

Goro Shimura

SPRINGER

MONOGRAPHS IN MATHEMATICS

# Arithmetic of Quadratic Forms



Springer

# *Springer Monographs in Mathematics*

For further volumes:

<http://www.springer.com/series/3733>



Goro Shimura

# Arithmetic of Quadratic Forms



Springer

Goro Shimura  
Department of Mathematics  
Princeton University  
Princeton, NJ 08544  
USA  
goro@math.princeton.edu

ISSN 1439-7382

ISBN 978-1-4419-1731-7

e-ISBN 978-1-4419-1732-4

DOI 10.1007/978-1-4419-1732-4

Library of Congress Control Number: 2010927446

Mathematics Subject Classification (2010): 11D09, 11E08, 11E12, 11E41, 11Rxx, 11Sxx, 17C20

©2010 Springer Science+Business Media, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

Springer is part of Springer Science+Business Media, LLC (springer.com)

## PREFACE

This book can be divided into two parts. The first part is preliminary and consists of algebraic number theory and the theory of semisimple algebras. The *raison d'être* of the book is in the second part, and so let us first explain the contents of the second part.

There are two principal topics:

- (A) Classification of quadratic forms;
- (B) Quadratic Diophantine equations.

Topic (A) can be further divided into two types of theories:

- (a1) Classification over an algebraic number field;
- (a2) Classification over the ring of algebraic integers.

To classify a quadratic form  $\varphi$  over an algebraic number field  $F$ , almost all previous authors followed the methods of Helmut Hasse. Namely, one first takes  $\varphi$  in the diagonal form and associates an invariant to it at each prime spot of  $F$ , using the diagonal entries. A superior method was introduced by Martin Eichler in 1952, but strangely it was almost completely ignored, until I resurrected it in one of my recent papers. We associate an invariant to  $\varphi$  at each prime spot, which is the same as Eichler's, but we define it in a different and more direct way, using Clifford algebras. In Sections 27 and 28 we give an exposition of this theory. At some point we need the Hasse norm theorem for a quadratic extension of a number field, which is included in class field theory. We prove it when the base field is the rational number field to make the book self-contained in that case.

The advantage of our method is that it enables us to discuss (a2) in a clear-cut way. The main problem is to determine the genera of quadratic forms with integer coefficients that have given local invariants. A quadratic form of  $n$  variables with integer coefficients can be given in the form  $\varphi[x] = \sum_{i,j=1}^n c_{ij}x_i x_j$  with a symmetric matrix  $(c_{ij})$  such that  $c_{ii}$  and  $2c_{ij}$  are integers for every  $i$  and  $j$ . If the matrix represents a *symmetric* form with integer coefficients, then  $c_{ij}$  is an integer for every  $(i, j)$ . Thus there are two types of classification

theories over the ring of integers: one for quadratic forms and the other for symmetric forms. In fact, the former is easier than the latter. There were several previous results in the unimodular case, but there were few, if any, investigations in the general case. We will determine the genera of quadratic or symmetric forms over the integers that are *reduced* in the sense that they cannot be represented by other quadratic or symmetric forms nontrivially. This class of forms contains forms with square-free discriminant.

We devote Section 32 to strong approximation in an indefinite orthogonal group of more than two variables, and as applications we determine the *classes* instead of the *genera* of indefinite reduced forms.

The origin of Topic (a2) is the investigation of Gauss concerning primitive representations of an integer as a sum of three squares. In our book of 2004 we gave a framework in which we could discuss similar problems for an arbitrary quadratic form of more than two variables over the integers. In Chapter VII we present an easier and more accessible version of the theory. Though Gauss treated sums of three squares, he did not state any general principle; he merely explained the technique by which he could solve his problems. In fact, we state results as two types of formulas for a quadratic form, which can be specialized in two different ways to what Gauss was doing. Without going into details here we refer the reader to Section 34 in which a historical perspective is given. Our first main theorem of quadratic Diophantine equations is given in Section 35, from which we derive the two formulas in Section 37.

Let us now come to the first part of the book in which we give preliminaries that are necessary for the main part concerning quadratic forms. Assuming that the reader is familiar with basic algebra, we develop algebraic number theory and also the theory of semisimple algebras more or less in standard ways, and even in old-fashioned ways, whenever we think that is the easiest and most suitable for beginners. In fact, almost all of the material in this part have been taken from the notes of my lectures at Princeton University. However, we have tried a few new approaches and included some theorems that cannot be found in ordinary textbooks. For instance, our formulation and proof of the quadratic reciprocity law in a generalized form do not seem to be well-known; the same may be said about the last theorem of Section 10, which is essentially strong approximation in a special linear group. In the same spirit, we add the classical theory of genera as the last section of the book.

We could have made the whole book self-contained by including an easy part of class field theory, but in order to keep the book a reasonable length, we chose a compromised plan. Namely, we prove basic theorems in local class field theory only in some special cases, and the Hilbert reciprocity law only

over the rational number field. However, we at least state the main theorems with an arbitrary number field as the base field, so that the reader who knows class field theory can learn the arithmetic theory of quadratic forms with no further references.

To conclude the preface, it is my great pleasure to express my deepest thanks to my friends Koji Doi, Tomokazu Kashio, Kaoru Okada, and Hiroyuki Yoshida, who kindly read earlier versions of the first two-thirds of the book and contributed many invaluable comments.

Princeton  
May, 2009

Goro Shimura





# CONTENTS

<b>Preface</b>	<b>v</b>
<b>Notation and terminology</b>	<b>xi</b>
<b>Chapter I. The quadratic reciprocity law</b>	<b>1</b>
1. Elementary facts	1
2. Structure of $(\mathbf{Z}/m\mathbf{Z})^\times$	4
3. The quadratic reciprocity law	5
4. Lattices in a vector space	11
5. Modules over a principal ideal domain	12
<b>Chapter II. Arithmetic in an algebraic number field</b>	<b>15</b>
6. Valuations and $p$ -adic numbers	15
7. Hensel's lemma and its applications	22
8. Integral elements in algebraic extensions	25
9. Order functions in algebraic extensions	27
10. Ideal theory in an algebraic number field	35
<b>Chapter III. Various basic theorems</b>	<b>47</b>
11. The tensor product of fields	47
12. Units and the class number of a number field	50
13. Ideals in an extension of a number field	57
14. The discriminant and different	59
15. Adeles and ideles	66
16. Galois extensions	71
17. Cyclotomic fields	75
<b>Chapter IV. Algebras over a field</b>	<b>79</b>
18. Semisimple and simple algebras	79
19. Central simple algebras	86
20. Quaternion algebras	95
21. Arithmetic of semisimple algebras	100
<b>Chapter V. Quadratic forms over a field</b>	<b>115</b>
22. Algebraic theory of quadratic forms	115
23. Clifford algebras	120
24. Clifford groups and spin groups	127

25. Lower-dimensional cases	133
26. The Hilbert reciprocity law	140
27. The Hasse principle	143
<b>Chapter VI. Deeper arithmetic of quadratic forms</b>	<b>153</b>
28. Classification of quadratic forms over local and global fields	153
29. Lattices in a quadratic space	161
30. The genus and class of a lattice and a matrix	171
31. Integer-valued quadratic forms	179
32. Strong approximation in the indefinite case	186
33. Integer-valued symmetric forms	197
<b>Chapter VII. Quadratic Diophantine equations</b>	<b>203</b>
34. A historical perspective	203
35. Basic theorems of quadratic Diophantine equations	206
36. Classification of binary forms	213
37. New mass formulas	224
38. The theory of genera	228
<b>References</b>	<b>233</b>
<b>Index</b>	<b>235</b>

## NOTATION AND TERMINOLOGY

In this book we assume that the reader is familiar with basic facts on groups, rings, and the theory of field extensions up to Galois theory. We write  $X \subset Y$  for two sets  $X$  and  $Y$  if  $X$  is a subset of  $Y$ , including the case  $X = Y$ , and denote by  $\#X$  or  $\#\{X\}$  the number of elements of  $X$  when it is finite. Following the standard convention, we do not call 0 of the ring  $A = \{0\}$  an identity element. Thus, whenever we speak of an identity element of a ring  $A$ , we assume that  $A \neq \{0\}$ . For submodules  $B$  and  $C$  of a ring  $A$  we denote by  $BC$  the set of all finite sums  $\sum_i b_i c_i$  with  $b_i \in B$  and  $c_i \in C$ .

The symbols **Z**, **Q**, **R**, and **C** will mean as usual the ring of integers and the fields of rational numbers, real numbers, and complex numbers, respectively. In addition, we put

$$\mathbf{T} = \{z \in \mathbf{C} \mid |z| = 1\},$$

and denote by **H** the Hamilton quaternion algebra; see §20.2. Given an associative ring  $A$  with identity element and an  $A$ -module  $X$ , we denote by  $A^\times$  the group of all invertible elements of  $A$ , and by  $X_n^m$  the  $A$ -module of all  $m \times n$ -matrices with entries in  $X$ ; we put  $X^m = X_1^m$  for simplicity. For an element  $y$  of  $X_1^m$  or  $X_m^1$  we denote by  $y_i$  the  $i$ -th entry of  $y$ . The zero element of  $A_n^m$  is denoted by  $0_n^m$  or simply by 0. When we view  $A_n^n$  as a ring, we usually denote it by  $M_n(A)$ . We denote the identity element of  $M_n(A)$  by  $1_n$  or simply by 1. The transpose, determinant, and trace of a matrix  $x$  are denoted by  ${}^t x$ ,  $\det(x)$ , and  $\text{tr}(x)$ . We put  $GL_n(A) = M_n(A)^\times$ , and

$$SL_n(A) = \{\alpha \in GL_n(A) \mid \det(\alpha) = 1\}$$

if  $A$  is commutative. For square matrices  $x_1, \dots, x_r$ ,  $\text{diag}[x_1, \dots, x_r]$  denotes the square matrix with  $x_1, \dots, x_r$  in the diagonal blocks and 0 in all other blocks.

For a group  $G$  we denote by  $[G : 1]$  the order of  $G$ , and for a subgroup  $H$  of  $G$  we denote by  $[G : H]$  the index of  $H$  in  $G$ . For a vector space  $V$  over a field  $F$  we denote by  $[V : F]$  the dimension of  $V$  over  $F$  and by  $\text{End}_F(V)$  the ring of all  $F$ -linear endomorphisms of  $V$ ; we put then  $GL_F(V) = \text{End}_F(V)^\times$  and  $SL_F(V) = \{\alpha \in GL_F(V) \mid \det(\alpha) = 1\}$ . The distinction of  $[V : F]$  from  $[G : H]$  will be clear from the context. If  $K$  is a field containing  $F$ , then  $[K : F]$  is the degree of the extension  $K$  of  $F$ . When  $F$  is clear from the context, we also write  $GL(V)$ ,  $SL(V)$ , and  $\dim(V)$  for  $GL_F(V)$ ,  $SL_F(V)$ , and  $[V : F]$ .

A polynomial in one variable with coefficients in a field is called **monic** if the leading coefficient is 1. Given a square matrix  $\xi$  with entries in a field  $F$ , by the **minimal** (or **minimum**) polynomial of  $\xi$  over  $F$  we understand a monic polynomial that generates  $\{\varphi \in F[x] \mid \varphi(\xi) = 0\}$ , where  $x$  is an indeterminate. We use the same terminology for an element  $\xi$  of an algebraic extension of  $F$ .



# THE QUADRATIC RECIPROCITY LAW

## 1. Elementary facts

**1.1.** In this section we recall several well-known elementary facts, mostly without proof. We give the proof for some of them. An ideal  $I$  of a commutative ring  $R$  is called a **prime ideal** if  $R/I$  has no zero divisors;  $I$  is called **principal** if  $I = \alpha R$  with some  $\alpha \in R$ . An integral domain (that is, a commutative ring with identity element that has no zero divisors)  $R$  is called a **principal ideal domain** if every ideal of  $R$  is principal. It is known that for a field  $F$  and an indeterminate  $x$  the polynomial ring  $F[x]$  is a principal ideal domain. Also, the ring  $\mathbf{Z}$  is a principal ideal domain. An integral domain is called a **unique factorization domain** if every principal ideal  $I$  of  $R$  different from  $\{0\}$  can be written uniquely in the form  $I = P_1^{e_1} \cdots P_r^{e_r}$  with prime ideals  $P_i$  that are principal and  $0 < e_i \in \mathbf{Z}$ .

**Theorem 1.2.** (i) *Let  $R$  be a unique factorization domain. Then the polynomial ring  $R[x]$  is a unique factorization domain. If  $s$  is a prime element of  $R$  (that is,  $s \notin R^\times$  and if  $s = gh$  with  $g, h \in R$ , then  $g \in R^\times$  or  $h \in R^\times$ ), then  $sR$  is a prime ideal of  $R$ . Conversely, every prime ideal of  $R$  that is principal and different from  $\{0\}$  is of the form  $sR$  with a prime element  $s$  of  $R$ .*

(ii) Let  $R$  be a principal ideal domain. Then  $R$  is a unique factorization domain, and every prime ideal  $P$  of  $R$  different from  $\{0\}$  is a maximal ideal, that is,  $R/P$  is a field.

**Theorem 1.3.** *Let  $R$  be a commutative ring with identity element, and let  $X_1, \dots, X_r$  be ideals of  $R$  such that  $X_i + X_j = R$  if  $i \neq j$ . Then*

$$(1.1) \quad R/(X_1 \cdots X_r) \cong R/X_1 \oplus \cdots \oplus R/X_r.$$

PROOF. We first prove the case  $r = 2$ . Define a map  $f : R \rightarrow R/X_1 \oplus R/X_2$  by

$$f(x) = (x \pmod{X_1}, x \pmod{X_2}).$$

Clearly  $f$  is a ring-homomorphism and  $\text{Ker}(f) = X_1 \cap X_2$ . Now  $X_1 \cap X_2 = (X_1 \cap X_2)(X_1 + X_2) \subset X_1 X_2 \subset X_1 \cap X_2$ , and so  $X_1 X_2 = X_1 \cap X_2$ . Take

$s \in X_1$  and  $t \in X_2$  so that  $s + t = 1$ . Given  $a, b \in R$ , put  $c = at + bs$ . Then  $c - a = a(t - 1) + bs = (b - a)s \in X_1$ , and similarly  $c - b \in X_2$ . Thus  $f(c) = (a \pmod{X_1}, b \pmod{X_2})$ , which means that  $f$  is surjective. Therefore  $R/(X_1X_2) = R/\text{Ker}(f) \cong R/X_1 \oplus R/X_2$ , which proves the case  $r = 2$ . Now suppose  $Z + X = Z + Y = R$  for ideals  $X, Y$ , and  $Z$  of  $R$ . Then  $R = (Z + X)(Z + Y) = Z + XZ + ZY + XY = Z + XY$ , since  $XZ + ZY \subset Z$ . Taking  $Z$  to be  $X_r$  and repeating the same argument, we obtain  $X_r + X_1 \cdots X_{r-1} = R$ , and so  $R/(X_1 \cdots X_r) \cong R/(X_1 \cdots X_{r-1}) \oplus R/X_r$ . Applying induction to  $R/(X_1 \cdots X_{r-1})$ , we can complete the proof.

Every infinite cyclic group is isomorphic to  $\mathbf{Z}$ ; every finite cyclic group is isomorphic to  $\mathbf{Z}/m\mathbf{Z}$ . Now the basic theorem on abelian groups can be stated as follows.

**Theorem 1.4.** *Every finitely generated abelian group is the direct product of finitely many cyclic groups of finite or infinite order. In particular, every finite abelian group is isomorphic to a direct sum of the form  $\sum_{m \in M} \mathbf{Z}/m\mathbf{Z}$  with a finite set  $M$  of positive integers.*

**Theorem 1.5.** *If  $F$  is a field, every finite subgroup of  $F^\times$  is cyclic. In particular,  $F^\times$  is a cyclic group if  $F$  is a finite field.*

PROOF. Let  $G$  be a finite subgroup of  $F^\times$ . Then by Theorem 1.4,  $G$  is isomorphic to  $\sum_{i=1}^r \mathbf{Z}/n_i\mathbf{Z}$  with positive integers  $n_i$ . We may assume that  $r > 1$  and  $n_i > 1$  for every  $i$ , since  $G$  is cyclic otherwise. Suppose  $n_1$  and  $n_2$  are divisible by a prime number  $p$ . Then  $(\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z})$  has  $p^2$  elements  $y$  such that  $py = 0$ . These elements  $y$  correspond to  $p^2$  elements  $x$  of  $G$  such that  $x^p = 1$ . Since  $F$  is a field, the equation  $X^p = 1$  can have at most  $p$  solutions in  $F$ , a contradiction. Thus  $n_1$  and  $n_2$  are relatively prime, and more generally,  $n_1, \dots, n_r$  are relatively prime. By (1.1),  $G$  is isomorphic to  $\mathbf{Z}/(n_1 \cdots n_r\mathbf{Z})$ , which is cyclic. This proves our theorem.

For example,  $(\mathbf{Z}/p\mathbf{Z})^\times$  is a cyclic group of order  $p - 1$ .

**Lemma 1.6.** *Let  $f$  be a homomorphism of a finite group  $G$  into  $\mathbf{C}^\times$ . Then*

$$\sum_{x \in G} f(x) = \begin{cases} [G : 1] & \text{if } f \text{ is trivial,} \\ 0 & \text{if } f \text{ is nontrivial.} \end{cases}$$

PROOF. Assuming  $f$  to be nontrivial, take  $y \in G$  such that  $f(y) \neq 1$ , and observe that  $\sum_{x \in G} f(x) = \sum_{x \in G} f(yx) = f(y) \sum_{x \in G} f(x)$ , and hence  $\sum_{x \in G} f(x) = 0$ . Our formula for trivial  $f$  is trivial.

For example, let  $\zeta$  be a primitive  $m$ -th root of unity with  $1 < m \in \mathbf{Z}$  and let  $r \in \mathbf{Z}$ . Then taking  $f(x) = \zeta^{rx}$ , from Lemma 1.6 we obtain

$$(1.2) \quad \sum_{a=0}^{m-1} \zeta^{ra} = \begin{cases} m & \text{if } r \in m\mathbf{Z}, \\ 0 & \text{if } r \notin m\mathbf{Z}. \end{cases}$$

**Lemma 1.7.** *Let  $R$  be a commutative ring with identity element. Suppose  $R = A_1 \oplus \cdots \oplus A_r = B_1 \oplus \cdots \oplus B_s$  with subrings  $A_i$  and  $B_j$  that are indecomposable. (Here a ring  $X$  is called **indecomposable** if  $X$  cannot be written in the form  $X = Y \oplus Z$  with subrings  $Y$  and  $Z$  that are different from  $\{0\}$ .) Then the  $A_i$  are the same as the  $B_j$  as a whole.*

PROOF. Clearly  $A_i$  and  $B_j$  are ideals of  $R$ . Let  $1_R = e_1 + \cdots + e_r$  with  $e_i \in A_i$ . Then we can easily show that  $B_1 = B_1 e_1 \oplus \cdots \oplus B_1 e_r$ . The indecomposability of  $B_1$  implies that  $B_1 = B_1 e_k$  for exactly one  $k$ . Changing the order of the  $A_i$ , we may assume that  $B_1 = B_1 e_1$ ; then  $B_1 \subset A_1$ . Exchanging  $\{A_i\}$  and  $\{B_j\}$ , we have  $A_1 \subset B_j$  for some  $j$ . Clearly  $j = 1$ , and so  $A_1 = B_1$ . Repeating the same argument, we eventually obtain the desired conclusion.

**Lemma 1.8.** *Let  $K$  be a separable quadratic extension of a field  $F$ , and  $\rho$  the nontrivial automorphism of  $K$  over  $F$ . Then*

$$\{y \in K^\times \mid yy^\rho = 1\} = \{x/x^\rho \mid x \in K^\times\}.$$

PROOF. If  $y = x/x^\rho$ , then clearly  $yy^\rho = 1$ . Thus our task is to show that if  $y \in K^\times$  and  $yy^\rho = 1$ , then  $y = x/x^\rho$  with some  $x \in K^\times$ . Suppose  $y = -1$ . If the characteristic of  $F$  is 2, then  $y = 1$  and there is no problem. If the characteristic is not 2, then  $K = F(x)$  with  $x$  such that  $x^2 \in F^\times$ . Then  $x^\rho = -x$ , and so  $-1 = x/x^\rho$ . Suppose  $y \neq -1$ ; put  $x = y + 1$ . Then  $x \neq 0$  and  $yx^\rho = 1 + y = x$ , and so  $y = x/x^\rho$  as expected.

**1.9. Finite fields.** In this subsection we recall some basic facts on finite fields. A field with a finite number of elements is called a **finite field**. For every prime number  $p$  the ring  $\mathbf{Z}/p\mathbf{Z}$  is a finite field with  $p$  elements. We denote this field by  $\mathbf{F}(p)$ . Every finite field is a finite algebraic extension of  $\mathbf{F}(p)$  for some  $p$ , and vice versa. Let us fix a prime number  $p$  and an algebraic closure of  $\mathbf{F}(p)$ , and denote it by  $\mathbf{F}(p^\infty)$ . For every positive integer  $n$  the field  $\mathbf{F}(p^\infty)$  contains exactly one algebraic extension of  $\mathbf{F}(p)$  of degree  $n$ . It has  $p^n$  elements, and we denote it by  $\mathbf{F}(p^n)$ . Put  $q = p^n$  with a fixed  $n$ . Then  $x^q = x$  for every  $x \in \mathbf{F}(q)$ , and in particular  $x^{q-1} = 1$  for every  $x \in \mathbf{F}(q)^\times$ . By Theorem 1.5,  $\mathbf{F}(q)^\times$  is a cyclic group of order  $q-1$ . For another positive integer  $m$  we have  $\mathbf{F}(p^n) \subset \mathbf{F}(p^m)$  if and only if  $m = \ell n$  with  $0 < \ell \in \mathbf{Z}$ , in which case  $\mathbf{F}(p^m)$  is a cyclic extension (that is, a Galois extension whose Galois group is cyclic) of  $\mathbf{F}(p^n)$  of degree  $\ell$ . The Galois group consists of the maps  $x \mapsto x^{q^a}$  for  $0 \leq a < \ell$ , where  $q = p^n$ . Write  $k = \mathbf{F}(p^n)$  and  $h = \mathbf{F}(p^m)$ . Then the maps  $\text{Tr}_{h/k} : h \rightarrow k$  and  $N_{h/k} : h^\times \rightarrow k^\times$  are surjective. Indeed, the surjectivity of the trace map is true for every separable extension. As for the norm map, we



have  $N_{h/k}(x) = x^r$  with  $r = \sum_{a=0}^{\ell-1} q^a = (q^\ell - 1)/(q - 1) = [h^\times : k^\times]$ , and we obtain the desired surjectivity.

## 2. Structure of $(\mathbf{Z}/m\mathbf{Z})^\times$

**2.1.** If  $m_1, \dots, m_r$  are relatively prime positive integers  $> 1$ , then from (1.1) we obtain  $\mathbf{Z}/(m_1 \cdots m_r \mathbf{Z}) \cong \mathbf{Z}/m_1 \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/m_r \mathbf{Z}$ , and so

$$(2.1) \quad (\mathbf{Z}/(m_1 \cdots m_r \mathbf{Z}))^\times \cong (\mathbf{Z}/m_1 \mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/m_r \mathbf{Z})^\times.$$

In particular, if  $m = p_1^{e_1} \cdots p_r^{e_r}$  is the prime decomposition of a positive integer  $m > 1$ , then

$$(2.1a) \quad (\mathbf{Z}/m\mathbf{Z})^\times \cong (\mathbf{Z}/p_1^{e_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_r^{e_r}\mathbf{Z})^\times.$$

Therefore the structure of  $(\mathbf{Z}/m\mathbf{Z})^\times$  for  $1 < m \in \mathbf{Z}$  can be reduced to the case where  $m$  is a prime power. The order of the group  $(\mathbf{Z}/m\mathbf{Z})^\times$  is traditionally denoted by  $\varphi(m)$ . In addition we put  $\varphi(1) = 1$ . This  $\varphi$  is called **Euler's function**. Observe that  $\varphi(m)$  equals the number of integers  $a$  prime to  $m$  such that  $0 < a \leq m$ . From (2.1) we obtain

$$(2.2) \quad \varphi(m_1 \cdots m_k) = \varphi(m_1) \cdots \varphi(m_k) \text{ if the } m_i \text{ are as in (2.1).}$$

We easily see that

$$(2.3) \quad \varphi(p^n) = p^{n-1}(p-1) \text{ if } p \text{ is a prime number and } 0 < n \in \mathbf{Z}.$$

**Lemma 2.2.** *Let  $p$  be an odd prime number and  $b$  an integer prime to  $p$ . Then for  $0 \leq e \in \mathbf{Z}$  we have  $(1+bp)^{p^e} = 1+cp^{e+1}$  with an integer  $c$  prime to  $p$ .*

PROOF. We prove this by induction on  $e$ . Since  $\binom{p}{k}$  is divisible by  $p$  if  $1 < k < p$ , by the binomial theorem we have  $(1+bp^e)^p = 1+bp^{e+1}+dp^f$  with  $d \in \mathbf{Z}$  and  $f > e+1$ , and so  $(1+bp^e)^p = 1+b'p^{e+1}$  with an integer  $b'$  prime to  $p$ . This proves the case  $e = 1$  of our lemma. Assuming our lemma for the exponent  $p^e$ , we have  $(1+bp)^{p^{e+1}} = ((1+bp)^{p^e})^p = (1+cp^{e+1})^p = 1+c'p^{e+2}$  with an integer  $c'$  prime to  $p$ , and we can complete the proof.

Notice that this lemma is false if  $p = 2$ . Indeed,  $(1+2)^2 = 1+2 \cdot 2^2$ .

**Theorem 2.3.** *If  $p$  is an odd prime number, then  $(\mathbf{Z}/p^n\mathbf{Z})^\times$  is a cyclic group for every  $n \in \mathbf{Z}, > 0$ .*

PROOF. Take an integer  $r$  that represents a generator of  $(\mathbf{Z}/p\mathbf{Z})^\times$ ; then  $r^{p-1} = 1+bp$  with  $b \in \mathbf{Z}$ . Choosing  $r$  suitably, we may assume that  $p \nmid b$ . Indeed, if  $p|b$ , take  $r+p$  instead of  $r$ . Since  $(r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + p^2s$  with  $s \in \mathbf{Z}$ , we have  $(r+p)^{p-1} = 1+pt$  with  $t = b - r^{p-2} + p(s + r^{p-2})$ , which is prime to  $p$  as desired. Thus assuming  $b$  to be prime to  $p$ , let  $g$  be

the order of the class of  $r \pmod{p^n}$  in  $(\mathbf{Z}/p^n\mathbf{Z})^\times$ . Then  $g|p^{n-1}(p-1)$ , and also  $(p-1)|g$ , as  $r$  generates  $(\mathbf{Z}/p\mathbf{Z})^\times$ . Thus  $g = (p-1)p^a$  with  $0 \leq a \leq n-1$ . Then by Lemma 2.2,  $r^g = (1+bp)^{p^a} = 1+cp^{a+1}$  with an integer  $c$  prime to  $p$ . Since  $r^g - 1 \in p^n\mathbf{Z}$ , we see that  $a+1 \geq n$ , and so  $a = n-1$ , which means that  $r \pmod{p^n}$  has order  $(p-1)p^{n-1}$ . This proves our theorem.

Any integer that represents a generator of  $(\mathbf{Z}/p^n\mathbf{Z})^\times$  is called a **primitive root modulo  $p^n$** .

As for the case  $p = 2$ , we first note that  $(\mathbf{Z}/2\mathbf{Z})^\times$  is trivial and  $(\mathbf{Z}/4\mathbf{Z})^\times$  is of order 2, and so they are cyclic. If  $a = 4k \pm 1$  with  $k \in \mathbf{Z}$ , then  $a^2 = 1 \pm 8k + 16k^2$ , and so  $a^2 - 1 \in 8\mathbf{Z}$  for every odd integer  $a$ . Thus  $(\mathbf{Z}/8\mathbf{Z})^\times$  has no element of order 4, and so it is not cyclic.

**Theorem 2.4.** *Let  $3 \leq n \in \mathbf{Z}$ . For  $2 \leq \nu \leq n$  let  $H_\nu$  denote the subgroup of  $(\mathbf{Z}/2^n\mathbf{Z})^\times$  consisting of all  $\alpha \pmod{2^n}$  such that  $\alpha - 1 \in 2^\nu\mathbf{Z}$ . Then  $H_\nu$  is cyclic of order  $2^{n-\nu}$  and  $(\mathbf{Z}/2^n\mathbf{Z})^\times = \{\pm 1\} \times H_2$ .*

PROOF. The order of  $(\mathbf{Z}/2^n\mathbf{Z})^\times$  is  $2^{n-1}$ , and so the order of any element of  $(\mathbf{Z}/2^n\mathbf{Z})^\times$  is a power of 2. By induction on  $m$  we can prove that  $(1+2^\nu)^{2^m} = 1+2^{m+\nu}k$  with an odd integer  $k$  for  $0 \leq m \in \mathbf{Z}$ . Therefore  $1+2^\nu$  is of order  $2^{n-\nu}$  in this group. Since every odd integer  $\alpha$  satisfies either  $\alpha - 1 \in 4\mathbf{Z}$  or  $\alpha + 1 \in 4\mathbf{Z}$ , we obtain  $(\mathbf{Z}/2^n\mathbf{Z})^\times = \{\pm 1\} \times H_2$ . Clearly  $\{1\} = H_n \subsetneq \cdots \subsetneq H_2$  and  $H_\nu$  has an element of order  $2^{n-\nu}$ . Therefore  $H_\nu$  is cyclic of order  $2^{n-\nu}$ . This completes the proof.

### 3. The quadratic reciprocity law

**3.0.** Here is a problem that motivates our investigation in this section. We consider a congruence  $f(x) \equiv 0 \pmod{m}$ , where  $f(x)$  is a polynomial with coefficients in  $\mathbf{Z}$  and  $m$  is a positive integer; we ask whether it has a solution  $x$  in  $\mathbf{Z}$ . If  $m$  is fixed, then we can answer the question by computing  $f(x)$  for  $0 \leq x < m$ . If we vary  $m$ , the question becomes more interesting. For example, we can ask: *For what kind of prime numbers  $p$  does the congruence*

$$(3.0) \quad 5x^2 \equiv 3 \pmod{p}$$

*have a solution  $x$  in  $\mathbf{Z}$ ?* We will give an answer in §3.8 after developing a general theory.

**3.1.** Let  $p$  be an odd prime number. Then  $(\mathbf{Z}/p\mathbf{Z})^\times$  is a cyclic group of order  $p-1$ , and  $p-1$  is even. Therefore  $(\mathbf{Z}/p\mathbf{Z})^\times$  has a unique subgroup  $R$  of order  $(p-1)/2$ , and so we have a homomorphism  $\lambda$  of  $(\mathbf{Z}/p\mathbf{Z})^\times$  onto  $\{\pm 1\}$  such that  $\text{Ker}(\lambda) = R$ . We then define a symbol  $\left(\frac{b}{p}\right)$  for  $b \in \mathbf{Z}$  by

$$\left(\frac{b}{p}\right) = \begin{cases} \lambda(b \pmod{p}) & \text{if } p \nmid b, \\ 0 & \text{if } p \mid b. \end{cases}$$

This is called the **quadratic residue symbol**. Clearly

$$\left(\frac{bc}{p}\right) = \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \quad \text{for } b, c \in \mathbf{Z}.$$

To explain the nature of this symbol, let  $r$  be a primitive root modulo  $p$ . Then  $R$  is generated by  $r^2 \pmod{p}$ . If  $b$  is an integer prime to  $p$ , then  $b \equiv r^a \pmod{p}$  with  $0 \leq a \in \mathbf{Z}$ . Since  $\left(\frac{r}{p}\right) = \lambda(r \pmod{p}) = -1$ , we have

$$\begin{aligned} \left(\frac{b}{p}\right) &= (-1)^a, \text{ and we easily see that} \\ \left(\frac{b}{p}\right) &= 1 \iff \bar{b} \in R \iff a \in 2\mathbf{Z} \\ &\iff b \equiv x^2 \pmod{p} \text{ for some } x \in \mathbf{Z} \text{ prime to } p, \\ \left(\frac{b}{p}\right) &= -1 \iff \bar{b} \notin R \iff a \notin 2\mathbf{Z} \\ &\iff b \not\equiv x^2 \pmod{p} \text{ for every } x \in \mathbf{Z}, \end{aligned}$$

where  $\bar{b}$  denotes the class of  $b$  modulo  $p\mathbf{Z}$ . We call an integer  $b$  a **quadratic residue modulo  $p$**  if  $\left(\frac{b}{p}\right) = 1$  and a **quadratic nonresidue modulo  $p$**  if  $\left(\frac{b}{p}\right) = -1$ .

**Theorem 3.2.** *For odd prime numbers  $p$  and  $q$  we have:*

$$(3.1) \quad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \quad \text{for every } a \in \mathbf{Z},$$

$$(3.2) \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

$$(3.3) \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}, \end{cases}$$

$$(3.4) \quad \left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \quad \text{if } p \neq q.$$

The last equality is called **the quadratic reciprocity law**.

PROOF. The first congruence is clear if  $p \mid a$ . Let  $a \equiv r^m \pmod{p}$  with a primitive root  $r$  modulo  $p$ . Then  $r^{(p-1)/2} \equiv -1 \pmod{p}$ , and so  $a^{(p-1)/2} \equiv (r^{(p-1)/2})^m \equiv (-1)^m \pmod{p}$ , which proves (3.1). Taking  $a = -1$ , we obtain (3.2). We will derive the last two relations in §3.5 as special cases of Theorem 3.4 below.

Formula (3.4) can be written also

$$(3.5) \quad \left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = -1 \iff p \equiv q \equiv 3 \pmod{4}.$$

Indeed,  $(p-1)(q-1)/4 = [(p-1)/2][(q-1)/2]$ , which is odd if and only if  $p \equiv q \equiv 3 \pmod{4}$ .

**3.3.** Let  $2 < r \in \mathbf{Z}$ . By a **Dirichlet character** (or simply, a **character**) **modulo**  $r$  we mean a homomorphism  $\chi : (\mathbf{Z}/r\mathbf{Z})^\times \rightarrow \mathbf{T}$ . We view  $\chi$  as a function on  $\mathbf{Z}$  by putting

$$\chi(c) = \begin{cases} \chi(c \pmod{r\mathbf{Z}}) & \text{if } c \text{ is prime to } r, \\ 0 & \text{if } c \text{ is not prime to } r, \end{cases}$$

We say that  $\chi$  is **primitive** if  $\chi$  is nontrivial (that is,  $\chi(a) \neq 1$  for some  $a$ ) and there is no character  $\xi$  modulo a proper divisor  $s$  of  $r$  such that  $\chi(c) = \xi(c)$  for every  $c$  prime to  $r$ .

To define the Gauss sum of  $\chi$ , we first put

$$(3.6) \quad \mathbf{e}(z) = \exp(2\pi iz) \quad (z \in \mathbf{C}).$$

In particular,  $\mathbf{e}(1/m)$  for  $0 < m \in \mathbf{Z}$  is a primitive  $m$ -th root of unity. Let  $\chi$  be a primitive Dirichlet character modulo  $r$ . Then we put

$$(3.7) \quad \tau(\chi) = \sum_{a=1}^r \chi(a) \mathbf{e}(a/r),$$

and call it **the Gauss sum of**  $\chi$ . Since  $\chi(r) = 0$ , we can use  $\sum_{a=1}^{r-1}$  in place of  $\sum_{a=1}^r$ . Now we have

$$(3.8a) \quad \sum_{a=1}^r \chi(a) \mathbf{e}(ab/r) = \overline{\chi}(b) \tau(\chi) \quad \text{for every } b \in \mathbf{Z},$$

$$(3.8b) \quad \tau(\chi) \tau(\overline{\chi}) = \chi(-1)r,$$

$$(3.8c) \quad |\tau(\chi)|^2 = r,$$

$$(3.8d) \quad \overline{\tau(\chi)} = \chi(-1) \tau(\overline{\chi}).$$

Formula (3.8a) is easy if  $b$  is prime to  $r$ . Let  $t$  be the greatest common divisor of  $b$  and  $r$ . Assuming that  $t > 1$ , put  $s = r/t$  and  $H = \{a \in (\mathbf{Z}/r\mathbf{Z})^\times \mid a \equiv 1 \pmod{s\mathbf{Z}}\}$ ; let  $(\mathbf{Z}/r\mathbf{Z})^\times = \bigsqcup_{y \in Y} Hy$  with a suitable  $Y$ . Since  $bs \in r\mathbf{Z}$ , we have  $bx \equiv b \pmod{r}$  for every  $x \in H$ . Also, since  $\chi$  is primitive,  $\chi$  cannot be trivial on  $H$ . Thus, putting  $\zeta = \mathbf{e}(1/r)$ , we have

$$\sum_{c=1}^r \chi(c) \zeta^{bc} = \sum_{y \in Y} \sum_{x \in H} \chi(yx) \zeta^{yxb} = \sum_{y \in Y} \zeta^{yb} \chi(y) \sum_{x \in H} \chi(x) = 0$$

because of Lemma 1.6. This proves (3.8a). Using this result, we have

$$\tau(\chi) \tau(\overline{\chi}) = \sum_{c=1}^r \tau(\chi) \overline{\chi}(c) \zeta^c = \sum_{b=1}^r \sum_{c=1}^r \chi(b) \zeta^{bc} \zeta^c = \sum_{b=1}^r \chi(b) \sum_{c=1}^r \zeta^{c(b+1)},$$

which equals  $\chi(-1)r$ , since the last sum over  $c$  is  $r$  or  $0$  according as  $b+1$  is zero or nonzero in  $\mathbf{Z}/r\mathbf{Z}$ . This proves (3.8b). Next, since  $\chi(-1) = \pm 1$ , we have

$$\overline{\tau(\chi)} = \sum_{c=1}^r \overline{\chi(c)} \zeta^{-c} = \sum_{c=1}^r \overline{\chi(-c)} \zeta^c = \overline{\chi(-1)} \tau(\overline{\chi}) = \chi(-1) \tau(\overline{\chi}).$$

This proves (3.8d), which combined with (3.8b) gives (3.8c).

We now present a formula which may be called a generalized quadratic reciprocity law, and from which we derive (3.3) and (3.4).

**Theorem 3.4.** *Let  $\chi$  be a primitive character modulo  $r$  such that  $\overline{\chi} = \chi$ . Then  $\chi(p) = \chi(-1)^{(p-1)/2} \left(\frac{r}{p}\right)$  for every odd prime number  $p$  prime to  $r$ .*

PROOF. Put  $\tau = \tau(\chi)$ ,  $\zeta = \mathbf{e}(1/r)$ , and  $R = \mathbf{Z}[\zeta]$ . Then  $\tau \in R$  and  $\tau^2 = \chi(-1)r$  by (3.8b). Let  $p$  be an odd prime number prime to  $r$ . Then

$$(*) \quad \tau^p = (\tau^2)^{(p-1)/2} \cdot \tau = \chi(-1)^{(p-1)/2} r^{(p-1)/2} \tau.$$

From the binomial theorem we easily see that  $(\alpha + \beta)^p \equiv \alpha^p + \beta^p \pmod{pR}$  for every  $\alpha, \beta \in R$ . We have therefore

$$\tau^p = \left( \sum_{a=1}^{r-1} \chi(a) \zeta^a \right)^p \equiv \sum_{a=1}^{r-1} \chi(a) \zeta^{ap} \equiv \chi(p) \tau \pmod{pR}$$

by (3.8a). Combining this with (\*) and (3.1), we obtain

$$\chi(p) \tau \equiv \tau^p \equiv \chi(-1)^{(p-1)/2} \left(\frac{r}{p}\right) \tau \pmod{pR}.$$

Multiplying this by  $\overline{\tau}$  and employing (3.8c), we obtain

$$(**) \quad \chi(p) r \equiv \chi(-1)^{(p-1)/2} \left(\frac{r}{p}\right) r \pmod{pR}.$$

Since  $pR \cap \mathbf{Z}$  is an ideal of  $\mathbf{Z}$  containing  $p$ , we have  $pR \cap \mathbf{Z} = p\mathbf{Z}$  or  $pR \cap \mathbf{Z} = \mathbf{Z}$ . If  $pR \cap \mathbf{Z} = \mathbf{Z}$ , then  $p^{-1} \in R$ . Since  $R = \sum_{m=0}^{r-1} \mathbf{Z} \zeta^m$ ,  $R$  is finitely generated over  $\mathbf{Z}$ , and so  $\bigcup_{n=1}^{\infty} \sum_{i=0}^n \mathbf{Z} p^{-i}$  must be finitely generated over  $\mathbf{Z}$ , which is impossible. Thus  $pR \cap \mathbf{Z} = p\mathbf{Z}$ . The quantities on both sides of (\*\*) belong to  $\mathbf{Z}$ , and so we have (\*\*) with  $p\mathbf{Z}$  in place of  $pR$ . Since  $p$  is prime to  $r$ , we have  $p(\varepsilon - \varepsilon')$ , where  $\varepsilon = \chi(p)$  and  $\varepsilon' = \chi(-1)^{(p-1)/2} \left(\frac{r}{p}\right)$ . Now  $\varepsilon$  and  $\varepsilon'$  are  $\pm 1$ , and so  $\varepsilon = \varepsilon'$ , which proves the theorem.

**3.5.** Let  $q$  be an odd prime number. As observed in §3.1,  $x \mapsto \left(\frac{x}{q}\right)$  is a character modulo  $q$ , which is clearly primitive. Taking this to be  $\chi$  in Theorem 3.4 and employing (3.2), we obtain (3.4).

Next, to prove (3.3), define  $\chi_1 : (\mathbf{Z}/8\mathbf{Z})^\times \rightarrow \{\pm 1\}$  by  $\chi_1(a) = 1$  if  $a \pm 1 \in 8\mathbf{Z}$ , and  $\chi_1(a) = -1$  if  $a \pm 3 \in 8\mathbf{Z}$ . We easily see that  $\chi_1$  is a primitive

character modulo 8 and  $\chi_1(-1) = 1$ . Therefore Theorem 3.4 shows that  $\left(\frac{2}{p}\right) = \left(\frac{8}{p}\right) = \chi_1(p)$  for every odd prime number  $p$ . This proves (3.3).

**3.6.** Let  $\xi$  be a nontrivial character modulo a positive integer  $t > 2$ . Then we can find a primitive character  $\chi$  modulo a divisor  $r$  of  $t$  such that  $\chi(a) = \xi(a)$  for every  $a$  prime to  $t$ , and such a  $\chi$  is unique for  $\xi$ . This can be shown as follows. If  $t$  is a power  $p^e$  of a prime number  $p$ , then we take  $r$  to be the smallest power  $p^c$  such that  $\xi(a) = 1$  if  $a - 1 \in p^c\mathbf{Z}$ . We can take  $\chi$  to be the same as  $\xi$  as a function on  $\mathbf{Z}$ . In the general case, we take the prime decomposition  $t = p_1^{e_1} \cdots p_s^{e_s}$  with prime numbers  $p_i$ . By (2.1a),  $(\mathbf{Z}/t\mathbf{Z})^\times \cong \prod_{i=1}^s (\mathbf{Z}/p_i^{e_i})^\times$ . Let  $\xi_i$  be the restriction of  $\xi$  to  $(\mathbf{Z}/p_i^{e_i})^\times$ . If  $\xi_i$  is trivial, we disregard  $(\mathbf{Z}/p_i^{e_i})^\times$  and  $\xi_i$ . For each nontrivial  $\xi_i$  we take the smallest power  $p_i^{c_i}$  such that  $\xi_i(a) = 1$  if  $a - 1 \in p_i^{c_i}\mathbf{Z}$ . Then we take  $r$  to be the product of all such  $p_i^{c_i}$  and define  $\chi$  in an obvious way.

