A can have only a subgroup complementer factor in H.

Now we state the theorem formally and prove it.

THEOREM 10.7

Let $G = A + B$ be a normalized factorization of the finite cyclic group G. If $|A| = q$ is a prime, $\langle A\rangle = G$, then B is a subgroup of G.

PROOF Assume on the contrary that there is a finite cyclic group G such that $G = A + B$ is a normalized factorization, $|A| = q$ is a prime, $\langle A\rangle = G$, and B is not a subgroup of G. We choose such a counter-example for which $|G|$ is minimal.

We claim that in a minimal counter-example none of the factors is periodic. To verify the claim, assume on the contrary that A or B are periodic. If A is periodic, then, since $|A| = q$ is a prime and $0 \in A$, it follows that A is a subgroup of G of order q. As $\langle A\rangle = G$, we get that $B = \{0\}$. This contradicts our assumption that B is not a subgroup of G. Thus we may assume that B is periodic. Let H be the subgroup of periods of B. By Lemma 2.8 (on page 18), there is a subset C of B such that $B = C + H$ is a factorization of B. From the factorization $G = A + (C + H)$, by considering the factor group

G/H we get the factorization

$$G/H = (A + H)/H + (C + H)/H.$$

By Lemma 2.7 (on page 17), the factor $(A + H)/H$ spans the whole of G/H. The minimality of the counter-example $G = A + B$ implies that $(C + H)/H$ is a subgroup of G/H. It follows that $B = C + H$ is a subgroup of G, contrary to our assumption.

To finish the proof, note that by Theorem 4.3 (on page 67), in the factorization $G = A + B$ at least one of the factors is always periodic. □

Notes

(1) Let p be a prime. If $Z(p) \setminus \{0\} = MS$ is a splitting, then there is a multiplicative factorization $G = AB$, where G is the multiplicative group $Z(p) \setminus \{0\}$. The multiplier set M admits a coset splitting if and only if in the factorization $G = AB$ the factor B can be replaced by a subgroup H to get the factorization $G = AH$.

(2) The strongest result about replacing a factor by a subgroup can be found in [121] and reads as follows. Let G be a nilpotent group of order $p^\alpha m$, where m is relatively prime to p. If G contains a normal subgroup K of order m and $G = AB$ is a factorization such that $|A| = p^\alpha$, $|B| = m$, then the factor B can be replaced by K in the factorization $G = AB$ to get the factorization $G = AK$.

(3) By Theorem 10.7 (on page 232), under certain conditions, not only can B be replaced by a subgroup but B itself is a subgroup.

Chapter 11

Some classical problems

11.1 Fuchs's problems

In his book [41] L. Fuchs lists problems at the end of each chapter. We give here the current position for those problems listed on page 321 at the end of his chapter on decomposition into direct sums of subsets.

Problem 77 of [41]. If $G = S + T$ is a factorization, where G is a finite (cyclic), can then one of the subsets S, T be replaced by a subgroup of G?

In the cyclic case this problem is tackled in Section 7.1 The answer, in general, is negative. The smallest counter-example occurs with $G = Z(8)$, as shown in Example 7.5 (on page 145). Theorems 7.1 (on page 141) and 7.2 (on page 142) show that the result is true for cyclic groups of order pn, where p is a prime and n is square-free, and Theorem 7.4 (on page 146) shows that these are the only finite cyclic groups for which the result holds.

Problem 78 of [41]. Which finite groups G have the property that $G = S+T$ implies that one of the subsets S, T is periodic?

In Section 4.2 the complete answer is given for cyclic groups. These are listed as $Z(n)$, where n is a divisor of one of the following numbers:

$$p^e q, \quad p^2q^2, \quad p^2qr, \quad pqrs,$$

provided n is large enough to admit such a factorization. Here p, q, r, s are distinct primes and e is any positive integer.

The solution is also known in the non-cyclic case, and a list of these groups is given in Sands [117].

The result on the cyclic case was a consequence of Theorem 4.3 (on page 67). An incomplete result can be proved independently of Theorem 4.3. In particular, the argument does not rely on characters or cyclotomic polynomials.

THEOREM 11.1

Let p, q, r, s be distinct primes and let G be a group of type

$$Z(p^2q^2), \quad Z(p^2qr), \quad Z(pqrs).$$

If $G = A + B$ is a normalized factorization of G, then A or B is periodic.

PROOF Suppose first that $|A|$ is a prime, say $|A| = p$. If each element $a \in A \setminus \{0\}$ has order p, then A is the unique subgroup K of G of order p and so A is periodic. We may assume that there is an $a \in A \setminus \{0\}$ whose order is not p. Set

$$A_1 = \{0, a, 2a, \ldots, (p-1)a\}.$$

In the normalized factorization $G = A + B$, by Lemma 8.4 (on page 177), the factor A can be replaced by A_1 to get the normalized factorization $G = A_1 + B$. By the proof of Lemma 6.1 (on page 122), it follows that $B = pa + B$. Therefore pa is a period of B, as required.

In the remaining part of the proof we may assume that both $|A|$ and $|B|$ are products of two primes. By Corollary 5.1 (on page 103), $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. We may assume that $H = \langle A \rangle \neq G$. Choose an element $b \in B$ and add $-b$ to both sides of the factorization $G = A + B$ to get the normalized factorization $G = A + (B - b)$. Restricting the factorization $G = A + (B - b)$ to H gives the normalized factorization $H = A + [(B - b) \cap H]$. Set $B_b = [(B - b) \cap H]$. Obviously $|B_b| = p$ is a prime and p does not depend on the choice of the element b. If B_b is not the unique subgroup K of G of order p, then A is periodic. Thus we may assume that $B_b = K$ for each choice of b. Now

$$K \subseteq \bigcap_{b \in B} (B - b).$$

By Lemma 2.8 (on page 18), it follows that the elements of $K \setminus \{0\}$ are periods of B. □

Problem 79 of [41]. Let $C(\infty) = \{a\} = S + T$, where $0 \in S$, $0 \in T$, S consists of p elements such that they generate $\{a\}$. Is then $T = \{pa\}$?

We note that in this book we use Z instead of $C(\infty)$. Here p is used to denote a prime.

We may use the results in Sections 6.2 and 4.1 to show that this question has a positive answer. First, it follows by Theorem 7.14 (on page 154) that T is periodic. So there exists a non-periodic subset T, containing 0 and a positive integer k such that $T = T_1 + kZ$. Then we have a factorization $S + T_1 + kZ = Z$ and so a factorization $\overline{S} + \overline{T}_1 = Z/kZ$, where

$$\overline{S} = (S + kZ)/kZ, \quad \overline{T}_1 = (T_1 + kZ)/kZ.$$

Since $|S| = |\overline{S}| = p$, it follows by Theorem 4.3 (on page 67) that either $\overline{S}$ or $\overline{T}_1$ is periodic. $\overline{T}_1$ being periodic would imply that T_1 had a larger group of periods than kZ. Hence $\overline{S}$ is periodic. Since $\overline{S}$ is of prime order and contains the zero element of Z/kZ, it follows that $\overline{S}$ is the subgroup $\big((k/p)Z\big)/kZ$. Hence all the elements of S belong to $(k/p)Z$. However, S generates Z.

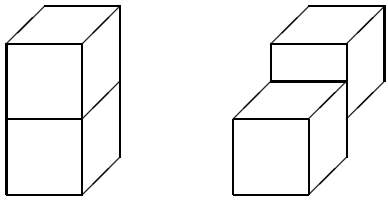

FIGURE 11.1: Twins and not twins.

Hence $k = p$. Therefore, $|T_1| = |\overline{T}_1| = k/p = 1$. Hence $T_1 = \{0\}$. It follows that $T = kZ = \{ka\}$, as required.

Problem 80 of [41]. Let G be finite and

$$G = K + [a_1, n_1] + \cdots + [a_r, n_r].$$

Does it follow that $n_r a_i$ is the difference of two elements of K for some i, $1 \leq i \leq r$?

Here $[a_i, n_i]$ stands for the set

$$\{0, a_i, 2a_i, \ldots, (n_i - 1)a_i\}.$$

This problem is an algebraic version of a geometric conjecture. Two n-dimensional unit cubes in the n-dimensional space form a *twin* if they share an entire $(n-1)$-dimensional face. Figure 11.1 (on page 237) shows a 3-dimensional twin and also a pair of non-twin 3-dimensional cubes. In 1930 O. H. Keller advanced the conjecture that if translated copies of an n-dimensional unit cube tile the whole n-dimensional space, then a twin must appear in this tiling. In 1941, O. Perron using geometric reasoning, verified the conjecture for $n \leq 6$. A typical 2-dimensional cube tiling is presented in Figure 11.2 (on page 238). In 1992, J. C. Lagarias and P. W. Shor [71] refuted Keller's conjecture by exhibiting counter-examples for $n \geq 10$. Later in 2002, J. Mackey [83] improved it to $n \geq 8$. These counter-examples involve groups of type $Z(4) \oplus \cdots \oplus Z(4)$. It is not known if there is a cyclic counter-example. By a result of S. Szabó [153], if there were a counter-example with odd $|G|$, then there would be a cyclic one, too.

Problem 81 of [41]. Is every decomposition $G = S + T$ of a finite G quasi-periodic in the sense that one of S, T, say T, splits into disjoint parts T_i, $1 \leq i \leq m$, $m > 1$ such that there is a subgroup H of order m with $S + t_i = h_i + (S + T_1)$ for different elements $h_i \in H$?