Given  $\xi$  we call  $\chi$  **the primitive character associated with  $\xi$** , and the integer  $r$  **the conductor of  $\xi$** . Thus a character  $\xi$  modulo  $t$  is primitive if and only if  $t$  is the conductor of  $\xi$ . We also see that the conductor of a character is either odd or divisible by 4, since  $(\mathbf{Z}/2\mathbf{Z})^\times$  is trivial.

We call a character  $\chi$  **real** if  $\overline{\chi} = \chi$ , or equivalently, if the nonzero values of  $\chi$  are  $\pm 1$ .

**Theorem 3.7.** *Let  $m$  be a square-free integer  $\neq 1$ . Let  $c = |m|$  if  $m - 1 \in 4\mathbf{Z}$  and  $c = 4|m|$  if  $m - 1 \notin 4\mathbf{Z}$ . Then there exists a real primitive character  $\chi$  of conductor  $c$  such that  $\chi(p) = \left(\frac{m}{p}\right)$  for every odd prime number  $p$  prime to  $m$ , and  $\chi(-1)m > 0$ . Moreover, every real primitive character is of this type.*

PROOF. There are three cases: (1)  $m - 1 \in 4\mathbf{Z}$ ; (2)  $m - 2 \in 4\mathbf{Z}$ ; (3)  $m - 3 \in 4\mathbf{Z}$ . The prime decompositions of  $c$  and  $m$  are as follows:

- (1)  $c = p_1 \cdots p_r q_1 \cdots q_s$ ,  $m = \varepsilon p_1 \cdots p_r q_1 \cdots q_s$ ,  $\varepsilon = (-1)^s$ ,
- (2)  $c = 8p_1 \cdots p_r q_1 \cdots q_s$ ,  $m = 2\varepsilon p_1 \cdots p_r q_1 \cdots q_s$ ,  $\varepsilon = \pm 1$ ,
- (3)  $c = 4p_1 \cdots p_r q_1 \cdots q_s$ ,  $m = \varepsilon p_1 \cdots p_r q_1 \cdots q_s$ ,  $\varepsilon = (-1)^{s-1}$ .

Here  $p_i$  and  $q_j$  are prime numbers;  $p_i - 1 \in 4\mathbf{Z}$ ,  $q_j + 1 \in 4\mathbf{Z}$ . Define  $\chi$  as follows:

$$(1') \quad \chi(a) = \prod_{i=1}^r \left(\frac{a}{p_i}\right) \prod_{j=1}^s \left(\frac{a}{q_j}\right),$$

$$(2') \quad \chi(a) = \chi_1(a) \chi_0(a)^{s+\kappa} \prod_{i=1}^r \left(\frac{a}{p_i}\right) \prod_{j=1}^s \left(\frac{a}{q_j}\right),$$

$$(3') \quad \chi(a) = \chi_0(a) \prod_{i=1}^r \left( \frac{a}{p_i} \right) \prod_{j=1}^s \left( \frac{a}{q_j} \right).$$

Here  $\chi_1$  is the character modulo 8 defined in §3.5, and  $\chi_0$  is the nontrivial character modulo 4;  $\kappa = 0$  if  $\varepsilon = 1$  and  $\kappa = 1$  if  $\varepsilon = -1$ . We easily see that in all three cases  $\chi$  is real and has conductor  $c$ . Notice that  $\chi_1(-1) = 1$  and  $\chi_0(-1) = -1$ , and so  $\chi(-1) = \varepsilon$  in all cases. By Theorem 3.4,  $\chi(p) = \chi(-1)^{(p-1)/2} \left( \frac{c}{p} \right) = \varepsilon^{(p-1)/2} \left( \frac{c}{p} \right) = \left( \frac{\varepsilon}{p} \right) \left( \frac{c}{p} \right) = \left( \frac{m}{p} \right)$ , since  $\varepsilon c$  is  $m$  or  $4m$ . This proves the first part of our theorem.

As for the second part, in view of what we said in §3.6, primitive characters can be reduced to the characters modulo a prime power  $p^e$ . Assuming  $p$  to be odd, let  $\rho$  be a primitive root modulo  $p^n$  and let  $H$  be the subgroup of  $(\mathbf{Z}/p^n\mathbf{Z})^\times$  consisting of all  $\alpha \pmod{p^n}$  such that  $\alpha - 1 \in p\mathbf{Z}$ . Then  $H$  has index  $p - 1$  in  $(\mathbf{Z}/p^n\mathbf{Z})^\times$  and is generated by  $\rho^{p^{n-1}}$ . If  $\xi$  is a real nontrivial character modulo  $p^n$ , then  $\xi(\rho^2) = 1$ , and so  $\xi(H) = 1$ . Thus  $\xi$  has conductor  $p$ , and  $\xi(a) = \left( \frac{a}{p} \right)$ ; see §3.1. Next we consider  $(\mathbf{Z}/2^n\mathbf{Z})^\times$ . For  $3 \leq n \in \mathbf{Z}$  and  $2 \leq \nu \leq n$  define  $H_\nu$  as in Theorem 2.4. If  $\xi$  is a nontrivial real character of  $(\mathbf{Z}/2^n\mathbf{Z})^\times$ , we see that  $\xi$  must be trivial on the subgroup of  $H_2$  of index 2, which is  $H_3$ . Thus  $\xi$  has conductor 4 or 8. Then we can easily verify that the above list exhausts all real primitive characters. This completes the proof.

**3.8.** Let us now return to (3.0) and determine the prime numbers  $p$  for which (3.0) has a solution. Clearly it has no solution if  $p = 5$ , and it has a solution if  $p = 2$  or  $3$ ; so we assume  $p \nmid 2 \cdot 3 \cdot 5$ . Put  $y = 5x$ . Then (3.0) is equivalent to  $y^2 \equiv 15 \pmod{p}$ , which has a solution if and only if  $\left( \frac{15}{p} \right) = 1$ . By Theorem 3.7, there is a character  $\chi$  of conductor 60 such that  $\left( \frac{15}{p} \right) = \chi(p)$ . Thus our congruence has a solution if and only if  $p \pmod{60}$  belongs to  $\text{Ker}(\chi)$ . More explicitly,

$$\chi(p) = \left( \frac{15}{p} \right) = \left( \frac{5}{p} \right) \left( \frac{3}{p} \right) = (-1)^{(p-1)/2} \left( \frac{p}{5} \right) \left( \frac{p}{3} \right).$$

Then we find that  $\chi(p) = 1$  exactly when  $p$  is congruent modulo 60 to one of the eight integers 1, 7, 11, 17, 43, 49, 53, 59. This settles our problem.

**Exercises. 1.** (a) Let  $m$  be an odd prime; put  $f(x) = x^{m-1} + x^{m-2} + \cdots + x + 1$ . Show that the congruence  $f(x) \equiv 0 \pmod{p}$  with a prime number  $p$  has a solution if and only if either  $p = m$  or  $p \equiv 1 \pmod{m}$ . (Hint: Check whether  $\mathbf{Z}/p\mathbf{Z}$  contains a primitive  $m$ -th root of unity.)

(b) Use this result to show that there are infinitely many prime numbers that are congruent to 1 modulo  $m$ . (Hint: Assuming that  $q_1, \dots, q_k$  are such

prime numbers, look at the prime factors of  $f(mq_1 \cdots q_k)$ .)

2. Prove that  $\sum_{a=0}^{p-1} \exp(2\pi i t a^2/p) = \chi(t)\tau(\chi)$  for every integer  $t$  prime to  $p$ . Here  $p$  is an odd prime number and  $\chi(a) = \left(\frac{a}{p}\right)$ .

3. (i) Let  $p$  be an odd prime number and  $f(x)$  a polynomial with coefficients in  $\mathbf{Z}$ . Show that the number of solutions  $(x, y)$  of the equation  $y^2 = f(x)$  in  $\mathbf{Z}/p\mathbf{Z}$  is given by

$$p + \sum_{a=0}^{p-1} \left( \frac{f(a)}{p} \right).$$

(ii) Prove that if  $p \equiv -1 \pmod{3}$ , then the equation  $y^2 = x^3 - c$  with a fixed integer  $c$  considered over  $\mathbf{Z}/p\mathbf{Z}$  has exactly  $p$  solutions  $(x, y)$ .

#### 4. Lattices in a vector space

4.1. Let  $R$  be a commutative ring. An  $R$ -module  $L$  is called a **free  $R$ -module of rank  $n$**  if  $L$  is isomorphic to the direct sum of  $n$  copies of  $R$ . This is so if and only if  $L$  has  $n$  elements  $e_1, \dots, e_n$  such that  $L = Re_1 + \cdots + Re_n$  and  $\sum_{i=1}^n a_i e_i = 0$  implies  $a_1 = \cdots = a_n = 0$ . We call then  $\{e_i\}_{i=1}^n$  an  **$R$ -basis** of  $L$ . We understand that  $\{0\}$  is a free  $R$ -module of rank 0. An  $R$ -module  $L$  is called **torsion-free** if  $ax \neq 0$  whenever  $0 \neq a \in R$  and  $0 \neq x \in L$ .

Hereafter in this section  $R$  denotes an integral domain,  $F$  the field of quotients of  $R$ , and  $V$  a vector space over  $F$  of finite dimension. (We tacitly assume that  $R \neq F$ , since our statements are trivially true if  $R = F$ .) We will often assume the following condition:

(4.1) *Every ideal of  $R$  is finitely generated over  $R$ .*

Clearly this is satisfied if  $R$  is a principal ideal domain.

By an  **$R$ -lattice** in  $V$  we understand a finitely generated  $R$ -submodule of  $V$  that spans  $V$  over  $F$ .

**Lemma 4.2.** *Let  $X$  be a finitely generated  $R$ -module. Then under (4.1) every  $R$ -submodule of  $X$  is finitely generated over  $R$ .*

PROOF. We have  $X = Rx_1 + \cdots + Rx_n$  with elements  $x_i$  of  $X$ . We prove our lemma by induction on  $n$ . Let  $Y$  be an  $R$ -submodule of  $X$ . We first assume that  $n > 1$  and put  $Z = Rx_1 + \cdots + Rx_{n-1}$  and  $J = \{b \in R \mid bx_n \in Y + Z\}$ . Clearly  $J$  is an ideal of  $R$ , and so by (4.1),  $J = Rb_1 + \cdots + Rb_r$  with  $b_1, \dots, b_r \in J$ . For each  $i$  we have  $b_i x_n = y_i + z_i$  with  $y_i \in Y$  and  $z_i \in Z$ . Take any element  $w$  of  $Y$ . We can put  $w = c_1 x_1 + \cdots + c_n x_n$  with  $c_i \in R$ . Then  $c_n \in J$ , and so  $c_n = \sum_{i=1}^r a_i b_i$  with  $a_i \in R$ , and  $w - \sum_{i=1}^r a_i y_i = \sum_{i=1}^{n-1} c_i x_i + \sum_{j=1}^r a_j z_j \in Z$ . This element is also contained in  $Y$ . Thus  $w - \sum_{i=1}^r a_i y_i \in Y \cap Z$ , which shows that  $Y = (Y \cap Z) + \sum_{i=1}^r Ry_i$ . Our argument is valid even when  $n = 1$ , if we take  $Z = \{0\}$ , in which case we have  $Y = \sum_{i=1}^r Ry_i$ . This



proves the case  $n = 1$ . Returning to the case  $n > 1$ , by induction,  $Y \cap Z$ , being an  $R$ -submodule of  $Z = \sum_{i=1}^{n-1} Rx_i$ , must be finitely generated over  $R$ , and so  $Y$  is finitely generated over  $R$ . This completes the proof.

**Lemma 4.3.** *Under (4.1) the following assertions hold:*

- (i) *If  $L$  and  $M$  are  $R$ -lattices in  $V$ , then  $L + M$  and  $L \cap M$  are  $R$ -lattices in  $V$  and  $cL \subset M$  for some  $c \in R$ ,  $c \neq 0$ .*
- (ii) *If  $W$  is a vector subspace of  $V$  and  $L$  is an  $R$ -lattice in  $V$ , then  $W \cap L$  is an  $R$ -lattice in  $W$ .*

PROOF. Given  $L$  and  $M$  as in (i), we can put  $L = \sum_{i=1}^m Rx_i$  and  $M = \sum_{j=1}^n Ry_j$  with some  $x_i$  and  $y_j$ . Since the  $y_j$  span  $V$  over  $F$ , we have  $x_i = \sum_{j=1}^n a_{ij}y_j$  with  $a_{ij} \in F$ . We can find  $c \in R$ ,  $c \neq 0$ , such that  $ca_{ij} \in R$  for every  $i$  and  $j$ , since  $F$  is the field of quotients of  $R$ . Then  $cx_i \in M$  for every  $i$ , and so  $cL \subset M$ . Thus  $cL \subset L \cap M$ , and so  $L \cap M$  spans  $V$  over  $F$ . By Lemma 4.2,  $L \cap M$  is finitely generated over  $R$ . Therefore  $L \cap M$  is an  $R$ -lattice in  $V$ . That  $L + M$  is an  $R$ -lattice in  $V$  is obvious. As for (ii), take an  $F$ -basis  $\{z_i\}$  of  $W$ . By the same argument as for  $x_i$ , we can find  $b \in R$ ,  $b \neq 0$ , such that  $bz_i \in L$ . Then  $bz_i \in L \cap W$ , and so  $L \cap W$  spans  $W$  over  $F$ . By Lemma 4.2,  $L \cap W$  is finitely generated over  $R$ , and so we obtain (ii).

**Lemma 4.4.** *Let  $V^*$  be the dual of  $V$ , and let  $\langle \ , \ \rangle : V \times V^* \rightarrow F$  be the pairing between  $V$  and  $V^*$ . Given an  $R$ -lattice  $L$  in  $V$ , put*

$$L^* = \{u \in V^* \mid \langle L, u \rangle \subset R\}.$$

*Then  $L^*$  is an  $R$ -lattice in  $V^*$ .*

PROOF. We can find an  $F$ -basis  $\{x_i\}_{i=1}^n$  of  $V$  contained in  $L$ . Put  $M = \sum_{i=1}^n Rx_i$ . By Lemma 4.3(i) we have  $cL \subset M$  for some  $c \in R$ ,  $c \neq 0$ . Then  $M \subset L \subset c^{-1}M$ , and we easily see that  $cM^* \subset L^* \subset M^*$ . Also we have  $M^* = \sum_{i=1}^n Ry_i$  with the basis  $\{y_i\}_{i=1}^n$  of  $V^*$  dual to  $\{x_i\}_{i=1}^n$ . Therefore by Lemma 4.2,  $L^*$  is finitely generated over  $R$ . Since  $cy_i \in L^*$ ,  $L^*$  spans  $V^*$  over  $F$ , and so  $L^*$  is an  $R$ -lattice in  $V^*$ .

## 5. Modules over a principal ideal domain

In this section  $R$  denotes a principal ideal domain,  $F$  its field of quotients, and  $V$  a vector space over  $F$  of finite dimension. We recall basic facts concerning  $R$ -modules, some without proof and some with proof.

**Theorem 5.1.** *Let  $L$  be a free  $R$ -module of rank  $n$ , and  $M$  an  $R$ -submodule of  $L$ . Then there exist  $n$  elements  $x_1, \dots, x_n$  of  $L$  and  $r$  elements  $a_1, \dots, a_r$  of  $R$  with  $r \leq n$  such that  $L = Rx_1 + \dots + Rx_n$ ,  $M = Ra_1x_1 + \dots + Ra_rx_r$ , and  $Ra_1 \supset Ra_2 \supset \dots \supset Ra_r \neq 0$ . Moreover,  $r$  and such ideals*

$Ra_i$  are uniquely determined by  $L$  and  $M$ . Consequently, every  $R$ -submodule of  $L$  is a free  $R$ -module of rank  $\leq n$ .

**Theorem 5.2.** *Every finitely generated  $R$ -module  $K$  is  $R$ -isomorphic to the direct sum of  $t$  ( $\geq 0$ ) copies of  $R$  and  $r$  ( $\geq 0$ ) modules  $R/a_1R, \dots, R/a_rR$  such that  $Ra_1 \supset Ra_2 \supset \dots \supset Ra_r \neq 0$ . Moreover,  $t$  and the ideals  $Ra_i$  are uniquely determined by  $K$ .*

Notice that Theorem 1.4 follows from this theorem with  $R = \mathbf{Z}$ .

**Theorem 5.3.** *Every  $R$ -lattice in  $V$  is a free  $R$ -module of rank  $[V : F]$ .*

PROOF. Let  $L$  be an  $R$ -lattice in  $V$ . Taking an  $F$ -basis  $\{x_i\}_{i=1}^n$  of  $V$ , put  $M = \sum_{i=1}^n Rx_i$ . By Lemma 4.3(i),  $cL \subset M$  with some  $c \in R, c \neq 0$ . By Theorem 5.1,  $cL$  is a free  $R$ -module of rank  $n$ . This proves our theorem, as  $L \cong cL$ .

**Theorem 5.4.** *In the setting of Lemma 4.4 with a principal ideal domain  $R$  we have  $L = \{x \in V \mid \langle x, L^* \rangle \subset R\}$ .*

PROOF. By Theorem 5.3 we have  $L = \sum_{i=1}^n Re_i$  with an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $V$ . Let  $\{f_i\}_{i=1}^n$  be the basis of  $V^*$  dual to  $\{e_i\}_{i=1}^n$ . Then  $L^* = \sum_{i=1}^n Rf_i$ , and our assertion can be shown easily.

**Lemma 5.5.** *Let  $M$  be an  $R$ -submodule of a finitely generated  $R$ -module  $L$ . Then  $L = M \oplus N$  with some torsion-free  $R$ -submodule  $N$  of  $L$  if and only if  $L/M$  is a free  $R$ -module of finite rank.*

PROOF. Suppose that  $L/M$  is a free  $R$ -module of rank  $r$ . Take  $r$  elements  $x_1, \dots, x_r$  of  $L$  so that the classes of the  $x_i$  modulo  $M$  generate  $L/M$  and put  $N = \sum_{i=1}^r Rx_i$ . Then we can easily verify that  $N$  is torsion-free and  $L = M \oplus N$ . The converse is obvious.

**Lemma 5.6.** *The group of all  $R$ -automorphisms of a free  $R$ -module of rank  $n$  is isomorphic to  $GL_n(R)$ .*

**Theorem 5.7.** *For every  $m \times n$ -matrix  $T$  of rank  $r$  with coefficients in  $R$ , there exists an element  $U$  of  $GL_m(R)$  and an element  $V$  of  $GL_n(R)$  such that*

$$UTV = \begin{bmatrix} D & 0_{n-r}^r \\ 0_{m-r}^{m-r} & 0_{n-r}^{m-r} \end{bmatrix}, \quad D = \text{diag}[e_1, \dots, e_r]$$

*with nonzero elements  $e_1, \dots, e_r$  in  $R$ ,  $e_i | e_{i+1}$ . The ideals  $e_i R$  are uniquely determined by  $T$ .*

This is essentially a restatement of Theorem 5.1.

**Lemma 5.8.** *Let  $L$  be a  $\mathbf{Z}$ -lattice in a vector space  $V$  over  $\mathbf{Q}$  of finite dimension, and  $T$  a  $\mathbf{Q}$ -linear automorphism of  $V$  that maps  $L$  into  $L$ . Then  $[L : TL] = |\det(T)|$ , where  $TL$  denotes the image of  $L$  under  $T$ .*

PROOF. We may assume that  $L = \mathbf{Z}_1^n$  and  $V = \mathbf{Q}_1^n$ ; then we may view  $T$  as an element of  $M_n(\mathbf{Z}) \cap GL_n(\mathbf{Q})$  acting on  $V$  by left multiplication. By Theorem 5.7, we can find  $U, V \in GL_n(\mathbf{Z})$  such that  $UTV = \text{diag}[e_1, \dots, e_n]$  with  $e_i \in \mathbf{Z}$ . Then  $L = UL = VL$ , and so  $[L : TL] = [L : UTVL] = |e_1 \cdots e_n| = |\det(T)|$  as expected.

**Exercises. 1.** Let  $G$  be a finite subgroup of  $GL_n(F)$ . Prove that there exists an element  $S$  of  $GL_n(F)$  such that  $STS^{-1}$  has coefficients in  $R$  for every  $T \in G$ . (Hint: Consider  $GL_n(F)$  the group of all linear transformations of  $V = F^n$ . Let  $M = \sum_{T \in G} T(L)$  with an  $R$ -lattice  $L$  in  $V$ ; show that  $T(M) = M$  for every  $T \in G$ .)

**2.** Let  $L$  be a free  $R$ -module of rank  $n$  with an  $R$ -basis  $\{x_1, \dots, x_n\}$ , and let  $y = \sum_{i=1}^n c_i x_i$  with  $n$  elements  $c_i$  of  $R$  which have no common divisors other than the elements of  $R^\times$ . Prove that  $L/Ry$  is torsion-free.

**3.** The notation being as in Lemma 4.4, define  $M^*$  in a similar way for an  $R$ -submodule  $M$  of  $L$ . Show that  $L^* \subset M^*$ , and  $L/M$  is isomorphic to  $M^*/L^*$ .

## ARITHMETIC IN AN ALGEBRAIC NUMBER FIELD

### 6. Valuations and $p$ -adic numbers

**6.1.** Let  $F$  be a field. A map  $\nu : F \rightarrow \mathbf{R} \cup \{\infty\}$  is called an **order function** of  $F$  if it satisfies the following conditions:

- (i)  $\nu(x) = \infty \iff x = 0$ ;
- (ii)  $\nu(xy) = \nu(x) + \nu(y)$ ;
- (iii)  $\nu(x + y) \geq \text{Min}\{\nu(x), \nu(y)\}$ ;
- (iv) *There exists an element  $z \in F, z \neq 0$ , such that  $\nu(z) \neq 0$ .*

Here  $\infty + a = a + \infty = \infty$  and  $\infty \geq a$  for every  $a \in \mathbf{R} \cup \{\infty\}$ . Taking  $z$  as in (iv), we have  $\infty \neq \nu(z) = \nu(z \cdot 1) = \nu(z) + \nu(1)$ , and so  $\nu(1) = 0$ . Then  $0 = \nu((-1)(-1)) = \nu(-1) + \nu(-1)$ , and so  $\nu(-1) = 0$ , and  $\nu(-x) = \nu(-1) + \nu(x) = \nu(x)$ . There is a noteworthy fact:

$$(6.1) \quad \nu(x + y) = \text{Min}\{\nu(x), \nu(y)\} \quad \text{if } \nu(x) \neq \nu(y).$$

Indeed, assuming that  $\nu(x) < \nu(y)$ , we have  $\nu(x) = \nu(x + y + (-y)) \geq \text{Min}\{\nu(x + y), \nu(y)\}$ , from which (6.1) follows.

An order function  $\nu$  is called **discrete** if there exists a positive real number  $t$  such that  $\nu(F^\times) = t\mathbf{Z}$ . A discrete order function is called **normalized** if  $\nu(F^\times) = \mathbf{Z}$ .

To find an example of an order function, take  $F = \mathbf{Q}$  and fix a prime number  $p$ . Given  $x \in \mathbf{Q}^\times$ , considering the prime decomposition of  $x$ , we can put  $x = p^m a/b$  with  $m \in \mathbf{Z}$  and nonzero integers  $a, b$  prime to  $p$ . We then put  $\nu_p(x) = m$ . We also put  $\nu_p(0) = \infty$ . It can easily be seen that this is a normalized order function.

**6.2.** Let  $F$  be a field. A map  $\varphi : F \rightarrow \{x \in \mathbf{R} \mid x \geq 0\}$  is called a **valuation** of  $F$  if it satisfies the following conditions:

- (i)  $\varphi(x) = 0 \iff x = 0$ ;
- (ii)  $\varphi(xy) = \varphi(x)\varphi(y)$ ;
- (iii)  $\varphi(x + y) \leq \varphi(x) + \varphi(y)$ ;
- (iv) *There exists an element  $z \in F, z \neq 0$ , such that  $\varphi(z) \neq 1$ .*

Such a  $\varphi$  is called **nonarchimedean** if

$$(v) \quad \varphi(x+y) \leq \text{Max}\{\varphi(x), \varphi(y)\}.$$

Otherwise it is called **archimedean**. Notice that (v) implies (iii). We easily see that  $\varphi(\pm 1) = 1$  and  $\varphi(-x) = \varphi(x)$ . Since  $\varphi(x) = \varphi(x - y + y) \leq \varphi(x - y) + \varphi(y)$ , we have  $\varphi(x) - \varphi(y) \leq \varphi(x - y)$ . Exchanging  $x$  and  $y$ , we obtain  $\varphi(y) - \varphi(x) \leq \varphi(y - x) = \varphi(x - y)$ . Thus

$$(6.2) \quad |\varphi(x) - \varphi(y)| \leq \varphi(x - y).$$

If there is an isomorphism  $\sigma$  of  $F$  onto a subfield of  $\mathbf{C}$ , then we obtain an archimedean valuation  $\psi$  of  $F$  by putting  $\psi(x) = |x^\sigma|$  for  $x \in F$ .

Given an order function  $\nu$  of  $F$ , put  $\varphi(x) = c^{\nu(x)}$  with a fixed real number  $c$  such that  $0 < c < 1$ . Then  $\varphi$  is a nonarchimedean valuation of  $F$ . Conversely, given a nonarchimedean valuation  $\varphi$  of  $F$ , put  $\nu(x) = -\log \varphi(x)$  for  $x \neq 0$  and  $\nu(0) = \infty$ . Then it can be shown that  $\nu$  is an order function of  $F$  and  $\varphi(x) = e^{-\nu(x)}$ .

Take  $F = \mathbf{Q}$ ; fix a prime number  $p$ . Define  $\nu_p$  as in §6.1 with this  $p$ . Usually we define a nonarchimedean valuation  $\varphi_p$  by  $\varphi_p(x) = p^{-\nu_p(x)}$ . For example,  $\varphi_p(\pm p^m) = p^{-m}$ .

**6.3.** Given a valuation  $\varphi$  of  $F$ , put  $\mu(x, y) = \varphi(x - y)$ . We can easily verify that  $F$  is a metric space with respect to  $\mu$ . Thus we can speak of open sets, closed sets, and continuity with respect to the topology defined by this metric. Then the maps  $(x, y) \mapsto x + y, x - y, xy, x/y$  are continuous. (Of course we assume  $y \neq 0$  for  $x/y$ .) The limit and convergence of an infinite sequence in  $F$  can be naturally defined. To be explicit, for an infinite sequence  $\{a_n\}_{n=1}^\infty$  in  $F$  and  $b \in F$  we write  $\lim_{n \rightarrow \infty} a_n = b$  if  $\lim_{n \rightarrow \infty} \varphi(a_n - b) = 0$ , which is so if and only if  $\lim_{n \rightarrow \infty} \nu(a_n - b) = \infty$  if  $\varphi$  is obtained from an order function  $\nu$ . If  $\lim_{n \rightarrow \infty} \sum_{k=1}^n a_k = c$ , then we write  $c = \sum_{k=1}^\infty a_k$ .

For example, if  $\nu_p$  is the order function of  $\mathbf{Q}$  defined at the end of §6.1, then  $\lim_{n \rightarrow \infty} p^n = 0$  and  $\sum_{k=0}^\infty p^k = (1 - p)^{-1}$ .

**6.4.** An infinite sequence  $\{x_n\}_{n=1}^\infty$  in  $F$  is called a **Cauchy sequence** (with respect to  $\varphi$ ) if for every  $\varepsilon > 0$  there exists a positive integer  $N$  such that  $\varphi(x_m - x_n) < \varepsilon$  for every  $m, n > N$ . If  $\varphi$  is obtained from an order function  $\nu$  as above, then  $\{x_n\}_{n=1}^\infty$  is a Cauchy sequence if for every  $C \in \mathbf{R}, > 0$ , there exists a positive integer  $N$  such that  $\nu(x_m - x_n) > C$  for every  $m, n > N$ . We call  $F$  **complete** (with respect to  $\varphi$ ) if every Cauchy sequence in  $F$  is convergent.

**Theorem 6.5.** *Given a valuation  $\varphi$  of a field  $F$ , we can find a field  $F^*$  and a valuation  $\varphi^*$  of  $F^*$  with the following properties:*

- (1)  $F^*$  is complete with respect to  $\varphi^*$ ;
- (2)  $F$  is a subfield of  $F^*$  and  $\varphi^* = \varphi$  on  $F$ ;

(3)  $F$  is dense in  $F^*$ .

(4) If  $\varphi$  is obtained from an order function  $\nu$  of  $F$ , then  $\varphi^*$  is obtained from an order function  $\nu^*$  of  $F^*$  that coincides with  $\nu$  on  $F$ . Moreover,  $(F^*, \varphi^*)$  is unique for  $(F, \varphi)$  up to isomorphism.

Since the whole proof is long and tedious, we merely give its idea. Let  $X$  be the set of all Cauchy sequences in  $F$ . This is a commutative ring with respect to componentwise operations. Let  $Y$  be the subset of  $X$  consisting of all the sequences convergent to 0. Then  $Y$  is a maximal ideal of  $X$ , and  $F^*$  can be obtained as  $X/Y$ .

The field  $F^*$  is called **the  $\varphi$ -completion** of  $F$  and also **the  $\nu$ -completion** of  $F$  if  $\varphi$  is obtained from an order function  $\nu$ .

**Lemma 6.6.** *Suppose that  $F$  is complete with respect to a nonarchimedean valuation  $\varphi$  obtained from an order function  $\nu$ . Then*

$$\sum_{n=1}^{\infty} a_n \text{ is convergent} \\ \iff \lim_{n \rightarrow \infty} a_n = 0 \iff \lim_{n \rightarrow \infty} \nu(a_n) = \infty \iff \lim_{n \rightarrow \infty} \varphi(a_n) = 0.$$

PROOF. Suppose  $\lim_{n \rightarrow \infty} \varphi(a_n) = 0$ ; put  $b_n = \sum_{k=1}^n a_k$ . Since  $b_{n+p} - b_n = a_{n+1} + \cdots + a_{n+p}$ , we have  $\varphi(b_{n+p} - b_n) \leq \text{Max}\{\varphi(a_{n+1}), \dots, \varphi(a_{n+p})\}$ . Then we see that  $\{b_n\}_{n=1}^{\infty}$  is a Cauchy sequence, and so it is convergent. The remaining part of our lemma is trivial.

**6.7.** Given an order function  $\nu$  of a field  $F$ , put

$$(6.3) \quad R = \{x \in F \mid \nu(x) \geq 0\}, \quad M = \{x \in F \mid \nu(x) > 0\}.$$

Clearly

$$(6.4) \quad a \in R, a \notin M \iff \nu(a) = 0 \iff a \in R^\times.$$

We easily see that  $R$  is a subring of  $F$ ,  $M$  is a maximal ideal of  $R$ , and  $F$  is the field of quotients of  $R$ . Moreover,  $M$  is the only maximal ideal of  $R$ . We call  $R$  **the valuation ring of  $\nu$**  and  $M$  **the maximal ideal of  $R$** .

Now suppose  $\nu$  is discrete and normalized; then an element  $\pi$  of  $F$  is called a **prime element** of  $F$  (with respect to  $\nu$ ) if  $\nu(\pi) = 1$ . For any such element  $\pi$  we have

$$\pi^m R = \{x \in F \mid \nu(x) \geq m\} = \{x \in F \mid \nu(x) > m - 1\}.$$

This is an open and closed subset of  $F$ , since  $\nu$  is continuous. Every nonzero ideal of  $R$  is of the form  $\pi^m R$  with  $m > 0$ . Thus  $R$  is a principal ideal domain. Every neighborhood of 0 contains  $\pi^m R$  for some  $m$ , and so the sets  $\pi^m R$  for all  $m \in \mathbf{Z}, > 0$ , form a base of neighborhoods of 0.

If  $\nu$  is the order function  $\nu_p$  of  $\mathbf{Q}$ , then

$$R = \{a/b \mid a \in \mathbf{Z}, b \in \mathbf{Z}, b \notin p\mathbf{Z}\},$$

$$M = pR, \quad R = M + \mathbf{Z}, \quad p\mathbf{Z} = M \cap \mathbf{Z}, \quad R/M \cong \mathbf{Z}/p\mathbf{Z}.$$

**Theorem 6.8.** *Let the notation be as in Theorem 6.5; suppose that  $\varphi$  is obtained from a discrete order function  $\nu$ . Let  $R$  resp.  $R^*$  be the valuation ring of  $\nu$  resp.  $\nu^*$  and let  $M$  resp.  $M^*$  be the maximal ideal of  $R$  resp.  $R^*$ . Then the following assertions hold:*

(i)  $\nu^*(F^*) = \nu(F)$ ; consequently  $\nu^*$  is discrete, and every prime element of  $F$  is a prime element of  $F^*$ .

(ii)  $R^*$  resp.  $M^*$  is the closure of  $R$  resp.  $M$  in  $F^*$ .

(iii)  $R^* = R + M^*$ ,  $M = R \cap M^*$ , and  $R/M \cong R^*/M^*$ .

(iv) Suppose that  $\nu$  is normalized. Let  $\{\pi_k\}_{k \in \mathbf{Z}}$  be a subset of  $F$  such that  $\nu(\pi_k) = k$ , and let  $S$  be a complete set of representatives for  $R/M$  containing 0. Then every element of  $F^*$  can be written uniquely in the form  $\sum_{k=m}^{\infty} s_k \pi_k$  with  $m \in \mathbf{Z}$  and  $s_k \in S$ . In particular, we can take  $\pi_k = \pi^k$  with any fixed prime element  $\pi$  of  $F$ . Also, we have  $\nu^*(\sum_{k=m}^{\infty} s_k \pi_k) = m$  if  $s_m \neq 0$ .

PROOF. We may assume that  $\nu$  is normalized. Since  $F$  is dense in  $F^*$ , given  $a \in F^*$ ,  $a \neq 0$ , and any positive number  $t$ , there exists an element  $b \in F$  such that  $\nu^*(b-a) > t$ . Take  $t$  so that  $t > \nu^*(a)$ . Then  $\nu(b) = \nu^*(b-a+a) = \nu^*(a)$  by (6.1), which proves (i). If  $a \in R^*$ , then  $\nu(b) = \nu^*(a) \leq 0$ , and so  $b \in R$ , which proves that  $R$  is dense in  $R^*$ . Similarly  $M$  is dense in  $M^*$ . This proves (ii). In the case  $a \in R^*$  we have  $a = a - b + b$ . Since  $\nu^*(a-b) > 0$ , we have  $a-b \in M^*$ , and so  $R^* = M^* + R$ . That  $M = R \cap M^*$  is trivial. Then  $R^*/M^* = (R + M^*)/M^* \cong R/(R \cap M^*) = R/M$ . This proves (iii). To prove (iv), given  $0 \neq x \in F^*$ , let  $m = \nu^*(x)$ . Observe that

$$(6.5) \quad S\pi_n \text{ represents } M^n/M^{n+1}.$$

Let us now prove by induction (on  $n \geq m$ ) that  $x - \sum_{k=m}^n s_k \pi_k \in M^{n+1}$  with suitable  $s_k \in S$ . If  $n = m$ , this follows from (6.5). Assume that we have found  $s_k$  for  $m \leq k \leq n$ . By (6.5) with  $n+1$  in place of  $n$  we can find a desired  $s_{n+1}$ . By Lemma 6.6,  $\sum_{k=m}^{\infty} s_k \pi_k$  is meaningful as an element of  $F^*$ . Call it  $y$ . Then  $x - y = \lim_{n \rightarrow \infty} (x - \sum_{k=m}^n s_k \pi_k) = 0$ , since the difference in the parentheses belongs to  $M^{n+1}$ . Thus  $x = y = \sum_{k=m}^{\infty} s_k \pi_k$ . To prove the uniqueness of  $s_k$ , suppose  $x = \sum_{k=\ell}^{\infty} t_k \pi_k$  with  $t_k \in S$ . Clearly  $m = \nu^*(x) \geq \ell$ . Putting  $s_k = 0$  for  $\ell \leq k < m$ , and  $u_k = s_k - t_k$ , we have  $0 = \sum_{k=\ell}^{\infty} u_k \pi_k$ . Then we easily see that  $u_k = 0$  by induction.

**Lemma 6.9.** *The notation being as in Theorem 6.8, suppose that  $\nu$  is discrete and  $R/M$  is finite. Then both  $R^*$  and  $(R^*)^\times$  are open compact sets and  $F^*$  is locally compact.*

PROOF. As observed in §6.7,  $R^*$  and  $M^*$  are open and closed subsets of  $F^*$ . Since  $(R^*)^\times$  is the complement of  $M^*$  in  $R^*$ , it must be open and

closed. To prove that  $R^*$  is compact, recall that a metric space is compact if every infinite sequence has a convergent subsequence. Let  $X = \{x_n\}_{n=1}^\infty$  with  $x_n \in R^*$ . We are going to construct a chain of subsequences  $X = X_0 \succ X_1 \succ \cdots \succ X_m \succ \cdots$  and a sequence  $\{c_m\}_{m=0}^\infty$  with  $c_m \in R^*$  such that  $X_m$  is contained in  $c_m + \pi^m R^*$ , where we write  $X \succ Y$  when  $Y$  is a subsequence of  $X$ . We first take  $c_0 = 0$ . Suppose  $X_m$  has been established. Observe that  $c_m + \pi^m R^* = \bigsqcup_{i=1}^q (d_i + \pi^{m+1} R^*)$ , where  $q = [R : M]$ . Therefore we can find an infinite subsequence  $X_{m+1}$  of  $X_m$  contained in  $d_i + \pi^{m+1} R^*$  with some  $i$ . Putting  $d_i = c_{m+1}$ , we obtain the desired  $\{X_m\}$  and  $\{c_m\}$ . Now pick  $y_m$  from  $X_m$  so that  $\{y_m\}_{m=1}^\infty$  is a subsequence of  $X$ . Then we see that  $y_k \in c_m + \pi^m R^*$  if  $k \geq m$ , and hence  $y_k - y_m \in \pi^m R^*$  if  $k \geq m$ . Thus  $\{y_m\}_{m=1}^\infty$  is a Cauchy sequence, and so is convergent. This proves that  $R^*$  is compact, and consequently  $F^*$  is locally compact. The group  $(R^*)^\times$ , being closed in  $R^*$ , must be compact. This completes the proof.

**6.10.** Fix a prime number  $p$  and define an order function  $\nu_p$  of  $\mathbf{Q}$  as in §6.2. The  $\nu_p$ -completion of  $\mathbf{Q}$  is called the  **$p$ -adic field** and denoted by  $\mathbf{Q}_p$ . The closure of  $\mathbf{Z}$  in  $\mathbf{Q}_p$  is denoted by  $\mathbf{Z}_p$ . An element of  $\mathbf{Q}_p$  (resp.  $\mathbf{Z}_p$ ) is called a  **$p$ -adic number** (resp.  **$p$ -adic integer**). By Theorem 6.8(iv),  $\mathbf{Q}_p$  consists of all the infinite sums  $\sum_{k=m}^\infty c_k p^k$  with  $m \in \mathbf{Z}$  and  $c_k \in \{0, 1, 2, \dots, p-1\}$ .  $\mathbf{Z}_p$  consists of all such sums with  $m = 0$ . By Lemma 6.9,  $\mathbf{Q}_p$  is a locally compact topological additive group; both  $\mathbf{Z}_p$  and  $\mathbf{Z}_p^\times$  are open and compact subsets of  $\mathbf{Q}_p$ .

Suppose  $p \neq 2$ . For every  $x \in \mathbf{Z}_p$  we define  $\left(\frac{x}{p}\right)$  by  $\left(\frac{x}{p}\right) = \left(\frac{\xi}{p}\right)$  with any  $\xi \in \mathbf{Z}$  such that  $x - \xi \in p\mathbf{Z}_p$ . Clearly this is well defined.

**Lemma 6.11.** *Let  $\mathbf{Z}_p^{\times 2} = \{x^2 \mid x \in \mathbf{Z}_p^\times\}$ . Then*

- (i)  $\mathbf{Z}_p^{\times 2} = \left\{x \in \mathbf{Z}_p^\times \mid \left(\frac{x}{p}\right) = 1\right\} \quad \text{if } p \neq 2,$
- (ii)  $\mathbf{Z}_p^{\times 2} = \{x \in \mathbf{Z}_p^\times \mid x - 1 \in 8\mathbf{Z}_p\} \quad \text{if } p = 2,$
- (iii)  $[\mathbf{Z}_p^\times : \mathbf{Z}_p^{\times 2}] = \begin{cases} 2 & \text{if } p \neq 2, \\ 4 & \text{if } p = 2, \end{cases}$
- (iv)  $[\mathbf{Q}_p^\times : \mathbf{Q}_p^{\times 2}] = \begin{cases} 4 & \text{if } p \neq 2, \\ 8 & \text{if } p = 2. \end{cases}$

**PROOF.** Clearly the left-hand side of (i) is contained in the right-hand side. To prove the opposite inclusion, let  $x \in \mathbf{Z}_p^\times$ . Now consider the natural homomorphism of  $(\mathbf{Z}_p/p^n \mathbf{Z}_p)^\times$  onto  $(\mathbf{Z}/p^n \mathbf{Z})^\times$ . In view of Theorem 2.3, we can find an element  $r \in \mathbf{Z}$  that generates  $(\mathbf{Z}_p/p^n \mathbf{Z}_p)^\times$  and such that  $x - r^k \in p^n \mathbf{Z}_p$  with some  $k$ . If  $\left(\frac{x}{p}\right) = 1$ , then  $k \in 2\mathbf{Z}$ , as  $\left(\frac{r}{p}\right) = -1$ . Thus we can find



an element  $y_n \in \mathbf{Z}$  such that  $y_n^2 - x \in p^n \mathbf{Z}_p$ . The sequence  $\{y_n\}_{n=1}^\infty$  has a subsequence that converges to an element  $z$  of  $\mathbf{Z}_p$  and clearly  $z^2 = x$ . This proves (i). We can prove (ii) in the same manner by means of Theorem 2.4. Then (iii) follows immediately from (i) and (ii). We have  $\mathbf{Q}_p^\times = \mathbf{Z}_p^\times \cdot \{p^m \mid m \in \mathbf{Z}\}$ , and so (iv) follows immediately from (iii).

**Theorem 6.12.** (i) *If  $p \neq 2$ , then  $\mathbf{Q}_p$  has exactly three nonisomorphic quadratic extensions  $\mathbf{Q}_p(\sqrt{r})$ ,  $\mathbf{Q}_p(\sqrt{p})$ , and  $\mathbf{Q}_p(\sqrt{pr})$ , where  $r$  is any quadratic nonresidue modulo  $p$ .*

(ii) *If  $p = 2$ , then  $\mathbf{Q}_p$  has exactly seven nonisomorphic quadratic extensions, which are represented by  $\mathbf{Q}_2(\sqrt{s})$ ,  $\mathbf{Q}_2(\sqrt{2s})$ , and  $\mathbf{Q}_2(\sqrt{2})$ , where  $s \in \{-1, \pm 3\}$ .*

PROOF. Observe that every extension  $K$  of  $\mathbf{Q}_p$  of degree  $\leq 2$  is of the form  $K = \mathbf{Q}_p(\sqrt{\alpha})$  with  $\alpha \in \mathbf{Q}_p^\times$ . Assigning  $\mathbf{Q}_p(\sqrt{\alpha})$  to  $\alpha$ , we obtain a bijection of  $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$  onto the set of all such extensions of  $\mathbf{Q}_p$  (contained in a fixed algebraic closure of  $\mathbf{Q}_p$ ). Suppose  $p = 2$ . By Lemma 6.11 (ii),  $\mathbf{Z}_2^\times / \mathbf{Z}_2^{\times 2}$  consists of  $\{\pm 1, \pm 3 \pmod{8\mathbf{Z}_2}\}$ , and so  $\mathbf{Q}_2^\times / \mathbf{Q}_2^{\times 2}$  can be represented by  $\{\pm 1, \pm 3, \pm 2, \pm 6\}$ . The identity element corresponds to the trivial extension  $\mathbf{Q}_2$  of  $\mathbf{Q}_2$ , and therefore we obtain (ii). If  $p \neq 2$ ,  $\mathbf{Q}_p^\times / \mathbf{Q}_p^{\times 2}$  can be represented by  $\{1, r, p, pr\}$ , and we obtain (i).

**Theorem 6.13.** *Let  $\varphi$  and  $\psi$  be valuations of a field  $F$ . Then the following conditions are equivalent to each other:*

- (1)  $\varphi(x) > 1 \iff \psi(x) > 1$ .
- (2)  $\varphi(a) > \varphi(b) \iff \psi(a) > \psi(b)$ .
- (3)  $\lim_{n \rightarrow \infty} \varphi(a_n) = 0 \iff \lim_{n \rightarrow \infty} \psi(a_n) = 0$ .

(4) *There exists a positive number  $\alpha$  such that  $\psi(x) = \varphi(x)^\alpha$  for every  $x \in F$ .*

PROOF. It is easy to see that (1)  $\iff$  (2) and (4)  $\implies$  (3). Taking  $a_n$  of (3) to be  $(b/a)^n$ , we can prove that (3)  $\implies$  (2). Let us now derive (4) from (1). Once we assume (1), then (2) holds. Also, taking  $a^{-1}$  in place of  $a$ , we find that  $\varphi(a) < 1 \iff \psi(a) < 1$ . Consequently,  $\varphi(a) = 1 \iff \psi(a) = 1$ . Take  $z \in F$  so that  $\varphi(z) > 1$ . Given  $a \in F^\times$ , we can find  $\lambda \in \mathbf{R}$  such that  $\varphi(a) = \varphi(z)^\lambda$ . Take integers  $m > 0$  and  $n$  so that  $n/m < \lambda$ . Then  $\varphi(z)^n < \varphi(z)^{\lambda m} = \varphi(a)^m$ , and so  $\psi(z)^n < \psi(a)^m$ . Thus  $\psi(z)^{n/m} < \psi(a)$ , which holds for all  $n/m$  smaller than  $\lambda$ , and so  $\psi(z)^\lambda \leq \psi(a)$ . Similarly taking  $n/m > \lambda$ , we can show that  $\psi(z)^\lambda \geq \psi(a)$ , and so  $\psi(z)^\lambda = \psi(a)$ . Take  $\alpha \in \mathbf{R}$ ,  $\alpha > 0$ , so that  $\psi(z) = \varphi(z)^\alpha$ . Then  $\psi(a) = \varphi(z)^{\alpha\lambda} = \varphi(a)^\alpha$ . This completes the proof.

We say that  $\varphi$  and  $\psi$  are **equivalent** if the conditions of the above theorem are satisfied. Clearly the topology of  $F$  depends only on the equivalence

class of valuations. Also, if  $\varphi$  and  $\psi$  correspond to order functions  $\nu$  and  $\mu$  as in §6.2, then  $\varphi$  and  $\psi$  are equivalent if and only if  $\nu = s\mu$  with  $0 < s \in \mathbf{R}$ , which is so if and only if  $\nu$  and  $\mu$  have the same valuation ring and maximal ideal.

**Theorem 6.14.** *For  $x \in \mathbf{Q}$  put  $\varphi_\infty(x) = |x|$  and  $\varphi_p(x) = p^{-\nu_p(x)}$  with a prime number  $p$  as in §6.2. Then every nonarchimedean (resp. archimedean) valuation of  $\mathbf{Q}$  is equivalent to  $\varphi_p$  for some  $p$  (resp.  $\varphi_\infty$ ). Moreover, these valuations are not equivalent to each other.*

PROOF. The last assertion can easily be seen by checking condition (1) of Theorem 6.13. To prove the main part, take a valuation  $\varphi$  of  $\mathbf{Q}$ . Then for  $0 < n \in \mathbf{Z}$  we have  $\varphi(n) \leq n\varphi(1) = n$ . We first assume that there exists a positive integer  $z$  such that  $\varphi(z) > 1$ . We can put  $\varphi(z) = z^\alpha$  with  $0 < \alpha \leq 1$ . Let  $0 < n \in \mathbf{Z}$ . Then we can put  $n = \sum_{i=0}^{k-1} c_i z^i$  with  $0 \leq c_i < z$  and  $1 \leq k \in \mathbf{Z}$ ,  $c_{k-1} \neq 0$ . Then  $z^{k-1} \leq n < z^k$  and

$$\varphi(n) \leq \sum_{i=0}^{k-1} c_i \varphi(z)^i \leq z \sum_{i=0}^{k-1} \varphi(z)^i = \frac{z[\varphi(z)^k - 1]}{\varphi(z) - 1} \leq \frac{z\varphi(z)}{\varphi(z) - 1} \cdot \varphi(z)^{k-1}.$$

Put  $A = z\varphi(z)/[\varphi(z) - 1]$ . Then  $\varphi(n) \leq Az^{\alpha(k-1)} \leq An^\alpha$ . Taking  $n^m$  in place of  $n$ , we obtain  $\varphi(n^m) \leq An^{m\alpha}$ , and so  $\varphi(n) \leq A^{1/m}n^\alpha$ . Making  $m$  tend to  $\infty$ , we obtain  $\varphi(n) \leq n^\alpha$ . Since  $z^{k-1} \leq n < z^k$ , we can put  $n = z^k - w$  with an integer  $w$  such that  $0 < w \leq z^k - z^{k-1}$ . Then  $\varphi(w) \leq w^\alpha \leq (z^k - z^{k-1})^\alpha$ , and so

$$\varphi(n) \geq \varphi(z^k) - \varphi(w) \geq z^{k\alpha} - (z^k - z^{k-1})^\alpha = z^{k\alpha} \{1 - (1 - z^{-1})^\alpha\}.$$

Put  $B = 1 - (1 - z^{-1})^\alpha$ . Then  $\varphi(n) \geq Bz^{k\alpha} > Bn^\alpha$ . Taking  $n^m$  in place of  $n$  and making  $m$  tend to  $\infty$ , we find that  $\varphi(n) \geq n^\alpha$ . Thus we obtain  $\varphi(n) = n^\alpha$ . For  $0 < n' \in \mathbf{Z}$  we have  $\varphi(\pm n'/n) = \varphi(n')/\varphi(n) = (n'/n)^\alpha$ . This means that  $\varphi$  is equivalent to  $\varphi_\infty$ , and proves the case in which  $\varphi(z) > 1$  for some positive integer  $z$ .

Next suppose  $\varphi(z) \leq 1$  for every  $z \in \mathbf{Z}$ . We can find a prime number  $p$  such that  $\varphi(p) < 1$ . (Otherwise, the prime decomposition of a rational number shows that  $\varphi(a) = 1$  for every  $a \in \mathbf{Q}^\times$ .) Suppose there is a prime number  $q \neq p$  such that  $\varphi(q) < 1$ . For every positive integer  $m$ , we can find integers  $r$  and  $s$  such that  $1 = rp^m + sq^m$ . Then  $1 = \varphi(1) \leq \varphi(r)\varphi(p)^m + \varphi(s)\varphi(q)^m \leq \varphi(p)^m + \varphi(q)^m$ , which tends to 0 as  $m \rightarrow \infty$ , a contradiction. Thus there is only one prime number  $p$  such that  $\varphi(p) < 1$ . Put  $\varphi(p) = p^c$  with  $c \in \mathbf{R}$ . Given  $x \in \mathbf{Q}^\times$ , we have  $x = \pm p^{\nu_p(x)} a/b$  with integers  $a$  and  $b$  whose prime decompositions do not involve  $p$ . Then  $\varphi(a) = \varphi(b) = 1$ , and so  $\varphi(x) = \varphi(p)^{\nu_p(x)} = p^{c\nu_p(x)} = \varphi_p(x)^c$ . Thus  $\varphi$  is equivalent to  $\varphi_p$ . This completes the proof.

**Theorem 6.15:** Product formula. For  $\varphi_\infty$  and  $\varphi_p$  as in Theorem 6.14 we have

$$\varphi_\infty(x) \prod_p \varphi_p(x) = 1 \text{ for every } x \in \mathbf{Q}^\times.$$

PROOF. Given  $x \in \mathbf{Q}^\times$ , we can put  $x = \pm \prod_p p^{a_p}$  with  $a_p \in \mathbf{Z}$ , where  $\prod_p$  means the product over all prime numbers  $p$ . Then  $\varphi_p(x) = p^{-a_p}$  and  $\varphi_\infty(x) = |x|$ , and clearly our formula holds.

**Exercises. 1.** Let  $R = \bigcup_{n=0}^\infty p^{-n}\mathbf{Z}$  with a prime number  $p$ . Prove: (i)  $R + \mathbf{Z}_p = \mathbf{Q}_p$  and  $R \cap \mathbf{Z}_p = \mathbf{Z}$ ; (ii)  $R/\mathbf{Z}$  as a module is isomorphic to  $\mathbf{Q}_p/\mathbf{Z}_p$ .

**2.** Let  $p$  be a prime number,  $S_n$  the group of all  $p^n$ -th roots of unity in  $\mathbf{C}$ , and  $S = \bigcup_{n=1}^\infty S_n$ . Using the results of Exercise 1, show that the multiplicative group  $S$  is isomorphic to the additive group  $\mathbf{Q}_p/\mathbf{Z}_p$ .

**3.** Show that  $\mathbf{Q}_p$ , if  $p \neq 2$ , contains no  $p$ -th root of unity other than 1.

**4.** Let  $\nu$  be a normalized discrete order function of a field  $F$ . Suppose that  $F$  is complete and the residue class field is a finite field with  $q$  elements. Let  $c \in F$  with  $\nu(c) = 0$ . Prove that the sequence  $\{c^{q^n}\}_{n=0}^\infty$  converges to an element  $b$  of  $F$  such that  $b^{q-1} = 1$  and  $\nu(b - c) > 0$ .

**5.** With  $F$  and  $\nu$  as in Exercise 4, let  $X$  be the cyclic group generated by a fixed prime element of  $F$ , and  $Y$  the group of all roots of unity  $y$  such that  $y^{q-1} = 1$ ; let  $1 + M = \{x \in F \mid \nu(x - 1) > 0\}$ . Prove that  $F^\times$  is the direct product of  $X$ ,  $Y$ , and  $1 + M$ .

**6.** Compute  $[\mathbf{Q}_p^\times : \mathbf{Q}_p^{\times 3}]$ , where  $\mathbf{Q}_p^{\times 3} = \{x^3 \mid x \in \mathbf{Q}_p^\times\}$ .

**7.** Prove in the following steps that every automorphism  $f$  of the field  $\mathbf{Q}_p$  is the identity map.

(a) Show that  $f$  is the identity map on  $\mathbf{Q}$ .

(b) Let  $x \in \mathbf{Z}_p^\times$ . Write  $f(x) = p^m z$  with  $z \in \mathbf{Z}_p^\times$  and an integer  $m$ . Derive a contradiction if  $m \neq 0$ , by showing that there exists a rational integer  $b$ , prime to  $p$ , such that  $bx = u^n$  with  $u \in \mathbf{Z}_p^\times$  and a positive integer  $n > |m|$ .

(c) Complete the proof by showing the continuity of  $f$ .

## 7. Hensel's lemma and its applications

In this section  $F$  is a field with a discrete order function  $\nu$ ;  $R$  denotes the valuation ring, and  $M$  its maximal ideal.

**Lemma 7.1.** Let  $a, b, c \in k[x]$ , where  $k$  is a field and  $x$  is an indeterminate. If  $a$  and  $b$  are relatively prime and  $b \neq 0$ , then there exist elements  $u, v \in k[x]$  such that  $c = au + bv$  and  $\deg(u) < \deg(b)$ .

PROOF. Take  $u, v$  without the condition  $\deg(u) < \deg(b)$ . We can put  $u = bq + u_1$  with  $q, u_1 \in k[x]$  such that  $\deg(u_1) < \deg(b)$ . Then  $c = au_1 + b(aq + v)$ , and we have only to replace  $(u, v)$  by  $(u_1, aq + v)$ .

**Theorem 7.2** (Hensel's lemma). *Suppose  $F$  is complete; put  $k = R/M$ . For  $a \in R$  (resp.  $a \in R[x]$ ) denote by  $\bar{a}$  the residue class of  $a$  modulo  $M$  (resp.  $M[x]$ ). Given  $f \in R[x]$ ,  $f \notin M[x]$ , suppose that  $\bar{f} = g^*h^*$  with  $g^*, h^* \in k[x]$  such that  $(g^*, h^*) = 1$ . Then there exist elements  $g, h \in R[x]$  such that  $f = gh$ ,  $\bar{g} = g^*$ ,  $\bar{h} = h^*$ , and  $\deg(g) = \deg(g^*)$ .*

PROOF. Let  $r = \deg(g^*)$ ,  $s = \deg(h^*)$ , and  $m = \deg(f)$ . Clearly  $r + s \leq m$ . We construct inductively two sequences  $\{g_i\}_{i=1}^\infty$  and  $\{h_i\}_{i=1}^\infty$  in  $R[x]$  so that

$$\begin{aligned} f &\equiv g_n h_n, & g_{n+1} &\equiv g_n, & h_{n+1} &\equiv h_n \pmod{M^n[x]}, \\ \deg(g_n) &= r, & \deg(h_n) &\leq m - r. \end{aligned}$$

First take  $g_1, h_1$  so that  $\bar{g}_1 = g^*$ ,  $\bar{h}_1 = h^*$ ,  $\deg(g_1) = r$ , and  $\deg(h_1) = s$ . Suppose  $g_n, h_n$  are already defined; take any  $c \in R$  so that  $\nu(c) = n$ . We can then put  $f - g_n h_n = ct$  with  $t \in R[x]$ . Let  $g_{n+1} = g_n + cu$  and  $h_{n+1} = h_n + cv$  with  $u, v \in R[x]$ . Since  $f - g_{n+1} h_{n+1} = c(t - uh_n - vg_n - cuv)$ , we have to take  $u, v$  so that  $\bar{u}h^* + \bar{v}g^* = \bar{t}$ . Since  $(g^*, h^*) = 1$ , we can find such  $u, v$ . By Lemma 7.1 we can take them so that  $\deg(u) = \deg(\bar{u}) < \deg(g^*) = r$  and  $\deg(v) = \deg(\bar{v})$ . Also  $\deg(g_{n+1}) = r$ , and  $\deg(v) + r = \deg(\bar{v}g^*) = \deg(\bar{t} - \bar{u}h^*) \leq m$ . Thus  $\deg(v) \leq m - r$ , and hence  $\deg(h_{n+1}) \leq m - r$ . We can therefore establish the desired sequences. Let  $g = \lim_{n \rightarrow \infty} g_n$  and  $h = \lim_{n \rightarrow \infty} h_n$ . (These are meaningful, since the degrees of  $g_n$  and  $h_n$  are bounded.) Then we obtain the desired conclusion.

**lemma 7.3.** *If  $F$  is complete and  $R/M$  is a finite field with  $q$  elements, then  $R$  has a primitive  $(q-1)$ st root of unity. Moreover, its powers, together with 0, form a complete set of representatives for  $R/M$ .*

PROOF. Apply Hensel's lemma to  $f(x) = x^{q-1} - 1$ .

**Theorem 7.4.** *Suppose  $F$  is complete; let  $g(x) = a_0 + a_1x + \cdots + a_nx^n$  be an irreducible element of  $F[x]$ . Then*

$$\text{Min}\{\nu(a_i) \mid 0 \leq i \leq n\} = \text{Min}\{\nu(a_0), \nu(a_n)\}.$$

PROOF. Assuming  $\text{Min}\{\nu(a_i) \mid 0 \leq i \leq n\} < \text{Min}\{\nu(a_0), \nu(a_n)\}$ , take the smallest  $j$  such that  $\nu(a_j) = \text{Min}\{\nu(a_i) \mid 0 \leq i \leq n\}$ . Then  $0 < j < n$  and  $a_j^{-1}a_k \in M$  for  $k < j$ , and so  $a_j^{-1}g \equiv x^j(1 + \cdots + c_nx^{n-j}) \pmod{M[x]}$  with  $c_n \in R$ . Applying Hensel's lemma to  $a_j^{-1}g$ , we find that  $g$  is reducible, a contradiction.

**Corollary 7.5.** *Let  $g(x) = x^n + b_1x^{n-1} + \cdots + b_n \in F[x]$ ; suppose  $F$  is complete,  $g$  is irreducible, and  $b_n \in R$ . Then  $g \in R[x]$ .*

This is merely a special case of Theorem 7.4.

**7.6.** Before proceeding further, let us recall the notion of the trace and norm maps of a finite algebraic extension  $K$  of a field  $F$ . To simplify our exposition, we consider only the case where  $K$  is separable over  $F$ . Given such a  $K$ , we can find a Galois extension  $M$  of  $F$  containing  $K$ . Put  $G = \text{Gal}(M/F)$  and  $H = \text{Gal}(M/K)$ . For  $\alpha \in M$  and  $\sigma \in G$  we denote by  $\alpha^\sigma$  the image of  $\alpha$  under  $\sigma$ . Thus  $H = \{\sigma \in G \mid \alpha^\sigma = \alpha \text{ for every } \alpha \in K\}$ . Take a subset  $R$  of  $G$  so that  $G = \bigsqcup_{\sigma \in R} H\sigma$ . Then for  $\alpha \in K$  we put

$$(7.1) \quad N_{K/F}(\alpha) = \prod_{\sigma \in R} \alpha^\sigma, \quad \text{Tr}_{K/F}(\alpha) = \sum_{\sigma \in R} \alpha^\sigma.$$

We easily see that these are elements of  $F$  determined independently of the choice of  $M$  and also of  $R$ .

Clearly

$$(7.2) \quad N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta),$$

$$(7.3) \quad \text{Tr}_{K/F}(c\alpha + d\beta) = c\text{Tr}_{K/F}(\alpha) + d\text{Tr}_{K/F}(\beta)$$

for  $\alpha, \beta \in K$  and  $c, d \in F$ .

**7.7.** The notation being as in §7.6, let  $[K : F] = n$  and  $R = \{\sigma_1, \dots, \sigma_n\}$ . Thus  $G = \bigsqcup_{i=1}^n H\sigma_i$ . Given  $n$  elements  $\alpha_1, \dots, \alpha_n$  of  $K$ , we put

$$(7.4) \quad D(\alpha_1, \dots, \alpha_n) = \det [\text{Tr}_{K/F}(\alpha_i \alpha_j)]_{i,j=1}^n,$$

$$(7.5) \quad \Delta(\alpha_1, \dots, \alpha_n) = \det(A), \quad A = \begin{bmatrix} \alpha_1^{\sigma_1} & \alpha_1^{\sigma_2} & \cdots & \alpha_1^{\sigma_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_n^{\sigma_1} & \alpha_n^{\sigma_2} & \cdots & \alpha_n^{\sigma_n} \end{bmatrix}.$$

Then we have

$$(7.6) \quad \Delta(\alpha_1, \dots, \alpha_n)^2 = D(\alpha_1, \dots, \alpha_n),$$

$$(7.7) \quad \Delta(1, \xi, \dots, \xi^{n-1}) = \prod_{i>j} (\xi^{\sigma_i} - \xi^{\sigma_j}) \quad (\xi \in K).$$

The last formula is well known. To prove (7.6), observe that the  $(i, k)$ -entry of  $A \cdot {}^t A$  is  $\sum_{j=1}^n \alpha_i^{\sigma_j} \alpha_k^{\sigma_j} = \text{Tr}_{K/F}(\alpha_i \alpha_k)$ . Therefore  $\det(A \cdot {}^t A) = D(\alpha_1, \dots, \alpha_n)$ , which gives (7.6). Take  $\xi \in K$  such that  $K = F(\xi)$ , and take  $\sigma_1 = 1$ , so that  $\xi^{\sigma_1} = \xi$ . Put  $f(x) = \prod_{i=1}^n (x - \xi^{\sigma_i})$ . Then  $f$  is the minimal polynomial of  $\xi$  over  $F$ , and we easily see the

$$(7.8) \quad \begin{aligned} \Delta(1, \xi, \dots, \xi^{n-1}) &= (-1)^{n(n-1)/2} \prod_{i=1}^n f'(\xi)^{\sigma_i} \\ &= (-1)^{n(n-1)/2} N_{K/F}[f'(\xi)]. \end{aligned}$$

**Theorem 7.8.** *For a finite separable extension  $K$  of  $F$ , the following assertions hold:*

(i) We have  $D(\alpha_1, \dots, \alpha_n) \neq 0$  if  $\{\alpha_i\}_{i=1}^n$  is an  $F$ -basis of  $K$ , and consequently the  $F$ -bilinear map  $(\alpha, \beta) \mapsto \text{Tr}_{K/F}(\alpha\beta)$  of  $K \times K$  into  $F$  is nondegenerate.

(ii) Let  $L$  be a finite algebraic extension of  $K$ . Then, for every  $\alpha \in L$ ,

$$N_{L/F}(\alpha) = N_{K/F}(N_{L/K}(\alpha)) \quad \text{and} \quad \text{Tr}_{L/F}(\alpha) = \text{Tr}_{K/F}(\text{Tr}_{L/K}(\alpha)).$$

(iii) Let the notation be as in (7.1), and for a fixed  $\alpha \in K$  let  $g(x)$  be the minimal polynomial of  $\alpha$  over  $F$ . Then  $\prod_{\sigma \in R}(x - \alpha^\sigma) = g(x)^k$ , where  $k = [K : F(\alpha)]$ .

(iv) For  $\alpha \in K$  let  $\rho(\alpha)$  denote the  $F$ -linear endomorphism  $\xi \mapsto \alpha\xi$  of  $K$  as a vector space over  $F$ . Then  $N_{K/F}(\alpha) = \det[\rho(\alpha)]$  and  $\text{Tr}_{K/F}(\alpha) = \text{tr}[\rho(\alpha)]$ .

PROOF. We prove here only (i), (iii), and (iv), as (ii) is an easy exercise. Our first task is to show that  $\det [\text{Tr}_{K/F}(\alpha_i \alpha_j)]_{i,j=1}^n \neq 0$  for an  $F$ -basis  $\{\alpha_i\}_{i=1}^n$  of  $K$ . Take an element  $\xi$  of  $K$  so that  $K = F(\xi)$ . Then  $\{\xi^\nu\}_{\nu=0}^{n-1}$  is an  $F$ -basis of  $K$ , and the desired fact follows from (7.6) and (7.7). Assertion (i) follows also from a well known fact that any finite number of distinct homomorphisms of a group into  $F^\times$  are linearly independent over  $F$ . To prove (iii), take  $M$  and  $G$  as in §7.6; let  $J = \text{Gal}(M/F(\alpha))$ . If  $\sigma$  runs over  $R$ , then we see that  $\alpha^\sigma$  runs over the conjugates of  $\alpha$  over  $F$  exactly  $[J : H]$  times. Assertion (iii) follows from this fact immediately. The notation being as in (iv), we easily see that  $g(x)$  is the minimal polynomial of  $\rho(\alpha)$ , since  $\alpha \mapsto \rho(\alpha)$  is injective. Let  $f(x)$  be the characteristic polynomial of  $\rho(\alpha)$ . It is well known that  $f$  divides the power of  $g$ . Since  $g$  is irreducible and  $f$  is of degree  $[K : F]$ , we see that  $f = g^k$ . Thus  $f(x) = \prod_{\sigma \in R}(x - \alpha^\sigma)$ , from which we obtain (iv).

## 8. Integral elements in algebraic extensions

In this section  $F$  is the field of quotients of an integral domain  $R$ .

**8.1.** Let  $\alpha$  be an element of an algebraic extension  $L$  of  $F$ . We call  $\alpha$  **integral over  $R$**  if

$$(8.1) \quad \alpha^n + c_1 \alpha^{n-1} + \dots + c_n = 0$$

with  $c_i \in R$  and  $n > 0$ . Let  $\xi \in L$ . Then  $\xi^m + b_1 \xi^{m-1} + \dots + b_m = 0$  with some  $b_i \in F$  and  $m > 0$ . We can find a nonzero element  $a$  of  $R$  such that  $ab_i \in R$  for all  $i$ . Then  $(a\xi)^m + ab_1(a\xi)^{m-1} + \dots + a^m b_m = 0$ , and so  $a\xi$  is integral over  $R$ . Thus any element of  $L$  times a suitable nonzero element of  $R$  is integral over  $R$ . The set of all the elements of  $L$  integral over  $R$  is called **the integral closure of  $R$  in  $L$** . We call  $R$  **integrally closed** if every element of  $F$  integral over  $R$  is contained in  $R$ .

**Lemma 8.2.** *Let  $R$  be a unique factorization domain. Then  $R$  is integrally closed, and more generally the polynomial ring  $R[x_1, \dots, x_n]$  with independent indeterminates  $x_1, \dots, x_n$  is integrally closed. In particular, a principal ideal domain is integrally closed.*

PROOF. Let  $\alpha = a/b$  with relatively prime elements  $a$  and  $b$  of  $R$ ; suppose (8.1) holds with  $c_i \in R$ . Then  $a^n = -b(c_1 a^{n-1} + \dots + c_n b^{n-1})$ . This is a contradiction if  $b \notin R^\times$ , and so  $b \in R^\times$ . Thus  $\alpha \in R$ , which means that  $R$  is integrally closed. By Theorem 1.2, any principal ideal domain and  $R[x_1, \dots, x_n]$  are unique factorization domains. Thus we obtain our lemma.

**Lemma 8.3.** *Let  $\alpha$  be an element of an algebraic extension  $L$  of  $F$ . Then  $\alpha$  is integral over  $R$  if and only if  $\alpha$  is contained in a subring of  $L$  that is a finitely generated  $R$ -module.*

PROOF. If (8.1) is satisfied with  $c_i \in R$ , then  $\alpha^m = -\sum_{i=1}^n c_i \alpha^{m-i}$  for  $m \geq n$ , and so we can show inductively that every power of  $\alpha$  belongs to  $\sum_{i=0}^{n-1} R\alpha^i$ , and so  $R[\alpha] = \sum_{i=0}^{n-1} R\alpha^i$ . Conversely, suppose  $\alpha \in B$  with a subring  $B$  of the form  $B = \sum_{i=1}^k R\beta_i$  of  $L$ . Then  $\alpha\beta_i = \sum_{j=1}^k c_{ij}\beta_j$  with  $c_{ij} \in R$ , and so the matrix  $\alpha 1_k - (c_{ij})$  annihilates the vector  $(\beta_i)$ . If  $\alpha \neq 0$ , then  $(\beta_i) \neq 0$ , so that  $\det[\alpha 1_k - (c_{ij})] = 0$ , which is an equation of the form (8.1), and so  $\alpha$  is integral over  $R$ .

**Lemma 8.4.** *Let  $\alpha, \beta$  be elements of an algebraic extension  $L$  of  $F$ , integral over  $R$ . Then  $\alpha \pm \beta$  and  $\alpha\beta$  are integral over  $R$ . Consequently the integral closure of  $R$  in  $L$  is a subring of  $L$ . Moreover,  $L$  is its field of quotients.*

PROOF. We have  $R[\alpha] = R + R\alpha + \dots + R\alpha^{n-1}$  and  $R[\beta] = R + R\beta + \dots + R\beta^{m-1}$  with some  $n$  and  $m$ . Then  $R[\alpha, \beta] = \sum_{i < n} \sum_{j < m} R\alpha^i \beta^j$ , and this ring contains  $\alpha \pm \beta$  and  $\alpha\beta$ . Therefore by Lemma 8.3, those elements are integral over  $R$ . Also every element of  $L$  times a suitable nonzero element of  $R$  is integral over  $R$ . Thus we obtain our proposition.

**Lemma 8.5.** *Let  $L$  be as above, and  $B$  a subring of  $L$  containing  $R$ ; let  $\alpha \in L$ . If  $\alpha$  is integral over  $B$  and every element of  $B$  is integral over  $R$ , then  $\alpha$  is integral over  $R$ . Consequently the integral closure of  $R$  in  $L$  is integrally closed.*

PROOF. Take (8.1) with  $c_i \in B$ . Since the  $c_i$  are integral over  $R$ , the same technique as in the proof of Lemma 8.4 shows that  $R[c_1, \dots, c_n] = \sum_{j=1}^m R d_j$  with some  $d_j$ . Then  $R[c_1, \dots, c_n, \alpha] = \sum_{k=1}^n \sum_{j=1}^m R \alpha^k d_j$ , and so by Lemma 8.3,  $\alpha$  is integral over  $R$ . Thus we obtain our lemma.

**Theorem 8.6.** *Suppose  $R$  is integrally closed; let  $f(x) \in R[x]$  and  $f = gh$  with monic  $g$  and  $h$  in  $F[x]$ . Then both  $g$  and  $h$  belong to  $R[x]$ .*

PROOF. Let  $g(x) = \prod_i (x - \alpha_i)$  in an extension of  $F$ . Then the  $\alpha_i$  are integral over  $R$  and so the coefficients of  $g$ , being the elementary symmetric functions of the  $\alpha_i$ , are integral over  $R$ . Since they belong to  $F$  and  $R$  is integrally closed, they belong to  $R$ .

As an immediate consequence of this theorem we obtain

**Corollary 8.7.** *Suppose  $R$  is integrally closed; let  $\alpha$  be an element of an extension of  $F$  integral over  $R$ . Then the minimal polynomial of  $\alpha$  over  $F$  has coefficients in  $R$ .*

**Lemma 8.8.** *Suppose  $R$  is integrally closed; let  $K$  be a separable extension of  $F$  of degree  $n$ , and  $B$  the integral closure of  $R$  in  $K$ . Then  $\text{Tr}_{K/F}$  and  $N_{K/F}$  maps  $B$  into  $R$ . Moreover, if  $R$  is a principal ideal domain, then  $B$  is a free  $R$ -module of rank  $n$ .*

PROOF. If  $\alpha \in B$ , then  $\alpha^\sigma$  of (7.1) also belongs to  $B$ , and so  $\text{Tr}_{K/F}(\alpha)$  and  $N_{K/F}(\alpha)$  are integral over  $R$ . This proves the first assertion, since  $R$  is integrally closed. Let  $\{\xi_i\}_{i=1}^n$  be an  $F$ -basis of  $K$ . Changing this for  $\{c\xi_i\}_{i=1}^n$  with a suitable  $c \in R$ , we may assume that  $\xi_i \in B$ . Let  $\alpha \in B$ . Put  $\alpha = \sum_i b_i \xi_i$  with  $b_i \in F$ . Then  $\sum_{i=1}^n b_i \text{Tr}_{K/F}(\xi_i \xi_j) = \text{Tr}_{K/F}(\alpha \xi_j) \in R$  for every  $j$ . Put  $d = \det(\text{Tr}_{K/F}(\xi_i \xi_j))$ . Since  $\text{Tr}_{K/F}(\xi_i \xi_j) \in R$ , we see that  $b_j \in d^{-1}R$ . Therefore  $B \subset d^{-1} \sum_{i=1}^n R \xi_i$ . By Theorem 5.1,  $B$  is a free  $R$ -module of finite rank; the rank must be  $n$ , since  $\xi_i \in B$ .

**8.9.** Let  $\overline{\mathbf{Q}}$  denote the algebraic closure of  $\mathbf{Q}$  in  $\mathbf{C}$ . An element of  $\overline{\mathbf{Q}}$  integral over  $\mathbf{Z}$  is called an **algebraic integer**. A subfield  $K$  of  $\overline{\mathbf{Q}}$  is called an **algebraic number field**. In general  $[K : \mathbf{Q}]$  may be infinite. In this book, however, whenever we speak of an algebraic number field, we always assume that it is of finite degree over  $\mathbf{Q}$ .

If  $K$  is an algebraic number field, the ring of all algebraic integers in  $K$  (that is, the integral closure of  $\mathbf{Z}$  in  $K$ ) is traditionally called **the maximal order of  $K$** . We denote it by  $J_K$ . By Lemma 8.8,  $J_K$  is a free  $\mathbf{Z}$ -module of rank  $[K : \mathbf{Q}]$ . We have

$$(8.2) \quad J_K^\times = \{\alpha \in J_K \mid N_{K/\mathbf{Q}}(\alpha) = \pm 1\}.$$

To prove this, take the Galois closure  $L$  of  $K$  over  $\mathbf{Q}$ . Let  $\alpha \in J_K$ . Then  $\alpha^\sigma \in J_L$  for every  $\sigma \in \text{Gal}(L/\mathbf{Q})$ , and so by (7.1),  $N_{K/\mathbf{Q}}(\alpha) = \alpha\beta$  with  $\beta \in J_L$ . If  $N_{K/\mathbf{Q}}(\alpha) = \pm 1$ , then  $\alpha^{-1} = \pm\beta \in J_L \cap K = J_K$ , and so  $\alpha \in J_K^\times$ . Conversely, if  $\alpha \in J_K^\times$ , then  $\beta \in J_L^\times$ , and so  $N_{K/\mathbf{Q}}(\alpha) \in J_L^\times \cap \mathbf{Q} = J_L^\times \cap \mathbf{Z} = \{\pm 1\}$ . Thus  $N_{K/\mathbf{Q}}(\alpha) = \pm 1$ , and we obtain (8.2).

## 9. Order functions in algebraic extensions

In this section  $F$  is a field with a discrete order function  $\nu$ ;  $R$  denotes the valuation ring, and  $M$  its maximal ideal; we put  $k = R/M$ .



**9.1.** Let  $K$  be a finite algebraic extension of  $F$ , and  $\mu$  an order function of  $K$  that coincides with  $c\nu$  on  $F$  with a positive real constant  $c$ . Let  $R'$  be the valuation ring of  $\mu$  and  $M'$  its maximal ideal. Clearly  $R = R' \cap F$  and  $M = M' \cap F$ . Put  $k' = R'/M'$ . then  $k$  can be viewed as a subfield of  $k'$ . We put

$$f(\mu/\nu) = [k' : k], \quad e(\mu/\nu) = [\mu(K^\times) : c\nu(F^\times)].$$

These are called **the residue class degree of  $\mu$  over  $\nu$**  and **the ramification index of  $\mu$  over  $\nu$** . We are going to show that they are finite. The finiteness implies that  $\mu$  is discrete if  $\nu$  is discrete.

We say that  $\nu$  is **ramified** (resp. **unramified**) in  $K$  if  $e(\mu/\nu) > 1$  for some  $\mu$  that extends  $\nu$  to  $K$  (resp. if  $e(\mu/\nu) = 1$  for every  $\mu$  that extends  $\nu$  to  $K$ ).

If  $L$  is a finite algebraic extension of  $K$  and  $\lambda$  is an order function of  $L$  that coincides with a constant multiple of  $\mu$  on  $K$ , then clearly

$$e(\lambda/\nu) = e(\lambda/\mu)e(\mu/\nu), \quad f(\lambda/\nu) = f(\lambda/\mu)f(\mu/\nu).$$

**Lemma 9.2.** *For  $\alpha \in R'$  let  $\bar{\alpha}$  denote its residue class modulo  $M'$ . Let  $\alpha_1, \dots, \alpha_m \in R'$ . If  $\bar{\alpha}_1, \dots, \bar{\alpha}_m$  are linearly independent over  $k$ , then  $\alpha_1, \dots, \alpha_m$  are linearly independent over  $F$ , and*

$$(*) \quad \mu(c_1\alpha_1 + \dots + c_m\alpha_m) = \text{Min}(\nu(c_1), \dots, \nu(c_m))$$

for  $c_i \in F$ .

PROOF. Take  $m$  elements  $c_i$  of  $F$ ; suppose at least one of them is nonzero. Let  $\nu(c_j) = \text{Min}(\nu(c_1), \dots, \nu(c_m))$ . Then  $c_j \neq 0$ . Put  $b_i = c_j^{-1}c_i$ . Then  $b_i \in R$  and  $\sum_i \bar{b}_i \bar{\alpha}_i \neq 0$ , since  $b_j = 1$ . Thus  $\mu(\sum_i b_i \alpha_i) = 0$ , and so  $\mu(\sum_i c_i \alpha_i) = \nu(c_j) < \infty$ , which gives (\*). Therefore  $\sum_i c_i \alpha_i \neq 0$ , which proves the linear independence of the  $\alpha_i$ .

**Theorem 9.3.**  $[K : F] \geq e(\mu/\nu)f(\mu/\nu)$ .

PROOF. For simplicity we assume that  $\mu = \nu$  on  $F$ . Take  $\alpha_1, \dots, \alpha_m \in R'$  so that  $\bar{\alpha}_1, \dots, \bar{\alpha}_m$  are linearly independent over  $k$ ; take  $y_1, \dots, y_t \in K^\times$  so that the cosets  $\nu(F^\times) + \mu(y_i)$  for  $1 \leq i \leq t$  form a disjoint union in  $\mu(K^\times)$ . Suppose  $\sum_{i,j} c_{ij} \alpha_i y_j = 0$  with some  $c_{ij} \in F$ . Put  $b_j = \sum_i c_{ij} \alpha_i$ . Then  $\sum_j b_j y_j = 0$ . If  $b_j \neq 0$ , then by Lemma 9.2,  $\mu(b_j) = \text{Min}(\nu(c_{1j}), \dots, \nu(c_{mj})) \in \nu(F^\times)$ , so that  $\mu(b_j y_j) \in \nu(F^\times) + \mu(y_j)$ . Thus the  $\mu(b_j y_j)$  for all  $j$  such that  $b_j \neq 0$  are all different, and so  $\sum_j b_j y_j \neq 0$ , a contradiction. Therefore  $b_j = 0$  for all  $j$ , that is,  $\sum_i c_{ij} \alpha_i = 0$  for all  $j$ . Since the  $\alpha_i$  are linearly independent over  $F$ , we obtain  $c_{ij} = 0$  for all  $i$  and  $j$ , which means that the  $\alpha_i y_j$  are linearly independent over  $F$ , and hence  $mt \leq [K : F]$ .

From this proof we immediately obtain

**Corollary 9.4.** *Suppose  $\mu = \nu$  on  $F$  and  $[K : F] = e(\mu/\nu)f(\mu/\nu)$ ; take  $\alpha_1, \dots, \alpha_f \in R'$  so that  $\overline{\alpha}_1, \dots, \overline{\alpha}_f$  form a  $k$ -basis of  $k'$  and take  $y_1, \dots, y_e \in K^\times$  so that  $\mu(K^\times) = \bigsqcup_{j=1}^e (\nu(F^\times) + \mu(y_j))$ . Then the  $\alpha_i y_j$  for  $1 \leq i \leq f$  and  $1 \leq j \leq e$  form an  $F$ -basis of  $K$ .*

**Theorem 9.5.** *Suppose  $F$  is complete; let  $K$  be a finite (separable or inseparable) algebraic extension of  $F$ . Then*

(1)  $\nu$  can be uniquely extended to an order function  $\mu$  of  $K$ .

(2)  $\mu$  is discrete.

(3)  $K$  is complete with respect to  $\mu$ .

(4)  $[K : F] = e(\mu/\nu)f(\mu/\nu)$ .

(5) Let  $R'$  be the valuation ring of  $\mu$ . Then  $R'$  is the integral closure of  $R$  in  $K$  and  $R'$  is a free  $R$ -module of rank  $[K : F]$ .

(6) Let  $b$  be an element of  $K$  such that  $\mu(b) > 0$  and let  $h_b(x) = x^m + \sum_{i=0}^{m-1} c_i x^i$  be the minimal polynomial for  $b$  over  $F$ . Then  $\nu(c_i) > 0$  for every  $i$ .

PROOF. Put  $n = [K : F]$  and  $\mu(a) = n^{-1}\nu(N_{K/F}(a))$  for every  $a \in K^\times$ ; put  $\mu(0) = \infty$ . Clearly  $\mu = \nu$  on  $F$  and  $\mu(ab) = \mu(a) + \mu(b)$ . For a fixed  $a \in K^\times$  let  $g$  be the minimal polynomial of  $a$  over  $F$ ,  $d = \deg(g)$ , and  $c$  the constant term of  $g$ . Then by Theorem 7.8(iii),  $N_{K/F}(a) = \pm c^{n/d}$ , and so  $\mu(a) = d^{-1}\nu(c)$ . Let us now prove

$$(*) \quad \mu(a) \geq 0 \implies \mu(1+a) \geq 0.$$

If  $\mu(a) \geq 0$ , then  $\nu(c) \geq 0$ , and so  $g \in R[x]$  by Corollary 7.5. Thus  $a$  is integral over  $R$ . In addition,  $1+a$  is a root of the polynomial  $h(x) = g(x-1)$ , whose constant term, say  $c'$ , belongs to  $R$ . Therefore  $\mu(1+a) = d^{-1}\nu(c') \geq 0$ , which proves (\*). If  $x, y \in K$  and  $\mu(x) \geq \mu(y)$ ,  $y \neq 0$ , then  $\mu(x/y) \geq 0$ ; hence  $\mu(x+y) = \mu(y) + \mu(1+(x/y)) \geq \mu(y)$  by (\*). Therefore  $\mu$  is an order function of  $K$ . (It satisfies condition (iv) of §6.1, since  $\mu = \nu$  on  $F$ .) Clearly it is discrete.

To prove the uniqueness of  $\mu$  and (5), let  $\lambda$  be an extension of  $\nu$  to  $K$  and let  $R^*$  be the integral closure of  $R$  in  $K$ ; let  $R'$  resp.  $R''$  be the valuation ring of  $\mu$  resp.  $\lambda$ , and  $M'$  resp.  $M''$  the maximal ideal of  $R'$  resp.  $R''$ . We have seen that  $R' \subset R^*$ . Now, if  $\alpha \in R^*$ , then  $\alpha^m + c_1 \alpha^{m-1} + \dots + c_m = 0$  with some  $c_i \in R$ . If  $\lambda(\alpha) < 0$ , then  $\alpha \neq 0$  and  $1 = -c_1 \alpha^{-1} - \dots - c_m \alpha^{-m}$ , and hence  $\lambda(1) > 0$ , a contradiction. Thus  $\lambda(\alpha) \geq 0$ . This shows that  $R^* \subset R''$ . Taking  $\mu$  as  $\lambda$ , we find that  $R^* = R'$ . Suppose  $R' \neq R''$ ; then  $R''$  has an element  $y$  such that  $\mu(y) < 0$ . We easily see that  $K = \bigcup_{k=0}^{\infty} y^k R' \subset R''$ , which is impossible. Therefore  $R' = R''$ , and  $M' = M''$ , since the valuation ring has a unique maximal ideal. Take  $\pi \in R'$  so that  $M' = \pi R'$ . Clearly  $\lambda(a) = \mu(a) = 0$  if  $a \in (R')^\times$ . If  $a \in \pi^r (R')^\times$  and  $r \neq 0$ , then  $\lambda(a)/\mu(a) =$

$r\lambda(\pi)/[r\mu(\pi)] = \lambda(\pi)/\mu(\pi)$ . Thus  $\lambda/\mu$  is a constant on the set of all such  $a$ 's, which must be 1, since  $\lambda = \mu$  on  $F$ .