Fuchs refers to Hajós [50] for this problem. Hajós actually asks it for the existence of a periodic subset H rather than a subgroup. Since a non-zero subgroup is periodic, it is clear that a positive answer to Fuchs's question

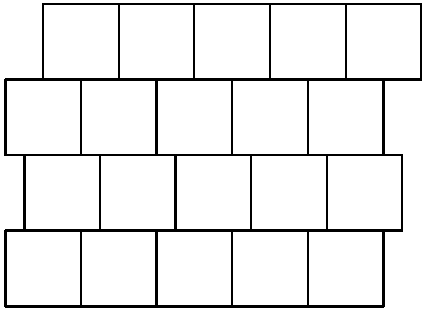

FIGURE 11.2: A 2-dimensional cube tiling.

implies a positive answer to that of Hajós. We have shown in Section 5.2 that the questions are in fact equivalent.

For cyclic groups this problem remains open. The answer is affirmative for groups with the Hajós 2-property and by Corollary 5.4 (on page 118) for groups of square-free order. For non-cyclic groups a counter-example has been given in Section 5.2.

Problem 82 of [41]. Is Theorem 84.6 of [41] true if G is a periodic subset?

We recall that Theorem 84.6 of [41] states that if a group G is represented as a direct sum of a finite number of weakly periodic sets A_i,

$$G = A_1 + \cdots + A_n$$

then at least one of the A_i's is periodic. A subset A of G is defined to be *weakly periodic* if there exists a non-zero element g in G such that A and $g + A$ differ in at most one element (that is, $g + A$ contains at most one element not in A and, conversely, A contains an element that is not in $g + A$). Furthermore, the elements not common to A and $g + A$ belong to the same coset modulo $\langle g \rangle$. The element g is called a *weak period* of A. It is clear that a cyclic subset $\{0, g, \ldots, (r-1)g\}$ is weakly periodic with weak period g.

This problem of Fuchs' is solved by O. Fraser and B. Gordon [39] in the negative. Example 6.1 (on page 127) exhibits one of their counter-examples.

In the particular case when the periodic subset $A_1 + \ldots + A_n$ has a complementer factor in G, then, by Theorem 6.1 (on page 124), the answer is affirmative for Fuchs's question. Theorem 6.1 (on page 124) states this only for finite cyclic group explicitly. However, the result can be extended for all finite abelian groups.

Problem 83 of [41]. Find all non-reduced (especially divisible) groups for which Hajós's theorem holds.

Chapter 8 is devoted to infinite groups. In particular, from Theorem 8.12 (on page 177), it follows that Hajós's theorem holds for groups of type $Z(p_1^\infty) \oplus$

$\cdots \oplus Z(p_s^\infty)$ when $p_1, \ldots, p_s$ are distinct primes. We would like to emphasize that the problem is unsolved if there are equals among the primes $p_1, \ldots, p_s$. Independently of Fuchs's, question in 1949, I. Fáry [34] has pointed out that Hajós's theorem holds for topological groups.

We list open problems related to this section

PROBLEM 11.1 Are there cyclic counter-examples for Keller's conjecture? Are there counter-examples for Keller's conjecture with odd order? □

PROBLEM 11.2 Does Hajós's theorem hold for groups of type $Z(p^\infty) \oplus \cdots \oplus Z(p^\infty)$? □

11.2 Full-rank factorizations

Lemma 2.4 (on page 15) shows that a non-full-rank factorization can be decomposed into a number of factorizations of a smaller group. The procedure then can be repeated if the smaller factorizations are not full-rank. Lemma 2.5 (on page 15) shows how to build a larger factorization from smaller ones. The ultimate building blocks of these constructions are full-rank factorizations. In Section 5.1 we have constructed full-rank factorizations. However, when we use Lemma 5.2 (on page 94) to construct full-rank factorization, the resulting factorization is always periodic. A factorization with a periodic factor easily reduces for factorizations of smaller subgroups until none of the factors is periodic. So only non-periodic full-rank factorizations can be considered to be ultimate building blocks.

We mention another reason behind construction full-rank non-periodic factorizations. A perfect error correcting code can be viewed as a factorization $G = A + B$, where G is the additive part of a finite linear space and A is an error sphere. The code itself is the subset B. Perfect error correcting codes are rare. But there are many 1-error correcting binary codes. These are the so-called Hamming codes. When B is a linear subspace of G, we talk about linear codes. In this case B is a subgroup of G and we call it a subgroup code. Now H, the subgroup of periods of B, and K, the span of B, are identical. The wider the subgroups H and K differ, the wider B differs form being a subgroup code.

We can particularize the situation to the case when G is an elementary 2-group of rank n. Let k, l be the ranks of K and L, respectively. The so-called rank-kernel problem from coding theory asks for determining the possible (n, k, l) values. For more details of the rank-kernel problem, see [55]. The next result is about non-periodic full-rank factorizations.

THEOREM 11.2

Let $r \geq 3$ be an integer and let G be a group of type $Z(n_1) \oplus \cdots \oplus Z(n_r)$. If each n_i is a product of at least two (not necessarily distinct) primes, then there is a normalized factorization $G = A + B$ such that $\langle A \rangle = \langle B \rangle = G$ and none of the factors are periodic.

PROOF Let G be a group of type $Z(n_1) \oplus \cdots \oplus Z(n_r)$ with basis elements $x_1, \ldots, x_r$ such that $|x_1| = n_1, \ldots, |x_r| = n_r$. Assume that $r \geq 3$ and $n_i = k_i m_i$, where k_i is the least prime divisor of n_i and $m_i \geq k_i$ for each i, $1 \leq i \leq r$. Let f be a cyclic permutation of the indices $1, \ldots, r$. For the sake of definiteness let f be the cyclic permutation

$$\begin{bmatrix} 1 & 2 & \ldots & r-1 & r \\ 2 & 3 & \ldots & r & 1 \end{bmatrix}.$$

Set

$$\begin{aligned} A_i &= \{0, x_i, 2x_i, \ldots, (k_i - 1)x_i\}, \ 1 \leq i \leq r, \\ H_i &= \langle k_i x_i \rangle, \qquad\qquad\qquad\quad 1 \leq i \leq r, \\ A &= A_1 + \cdots + A_r, \\ H &= H_1 + \cdots + H_r. \end{aligned}$$

Clearly $Z(n_i) = A_i + H_i$ is a normalized factorization of $Z(n_i) = \langle x_i \rangle$ and so

$$\begin{aligned} A + H &= (A_1 + \cdots + A_r) + (H_1 + \cdots + H_r) \\ &= (A_1 + H_1) + \cdots + (A_r + H_r) \\ &= \langle x_1 \rangle + \cdots + \langle x_r \rangle \\ &= G. \end{aligned}$$

Consequently, $G = A + H$ is a normalized factorization of G. Plainly the subgroup H is partitioned into cosets modulo the subgroup H_i and $k_{f(i)} x_{f(i)} \in H$. Let us consider the coset $H_i + k_{f(i)} x_{f(i)}$ in this partition. The element $k_{f(i)} x_{f(i)} + x_i$ does not belong to H, and so the coset $H_i + k_{f(i)} x_{f(i)} + x_i$ is not a member of the above partition. The next computation shows that x_i is a period of $A + H_i$. Indeed,

$$\begin{aligned} A + H_i &= \Big(\sum_{j=1}^{r} A_i \Big) + H_i \\ &= \Big(\sum_{\substack{j=1 \\ j \neq i}}^{r} A_i \Big) + (A_i + H_i) \\ &= \Big(\sum_{\substack{j=1 \\ j \neq i}}^{r} A_i \Big) + \langle x_i \rangle. \end{aligned}$$

Therefore

$$A + H_i + k_{f(i)} x_{f(i)} = A + H_i + k_{f(i)} x_{f(i)} + x_i.$$

TABLE 11.1: Equation relations among i, j, $f(i)$, and $f(j)$

	i	j	$f(i)$	$f(j)$
i	$=$	$\neq$	$\neq$	
j	$\neq$	$=$		$\neq$
$f(i)$	$\neq$		$=$	$\neq$
$f(j)$		$\neq$	$\neq$	$=$

We claim that the sets

$$A + H_i + k_{f(i)}x_{f(i)}, \quad A + H_j + k_{f(j)}x_{f(j)}$$

are disjoint for each i, j, $1 \leq i, j \leq r$, $i \neq j$. In order to prove the claim, assume that g is a common element of the two sets. Now g can be represented in the forms

$$a_i + b_i k_i x_i + k_{f(i)}x_{f(i)}, \quad a_j + b_j k_j x_j + k_{f(j)}x_{f(j)},$$

where $a_i, a_j \in A$, $0 \leq b_i \leq m_i - 1$, $0 \leq b_j \leq m_j - 1$. As $G = A + H$ is a factorization of G from

$$g = \underbrace{a_i}_{\in A} + \underbrace{b_i k_i x_i + k_{f(i)}x_{f(i)}}_{\in H} = \underbrace{a_j}_{\in A} + \underbrace{b_j k_j x_j + k_{f(j)}x_{f(j)}}_{\in H},$$

it follows that $a_i = a_j$ and

$$b_i k_i x_i + k_{f(i)}x_{f(i)} = b_j k_j x_j + k_{f(j)}x_{f(j)}. \tag{11.1}$$

To analyze equation (11.1) we use the fact that $x_1, \ldots, x_r$ form a basis of G. The permutation f has no fixed point, so it follows that $i \neq f(i)$, $j \neq f(j)$. Using that $i \neq j$ we get that $f(i) \neq f(j)$. The situation is summarized in Table 11.1 (on page 241).

If $f(i) \neq j$, then, considering $k_{f(i)}x_{f(i)}$ on the left-hand side of equation (11.1), we can draw the conclusion that $k_{f(i)}x_{f(i)} = 0$, which gives the contradiction $n_{f(i)} \mid k_{f(i)}$. If $f(j) \neq i$, then, considering $k_{f(j)}x_{f(j)}$ on the right-hand side of equation (11.1), we can draw the conclusion that $k_{f(j)}x_{f(j)} = 0$, which gives the contradiction $n_{f(j)} \mid k_{f(j)}$. Thus we may assume that $i = f(j)$, $j = f(i)$. Now $i = f(i) = f(f(i))$ and so (i, j) is a cycle of f. This contradicts the fact that f is a cyclic permutation of more than two elements.

We construct the factor B from the subgroup H by removing the sets $H_i + k_{f(i)}x_{f(i)}$ and adding the sets $H_i + k_{f(i)}x_{f(i)} + x_i$ for each i, $1 \leq i \leq r$. The computation

$$A + B = A + \Big[H \cup \Big(\bigcup_{i=1}^{r} H_i + k_{f(i)}x_{f(i)} + x_i\Big)$$

$$\begin{aligned}
&\setminus\Big(\bigcup_{i=1}^{r} H_i + k_{f(i)}x_{f(i)}\Big)\Big] \\
&= (A+H) \cup \Big(\bigcup_{i=1}^{r}(A + H_i + k_{f(i)}x_{f(i)} + x_i)\Big) \\
&\quad \setminus\Big(\bigcup_{i=1}^{r}(A + H_i + k_{f(i)}x_{f(i)})\Big) \\
&= A + H \\
&= G.
\end{aligned}$$

shows that $G = A + B$ is a factorization of G.

Next we verify that $\langle A\rangle = \langle B\rangle = G$. Clearly $x_1, \ldots, x_r \in A$, which implies that $\langle A\rangle = G$. Note that $x_i, k_{f(i)}x_{f(i)} + x_i \in B$ and so $k_{f(i)}x_{f(i)} \in \langle B\rangle$. Now $k_{f(i)}x_{f(i)} + x_i \in B$ and $k_{f(i)}x_{f(i)} \in \langle B\rangle$ give that $x_i \in \langle B\rangle$ for each i, $1 \le i \le r$ and so $\langle B\rangle = G$.

We are going to prove that A is not periodic. Assume the contrary, that A is periodic and g is a period of A. We may assume that the order of g is a prime, say $|g| = p$. As $A + g = A$, there is an $a \in A$ such that $0 + g = a$. There are integers $a_1, \ldots, a_r$ such that $a = a_1x_1 + \cdots + a_rx_r$ and

$$0 \le a_1 \le k_1 - 1, \ldots, 0 \le a_r \le k_r - 1.$$

Multiplying by p we get $0 = pa_1x_1 + \cdots + pa_rx_r$. Since $x_1, \ldots, x_r$ is a basis of G, it follows that $pa_ix_i = 0$ for each i, $1 \le i \le r$. We distinguish two cases depending on if p divides the order of x_i or not. If p does not divide the order of x_i, then $pa_ix_i = 0$ implies $a_ix_i = 0$. Therefore $n_i \mid a_i$. This gives the contradiction that $n_i \le a_i$. Thus we may assume that $p \mid n_i$. Now $p \le m_i$ as we have chosen k_i to be the least prime divisor of n_i. Using the facts that $n_i = k_im_i$, $a_i < k_i$, $p \le m_i$, we get the contradiction $n_i \le pa_i < k_im_i = n_i$.

Finally we show that B is not periodic. Assume the contrary, that B is periodic. Let g be a period of B. We may assume that the order of g is a prime, say $|g| = p$. First let us consider the case when $g \notin H$. There is a $b \in B$ such that $0 + g = b$. Now $b \notin H$ and so $b = tk_{f(i)}x_{f(i)} + x_i$ for some integer t, $0 \le t \le m_{f(i)} - 1$. Multiplying by p gives that $0 = ptk_{f(i)}x_{f(i)} + px_i$. As $x_{f(i)}, x_i$ are part of a basis of G, it follows that $px_i = 0$ and we get the contradiction that $n_i \mid p$. Thus we may assume that $g \in H$.

Consider the element $k_{f(1)}x_{f(1)} + x_1 = k_2x_2 + x_1$. As $k_2x_2 + x_1 \notin H$, it follows that $k_2x_2 + x_1 + g \notin H$. There is an element $tk_{f(i)}x_{f(i)} + x_i$ such that

$$k_2x_2 + x_1 + g = tk_{f(i)}x_{f(i)} + x_i.$$

It follows that $x_1 - x_i \in H$. This implies $i = 1$. Now

$$g = tk_{f(i)}x_{f(i)} - k_2x_2 = tk_2x_2 - k_2x_2$$

and so $g \in H_2$.

Consider the element $k_{f(2)}x_{f(2)} + x_2 = k_3x_3 + x_2$. As $k_3x_3 + x_2 \notin H$ and $g \in H$, it follows that $k_3x_3 + x_2 + g \notin H$. There is an element $tk_{f(i)}x_{f(i)} + x_i$ such that

$$k_3x_3 + x_2 + g = tk_{f(i)}x_{f(i)} + x_i.$$

It follows that $x_2 - x_i \in H$. This implies $i = 2$. Therefore, $g = tk_3x_3 - k_3x_3$ and so $g \in H_3$. This leads to the $g \in H_2 \cap H_3 = \{0\}$ contradiction. □

The next exercise suggests an alternative way to show that the factor A is not periodic in the previous proof.

EXERCISE 11.1 Note that A is a direct product of non-periodic cyclic subsets $A_1, \ldots, A_r$. Suppose that A is periodic, then use Theorem 6.1 (on page 124) to show that one of $A_1, \ldots, A_r$ is periodic. □

11.3 Z-subsets

This book deals with the factorization theory of abelian groups, focusing mainly on results related to finite cyclic groups. One might have the impression that these results must be trivial. Indeed, there are results that become trivial or almost trivial when we restrict them to the case of finite cyclic groups. In these cases, the difficulty lies in the non-cyclic case. On the other hand, there are problems where the cyclic case is hard. For instance, we do not know if there is any non-quasi-periodic factorization for a finite cyclic group. Similarly, we do not know if there is a cyclic counter-example for Keller's conjecture. In the remaining part of this section we will touch upon problems that are fairly straightforward for the cyclic case.

A classical theorem of G. Hajós [48] asserts that if a finite abelian group is a direct sum of cyclic subsets, then at least one of the factors must be a subgroup. A subset A of a finite abelian group G is called cyclic if it is in the form

$$A = \{0, a, 2a, \ldots, (r-1)a\}.$$

Here a is a non-zero element of G and $r \geq 2$ is an integer not exceeding the order of the element a. Clearly A is a subgroup of G if and only if $r = |g|$. Theorem 6.2 (on page 125) generalizes Hajós's theorem for cyclic groups. The proof shows that, in case of Hajós's theorem, the difficulty clearly lies in the non-cyclic case.

In 1965 L. Rédei [107] proved the following theorem. If $G = A_1 + \cdots + A_k$ is a normalized factorization of a finite abelian group G, where each $|A_i|$ is a prime, then at least one of the factors $A_1, \ldots, A_k$ is a subgroup of G. It is easy to prove Rédei's theorem for cyclic groups.

THEOREM 11.3

Let G be a finite cyclic group and let $G = A_1 + \cdots + A_k$ be a normalized factorization of G, where $|A_i|$ is a prime for each i, $1 \leq i \leq k$. Then at least one of the factors $A_1, \ldots, A_k$ must be a subgroup of G.

PROOF Let $A_1 = \{a_1, \ldots, a_p\}$, where p is a prime and $a_1 = 0$. As G is cyclic and p is a prime divisor of $|G|$, there is a unique subgroup H of G for which $|H| = p$. If $|a_i| = p$ for each i, $2 \leq i \leq p$, then A_1 is equal to H and we are done. Thus we may assume that $|a_2| \neq p$. Set $A_1' = \{0, a_2, 2a_2, \ldots, (p-1)a_2\}$. Clearly A_1' is not a subgroup of G. By Lemma 8.4 (on page 177), in the factorization $G = A_1 + \cdots + A_k$, the factor A_1 can be replaced by A_1' to get the normalized factorization $G = A_1' + A_2 + \cdots + A_k$. If there is no subgroup among the factors $A_2, \ldots, A_k$, then, repeating the above argument, we get a normalized factorization $G = A_1' + \cdots + A_k'$, where each factor is a non-subgroup cyclic subset. This contradicts Hajós's theorem. Thus at least one of the factors $A_1, \ldots, A_k$ must be a subgroup of G. □

The following is an unsolved problem of K. Corrádi [23]. Let $G = A_1 + \cdots + A_k$ be a factorization of a finite abelian group G and let $K_1, \ldots, K_k$ be the Corrádi subgroups of the factors $A_1, \ldots, A_k$, respectively. Does it follow that $K_i = \{0\}$ for some i, $1 \leq i \leq k$?

By considering a character χ of G that is a one-to-one map from G to the multiplicative group of the $|G|$th roots of unity, the reader can verify that the answer is affirmative when G is a finite cyclic group.