Put  $e = e(\mu/\nu)$  and  $f = f(\mu/\nu)$ . Then  $ef \leq n$  by Theorem 9.3. To prove the remaining part of our theorem, we may assume that  $\mu(K^\times) = \mathbf{Z}$ ; then  $\nu(F^\times) = e\mathbf{Z}$ . Take a complete set of representatives  $S$  for  $k = R/M$  including 0; take also  $\alpha_1, \dots, \alpha_f \in R'$  so that  $\bar{\alpha}_1, \dots, \bar{\alpha}_f$  form a  $k$ -basis of  $R'/M'$ . Let  $T$  be the set of all linear combinations  $\sum_{i=1}^f s_i \alpha_i$  with  $s_i \in S$ . We easily see that  $T$  gives a complete set of representatives for  $R'/M'$ . Let  $\pi$  resp.  $\tau$  be a prime element of  $R'$  resp.  $R$ . For  $0 < m \in \mathbf{Z}$  we put  $\pi_m = \pi^i \tau^j$  with nonnegative integers  $i$  and  $j$  such that  $i < e$  and  $m = ej + i$ . Then,  $\mu(\pi_m) = m$ , and given  $a \in R'$ , by the same argument as in the proof of Theorem 6.8(iv), we can find  $\{t_m\}_{m=0}^\infty \subset T$  such that  $a - \sum_{m=0}^N t_m \pi_m \in (M')^{N+1}$  for every  $N \in \mathbf{Z}$ ,  $N > 0$ . This can be written in the form  $a - \sum_{i=0}^{e-1} \sum_{j=0}^{f-1} t_{ij} \pi^i \tau^j \in (M')^{re}$  with  $t_{ij} \in T$  for  $0 < r \in \mathbf{Z}$ . We have  $t_{ij} = \sum_{h=1}^f s_{hij} \alpha_h$  with  $s_{hij} \in S$ . Put  $b_{hi} = \sum_{j=0}^\infty s_{hij} \tau^j$ . This is meaningful as an element of  $F$ , since  $F$  is complete. Then  $a - \sum_{i=0}^{e-1} \sum_{h=1}^f b_{hi} \pi^i \alpha_h \in (M')^{re}$  for every  $r \in \mathbf{Z}$ ,  $r > 0$ , and so  $a = \sum_{i=0}^{e-1} \sum_{h=1}^f b_{hi} \pi^i \alpha_h$ . This shows that  $R' = \sum_{i=0}^{e-1} \sum_{h=1}^f R \pi^i \alpha_h$  and consequently  $K = \sum_{i=0}^{e-1} \sum_{h=1}^f F \pi^i \alpha_h$ . Since  $ef \leq n = [K : F]$ , we see that the elements  $\pi^i \alpha_h$  form an  $F$ -basis of  $K$  and  $ef = n$ ; also  $R'$  is a free  $R$ -module of rank  $n$ .

To prove that  $K$  is complete, we first note that if  $a = \sum_{h,i} b_{hi} \pi^i \alpha_h$  with  $b_{hi} \in F$ , then

$$(**) \quad \mu(a) \geq re \implies \nu(b_{hi}) \geq r.$$

Indeed, if  $\mu(a) \geq re$ , then  $\sum_{h,i} \tau^{-r} b_{hi} \pi^i \alpha_h = \tau^{-r} a \in R'$ , and so  $\tau^{-r} b_{hi} \in R$ , which proves (\*\*). Now let  $\{a_m\}_{m=1}^\infty$  be a Cauchy sequence in  $K$ . Put  $a_m = \sum_{h,i} b_{mhi} \pi^i \alpha_h$  with  $b_{mhi} \in F$ . By (\*\*) we easily see that  $\{b_{mhi}\}_{m=1}^\infty$  is a Cauchy sequence in  $F$  for every  $(h, i)$ , and therefore convergent. Thus we obtain the desired convergence of  $\{a_m\}$ , which proves (3). Let  $b$  and  $h_b$  be as in (6). Take the smallest normal extension  $L$  of  $F$  containing  $K$  and the roots of  $h_b$ . Then  $h_b(x) = \prod_{i=1}^m (x - \beta_i)$  with  $\beta_i \in L$ . For each fixed  $i$  there exists an isomorphism  $\sigma$  of  $F(b)$  onto  $F(\beta_i)$  over  $F$  such that  $b^\sigma = \beta_i$ . This  $\sigma$  can be extended to an automorphism of  $L$  over  $F$ . Applying (1) to  $L$ , we can extend  $\mu$  uniquely to an order function  $\lambda$  of  $L$ . The uniqueness shows that  $\lambda(a^\sigma) = \lambda(a)$  for every  $a \in L$ , and so  $\lambda(\beta_i) = \lambda(b) = \mu(b) > 0$ . This is so for every  $i$ , and the conclusion of (6) follows from this fact. This completes the proof of our theorem.

Since  $\mu$  is unique, we often write  $e(K/F)$  and  $f(K/F)$  for  $e(\mu/\nu)$  and  $f(\mu/\nu)$ . We say that  $K$  is **ramified**, **totally ramified**, or **unramified** over  $F$  according as  $e(K/F) > 1$ ,  $e(K/F) = [K : F]$ , or  $e(K/F) = 1$ .

**Corollary 9.6.** *If  $K$  is a finite algebraic extension of  $F$ , then  $\nu$  can be extended to an order function of  $K$  (even if  $F$  is not complete).*

PROOF. We have  $K = F(\alpha_1, \dots, \alpha_m)$  with some  $\alpha_i$ , and so it is sufficient to prove the case  $K = F(\alpha)$  with a single element  $\alpha$ . Take an irreducible polynomial  $g(x)$  in  $F[x]$  such that  $g(\alpha) = 0$ . Let  $F^*$  be the  $\nu$ -completion of  $F$ . Take an extension  $F^*(\beta)$  with a root of  $g$  considered over  $F^*$ . The above theorem guarantees an extension of  $\nu$  to  $F^*(\beta)$ . Since  $F(\alpha)$  is isomorphic to the subfield  $F(\beta)$  of  $F^*(\beta)$ , we obtain our assertion for such a  $K$ .

**Theorem 9.7.** *Suppose  $F$  is complete and  $k$  is a finite field with  $q$  elements; let  $L$  be a finite algebraic extension of  $F$ , and let  $f = f(L/F)$ . Then the following assertions hold:*

- (i) *There is an extension  $K$  of  $F$  contained in  $L$  such that  $e(K/F) = 1$  and  $[K : F] = f(K/F) = f$ . (Consequently  $f(L/K) = 1$  and  $e(L/K) = e(L/F)$ .)*
- (ii) *Every unramified extension of  $F$  contained in  $L$  is contained in  $K$ . Consequently  $K$  is uniquely determined by property (i).*
- (iii)  *$K = F(\gamma)$  with a root of unity  $\gamma$  of order  $q^f - 1$ , where  $q$  is the number of elements of  $k$ .*

PROOF. We first recall that for every positive integer  $n$ ,  $k$  has a unique extension of degree  $n$ , which is generated by a root of unity of order  $q^n - 1$ ; see §1.9. Now put  $m = q^f - 1$ . By Lemma 7.3,  $L$  contains a root of unity  $\gamma$  of order  $m$ . Let  $K = F(\gamma)$  and let  $k_0$  (resp.  $k_1$ ) be the valuation ring of  $K$  (resp.  $L$ ) modulo its maximal ideal. Since  $\overline{\gamma}$ , the residue class of  $\gamma$ , is contained in  $k_0$ , the last part of Theorem 7.2 shows that  $\overline{\gamma}$  is of order  $m$ , and  $k_0 = k_1$ . This shows that  $f(K/F) = f$ . Let  $g(x)$  be the minimal polynomial of  $\gamma$  over  $F$ . Then  $\overline{g}$  divides  $x^m - 1$ , and so has no multiple root. Therefore Hensel's lemma shows that  $\overline{g}$  is irreducible over  $k$ . Thus  $[K : F] = \deg(g) = \deg(\overline{g}) = f$ , as  $\overline{\gamma}$  is of order  $m$ . This proves (i). Since  $e(K/F)f(K/F) = [K : F]$ , we obtain  $e(K/F) = 1$ . Notice that  $L = K$  if  $L$  is unramified over  $F$ . Now let  $H$  be an unramified extension of  $F$  contained in  $L$ ; let  $h = f(H/F)$ . Take  $H$  in place of  $L$ . Then  $H$  is generated over  $F$  by a root of unity of order  $q^h - 1$ . Since  $h|f$ , that root of unity is a power of  $\gamma$ , and so  $H \subset K$ . This proves (ii). Once we know the uniqueness of  $K$ , then (iii) is included in the first part of our proof.

**Theorem 9.8.** *Suppose  $F$  is complete; let  $\tilde{F}$  be an algebraic closure of  $F$ ; let  $q$  be the number of elements in  $k$ . Then the following assertions hold:*

- (i) *For every positive integer  $n$ ,  $\tilde{F}$  contains a unique unramified extension of  $F$  of degree  $n$ .*
- (ii) *Such an extension is cyclic over  $F$  and generated by a primitive  $m$ -th root of unity, where  $m = q^n - 1$ .*

PROOF. Let  $K$  be the splitting field of  $x^m - 1$  over  $F$  contained in  $\tilde{F}$  with  $m$  as above. Observe that the characteristic of  $F$  is either 0 or the prime number that divides  $q$ . Since  $x^m - 1$  has no multiple root, we have  $K = F(\alpha)$  with a primitive  $m$ -th root of unity  $\alpha$ . Then  $x^m - 1 = \prod_{i=0}^{m-1} (x - \alpha^i)$ . Let  $g$  be the minimal polynomial of  $\alpha$  over  $F$ . Repeating the last part of the proof of Theorem 9.7, we see that  $\bar{g}$  is irreducible. Now  $x^m - 1 = \prod_{i=0}^{m-1} (x - \bar{\alpha}^i)$  in the residue field, and since  $x^m - 1$  is a separable polynomial over  $k$ , we see that  $\bar{\alpha}$  is of order  $m$ . Therefore the first statement of the proof of Theorem 9.7 shows that  $n = \deg(\bar{g}) = \deg(g) = [K : F]$ . Then clearly  $n = f(K/F)$ , and so  $e(K/F) = 1$ . To prove the uniqueness, take an unramified extension  $L$  of  $F$  of degree  $n$ . By Theorem 9.7(i, iii),  $L$  is generated by a root of unity of order  $m$ , and so must coincide with the above  $K$ .

In the setting of the above proof let  $G = \text{Gal}(K/F)$ . Then  $g(x) = \prod_{\sigma \in G} (x - \alpha^\sigma)$ . Since the extension of the order function of  $F$  to  $K$  is unique by Theorem 9.5, we see that every  $\sigma \in G$  sends  $R_K$  and  $M_K$  onto themselves, and so  $\sigma$  induces an automorphism of  $R_K/M_K$ , which we denote by  $\bar{\sigma}$ . We have then  $\bar{g}(x) = \prod_{\sigma \in G} (x - (\bar{\alpha})^{\bar{\sigma}})$ . Since  $\bar{g}$  is irreducible, this means that  $\text{Gal}(\kappa/\varphi) = \{\bar{\sigma} \mid \sigma \in G\}$ , where  $\kappa = R_K/M_K$  and  $\varphi = R_F/M_F$ . Therefore  $\sigma \mapsto \bar{\sigma}$  gives an isomorphism of  $\text{Gal}(K/F)$  onto  $\text{Gal}(\kappa/\varphi)$ , and we easily see that

$$(9.1) \quad N_{\kappa/\varphi}(\bar{a}) = \overline{N_{K/F}(a)} \quad \text{and} \quad \text{Tr}_{\kappa/\varphi}(\bar{a}) = \overline{\text{Tr}_{K/F}(a)} \quad (a \in R_K).$$

**Theorem 9.9.** *Suppose  $F$  is complete; let  $K$  be a finite algebraic extension of  $F$ .*

- (i) *If  $K$  is unramified over  $F$ , then  $R_K = R_F[\gamma]$  with a root of unity  $\gamma$  as in Theorem 9.7(iii).*
- (ii) *If  $K$  is totally ramified over  $F$ , then  $R_K = R_F[\pi]$  with any prime element  $\pi$  of  $K$ .*

PROOF. Our assertions are special cases of the formula  $R_K = \sum_{i,j} R_F \alpha_i \pi^j$  shown in the proof of Theorem 9.5.

**Theorem 9.10.** *Let  $F$  be a finite algebraic extension of  $\mathbf{Q}_p$ . Then the following assertions hold:*

- (i) *If  $K$  is an abelian extension of  $F$  of degree  $n$ , then  $[F^\times : N_{K/F}(K^\times)] = n$ .*
- (ii) *In particular, if  $K$  is unramified over  $F$ , then  $N_{K/F}(R_K^\times) = R_F^\times$ , and  $F^\times/N_{K/F}(K^\times)$  is generated by the coset represented by a prime element of  $F$ .*
- (iii) *Let  $\tilde{F}$  be an algebraic closure of  $F$ . Then, assigning  $N_{K/F}(K^\times)$  to every finite abelian extension  $K$  of  $F$  contained in  $\tilde{F}$ , we obtain a bijection of the set of such  $K$  onto the set of all subgroups of  $F^\times$  of finite index.*

PROOF. These are basic facts in local class field theory, which was first presented by Chevalley in [C]. Here we prove (ii) as stated; we prove (i) only in the following two cases: (a)  $K$  is unramified over  $F$ ; (b)  $[K : F] = 2$ . The latter case will be proven in Theorem 21.15. As for (iii), we will prove it only when  $F = \mathbf{Q}_p$  and  $n = 2$ . We first discuss (ii) by considering an unramified extension  $K$  of  $F$ . Take any prime element  $\pi$  of  $F$  and let  $G = \text{Gal}(K/F)$ . Then for every  $b \in R_K$  and  $0 < a \in \mathbf{Z}$  we have  $N_{K/F}(1 + \pi^a b) = 1 + \pi^a \text{Tr}_{K/F}(b) + \pi^{a+1} c$  with  $c \in R_K$ . Clearly  $c \in R_F$ , and so  $N_{K/F}(1 + \pi^a b) \equiv 1 + \pi^a \text{Tr}_{K/F}(b) \pmod{M_F^{a+1}}$ . Given  $1 + \pi^a \beta$  with  $\beta \in R_F$ , we can find, in view of (9.1), an element  $b \in R_K$  such that  $\text{Tr}_{K/F}(b) - \beta \in M_F$ , as  $\text{Tr}_{\kappa/\varphi}(\kappa) = \varphi$ , where  $\kappa = R_K/M_K$  and  $\varphi = R_F/M_F$ . Then  $N_{K/F}(1 + \pi^a b) \equiv 1 + \pi^a \beta \pmod{M_F^{a+1}}$ . Applying the same procedure to  $(1 + \pi^a \beta)^{-1} N_{K/F}(1 + \pi^a b)$  with  $a + 1$  in place of  $a$ , we eventually find that  $N_{K/F}(1 + M_K) = 1 + M_F$ . Since  $N_{\kappa/\varphi}(\kappa^\times) = \varphi^\times$ , given  $\gamma \in R_F^\times$ , we can find an element  $\varepsilon \in R_K^\times$  such that  $N_{\kappa/\varphi}(\bar{\varepsilon}) = \bar{\gamma}$ , that is,  $\gamma N_{K/F}(\varepsilon)^{-1} \in 1 + M_F$ . Thus  $\gamma \in (1 + M_F) N_{K/F}(R_K^\times) \subset N_{K/F}(R_K^\times)$ , and so  $R_F^\times = N_{K/F}(R_K^\times)$ . Since  $K^\times = \bigsqcup_{h \in \mathbf{Z}} \pi^h R_K^\times$ , we have  $N_{K/F}(K^\times) = \bigsqcup_{h \in \mathbf{Z}} \pi^{nh} R_F^\times$ , which shows that  $[F^\times : N_{K/F}(K^\times)] = n$ .

Next suppose  $F = \mathbf{Q}_p$  and  $n = 2$ . In Theorem 6.12 we enumerated all quadratic extensions  $K$  of  $F$ . For each  $p$  there exists a unique unramified quadratic extension by Theorem 9.8. We have to consider only the case in which  $K$  is ramified over  $F$ , as the unramified case has been proved in general. We first treat the case  $p \neq 2$ . By Theorem 6.12(i) we see that  $K = \mathbf{Q}_p(\sqrt{p})$  or  $K = \mathbf{Q}_p(\sqrt{pr})$ , where  $r$  is a quadratic nonresidue, and  $R_K = \mathbf{Z}_p[\sqrt{p}]$  or  $R_K = \mathbf{Z}_p[\sqrt{pr}]$  accordingly by Theorem 9.9(ii). For simplicity let us write  $R$  and  $N$  for  $R_K$  and  $N_{K/F}$ . If  $a + b\sqrt{p} \in R^\times$  with  $a, b \in \mathbf{Z}_p$ , then  $a \in \mathbf{Z}_p^\times$ , and  $N(a + b\sqrt{p}) = a^2 - b^2 p \equiv a^2 \pmod{p\mathbf{Z}_p}$ . This combined with Lemma 6.11 (i) shows that  $N(R^\times) = \mathbf{Z}_p^{\times 2}$ . Since  $-p = N(\sqrt{p})$ , we obtain the first of the following two formulas:

$$(9.2) \quad N(K^\times) = \{(-p)^m \mid m \in \mathbf{Z}\} \cdot \mathbf{Z}_p^{\times 2} \quad \text{if } K = \mathbf{Q}_p(\sqrt{p}), p \neq 2,$$

$$(9.3) \quad N(K^\times) = \{(-rp)^m \mid m \in \mathbf{Z}\} \cdot \mathbf{Z}_p^{\times 2} \quad \text{if } K = \mathbf{Q}_p(\sqrt{pr}), p \neq 2.$$

Here  $r$  is a quadratic nonresidue modulo  $p$ . The latter formula can be shown by the same argument. We thus obtain  $[\mathbf{Q}_p^\times : N(K^\times)] = 2$  in both cases. In the unramified case we have  $N(K^\times) = \bigsqcup_{m \in \mathbf{Z}} p^{2m} \mathbf{Z}_p^\times$ . Therefore  $N(K^\times)$  determines  $K$  when  $p \neq 2$ .

Next suppose  $p = 2$ . There are seven quadratic extensions of  $\mathbf{Q}_2$  as listed in Theorem 6.12 (ii). Let  $\zeta = (-1 + \sqrt{-3})/2$ . Then  $\mathbf{Q}_2(\zeta) = \mathbf{Q}_2(\sqrt{-3})$ , which is unramified over  $\mathbf{Q}_2$  by Theorem 9.8 (ii). In this case the general results we proved show that  $N(R_K) = \mathbf{Z}_2^\times$  and  $[\mathbf{Q}_2^\times : N(K^\times)] = 2$ . We now present the table of  $N(K^\times)$  for the seven quadratic extensions  $K$  of  $\mathbf{Q}_2$ .

$K$	$N_{K/\mathbf{Q}_2}(K^\times)$
$\mathbf{Q}_2(\sqrt{-3})$	$4^{\mathbf{Z}}\mathbf{Z}_2^\times$
$\mathbf{Q}_2(\sqrt{-1})$	$2^{\mathbf{Z}} \cdot \{x \in \mathbf{Z}_2 \mid x-1 \in 4\mathbf{Z}_2\}$
$\mathbf{Q}_2(\sqrt{3})$	$(-2)^{\mathbf{Z}} \cdot \{x \in \mathbf{Z}_2 \mid x-1 \in 4\mathbf{Z}_2\}$
$\mathbf{Q}_2(\sqrt{2})$	$2^{\mathbf{Z}} \cdot \{x \in \mathbf{Z}_2 \mid x \pm 1 \in 8\mathbf{Z}_2\}$
$\mathbf{Q}_2(\sqrt{-2})$	$2^{\mathbf{Z}} \cdot \{x \in \mathbf{Z}_2 \mid x-1 \in 8\mathbf{Z}_2 \text{ or } x-3 \in 8\mathbf{Z}_2\}$
$\mathbf{Q}_2(\sqrt{6})$	$(-2)^{\mathbf{Z}} \cdot \{x \in \mathbf{Z}_2 \mid x-1 \in 8\mathbf{Z}_2 \text{ or } x-3 \in 8\mathbf{Z}_2\}$
$\mathbf{Q}_2(\sqrt{-6})$	$6^{\mathbf{Z}} \cdot \{x \in \mathbf{Z}_2 \mid x \pm 1 \in 8\mathbf{Z}_2\}$

Here  $a^{\mathbf{Z}} = \{a^m \mid m \in \mathbf{Z}\}$ . To prove these, we note that

$$\{x \in \mathbf{Z}_2 \mid x-1 \in 8\mathbf{Z}_2\} = \mathbf{Z}_2^{\times 2} \subset N(R^\times).$$

Let  $K = \mathbf{Q}_2(\sqrt{-1})$  and  $\pi = 1 + \sqrt{-1}$ . Then  $N(\pi) = 2$  and  $R = \mathbf{Z}_2[\pi]$ . If  $a+b\pi \in R^\times$  with  $a, b \in \mathbf{Z}_2$ , then  $a \in \mathbf{Z}_2^\times$  and  $N(a+b\pi) = a^2+2b(a+b) \equiv a^2 \equiv 1 \pmod{4\mathbf{Z}_2}$  and  $5 = N(1+2\sqrt{-1})$ . Since  $\{x \in \mathbf{Z}_2 \mid x-1 \in 4\mathbf{Z}_2\}$  is generated by  $\mathbf{Z}_2^{\times 2}$  and 5, we obtain  $N(K^\times)$  for  $K = \mathbf{Q}_2(\sqrt{-1})$ . If  $K = \mathbf{Q}_2(\sqrt{3})$ , we can use the same technique with  $\pi = 1 + \sqrt{3}$ , and observe that  $N(\pi) = -2$  and  $N(3+2\sqrt{3}) = -3$ . In the remaining four cases we have  $R = \mathbf{Z}_2 + \mathbf{Z}_2\sqrt{m}$  with a multiple  $m$  of 2, and for  $a, b \in \mathbf{Z}_2$  we have  $a + b\sqrt{m} \in R^\times$  if and only if  $a \in \mathbf{Z}_2^\times$ . Thus  $N(R^\times) = \mathbf{Z}_2^{\times 2} \cdot N(1 + \mathbf{Z}_2\sqrt{m}) = \mathbf{Z}_2^{\times 2} \cdot \{1 - b^2m \mid b \in \mathbf{Z}_2\}$ . Now  $1 - b^2m \in 1 + 8\mathbf{Z}_2$  if  $b \in 2\mathbf{Z}_2$  and  $1 - b^2m \equiv 1 - m \pmod{8\mathbf{Z}_2}$  if  $b \notin 2\mathbf{Z}_2$ . Also,  $N(2 + \sqrt{2}) = 2$ ,  $N(\sqrt{-2}) = 2$ , and  $N(\sqrt{-6}) = 6$ . Thus we obtain  $N(K^\times)$  as given in the above table. Clearly  $[\mathbf{Q}_2^\times : N(K^\times)] = 2$  in all cases. If  $H$  is a subgroup of  $\mathbf{Q}_2^\times$  of index 2, then  $\mathbf{Q}_2^{\times 2} \subset H$ . Since  $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$  is isomorphic to  $(\mathbf{Z}/2\mathbf{Z})^3$ , we see that there are exactly seven such  $H$ , and clearly the above  $N(K^\times)$  exhaust them.

**Exercises. 1.** Let  $F$  be a field with a normalized discrete order function  $\nu$ , and let  $f(x) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$  with  $c_i \in F$ ; suppose that  $\nu(c_1) > 0, \dots, \nu(c_{n-1}) > 0$ ,  $\nu(c_n) = 1$ . (Such an  $f$  is called an **Eisenstein polynomial**,  $f = 0$  an **Eisenstein equation**.)

(a) Let  $\mu$  be an extension of  $\nu$  to  $F(s)$  with any root  $s$  of  $f$ . Prove that  $\mu(s) = 1/n$ .

(b) Using (a), prove that  $f$  is irreducible over  $F$ .

(c) Prove that every totally ramified extension of  $F$  is generated by such an  $s$ .

**2.** Let  $F$  be a field complete with respect to a discrete order function  $\nu$ , and  $K$  a finite algebraic extension of  $F$  of degree  $n$ . Suppose that  $K$  is totally ramified over  $F$  (that is,  $e(K/F) = n$ ), and the characteristic of the residue class field  $k$  of  $\nu$  does not divide  $n$ . Prove that  $K = F(\alpha)$  with an  $n$ -th root  $\alpha$  of a prime element of  $F$ . (Hint: Take a prime element  $\beta$  of  $K$

and find a prime element  $\gamma$  of  $F$  such that  $\nu(\gamma^{-1}\beta^n - 1) > 0$ . Use Hensel's lemma to find an  $n$ -th root of  $\gamma^{-1}\beta^n$ .)

3. Let  $F$ ,  $k$ , and  $\nu$  be as in Exercise 2; suppose that  $k$  is a finite field with  $q$  elements. Let  $K$  be a finite separable algebraic extension of  $F$ ; let  $R_K$  resp.  $R_F$  denote the valuation ring of  $K$  resp.  $F$ . Prove that  $R_K = R_F[\alpha]$  for some  $\alpha \in J_K$ . (Hint: Let  $M = F(\gamma)$  ( $\gamma^m = 1$ ,  $m = q^f - 1$ ) be the maximal unramified extension of  $F$  contained in  $K$ , and  $\pi$  a prime element of  $K$ . If  $K \neq M$ , put  $\beta = \gamma + \pi$  and show that  $\beta^m - 1$  is a prime element. Recall the formula  $R_K = \sum_{i,j} R_F \alpha_i \pi^j$ .)

4. Let  $F$  be a finite algebraic extension of  $\mathbf{Q}_p$  and  $K$  a finite abelian extension of  $F$ . Employing Theorem 9.10, prove that  $K$  is unramified over  $F$  if every unit of  $F$  is contained in  $N_{K/F}(K^\times)$ . (Hint: Let  $\pi$  be a prime element of  $F$ . Then  $\bigcup_{i \in \mathbf{Z}} R_F^\times \pi^{in} \subset N_{K/F}(K^\times)$ , where  $n = [K : F]$ .)

### 10. Ideal theory in an algebraic number field

In this section  $\overline{\mathbf{Q}}$  denotes the algebraic closure of  $\mathbf{Q}$  in  $\mathbf{C}$ ,  $F$  an algebraic number field of finite degree contained in  $\overline{\mathbf{Q}}$ , and  $J = J_F$  its maximal order.

**10.1.** By a **fractional ideal** in  $F$  we mean a  $J$ -submodule  $X$  of  $F$  such that  $\{0\} \neq \alpha X \subset J$  for some  $\alpha \in F^\times$ . Let  $Y$  be an ideal of  $J$  different from  $\{0\}$ , and let  $c$  be a nonzero element of  $Y$ . Then  $cJ \subset Y \subset J$ . By Lemma 8.8,  $J$  is a free  $\mathbf{Z}$ -module of rank  $n$ , where  $n = [F : \mathbf{Q}]$ , and so  $Y$  is a free  $\mathbf{Z}$ -module of rank  $n$  by Theorem 5.1. Thus, every fractional ideal in  $F$  is a free  $\mathbf{Z}$ -module of rank  $n$ , and consequently contains a  $\mathbf{Q}$ -basis of  $F$ . Thus every fractional ideal is a  $\mathbf{Z}$ -lattice in  $F$ , and every  $\mathbf{Z}$ -lattice in  $F$  that is a  $J$ -submodule is a fractional ideal.

We call a fractional ideal  $Y$  **integral** if  $Y \subset J$ . A fractional ideal that is integral is called an **integral ideal**. An integral ideal is an ideal of  $J$  different from  $\{0\}$ , and vice versa. Thus  $[J : Y]$  is finite if  $Y$  is an integral ideal, in which case we put

$$(10.1) \quad N(Y) = [J : Y],$$

and call  $N(Y)$  the **norm** of  $Y$ . Clearly  $N(Y) < N(X)$  if  $X \subsetneq Y$ . For every  $\alpha \in F^\times$ , the set  $\alpha J$  is a fractional ideal. Such an ideal is called a **principal ideal** (even if it may not be contained in  $J$ ).

**Lemma 10.2.** *Let  $P$  be a prime ideal of  $J$  different from  $\{0\}$ . Then  $P$  is a maximal ideal of  $J$  and  $J/P$  is a finite field.*

PROOF. This is because  $J/P$  is a finite integral domain, and so must be a field.

Let  $p$  be the characteristic of the field  $J/P$ . Then  $N(P) = p^f$  with  $0 < f \in \mathbf{Z}$  and  $p\mathbf{Z} = \mathbf{Z} \cap P = \mathbf{Q} \cap P$ . By a **prime ideal** in  $F$  we always mean  $P$



of this type. (In other words, we exclude the ideal  $\{0\}$ .) Now the basic results of classical ideal theory in an algebraic number field can be stated as follows.

**Theorem 10.3.** (i) *All the fractional ideals of  $F$  form an abelian group with respect to the multiplication law  $(X, Y) \mapsto XY$ , where  $XY$  is the submodule of  $F$  consisting of all the finite sums  $\sum_i x_i y_i$  with  $x_i \in X$  and  $y_i \in Y$ . (This group is called **the ideal group** of  $F$ .)*

(ii)  *$J$  is the identity element of this group, and  $X^{-1} = \{x \in F \mid xX \subset J\}$ .*

(iii) *Every fractional ideal  $X$  different from  $J$  can be uniquely written as a product  $X = P_1^{m_1} \cdots P_r^{m_r}$  with different prime ideals  $P_1, \dots, P_r$  and  $m_i \in \mathbf{Z}, \neq 0$ . This  $X$  is integral if and only if  $m_i > 0$  for every  $i$ .*

That  $XY$  as in (i) is a fractional ideal is clear. It is also easy to see that it defines an associative and commutative law of multiplication. We settle the remaining points after proving several facts (A, B, C, D, E, F) below.

(A) *Let  $P$  be a prime ideal. If  $AB \subset P$  for two integral ideals  $A$  and  $B$ , then  $A \subset P$  or  $B \subset P$ .*

PROOF. Suppose  $A \not\subset P$  and  $B \not\subset P$ ; then  $A$  has an element  $a$  not contained in  $P$ , and  $B$  has an element  $b$  not contained in  $P$ . Since  $P$  is a prime ideal,  $ab \notin P$ , which contradicts the assumption  $AB \subset P$ .

(B) *Every integral ideal  $M$  other than  $J$  contains a product of prime ideals.*

PROOF. We prove this by induction on  $N(M)$ . There is no problem if  $M$  is a prime ideal, and so we assume that  $M$  is not a prime ideal. Then  $J$  has elements  $a$  and  $b$  not contained in  $M$  such that  $ab \in M$ . Put  $A = M + Ja$  and  $B = M + Jb$ . Then  $AB \subset M$  and  $N(A) < N(M)$ , since  $M \subsetneq A$ . Similarly  $N(B) < N(M)$ . Applying our induction to  $A$  and  $B$ , we obtain our assertion.

(C) *For a fractional ideal  $M$  put  $M^{-1} = \{x \in F \mid xM \subset J\}$ . If  $M \subsetneq J$ , then  $J \subsetneq M^{-1}$ .*

PROOF. Suppose  $M \subsetneq J$ ; then clearly  $J \subset M^{-1}$ . Take a maximal ideal  $P$  containing  $M$ . Then  $P$  is a prime ideal and  $J \subset P^{-1} \subset M^{-1}$ . Suppose  $J = M^{-1}$ . Then  $P^{-1} = J$ . Take any nonzero element  $a \in P$ . By (B) we can find prime ideals  $\{P_i\}_{i=1}^r$  such that  $P_1 \cdots P_r \subset aJ$ . For a fixed  $a$  take such a set  $\{P_i\}_{i=1}^r$  with the smallest  $r$ . By (A),  $P_i \subset P$  for some  $i$ . We may assume that  $i = 1$ . Since  $P_1$  is maximal, we have  $P = P_1$ . Put  $X = P_2 \cdots P_r$ . Then  $PX \subset aJ$ , and so  $a^{-1}PX \subset J$ . Thus  $a^{-1}X \subset P^{-1}$ , and so  $X \subset aP^{-1} \subset aJ$ , which is a contradiction, since  $X$  is the product of  $r - 1$  prime ideals. This proves (C).

(D) *If  $\alpha \in F$  and  $\alpha X \subset X$  with a  $\mathbf{Z}$ -lattice  $X$  in  $F$ , then  $\alpha \in J$ .*

PROOF. Take a  $\mathbf{Z}$ -basis  $\{e_i\}_{i=1}^n$  of  $X$ . Then  $\alpha e_i = \sum_{j=1}^n c_{ij} e_j$  with  $c_{ij} \in \mathbf{Z}$ , and so the matrix  $\alpha 1_n - (c_{ij})$  annihilates the nonzero vector  $(e_i)$ , and so  $\det[\alpha 1_n - (c_{ij})] = 0$ , which is an equation of type (8.1). Thus  $\alpha$  is integral over  $\mathbf{Z}$ , and so  $\alpha \in J$ .

(E)  $MM^{-1} = J$  for every fractional ideal  $M$ .

PROOF. Clearly  $MM^{-1} \subset J$ . Suppose  $MM^{-1} \neq J$ . Then  $MM^{-1} \subset P \subset J$  for some maximal ideal  $P$ . Then  $J \subsetneq P^{-1}$  by (C), and  $P^{-1} \subset (MM^{-1})^{-1}$ . Clearly  $(MM^{-1})^{-1}MM^{-1} \subset J$ , and so  $(MM^{-1})^{-1}M^{-1} \subset M^{-1}$ . Taking  $M^{-1}$  as  $X$  in (D), we obtain  $(MM^{-1})^{-1} \subset J$ , a contradiction. Thus  $MM^{-1} = J$ .

(F) Let  $X$  and  $Y$  be fractional ideals of  $F$ . Then  $X \subset Y \iff XY^{-1} \subset J \iff X = YA$  with an integral ideal  $A$ .

The proof may be left to the reader, as it is straightforward. If  $X$  and  $Y$  as in (F) we say that  $Y$  **divides**  $X$ .

Once (E) is established it is easy to see that (i) and (ii) of Theorem 10.3 hold. We prove that every integral  $M$  is a product of prime ideals by induction on  $N(M)$ . We may assume that  $M \neq J$  and  $M$  is not a prime ideal. Given such an  $M$ , define  $A$  and  $B$  as in the proof of (B). We have seen that  $N(B) < N(M)$  and  $AB \subset M \subsetneq A$ , and so  $B \neq J$ . Put  $C = B^{-1}M$ . Then  $M = BC \subset C$  and  $M \neq C$ , since  $B \neq J$ . Thus  $N(C) < N(M)$ . By induction,  $B$  and  $C$  are products of prime ideals, and so  $M$  is a product of prime ideals. The uniqueness of such a product expression for  $M$  follows from (A). We have to extend the result from integral ideals to fractional ideals, which is easy, and so may be left to the reader.

**Lemma 10.4.** Let  $A$ ,  $B$ , and  $C$  be integral ideals of  $F$ . Then  $A + B = J$  if and only if there is no prime ideal that divides both  $A$  and  $B$ . For such  $A$  and  $B$  we have  $AB = A \cap B$  and  $J/AB$  is ring-isomorphic to  $(J/A) \oplus (J/B)$ ; moreover, if  $A$  divides  $BC$ , then  $A$  divides  $C$ .

PROOF. Suppose  $A + B = J$ . If an integral ideal  $D$  divides both  $A$  and  $B$ , then  $J = A + B \subset D$ , and so  $D = J$ . If  $A + B \neq J$ , then taking a maximal ideal containing  $A + B$ , we find a prime ideal  $P$  that divides both  $A$  and  $B$ . This proves the first assertion. If  $A + B = J$ , then  $A \cap B = (A \cap B)J = (A \cap B)A + (A \cap B)B \subset BA + AB = AB$ . Clearly  $AB \subset A \cap B$ , and so  $AB = A \cap B$ . By Theorem 1.3,  $J/AB \cong (J/A) \oplus (J/B)$ . Finally suppose  $BC \subset A$ . Since  $AC \subset A$ , we have  $C = JC = AC + BC \subset A$ , which proves the last assertion.

For integral ideals  $A$  and  $B$  we say that  $A$  is **prime to**  $B$  if  $A + B = J$ .

**Lemma 10.5.** *Let  $X$  be a fractional ideal and  $C$  an integral ideal. Then the following assertions hold:*

- (i) *There exist an integral ideal  $B$  and an element  $\alpha$  of  $F$  such that  $B+C = J$  and  $B = \alpha X$ .*
- (ii)  *$X/CX$  and  $J/C$  are isomorphic as  $J$ -modules.*
- (iii) *Suppose  $C$  is prime to  $mJ$  with  $0 \neq m \in \mathbf{Z}$ ; then  $N(C)$  is prime to  $m$ .*

PROOF. Assuming that  $C \neq J$ , let  $P_1, \dots, P_r$  be the prime ideals dividing  $C$ ; put  $Y = X^{-1}P_1 \cdots P_r$ . Then  $Y \subsetneq YP_i^{-1} \subset X^{-1}$ . Take  $\alpha_i \in YP_i^{-1}$ ,  $\alpha_i \notin Y$ , and put  $\alpha = \alpha_1 + \cdots + \alpha_r$ . Then  $\alpha_i \in X^{-1}P_j$  if  $i \neq j$ . Suppose  $\alpha_1 \in X^{-1}P_1$ . Then  $\alpha_1 X \subset P_1 \cap P_2 \cap \cdots \cap P_r = P_1 \cdots P_r$ , so that  $\alpha_1 \in Y$ , a contradiction. Thus  $\alpha_1 \notin X^{-1}P_1$ . Since  $\alpha_i \in X^{-1}P_1$  for  $i \neq 1$ , we see that  $\alpha \notin X^{-1}P_1$ . Similarly  $\alpha \notin X^{-1}P_i$  for every  $i$ . Thus  $\alpha X \not\subset P_i$  for every  $i$ . Put  $B = \alpha X$ . Then  $B$  is integral and prime to every  $P_i$ , so that  $B$  is prime to  $C$ , which proves (i). To prove (ii), Take  $\alpha$  and  $B$  as in (i). By Lemma 10.4,  $BC = B \cap C$ , and the map  $x \mapsto \alpha x$  sends  $X/XC$  onto  $B/BC$  which is isomorphic to  $J/C$  as expected. To prove (iii), take a prime ideal  $P$  dividing  $C$ . Then  $P + mJ = J$ , and so  $m$  is invertible in  $J/P$ . Thus  $m$  is prime to  $N(P)$ . Since  $N(C)$  is the product of powers of  $N(P)$  for all prime factors  $P$  of  $C$ , we obtain (iii).

**Lemma 10.6.** *Every fractional ideal is generated over  $J$  by two elements.*

PROOF. Given a fractional ideal  $Y$ , take a nonzero element  $\beta \in Y$  and put  $X = Y^{-1}$  and  $C = \beta X$ . Then  $C$  is an integral ideal. Applying Lemma 10.5(i) to this  $X$  and  $C$ , we obtain an element  $\alpha$  such that  $\alpha X + C = J$ . Multiplying by  $Y$ , we obtain  $\alpha J + \beta J = Y$ , which proves our lemma.

**Lemma 10.7.**  *$N(XY) = N(X)N(Y)$  if  $X$  and  $Y$  are integral ideals.*

PROOF. By Lemma 10.5(ii) we have  $X/YX \cong J/Y$ , and so  $[X : YX] = [J : Y]$ . Thus  $N(XY) = [J : YX] = [J : X][X : YX] = [J : X][J : Y] = N(X)N(Y)$ .

**10.8.** Given a fractional ideal  $X$ , take integral ideals  $S$  and  $T$  so that  $X = S^{-1}T$ , and put  $N(X) = N(S)^{-1}N(T)$ . From Lemma 10.7 we easily see that this is well defined, and  $X \mapsto N(X)$  is a homomorphism of the ideal group of  $F$  into  $\mathbf{Q}^\times$ ;  $N(X)$  is called **the norm of  $X$** . In particular,

$$(10.2) \quad N(\alpha J) = |N_{F/\mathbf{Q}}(\alpha)| \quad \text{for every } \alpha \in F^\times.$$

It is sufficient to prove this when  $\alpha \in J$ . For  $0 \neq \alpha \in J$  let  $\rho(\alpha)$  denote the matrix representing the  $\mathbf{Q}$ -linear automorphism  $\xi \mapsto \alpha\xi$  of the vector space  $F$  with respect to a  $\mathbf{Z}$ -basis of  $J$ . By Theorem 7.8(iv) we have  $N_{F/\mathbf{Q}}(\alpha) = \det[\rho(\alpha)]$ . By Lemma 5.8,  $[J : \alpha J] = |\det[\rho(\alpha)]|$ , which gives (10.2).

**10.9.** Hereafter we put  $[F : \mathbf{Q}] = n$ . Let  $X$  be a  $\mathbf{Z}$ -lattice in  $F$  and  $\{\xi_i\}_{i=1}^n$  a  $\mathbf{Z}$ -basis of  $X$ . Then we put

$$(10.3) \quad D(X) = D(\xi_1, \dots, \xi_n) = \det(\mathrm{Tr}_{F/\mathbf{Q}}(\xi_i \xi_j)).$$

This is a special case of (7.4), and is called **the discriminant of  $X$** . In the present situation  $\mathrm{Tr}_{F/\mathbf{Q}}(\xi_i \xi_j) \in \mathbf{Q}$  and  $D(X) \neq 0$  by Theorem 7.8(i), and so  $D(X) \in \mathbf{Q}^\times$ . We easily see that it is determined independently of the choice of  $\{\xi_i\}_{i=1}^n$ . In particular, if  $X = J$ , then  $\mathrm{Tr}_{F/\mathbf{Q}}(\xi_i \xi_j) \in \mathbf{Z}$  by Lemma 8.8. Thus  $D(J)$  is a nonzero positive or negative integer. We put  $D_F = D(J)$  and call  $D_F$  **the discriminant of  $F$** . Let  $\sigma_1, \dots, \sigma_n$  be all the different isomorphic embeddings of  $F$  into  $\overline{\mathbf{Q}}$ . Then by (7.6),

$$(10.4) \quad D(X) = \det(\xi_j^{\sigma_i})^2.$$

**Lemma 10.10.** (i) *If  $X$  and  $Y$  are  $\mathbf{Z}$ -lattices in  $F$  and  $X \subset Y$ , then  $[Y : X]^2 = D(X)/D(Y)$ .*

(ii) *If  $X$  is a fractional ideal of  $F$ , then  $N(X)^2 = D(X)/D_F$ .*

The proof of these statements is left to the reader, as it is an easy exercise.

**10.11.** Let  $p$  be a prime number and let  $P_1, \dots, P_g$  be the prime ideals dividing  $pJ$ . Then  $N(P_i) = p^{f_i}$  and

$$(10.5) \quad pJ = P_1^{e_1} \cdots P_g^{e_g}.$$

with positive integers  $e_i$  and  $f_i$ . Taking the norm of both sides, we obtain  $p^n = N(pJ) = \prod_{i=1}^g p^{e_i f_i}$ , and so

$$(10.6) \quad n = \sum_{i=1}^g e_i f_i.$$

**10.12.** Fix a prime ideal  $P$  of  $F$ . Given  $a \in F$ , put  $aJ = P^m X$  with  $m \in \mathbf{Z}$  and a fractional ideal  $X$  that does not involve  $P$ . Put then  $m = \nu_P(a)$ ; put also  $\nu_P(0) = \infty$ . Then we can easily verify that  $\nu_P$  is a normalized discrete order function. We call the  $\nu_P$ -completion of  $F$  **the  $P$ -completion of  $F$** . Every order function of  $F$  is equivalent to  $\nu_P$  with a unique  $P$ .

Let  $R_P$  be the valuation ring of  $\nu_P$ , and  $M_P$  the maximal ideal of  $R_P$  (see §6.7). Then

$$(10.7) \quad R_P = \{u/v \mid u, v \in J, v \notin P\},$$

$$(10.8) \quad R_P = J + M_P, \quad P = J \cap M_P, \quad R_P/M_P \cong J/P.$$

To prove these, denote by  $R'$  the right-hand side of (10.7). Clearly  $R' \subset R_P$ . To prove the opposite inclusion, let  $a \in R_P$  and  $aJ = P^m X$  as above. Then  $m \geq 0$ . We can put  $X = YZ^{-1}$  with relatively prime integral ideals  $Y$  and  $Z$ . By Lemma 10.5(i) there exist an integral ideal  $B$  and an element  $\gamma$  of  $F$  such that  $B + P = J$  and  $B = \gamma Z^{-1}$ . Then  $\gamma aJ = P^m YB \subset J$ , and so  $\gamma a \in J$ .

Since both  $B$  and  $Z$  are prime to  $P$  and  $\gamma J = BZ$ , we see that  $\gamma \notin P$ . Thus  $a = \gamma a/\gamma \in R'$ , which proves (10.7).

To prove (10.8), let  $u, v \in J$  and  $v \notin P$ . Since  $J/P$  is a field,  $J$  has an element  $w$  such that  $wv - 1 \in P$ . Then  $u/v - wu = u(1 - wv)/v$ , which clearly belongs to  $M_P$ . Thus  $R_P = J + M_P$ . That  $J \cap M_P = P$  is clear from the definition of  $\nu_P$ . Then  $R_P/M_P = (J + M_P)/M_P \cong J/(J \cap M_P) = J/P$ . Thus we obtain (10.8).