In connection with tiling the n-dimensional space by crosses and semi-crosses, in Chapter 10 we introduced the concept of splitting an abelian group. Later in the same chapter we saw that splitting was connected to certain error correcting integer codes. A splitting $G \setminus \{0\} = MS$ is called non-singular if every integer in M is relatively prime to $|G|$. Otherwise, it is called singular. It is shown in [44] that a multiplier set M splits the finite abelian group G non-singularly if and only if M splits $Z(p)$ for each prime divisor p of $|G|$. Thus the problem of the existence of non-singular splittings reduces to the problem of the existence of splitting of cyclic groups of prime order.

A singular splitting $G \setminus \{0\} = MS$ is called purely singular if every prime divisor of $|G|$ divides some elements in M. It is shown in [57] that the study of splitting can be reduced to the study of non-singular and purely singular splittings.

For the particular case when M is $\{-k, \ldots, -1, 1, \ldots, k\}$ or $\{1, 2, \ldots, k\}$, [57] proves that if M splits a finite abelian group of order n, then M splits $Z(n)$ too. In other words, the problem of whether a cross or semicross tile the n-dimensional space can be reduced to the problem of splitting finite cyclic groups. It was shown in [154], how thinly Z-lattice translated copies of an $(n, 2)$-semicross can cover the n-dimensional space, can also be reduced to a covering problem of cyclic groups.

If $G = A + B$ is a normalized factorization of a finite abelian group G and k is an integer relatively prime to $|A|$, then by Theorem 3.17 (on page 58), in the factorization $G = A + B$, factor A can be replaced by kA to get the factorization $G = kA + B$. This replacement sometimes helps us to gain some insight into the structure of the factorization $G = A+B$. However, if $kA = A$, then the replacement cannot provide any information which was not already contained in $G = A + B$. This motivates the following definition. Let A be a normalized subset of a finite abelian group G. If $kA = A$ for each integer k, then we call A a *Z-subset*. Clearly a Z-subset of G is a union of cyclic subgroups of G. Z-subsets were introduced by C. Okuda [95] in 1975. He characterized all finite abelian groups that admit only periodic factorizations into Z-subsets. We will show that Okuda's result particularized to finite cyclic groups can be proved in a relatively straightforward manner.

LEMMA 11.1

Let G be a finite abelian group. Let $G = A_1+A_2$ be a normalized factorization of G, where A_1, A_2 are Z-subsets. Suppose that $G = K_1+K_2$ is a factorization of G, where K_1, K_2 are subgroups such that $|K_1|$, $|K_2|$ are relatively primes. Then

$$A_1 = (K_1 \cap A_1) + (K_2 \cap A_1), \tag{11.2}$$

$$A_2 = (K_1 \cap A_2) + (K_2 \cap A_2), \tag{11.3}$$

$$K_1 = (K_1 \cap A_1) + (K_1 \cap A_2), \tag{11.4}$$

$$K_2 = (K_2 \cap A_1) + (K_2 \cap A_2) \tag{11.5}$$

are factorizations.

PROOF Since $(K_1 \cap A_1) \subseteq K_1$, $(K_2 \cap A_1) \subseteq K_2$, and the sum $K_1 + K_2$ is direct, it follows that the sum $(K_1 \cap A_1) + (K_2 \cap A_1)$ is direct. Similar reasonings give that the sums on the right-hand sides of (11.3), (11.4), and (11.5) are direct.

To prove $A_1 \subseteq (K_1 \cap A_1) + (K_2 \cap A_1)$, choose an element $a_1 \in A_1$. Since $G = K_1 + K_2$ is a factorization of G, a_1 can be represented in the form

$$a_1 = k_1 + k_2, \quad k_1 \in K_1, \quad k_2 \in K_2.$$

Note that $|k_1|$, $|k_2|$ are relatively primes. There is an integer t_1 such that $t_1|k_2| \equiv 1 \pmod{|k_1|}$. Multiplying by $t_1|k_2|$ gives that

$$\begin{aligned}(t_1|k_2|)a_1 &= (t_1|k_2|)k_1 + (t_1|k_2|)k_2 \\ &= (t_1|k_2|)k_1 \\ &= k_1.\end{aligned}$$

As $(t_1|k_2|)a_1 \in A_1$, it follows that $k_1 \in A_1$ and so $k_1 \in (K_1 \cap A_1)$. In a similar way we get that $k_2 \in (K_2 \cap A_1)$. Thus $a_1 \in (K_1 \cap A_1) + (K_2 \cap A_1)$ and so $A_1 \subseteq (K_1 \cap A_1) + (K_2 \cap A_1)$.

To show that $A_1 \supseteq (K_1 \cap A_1) + (K_2 \cap A_1)$, choose $k_1 \in (K_1 \cap A_1)$ and $k_2 \in (K_2 \cap A_1)$. Since $G = A_1 + A_2$ is a factorization, the element $k_1 + k_2$ can be represented in the form

$$k_1 + k_2 = a_1 + a_2, \quad a_1 \in A_1, \quad a_2 \in A_2.$$

As $G = K_1 + K_2$ is a factorization, a_1, a_2 can be represented in the forms

$$\begin{aligned} a_1 &= k_{1,1} + k_{1,2}, \quad k_{1,1} \in K_1, \quad k_{1,2} \in K_2, \\ a_2 &= k_{2,1} + k_{2,2}, \quad k_{2,1} \in K_1, \quad k_{2,2} \in K_2. \end{aligned}$$

As we have seen earlier, from these we get that

$$\begin{aligned} k_{1,1} &\in (K_1 \cap A_1), \quad k_{1,2} \in (K_2 \cap A_1), \\ k_{2,1} &\in (K_1 \cap A_2), \quad k_{2,2} \in (K_2 \cap A_2). \end{aligned}$$

Now

$$\begin{aligned} k_1 + k_2 &= a_1 + a_2 \\ &= (k_{1,1} + k_{1,2}) + (k_{2,1} + k_{2,2}) \\ &= (k_{1,1} + k_{2,1}) + (k_{1,2} + k_{2,2}). \end{aligned}$$

Since $G = K_1 + K_2$ is a factorization from

$$\underbrace{k_1}_{\in K_1} + \underbrace{k_2}_{\in K_2} = \underbrace{(k_{1,1} + k_{2,1})}_{\in K_1} + \underbrace{(k_{1,2} + k_{2,2})}_{\in K_2},$$

it follows that

$$k_1 = k_{1,1} + k_{2,1}, \quad k_2 = k_{1,2} + k_{2,2}.$$

Since $G = A_1 + A_2$ is a factorization from

$$\underbrace{k_1}_{\in A_1} = \underbrace{k_{1,1}}_{\in A_1} + \underbrace{k_{2,1}}_{\in A_2},$$

$$\underbrace{k_2}_{\in A_1} = \underbrace{k_{1,2}}_{\in A_1} + \underbrace{k_{2,2}}_{\in A_2},$$

it follows that $k_{2,1} = k_{2,2} = 0$. Thus $k_1 + k_2 = k_{1,1} + k_{1,2}$. Using $k_{1,1} + k_{1,2} \in A_1$, we get $A_1 \supseteq (K_1 \cap A_1) + (K_2 \cap A_1)$. Equation (11.3) can be verified in a similar way.

Let us turn to equation (11.4). To verify $K_1 \subseteq (K_1 \cap A_1) + (K_1 \cap A_2)$, choose a $k_1 \in K_1$. As $G = A_1 + A_2$ is a factorization, k_1 can be represented in the form

$$k_1 = a_1 + a_2, \quad a_1 \in A_1, \quad a_2 \in A_2.$$

Since $G = K_1 + K_2$ is a factorization, a_1, a_2 can be represented in the forms

$$\begin{aligned} a_1 &= k_{1,1} + k_{1,2}, \quad k_{1,1} \in K_1, \quad k_{1,2} \in K_2, \\ a_2 &= k_{2,1} + k_{2,2}, \quad k_{2,1} \in K_1, \quad k_{2,2} \in K_2. \end{aligned}$$

As we have seen earlier, we can draw the conclusion that

$$k_{1,1} \in (K_1 \cap A_1), \quad k_{1,2} \in (K_2 \cap A_1),$$
$$k_{2,1} \in (K_1 \cap A_2), \quad k_{2,2} \in (K_2 \cap A_2).$$

Then

$$\begin{aligned} k_1 &= a_1 + a_2 \\ &= (k_{1,1} + k_{1,2}) + (k_{2,1} + k_{2,2}) \\ &= (k_{1,1} + k_{2,1}) + (k_{1,2} + k_{2,2}). \end{aligned}$$

Since $G = K_1 + K_2$ is a factorization from

$$\underbrace{k_1}_{\in K_1} = \underbrace{(k_{1,1} + k_{2,1})}_{\in K_1} + \underbrace{(k_{1,2} + k_{2,2})}_{\in K_2},$$

it follows that $k_1 = k_{1,1} + k_{2,1}$. Using $k_{1,1} \in (K_1 \cap A_1)$, $k_{2,1} \in (K_1 \cap A_2)$ we get $k_1 \in (K_1 \cap A_1) + (K_1 \cap A_2)$ and so $K_1 \subseteq (K_1 \cap A_1) + (K_1 \cap A_2)$.

The containment $K_1 \supseteq (K_1 \cap A_1) + (K_1 \cap A_2)$ plainly holds as $(K_1 \cap A_1) \subseteq K_1$, $(K_1 \cap A_2) \subseteq K_1$ and K_1 is a subgroup. Equation (11.5) can be verified in a similar way. □

Let G be a finite abelian group. We say that G is *Z-good* if, from each factorization $G = A + B$, where A, B are Z-subsets, it follows that either A or B is periodic. If G admits factorization $G = A + B$ into non-periodic Z-subsets, then G is called *Z-bad*.

LEMMA 11.2

Let the finite abelian group G be the direct sum of the subgroups H, K such that $|H|$ and $|K|$ are relatively primes. If H is Z-good, then so is G.

PROOF Consider a factorization $G = A + B$, where A, B are Z-subsets. Assume that H is Z-good. We want to prove that A or B is periodic. From the factorizations $G = H + K$, $G = A + B$, by Lemma 11.1 (on page 245), it follows that

$$A = (H \cap A) + (K \cap A), \tag{11.6}$$
$$B = (H \cap B) + (K \cap B), \tag{11.7}$$
$$H = (H \cap A) + (H \cap B), \tag{11.8}$$
$$K = (K \cap A) + (K \cap B) \tag{11.9}$$

are factorizations. If $H \cap A = \{0\}$, then, by equation (11.8), $H = H \cap B$. By equation (11.7), $B = H + (K \cap B)$ and B is periodic. The subgroup of periods of B contains H. Similarly, if $H \cap B = \{0\}$, then, by equation (11.8),

$H = H \cap A$. By equation (11.6), $A = H + (K \cap A)$ and so A is periodic. Thus we may assume that $H \cap A \neq \{0\}$ and $H \cap B \neq \{0\}$.

Note that $H \cap A$, $H \cap B$ are Z-subsets of H. Since H is Z-good, from factorization (11.8) we get that $H \cap A$ or $H \cap B$ is periodic. We may assume that $H \cap A$ is periodic since this is only a matter of interchanging A and B in the factorization $G = A + B$. Let h be a period of $H \cap A$. The computation

$$\begin{aligned} h + A &= h + [(H \cap A) + (K \cap A)] \\ &= [h + (H \cap A)] + (K \cap A) \\ &= (H \cap A) + (K \cap A) \\ &= A \end{aligned}$$

shows that h is a period of A. □

LEMMA 11.3

Let the finite abelian group G be the direct sum of the subgroups H and K. If H, K are both Z-bad, then so is G.

PROOF There are non-periodic Z-subsets A_1, B_1, A_2, B_2 such that $H = A_1 + B_1$, $K = A_2 + B_2$ are factorizations. Set $A = A_1 + A_2$, $B = B_1 + B_2$. Note that A and B are Z-subsets of G. The computation

$$\begin{aligned} G &= H + K \\ &= (A_1 + B_1) + (A_2 + B_2) \\ &= (A_1 + A_2) + (B_1 + B_2) \\ &= A + B \end{aligned}$$

shows that $G = A + B$ is a factorization of G. Note that the sets A_1 and A_2 satisfy the hypotheses of Theorem 3.1 and so $A = A_1 + A_2$ is not periodic. A similar argument gives that B is not periodic either. □

Let G be a finite abelian group and let $p_1, \ldots, p_s$ be the distinct prime divisors of $|G|$. There is a unique subgroup L_i of G that contains each p_i-element of G. Here $|L_i|$ is a power of p_i and G is the direct sum of the subgroups $L_1, \ldots, L_s$. The subgroup L_i is called the *p_i-component* of G and the subgroup $L_1 + \cdots + L_{i-1} + L_{i+1} + \cdots + L_s$ is called the *p_i'-component* of G.

COROLLARY 11.1

A finite abelian group G is Z-good if and only if at least one p-component of G is Z-good.

PROOF Let p be a prime divisor of $|G|$. Let H be the p-component of G and let K be the p'-component of G. Assume that H is Z-good. Then, by Lemma 11.2 (on page 247), G is Z-good.

Next let $p_1, \ldots, p_s$ be the distinct prime divisors of $|G|$ and let L_i be the p_i-component of G. Assume that L_i is Z-bad for each i, $1 \leq i \leq s$. By Lemma 11.3 (on page 248), $L_1 + L_2$ is Z-bad. Then $(L_1 + L_2) + L_3$ is Z-bad. Continuing in this way, we get that $(L_1 + \cdots + L_{s-1}) + L_s = G$ is Z-bad. □

COROLLARY 11.2
Every finite cyclic group is Z-good.

PROOF Let G be a finite cyclic group and let $p_1, \ldots, p_s$ be the distinct prime divisors of $|G|$. Let L_i be the p_i-component of G. Now L_i is a cyclic subgroup whose order is a power of p_i. By Theorem 4.4, L_i is Z-good. Then, by Lemma 11.2 (on page 247), G is Z-good. □

Next we will show how to construct factorizations consisting of non-periodic Z-sets. Let p be a prime such that $p \geq 3$. Let G be a group of type $Z(p) \oplus Z(p) \oplus Z(p) \oplus Z(p)$ with basis elements x, y, u, v. Set

$$A = \langle x \rangle \cup \langle x + y \rangle \cup \cdots \cup \langle x + (p-1)y \rangle \cup \langle y + u \rangle,$$
$$B = \langle u \rangle \cup \langle 2y + u + v \rangle \cup \cdots \cup \langle 2y + u + (p-1)v \rangle \cup \langle v \rangle.$$

It is clear that neither A nor B is periodic.

LEMMA 11.4
$G = A + B$ is a factorization of G.

PROOF It is enough to verify that $|A| = |B| = p^2$ and $(A-A) \cap (B-B) = (A+A) \cap (B+B) = \{0\}$. We will verify that the subgroups

$$\langle x \rangle, \langle x + y \rangle, \ldots, \langle x + (p-1)y \rangle, \langle y + u \rangle$$

are pair-wise distinct. From this it follows that $|A| = (p+1)(p-1) + 1 = p^2$. It remains to check that

$$\begin{aligned}
\langle x \rangle \cap \langle x + \alpha y \rangle &= \{0\}, 1 \leq \alpha \leq p-1, \\
\langle x \rangle \cap \langle y + u \rangle &= \{0\}, \\
\langle x + \alpha y \rangle \cap \langle x + \beta y \rangle &= \{0\}, 1 \leq \alpha < \beta \leq p-1, \\
\langle x + \alpha y \rangle \cap \langle y + u \rangle &= \{0\}.
\end{aligned}$$

As an illustration let us check the third one. Suppose that

$$i(x + \alpha y) - j(x + \beta y) = 0.$$

This is equivalent to the system of equations

$$i - j = 0, \quad \alpha i - \beta j = 0.$$

The only solution of this system is $i = j = 0$, as required. (The system of equations is understood in the finite field of order p.) A similar argument gives that $|B| = p^2$.

We would like to prove that $(A+A)\cap(B+B) = \{0\}$. It is enough to check the following 16 equations:

$$\begin{aligned}
\langle x, x+\alpha y\rangle \cap \langle u, 2y+u+\gamma v\rangle &= \{0\},\\
\langle x, x+\alpha y\rangle \cap \langle u, v\rangle &= \{0\},\\
\langle x, x+\alpha y\rangle \cap \langle 2y+u+\gamma v, 2y+u+\delta v\rangle &= \{0\},\\
\langle x, x+\alpha y\rangle \cap \langle 2y+u+\gamma v, v\rangle &= \{0\},\\
\langle x, y+u\rangle \cap \langle u, 2y+u+\gamma v\rangle &= \{0\},\\
\langle x, y+u\rangle \cap \langle u, v\rangle &= \{0\},\\
\langle x, y+u\rangle \cap \langle 2y+u+\gamma v, 2y+u+\delta v\rangle &= \{0\},\\
\langle x, y+u\rangle \cap \langle 2y+u+\gamma v, v\rangle &= \{0\},\\
\langle x+\alpha y, x+\beta y\rangle \cap \langle u, 2y+u+\gamma v\rangle &= \{0\},\\
\langle x+\alpha y, x+\beta y\rangle \cap \langle u, v\rangle &= \{0\},\\
\langle x+\alpha y, x+\beta y\rangle \cap \langle 2y+u+\gamma v, 2y+u+\delta v\rangle &= \{0\},\\
\langle x+\alpha y, x+\beta y\rangle \cap \langle 2y+u+\gamma v, v\rangle &= \{0\},\\
\langle x+\alpha y, y+u\rangle \cap \langle u, 2y+u+\gamma v\rangle &= \{0\},\\
\langle x+\alpha y, y+u\rangle \cap \langle u, v\rangle &= \{0\},\\
\langle x+\alpha y, y+u\rangle \cap \langle 2y+u+\gamma v, 2y+u+\delta v\rangle &= \{0\},\\
\langle x+\alpha y, y+u\rangle \cap \langle 2y+u+\gamma v, v\rangle &= \{0\}.
\end{aligned}$$

In order to check the 4th equation, suppose that

$$ix + j(x+\alpha y) - k(2y+u+\gamma v) - lv = 0.$$

This means that

$$\begin{aligned}
i + \ \ j \qquad\qquad &= 0,\\
\alpha j - 2k \qquad &= 0,\\
k \qquad &= 0,\\
\gamma k + l &= 0.
\end{aligned}$$

A routine computation shows that the system has the only solution $i = j = k = l = 0$, as required. A similar argument can be used to verify all the 16 equations. ∎

We give a second proof of Lemma 11.4 (on page 249) which uses characters.