For  $p, P_i, e_i$ , and  $f_i$  as in (10.5) and (10.6), put  $\nu_i = e_i^{-1}\nu_{P_i}$ . Then  $\nu_i$  coincides with  $\nu_p$  on  $\mathbf{Q}$ , and

$$(10.9) \quad e_i = e(\nu_i/\nu_p), \quad f_i = f(\nu_i/\nu_p).$$

Indeed, (10.5) shows that  $\nu_i(p) = 1$ , and so  $\nu_i(\mathbf{Q}^\times) = \mathbf{Z}$ , whereas  $\nu_i(F^\times) = e_i^{-1}\mathbf{Z}$ . Thus  $e_i = e(\nu_i/\nu_p)$ . Next,  $\mathbf{Z}/p\mathbf{Z} \cong \mathbf{Z}_p/p\mathbf{Z}_p$ , which is contained in  $R_{P_i}/M_{P_i} \cong J/P_i$ . Since  $[J : P_i] = N(P_i) = p^{f_i}$ , we have  $[J/P_i : \mathbf{Z}/p\mathbf{Z}] = f_i$ , and so  $f_i = f(\nu_i/\nu_p)$ .

We say that  $p$  is **ramified in  $F$**  if  $e_i > 1$  for some  $i$ , and  $p$  is **unramified in  $F$**  if  $e_i = 1$  for every  $i$ .

**Theorem 10.13.** *A prime number  $p$  is ramified in  $F$  if and only if  $p|D_F$ .*

**Theorem 10.14.** *Let  $\theta$  be an element of  $J$  such that  $F = \mathbf{Q}(\theta)$ , and  $h(x)$  the minimal polynomial of  $\theta$  over  $F$ . Let  $p$  be a prime number that does not divide  $[J : \mathbf{Z}[\theta]]$ . Denote by  $\bar{h}$  the class of  $h$  modulo  $p\mathbf{Z}[x]$ . Let  $\bar{h}(x) = \prod_{i=1}^g k_i(x)^{e_i}$  be the decomposition of  $\bar{h}$  in  $(\mathbf{Z}/p\mathbf{Z})[x]$  with different irreducible polynomials  $k_i$ . Then we have  $pJ = P_1^{e_1} \cdots P_g^{e_g}$  with exactly  $g$  different prime ideals  $P_i$  such that  $N(P_i) = p^{f_i}$  with  $f_i = \deg(k_i)$ .*

We do not give the proof of these two theorems here, since we will later prove generalizations of these as Theorems 14.10 and 14.11.

**10.15.** An algebraic extension of  $\mathbf{Q}$  of degree 2 is traditionally called a **quadratic field**. Such a field is given as  $F = \mathbf{Q}(\sqrt{\alpha})$  with an element  $\alpha$  of  $\mathbf{Q}^\times$  that is not a square in  $\mathbf{Q}$ . We call  $F$  a **real** or **imaginary quadratic field** according as  $\alpha > 0$  or  $\alpha < 0$ . Replacing  $\alpha$  by its suitable integer multiple, we may assume that  $F = \mathbf{Q}(\sqrt{m})$  with a square-free positive or negative integer  $m \neq 1$ . Let  $J = J_F$  as before. Then

$$(10.10a) \quad J = \mathbf{Z}[\mu], \quad \mu = (1 + \sqrt{m})/2 \quad \text{if} \quad m - 1 \in 4\mathbf{Z}.$$

$$(10.10b) \quad J = \mathbf{Z}[\sqrt{m}] \quad \text{if} \quad m - 1 \notin 4\mathbf{Z}.$$

To prove these, take  $\xi = \alpha + \beta\sqrt{m} \in J$  with  $\alpha, \beta \in \mathbf{Q}$ . Then  $2\alpha = \text{Tr}_{F/\mathbf{Q}}(\xi) \in \mathbf{Z}$  and  $\alpha^2 - \beta^2 m = N_{F/\mathbf{Q}}(\xi) \in \mathbf{Z}$ . Put  $a = 2\alpha$  and  $b = 2\beta$ . Then  $a \in \mathbf{Z}$  and  $b^2 m \in \mathbf{Z}$ . Since  $m$  is square-free, we easily see that  $b \in \mathbf{Z}$ . Now  $a^2 - b^2 m = 4(\alpha^2 - \beta^2 m) \in 4\mathbf{Z}$ . We easily see that  $a \in 2\mathbf{Z}$  if and only if  $b \in 2\mathbf{Z}$ , in which

case  $\alpha, \beta \in \mathbf{Z}$ , and so  $\xi \in \mathbf{Z} + \mathbf{Z}\sqrt{m} = \mathbf{Z}[\sqrt{m}]$ . Therefore  $a \notin 2\mathbf{Z}$  if and only if  $b \notin 2\mathbf{Z}$ , in which case  $m-1 \in 4\mathbf{Z}$ , since  $a^2 \equiv b^2 \equiv 1 \pmod{4}$ .

Case I:  $m-1 \notin 4\mathbf{Z}$ . In this case we always have  $a, b \in 2\mathbf{Z}$ , and so  $\xi \in \mathbf{Z}[\sqrt{m}]$ . Thus  $J = \mathbf{Z}[\sqrt{m}]$ , which proves (10.10b).

Case II:  $m-1 \in 4\mathbf{Z}$ . Put  $\mu = (1 + \sqrt{m})/2$ . Then  $\mu^2 - \mu = (m-1)/4$ , and so  $\mu$  is integral over  $\mathbf{Z}$ ; thus  $\mu \in J$ ,  $\sqrt{m} = 2\mu - 1 \in \mathbf{Z}[\mu]$ . We have to consider the case in which  $a \notin 2\mathbf{Z}$  and  $b \notin 2\mathbf{Z}$ . Then  $\xi - \mu = (a-1)/2 + \sqrt{m}(b-1)/2 \in \mathbf{Z}[\sqrt{m}] \subset \mathbf{Z}[\mu]$ . Thus  $J = \mathbf{Z}[\mu]$ , which proves (10.10a).

An easy calculation shows that

$$(10.11) \quad D_F = m \quad \text{if } m-1 \in 4\mathbf{Z}, \quad D_F = 4m \quad \text{if } m-1 \notin 4\mathbf{Z}.$$

**10.16.** Still in the setting of §10.15, let us now study the decomposition of a prime number  $p$  in  $F$ . Since  $n = 2$ , (10.5) can take only the following three forms:

$$(10.12a) \quad pJ = P_1P_2, \quad P_1 \neq P_2, \quad N(P_1) = N(P_2) = p,$$

$$(10.12b) \quad pJ = P, \quad N(P) = p^2,$$

$$(10.12c) \quad pJ = P^2, \quad N(P) = p.$$

Here  $P$  and  $P_i$  are prime ideals in  $F$ ;  $p$  is unramified in  $F$  in Cases (10.12a) and (10.12b);  $p$  is ramified in  $F$  in Case (10.12c). By Theorem 10.13,  $p$  is ramified in  $F$  exactly when  $p|m$  or  $p|4m$  according as  $m-1 \in 4\mathbf{Z}$  or  $m-1 \notin 4\mathbf{Z}$ . For instance, take  $m = -1$  and  $F = \mathbf{Q}(\sqrt{-1})$ ; put  $P = (1 + \sqrt{-1})J$ . Then  $P^2 = 2\sqrt{-1}J = 2J$ , which is a special case of (10.12c).

Next, take  $\sqrt{m}$  to be  $\theta$  of Theorem 10.14. Then  $[J : \mathbf{Z}[\sqrt{m}]] = 1$  if  $m-1 \notin 4\mathbf{Z}$  and  $[J : \mathbf{Z}[\sqrt{m}]] = 2$  if  $m-1 \in 4\mathbf{Z}$ , which can be seen from Lemma 10.10(i), for example. Therefore Theorem 10.14 is applicable to every odd prime number  $p$ . We have  $h(x) = x^2 - m$ , and so  $pJ = P_1P_2$  as in (10.12a) if and only if  $x^2 - m$  has two roots in  $\mathbf{Z}/p\mathbf{Z}$ , and  $pJ = P$  as in (10.12b) if and only if  $x^2 - m$  has no root in  $\mathbf{Z}/p\mathbf{Z}$ . Recalling the definition of the quadratic residue symbol in §3.1, we see that for every odd prime number  $p$  that does not divide  $m$ ,

$$(10.13) \quad pJ = P_1P_2 \iff \left(\frac{m}{p}\right) = 1, \quad pJ = P \iff \left(\frac{m}{p}\right) = -1.$$

Now Theorem 3.7 can be reformulated as follows. *To each quadratic field  $F = \mathbf{Q}(\sqrt{m})$  as above we can assign a real primitive character  $\chi$  of conductor  $|D_F|$  such that  $\chi(p) = \left(\frac{m}{p}\right)$  for every odd prime number  $p$  prime to  $m$ , and the correspondence  $F \leftrightarrow \chi$  is one-to-one. Moreover,  $\chi(-1)D_F > 0$ . Here  $D_F$  is determined by (10.11). This combined with (10.13) determines the decomposition of  $pJ$  in  $F$ . For example, the result given in §3.8 determines the prime numbers  $p$  such that  $pJ$  decomposes into the product of two prime ideals in  $\mathbf{Q}(\sqrt{15})$ .*

**10.17.** We cannot say anything about  $2J$  by (10.13). By Theorem 10.13, 2 is ramified in  $F$  if  $D_F$  is even, which is so if and only if  $m - 1 \notin 4\mathbf{Z}$ . Assuming that  $m - 1 \in 4\mathbf{Z}$ , put  $\mu = (1 + \sqrt{m})/2$  as we did in (10.10a). Then the minimal polynomial of  $\mu$  over  $\mathbf{Q}$  is  $x^2 - x - (m - 1)/4$ . By Theorem 10.14,  $2J$  is a prime ideal in  $F$  if and only if this polynomial is irreducible over  $\mathbf{Z}/2\mathbf{Z}$ , which is so if and only if  $m - 5 \in 8\mathbf{Z}$ . Thus

$$(10.14) \quad 2J = P_1 P_2 \iff m - 1 \in 8\mathbf{Z}, \quad 2J = P \iff m - 5 \in 8\mathbf{Z}.$$

Let us now show that if  $\chi$  is the real character of conductor  $|D_F|$  corresponding to  $F$ , then

$$(10.15) \quad 2J = P_1 P_2 \iff \chi(2) = 1, \quad 2J = P \iff \chi(2) = -1.$$

Indeed, as shown in §3.5, we have  $\left(\frac{2}{p}\right) = \chi_1(p)$ , and so by (1') in the proof of Theorem 3.7 we have  $\chi(2) = \chi_1(p_1 \cdots p_r q_1 \cdots q_s) = \chi_1(\varepsilon m) = \chi_1(m)$ . Thus  $\chi(2) = 1$  if  $m - 1 \in 8\mathbf{Z}$  and  $\chi(2) = -1$  if  $m - 5 \in 8\mathbf{Z}$ , and so we obtain (10.15) from (10.14). We will give a conceptual meaning of (10.15) in §17.7.

**10.18.** Let  $\mathcal{I}$  (or  $\mathcal{I}_F$ ) denote the ideal group of  $F$  and  $\mathcal{P}$  the subgroup of  $\mathcal{I}$  consisting of all the principal ideals of  $F$ . Then  $\mathcal{I}/\mathcal{P}$  is called **the ideal class group of  $F$** , which is a finite group as will be shown in Theorem 12.7 below. We call  $[\mathcal{I} : \mathcal{P}]$  **the class number of  $F$** . Each coset of  $\mathcal{I}/\mathcal{P}$  is called an **ideal class of  $F$** ; in particular, the coset  $X\mathcal{P}$  for  $X \in \mathcal{I}$  is called **the ideal class of  $X$** .

**Theorem 10.19.** *Let  $L$  be a  $J$ -lattice in a vector space  $V$  over  $F$  of dimension  $n$ , and  $\{e_i\}_{i=1}^n$  an  $F$ -basis of  $V$ . Then the following assertions hold:*

(i) *There exist an  $F$ -basis  $\{g_i\}_{i=1}^n$  of  $V$  and  $n$  fractional ideals  $A_1, \dots, A_n$  in  $F$  such that  $L = \sum_{i=1}^n A_i g_i$ . Moreover,  $\{g_i\}$  can be chosen so that  $g_i \in \sum_{k=i}^n F e_k$ .*

(ii) *Let  $L = \sum_{i=1}^n A_i g_i$  with an  $F$ -basis  $\{g_i\}_{i=1}^n$  of  $V$  and  $n$  fractional ideals  $A_i$  in  $F$ . Then the isomorphism class of  $L$  as a  $J$ -module is determined by the ideal class of  $A_1 \cdots A_n$ .*

PROOF. Assertion (i) is obvious if  $n = 1$ . Therefore we prove (i) by induction on  $n$ . Given  $L$  and an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $V$  with  $n > 1$ , put  $A = \{a_1 \mid \sum_{i=1}^n a_i e_i \in L\}$ , where  $a_i \in F$ . Clearly  $A$  is a fractional ideal in  $F$ . If  $\sum_{i=1}^n b_i e_i \in A^{-1}L$ , then  $\alpha b_1 \in A$  for every  $\alpha \in A$ , and so  $b_1 \in J$ . Also,  $1 = \sum_{\nu=1}^k \beta_\nu \alpha_\nu$  with  $\beta_\nu \in A^{-1}$  and  $\alpha_\nu \in A$ . We can find elements  $x_\nu = \sum_{i=1}^n \alpha_{\nu i} e_i$  of  $L$  such that  $\alpha_{\nu 1} = \alpha_\nu$ . Put  $g_1 = \sum_{\nu=1}^k \beta_\nu x_\nu$  and  $\gamma_i = \sum_{\nu=1}^k \beta_\nu \alpha_{\nu i}$ . Then  $g_1 \in A^{-1}L$ ,  $g_1 = \sum_{i=1}^n \gamma_i e_i$ , and  $\gamma_1 = 1$ . This proves that  $J = \{b_1 \mid \sum_{i=1}^n b_i e_i \in A^{-1}L\}$ . Let  $x = \sum_{i=1}^n c_i e_i \in A^{-1}L$

and  $M = A^{-1}L \cap (\sum_{i=2}^n Fe_i)$ . Then  $c_1 \in J$  and  $x - c_1g_1 \in M$ , and so  $A^{-1}L = Jg_1 + M$ . Now  $M$  is a  $J$ -lattice in  $\sum_{i=2}^n Fe_i$  by Lemma 4.3(ii). Applying our induction to  $M$  and multiplying by  $A$ , we obtain (i). To prove (ii), we need the following facts:

(10.16) *Two fractional ideals  $X$  and  $Y$  in  $F$  are isomorphic as  $J$ -modules if and only if  $X = \beta Y$  with  $\beta \in F^\times$ .*

(10.17) *For two fractional ideals  $A$  and  $B$  in  $F$ ,  $A \oplus B$  and  $J \oplus AB$  are isomorphic as  $J$ -modules.*

We leave the proof of (10.16) to the reader as an easy exercise. (Hint: Assume  $X \subset J$ ; for  $x, y \in X$  and a  $J$ -isomorphism  $g$  of  $X$  onto  $Y$  we have  $xg(y) = g(xy) = yg(x)$ .) To prove (10.17), we may assume that both  $A$  and  $B$  are integral. Also, by Lemma 10.5(i), replacing  $B$  by  $\gamma B$  with a suitable  $\gamma \in F^\times$ , we may assume that  $A + B = J$ . Then we can find elements  $a \in A$  and  $b \in B$  such that  $a + b = 1$ . We view  $A \oplus B$  as a subset of  $F \oplus F = F_2^1$ , and we let  $GL_2(F)$  act on the right of  $F_2^1$ . Put  $\sigma = \begin{bmatrix} 1 & -b \\ 1 & a \end{bmatrix}$ ; then  $\sigma^{-1} = \begin{bmatrix} a & b \\ -1 & 1 \end{bmatrix}$ . The right action of  $\sigma$  sends  $A \oplus B$  into  $J \oplus AB$ , and that of  $\sigma^{-1}$  sends  $J \oplus AB$  into  $A \oplus B$ . This proves (10.17). To prove (ii), take an  $F$ -basis  $\{x_i\}_{i=1}^n$  of  $V$ . Given a  $J$ -lattice  $L$  in  $V$ , take an  $F$ -basis  $\{y_i\}_{i=1}^n$  contained in  $L$ , put  $y_i = \sum_{j=1}^n c_{ij}x_j$ , and denote by  $\lambda(L)$  the fractional ideal generated by  $\det[(c_{ij})]$  for all possible choices of  $\{y_i\}_{i=1}^n$ . (Alternatively,  $\lambda(L)$  is defined by  $\bigwedge^n L = \lambda(L)x_1 \wedge \cdots \wedge x_n$ .) Clearly the ideal class of  $\lambda(L)$  does not depend on the choice of  $\{x_i\}_{i=1}^n$ . If  $L = \sum_{i=1}^n A_i g_i$  as in (ii), then  $\lambda(L) = \varepsilon A_1 \cdots A_n$  with  $\varepsilon \in F^\times$ . Also, (10.17) shows that  $L \cong J_{n-1}^1 \oplus A_1 \cdots A_n$ . This combined with (10.16) proves (ii).

**Lemma 10.20.** (i) *Given  $a, b, c \in J$ ,  $a \neq 0$ , there exists an element  $k \in J$  such that  $aJ + bJ + cJ = aJ + (b + kc)J$ .*

(ii) *Suppose  $n > 1$  and  $\sum_{i=1}^n a_i J + X = J$  with  $a_i \in J$  and an integral ideal  $X$ . Then there exist  $n$  elements  $b_i \in J$  such that  $\sum_{i=1}^n b_i J = J$  and  $b_i - a_i \in X$  for every  $i$ .*

PROOF. To prove (i), we may assume that  $c \neq 0$ ; replacing  $b$  by a suitable element of  $b + cJ$ , we may also assume that  $b \neq 0$ . Put  $aJ + bJ + cJ = Y$ ,  $aJ = AY$ ,  $bJ = BY$ , and  $cJ = CY$  with ideals  $Y, A, B, C$ . Then  $A + B + C = J$ . If  $A = J$ , then  $Y = aJ$ , and so  $aJ + bJ = Y$ . Thus we may assume that  $A \neq J$ . Let  $S$  be the set of all prime ideals that divide  $A$ . For each  $P \in S$  put  $m_P = 1$  if  $B \subset P$  and  $m_P = 0$  otherwise. We see that  $C \not\subset P$  if  $m_P = 1$ . By Theorem 1.3 we can take  $k \in J$  so that  $k - m_P \in P$  for every  $P \in S$ . Then  $b + kc \notin PY$  for every  $P \in S$ . (Indeed, if  $B \subset P$ , then  $b \in PY$ ,  $kc - c \in cP \subset PY$ , and  $c \notin PY$ , and so  $b + kc \notin PY$ ; if  $B \not\subset P$ , then  $b \notin PY$  and  $kc \in PY$ , and



so  $b + kc \notin PY$ .) Thus we can put  $(b + kc)J = DY$  with an integral ideal  $D$  prime to  $A$ , and consequently  $aJ + (b + kc)J = Y$ , which proves (i).

If the  $a_i$  and  $X$  are given as in (ii), then  $\sum_{i=1}^n a_i g_i + h = 1$  with some  $g_i \in J$  and  $h \in X$ . Then  $\sum_{i=1}^n a_i J + hJ = J$ . There is no problem if  $h = 0$ , and so we assume that  $h \neq 0$ . Replacing  $a_1$  by a suitable element of  $a_1 + hJ$ , we may assume that  $a_1 \neq 0$ . By (i), we have  $a_1 J + a_2 J + hJ = a_1 J + (a_2 + kh)J$  for some  $k \in J$ . Then  $a_1 J + (a_2 + kh)J + \sum_{i=3}^n a_i J = \sum_{i=1}^n a_i J + hJ = J$ , which proves (ii).

**Theorem 10.21.** *Given  $\alpha \in M_n(J)$  such that  $\det(\alpha) - d \in X$  with an integral ideal  $X$  and an element  $d$  of  $J$  prime to  $X$ , there exists an element  $\xi$  of  $M_n(J)$  such that  $\det(\xi) = d$  and  $\xi - \alpha \in X_n^n$ . In particular, the natural map of  $M_n(J)$  onto  $M_n(J/X)$  gives a surjection of  $SL_n(J)$  onto  $SL_n(J/X)$ .*

PROOF. We first prove this for  $d = 1$  by induction on  $n$ . The case  $n = 1$  is obvious and so we assume  $n > 1$ . Let  $\alpha_i$  denote the  $i$ -th row of  $\alpha$  and let  $\alpha_n = [a_1 \ \cdots \ a_n]$  with  $a_i \in J$ . Since  $\det(\alpha) - 1 \in X$ , we see that  $\sum_{i=1}^n a_i c_i - 1 \in X$  with some  $c_i \in J$ , and so  $\sum_{i=1}^n a_i J + X = J$ . By Lemma 10.20(ii) we can find elements  $b_i \in J$  such that  $\sum_{i=1}^n b_i J = J$  and  $b_i - a_i \in X$  for every  $i$ . Replacing  $a_i$  by  $b_i$ , we may assume that  $\sum_{i=1}^n a_i J = J$ . Let  $L = J_n^1$ . Then  $J = \{b \in F \mid b\alpha_n \in L\}$ . By Theorem 10.19(i) we can put  $L = \sum_{i=1}^n A_i \xi_i$  with fractional ideals  $A_i$  and an  $F$ -basis  $\{\xi_i\}_{i=1}^n$  of  $F_n^1$  such that  $\xi_i \in \sum_{k=i}^n F\alpha_k$ . Then  $\xi_n \in F\alpha_n$ . Put  $N = \sum_{i=1}^{n-1} A_i \xi_i$ . Then we easily see that  $A_n \xi_n = J\alpha_n$  and  $L = N \oplus J\alpha_n$ . By Theorem 10.19(ii),  $A_2 \cdots A_n$  is a principal ideal, and so by the same theorem we can put  $N = \sum_{i=1}^{n-1} J\varepsilon_i$  with  $n-1$  elements  $\{\varepsilon_i\}_{i=1}^{n-1}$ , which together with  $\alpha_n$  form a  $J$ -basis of  $L$ . Changing the coordinate system of  $L$  (which means the replacement of  $\alpha$  by  $\sigma\alpha\sigma^{-1}$  with an element  $\sigma$  of  $GL_n(J)$ ), we may assume that  $\{\varepsilon_i\}_{i=1}^n$  is the standard  $J$ -basis of  $L$ , where we put  $\varepsilon_n = \alpha_n$ . For each  $i < n$  we have  $\alpha_i = \beta_i + c_i \varepsilon_n$  with  $\beta_i \in N$  and  $c_i \in J$ . Then

$$\begin{bmatrix} 1 & \cdots & 0 & -c_1 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & -c_{n-1} \\ 0 & \cdots & 0 & 1 \end{bmatrix} \alpha = \begin{bmatrix} \beta & 0 \\ 0 & 1 \end{bmatrix} \quad \text{with} \quad \beta = \begin{bmatrix} \beta_1 \\ \cdots \\ \beta_{n-1} \end{bmatrix}.$$

We see that  $\det(\beta) - 1 \in X$ . Applying our induction to  $\beta$ , we can find  $\gamma \in SL_{n-1}(J)$  such that  $\gamma - \beta \in X_{n-1}^{n-1}$ . Putting

$$\xi = \begin{bmatrix} 1 & \cdots & 0 & c_1 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & c_{n-1} \\ 0 & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} \gamma & 0 \\ 0 & 1 \end{bmatrix},$$

we have  $\det(\xi) = 1$  and  $\xi - \alpha \in X_n^n$ . This proves the case  $d = 1$ . Given  $\alpha$  and  $d$  as in our theorem, take  $e \in J$  so that  $de - 1 \in X$  and put  $\alpha' =$

$\alpha \cdot \text{diag}[1_{n-1}, e]$ . Then  $\det(\alpha') - 1 \in X$  and so we can find  $\xi' \in SL_n(J)$  such that  $\xi' - \alpha' \in X_n^n$ . Put  $\eta = \xi' \cdot \text{diag}[1_{n-1}, d]$ . Then  $\det(\eta) = d$  and  $\eta - \alpha \in X_n^n$ . This completes the proof.

**Exercises. 1.** Let  $A$  be either a principal ideal domain or the maximal order of an algebraic number field. Let  $P$  be a prime ideal of  $A$  and let  $0 < e \in \mathbf{Z}$ . Prove that  $A/P^e$  cannot be decomposed into the direct sum of two nontrivial subrings. (Hint: Every subring (or ideal) of  $A/P^e$  is of the form  $X/P^e$  with some  $X$ .)

**2.** Let  $F$  be an algebraic number field,  $J$  the maximal order of  $F$ ,  $P$  a prime ideal in  $F$ , and  $p$  the rational prime divisible by  $P$ . Under what condition on  $P$  can  $J/P^m$  be isomorphic to  $\mathbf{Z}/p^m\mathbf{Z}$  as a  $\mathbf{Z}$ -module?

**3.** Prove the following classical theorem: *A square-free positive rational integer  $c$  can be written in the form  $c = a^2 + b^2$  with rational integers  $a$  and  $b$  if and only if  $c$  has no prime factor  $p$  of the form  $p \equiv 3 \pmod{4}$ .* (Hint: If  $c$  is divisible by such a  $p$ ,  $a + b\sqrt{-1}$  or  $a - b\sqrt{-1}$  is divisible by  $p$ .)

**4.** Prove that if  $A + B = C$  for fractional ideals  $A$ ,  $B$ , and  $C$  in  $F$ , then  $A^m + B^m = C^m$  for every  $m \in \mathbf{Z}$ ,  $m > 0$ .



## VARIOUS BASIC THEOREMS

### 11. The tensor product of fields

**11.1.** Let  $A$  be a vector space over  $F$  that has a law of multiplication which, together with the existing law of addition, makes  $A$  an associative ring. We call  $A$  an **algebra** over  $F$ , or simply an  **$F$ -algebra**, if  $c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta)$  for every  $c \in F$  and  $\alpha, \beta \in A$ . If  $A$  has an identity element  $1_A$ , then identifying  $c$  with  $c1_A$ , we can view  $F$  as a subfield of  $A$ . Notice that  $c\alpha = (c1_A)\alpha = \alpha(c1_A)$ , and so two laws of multiplication for the elements of  $F$  (one in the vector space and the other in the ring) are the same. Every field extension of  $F$  can naturally be viewed as an  $F$ -algebra.

Let  $A$  be a commutative  $F$ -algebra with identity element. For  $\alpha \in A$  let  $\rho(\alpha)$  denote the  $F$ -linear endomorphism  $\xi \mapsto \alpha\xi$  of  $A$  as a vector space over  $F$ . Then  $\rho$  gives a ring-homomorphism of  $A$  into  $\text{End}_F(A)$ , which we call the **regular representation** of  $A$  over  $F$ . This is injective, because if  $\rho(\alpha) = 0$ , then  $\alpha = \alpha \cdot 1_A = \rho(\alpha)1_A = 0$ .

Let  $K$  be a simple finite algebraic extension of  $F$  of degree  $n$ . Let  $L$  be a finite or an infinite field extension of  $F$ . We now consider  $K \otimes_F L$ , which can be defined as a vector space over  $F$ . We can make this an  $F$ -algebra so that  $(\alpha \otimes \beta)(\alpha' \otimes \beta') = \alpha\alpha' \otimes \beta\beta'$  for  $\alpha, \alpha' \in K$  and  $\beta, \beta' \in L$ . The easiest way to do so is as follows. Take an  $F$ -basis  $\{\varepsilon_i\}_{i=1}^n$  of  $K$ . Then  $K \otimes_F L = \bigoplus_{i=1}^n (\varepsilon_i \otimes L)$ , so that every element of  $K \otimes_F L$  is of the form  $\sum_{i=1}^n (\varepsilon_i \otimes a_i)$  with  $a_i \in L$ . Now  $\varepsilon_i \varepsilon_j = \sum_{k=1}^n c_{ijk} \varepsilon_k$  with  $c_{ijk} \in F$ . We now define  $\sum_{i=1}^n (\varepsilon_i \otimes a_i) \sum_{j=1}^n (\varepsilon_j \otimes b_j) = \sum_{k=1}^n (\varepsilon_k \otimes \sum_{i,j} c_{ijk} a_i b_j)$  for  $a_i, b_j \in F$ . Then  $K \otimes_F L$  becomes an  $F$ -algebra with  $1_K \otimes 1_L$  as its identity element. We can view  $K$  and  $L$  as subrings of  $K \otimes_F L$  with the same identity element, by identifying them with  $K \otimes 1_L$  and  $1_K \otimes L$ .

Suppose  $K$  is given as  $K = F(\xi)$  with an element  $\xi$ . Let  $h(x)$  be the minimal polynomial of  $\xi$  over  $F$ , that is, an irreducible polynomial over  $F$  whose leading coefficient is 1 and such that  $h(\xi) = 0$ . Then  $h$  has degree  $n$  and  $K \cong F[x]/(h)$ , where  $(h)$  denotes the ideal of the polynomial ring  $F[x]$  generated by  $h$ . (It is a standard fact that every finite separable extension  $K$  of  $F$  is such a simple extension.)

We now investigate  $K \otimes_F L$  for a finite or an infinite field extension  $L$  of  $F$ . We have  $K = F \oplus F\xi \oplus \cdots \oplus F\xi^{n-1}$ , and so

$$(11.1) \quad K \otimes_F L = L \oplus L(\xi \otimes 1) \oplus \cdots \oplus L(\xi \otimes 1)^{n-1}.$$

We consider the polynomial ring  $L[x]$ , and to each  $g(x) \in L[x]$  we assign  $g(\xi \otimes 1)$ . Then we obtain an  $L$ -linear homomorphism of  $L[x]$  onto  $K \otimes L$ , and we find that  $L[x]/I \cong K \otimes L$ , where  $I = \{g \in L[x] \mid g(\xi \otimes 1) = 0\}$ . Let  $t(x)$  be a generator of  $I$ . As can be seen from (11.1), the elements  $(\xi \otimes 1)^a$  for  $0 \leq a < n$  are linearly independent over  $L$ , and so  $\deg(t) \geq n$ . Since  $h \in I$  and  $\deg(h) = n$ , we can take  $h$  as  $t$ . Thus  $I = hL[x]$  and  $K \otimes_F L \cong L[x]/hL[x]$ . Put  $h = g_1^{e_1} \cdots g_r^{e_r}$  with  $r$  irreducible polynomials  $g_i$  in  $L[x]$  and  $0 < e_i \in \mathbf{Z}$ . We assume that  $g_i/g_j$  is not a constant if  $i \neq j$ . Then by Theorem 1.3,

$$L[x]/hL[x] \cong L[x]/g_1^{e_1}L[x] \oplus \cdots \oplus L[x]/g_r^{e_r}L[x].$$

**11.2.** Let us now assume that  $K$  is a separable extension of  $F$ . Then  $h$  has no multiple roots, and so  $h = g_1 \cdots g_r$ . Thus

$$(11.2) \quad K \otimes_F L \cong L[x]/(g_1) \oplus \cdots \oplus L[x]/(g_r),$$

where  $(g_i) = g_iL[x]$ , and  $L[x]/(g_i)$  is a separable extension of  $L$ .

To describe  $K \otimes L$  in a different way, let us fix a Galois extension  $\Omega$  of  $L$  containing the roots of  $h$ . (We can take, for example,  $\Omega$  to be the field generated over  $L$  by the roots of  $h$ .) Put  $G = \text{Gal}(\Omega/L)$  and denote by  $\text{Inj}_F(K, \Omega)$  the set of all  $F$ -linear ring-injections of  $K$  into  $\Omega$ . Since  $G$  acts on the right of  $\text{Inj}_F(K, \Omega)$ , we can consider the orbit set  $\text{Inj}_F(K, \Omega)/G$ .

Every element  $\sigma$  of  $\text{Inj}_F(K, \Omega)$  is determined by  $\xi^\sigma$ , and  $g_i(\xi^\sigma) = 0$  for exactly one  $i$ . Take another element  $\tau$  of  $\text{Inj}_F(K, \Omega)$ . If  $g_i(\xi^\tau) = 0$  with the same  $i$ , then there exists an  $L$ -linear isomorphism  $\alpha$  of  $L(\xi^\sigma)$  onto  $L(\xi^\tau)$  such that  $\xi^\tau = \xi^{\sigma\alpha}$ , that is,  $\tau = \sigma\alpha$ . This  $\alpha$  can be extended to an element of  $G$ . Conversely, if  $\tau = \sigma\alpha$  with  $\alpha \in G$ , then  $g_i(\xi^\sigma) = g_i(\xi^\tau) = 0$  for some  $i$ . Thus the direct summands  $L[x]/(g_i)$  of (11.2) correspond bijectively to the set  $\text{Inj}_F(K, \Omega)/G$ .

**Theorem 11.3.** *Let  $S$  be a complete set of representatives for the orbit set  $\text{Inj}_F(K, \Omega)/G$ . For each  $\sigma \in S$  denote by  $U_\sigma$  the composite field of  $K^\sigma$  and  $L$  in  $\Omega$ . Then there exists an isomorphism*

$$(11.3) \quad \psi : K \otimes_F L \rightarrow \bigoplus_{\sigma \in S} U_\sigma$$

such that  $\psi(a \otimes b) = (a^\sigma b)_{\sigma \in S}$  for every  $a \in K$  and  $b \in L$ . Moreover, for every  $a \in K$  we have

$$(11.4) \quad N_{K/F}(a) = \prod_{\sigma \in S} N_{U_\sigma/L}(a^\sigma), \quad \text{Tr}_{K/F}(a) = \sum_{\sigma \in S} \text{Tr}_{U_\sigma/L}(a^\sigma).$$

Notice that we cannot consider the composite field of  $K$  and  $L$ . Once we choose  $\sigma$ , the composite field of  $K^\sigma$  and  $L$  is meaningful.

PROOF. We can rewrite  $h = \prod_{i=1}^r g_i$  as  $h = \prod_{\sigma \in S} g_\sigma$  by putting  $g_i = g_\sigma$  when  $g_i(\xi^\sigma) = 0$ . Then  $L[x]/(g_\sigma) \cong L(\xi^\sigma) = U_\sigma$ . The isomorphism of  $L[x]/(g_\sigma)$  onto  $L(\xi^\sigma)$  maps  $f(x)$  modulo  $(g_\sigma)$  to  $f(\xi^\sigma)$ . Let  $p(x) \in F[x]$  and  $b \in L$ . Then the element  $p(\xi) \otimes b$  of  $K \otimes L$  is represented by  $bp(x)$  of  $L[x]/(h)$ , whose image under the isomorphism of (11.2) is  $(bp(\xi^\sigma))_{\sigma \in S}$ . Putting  $a = p(\xi)$ , we find that  $a \otimes b$  is mapped onto  $(a^\sigma b)_{\sigma \in S}$ . This proves our assertion concerning  $\psi$ . To prove (11.4), we take the regular representation of  $K$  over  $F$ . This can be  $L$ -linearly extended to the regular representation  $\rho$  of  $K \otimes L$  over  $L$ . Let  $\rho_\sigma$  be the regular representation of  $U_\sigma$  over  $L$ . In view of (11.3) we see that  $\rho$  is equivalent to the direct sum of the  $\rho_\sigma$  for all  $\sigma \in S$ . Taking the determinant and trace of this equality with  $b = 1$ , we obtain (11.4) by virtue of Theorem 7.8(iv).

**11.4.** As an easy special case of Theorem 11.3, we consider the case in which  $L = K$  and  $K$  is a separable quadratic extension of  $F$ . Let  $\sigma$  be the nontrivial automorphism of  $K$  over  $F$ . Then we can take  $\{1, \sigma\}$  as  $S$  and  $U_1 = U_\sigma = K$ . Thus the isomorphism  $\psi : K \otimes K \rightarrow K \oplus K$  is given by  $\psi(a \otimes b) = (ab, a^\sigma b)$ . In other words, if we extend  $\sigma$  from  $K \otimes 1$  to  $K \otimes K$  by putting  $(a \otimes b)^\sigma = a^\sigma \otimes b$ , then this automorphism considered on  $K \oplus K$  is given by  $(x, y)^\sigma = (y, x)$ .

**Theorem 11.5.** *Let  $F$  be a field with a discrete order function  $\nu$ , and  $L$  the  $\nu$ -completion of  $F$ ; let  $K$  be a finite separable extension of  $F$ . Take  $\Omega$  as in §11.2 for these  $K$  and  $L$ ; let  $\mu$  be the unique extension of  $\nu$  to  $\Omega$ , as guaranteed by Theorem 9.5.*

(i) *Define  $S$  and  $U_\sigma$  as in Theorem 11.3, and put  $\mu_\sigma(a) = \mu(a^\sigma)$  for  $a \in K$  and  $\sigma \in \text{Inj}_F(K, \Omega)$ . Then the  $\mu_\sigma$  for  $\sigma \in S$  form the set of all extensions of  $\nu$  to  $K$ .*

(ii) *If we identify  $(K, \mu_\sigma)$  with  $(K^\sigma, \mu)$ , then  $U_\sigma$  is the  $\mu_\sigma$ -completion of  $K$ .*

(iii)  $[K : F] = \sum_{\sigma \in S} e(\mu_\sigma/\nu) f(\mu_\sigma/\nu)$ .

PROOF. Since  $\mu$  is unique, we have  $\mu(x^\alpha) = \mu(x)$  for every  $x \in L$  and every  $\alpha \in G$ . Thus  $\mu_{\sigma\alpha} = \mu_\sigma$  for every  $\alpha \in G$ . Now  $U_\sigma = K^\sigma L$ , which is a finite algebraic extension of  $L$ , and so complete with respect to the restriction of  $\mu$  to  $U_\sigma$ . Thus it contains the completion of  $K^\sigma$ , which naturally contains the completion of  $F$ , which is  $L$ . This means that  $U_\sigma$  is the completion of  $K^\sigma$ . This proves (ii). Suppose  $\mu_\sigma = \mu_\tau$  for  $\sigma, \tau \in S$ . Define an isomorphism  $\gamma$  of  $K^\sigma$  onto  $K^\tau$  by  $\gamma = \sigma^{-1}\tau$ . Then for  $a \in K^\sigma$  we have  $\mu(a) = \mu_\sigma(a^{\sigma^{-1}}) = \mu_\tau(a^{\sigma^{-1}}) = \mu(a^\gamma)$ . Thus  $\gamma$  is an isomorphism of the structure  $(K^\sigma, \mu)$  onto

$(K^\tau, \mu)$ , and can be extended to an isomorphism between their completions. Thus  $\gamma$  can be extended to an  $L$ -linear isomorphism of  $U_\sigma$  onto  $U_\tau$ . Such an isomorphism can be extended to an element  $\alpha$  of  $G$ , and so  $\tau = \sigma\alpha$ . Since we took  $\sigma$  and  $\tau$  from  $S$ , we have  $\sigma = \tau$ . Thus the  $\mu_\sigma$  for  $\sigma \in S$  are all different.

To show that the  $\mu_\sigma$  exhaust all extensions of  $\nu$  to  $K$ , take any extension  $\lambda$  of  $\nu$  to  $K$ . Let  $K^*$  be the  $\lambda$ -completion of  $K$  and  $F^*$  the closure of  $F$  in  $K^*$ . Then there is an isomorphism  $\varepsilon$  of  $F^*$  onto  $L$  such that  $\lambda(a) = \mu(a^\varepsilon)$  for every  $a \in F^*$ . Take  $\alpha$  so that  $K = F(\alpha)$ . Then  $K^* = KF^* = F^*(\alpha)$ , and so  $\varepsilon$  can be extended to a ring-injection of  $K^*$  into  $\Omega$ . Thus  $\alpha^\varepsilon = \alpha^\sigma$  for some  $\sigma \in \text{Inj}_F(K, \Omega)$ . Then  $(K^*)^\varepsilon = K^\sigma L = U_\sigma$  and  $\varepsilon$  sends  $\lambda$  to the restriction of  $\mu$  to  $U_\sigma$ , that is,  $\lambda = \mu_\sigma$  on  $K$ , which completes the proof of (i). Finally we have  $[K : F] = [K \otimes L : L] = \sum_{\sigma \in S} [U_\sigma : L]$ . By Theorem 9.5(4),  $[U_\sigma : L] = e(\mu_\sigma/\nu)f(\mu_\sigma/\nu)$ , and so we obtain (iii).

## 12. Units and the class number of a number field

**12.1.** Let  $V$  be a vector space over  $\mathbf{R}$  of dimension  $n$ . We call a  $\mathbf{Z}$ -submodule  $Y$  of  $V$  a **lattice** in  $V$  if  $Y$  is a free  $\mathbf{Z}$ -submodule of rank  $n$  and spans  $V$  over  $\mathbf{R}$ . This is different from what we defined in §4.1, but the distinction will be clear from the context. In particular, if  $V = \mathbf{R}^n$ , then we have the standard measure on  $\mathbf{R}^n$ , and so for a lattice  $Y$  in  $\mathbf{R}^n$ , we can speak of the measure of  $\mathbf{R}^n/Y$ , which we denote by  $\text{vol}(\mathbf{R}^n/Y)$ . For example,  $\text{vol}(\mathbf{R}^n/\mathbf{Z}^n) = 1$ . More generally, if  $X = \sum_{i=1}^n \mathbf{Z}u_i$  with  $n$ -dimensional column vectors  $u_i$ , then  $X$  is a lattice in  $\mathbf{R}^n$  if and only if  $\det[u_1 \cdots u_n] \neq 0$ , in which case  $\text{vol}(\mathbf{R}^n/X) = |\det[u_1 \cdots u_n]|$ . We define the measure on  $\mathbf{C}$  by means of the bijection  $(x, y) \mapsto x + iy \in \mathbf{C}$  of  $\mathbf{R}^2$  onto  $\mathbf{C}$ .

**12.2.** Let  $F$  be an algebraic number field of degree  $n$  over  $\mathbf{Q}$ , and  $J$  the maximal order of  $F$ . Let  $\sigma_i$  for  $1 \leq i \leq n$  be as in §10.9. We rearrange them so that  $\sigma_i$  maps  $F$  into  $\mathbf{R}$  if and only if  $i \leq r$ . (If there is no such  $\sigma_i$ , then  $r=0$ .) Then  $n-r=2s$  with a nonnegative integer  $s$ , and the set of the remaining  $\sigma_i$  consists of  $s$  pairs  $\{\tau_1, \tau'_1, \dots, \tau_s, \tau'_s\}$  such that  $a^{\tau'_i}$  is the complex conjugate of  $a^{\tau_i}$  for every  $a \in F$ . We can define archimedean valuations  $\varphi_1, \dots, \varphi_{r+s}$  of  $F$  by  $\varphi_i(a) = |a^{\sigma_i}|$  for  $1 \leq i \leq r$  and  $\varphi_{r+i}(a) = |a^{\tau_i}|$  for  $1 \leq i \leq s$ , where  $|\cdot|$  is the standard absolute value in  $\mathbf{C}$ .

Now, for each prime ideal  $P$  in  $F$  define  $\nu_P$  as in §10.12 and put  $\varphi_P(x) = N(P)^{-\nu_P(x)}$  for every  $x \in F^\times$ . Then we have **the product formula**

$$(12.1) \quad \prod_{i=1}^r \varphi_i(x) \prod_{j=1}^s \varphi_{r+j}(x)^2 \prod_P \varphi_P(x) = 1$$

for every  $x \in F^\times$ , where  $P$  runs over all the prime ideals in  $F$ . To prove this, we observe that  $\alpha J = \prod_P P^{\nu_P(\alpha)}$ . Combining this with (10.2), we obtain

$\prod_P N(P)^{\nu_P(\alpha)} = |N_{F/\mathbf{Q}}(\alpha)|$ , which equals  $\prod_{i=1}^r |\alpha^{\sigma_i}| \prod_{j=1}^s |\alpha^{\tau_j}|^2$ , and so we obtain (12.1).