PROOF Choose a root of unity ρ of order p and define a character χ of G by

$$\chi(x) = \rho^a, \quad \chi(y) = \rho^b, \quad \chi(u) = \rho^c, \quad \chi(v) = \rho^d,$$

where $0 \le a, b, c, d \le p-1$. We will show that if χ is not the principal character of G, then either $\chi(A) = 0$ or $\chi(B) = 0$. Using that $|A| = |B| = p^2$, Theorem 3.7 (on page 46) will imply that $G = A + B$ is a factorization of G.

Note that

$$\chi(A) = -p + \sum_{j=0}^{p-1}\sum_{i=0}^{p-1} \rho^{i(a+bj)} + \sum_{i=0}^{p-1} \rho^{i(b+c)},$$
$$\chi(B) = -p + \sum_{i=0}^{p-1} \rho^{ic} + \sum_{j=1}^{p-1}\sum_{i=0}^{p-1} \rho^{i(2b+c+dj)} + \sum_{i=0}^{p-1} \rho^{id}.$$

We distinguish 16 cases depending on whether the exponents a, b, c, d are equal to zero or distinct from zero. If $a = b = c = d = 0$, then χ is the principal character of G and we have nothing to do. We are left with 15 cases. We settle only three of them since the other cases are more or less similar.

Suppose $a = 0$, $b = 0$, $c = 0$, $d \neq 0$. Now

$$p = \sum_{i=0}^{p-1} \rho^{ic},$$
$$0 = \sum_{i=0}^{p-1} \rho^{i(2b+c+dj)}, \quad 1 \leq j \leq p-1,$$
$$0 = \sum_{i=0}^{p-1} \rho^{id}$$

and so $\chi(B) = 0$, as required.

Suppose $a \neq 0$, $b \neq 0$, $c = 0$, and $d = 0$. As $b \neq 0$, b is relatively prime to p and there is a unique β such that $1 \leq \beta \leq p-1$ and $a + b\beta \equiv 0 \pmod{p}$. Now

$$\sum_{i=0}^{p-1} \rho^{i(a+bj)} = \begin{cases} 0, & \text{if} \quad j \neq \beta, \\ p, & \text{if} \quad j = \beta, \end{cases}$$

$$0 = \sum_{i=0}^{p-1} \rho^{i(b+c)}$$

and so $\chi(A) = 0$, as required.

Finally, suppose that $a \neq 0$, $b \neq 0$, $c \neq 0$, and $d \neq 0$. As $d \neq 0$, d is relatively prime to p and there is a unique δ such that $1 \leq \delta \leq p-1$ and $2b + c + d\delta \equiv 0 \pmod{p}$. Now

$$\sum_{i=0}^{p-1} \rho^{i(2b+c+dj)} = \begin{cases} 0, & \text{if} \quad j \neq \delta, \\ p, & \text{if} \quad j = \delta, \end{cases}$$

$$0 = \sum_{i=0}^{p-1} \rho^{ic},$$

$$0 = \sum_{i=0}^{p-1} \rho^{id}$$

and so $\chi(B) = 0$, as required. □

PROBLEM 11.3 Is there any non-quasi-periodic factorization of a finite abelian group into Z-subset factors? □

References

[1] K. Amin, K. Corrádi, and A. D. Sands, The Hajós property for 2-groups, *Acta Math. Hungar.* **89** (2000), 189–198.

[2] I. Anderson, *Combinatorial Designs and Tournaments*, Clarendon Press, Oxford, 1997.

[3] G. Bacsó, L. Héthelyi, and P. Sziklai, New near-factorizations of finite groups (in print).

[4] J. Berstel and D. Perrin, *Theory of Codes*, Academic Press, New York, 1985.

[5] A. Biró, Divisibility of integer polynomials and tiling of the integers, *Acta Arithmetica* **118** (2005), 117–127.

[6] A. Blokhuis, G. Kiss, I. Kovács, A. Malnič, D. Marušič, and J. Ruff, Semiovals contained in the union of three concurrent lines, *J. of Comb. Designs* **15** (2007), 491–501.

[7] O. Bodoni and E. Rivals, Tiling an interval of the discrete line, in: *Combinatorial Pattern Matching*, Lecture Notes in Comp. Sci., Springer, New York, 2006, 117–128.

[8] V. Božović and N. Pace, On group factorizations using free mappings, *J. of Algebra and Its Appl.* **7** (2008), 647–662.

[9] N. G. de Bruijn, On bases for the set of integers, *Publ. Math. Debrecen* **1** (1950), 232–242.

[10] N. G. de Bruijn, On the factorization of finite abelian groups, *Indag. Math. Kon. Ned. Akad. Wetersch.* **15** (1953), 258–264.

[11] N. G. de Bruijn, On the factorization of finite cyclic groups, *Indag. Math. Kon. Ned. Akad. Wetersch.* **15** (1953), 370–377.

[12] N. G. de Bruijn, On number systems, *Nieuw Arch. Wisk.* **3** (1956), 15–17.

[13] N. G. de Bruijn, Some direct decompositions of the set of integers, *Math. of Comp.* **18** (1964), 537–546.

[14] V. Bruyère and M. Latteux, *Variable-Length Maximal Codes*, Lecture Notes in Comp. Sci., Springer, New York, **1099**, 1996, 24–47.

[15] D. De Caen, D. A. Gregory, I. G. Hughes, and D. L. Kreher, Near-factors of finite groups, *Ars Combinatoria* **29** (1990), 53–63.

[16] A. L. Cauchy, Recherches sur les nombres, *J. Ecole Polytechniques* **9** (1813), 99–123.

[17] J. Charlebois, Tiling by (k, n)-crosses, *Electronic J. of Undergraduate Math.* **7** (2001), 1–11.

[18] V. Chvatal, R. L. Graham, A. F. Perold, and S. H. Whitesides, Combinatorial designs related to the perfect graph conjecture, *Annals Discrete Math.*, **1984**, 197–206.

[19] G. D. Cohen, S. Litsyn, A. Vardy, and G. Zémor, Tiling of binary spaces, *SIAM J. Discrete Math.* **3** (1996), 393–412.

[20] D. Coppersmith and J. P. Steiberger, On the entry sum of cyclotomic arrays, *Electronic J. of Comb. and Additive Number Theory* (to appear).

[21] K. Corrádi and S. Szabó, Factoring certain infinite groups by cyclic subsets, *Pure Math. and Appl.* A **2** (1992), 285–290.

[22] K. Corrádi and S. Szabó, Solution to a problem of A. D. Sands, *Communications in Algebra* **23** (1995), 1503–1510.

[23] K. Corrádi and S. Szabó, Annihilators in factorizations, *Internat. J. of Math. and Analysis* **1** (2006), 1–22.

[24] E. M. Coven and A. Meyerowitz, Tiling the integers with translates of one finite set, *J. of Algebra* **212** (1999), 161–174.

[25] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.

[26] M. Dinitz, Full rank tilings of finite abelian groups, *SIAM J. Discrete Math.* **20** (2006), 160–170.

[27] S. J. Eigen and V. S. Prasad, Solution to a problem of Sands on the factorization of groups, *Indag. Mathem.* **14** (2003), 11–14.

[28] S. J. Eigen and V. S. Prasad, Tiling abelian groups with a single tile, *Discrete and Cont. Dynamical Syst.* **16** (2006), 361–366.

[29] P. Erdős, Graph theory and probability, *Canadian J. of Math.* **11** (1959), 24–38.

[30] T. Etzion and A. Vardy, On perfect codes and tilings, *SIAM J. Discrete Math.* **11** (1998), 205–223.

[31] L. Euler, *Opera Omnia* 7 1923, 291–292.

[32] H. Everett and D. R. Hickerson, Packing and covering of translates of certain noncovex bodies, *Proc. Amer. Math. Soc.* **75** (1979), 87–91.

[33] H. Fan, *Group Factorizations and Cryptography*, MSc. Thesis, Dept. of Comp. Sci. and Engineering, Univ. of Nebrasca-Lincoln, 1999, 1–58.

[34] I. Fáry, Die Aequivalente des Minkowski-Hajósschen Satzes in der Theorie der topologischen Gruppen, *Comm. Math. Helv.* **23** (1949), 283–287.

[35] C. De Felice, Completing codes by Hajós factorization of groups, in: J. Almeida, G. M. S. Gomes, P. V. Silva (Editors), *Semigroups, Automata and Languages*, World Scientific, Porto, 1996, 59–66.

[36] C. De Felice, An application of Hajós factorization to variable length codes, *Theoret. Comp. Sci.* **164** (1996), 223–252.

[37] C. De Felice, Hajós factorizations of cyclic groups–a simpler proof of a characterization, *J. of Automata, Languages and Comb.* **4** (1999), 111–116.

[38] C. De Felice, Finite completions via factorizing codes, *Internat. J. Algebra Comput.* **17** (2007), 715–760.

[39] O. Fraser and B. Gordon, Solution to a problem of L. Fuchs, *Quart. J. Math. Oxford* **25** (1974), 1–8.

[40] O. Fraser and B. Gordon, Solution to a problem of A. D. Sands, *Glasgow Math. J.* **20** (1979), 115–117.

[41] L. Fuchs, On the possibility of extending Hajós' theorem to infinite abelian groups, *Publ. Math., Debrecen* **5** (1959), 338–347.

[42] L. Fuchs, *Abelian Groups*, Akadémia Kiadó, Budapest 1958.

[43] L. Fuchs, Abelian groups in Hungary, *Rocky Mountain J. of Math.*, **32** (2002), 1181–1195.

[44] S. Galovich and S. K. Stein, Splittings of abelian groups by integers, *Aequationes Math.* **22** (1981), 249–267.

[45] C. F. Gauss, *Werke*, König. Gesellshaft des Wiss., Göttingen, 1876.

[46] H. Haanpa, P. R. J. Östergård, and S. Szabó, Small p-groups without full-rank factorization, *International Journal of Algebra and Computation* **18** (2008), 1019–1034.

[47] G. Hajós, Covering multidimensional spaces by cube lattices, *Mat. Fiz. Lapok* **45** (1938), 171–190 (in Hungarian).

[48] G. Hajós, Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, *Math. Zeit.* **47** (1942), 427–467.

[49] G. Hajós, Sur la factorisation des groupes abèliens, *Časopis Pěs. Mat. Fys.* **74** (1949), 157–162.

[50] G. Hajós, Sur la problème de factorisation des groupes cycliques, *Acta Math. Acad. Sci. Hungar.* **1** (1950), 189–195.

[51] M. Hall, Jr., A combinatorial problem on abelian groups, *Proc. Amer. Math. Soc.* **3** (1952), 584–587.

[52] M. Hall, Jr. and L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **5** (1955), 541–549.

[53] W. Hamaker and S. K. Stein, Splitting groups by integers, *Proc. Amer. Math. Soc.* **46** (1974), 322–324.

[54] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 2003.

[55] O. Heden, A full rank perfect code of length 31, *Designs, Codes and Cryptography* **38** (2006), 125–129.

[56] M. Herzog and J. Schönheim, Group partition, factorization and vector covering problem, *Canadian Math. Bull.* **15** (1972), 207–214.

[57] D. R. Hickerson, Splittings of finite groups, *Pacific J. Math.* **1983**, 141–171.

[58] D. R. Hickerson and S. K. Stein, Abelian groups and packing by semicrosses, *Pacific J. Math.* **122** (1986), 95–109.

[59] R. Hill and R. W. Irving, On group partitions associated with lower bounds for symmetric Ramsey numbers, *European J. of Comb.* **3** (1982), 35–50.

[60] J. M. Irwin and E. A. Walker, *Topics in Abelian groups*, Glenview, Illinois, 1963.

[61] I. Kaplansky, *Infinite Abelian Groups*, University of Michigan Press, Ann Arbor, Michigan, 1969.

[62] F. Kárteszi, *An Introduction to Finite Geometries*, Akadémia Kiadó, 1972 (in Hungarian).

[63] F. Kárteszi, Su una proprietà combinatoria dei poligoni regolari, *Boll. Un. Mat. Ital.* (5) 13A (1976), 139–141.

[64] O. H. Keller, Über die lückenlose Einfüllung des Raumes mit Würfeln, *J. Reine Angew. Math.* **163** (1930), 231–248.

[65] J. H. E. Kempermen, On small sumsets in an abelian group, *Acta Math.* **103** (1960), 63–88.

[66] Gy. Kiss and T. Szőnyi, *Finite Geometries*, Polygon, Szeged, 2001 (in Hungarian).

[67] M. N. Kolountzakis, Translational tilings of the integers with long periods, *The Electronic J. of Comb.* **10** (2003), #R22.

[68] M. N. Kolountzakis and J. C. Lagarias, Structure of tilings of the line by a function, *Duke Math. J.* **82** (1996), 653–678.

[69] M. Krasner and B. Ranulac, Sur une propriété des polynômes de la division du cercle, *C. R. Acad. Sci. Paris* **240** (1937), 397–399.

[70] L. Kronecker, Mèmoire sur les facteurs irreductibles de l'ex-pression $x^n - 1$, *Liouville J. Math. Pures Appl.* **19** (1854), 177–192.

[71] J. C. Lagarias and P. W. Shor, Keller's cube tiling conjecture is false in high dimension, *Bull. Amer. Math. Soc.* **27** (1992), 279–283.

[72] J. C. Lagarias and P. W. Shor, Cube tilings of R^n and nonlinear codes, *Disc. and Comp. Geom.* **11** (1994), 359–391.

[73] J. C. Lagarias and S. Szabó, Universal spectra and Tijdeman's conjecture on factorization of cyclic groups, *The J. of Fourier Analysis and Appl.* **7** (2001), 63–70.

[74] J. C. Lagarias and Y. Wang, Tiling the line with translates of one tile, *Invent. Math.* **124** (1996), 341–365.

[75] J. C. Lagarias and Y. Wang, Spectral sets and factorizations of finite abelian groups, *J. of Funct. Analysis* **145** (1997), 73–98.

[76] N. H. Lam, A property of finite maximal codes, *Acta Math. Vietnamica* **21** (1996), 279–288.

[77] N. H. Lam, Hajós factorizations and completion of codes, *Theoret. Comp. Sci.* **182** (1997), 245–256.

[78] V. I. Levenstein, Binary codes capable of correcting deletions, insertions and reversals, *Doklady Akademii Nauk SSSR* 163 (1965), 845–848 (in Russian). English translation in *Soviet Physics Dokl.* 10 (1966), 707–710.

[79] B. Lindström, On group and nongroup perfect codes in q symbols, *Math. Scand.* **25** (1969), 149–158.

[80] B. Lindström, Group partitions and mixed perfect codes, *Canadian Math. Bull.* **18** (1975), 57–60.

[81] C. T. Long, Addition theorems for sets of integers, *Pacific J. of Math.* **23** (1967), 107–112.

[82] L. Lovász, A characterization of perfect graphs, *J. Comb. Theory Series B* **13** (1972), 95–98.

[83] J. Mackey, A cube tiling of dimension eight with no facesharing, *Disc. and Comput. Geom.* **28** (2002), 275–279.

[84] S. S. Magliveras, A cryptosystem from logarithmic signatures over finite groups, *Proceedings 29th Midwest Symposium on Circuits and Systems*, Elsevier, New York, 1986, 972–975.

[85] S. S. Magliveras, Secret- and public-key cryptosystems from group factorizations, *Tatra Mountains Math. Publ.* **25** (2002), 1–12.

[86] J. Marconi and J. A. Foster, Finding cliques in Keller graphs with genetic algorithms, *Proc. Int. Conf. On Evolutionary Comp.* (ICEC), D. B. Fogel and P. J. Angeline (Editors), IEEE Press, Piscataway, NY, 1998, 650–655..

[87] M. Matolcsi, J. Réffy, and F. Szöllősi, Construction of complex Hadamard matrices via tiling abelian groups, *OSID* **14** (2007) (in print).

[88] H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1896.

[89] E. Molnár, Hajós' proof of Minkowski's conjecture, *Mat. Lapok* **34** (1987), 11–24 (in Hungarian).

[90] A. Munemasa, On perfect t-shift codes in abelian groups, *Designs, Codes, and Cryptography* **5** (1995), 253–259.

[91] M. B. Natanson, *Additive Number Theory, Inverse Problems and the Geometry of Sumsets*, GTM **165** Springer, New York, 1996.

[92] D. J. Newman, Complementsof finite sets of integers, *Michigen Math. J.* **14** (1967), 481–486.

[93] D. J. Newman, Tessellation of integers, *J. of Number Theory* **9** (1977), 107–111.

[94] E. E. Obaid, On a variation of Sands' method, *Internat. J. Math. Math. Sci.* **9** (1986), 597–604.

[95] C. Okuda, *The factorization of abelian groups*, Ph.D. Thesis, The Pennsylvania State Univ., 1975.

[96] J. E. Olson, On a combinatorial problem of finite abelian groups I, II, *J. of Number Theory* **1** (1969), 8–10, 195–199.

[97] J. E. Olson, On a combinatorial problem of Erdös, Ginzburg and Ziv, *J. of Number Theory* **8** (1976), 52–57.

[98] J. E. Olson, An addition theorem for finite abelian groups, *J. of Number Theory* **9** (1977), 63–70.

[99] J. E. Olson, A problem of Erdős on abelian groups, *Combinatorica* **7** (1987), 285–289.

[100] P. R. J. Östergård and S. Szabó, Elementary p-groups with the Rédei property, *Internat. J. of Algebra and Comp.*, **17** (2007), 171–178.

[101] P. R. J. Östergård and A. Vardy, Resolving the existence of full-rank tilings of binary Hamming spaces, *SIAM J. Discrete Math.* **18** (2004), 382–387.

[102] M. W. Padberg, Perfect zero-one matrices, *Math. Programming* **6** (1974), 180–196.

[103] L. J. Paige, A note on finite abelian groups, *Bull. Amer. Math. Soc.* **53** (1947), 590–593.

[104] A. Pêcher, *Graphes de Cayley partitionnables*, Ph.D. Thesis, 2000.

[105] Minghua Qu and S. A. Venstone, Factorizations in the elementary abelian p-groups and their cryptographic significance, *J. of Cryptography* **7** (1994), 201–212.

[106] F. P. Ramsey, On a problem of formal logic, *Proc. London Math. Soc.* **30** (1929), 264–286.

[107] L. Rédei, Die neue Theorie der endlichen Abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós, *Acta Math. Acad. Sci. Hungar.* **16** (1965), 329–373.

[108] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel, 1970 (English translation: *Lacunary Polynomials over Finite Fields*, North-Holland, Amsterdam, 1973.)