**Theorem 12.3.** (i) *Every archimedean valuation of  $F$  is equivalent to exactly one of these  $r + s$  valuations.*

(ii) *There is an  $\mathbf{R}$ -linear isomorphism  $f$  of  $F_{\mathbf{R}} = F \otimes_{\mathbf{Q}} \mathbf{R}$  onto  $\mathbf{R}^r \times \mathbf{C}^s$  such that  $f(a) = (a^{\sigma_1}, \dots, a^{\sigma_r}, a^{\tau_1}, \dots, a^{\tau_s})$  for every  $a \in F$ , where we identify  $F$  with the subset  $F \otimes 1$  of  $F_{\mathbf{R}}$ .*

(iii) *For  $1 \leq i \leq r$  the projection map of  $F_{\mathbf{R}}$  to the factor  $\mathbf{R}$  corresponding to  $\sigma_i$  identifies  $\mathbf{R}$  with the  $\varphi_i$ -completion of  $F$ . Similarly, for  $1 \leq j \leq s$  the projection map of  $F_{\mathbf{R}}$  to the factor  $\mathbf{C}$  corresponding to  $\tau_j$  identifies  $\mathbf{C}$  with the  $\varphi_{r+j}$ -completion of  $F$ .*

(iv) *If  $X$  is a  $\mathbf{Z}$ -lattice in  $F$ , then  $f(X)$  is a lattice in  $\mathbf{R}^r \times \mathbf{C}^s$  and*

$$(12.2) \quad \text{vol}((\mathbf{R}^r \times \mathbf{C}^s)/f(X)) = 2^{-s}|D(X)|^{1/2},$$

*which equals  $2^{-s}|D_F|^{1/2}N(X)$  if  $X$  is a fractional ideal.*

PROOF. Assertion (i) will be proven in §12.4. Assertion (ii) is a special case of Theorem 11.3. Indeed, take  $\{\mathbf{Q}, F, \mathbf{R}, \mathbf{C}\}$  as  $\{F, K, L, \Omega\}$  of §11.2. Let  $G = \text{Gal}(\mathbf{C}/\mathbf{R}) = \{1, \rho\}$ , where  $\rho$  is complex conjugation. Then  $\{\sigma_1, \dots, \sigma_r, \tau_1, \tau'_1, \dots, \tau_s, \tau'_s\} = \text{Inj}_{\mathbf{Q}}(F, \mathbf{C})$  and  $\text{Inj}_{\mathbf{Q}}(F, \mathbf{C})/G$  is represented by  $\{\sigma_1, \dots, \sigma_r, \tau_1, \dots, \tau_s\}$ , which we take to be  $S$  of Theorem 11.3. Define  $U_{\sigma}$  as in that theorem. Then  $U_{\sigma} = \mathbf{R}$  if  $\sigma = \sigma_i$  and  $U_{\sigma} = \mathbf{C}$  if  $\sigma = \tau_j$ . Thus  $\psi$  of (11.3) gives  $f$  of (ii). To prove (iii), we first note that  $\mathbf{Q}^n$  is dense in  $\mathbf{R}^n$ , and so  $F$  is dense in  $F_{\mathbf{R}}$ . Thus  $f(F)$  is dense in  $\mathbf{R}^r \times \mathbf{C}^s$ , and so  $F^{\sigma_i}$  or  $F^{\tau_j}$  is dense in  $\mathbf{R}$  or  $\mathbf{C}$ . Then (iii) is obvious. To prove (iv), let  $X = \sum_{k=1}^n \mathbf{Z}\alpha_k$ . For  $\alpha \in F$  denote by  $\varphi(\alpha)$  and  $\psi(\alpha)$  the column vectors whose components are

$$\begin{aligned} &(\alpha^{\sigma_1}, \dots, \alpha^{\sigma_r}, \text{Re}(\alpha^{\tau_1}), \dots, \text{Re}(\alpha^{\tau_s}), \text{Im}(\alpha^{\tau_1}), \dots, \text{Im}(\alpha^{\tau_s})) \text{ and} \\ &(\alpha^{\sigma_1}, \dots, \alpha^{\sigma_r}, \alpha^{\tau_1}, \dots, \alpha^{\tau_s}, \alpha^{\tau_1\rho}, \dots, \alpha^{\tau_s\rho}), \end{aligned}$$

where  $\tau_k\rho = \tau'_k$ . Define  $(n \times n)$ -matrices  $A$  and  $B$  by

$$A = [\varphi(\alpha_1) \ \cdots \ \varphi(\alpha_n)], \quad B = [\psi(\alpha_1) \ \cdots \ \psi(\alpha_n)].$$

Then by (10.4),  $D(X) = \det(B)^2$ ,  $f(X) = \sum_{i=1}^n \mathbf{Z}\varphi(\alpha_i)$ , and

$$\text{diag} \left[ 1_r, 2^{-1} \begin{bmatrix} 1_s & 1_s \\ -i1_s & i1_s \end{bmatrix} \right] \cdot B = A.$$

Thus  $2^{-s}|D(X)|^{1/2} = |\det(A)| = \text{vol}((\mathbf{R}^r \times \mathbf{C}^s)/f(X))$ , which combined with Lemma 10.10(ii) proves (iv). That  $f(X)$  is a lattice in  $\mathbf{R}^r \times \mathbf{C}^s$  follows from the fact that  $D(X) \neq 0$ .

**12.4.** Let us now prove that every archimedean valuation of  $F$  is equivalent to one of the  $\varphi_i$  ( $1 \leq i \leq r + s$ ) defined in §12.2. We first show that if a



valuation  $\varphi$  of  $\mathbf{C}$  satisfies  $\varphi(x) = |x|$  for every  $x \in \mathbf{R}$ , then  $\varphi(z) = |z|$  for every  $z \in \mathbf{C}$ . For that purpose, first suppose that  $\varphi(w) > \varphi(\overline{w})$  for some  $w \in \mathbf{C}$ . Put  $x = \overline{w}/w$  and  $y_n = (w^n + \overline{w}^n)/(w^{n-1} + \overline{w}^{n-1})$  for  $0 < n \in \mathbf{Z}$ . Then  $y_n \in \mathbf{R}$  and  $y_n = w(1 + x^n)/(1 + x^{n-1})$ , which tends to  $w$  as  $n \rightarrow \infty$  with respect to the  $\varphi$ -topology, that is,  $\lim_{n \rightarrow \infty} \varphi(y_n - w) = 0$ . Since  $y_n \in \mathbf{R}$ , we have  $w \in \mathbf{R}$ , a contradiction. Therefore  $\varphi(z) = \varphi(\overline{z})$  for every  $z \in \mathbf{C}$ , and so  $\varphi(z)^2 = \varphi(z\overline{z}) = \varphi(|z|^2) = |z|^2$ . Thus  $\varphi(z) = |z|$  for every  $z \in \mathbf{C}$  as expected.

Turning to our main question, take  $\{\mathbf{Q}, F, \mathbf{R}, \mathbf{C}\}$  as  $\{F, K, L, \Omega\}$  of §11.2 as we did in the proof of Theorem 12.3. Let  $\varphi$  be an archimedean valuation of  $F$ ,  $F^*$  the  $\varphi$ -completion of  $F$ , and  $\mathbf{Q}^*$  the closure of  $\mathbf{Q}$  in  $F^*$ . By Theorem 6.14 all archimedean valuations of  $\mathbf{Q}$  are equivalent, and so we may assume that  $\varphi(x) = |x|$  for  $x \in \mathbf{Q}$ . Thus there is an isomorphism  $\varepsilon$  of  $\mathbf{Q}^*$  onto  $\mathbf{R}$  such that  $\varphi(x) = |x^\varepsilon|$  for every  $x \in \mathbf{Q}^*$ . Now  $F^*$  is the composite field  $F\mathbf{Q}^*$ , and so there is an element  $\sigma$  of  $\text{Inj}_{\mathbf{Q}}(F^*, \mathbf{C})$  that coincides with  $\varepsilon$  on  $F$ . Since the valuation of  $\mathbf{C}$  that extends the valuation  $|\cdot|$  on  $\mathbf{R}$  is unique as proved above, we have  $\varphi(x) = |x^\sigma|$  for  $x \in F$ . We can take  $\sigma$  from the set  $\{\sigma_i, \tau_j\}$  as in Theorem 12.3(ii), and so we find that  $\varphi$  coincides with one of the  $\varphi_i$  of §12.2. Since  $F$  is dense in  $F_{\mathbf{R}}$ , if  $i \neq j$ , then we can find an element  $\alpha$  of  $F$  such that  $\varphi_i(\alpha) > 1$  and  $\varphi_j(\alpha) < 1$ , and so  $\varphi_i$  is not equivalent to  $\varphi_j$ . Thus we obtain the desired result.

**Theorem 12.5** (Minkowski's lemma). (i) *Let  $L$  be a lattice in  $\mathbf{R}^n$  and let  $\Delta = \text{vol}(\mathbf{R}^n/L)$ ; let  $Y$  be a bounded convex set in  $\mathbf{R}^n$  such that  $-x \in Y$  for every  $x \in Y$ . If  $\text{vol}(Y) > 2^n \Delta$ , then  $Y \cap L$  has a nonzero element. Moreover, if  $Y$  is closed, then the conclusion is valid even when  $\text{vol}(Y) = 2^n \Delta$ .*

(ii) *Let  $f_i(x) = \sum_{j=1}^n a_{ij}x_j$  with  $a_{ij} \in \mathbf{R}$  for  $x \in \mathbf{R}^n$  and  $1 \leq i \leq n$ . If  $0 < |\det(a_{ij})| \leq b_1 \cdots b_n$  with positive numbers  $b_i$ , then there exists  $\xi \in \mathbf{Z}^n$ ,  $\neq 0$ , such that  $|f_i(\xi)| \leq b_i$  for every  $i$ .*

PROOF. We first prove that if  $Z$  is a bounded set in  $\mathbf{R}^n$  and  $Z \cap (Z + \ell) = \emptyset$  for every  $\ell \in L$ ,  $\neq 0$ , then  $\text{vol}(Z) \leq \Delta$ . Take a fundamental domain  $T$  for  $\mathbf{R}^n/L$ . Then  $\text{vol}((Z + \ell) \cap T) = \text{vol}(Z \cap (T - \ell))$  and  $Z = \bigsqcup_{\ell \in L} [Z \cap (T - \ell)]$ , so that  $\text{vol}(Z) = \sum_{\ell \in L} \text{vol}((Z + \ell) \cap T) \leq \text{vol}(T) = \Delta$  as desired. Now given  $Y$  as above, take  $Z = (1/2)Y$ . If  $\text{vol}(Z) > \Delta$ , then there exists  $\ell \in L$ ,  $\neq 0$ , such that  $Z \cap (Z + \ell) \neq \emptyset$ . Thus  $\ell + z = z'$  with  $z, z' \in Z$ . Put  $y = 2z$  and  $y' = 2z'$ . Then  $\ell = 2^{-1}(y' - y) \in Y$ , since  $y', -y \in Y$ . This proves the first part of (i). Next, suppose that  $Y$  is closed; take  $0 \neq x_m \in (1 + m^{-1})Y \cap L$ . Then  $\{x_m\}$  has a convergent subsequence. Since  $L$  is discrete, we can choose a "constant" subsequence consisting of a nonzero element  $\ell$  of  $L$ . Put  $x_m = (1 + m^{-1})y_m$  with  $y_m \in Y$ . Then  $\ell$  is the limit of a subsequence of  $\{y_m\}$ . This completes the proof of (i).

To prove (ii), let  $Y$  be the set of all  $x \in \mathbf{R}^n$  such that  $|f_i(x)| \leq b_i$  for every  $i$ , and let  $A = |\det(a_{ij})|$ . Then  $Y$  is a set of the type considered in (i). Since  $Y$  is mapped onto  $\prod_{i=1}^n [-b_i, b_i]^n$  under the map  $x \mapsto (f_i(x))_{i=1}^n$ , we see that  $\text{vol}(Y) = 2^n A^{-1} b_1 \cdots b_n \geq 2^n \text{vol}(\mathbf{R}^n/\mathbf{Z}^n)$  if  $b_1 \cdots b_n \geq A$ . Therefore, by (i),  $Y \cap \mathbf{Z}^n$  contains a nonzero element, which proves (ii).

**Theorem 12.6.** *Let  $n$  and  $s$  be as in §12.2. Then every ideal class contains an integral ideal  $B$  such that*

$$N(B) \leq \frac{n!}{n^n} \left( \frac{4}{\pi} \right)^s |D_F|^{1/2}.$$

PROOF. For  $0 < c \in \mathbf{R}$  put

$$Y_c = \left\{ (x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbf{R}^r \times \mathbf{C}^s \mid \sum_{\mu=1}^r |x_\mu| + 2 \sum_{\nu=1}^s |z_\nu| \leq c \right\}.$$

Putting  $z_\nu = 2^{-1} t_\nu e^{i\theta_\nu}$  we find that

$$\text{vol}(Y_1) = 2^r (\pi/2)^s \int_Z t_1 \cdots t_s dx_1 \cdots dx_r dt_1 \cdots dt_s,$$

where

$$Z = \left\{ (x_1, \dots, x_r, t_1, \dots, t_s) \in \mathbf{R}^{r+s} \mid x_\mu \geq 0, t_\nu \geq 0, \sum_{\mu=1}^r x_\mu + \sum_{\nu=1}^s t_\nu \leq 1 \right\}.$$

It is an easy exercise to show that  $\int_Z = 1/n!$ . Thus  $\text{vol}(Y_c) = 2^{r-s} \pi^s c^n / n!$ . Given a fractional ideal  $A$ , take  $c$  so that  $c^n = n! (4/\pi)^s N(A^{-1}) |D_F|^{1/2}$ . Then  $\text{vol}(Y_c) = 2^n \text{vol}(\mathbf{R}^n / f(A^{-1}))$ . By Theorem 12.5(i) we find  $\alpha \in A^{-1}$ ,  $\neq 0$ , such that  $f(\alpha) \in Y_c$ . Then  $\alpha A$  is integral, and

$$|N(\alpha)|^{1/n} = \left\{ \prod_{j=1}^r |\alpha^{\sigma_j}| \prod_{k=1}^s |\alpha^{\tau_k}|^2 \right\}^{1/n} \leq n^{-1} \left( \sum_{j=1}^r |\alpha^{\sigma_j}| + 2 \sum_{k=1}^s |\alpha^{\tau_k}| \right) \leq c/n.$$

Thus  $N(\alpha A) \leq n^{-n} c^n N(A) = n! n^{-n} (4/\pi)^s |D_F|^{1/2}$ . This proves our theorem.

**Theorem 12.7.** (i) *For  $\mathcal{I}$  and  $\mathcal{P}$  as in §10.18 we have  $[\mathcal{I} : \mathcal{P}] < \infty$ .*

(ii)  *$|D_F| > 1$  if  $F \neq \mathbf{Q}$ .*

(iii) *If  $F \neq \mathbf{Q}$ , then there exists a prime number ramified in  $F$ .*

PROOF. To prove (i), in view of Theorem 12.6 it is sufficient to show that there are only finitely many integral ideals  $B$  such that  $N(B) \leq C$  with a constant  $C$ . Any prime factor  $P$  of such a  $B$  has the same property, and the rational prime divisible by  $P$  is  $\leq C$ . Then the desired conclusion can easily be verified. Put  $A_n = (\pi/4)^{n/2} n^n / n!$ ; then Theorem 12.6 shows that  $|D_F|^{1/2} \geq A_n$  if  $[F : \mathbf{Q}] = n$ . We have  $A_2 = \pi/2 > 1$ , and  $A_{n+1}/A_n = (1 + n^{-1})^n \sqrt{\pi}/2 > 1$ , which proves (ii). Assertion (iii) follows from (ii) combined with Theorem 10.13.

**Theorem 12.8.** (i) *All roots of unity in  $F$  form a finite cyclic group.*

(ii) *An element  $\alpha$  of  $J$  is a root of unity if and only if  $|\alpha^\sigma| = 1$  for every isomorphic embedding  $\sigma$  of  $F$  into  $\mathbf{C}$ .*

PROOF. Suppose  $\alpha \in J$  and  $|\alpha^\sigma| = 1$  for every isomorphic embedding  $\sigma$  of  $F$  into  $\mathbf{C}$ . Take  $f$  as in Theorem 12.3(ii). Since  $f(J)$  is a lattice in  $\mathbf{R}^r \times \mathbf{C}^s$ , the intersection of  $f(J)$  with a bounded set is a finite set. Therefore the powers of such an  $\alpha$  form a finite set, and so  $\alpha$  must be a root of unity. This also shows that there are only finitely many roots of unity, which combined with Theorem 1.5 proves (i).

**Theorem 12.9.** *The notation being the same as in Theorem 12.3, define a homomorphism  $\lambda : F_{\mathbf{R}}^\times = (\mathbf{R}^\times)^r \times (\mathbf{C}^\times)^s \rightarrow \mathbf{R}^{r+s}$  by*

$$\lambda(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s) = (\log |\alpha_1|, \dots, \log |\alpha_r|, 2 \log |\beta_1|, \dots, 2 \log |\beta_s|).$$

(Clearly  $\lambda(f(a)) = (\log |a^{\sigma_1}|, \dots, \log |a^{\sigma_r}|, \log |a^{\tau_1}|^2, \dots, \log |a^{\tau_s}|^2)$  for every  $a \in F^\times$ .) Put  $V = \{x \in \mathbf{R}^{r+s} \mid \sum_{i=1}^{r+s} x_i = 0\}$ ; let  $W$  denote the group of all roots of unity in  $F$ . Then  $\lambda(J^\times)$  is a lattice in  $V$ , and  $W = J^\times \cap \text{Ker}(\lambda)$ .

PROOF. We first note that any discrete subgroup of  $\mathbf{R}^m$  that spans  $\mathbf{R}^m$  over  $\mathbf{R}$  is a lattice in  $\mathbf{R}^m$ . Also in this proof we identify  $F$  with the subset  $f(F)$  of  $\mathbf{R}^r \times \mathbf{C}^s$ . To show that  $\lambda(J^\times)$  is discrete, let  $T_c = \{\alpha \in J^\times \mid \|\lambda(\alpha)\| < c\}$  with  $0 < c \in \mathbf{R}$ , where  $\|x\| = (\sum_{k=1}^{r+s} |x_k|^2)^{1/2}$ . Observe that if  $\alpha \in T_c$ , then  $|\alpha'| < e^c$  for every conjugate  $\alpha'$  of  $\alpha$ , and therefore  $T_c$  is bounded. Since  $T_c$  is contained in the lattice  $J$ ,  $T_c$  must be finite, which means that  $\lambda(J^\times)$  is discrete.

To show that  $\lambda(J^\times)$  spans  $V$ , put

$$S = \{(x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbf{R}^r \times \mathbf{C}^s \mid |x_1 \cdots x_r z_1^2 \cdots z_s^2| = 1\},$$

$$X = \{(x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbf{R}^r \times \mathbf{C}^s \mid |x_\mu| \leq c_\mu, |z_\nu|^2 \leq d_\nu\}$$

with positive numbers  $c_\mu$  and  $d_\nu$ . Then  $\text{vol}(X) = 2^r \pi^s c_1 \cdots c_r d_1 \cdots d_s$ . Take  $c_\mu$  and  $d_\nu$  so that  $\text{vol}(X) > 2^n \text{vol}((\mathbf{R}^r \times \mathbf{C}^s)/J)$ . Let  $\alpha_1 J, \dots, \alpha_t J$  be the integral principal ideals such that  $N(\alpha_i J) \leq c_1 \cdots c_r d_1 \cdots d_s$ . Put  $Y = \bigcup_{i=1}^t \alpha_i^{-1} X$ . If  $u \in S$ , then  $\text{vol}(u^{-1} X) = \text{vol}(X)$ , so that by Theorem 12.5,  $u^{-1} X \cap J$  contains a nonzero element  $\alpha$ . Then  $|N(\alpha)| \leq c_1 \cdots c_r d_1 \cdots d_s$ , and so  $\alpha J = \alpha_i J$  for some  $i$ , which means  $\alpha = \alpha_i \varepsilon$  with  $\varepsilon \in J^\times$ . Then  $u \alpha_i \varepsilon = u \alpha \in X$ , so that  $u \varepsilon \in \alpha_i^{-1} X \subset Y$ . Clearly  $u \varepsilon \in S$ . Thus  $u \varepsilon \in Y \cap S$ , and hence  $\lambda(u) \in \lambda(J^\times) + \lambda(Y \cap S)$ . Since  $V = \lambda(S)$ , we have  $V \subset \lambda(J^\times) + \lambda(Y \cap S)$ . Observe that  $\lambda(Y \cap S)$  is bounded. Therefore  $\lambda(J^\times)$  must span the whole  $V$ . Consequently  $\lambda(J^\times)$  is a lattice in  $V$ . That  $W = J^\times \cap \text{Ker}(\lambda)$  follows from Theorem 12.8(ii).

**Theorem 12.10.**  $J^\times$  is isomorphic to  $W \times \mathbf{Z}^{r+s-1}$ .

PROOF. The above theorem shows that  $J^\times/W$  is isomorphic to a lattice in the vector space  $V$ , which has dimension  $r+s-1$ , so that  $J^\times/W$  is isomorphic to  $\mathbf{Z}^{r+s-1}$ . Therefore, in view of Lemma 5.5 we obtain our theorem.

**Lemma 12.11.** Let  $V = \{x \in \mathbf{R}^q \mid \sum_{i=1}^q x_i = 0\}$ , and let  $L$  be a lattice in  $V$ . Suppose  $L = \sum_{\nu=1}^{q-1} \mathbf{Z}u_\nu$  with  $u_\nu = (a_{1\nu}, \dots, a_{q\nu}) \in \mathbf{R}^q$ . Then

$$\text{vol}(V/L) = \sqrt{q} \left| \det(a_{ij})_{i,j=1}^{q-1} \right|.$$

PROOF. Let  $w$  be the element of  $\mathbf{R}^q$  whose components are all equal to 1. Then  $w$  has length  $\sqrt{q}$ , it is orthogonal to  $V$ , and  $\mathbf{R}^q = V \oplus \mathbf{R}w$ . Put  $M = L \oplus \mathbf{Z}w$ . Then  $M$  is a lattice in  $\mathbf{R}^q$ , and  $\sqrt{q} \text{vol}(V/L) = \text{vol}(\mathbf{R}^q/M) = |\det(U)|$ , where  $U = [u_1 \ \cdots \ u_{q-1} \ w]$ . Adding the first  $q-1$  rows of  $U$  to the last row, we find that

$$\det(U) = \det \begin{bmatrix} a_{11} & \cdots & a_{1t} & 1 \\ \cdots & \cdots & \cdots & \cdots \\ a_{t1} & \cdots & a_{tt} & 1 \\ 0 & \cdots & 0 & q \end{bmatrix},$$

where  $t = q-1$ . From this we obtain  $\text{vol}(V/L)$  as given in our lemma.

**12.12.** The notation being as in §12.2, put  $q = r+s$  and  $t = q-1$ . By Theorem 12.10 we can find  $t$  elements  $\varepsilon_1, \dots, \varepsilon_t$  of  $J^\times$  that generate  $J^\times/W$ . For  $1 \leq i \leq q$  and  $1 \leq j \leq t$  put  $c_{ij} = \log |\varepsilon_j^{\sigma_i}|$  if  $i \leq r$  and  $c_{ij} = 2 \log |\varepsilon_j^{\tau_k}|$  if  $i = r+k$ ,  $1 \leq k \leq s$ . Then we put

$$(12.3) \quad R_F = \left| \det \begin{bmatrix} c_{11} & \cdots & \cdots & c_{1t} \\ \cdots & \cdots & \cdots & \cdots \\ c_{t1} & \cdots & \cdots & c_{tt} \end{bmatrix} \right|,$$

and call  $R_F$  **the regulator of  $F$** . By means of the same technique as in the above proof we can show that

$$qR_F = \left| \det \begin{bmatrix} c_{11} & \cdots & c_{1t} & 1 \\ \cdots & \cdots & \cdots & \cdots \\ c_{q1} & \cdots & c_{qt} & 1 \end{bmatrix} \right|.$$

Take  $\lambda$  and  $V$  as in Theorem 12.9. Then Lemma 12.11 shows that  $\sqrt{q} R_F = \text{vol}(V/\lambda(J^\times))$ .

There is another measure on  $V$  with which  $R_F$  gives exactly the measure of  $V/\lambda(J^\times)$ . Define  $p : \mathbf{R}^q \rightarrow \mathbf{R}$  by  $p(x) = \sum_{i=1}^q x_i$ . Then  $V = \text{Ker}(p)$  and  $\mathbf{R}^q/V \cong \mathbf{R}$ . Taking the standard measures on  $\mathbf{R}^q$  and  $\mathbf{R}$ , we can define a measure  $\mu$  on  $V$  so that

$$\int_{\mathbf{R}^q} f(x) dx = \int_{\mathbf{R}} \int_V f(x+v) d\mu(v) dp(x)$$

holds for integrable functions  $f$  on  $\mathbf{R}^q$ . This is a special case of  $\int_G f(g) dg = \int_{G/H} \int_H f(gh) dh d(gH)$ . Then we easily find that  $\mu(V/L) = \sqrt{q} \text{vol}(V/L)$  for every lattice  $L$  in  $V$ . Thus  $R_F = \mu(V/\lambda(J^\times))$ .

**12.13.** If  $F = \mathbf{Q}$ , we have  $J = \mathbf{Z}$  and  $\mathbf{Z}^\times = \{\pm 1\}$ ; also  $r = 1$  and  $s = 0$ . In this case  $R_{\mathbf{Q}} = 1$ .

Next we take a quadratic field as  $F$ . If  $F$  is imaginary, then  $r = 0$  and  $s = 1$ , and so  $J^\times$  equals the group of all roots of unity  $W$  in  $F$ . Thus  $R_F = 1$ . We have  $W = \{\pm 1\}$  except when  $F = \mathbf{Q}(\sqrt{-1})$  or  $F = \mathbf{Q}(\sqrt{-3})$ , in which case  $W$  has order 4 or 6 accordingly.

Suppose  $F$  is real quadratic; then  $r = 2$ ,  $s = 0$ , and  $W = \{\pm 1\}$ . Take  $\varepsilon \in J^\times$  that generates  $J^\times / \{\pm 1\}$ . Then  $J^\times = \{\pm \varepsilon^n \mid n \in \mathbf{Z}\}$ . Viewing  $F$  as a subfield of  $\mathbf{R}$ , we can choose  $\varepsilon$  so that  $\varepsilon > 1$ . Then  $\varepsilon$  is uniquely determined, and called **the fundamental unit of  $F$** . Clearly  $R_F = \log \varepsilon$ .

**12.14.** Though we do not discuss the zeta function and  $L$ -functions of a number field in this book, let us at least explain the significance of the regulator in this connection. For  $F$ ,  $J$ ,  $r$ ,  $s$ , and  $W$  as in §12.2 and Theorem 12.9, we put  $J^\times = E_F$ ,  $r = r_F$ ,  $s = c_F$ ,  $W = W_F$ , and

$$(12.4) \quad t_F = r_F + c_F - 1,$$

$$(12.5) \quad \zeta_F(s) = \sum_A N(A)^{-s} \quad (s \in \mathbf{C}),$$

where  $A$  runs over the integral ideals in  $F$ . The function  $\zeta_F$  is called the **Dedekind zeta function** of  $F$ . It can be shown that the infinite series of (12.5) is convergent for  $\operatorname{Re}(s) > 1$ , and so defines a holomorphic function of  $s$  there, which can be continued as a meromorphic function of  $s$  to the whole  $s$ -plane. Moreover  $\zeta_F$  has a simple pole at  $s = 1$ , and

$$(12.6) \quad \operatorname{Res}_{s=1} \zeta_F(s) = 2^{r_F} (2\pi)^{c_F} [W_F : 1]^{-1} |D_F|^{-1/2} h_F R_F,$$

where  $h_F$  is the class number of  $F$  and  $R_F$  the regulator of  $F$ . This result is due to Dedekind, and its proof can be found in any advanced textbook of algebraic number theory.

Let  $K$  be a quadratic extension of  $F$ . Then  $\zeta_K(s) = \zeta_F(s)L(s, \lambda)$  with a certain function  $L(s, \lambda)$ , called the  $L$ -function of a character  $\lambda$ , defined by  $L(s, \lambda) = \sum_A \lambda(A)N(A)^{-s}$ , where  $\lambda$  is a multiplicative map  $\mathcal{J} \rightarrow \{\pm 1, 0\}$ . It can be shown that  $L(s, \lambda)$  is an entire function. From (12.6) we see that  $L(1, \lambda)$  is easy factors times  $(h_K/h_F) \cdot (R_K/R_F)$ . Thus we can ask the following natural question: *Is there a formula for  $R_K/R_F$ ?* Indeed,  $R_K/R_F$  is the quotients of two determinants, which involve many units, and so it is desirable to express it with fewer units. We can actually give an answer not only for a quadratic extension, but also for an extension of an arbitrary degree.

To be explicit, denote by  $\Phi_F$  the set  $\{\varphi_1, \dots, \varphi_{r+s}\}$  with  $\varphi_i$  of §12.2. Let  $K$  be an extension of  $F$  of degree  $m (> 1)$ . Put  $b = t_K - t_F$  and take a disjoint decomposition  $\Phi_K = \Psi \cup \Psi'$  such that  $\#\Psi' = \#\Phi_F$  and the restrictions of the members of  $\Psi'$  to  $F$  give the members of  $\Phi_F$  up to equivalence. Put

$$(12.7) \quad U = \{u \in E_K \mid N_{K/F}(u) = 1\}.$$

Then we have:

**Theorem 12.15.** *In the above setting we have  $\#\Psi = b$  and  $U/(U \cap W_K) \cong \mathbf{Z}^b$ . Moreover, let  $\eta_1, \dots, \eta_b$  be elements of  $U$  that generate  $U/(U \cap W_K)$  and let  $\Psi = \{\psi_1, \dots, \psi_b\}$ . Put  $R(K/F) = |\det(e_i \log \psi_i(\eta_j))|$ , where  $e_i = 1$  if  $\psi_i$  is real and  $e_i = 2$  if  $\psi_i$  is imaginary. Then*

$$(12.8) \quad R_K/R_F = [W_F : N_{K/F}(W_K)]^{-1} [E_F : N_{K/F}(E_K)] R(K/F).$$

Thus  $R_K/R_F$  is a rational number times a determinant of size  $b$ . The proof is not difficult; we refer the reader to [S01], in which some identities between the class numbers and regulators of number fields are given.

**Exercises. 1.** Prove that  $(1 + \sqrt{-31})/2$  generates  $P^3$  with a prime ideal  $P$  of  $\mathbf{Q}(\sqrt{-31})$  dividing 2. Show that the class number of  $\mathbf{Q}(\sqrt{-31})$  is 3.

**2.** With  $F = \mathbf{Q}(\sqrt{101})$  determine the decomposition of all rational primes less than 10 in  $F$ , and show that the class number of  $F$  is one.

### 13. Ideals in an extension of a number field

In this section  $F$  denotes an algebraic number field and  $K$  an extension of  $F$  of degree  $d < \infty$ ;  $J_K$  resp.  $J_F$  denotes the maximal order of  $K$  resp.  $F$ .

**Lemma 13.1.** *We have  $XJ_K \cap F = X$  for every fractional ideal  $X$  of  $F$ . Consequently the map  $X \mapsto XJ_K$  defines an injective homomorphism of the ideal group  $\mathcal{I}_F$  of  $F$  into the ideal group  $\mathcal{I}_K$  of  $K$ .*

PROOF. We easily see that  $XJ_K$  is a fractional ideal in  $K$ . Suppose  $XJ_K = YJ_K$  for another fractional ideal  $Y$  in  $K$ . Put  $A = X^{-1}Y$ . Then  $AJ_K = J_K$ , so that  $A \subset J_K \cap F = J_F$ , and similarly  $A^{-1} \subset J_F$ , and so  $A = J_F$ . Thus  $X = Y$ . Given  $X$ , put  $Z = XJ_K \cap F$ . Then  $Z$  is a fractional ideal in  $F$  and  $X \subset Z$ , and so  $XJ_K \subset ZJ_K \subset XJ_K$ . Thus  $XJ_K = ZJ_K$ , and so  $X = Z$ . This completes the proof.

**Lemma 13.2.**  $N(XJ_K) = N(X)^d$  for every  $X \in \mathcal{I}_F$ .

PROOF. It is sufficient to prove this when  $X$  is integral. By Lemma 10.5 we can find  $\alpha \in F^\times$  such that  $\alpha X^{-1}$  is an integral ideal prime to  $N(XJ_K)$ . Put  $Y = \alpha X^{-1}$ . Then by Lemma 10.5(iii),  $N(Y)$  is prime to  $N(XJ_K)$ . Now  $N(XJ_K)N(YJ_K) = N(\alpha J_K) = |N_{K/\mathbf{Q}}(\alpha)| = |N_{F/\mathbf{Q}}(\alpha)|^d = N(\alpha J_F)^d = N(X)^d N(Y)^d$ . Since  $N(Y)$  is prime to  $N(XJ_K)$ , we see that  $N(XJ_K)$  divides  $N(X)^d$ . This is valid for every integral ideal  $X$ , and so  $N(YJ_K)$  divides  $N(Y)^d$ . Thus we obtain  $N(XJ_K) = N(X)^d$ .

**13.3.** Let  $P$  be a prime ideal in  $F$  and let  $Q_1, \dots, Q_g$  be the prime factors of  $PJ_K$  in  $K$ . Then we have

$$(13.1) \quad PJ_K = Q_1^{e_1} \cdots Q_g^{e_g}$$

with positive integers  $e_i$ . Since  $P = Q_i \cap J_F$ , we can view  $J_F/P$  as a subfield of  $J_K/Q_i$ . Put  $f_i = [J_K/Q_i : J_F/P]$ . Counting the number of elements in these fields, we obtain  $N(Q_i) = N(P)^{f_i}$ . By Lemma 13.2 and (13.1) we obtain  $N(P)^d = N(P)^{e_1 f_1} \cdots N(P)^{e_g f_g}$ , and hence

$$(13.2) \quad [K : F] = d = \sum_{i=1}^g e_i f_i,$$

which is a generalization of (10.6). We write  $f_i = f(Q_i/P)$  and  $e_i = e(Q_i/P)$ . We say that  $P$  is **ramified** in  $K$  if  $e_i > 1$  for some  $i$ , and that  $P$  is **unramified** in  $K$  if  $e_1 = \cdots = e_g = 1$ .

We are going to define a homomorphism  $N_{K/F} : \mathcal{J}_K \rightarrow \mathcal{J}_F$ . First, given a prime ideal  $Q$  in  $K$ , let  $P = Q \cap F$  and  $f = [J_K/Q : J_F/P]$ . (If we start from  $P$ , then  $Q$  is one of the  $Q_i$ .) We then put  $N_{K/F}(Q) = P^f$ , and extend the map  $N_{K/F}$  to the whole  $\mathcal{J}_K$  multiplicatively.

**13.4.** Let us apply Theorem 11.5 to the case where  $F$  is an algebraic number field. Take a prime ideal  $P$  of  $F$  and take  $Q_i$ ,  $e_i$ , and  $f_i$  as in (13.2); put  $n_i = e_i f_i$ . Let  $\nu$  (resp.  $\mu_i$ ) be the order function associated with  $P$  (resp.  $Q_i$ ) (see §10.12). The  $e_i^{-1} \mu_i$  are extensions of  $\nu$  to  $K$ , which are clearly different. Let  $F^*$  (resp.  $K_i^*$ ) be the  $\nu$ -completion of  $F$  (resp.  $\mu_i$ -completion of  $K$ .) Comparing (13.2) with Theorem 11.5(iii), we see that the set  $\{U_\sigma\}_{\sigma \in S}$  of Theorem 11.3 is exactly  $\{K_i^*\}_{i=1}^g$ , and the  $e_i^{-1} \mu_i$  are exactly the extensions  $\mu_\sigma$  of  $\nu$  to  $K$  determined in Theorem 11.5. Then we easily see that  $f(Q_i/P) = f(K_i^*/F^*)$  and  $e(Q_i/P) = e(K_i^*/F^*)$ ; also, by (11.3) and (11.4) we have

$$(13.3) \quad K \otimes_F F^* \cong K_1^* \oplus \cdots \oplus K_g^*,$$

$$(13.4) \quad N_{K/F}(a) = \prod_{i=1}^g N_{K_i^*/F^*}(a), \quad \text{Tr}_{K/F}(a) = \sum_{i=1}^g \text{Tr}_{K_i^*/F^*}(a) \quad (a \in K).$$

Let us now take  $F = \mathbf{Q}$ ; let  $\varphi$  be a nonarchimedean valuation of  $K$ , and  $\lambda$  the order function of  $K$  corresponding to  $\varphi$ . By Theorem 6.14 the restriction of  $\varphi$  to  $\mathbf{Q}$  is equivalent to  $\varphi_p$  for some prime number  $p$ . Replacing  $\varphi$  by its suitable power, we may assume that  $\lambda = \nu_p$  on  $\mathbf{Q}$ . Take  $P = p\mathbf{Z}$  in the above discussion. Then we see that  $\lambda$  must be  $e_i^{-1} \mu_i$  for some  $i$ . Thus  $\varphi$  is equivalent to  $\varphi_{Q_i}$  in the sense of §10.12.

**Theorem 13.5.** *The map  $N_{K/F} : \mathcal{J}_K \rightarrow \mathcal{J}_F$  has the following properties, in which  $X$  denotes a fractional ideal in  $K$  :*

- (1)  $N_{K/F}(X)$  is the  $J_F$ -submodule of  $F$  generated by  $N_{K/F}(\xi)$  for all  $\xi \in X$ .
- (2)  $N_{K/F}(\alpha J_K) = N_{K/F}(\alpha) J_F$  for every  $\alpha \in K^\times$ .
- (3)  $N_{L/F}(X) = N_{K/F}(N_{L/K}(X))$  if  $L$  is a finite extension of  $K$ .
- (4)  $N_{K/\mathbf{Q}}(X) = N(X)\mathbf{Z}$ .

(5)  $N(N_{K/F}(X)) = N(X)$ .

(6) If  $K$  is a Galois extension of  $F$  and  $G = \text{Gal}(K/F)$ , then  $N_{K/F}(X)J_K = \prod_{\sigma \in G} X^\sigma$ .

PROOF. To prove (2), we use the notation of §13.4. Since  $e_i^{-1}\mu_i$  is the extension of  $\nu$  to  $K_i^*$ , the proof of Theorem 9.5 shows that  $\nu(N_{K_i^*/F^*}(\alpha)) = n_i e_i^{-1}\mu_i(\alpha) = f_i\mu_i(\alpha)$  for  $\alpha \in K$ . Therefore by (13.4) we have  $\nu(N_{K/F}(\alpha)) = \sum_{i=1}^g f_i\mu_i(\alpha)$ . We can put  $\alpha J_K = \prod_P \prod_{i=1}^g Q_i^{\mu_i(\alpha)}$ , where  $P$  runs over the prime ideals in  $F$  and  $\{Q_i\}_{i=1}^g$  is the set of prime factors of  $P$  in  $K$ . Thus  $N_{K/F}(\alpha J_K) = \prod_P P^{\sum_i f_i\mu_i(\alpha)} = N_{K/F}(\alpha)J_F$ , which is (2).

To prove (1), let  $\xi \in X$ . Then  $\xi X^{-1} \subset J_K$ , and so our definition of  $N_{K/F}(\xi X^{-1})$  shows that  $N_{K/F}(\xi X^{-1}) \subset J_F$ . Employing (2), we see that  $N_{K/F}(\xi)N_{K/F}(X^{-1}) \subset J_F$ , and so

$$(*) \quad N_{K/F}(\xi) \in N_{K/F}(X) \quad \text{for every } \xi \in X.$$

Given any prime ideal  $P$  in  $F$ , Lemma 10.5(i) guarantees an element  $\alpha$  of  $K$  such that  $\alpha X^{-1} + PJ_K = J_K$ . Then  $\alpha \in X$  and  $N_{K/F}(\alpha X^{-1})$ , because of its definition, must be prime to  $P$ . Combining this with (\*), we obtain (1).

To prove (6), put  $Y = \prod_{\sigma \in G} X^\sigma$  and let  $\xi \in X$ . Then  $N_{K/F}(\xi) = \prod_{\sigma \in G} \xi^\sigma \in Y$ , and so  $N_{K/F}(X)J_K \subset Y$  by (1). Suppose  $N_{K/F}(X)Y^{-1} \subset Q$  with a prime ideal  $Q$  in  $K$ ; put  $P = Q \cap F$ . By Lemma 10.5(i), there exists an element  $\alpha$  of  $K^\times$  such that  $\alpha X^{-1} + PJ_K = J_K$ . Then  $\alpha \in X$  and  $(\alpha X^{-1})^\sigma + PJ_K = J_K$  for every  $\sigma \in G$ , and so  $N_{K/F}(\alpha)Y^{-1} + PJ_K = J_K$ . Since  $N_{K/F}(\alpha)Y^{-1} \subset N_{K/F}(X)Y^{-1} \subset J_K$ , we have  $N_{K/F}(X)Y^{-1} + Q = J_K$ , a contradiction. Thus  $N_{K/F}(X)Y^{-1} = J_K$ , which proves (6). The remaining assertions (3), (4), and (5) follow easily from our definition.

## 14. The discriminant and different

**14.1.** In this section  $F$  is either an algebraic number field of finite degree or its completion at a prime ideal. We call  $F$  **local** in the latter case. We denote by  $J$  or  $J_F$  the maximal order of  $F$  or the valuation ring of  $F$ , accordingly;  $K$  is a finite algebraic extension of  $F$  of degree  $n$  and  $J_K$  the maximal order of  $K$ . Also, when  $F$  is local, by a *fractional ideal* in  $K$  we understand a  $J$ -submodule of  $K$  of rank 1, which we call an *integral ideal* if it is contained in  $J_K$ .

Let  $\tilde{F}$  be an algebraic closure of  $F$ , and let  $\sigma_1, \dots, \sigma_n$  be all the different isomorphic embeddings of  $K$  into  $\tilde{F}$  over  $F$ . Given  $\alpha \in K$ , put  $h(x) = \prod_{i=1}^n (x - \alpha^{\sigma_i})$  and  $\delta_{K/F}(\alpha) = h'(\alpha)$ . If we take  $\alpha = \alpha^{\sigma_1}$ , then  $\delta_{K/F}(\alpha) = \prod_{i>1} (\alpha - \alpha^{\sigma_i})$ . Clearly  $h(x)$  belongs to  $F[x]$ , and  $K = F(\alpha)$  if and only if  $\delta_{K/F}(\alpha) \neq 0$ , in which case  $h$  is the minimal polynomial of  $\alpha$  over  $F$ .

The **different of  $K$  relative to  $F$**  is the integral ideal  $d(K/F)$  in  $K$  determined by



$$(14.1) \quad d(K/F)^{-1} = \{x \in K \mid \text{Tr}_{K/F}(xJ_K) \subset J_F\}.$$

To make this definition meaningful, we consider the  $F$ -bilinear form  $(\alpha, \beta) \mapsto \text{Tr}_{K/F}(\alpha\beta)$  of  $K \times K$  to  $F$ , which is nondegenerate by Theorem 7.8(i). Let  $X$  be the right-hand side of (14.1). Then by Lemma 4.4,  $X$  is a  $J_F$ -lattice in  $K$ . Clearly  $J_K X \subset X$ , and so  $X$  is a fractional ideal in  $K$ . From Lemma 8.8 we see that  $J_K \subset X$ , and so  $X^{-1} \subset J_K$ , which establishes  $d(K/F)$  as an integral ideal in  $K$ . We note that

$$(14.1a) \quad \text{Tr}_{K/F}(d(K/F)^{-1}) = J_F.$$

To show this, put  $A = \text{Tr}_{K/F}(d(K/F)^{-1})$ . By (14.1),  $A \subset J_F$ ; also  $\{0\} \neq \text{Tr}_{K/F}(J_K) \subset A$ . Thus  $A$  is an integral ideal, and so  $\text{Tr}_{K/F}(A^{-1}d(K/F)^{-1}) = A^{-1}A = J_F$ . By (14.1) we have  $A^{-1}d(K/F)^{-1} \subset d(K/F)^{-1}$ . Therefore  $A^{-1} \subset J_K \cap F = J_F$ , and so  $A = J_F$  as expected.

We now put

$$(14.2) \quad D(K/F) = N_{K/F}(d(K/F))$$

and call  $D(K/F)$  the **relative discriminant of  $K$  over  $F$** . This is an integral ideal in  $F$ .

**Theorem 14.2.** *If  $L$  is a finite extension of  $K$ , then*

$$d(L/F) = d(L/K)d(K/F).$$

PROOF. We have

$$\begin{aligned} \text{Tr}_{L/F}(d(K/F)^{-1}d(L/K)^{-1}) &= \text{Tr}_{K/F}(\text{Tr}_{L/K}(d(K/F)^{-1}d(L/K)^{-1})) \\ &= \text{Tr}_{K/F}(d(K/F)^{-1}\text{Tr}_{L/K}(d(L/K)^{-1})) \subset \text{Tr}_{K/F}(d(K/F)^{-1}J_K) \subset J_F, \end{aligned}$$

and so  $d(K/F)^{-1}d(L/K)^{-1} \subset d(L/F)^{-1}$ . On the other hand,

$$\text{Tr}_{K/F}(J_K \text{Tr}_{L/K}(d(L/F)^{-1})) = \text{Tr}_{L/F}(d(L/F)^{-1}) \subset J_F,$$

and so  $\text{Tr}_{L/K}(d(L/F)^{-1}) \subset d(K/F)^{-1}$ . Thus  $\text{Tr}_{L/K}(d(K/F)d(L/F)^{-1}) \subset J_K$ , which implies that  $d(K/F)d(L/F)^{-1} \subset d(L/K)^{-1}$ . Combining this with the inclusion we already have, we obtain our theorem.

**Lemma 14.3.** *If  $\alpha \in J_K$  and  $K = F(\alpha)$ , then*

$$\{\xi \in K \mid \text{Tr}_{K/F}(\xi J_F[\alpha]) \subset J_F\} = \delta_{K/F}(\alpha)^{-1} J_F[\alpha].$$

PROOF. Let  $h(x)$  and  $\sigma_i$  be as in §14.1; put  $\alpha_i = \alpha^{\sigma_i}$ . Recall that for every  $g(x) = \sum_{i=0}^{n-1} b_i x^i \in F[x]$  we have

$$(14.3) \quad g(x) = \sum_{i=1}^n \frac{g(\alpha_i)}{h'(\alpha_i)} \frac{h(x)}{x - \alpha_i}.$$

Comparing the coefficients of  $x^{n-1}$  on both sides, we obtain  $b_{n-1} = \sum_{i=1}^n h'(\alpha_i)^{-1}g(\alpha_i) = \text{Tr}_{K/F}(h'(\alpha)^{-1}g(\alpha))$ . Now take  $\beta \in h'(\alpha)^{-1}J[\alpha]$ . Then for every  $\gamma \in J[\alpha]$  we can put  $\beta\gamma = h'(\alpha)^{-1}g(\alpha)$  with some  $g$  of the above type with coefficients in  $J$ , and so  $\text{Tr}_{K/F}(\beta\gamma) = b_{n-1} \in J$ . Conversely, suppose  $\beta \in K$  and  $\text{Tr}_{K/F}(\beta J[\alpha]) \subset J$ . Put  $h'(\alpha)\beta = g(\alpha)$  with  $g \in F[x]$ ,  $\deg(g) < n$ . Put  $f(x) = h(x)/(x-\alpha)$ . Then  $f \in J[\alpha][x]$ , and (14.3) can be written  $g(x) = \sum_{i=1}^n \beta^{\sigma_i} f^{\sigma_i}(x)$ . Each coefficient of the last sum belongs to  $\text{Tr}_{K/F}(\beta J[\alpha])$  which is contained in  $J$ , so that  $g \in J[x]$ . Thus  $\beta \in h'(\alpha)^{-1}J[\alpha]$ . This proves our lemma.

**Theorem 14.4.** (i) *The ideal  $d(K/F)$  is generated by  $\delta_{K/F}(\alpha)$  for all  $\alpha \in J_K$  such that  $K = F(\alpha)$ . Moreover,*

$$(14.4) \quad \delta_{K/F}(\alpha)d(K/F)^{-1} = \{\xi \in K \mid \xi J_K \subset J_F[\alpha]\}$$

for such an  $\alpha$ .

(ii) *The ideal  $D(K/F)$  is generated by  $N_{K/F}(\delta_{K/F}(\alpha))$  for all  $\alpha \in J_K$ .*

PROOF. Since  $\text{Tr}_{K/F}(d(K/F)^{-1}J_F[\alpha]) \subset J_F$ , by Lemma 14.3,  $d(K/F)^{-1} \subset \delta_{K/F}(\alpha)^{-1}J_F[\alpha] \subset \delta_{K/F}(\alpha)^{-1}J_K$ , and so  $\delta_{K/F}(\alpha)J_K \subset d(K/F)$ . Take any  $\xi \in K$ . Then by Lemma 14.3,

$$\begin{aligned} \xi J_K \subset J_F[\alpha] &\Rightarrow \text{Tr}_{K/F}(\xi \delta_{K/F}(\alpha)^{-1}J_K) \subset J_F \Rightarrow \xi \delta_{K/F}(\alpha)^{-1} \in d(K/F)^{-1} \\ &\Rightarrow \xi J_K \subset \delta_{K/F}(\alpha)d(K/F)^{-1} \Rightarrow \xi J_K \subset J_F[\alpha], \end{aligned}$$

which proves (14.4). We also see that  $\delta_{K/F}(\alpha) \in d(K/F)$  if  $\alpha \in J_K$  and  $K = F(\alpha)$ . That  $d(K/F)$  is generated by the  $\delta_{K/F}(\alpha)$  will be proven in §14.14. Once (i) is established, (ii) follows from it and Theorem 13.5(1). Notice also that  $N_{K/F}(\delta_{K/F}(\alpha)) = \pm \Delta(1, \alpha, \dots, \alpha^{n-1})$  by (7.8) if  $n = [K : F]$ .

From (14.4) we immediately obtain

**Corollary 14.5.**  $J_K = J_F[\alpha] \iff d(K/F) = \delta_{K/F}(\alpha)J_K$ .

**Theorem 14.6.** *Suppose  $F$  is local. Then  $K$  is unramified over  $F$  if and only if  $d(K/F) = J_K$ .*

PROOF. Suppose that  $K$  is unramified over  $F$ ; then by Theorems 9.7 and 9.9(i),  $K = F(\gamma)$  and  $J_K = J_F[\gamma]$  with a primitive  $m$ -th root of unity  $\gamma$ , where  $m = q^n - 1$ . Observe that  $m \in J_F^\times$ . Let  $g$  be the minimal polynomial of  $\gamma$  over  $F$ , and let  $x^m - 1 = g(x)h(x)$ . Then  $g'(\gamma)h(\gamma) = m\gamma^{m-1} \in J_K^\times$ , and so  $\delta_{K/F}(\gamma) = g'(\gamma) \in J_K^\times$ . Thus  $d(K/F) \supset \delta_{K/F}(\gamma)J_K = J_K$ , so that  $d(K/F) = J_K$ . Next assume that  $K$  is ramified over  $F$ . By Theorem 9.7(i),  $K$  is a totally ramified extension of an unramified extension  $M$  of  $F$ . Then  $d(K/F) = d(K/M)d(M/F) = d(K/M)$ . Thus our task is to show that  $d(K/M) \neq J_K$ . This is included in the following theorem.

**Theorem 14.7.** *Suppose  $F$  is local; let  $e = e(K/F)$  and let  $\pi$  be a prime element of  $K$ ; further let  $d(K/F) = \pi^t J_K$  with  $t \in \mathbf{Z}$ . Then  $t = e - 1$  if  $e \in J_F^\times$  and  $t \geq e$  if  $e \notin J_F^\times$ .*

PROOF. Take  $M$  as above. Let  $f(x) = x^e + c_1 x^{e-1} + \cdots + c_e$  be the minimal polynomial of  $\pi$  over  $M$ . Let  $\lambda$  be the normalized order function of  $M$ , and  $\mu$  its extension to  $K$ . Then  $\mu(\pi) = e^{-1}$ . Let  $H$  be the Galois closure of  $K$  over  $M$ . Then  $f(x) = \prod_{i=1}^e (x - \pi_i)$  with the conjugates  $\pi_i$  of  $\pi$  over  $M$ . Let  $\kappa$  be the extension of  $\mu$  to  $H$ . Since  $\kappa$  is unique, we have  $\kappa(\pi_i) = \mu(\pi) = e^{-1}$ . Therefore  $\lambda(c_e) = 1$  and  $\lambda(c_i) > 0$  for every  $i$ . Since  $\lambda(M^\times) = \mathbf{Z}$ , we have  $\lambda(c_i) \geq 1$  for every  $i$ , and  $\delta_{K/M}(\pi) = f'(\pi) = e\pi^{e-1} + (e-1)c_1\pi^{e-2} + \cdots + c_{e-1}$ . Therefore, if  $e \in J_F^\times$ , then  $\mu(\delta_{K/M}(\pi)) = (e-1)/e$ . This combined with Theorem 9.9(ii) and Corollary 14.5 shows that  $d(K/F) = d(K/M) = \pi^{e-1} J_K$ . If  $e \notin J_F^\times$ , then  $\mu(\delta_{K/M}(\pi)) \geq 1$ , which proves the other case.

**Theorem 14.8.** *If  $F$  is an algebraic number field, then  $D(F/\mathbf{Q}) = D_F \mathbf{Z}$ .*

PROOF. Let  $\{\alpha_i\}_{i=1}^n$  be a  $\mathbf{Z}$ -basis of  $J_F$ . Then (14.1) shows that

$$d(F/\mathbf{Q})^{-1} = \left\{ \sum_{i=1}^n b_i \alpha_i \mid \sum_{i=1}^n b_i \text{Tr}_{F/\mathbf{Q}}(\alpha_i \alpha_j) \in \mathbf{Z} \text{ for every } j \right\}.$$

Therefore  $N(d(F/\mathbf{Q})) = [d(F/\mathbf{Q})^{-1} : J_F] = |\det(\text{Tr}_{F/\mathbf{Q}}(\alpha_i \alpha_j))| = |D_F|$ , and so  $D(F/\mathbf{Q}) = N_{F/\mathbf{Q}}(d(F/\mathbf{Q})) = N(d(F/\mathbf{Q}))\mathbf{Z} = D_F \mathbf{Z}$ .

**14.9.** Let us now assume that  $F$  is an algebraic number field. For a prime ideal  $P$  in  $F$  we let  $F_P$  denote the  $P$ -completion of  $F$  and  $J_P$  its valuation ring. Given a finite-dimensional vector space  $V$  over  $F$  and a  $J$ -lattice  $L$  in  $V$ , we put  $V_P = V \otimes_F F_P$  and denote by  $L_P$  the  $J_P$ -span of  $L$  in  $V_P$ . Observe that  $L_P$  is the closure of  $L$  in  $V_P$ ; it is a  $J_P$ -lattice in  $V_P$  and compact. If  $\varphi : V \times V \rightarrow F$  is an  $F$ -bilinear form and  $L' = \{x \in V \mid \varphi(x, L) \subset J\}$ , then  $L'$  is a  $J$ -lattice in  $V$  by Lemma 4.4. Moreover, it can easily be shown that

$$(14.5) \quad L'_P = \{x \in V_P \mid \varphi_P(x, L_P) \subset J_P\},$$

where  $\varphi_P$  is the  $F_P$ -bilinear extension of  $\varphi$  to  $V_P \times V_P$ .

Take a finite algebraic extension  $K$  of  $F$  and put  $K_P = K \otimes_F F_P$ . Let  $Q_1, \dots, Q_g$  be the prime factors of  $P$  in  $K$ ; denote by  $K_{Q_i}$  the  $Q_i$ -completion of  $K$ . Then (13.3) can be written

$$(14.6) \quad K_P = K_{Q_1} \oplus \cdots \oplus K_{Q_g}.$$

Moreover, as will be proven in §21.8, we have

$$(14.7) \quad J_K \otimes_{J_F} J_P = J_{Q_1} \oplus \cdots \oplus J_{Q_g}.$$

Let  $X = Q_1^{a_1} \cdots Q_g^{a_g} S$  with integers  $a_i$  and a fractional ideal  $S$  of  $K$  that does not involve the  $Q_i$ . Let  $Q_i^*$  be the maximal ideal of  $J_{Q_i}$ . Then

$$(14.8) \quad X \otimes_{J_F} J_P = (Q_1^*)^{a_1} \oplus \cdots \oplus (Q_g^*)^{a_g}.$$

This can easily be shown by observing that every ideal of  $\bigoplus_{i=1}^g J_{Q_i}$  is of the form  $\bigoplus_{i=1}^g (Q_i^*)^{b_i}$ .

**Theorem 14.10.** *Suppose  $F$  is an algebraic number field; let  $Q$  be a prime ideal in  $K$  and let  $P = Q \cap F$ . Then  $P$  is ramified in  $K$  if and only if  $P$  divides  $d(K/F)$ ;  $Q$  is ramified over  $F$  if and only if  $Q$  divides  $d(K/F)$ . Moreover, let  $e = e(Q/P)$ . If  $e \notin P$ , then  $Q^{e-1}$  is the exact power of  $Q$  dividing  $d(K/F)$ ; if  $e \in P$ , then  $Q^e$  divides  $d(K/F)$ .*

PROOF. Take  $\varphi(\alpha, \beta) = \text{Tr}_{K/F}(\alpha\beta)$  in (14.5) and apply the result to (14.1). Employing the second formula of (13.4), we obtain

$$\begin{aligned} d(K/F)^{-1} \otimes J_P &= \left\{ (x_i) \in \bigoplus_{i=1}^g K_{Q_i} \mid \sum_{i=1}^g \text{Tr}_{K_{Q_i}/F_P}(x_i J_{Q_i}) \subset J_P \right\} \\ &= \bigoplus_{i=1}^g d(K_{Q_i}/F_P)^{-1}. \end{aligned}$$

Put  $d(K_{Q_i}/F_P) = (Q_i^*)^{t_i}$  with  $t_i \in \mathbf{Z}$ . Then by (14.8) we have  $d(K/F) = S \prod_{i=1}^g Q_i^{t_i}$  with an integral ideal  $S$  prime to  $P$ . This proves the first part of our theorem. The remaining part follows from Theorem 14.7.

**Theorem 14.11.** *Suppose  $F$  is an algebraic number field; let  $\alpha$  be an element of  $J_K$  such that  $K = F(\alpha)$ . Let  $h(x)$  be the minimal polynomial of  $\alpha$  over  $F$ , and  $P$  a prime ideal of  $F$  prime to  $d(K/F)^{-1} \delta_{K/F}(\alpha)$ . Let  $\bar{h}(x) = \prod_{i=1}^g k_i(x)^{e_i}$  be the decomposition of  $\bar{h}$  (the class of  $h$  modulo  $P[x]$ ) in  $(J_F/P)[x]$  with different irreducible polynomials  $k_i$ . Then we have  $PJ_K = Q_1^{e_1} \cdots Q_g^{e_g}$  with suitable prime ideals  $Q_i$  in  $K$  such that  $N(Q_i) = N(P)^{f_i}$  with  $f_i = \deg(k_i)$ .*

PROOF. Put  $n = [K : F]$  and  $C = \delta_{K/F}(\alpha) d(K/F)^{-1}$ . By (14.4),  $C \subset J_F[\alpha]$ . Suppose  $P$  is prime to  $C$ . Then  $J_K = PJ_K + C = PJ_K + J_F[\alpha]$ . Let  $PJ_K = Q_1^{a_1} \cdots Q_r^{a_r}$  with prime ideals  $Q_i$  in  $K$  and  $a_i \in \mathbf{Z}$ . We have  $J_F[\alpha] = J_F \oplus J_F \alpha \oplus \cdots \oplus J_F \alpha^{n-1}$ ,  $PJ_F[\alpha] = P \oplus P\alpha \oplus \cdots \oplus P\alpha^{n-1}$ ,  $PJ_F[\alpha] \subset PJ_K \cap J_F[\alpha]$ , and  $J_F[\alpha]/(PJ_K \cap J_F[\alpha]) \cong J_K/PJ_K \cong J_K/Q_1^{a_1} \oplus \cdots \oplus J_K/Q_r^{a_r}$ . The number of elements of the last direct sum is  $\prod_i N(Q_i)^{a_i} = N(PJ_K) = N(P)^n$  by Theorem 13.2. We see that  $[J_F[\alpha] : PJ_F[\alpha]] = [J_F : P]^n = N(P)^n$ . Thus we obtain  $PJ_K \cap J_F[\alpha] = PJ_F[\alpha]$ , and  $J_K/PJ_K \cong J_F[\alpha]/PJ_F[\alpha]$ . Now  $J_F[x]/hJ_F[x] \cong J_F[\alpha]$ . Put  $\Phi = J_F/P$ . Given  $\gamma \in J_F[\alpha]$ , take  $t(x) \in J_F[x]$  so that  $\gamma = t(\alpha)$  and assign  $\bar{t}(x) \pmod{\bar{h}}$  in  $\Phi[x]/(\bar{h})$  to  $\gamma$ . Then we obtain a homomorphism of  $J_F[\alpha]$  onto  $\Phi[x]/(\bar{h})$ . It is easy to see that its kernel is  $PJ_F[\alpha]$ . Thus

$$\bigoplus_{i=1}^r J_K/Q_i^{a_i} \cong J_K/PJ_K \cong J_F[\alpha]/PJ_F[\alpha] \cong \Phi[x]/(\bar{h}) \cong \bigoplus_{i=1}^g \Phi[x]/(k_i^{e_i}).$$

It is easy to prove that the rings  $J_K/Q_i^{a_i}$  and  $\Phi[x]/(k_i^{e_i})$  are indecomposable

in the sense defined in Lemma 1.7; see Exercise 1 at the end of Section 10. Therefore by that lemma, after changing the ordering, we have  $r = g$  and  $J_K/Q_i^{a_i} \cong \Phi[x]/(k_i^{e_i})$  for every  $i$ , and so  $N(Q_i)^{a_i} = N(P)^{e_i f_i}$ , where  $f_i = \deg(k_i)$ . Looking at the set of nilpotent elements, we find that  $J_K/Q_i \cong \Phi[x]/(k_i)$ . Thus  $N(Q_i) = N(P)^{f_i}$ , and so  $a_i = e_i$ . This completes the proof.

**Remark.** The prime ideal  $Q_\nu$  corresponding to  $k_i$  can be determined as follows. With  $\alpha$  as above, for a fixed  $i$ , the element  $k_i(\alpha)$  of  $J_F[\alpha]$  goes to an invertible element of  $\Phi[x]/(k_j^{e_j})$  if  $j \neq i$ . Therefore  $k_i(\alpha) \in Q_\nu$  for exactly one  $\nu$ . Then  $e(Q_\nu/P) = e_i$  and  $f(Q_\nu/P) = \deg(k_i)$ .

**Corollary 14.12.** *Suppose  $F$  is an algebraic number field; let  $\alpha$  be an element of  $J_K$  such that  $K = F(\alpha)$ . Let  $h(x)$  be the minimal polynomial of  $\alpha$  over  $F$ . If  $\bar{h}(x) = \prod_{i=1}^g \ell_i(x)$  in  $(J_F/P)[x]$  with different irreducible polynomials  $\ell_i$ , then  $PJ_K = Q_1 \cdots Q_g$  with different prime ideals  $Q_i$  in  $K$  such that  $N(Q_i) = N(P)^{f_i}$  with  $f_i = \deg(\ell_i)$ .*

PROOF. In this case we see that  $h$  modulo  $Q$  for any prime factor  $Q$  of  $P$  has no multiple root, and therefore  $h'(\alpha) \notin Q$ . Thus  $\delta_{K/F}(\alpha)$  is prime to  $Q$ , and so the above theorem is applicable.

**Lemma 14.13.** *Let  $Q$  be a prime ideal in  $K$  and let  $P = Q \cap F$ . Then the following assertions hold:*

- (i) *For  $\xi \in J_K$  we have  $J_Q = J_P[\xi]$  if  $J_Q = J_P[\xi] + Q^2 J_Q$ .*
- (ii) *Such a  $\xi$  indeed exists.*

PROOF. Suppose  $\xi \in J_K$  and  $J_Q = J_P[\xi] + Q^2 J_Q$ . Take a prime element  $\pi$  of  $K_Q$ . Then  $\pi - \pi_1 \in \pi^2 J_Q$  with some  $\pi_1 \in J_P[\xi]$ . Clearly  $\pi_1$  is a prime element of  $K_Q$ , and so  $\pi^2 J_Q = \pi_1^2 J_Q$ . Thus  $J_Q = J_P[\xi] + \pi_1^2 J_Q$ . Since  $\pi_1 \in J_P[\xi]$ , we can show, by induction, that  $J_Q = J_P[\xi] + \pi_1^k J_Q$  for every  $k \in \mathbf{Z}, > 0$ . The set  $J_P[\xi]$ , being a  $J_P$ -lattice, is closed, and so we obtain  $J_Q = J_P[\xi]$ . This proves (i). To prove (ii), take  $\gamma \in K_Q$  so that  $J_Q = J_P[\gamma]$ ; see Exercise 3 at the end of Section 9. Take also  $\xi \in J_K$  so that  $\xi - \gamma \in Q^2 J_Q$ . Then  $J_Q = J_P[\xi] + Q^2 J_Q$ , which proves (ii).

**14.14.** Let us now prove that  $d(K/F)$  is generated by  $\delta_{K/F}(\alpha)$  as stated in Theorem 14.4. If  $F$  is local,  $J_K = J_F[\alpha]$  for some  $\alpha$ ; see Exercise 3 at the end of Section 9. Then Corollary 14.5 gives the desired fact. Thus we take  $F$  to be global. Our task is to show that given a prime ideal  $Q$  in  $K$ , there exists an element  $\alpha$  of  $J_K$  such that  $K = F(\alpha)$  and  $\delta_{K/F}(\alpha)d(K/F)^{-1}$  is prime to  $Q$ . Put  $P = Q \cap F$  and  $PJ_K = Q^e T$  with an integral ideal  $T$  in  $K$  prime to  $Q$ . By Lemma 14.13, we have  $J_Q = J_P[\xi]$  with a suitable  $\xi \in J_K$ . Replacing  $\xi$  by  $1 + \xi$  if necessary, we may assume that  $\xi \notin Q$ . In view of (1.1), we can find  $\alpha \in T$  such that  $\alpha - \xi \in Q^2$ . Then  $J_Q = J_P[\alpha] + Q^2 J_Q$ , and so  $J_Q = J_P[\alpha]$  by Lemma 14.13(i). Also,  $\alpha \notin Q$ . We may assume that  $K = F(\alpha)$ . (Indeed, take

$\eta \in J_K$  so that  $K = F(\eta)$  and replace  $\alpha$  by  $p^{2\nu}\eta + \alpha$  with  $0 \neq p \in P$  and  $0 < \nu \in \mathbf{Z}$ . If  $p^{2\nu}\eta + \alpha$  and  $p^{2\mu}\eta + \alpha$  belong to the same proper subfield of  $K$  for  $\mu \neq \nu$ , then  $\eta$  belongs to that subfield, a contradiction. Since there are only finitely many subfields of  $K$ , we have  $K = F(\alpha')$  with  $\alpha' = p^{2\nu}\eta + \alpha$  for a suitable  $\nu$ , without losing the properties  $J_Q = J_P[\alpha']$ ,  $\alpha' \in T$ , and  $\alpha' \notin Q$ .) Now  $J_K = J_F[\alpha] + Q^m$  for every  $m \in \mathbf{Z}$ ,  $m > 0$ . (Indeed, let  $\varepsilon \in J_K$ ; then  $\varepsilon = \sum_{i=0}^t c_i \alpha^i$  with  $c_i \in J_P$ ,  $t \in \mathbf{Z}$ . Take  $b_i \in J_F$  so that  $b_i - c_i \in P^m J_P$  and put  $\beta = \sum_{i=0}^t b_i \alpha^i$ . Then  $\varepsilon - \beta \in J_K \cap P^m J_P \subset Q^m$ .) Put  $A = \delta_{K/F}(\alpha) d(K/F)^{-1}$  and let  $0 \neq c \in J_F \cap A$ . If  $c$  is prime to  $P$ , then  $A$  is prime to  $P$ , which settles our problem. Suppose  $cJ_F = P^s X$  with  $0 < s \in \mathbf{Z}$  and an integral ideal  $X$  prime to  $P$ . By Lemma 10.5(i), there is an element  $\zeta$  of  $F^\times$  such that  $J_F = P + \zeta X^{-1}$ . Put  $Y = \zeta X^{-1}$ . Then  $\zeta J_F = XY$ , and so  $\zeta J_F$  is prime to  $P$ , and  $\zeta \alpha^s J_K = \zeta \alpha^s J_F[\alpha] + \zeta \alpha^s Q^{es}$ . Clearly  $\zeta \alpha^s J_F[\alpha] \subset J_F[\alpha]$ ; also,  $\zeta \alpha^s Q^{es} \subset XY T^s Q^{es} = XY P^s J_K \subset cJ_K \subset AJ_K \subset J_F[\alpha]$ , as can be seen from (14.4). Thus  $\zeta \alpha^s J_K \subset J_F[\alpha]$ , and so  $\zeta \alpha^s \in A$  by (14.4). Since both  $\zeta$  and  $\alpha$  are prime to  $Q$ ,  $A$  must be prime to  $Q$  as expected. This completes the proof.

**14.15.** Let us now consider the case  $[K : F] = 2$  with local or global  $F$ . Let  $\sigma$  be the nontrivial automorphism of  $K$  over  $F$ . Then  $\delta_{K/F}(\alpha) = \alpha - \alpha^\sigma$ . Thus  $d(K/F)$  is generated by  $\alpha - \alpha^\sigma$  for all  $\alpha \in J_K$ . Thus, if  $[K : F] = 2$ , Corollary 14.5 can be written

$$(14.9) \quad J_K = J_F[\alpha] \iff d(K/F) = (\alpha - \alpha^\sigma) J_K.$$

Take  $F = \mathbf{Q}$  and  $K = \mathbf{Q}(\sqrt{m})$  with a square-free integer  $m \neq 1$  as in §10.15. Then from (10.10a, b) and (14.9) we obtain

$$(14.10a) \quad d(K/\mathbf{Q}) = \sqrt{m} J_K \quad \text{if } m - 1 \in 4\mathbf{Z},$$

$$(14.10b) \quad d(K/\mathbf{Q}) = 2\sqrt{m} J_K \quad \text{if } m - 1 \notin 4\mathbf{Z}.$$

**Exercises. 1.** Let  $F = \mathbf{Q}(\alpha)$ ,  $\alpha^3 = p$ , with a prime number  $p$  of the form  $p = 3t - 1$ ,  $3 \nmid t$ . Prove in the following steps that  $J = \mathbf{Z}[\alpha]$ .

(a) Compute the discriminant of  $\mathbf{Z}[\alpha]$ , and show that  $[J : \mathbf{Z}[\alpha]] = 3^e p^f$  with integers  $e$  and  $f$ .

(b) Show that  $\mathbf{Z}_p[\alpha]$  is the valuation ring of  $\mathbf{Q}_p(\alpha)$ .

(c) Showing that  $\alpha + 1$  satisfies an Eisenstein equation with respect to 3, prove that  $\mathbf{Z}_3[\alpha]$  is the valuation ring of  $\mathbf{Q}_3(\alpha)$ .

(d) Complete the proof by showing that if  $a + b\alpha + c\alpha^2 \in J$  with  $a, b, c \in \mathbf{Q}$ , then  $a, b, c \in \mathbf{Z}_q$  for every prime  $q$ . (Hint: Employ Theorem 9.9(ii).)

**2.** Employing Theorem 12.6, prove that  $\mathbf{Q}(\sqrt{-1})$  has no nontrivial unramified extension.

**3.** Prove that if  $K = F(c) \neq F$  and  $c^2 \in F$ , then  $d(K/F) = cAJ_K$  with a fractional ideal  $A$  in  $F$ .

4. Let  $K$  and  $L$  be finite extensions of  $F$  contained in an algebraic closure of  $F$ . Prove:

(i)  $d(KL/L)$  divides  $d(K/F)$ ; (ii) if a prime ideal of  $F$  is unramified both in  $K$  and in  $L$ , it is unramified in  $KL$ ; (iii) if  $d(K/F)$  is prime to  $d(L/F)$ , then  $d(KL/L) = d(K/F)J_{KL}$  and  $d(KL/F) = d(K/F)d(L/F)J_{KL}$ .

5. Let  $\mathbf{Q}(\sqrt{m})$  and  $\mathbf{Q}(\sqrt{n})$  be quadratic fields with discriminant  $m$  and  $n$ . Show that  $\mathbf{Q}(\sqrt{m}, \sqrt{n})$  is unramified over  $\mathbf{Q}(\sqrt{mn})$  if  $n$  is prime to  $m$ .

6. Prove that if  $[F : \mathbf{Q}] = 3$  and  $D_F$  is square-free, then  $F(\sqrt{D_F})$  is unramified over  $\mathbf{Q}(\sqrt{D_F})$ . (Hint: Show that  $F(\sqrt{D_F})$  is cyclic over  $\mathbf{Q}(\sqrt{D_F})$ .)

### 15. Adeles and ideles

**15.1.** In this section  $F$  denotes an algebraic number field of finite degree, and  $J$  its maximal order. We now consider the valuations  $\varphi_P$  and  $\varphi_i$  introduced in §§10.12 and 12.2. As shown in §§12.4 and 13.4, these represent all the equivalence classes of valuations of  $F$ . We call each equivalence class of valuations of  $F$  a **prime** of  $F$ ; we call it an **archimedean prime** or a **nonarchimedean prime** of  $F$ , according to the nature of the corresponding valuations. We denote by  $\mathbf{a}$  (resp.  $\mathbf{h}$ ) the set of all archimedean (resp. nonarchimedean) primes of  $F$ , and put  $\mathbf{v} = \mathbf{a} \cup \mathbf{h}$ . Thus each element of  $\mathbf{h}$  is represented by  $\varphi_P$  with a prime ideal  $P$  in  $F$ , and each element of  $\mathbf{a}$  is represented by  $\varphi_i$  as in §12.2.

For each  $v \in \mathbf{v}$  we denote by  $F_v$  the completion of  $F$  with respect to the valuations belonging to  $v$ , and call it the  **$v$ -completion** of  $F$ . We call an archimedean prime  $v$  **real** or **imaginary** according as  $F_v \cong \mathbf{R}$  or  $F_v \cong \mathbf{C}$ . For  $x \in F_v$  we define  $|x|_v$  as follows: if  $v$  corresponds to a prime ideal  $P$ , then  $|x|_v = \varphi_P(x)$ ; if  $v$  is real archimedean and corresponds to  $\sigma_i$  of §12.2, then  $|x|_v = \varphi_i(x)$ ; if  $v$  is imaginary and corresponds to  $\tau_i$ , then  $|x|_v = \varphi_{\tau+i}(x)^2$ . Then (12.1) can be written

$$(15.1) \quad \prod_{v \in \mathbf{v}} |x|_v = 1 \quad \text{for every } x \in F^\times.$$

Let  $K$  be a finite algebraic extension of  $F$ . We say that a prime  $v \in \mathbf{h}$  is **ramified** or **unramified** in  $K$  according as the prime ideal corresponding to  $v$  is ramified or unramified in  $K$  in the sense of §13.3. For  $v \in \mathbf{a}$  we say that  $v$  is **ramified** in  $K$  if  $v$  is real and  $v$  has an extension in  $K$  that is imaginary. Otherwise we say that  $v$  is **unramified** in  $K$ .

**15.2.** For  $v \in \mathbf{h}$  and a fractional ideal  $A$  in  $F$  we denote by  $A_v$  the closure of  $A$  in  $F_v$ . In particular,  $J_v$  is the valuation ring of  $F_v$  and  $A_v$  is the  $J_v$ -linear span of  $A$  in  $F_v$ . We now define **the adele ring**  $F_{\mathbf{A}}$  of  $F$  by

$$(15.2) \quad F_{\mathbf{A}} = \left\{ x \in \prod_{v \in \mathbf{v}} F_v \mid x_v \in J_v \text{ for almost all } v \in \mathbf{h} \right\}.$$

We easily see that  $F_{\mathbf{A}}$  is a ring with respect to componentwise addition and multiplication. Also we can view  $F_v$  for each  $v \in \mathbf{v}$  as a subring of  $F_{\mathbf{A}}$  through the standard injection  $F_v \rightarrow \prod_{v \in \mathbf{v}} F_v$ . Identifying an element  $x$  of  $F$  with the element of  $F_{\mathbf{A}}$  whose components are all equal to  $x$ , we view  $F$  as a subring of  $F_{\mathbf{A}}$ . We put  $F_{\mathbf{a}} = \prod_{v \in \mathbf{a}} F_v$ , which can be identified with  $F \otimes_{\mathbf{Q}} \mathbf{R}$ , as shown in Theorem 12.3(iii). If  $v \in \mathbf{a}$ ,  $F_v$  is either  $\mathbf{R}$  or  $\mathbf{C}$  and so is locally compact. The same is true for  $v \in \mathbf{h}$ , as shown in Lemma 6.9, which also shows that both  $J_v$  and  $J_v^\times$  are open in  $F_v$  and compact.

Put  $B = F_{\mathbf{a}} \times \prod_{v \in \mathbf{h}} J_v$ . Then  $B$  has a structure of a locally compact topological (additive) group with respect to the standard product topology. We make  $F_{\mathbf{A}}$  a topological group by taking  $B$  to be its open subgroup. Then  $F_{\mathbf{A}}$  is locally compact.

**Lemma 15.3.** (i) *Let  $X$  be a fractional ideal in  $F$  and let  $Y = F_{\mathbf{a}} \times \prod_{v \in \mathbf{h}} X_v$ . Then  $F_{\mathbf{A}} = F + Y$  and  $X = F \cap Y$ .*

(ii) *For every finite subset  $\mathbf{p}$  of  $\mathbf{h}$  the projection of  $F$  on  $F_{\mathbf{a}} \times \prod_{v \in \mathbf{p}} F_v$  is dense. (We will prove a similar result in a stronger form in Lemma 15.10.)*

PROOF. The last equality of (i) is clear. As for the first equality, it is sufficient to prove it when  $X = J$ , since  $cJ \subset X$  for some  $c \in F^\times$ . Given  $z \in F_{\mathbf{A}}$ , take  $a \in J$ ,  $a \neq 0$ , so that  $az_v \in J_v$  for every  $v \in \mathbf{h}$ . Such an  $a$  exists because of our definition of  $F_{\mathbf{A}}$ . In view of (1.1) we can find  $b \in J$  such that  $b - az_v \in aJ_v$  whenever  $a \notin J_v^\times$ . Then we see that  $a^{-1}b - z_v \in J_v$  for every  $v \in \mathbf{h}$ , that is,  $z \in F + (F_{\mathbf{a}} \times \prod_{v \in \mathbf{h}} J_v)$ . This proves (i).

Next, denote by  $J'$  the image of  $J$  under the natural projection map of  $F$  into  $F_{\mathbf{a}}$ . By Theorem 12.3(iv),  $J'$  is a lattice in  $F_{\mathbf{a}}$ , and so there is a compact subset  $C$  of  $F_{\mathbf{a}}$  that covers  $F_{\mathbf{a}}/J'$ . Let  $t = \max\{|\xi_v|_v \mid \xi \in C, v \in \mathbf{a}\}$ . To prove (ii), it is sufficient to show that given  $\varepsilon \in \mathbf{R}$ ,  $\varepsilon > 0$ ,  $0 < N \in \mathbf{Z}$ ,  $\xi \in F_{\mathbf{a}}$ , and  $(\eta_v)_{v|N} \in \prod_{v|N} F_v$ , there exists an element  $\alpha$  of  $F$  such that  $|\xi_v - \alpha|_v < \varepsilon$  for every  $v \in \mathbf{a}$  and  $\eta_v - \alpha \in NJ_v$  for every  $v|N$ . Replacing  $\xi$  and  $\eta_v$  by their suitable integer multiples, we may assume that  $\eta_v \in J_v$  for every  $v|N$ . Since  $J/NJ \cong \prod_{v|N} J_v/NJ_v$ , we can find  $\beta \in J$  such that  $\beta - \eta_v \in NJ_v$  for every  $v|N$ . Take a positive integer  $k$  so that  $(1 + kN)^{-1}Nt < \varepsilon$ . Since  $C$  covers  $F_{\mathbf{a}}/J'$ , we can find  $\gamma \in J$  such that  $|(1 + kN)N^{-1}(\xi_v - \beta) - \gamma|_v \leq t$  for every  $v \in \mathbf{a}$ . Put  $\alpha = \beta + (1 + kN)^{-1}N\gamma$ . Then  $|\xi_v - \alpha|_v < \varepsilon$  for every  $v \in \mathbf{a}$  and  $\alpha - \eta_v \in NJ_v$  for every  $v|N$ . This proves (ii).

**Theorem 15.4.**  *$F$  is discrete in  $F_{\mathbf{A}}$ , and  $F_{\mathbf{A}}/F$  is compact.*

PROOF. Let  $J'$  be the image of  $J$  under the projection map of  $F_{\mathbf{A}}$  onto  $F_{\mathbf{a}}$ . Then  $J'$  is a lattice in  $F_{\mathbf{a}}$  (see Theorem 12.3(iii, iv)), and so we can find an open subset  $B$  of  $F_{\mathbf{a}}$  such that  $B \cap J' = \{0\}$ . Then  $F \cap (B \times \prod_{v \in \mathbf{h}} J_v) = \{0\}$ , and so  $F$  is discrete in  $F_{\mathbf{A}}$ . Next, take a compact subset  $C$  of  $F_{\mathbf{a}}$  so that  $C$  covers



$F_{\mathbf{a}}/J'$ . Put  $D = C \times \prod_{v \in \mathbf{h}} J_v$ . Then  $D$  is compact, and  $F_{\mathbf{a}} \subset D + J$ . Therefore  $D + J = F_{\mathbf{a}} \times \prod_{v \in \mathbf{h}} J_v$ , and so  $D + F \supset D + J + F = (F_{\mathbf{a}} \times \prod_{v \in \mathbf{h}} J_v) + F = F_{\mathbf{A}}$  by Lemma 15.3. This shows that  $F_{\mathbf{A}}/F$  is compact.

**15.5. The idele group of  $F$**  is the group  $F_{\mathbf{A}}^{\times}$  of the invertible elements of  $F_{\mathbf{A}}$ . We easily see that

$$(15.3) \quad F_{\mathbf{A}}^{\times} = \{x \in \prod_{v \in \mathbf{v}} F_v^{\times} \mid x_v \in J_v^{\times} \text{ for almost all } v \in \mathbf{h}\}.$$

We consider  $F^{\times}$  as a subgroup of  $F_{\mathbf{A}}^{\times}$  through the injection  $F^{\times} \rightarrow F_{\mathbf{A}}^{\times}$  obtained from the injection  $F \rightarrow F_{\mathbf{A}}$  of §15.2. We also consider  $F_v^{\times}$  for each  $v \in \mathbf{v}$  a subgroup of  $F_{\mathbf{A}}^{\times}$  through the natural injection  $F_v^{\times} \rightarrow F_{\mathbf{A}}^{\times}$ . We put

$$(15.4) \quad F_{\mathbf{a}}^{\times} = \{x \in F_{\mathbf{A}}^{\times} \mid x_v = 1 \text{ for every } v \in \mathbf{h}\},$$

$$(15.5) \quad F_{\mathbf{h}}^{\times} = \{x \in F_{\mathbf{A}}^{\times} \mid x_v = 1 \text{ for every } v \in \mathbf{a}\}.$$

These are subgroups of  $F_{\mathbf{A}}^{\times}$ , and  $F_{\mathbf{A}}^{\times} = F_{\mathbf{a}}^{\times} F_{\mathbf{h}}^{\times}$ . For  $x \in F_{\mathbf{A}}^{\times}$  we denote its projections to  $F_{\mathbf{a}}^{\times}$  and  $F_{\mathbf{h}}^{\times}$  by  $x_{\mathbf{a}}$  and  $x_{\mathbf{h}}$ . Put

$$(15.6) \quad U = F_{\mathbf{a}}^{\times} \times \prod_{v \in \mathbf{h}} J_v^{\times}.$$

Then  $U$  has a structure of a locally compact topological (multiplicative) group with respect to the standard product topology. We make  $F_{\mathbf{A}}^{\times}$  a topological group by taking  $U$  to be its open subgroup. Then  $F_{\mathbf{A}}^{\times}$  is locally compact. This topology of  $F_{\mathbf{A}}^{\times}$  is **not** induced from the topology of  $F_{\mathbf{A}}$ .

For  $x \in F_{\mathbf{A}}^{\times}$  and a fractional ideal  $Y$  in  $F$  we denote by  $xY$  the fractional ideal in  $F$  such that  $(xY)_v = x_v Y_v$ . To see that such a fractional ideal exists, let  $\mathbf{p} = \{v \in \mathbf{h} \mid x_v \notin J_v^{\times} \text{ or } Y_v \neq J_v\}$ . Then  $\mathbf{p}$  is a finite set, and  $x_v Y_v = J_v$  if  $v \notin \mathbf{p}$ . For each  $v \in \mathbf{p}$  let  $P_{(v)}$  denote the prime ideal in  $F$  corresponding to  $v$ . Then  $x_v Y_v = (P_{(v)} J_v)^{m_v}$  with  $m_v \in \mathbf{Z}_v$ . Then define  $xY = \prod_{v \in \mathbf{p}} P_{(v)}^{m_v}$ , which gives the desired ideal.

In particular,  $xJ$  is a fractional ideal for  $x \in F_{\mathbf{A}}^{\times}$ . Clearly the map  $x \mapsto xJ$  gives an isomorphism of  $F_{\mathbf{A}}^{\times}/U$  onto the ideal group of  $F$ , and also an isomorphism of  $F_{\mathbf{A}}^{\times}/(F^{\times}U)$  onto the ideal class group of  $F$ . If the class number of  $F$  is 1, then  $F_{\mathbf{A}}^{\times} = F^{\times} F_{\mathbf{a}}^{\times} \prod_{v \in \mathbf{h}} J_v^{\times}$ . In particular, for  $F = \mathbf{Q}$  we have

$$(15.6a) \quad \mathbf{Q}_{\mathbf{A}}^{\times} = \mathbf{Q}^{\times} \mathbf{R}^{\times} \prod_p \mathbf{Z}_p^{\times}.$$

**15.6.** Given  $x \in F_{\mathbf{A}}^{\times}$ , we define its **idele norm**  $|x|_{\mathbf{A}}$  by

$$(15.7) \quad |x|_{\mathbf{A}} = \prod_{v \in \mathbf{v}} |x|_v,$$

where  $|x|_v = |x_v|_v$  with  $| \cdot |_v$  of §15.1. We put then

$$(15.8) \quad D = \{x \in F_{\mathbf{A}}^{\times} \mid |x|_{\mathbf{A}} = 1\}.$$

From (15.1) we see that  $|\xi|_{\mathbf{A}} = 1$  for every  $\xi \in F^{\times}$ , and so  $F^{\times} \subset D$ . Also, from the definition of  $|x|_v$  for  $v \in \mathbf{h}$  we see that

$$(15.9a) \quad |x_{\mathbf{h}}|_{\mathbf{A}} = N(xJ)^{-1} \quad \text{for every } x \in F_{\mathbf{A}}^{\times},$$

$$(15.9b) \quad |\xi_{\mathbf{h}}|_{\mathbf{A}}^{-1} = |\xi_{\mathbf{a}}|_{\mathbf{A}} = |N_{F/\mathbf{Q}}(\xi)| \quad \text{for every } \xi \in F^{\times}.$$

For  $x \in F_{\mathbf{A}}^{\times}$  we put

$$(15.10) \quad T(x) = \#S(x), \quad S(x) = \{\alpha \in xJ \mid |\alpha|_v \leq |x|_v \text{ for every } v \in \mathbf{a}\},$$

where  $\#X$  is the number of elements in a set  $X$ . Since the projection of  $xJ$  to  $F_{\mathbf{a}}$  is a lattice,  $T(x)$  is well defined (that is, it is finite, not  $\infty$ ). We easily see that  $T(\beta x) = T(x)$  for every  $\beta \in F^{\times}$ .