[109] A. Restivo, S. Salemi, and T. Sportelli, Completing codes, *Theoret. Informatics and Appl.* **23** (1989), 135–147.

[110] R. M. Robinson, Multiple tilings of n-dimensional space by unit cubes, *Math. Zeit.* **166** (1979), 225–264.

[111] O. Rothaus and J. G. Thompson, A combinatorial problem in the symmetric group, *Pacific J. of Math.* **18** (1966), 175–178.

[112] L. Z. Ruzsa, Appendix to [170]

[113] S. Saidi, Codes for perfectly correcting errors of limited size, *Discrete Math.* **118** (1993), 207–223.

[114] S. Saidi, Semicrosses and quadratic forms, *European J. of Comb.* **16** (1995), 191–196.

[115] A. D. Sands, On the factorisation of finite abelian groups, *Acta Math. Acad. Sci. Hungar.* **8** (1957), 65–86.

[116] A. D. Sands, The factorization of abelian groups, *Quart. J. Math. Oxford* **10** (1959), 81–91.

[117] A. D. Sands, On the factorisation of finite abelian groups II, *Acta Math. Acad. Sci. Hungar.* **13** (1962), 153–169.

[118] A. D. Sands, The factorization of abelian groups II, *Quart. J. Math. Oxford* **13** (1962), 45–54.

[119] A. D. Sands, On a problem of L. Fuchs, *J. London Math. Soc.* **37** (1962), 277–284.

[120] A. D. Sands, Factorization of cyclic groups, *Proc. Coll. on Abelian Groups*, Tihany, Hungary, 1963, 139–146.

[121] A. D. Sands, On the factorization on finite groups, *J. London Math. Soc.* **1974**, 627–631.

[122] A. D. Sands, On the factorisation of finite abelian groups III, *Acta Math. Acad. Sci. Hungar.* **25** (1974), 279–284.

[123] A. D. Sands, On a conjecture of G. Hajós, *Glasgow Math. J.* **15** (1974), 88–89.

[124] A. D. Sands, On the factorization of finite groups, *J. London Math. Soc.* **7** (1974), 627–631.

[125] A. D. Sands, On Keller's conjecture for certain cyclic groups, *Proc. Edinburgh Math. Soc.* **22** (1979), 17–21.

[126] A. D. Sands, Simulated factorizations II, *Aequationes Math.* **44** (1992), 48–59.

[127] A. D. Sands, Simulated factorizations III, *Algebra Colloq.* **6** (1999), 177–185.

[128] A. D. Sands, Replacement of factors by subgroups in the factorization of abelian groups, *Bull. London Math. Soc.* **32** (2000), 297–304.

[129] A. D. Sands, Factoring finite abelian groups, *J. of Algebra* **274** (2004), 540–549.

[130] A. D. Sands, Factorizations of abelian groups involving simulated factors and one other factor, *Acta Sci. Math. (Szeged)* **73** (2007), 511–517.

[131] A. D. Sands, A question concerning the factorization of cyclic groups, *International Journal of Algebra and Computation* **8** (2007), 1573–1575.

[132] A. D. Sands, A generalization of Hajós' theorem, *Internat. Electronic J. of Algebra* **3** (2008), 83–95.

[133] A. D. Sands, A note on quasi-periodic factorizations, *International Journal of Algebra and Computation* **18** (2008), 421–422.

[134] A. D. Sands and S. Szabó, Factorization of periodic subsets, *Acta Math. Acad. Sci. Hungar.* **57** (1991), 159–167.

[135] A. D. Sands and S. Szabó, The possibility of extending factorization results to infinite abelian groups, *Beiträge zur Alg. und Geom.* **48** (2007), 151–173.

[136] A. D. Sands and S. Szabó, Non-quasi-periodic factorizations for certain finite abelian groups, *Internat. J. of Algebra and Comp.* **17** (2007), 837–849.

[137] I. J. Schoenberg, A note on the cyclotomic polynomial, *Mathematika* **11** (1964), 131–136.

[138] P. W. Shor, A counterexample to the triangle conjecture, *J. of Comb. Theory* A **39** (1985), 110–112.

[139] H. S. Sneveli, The Cayley addition table of Z_n, *Amer. Math. Monthly* **106** (1999), 584–585.

[140] S. K. Stein, Algebraic tiling, *Amer. Math. Monthly* **81** (1974), 445–462.

[141] S. K. Stein, Tiling packing, and covering by clusters, *Rocky Mount. J. of Math.* **16** (1986), 277–321.

[142] S. K. Stein and S. Szabó, *Algebra and Tiling: Homomorphisms in the Service of Geometry*, Mathematical Association of America, 1994, (Carus mathematical monographs, 25).

[143] J. P. Steinberger, A class of prototiles with doubly generated level semigroups, *J. of Comb. Theory*, Series A, **106** No. 1 (2004)

[144] J. P. Steinberger, Multiple tilings of Z with long periods, and tiles with many-generated level semigroups, *New York J. of Math.* **11** (2005), 445–456

[145] J. P. Steinberger, Indecomposable tilings of the integers with exponentially long periods, *Electronic J. of Comb.* **12** (2005)

[146] J. P. Steinberger, Quasiperiodic group factorizations, *Results Math.* **51** (2008), 319–338.

[147] J. P. Steinberger, Tiling of the integers can have superpolynomial periods, *Combinatorica* (to appear).

[148] J. P. Steinberger, Minimal vanishing sums of roots of unity with large coefficients, (preprint).

[149] J. P. Steinberger, *Tilings the Integers, Vanishing Sums of Roots of Unity, and Cyclotomic Arrays*, Ph.D. Thesis, Univ. of California at Davis, 2007.

[150] J. Surányi, A way of representing finite abelian groups, *Mat. Lapok* **23** (1972), 257–259 (in Hungarian).

[151] S. Szabó, A remark on regular polygons, *Mat. Lapok* **28** (1980), 199–202 (in Hungarian).

[152] S. Szabó, A type of factorization of finite abelian groups, *Discrete Math.* **54** (1985), 121–125.

[153] S. Szabó, A reduction of a problem of G. Hajós, *K. Marx Univ. Dept. of Math. Budapest* 1985, 1–13.

[154] S. Szabó, Lattice covering by semi-crosses of arm length two, *European J. of Comb.* **12** (1991), 263–266.

[155] S. Szabó, On finite abelian groups and parallel edges on polygons, *Math. Magazine* **66** (1993), 36–39.

[156] S. Szabó, Factoring an infinite abelian group by subsets, *Period. Math. Hungar.* **40** (2000), 135–140.

[157] S. Szabó, *Topics in Factorization of Abelian Groups*, Birkhäuser Verlag, Basel, 2004.

[158] S. Szabó, Completing codes and the Rédei property of groups, *Theoret. Comp. Sci.* **359** (2006), 449–454.

[159] S. Szabó, Quasi-periodic factorizations, *J. of Algebra and Its Appl.* **6** (2006), 793–797.

[160] S. Szabó, Nonfull-rank factorizations of elementary 3-groups, *Internat. Electronic J. of Algebra* **3** (2008), 96–102.

[161] S. Szabó, Full-rank non-periodic factorizations of elementary p-groups, *Demostratio Math.* **41** (2008), 45–56.

[162] S. Szabó, Groups admitting only quasi-periodic factorizations, *Annales Univ. Sci. Budapest., Sect. Comp.* **29** (2008), 239–243.

[163] S. Szabó and C. Ward, Factoring abelian groups and tiling binary spaces, *Pure Math. and Appl.* **8** (1997), 111–115.

[164] S. Szabó and C. Ward, Factoring elementary groups of prime cube order into subsets, *Math. of Comp.* **67** (1998), 1199–1206.

[165] S. Szabó and C. Ward, Factoring groups having periodic maximal subgroups, *Bol. Soc. Mat. Mexicana* **3** (1999), 327–333.

[166] M. Szegedy, Algorithms to tile the infinite grid with finite clusters, preprint 1998 www.cs.rutgers.edu/˜szegedy/

[167] C. B. Swenson, *Direct sum subset decompositions of abelian groups*, Ph.D. Thesis, Washington State Univ., 1972.

[168] C. B. Swenson, Direct sum subset decompositions of Z, *Pacific J. of Math.* **53** (1974), 629–633.

[169] U. Tamm, Splittings of cyclic groups and perfect shift codes, *IEEE Trans. on Information Theory* **44** (1998), 2003–2009.

[170] R. Tijdeman, Decomposition of the integers as a direct sum of two subsets, Number Theory (Paris 1992–1993) London Math. Soc. Lecture Note **215**, Cambridge Univ. Press, Cambridge, 1995, 261–276.

[171] R. R. Varshamov and G. M. Tenengolts, Codes which corrects single asymmetric errors, *Autamatika i Telemekhanika* **26** (1965), 288–292. (in Russian) English translation in *Automation and Remote Control* **26** (1965), 286–290.

[172] E. C. Wittmann, Einfacher Beweis des Hauptsatzes von Hajós-Rédei für elementare Gruppen von Primzahlquadratordnung, *Acta Math. Acad. Sci. Hungar.* **20** (1969), 227–230.

[173] A. J. Woldar, A reduction theorem on purely singular splittings of cyclic groups, *Proc. of Amer. Math. Soc.*, **173** (1995), 2955–2959.

[174] A. Zykov, On some problem of linear complexes, *Mat. Sbornik N. S.* **24** (1949), 163–188. English translation in Amer. Math. Soc. Transl. **79** (1952).