**Theorem 15.7.**  $F^{\times}$  is discrete in  $F_{\mathbf{A}}^{\times}$  and  $D/F^{\times}$  is compact.

PROOF. To prove the first assertion, it is sufficient to prove that  $J^{\times}$  is discrete in  $U$ , since  $U$  is open and  $U \cap F^{\times} = J^{\times}$ . Observe that

$$D/[F^{\times}(D \cap U)] = D/(D \cap F^{\times}U) \cong (F^{\times}UD)/(F^{\times}U) \subset F_{\mathbf{A}}^{\times}/(F^{\times}U).$$

Thus  $D/[F^{\times}(D \cap U)]$  is finite. Therefore, to prove that  $D/F^{\times}$  is compact, it is sufficient to prove that  $[F^{\times}(D \cap U)]/F^{\times}$  is compact. Now this group is isomorphic to  $(D \cap U)/J^{\times}$ , since  $J^{\times} = F^{\times} \cap U$ . Put  $Y = D \cap F_{\mathbf{a}}^{\times}$ . Then  $D \cap U = Y \prod_{v \in \mathbf{h}} J_v^{\times}$ . Thus our aim is to show that  $[Y \prod_{v \in \mathbf{h}} J_v^{\times}]/J^{\times}$  is compact. Define the map  $\lambda : F_{\mathbf{a}}^{\times} \rightarrow \mathbf{R}^{r+s}$  and  $V$  as in Theorem 12.9. Let  $J^*$  be the projection of  $J^{\times}$  to  $F_{\mathbf{a}}^{\times}$ . We showed in Theorem 12.9 that  $\lambda(J^*)$  is a lattice in  $V$ . (In that theorem we viewed  $F^{\times}$  as a subset of  $F_{\mathbf{a}}^{\times}$ , and so  $J^*$  is  $J^{\times}$  there.) Now  $\lambda$  maps  $Y/J^*$  onto  $V/\lambda(J^*)$ , which is compact. Thus we can find a compact subset  $C$  of  $Y$  such that  $\lambda(C)$  covers  $V/\lambda(J^*)$ . Put  $X = \text{Ker}(\lambda)C$ . Since  $\text{Ker}(\lambda)$  is compact,  $X$  is compact. We easily see that  $X$  covers  $Y/J^*$ , and so  $X \prod_{v \in \mathbf{h}} J_v^{\times}$  covers  $(Y \prod_{v \in \mathbf{h}} J_v^{\times})/J^{\times}$ . This proves our theorem.

**Lemma 15.8.** *The notation being as in (15.10), there exists a constant  $C > 1$  depending only on  $F$  such that  $|x|_{\mathbf{A}} < CT(x)$  for every  $x \in F_{\mathbf{A}}^{\times}$ .*

PROOF. Take a  $\mathbf{Q}$ -basis  $\{e_i\}_{i=1}^n$  of  $F$  contained in  $J$ . Replacing  $\{e_i\}$  by  $\{ke_i\}$  with a suitable integer  $k$ , we may assume that  $|e_i|_v \geq 1$  for every  $i$  and every  $v \in \mathbf{a}$ . Put  $E = \text{Max}\{|e_i|_v \mid 1 \leq i \leq n, v \in \mathbf{a}\}$  and take an integer  $\lambda > nE$ . Since the projection of  $F$  to  $F_{\mathbf{a}}$  is dense, given  $x \in F_{\mathbf{A}}^{\times}$ , we can find an element  $\beta$  of  $F$  such that  $|2\lambda|_v < |\beta x|_v < |3\lambda|_v$  for every  $v \in \mathbf{a}$ . Take a positive integer  $\mu$  so that  $\mu\beta xJ \subset J$  and put  $x' = \mu\beta x$ . Then  $|x'|_{\mathbf{A}} = |x|_{\mathbf{A}}$  and  $T(x') = T(x)$ . Thus, replacing  $x$  by  $x'$ , we may assume that  $xJ \subset J$  and  $|2\mu\lambda|_v < |x|_v < |3\mu\lambda|_v$  for every  $v \in \mathbf{a}$ . Let  $y$  be the element of  $F_{\mathbf{A}}^{\times}$  such that  $y_{\mathbf{h}} = 1$  and  $y_v = \mu\lambda$  for every  $v \in \mathbf{a}$ . Now, for  $\alpha = \sum_{i=1}^n \nu_i e_i$  with  $\nu_i \in \mathbf{Z}$  such that  $|\nu_i| \leq \mu$ , we have  $\alpha \in J = yJ$  and  $|\alpha|_v \leq |n\mu|_v E < |\mu\lambda|_v$  for every  $v \in \mathbf{a}$ . (This is so even for imaginary  $v$ , as  $|n\mu|_v = n^2\mu^2$ .) Thus  $\alpha \in S(y)$ , and so  $T(y) \geq (2\mu+1)^n > \mu^n$ . Put  $X = xJ$ . If  $\gamma \in S(y)$ , then  $\gamma \in J$  and  $\gamma$  belongs to a residue class of  $J$  modulo  $X$ . Let  $r$  be the smallest integer  $> \mu^n/N(X)$ . Then

one of the residue classes modulo  $X$  must contain  $r$  elements  $\xi_1, \dots, \xi_r$  belonging to  $S(y)$ . Then the  $r$  elements  $\xi_i - \xi_1$  for  $1 \leq i \leq r$  belong to  $S(x)$ . By (15.9),  $N(X) = |x_{\mathbf{h}}|_{\mathbf{A}}^{-1}$ , and so we have  $T(x)|x|_{\mathbf{A}}^{-1} > \mu^n |x_{\mathbf{a}}|_{\mathbf{A}}^{-1} > \mu^n (3\mu\lambda)^{-n} = (3\lambda)^{-n}$ . This proves our lemma.

**Lemma 15.9.** *Let  $u \in \mathbf{a}$ . If  $\mathbf{a} \neq \{u\}$ , then  $\mathbf{g}^\times$  has an element  $\varepsilon$  such that  $|\varepsilon|_u > 1$  and  $|\varepsilon|_v < 1$  for every  $v \in \mathbf{a}, \neq u$ .*

PROOF. Take  $C$  as in Lemma 15.8. Let  $\mathbf{p}$  be the set of all  $v$  in  $\mathbf{h}$  corresponding to the prime ideals  $\mathfrak{p}$  such that  $N(\mathfrak{p}) \leq C$ . Then  $\mathbf{p}$  is a finite set. Let  $Y = \{y \in F^\times \mid C^{-1} \leq |y|_v \leq 1 \text{ for every } v \in \mathbf{h}\}$ . If  $y \in Y, v \in \mathbf{h}, \notin \mathbf{p}$ , and  $\pi$  is a prime element at  $v$ , then  $|\pi|_v < C^{-1} \leq |y|_v \leq 1$ , and so  $|y|_v = 1$ . Thus  $y$  is a  $v$ -unit for every  $v \in \mathbf{h}, \notin \mathbf{p}$ . Let  $\mu_v$  be the normalized order function at  $v$ . Then the image of  $Y$  under the map  $y \mapsto (\mu_v(y))_{v \in \mathbf{h}}$  is finite. Two elements  $y$  and  $y'$  of  $Y$  have the same image under this map if and only if  $y/y' \in \mathbf{g}^\times$ , and so  $Y = \bigcup_{\beta \in B} \mathbf{g}^\times \beta$  with a finite subset  $B$  of  $Y$ . Take an element  $x$  of  $F_{\mathbf{A}}^\times$  such that  $x_v = 1$  for every  $v \in \mathbf{h}$ , and  $|x|_v < |\beta|_v$  for every  $\beta \in B$  and every  $v \in \mathbf{a}, \neq u$ . We can take  $x$  so that  $|x|_{\mathbf{A}} = C$ , since  $\mathbf{a} \neq \{u\}$ . By Lemma 15.8,  $T(x) \neq \emptyset$ . Thus there is an element  $\alpha$  of  $J$  such that  $|\alpha_{\mathbf{a}}|_{\mathbf{A}} \leq |x|_{\mathbf{A}} = C$ . Then  $1 = |\alpha|_{\mathbf{A}} = |\alpha_{\mathbf{a}}|_{\mathbf{A}} |\alpha_{\mathbf{h}}|_{\mathbf{A}} \leq C |\alpha_{\mathbf{h}}|_{\mathbf{A}} \leq C |\alpha|_v$  for every  $v \in \mathbf{h}$ , since  $\alpha \in J$ . Therefore  $\alpha \in Y$ , and so  $\alpha = \beta \varepsilon$  with some  $\beta \in B$  and  $\varepsilon \in \mathbf{g}^\times$ . Then for  $v \in \mathbf{a}, \neq u$ , we have  $|\varepsilon|_v = |\alpha/\beta|_v \leq |x|_v/|\beta|_v < 1$ . Since  $\varepsilon \in \mathbf{g}^\times$  and  $|\varepsilon|_{\mathbf{A}} = 1$ , we have  $|\varepsilon|_u > 1$ . This proves our lemma.

**Lemma 15.10.** *Let  $\mathbf{p}$  be a finite subset of  $\mathbf{h}$  and let  $\mathbf{a} = \{u\} \cup \mathbf{b}$  with an arbitrarily fixed  $u \in \mathbf{a}$ . Given  $(\xi_v) \in \prod_{v \in \mathbf{p} \cup \mathbf{b}} F_v$  and  $\varepsilon > 0$ , there exists an element  $\alpha \in F$  such that  $|\alpha - \xi_v|_v < \varepsilon$  for every  $v \in \mathbf{p} \cup \mathbf{b}$ ,  $|\alpha|_u > 1/\varepsilon$ , and  $\alpha \in \mathbf{g}_v$  for every  $v \in \mathbf{h}, \notin \mathbf{p}$ .*

PROOF. In this proof  $\varepsilon_1, \varepsilon_2$ , etc. mean small positive numbers. By Lemma 15.3(ii) there is an element  $\beta \in F$  such that  $|\beta - \xi_v|_v < \varepsilon_1$  for every  $v \in \mathbf{p} \cup \mathbf{b}$ . Put  $\mathbf{x} = \{v \in \mathbf{h} \mid v \notin \mathbf{p}, \beta \notin \mathbf{g}_v\}$ ; let  $\mathfrak{x}$  be the integral ideal such that  $\mathfrak{x}_v = \beta^{-1} \mathbf{g}_v$  for every  $v \in \mathbf{x}$  and  $\mathfrak{x}_v = \mathbf{g}_v$  for every  $v \in \mathbf{h}, \notin \mathbf{x}$ . Let  $R$  be a complete set of representatives for  $\mathbf{g}/\mathfrak{x}$ , and  $\mathfrak{q}$  an integral ideal such that  $\mathfrak{q}_v \neq \mathbf{g}_v$  if and only if  $v \in \mathbf{p}$ . If  $h$  is a multiple of the class number of  $F$ , then  $\mathfrak{q}^h = c\mathbf{g}$  with  $c \in \mathbf{g}$ . Taking a suitably large  $h$ , we can take  $c$  so that  $|c\zeta|_v < \varepsilon_2$  for every  $\zeta \in R$  and every  $v \in \mathbf{p}$ . By Lemma 15.9 there exists an element  $\delta$  of  $\mathbf{g}^\times$  such that  $|\delta|_v < 1$  for every  $v \in \mathbf{b}$ . Replacing  $\delta$  by its suitable power, we may assume that  $|\delta c \zeta|_v < \varepsilon_3$  for every  $\zeta \in R$  and every  $v \in \mathbf{b}$ . Since  $\delta c$  is prime to  $\mathfrak{x}$ , we have  $\delta c \zeta + 1 \in \mathfrak{x}$  for some  $\zeta \in R$ . Put  $\gamma = \delta c \zeta + 1$ . Then  $\gamma \in \mathbf{g}$ , and in view of our definition of  $\mathfrak{x}$  we see that  $\gamma \beta \in \mathbf{g}_v$  for  $v \in \mathbf{h}, \notin \mathbf{p}$ . We can take  $\gamma \beta$  to be the desired  $\alpha$  of our lemma in a weaker form in which the condition on  $|\alpha|_u$  is dropped. Indeed, if  $v \in \mathbf{p}$ , then  $|\gamma - 1|_v = |\delta c \zeta|_v = |c \zeta|_v < \varepsilon_2$ , and if  $v \in \mathbf{b}$ ,

then  $|\gamma - 1|_v = |\delta c \zeta|_v < \varepsilon_3$ . Therefore, with suitable  $\varepsilon_1, \varepsilon_2$ , and  $\varepsilon_3$ , we have  $|\gamma\beta - \xi_v|_v < \varepsilon$  for  $v \in \mathbf{p} \cup \mathbf{b}$  as expected. To include the condition on  $|\alpha|_u$ , pick any prime  $w \in \mathbf{h}, \notin \mathbf{p}$ . Replacing  $\mathbf{p}$  by  $\{w\} \cup \mathbf{p}$ , we find an element  $\alpha$  of  $F$  such that  $0 < |\alpha|_w < \varepsilon_4$ ,  $|\alpha - \xi_v|_v < \varepsilon$  for  $v \in \mathbf{p} \cup \mathbf{b}$ , and  $\alpha \in \mathfrak{g}_v$  for  $v \in \mathbf{h}, \notin \{w\} \cup \mathbf{p}$ . Then  $1 = |\alpha|_{\mathbf{A}} \leq \varepsilon_4 |\alpha|_u \prod_{v \in \mathbf{p} \cup \mathbf{b}} |\alpha|_v \leq \varepsilon_4 |\alpha|_u \prod_{v \in \mathbf{p} \cup \mathbf{b}} (|\xi_v|_v + \varepsilon)$ . Taking a sufficiently small  $\varepsilon_4$ , we obtain  $|\alpha|_u > 1/\varepsilon$  as desired.

## 16. Galois extensions

The notation is the same as in Section 14. We first assume that  $F$  is an algebraic number field.

**Theorem 16.1.** *Let  $K$  be a Galois extension of  $F$  of degree  $d$ ,  $P$  a prime ideal in  $F$ , and  $Q$  a prime ideal in  $K$  that divides  $P$ . Put  $G = \text{Gal}(K/F)$ ,  $e = e(Q/P)$ , and  $f = f(Q/P)$ . Then the following assertions hold:*

(1) *Let  $Q_1, \dots, Q_g$  denote all the different prime factors of  $P$  in  $K$ . Then the ideals  $Q^\sigma$  for  $\sigma \in G$  are exactly  $Q_1, \dots, Q_g$  with each  $Q_i$  repeated  $ef$  times.*

(2) *Let  $Z = \{\sigma \in G \mid Q^\sigma = Q\}$ . Then  $[Z : 1] = ef$ ,  $[G : Z] = g$ , and  $d = efg$ .*

(3)  $PJ_K = (Q_1 \cdots Q_g)^e$ .

(4)  $e(Q_i/P) = e$  and  $f(Q_i/P) = f$  for every  $i$ .

PROOF. Clearly for every  $\sigma \in G$ ,  $Q^\sigma$  must coincide with one of the  $Q_i$ . Suppose there is an  $i$  such that  $Q_i \neq Q^\sigma$  for every  $\sigma \in G$ . Then  $Q_i^\sigma \neq Q$  for every  $\sigma \in G$ . By Lemma 10.5(i),  $\alpha Q^{-1} + \prod_{\sigma \in G} Q_i^\sigma = J_K$  for some  $\alpha \in K^\times$ . Then  $\alpha \in Q$  and  $\alpha J_K = \alpha Q^{-1} Q$ , so that  $\alpha J_K$  is prime to  $\prod_{\sigma \in G} Q_i^\sigma$ . On the other hand,  $N_{K/F}(\alpha) \in Q \cap J_F = P \subset Q_i$ , a contradiction. Thus  $Q_i = Q^\sigma$  for some  $\sigma \in G$ . Then we easily see that the  $Q^\sigma$  for all  $\sigma \in G$  coincide with the  $Q_i$  repeated  $[Z : 1]$  times. Thus  $d = g[Z : 1]$ . Clearly  $e(Q^\sigma/P) = e$  and  $f(Q^\sigma/P) = f$  for every  $\sigma \in G$ , and hence we obtain (4) and (3). By (13.2), we obtain  $d = efg$ , so that  $[Z : 1] = ef$  and  $g = [G : Z]$ .

The group  $Z$  is called **the decomposition group of  $Q$**  (relative to  $F$ ). We write  $Z = Z(Q/P)$ . Clearly  $\sigma^{-1}Z(Q/P)\sigma = Z(Q^\sigma/P)$  for every  $\sigma \in G$ .

**Lemma 16.2.** *The notation being as in Theorem 16.1, put*

$$M = \{a \in K \mid a^\sigma = a \text{ for every } \sigma \in Z\}, \quad R = Q \cap M.$$

*Then  $e(Q/R) = e(Q/P)$ ,  $f(Q/R) = f(Q/P)$ ,  $e(R/P) = f(R/P) = 1$ , and  $RJ_K = Q^e$ .*

PROOF. Since  $Z = \text{Gal}(K/M)$ , the decomposition group of  $Q$  relative to  $M$  is the whole  $Z$ . Applying Theorem 16.1(2) to  $K/M$  instead of  $K/F$ ,

we find that  $e(Q/R)f(Q/R) = [Z : 1] = e(Q/P)f(Q/P)$ . Since  $e(Q/P) = e(Q/R)e(R/P)$  and  $f(Q/P) = f(Q/R)f(R/P)$ , we obtain our assertions.

**Lemma 16.3.** *The notation being as above, let  $k_Q = J_K/Q$  and  $k_P = J_F/P$ . To each  $\sigma \in Z$  assign its natural action on  $k_Q$ . Then we obtain a surjective homomorphism of  $Z$  onto  $\text{Gal}(k_Q/k_P)$ .*

PROOF. The only point is the surjectivity. Take  $\theta \in J_K$  so that  $k_Q = k_P(\bar{\theta})$ , where  $\bar{a}$  denotes the class of  $a \pmod{Q}$ . Put  $h(x) = \prod_{\sigma \in Z} (x - \theta^\sigma)$ . Then  $h \in J_M[x]$ . Since  $f(R/P) = 1$ , we have  $k_R = k_P$ , and so  $\bar{h}$  has coefficients in  $k_P$ . Now  $\bar{h}(\bar{\theta}) = \bar{h}(\bar{\theta}) = 0$ , and so  $\bar{h}(\bar{\theta}^\tau) = 0$  for every  $\tau \in \text{Gal}(k_Q/k_P)$ . Since  $\bar{h}(x) = \prod_{\sigma \in Z} (x - \bar{\theta}^\sigma)$ , we have  $\bar{\theta}^\tau = \bar{\theta}^\sigma$  for some  $\sigma \in Z$ , which proves the surjectivity.

**Lemma 16.4.** *The notation being as above, put*

$$T = \{\sigma \in Z \mid a^\sigma - a \in Q \text{ for every } a \in J_K\}.$$

*Then  $[T : 1] = e$ ,  $[Z : T] = f$ ,  $T$  is normal in  $Z$ ,  $Z/T$  is cyclic, and the homomorphism of Lemma 16.3 gives an isomorphism of  $Z/T$  onto  $\text{Gal}(k_Q/k_P)$ .*

PROOF. The last assertion is clear, since  $T$  is the kernel of the homomorphism of Lemma 16.3. Thus  $[Z : T] = [\text{Gal}(k_Q/k_P) : 1] = f$ , so that  $[T : 1] = [Z : 1]/[Z : T] = e$ . Also,  $Z/T$ , being isomorphic to  $\text{Gal}(k_Q/k_P)$ , must be cyclic.

The group  $T$  is called **the inertia group of  $Q$**  (relative to  $F$ ). We write  $T = T(Q/P)$ . Clearly  $\alpha^{-1}T(Q/P)\alpha = T(Q^\alpha/P)$  for every  $\alpha \in G$ .

**Lemma 16.5.** *The notation being as above, put*

$$L = \{a \in K \mid a^\sigma = a \text{ for every } \sigma \in T\}, \quad S = Q \cap L.$$

*Then  $RJ_L = S$ ,  $SJ_K = Q^e$ , and  $f(Q/S) = 1$ .*

PROOF. Apply Lemma 16.4 to the extension  $K/L$ . Then  $T = \text{Gal}(K/L)$  and  $T$  is the decomposition group and also the inertia group of  $Q$  relative to  $L$ . Therefore we easily obtain our assertions.

Notice that  $L$  is a Galois extension of  $M$ , but  $L$  and/or  $M$  may or may not be normal over  $F$ . The decomposition of the type  $PJ_M = R_1 \cdots R_g$  in  $M$  can happen in some cases, but is false in general.

**16.6.** Since  $k_P$  is a finite field with  $N(P)$  elements,  $\text{Gal}(k_Q/k_P)$  is cyclic, and generated by the automorphism  $x \mapsto x^{N(P)}$ . Therefore Lemma 16.3 guarantees an element  $\varphi$  of  $Z$  such that

$$(16.1) \quad a^\varphi \equiv a^{N(P)} \pmod{Q} \text{ for every } a \in J_K.$$

Such a  $\varphi$  is called a **Frobenius automorphism of  $K$  at  $Q$** . Notice that  $Z/T$  is cyclic and generated by  $\varphi T$ . The coset  $\varphi T$  is uniquely determined; in particular, if  $T = \{1\}$  (which is the case if and only if  $P$  is unramified in  $K$ ), then  $\varphi$  is uniquely determined by  $Q$ . In such a case, we can speak of **the** Frobenius automorphism at  $Q$ , and we put

$$(16.2) \quad \varphi = \left[ \frac{K/F}{Q} \right].$$

Then  $\varphi$  has order  $f$ , and for every  $\alpha \in G$  we have

$$(16.3) \quad \left[ \frac{K/F}{Q^\alpha} \right] = \alpha^{-1} \left[ \frac{K/F}{Q} \right] \alpha.$$

Notice that  $f$  is the order of an element of  $G$ . This is a nontrivial condition on  $f$ . For example, if  $\text{Gal}(K/F)$  is a noncyclic group of order 4, we have  $f(Q/P) \leq 2$ . On the other hand, if  $\text{Gal}(K/F)$  is cyclic of order  $d$ , then  $f(Q/P) = d$  can happen.

**16.7.** The above discussion is applicable to the local case. Indeed, let  $K$  be a Galois extension of a local field  $F$  in the sense of §14.1; let  $P = Q \cap F$  with a prime ideal  $Q$  in  $K$ . Theorem 16.1, as well as the symbols  $Z$  and  $T$ , is meaningful. However, since  $Q$  is unique for  $P$  in this case, we have  $G = Z$  and  $g = 1$ . Thus  $M = F$  and  $PJ_K = Q^e$ .

**16.8.** Let us now take our setting to be that of §§13.3 and 13.4, assuming that  $K$  is a Galois extension of  $F$ . Identify  $F_P$  with the closure of  $F$  in  $K_Q$ . Then we easily see that  $K_Q$  is the composite of  $K$  and  $F_P$ , and  $K_Q$  is a Galois extension of  $F_P$ ; moreover  $\text{Gal}(K_Q/F_P)$  is canonically isomorphic to  $\text{Gal}(K/(K \cap F_P))$ . Define  $M$  and  $R$  as in Lemma 16.2; let  $M^*$  be the closure of  $M$  in  $K_Q$ . Then  $M^*$  can be identified with the  $R$ -completion of  $M$ . Since  $e(R/P) = f(R/P) = 1$ , we have  $M^* = F_P$ . Thus  $M \subset K \cap F_P$ . On the other hand,  $[K : M] = ef = [K_Q : F_P] = [K : K \cap F_P]$ . Therefore  $M = K \cap F_P$ .

**Theorem 16.9.** *Let the notation be as in Theorem 16.1 and the above lemmas. Let  $E$  be a subfield of  $K$  containing  $F$  and let  $H = \text{Gal}(K/E)$ . Then  $Z\sigma H \mapsto Q^\sigma \cap E$  gives a bijection of  $Z \backslash G/H$  onto the set of all the prime factors of  $P$  in  $E$ . Moreover,  $Z(Q^\sigma/(Q^\sigma \cap E)) = \sigma^{-1}Z\sigma \cap H$ ,  $T(Q^\sigma/(Q^\sigma \cap E)) = \sigma^{-1}T\sigma \cap H$ , and*

$$e((Q^\sigma \cap E)/P) = [\sigma^{-1}T\sigma : \sigma^{-1}T\sigma \cap H] = [T : T \cap \sigma H \sigma^{-1}],$$

$$e((Q^\sigma \cap E)/P)f((Q^\sigma \cap E)/P) = [\sigma^{-1}Z\sigma : \sigma^{-1}Z\sigma \cap H] = [Z : Z \cap \sigma H \sigma^{-1}].$$

**PROOF.** Clearly  $Q^\sigma \cap E$  is a prime ideal in  $E$  dividing  $P$ . Let  $A$  be a prime factor of  $P$  in  $E$ . By Theorem 16.1(1),  $A \subset Q^\sigma$  for some  $\sigma \in G$ , and so  $A = Q^\sigma \cap E$ . Suppose  $Q^\sigma \cap E = Q^\tau \cap E$ . By Theorem 16.1(1) with  $E$  as  $F$ , we have  $Q^\sigma = Q^{\tau\alpha}$  for some  $\alpha \in H$ . Then  $\tau\alpha\sigma^{-1} \in Z$ , so that  $\tau \in Z\sigma H$ .

Conversely, if  $\tau = \zeta\sigma\beta$  with  $\beta \in H$  and  $\zeta \in Z$ , then  $Q^{\tau\beta^{-1}} = Q^{\zeta\sigma} = Q^\sigma$ , and so  $Q^\sigma \cap E = Q^{\tau\beta^{-1}} \cap E = (Q^\tau \cap E)^{\beta^{-1}} = Q^\tau \cap E$ . This proves the first assertion. The remaining part follows easily from the definition of  $Z$  and  $T$ .

**Corollary 16.10.** *Let the notation be as in Theorem 16.9. Then we have  $e((Q \cap E)/P) = 1$  if and only if  $E \subset L$ ;  $e((Q \cap E)/P) = f((Q \cap E)/P) = 1$  if and only if  $E \subset M$ .*

This follows immediately from the above theorem.

**16.11.** Let us now assume that  $G$  is abelian, in which case we say that  $K$  is abelian over  $F$ . Then  $M$  is a Galois extension of  $F$ , and hence taking  $M$  to be  $K$  in Theorem 16.1(3), we obtain  $PJ_M = R_1 \cdots R_g$ . If we take  $E$  to be  $M$  in Theorem 16.9, then we can put  $R_i = Q_i \cap M$ , and so  $R_i J_K = Q_i^e$ . Assume that  $e = 1$ . Then, by (16.3) we have  $\left[\frac{K/F}{Q^\alpha}\right] = \left[\frac{K/F}{Q}\right]$  for every  $\alpha \in G$ . Thus the Frobenius automorphism in question depends only on  $P$ , and not on the choice of its prime factor in  $K$ . Therefore we denote it by  $\left(\frac{K/F}{P}\right)$ . Since  $PJ_K = \bigcap_{\sigma \in G} Q^\sigma$ , from (16.1) we obtain, for  $\varphi = \left(\frac{K/F}{P}\right)$ ,

$$(16.4) \quad a^\varphi \equiv a^{N(P)} \pmod{PJ_K} \quad \text{for every } a \in J_K.$$

Let  $\mathcal{J}_{K/F}$  be the group of all the fractional ideals in  $F$  not involving prime ideals ramified in  $K$ . For  $X \in \mathcal{J}_{K/F}$  we take its prime decomposition  $X = \prod_P P^{a(P)}$  with  $P$  unramified in  $K$  and  $a(P) \in \mathbf{Z}$ . Then we put

$$(16.5) \quad \left(\frac{K/F}{X}\right) = \prod_P \left(\frac{K/F}{P}\right)^{a(P)}.$$

Clearly  $X \mapsto \left(\frac{K/F}{X}\right)$  is a homomorphism of  $\mathcal{J}_{K/F}$  into  $\text{Gal}(K/F)$ . Though we will not discuss class field theory in this book, we note at least one of its basic facts: *the map  $X \mapsto \left(\frac{K/F}{X}\right)$  is surjective.*

**Lemma 16.12.** *Let  $K$  be a finite abelian extension of  $F$  as above, and  $M$  a subfield of  $K$  containing  $F$ . Let  $P$  be a prime ideal in  $F$  unramified in  $K$ . Then  $\left(\frac{K/F}{P}\right)$  restricted to  $M$  gives  $\left(\frac{M/F}{P}\right)$ .*

This follows immediately from (16.4).

**Exercises. 1.** Let  $M$  be a finite extension of  $F$ , and  $K$  the smallest Galois extension of  $F$  containing  $M$ . Prove: (i) a prime of  $F$  is ramified in  $K$  if and only if it is ramified in  $M$ ; (ii) a prime of  $F$  decomposes completely in  $M$  if and only if it decomposes completely in  $K$ .

**2.** Let  $K$  be a cyclic extension of  $F$  of degree  $q^m$ ,  $m > 1$ , with a prime number  $q$ , and  $M$  a proper subfield of  $K$  containing  $F$ . Prove that a prime of  $M$  ramified over  $F$  is ramified in  $K$ .

**3.** Enumerate all possible types of prime decomposition in  $\mathbf{Q}(\sqrt{3}, \sqrt{-5})$  and give an example of a prime for each type.

**4.** Do the same for  $\mathbf{Q}(p^{1/5}, e^{2\pi i/5})$  with a rational prime  $p \neq 5$ ,  $p^4 \not\equiv 1 \pmod{25}$ .

**5.** Let  $K$  and  $K'$  be Galois extensions of  $F$  contained in an extension of  $F$  such that  $K \cap K' = F$ . Let  $P = Q \cap K$  and  $P' = Q \cap K'$  with a prime ideal  $Q$  in  $KK'$ . Prove:

(i) If both  $P$  and  $P'$  are unramified over  $F$ , then  $Q$  is unramified over  $F$ .

(ii) If  $Q$  is unramified over  $F$ , then  $\left[ \frac{KK'/F}{Q} \right] = \left[ \frac{K/F}{P} \right] \left[ \frac{K'/F}{P'} \right]$  under suitable identification of Galois groups.

**6.** Let  $K$  be a Galois extension of  $F$  such that  $\text{Gal}(K/F)$  is isomorphic to  $S_n$ ,  $n > 2$ ; let  $L$  and  $M$  be the subfields of  $K$  corresponding to  $S_{n-1}$  and  $A_n$ , respectively. Prove that if  $D(L/F)$  is square-free and divides  $D(M/F)$ , then every prime ideal of  $M$  is unramified in  $K$ . (This gives an example of a nonsolvable unramified extension.)

## 17. Cyclotomic fields

In the following we work within  $\overline{\mathbf{Q}}$ , and denote by  $\zeta$  a primitive  $m$ -th root of unity contained in  $\overline{\mathbf{Q}}$  with an integer  $m > 1$ .

**Lemma 17.1.** *Let  $\mathcal{P}_n = \mathcal{P}(n)$  be the set of all primitive  $n$ -th roots of unity; put  $g(x; n) = \prod_{\xi \in \mathcal{P}_n} (x - \xi)$ . Then,  $g$  has coefficients in  $\mathbf{Z}$ , and for  $1 \leq n \in \mathbf{Z}$ ,  $1 \leq r \in \mathbf{Z}$ , and a prime number  $\ell$  not dividing  $n$ , we have*

$$g(x; n\ell^r) = g(x^{\ell^r}; n)/g(x^{\ell^{r-1}}; n).$$

PROOF. The first assertion is easy. Clearly

$$g(x^{\ell^r}; n) = \prod_{\xi \in \mathcal{P}_n} (x^{\ell^r} - \xi) = \prod_{\eta} (x - \eta),$$

where  $\eta$  runs over the set  $\mathcal{Y}(\ell^r, n)$  of all numbers such that  $\eta^{\ell^r} \in \mathcal{P}_n$ . Observing that  $\mathcal{P}(n\ell^r)$  is the set of all  $\eta \in \mathcal{Y}(\ell^r, n)$  not belonging to  $\mathcal{Y}(\ell^{r-1}, n)$ , we obtain our assertion.

**Lemma 17.2.** (1) *If  $\zeta'$  is another primitive  $m$ -th root of unity, then  $(1 - \zeta')/(1 - \zeta)$  is a unit.*

(2) *If  $m$  has two different prime factors, then  $1 - \zeta$  is a unit.*

(3)  *$1 + \zeta$  is a unit if  $m$  is odd.*



PROOF. Since  $\zeta' = \zeta^a$  with some  $a \in \mathbf{Z}$ , we see that  $(1 - \zeta')/(1 - \zeta)$  is an algebraic integer. Exchanging  $\zeta'$  for  $\zeta$ , we obtain (1). Next, Lemma 17.1 shows that  $g(1, m) = 1$  if  $m$  has two different prime factors, which proves (2). Finally, if  $m$  is odd, then  $-\zeta$  is of order  $2m$ , and so (3) follows from (2).

**Theorem 17.3.** *Suppose that  $m$  is odd or  $4|m$ . Then a prime number  $p$  is ramified in  $\mathbf{Q}(\zeta)$  if and only if  $p|m$ .*

PROOF. Let  $K = \mathbf{Q}(\zeta)$  and let  $f(x)$  be the minimal polynomial for  $\zeta$  over  $\mathbf{Q}$ . Then  $\delta_{K/\mathbf{Q}}(\zeta) = \prod(\zeta - \xi)$ , where  $\xi$  runs over the roots of  $f$  other than  $\zeta$ . Let  $d = \deg(f)$ . Then the product can be written  $\zeta^d \prod(1 - \zeta^{-1}\xi)$ , which divides  $\prod_{\eta}(1 - \eta)$ , where  $\eta$  runs over all the roots of  $(x^m - 1)/(x - 1)$ . Since the last quotient takes the value  $m$  for  $x = 1$ , we can conclude that  $\delta_{K/\mathbf{Q}}(\zeta)$  divides  $m$ , and so  $d(K/\mathbf{Q}) \supset mJ_K$  by Theorem 14.4. Thus, by Theorem 14.10,  $p$  is unramified in  $K$  if  $p \nmid m$ . (Up to this point everything is all right for any  $m > 1$ .) The converse part will be proven after the proof of Theorem 17.5.

**Theorem 17.4.** *Let  $\varphi$  be Euler's function of §2.1. Then  $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(m)$ ,  $g(x; m)$  is irreducible, and  $\text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$  is isomorphic to  $(\mathbf{Z}/m\mathbf{Z})^\times$ . Moreover, for a prime number  $p$  that does not divide  $m$  let  $f$  be the order of  $p \pmod{m}$  in  $(\mathbf{Z}/m\mathbf{Z})^\times$  and let  $g = \varphi(m)/f$ . Then  $pJ_K = Q_1 \cdots Q_g$  with  $g$  different prime ideals  $Q_i$  in  $K$  such that  $N(Q_i) = p^f$ .*

PROOF. Let  $K = \mathbf{Q}(\zeta)$  and  $G = \text{Gal}(K/\mathbf{Q})$ . To each  $\sigma \in G$  take an integer  $a \in \mathbf{Z}$  such that  $\zeta^\sigma = \zeta^a$ . Then we easily see that  $\sigma \mapsto a \pmod{m}$  defines an injective homomorphism of  $G$  into  $(\mathbf{Z}/m\mathbf{Z})^\times$ . Therefore  $K$  is abelian over  $\mathbf{Q}$ . Take a prime number  $p$  not dividing  $m$ , and put  $\sigma = \left(\frac{K/\mathbf{Q}}{p\mathbf{Z}}\right)$ . This is meaningful since  $p$  is unramified in  $K$ . Then  $\zeta^\sigma - \zeta^p \in pJ_K$  by (16.4). Suppose  $\zeta^\sigma \neq \zeta^p$ . The proof of Lemma 17.3 shows that  $\zeta^\sigma - \zeta^p$  divides  $m$ , and hence  $p|m$ , a contradiction. Thus  $\zeta^\sigma = \zeta^p$ . Now take any positive integer  $b$  prime to  $m$ . Since  $b$  is the product of some primes not dividing  $m$ , we can find an element  $\tau$  of  $G$  such that  $\zeta^\tau = \zeta^b$ . Thus our assertion concerning  $\text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$  follows easily from this fact. Also we find that

$$(17.1) \quad \zeta^\tau = \zeta^b \quad \text{if} \quad \tau = \left(\frac{\mathbf{Q}(\zeta)/\mathbf{Q}}{b\mathbf{Z}}\right) \quad \text{and} \quad 0 < b \in \mathbf{Z}, \quad (b, m) = 1.$$

This means that the inverse map of the homomorphism  $\sigma \mapsto a \pmod{m}$  can be obtained by  $a \mapsto \left(\frac{\mathbf{Q}(\zeta)/\mathbf{Q}}{a\mathbf{Z}}\right)$  for  $0 < a \in \mathbf{Z}$ . Thus, if  $p \pmod{m}$  has order  $f$  in  $(\mathbf{Z}/m\mathbf{Z})^\times$ , then  $\left(\frac{\mathbf{Q}(\zeta)/\mathbf{Q}}{p\mathbf{Z}}\right)$  has order  $f$ , which must be the residue class degree as noted in §16.6. Therefore we obtain the last assertion of our theorem.

**Theorem 17.5.** *Suppose  $m = \ell^r$  with a prime number  $\ell$  and  $0 < r \in \mathbf{Z}$ ; assume  $r > 1$  if  $\ell = 2$ ; put  $K = \mathbf{Q}(\zeta)$ . Then  $(1 - \zeta)J_K$  is a prime ideal in  $K$ ,  $\ell J_K = (1 - \zeta)^d J_K$ ,  $d(K/\mathbf{Q}) = \delta_{K/\mathbf{Q}}(\zeta)J_K = (1 - \zeta)^e J_K$ , and  $|D_K| = \ell^e$ , where  $d = \varphi(\ell^r) = [K : \mathbf{Q}]$  and  $e = r\ell^r - \ell^{r-1}(r + 1)$ . Thus  $\ell$  is completely ramified in  $K$ .*

PROOF. Put  $g(x) = g(x; \ell^r)$ . Taking  $n = 1$  in Lemma 17.1, we obtain  $g(x) = (x^{\ell^r} - 1)/(x^{\ell^{r-1}} - 1) = \sum_{\nu=0}^{\ell-1} x^{\nu\ell^{r-1}}$ , and so

$$\prod_{\xi \in \mathcal{P}(\ell^r)} (1 - \xi) = g(1) = \ell.$$

Put  $R = (1 - \zeta)J_K$ . By lemma 17.2(1),  $R = (1 - \xi)J_K$  for every  $\xi \in \mathcal{P}(\ell^r)$ , so that  $R^d = \ell J_K$ . Therefore  $R$  must be a prime ideal and  $1 - \zeta$  is a prime element, and so “the  $R$ -part” of  $d(K/\mathbf{Q})$  is  $\delta_{K/\mathbf{Q}}(1 - \zeta)J_K$ . Since  $d(K/\mathbf{Q})$  involves no other primes and  $\delta_{K/\mathbf{Q}}(\zeta - 1) = \delta_{K/\mathbf{Q}}(\zeta)$ , we obtain  $d(K/\mathbf{Q}) = \delta_{K/\mathbf{Q}}(\zeta)J_K = g'(\zeta)J_K$ . Now  $g'(\zeta)(\zeta^{\ell^{r-1}} - 1) = \ell^r \zeta^{\ell^{r-1}}$ . Since  $\zeta^{\ell^{r-1}} \in \mathcal{P}(\ell)$ , we have  $(\zeta^{\ell^{r-1}} - 1)J_K = R^{\ell^{r-1}}$ , and so  $g'(\zeta)J_K = R^e$  with  $e = rd - \ell^{r-1}$ . Thus we obtain all the formulas stated in our theorem.

Let us now prove the “if”-part of Theorem 17.3. Denote by  $K(m)$  the field  $\mathbf{Q}(\zeta)$ . We can put  $m = m_1 \cdots m_s$ , where each  $m_i$  is a prime power  $\ell^r$  as above; put  $K_i = K(m_i)$ . Then  $K(m)$  is the composite of  $K_1, \dots, K_s$ . If  $p|m$ , then  $p|m_i$  for some  $i$ . The above theorem shows that  $p$  is completely ramified in  $K_i$ , and hence is ramified in  $K(m)$ .

**Theorem 17.6.** *If  $K = \mathbf{Q}(\zeta)$  with a primitive  $m$ -th root of unity  $\zeta$ , then  $J_K = \mathbf{Z}[\zeta]$ .*

PROOF. If  $2|m$  and  $4 \nmid m$ , then  $-\zeta^2$  is of order  $m$  and  $\mathbf{Z}[\zeta] = \mathbf{Z}[\zeta^2]$ . Therefore changing  $(\zeta, m)$  for  $(\zeta^2, m/2)$  in such a case, we may assume that  $m$  is odd or  $4|m$ . Take  $m_i$  and  $K_i$  as above. We prove our theorem by induction on  $s$ . If  $s = 1$ , our assertion follows from Theorem 17.5 and Corollary 14.5. Let  $L = K_2 \cdots K_s$  and  $\xi = \zeta^{m_1}$ . We assume  $J_L = \mathbf{Z}[\xi]$  by induction. Now  $d(K_1 L/L) = d(K_1/\mathbf{Q})J_K$  by Exercise 4 at the end of Section 14. This equals  $\delta_{K_1/\mathbf{Q}}(\zeta_1)J_K$ , where  $\zeta_1$  is a primitive  $m_1$ -th root of unity. Since no prime is ramified in  $K_1 \cap L$ , we have  $K_1 \cap L = \mathbf{Q}$ , and hence  $\delta_{K_1/\mathbf{Q}}(\zeta_1) = \delta_{K/L}(\zeta_1)$ . Therefore  $J_K = J_L[\zeta_1]$  by Corollary 14.5, and so  $J_K = \mathbf{Z}[\xi][\zeta_1] \subset \mathbf{Z}[\zeta]$ , which completes the proof.

**17.7.** Theorem 17.4 shows that the prime decomposition of  $p$  in  $\mathbf{Q}(\zeta)$  is determined by  $p \pmod{m}$ . The same idea works for quadratic fields. Given a square-free integer  $m \neq 1$ , Put  $c = |m|$  if  $m - 1 \in 4\mathbf{Z}$  and  $c = 4|m|$  if  $m - 1 \notin 4\mathbf{Z}$ . Let  $\chi$  be the real primitive character modulo  $c$  of Theorem 3.7; put  $\tau = \tau(\chi)$ . By (3.8b), we have  $\tau^2 = \chi(-1)c$ . Since  $\chi(-1)c$  is  $m$  or  $4m$  as

shown in the proof of that theorem, we have  $\mathbf{Q}(\sqrt{m}) = \mathbf{Q}(\tau) \subset \mathbf{Q}(\zeta)$ , where  $\zeta = \mathbf{e}(1/c)$ . Let  $G = \text{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ ,  $F = \mathbf{Q}(\sqrt{m})$ , and  $H = \text{Gal}(\mathbf{Q}(\zeta)/F)$ . Then  $G/H = \text{Gal}(F/\mathbf{Q})$ . Let  $\sigma = \left(\frac{\mathbf{Q}(\zeta)/\mathbf{Q}}{p\mathbf{Z}}\right)$  with a prime number  $p$  prime to  $c$ . Then  $\zeta^\sigma = \zeta^p$  by (17.1), and so  $\tau^\sigma = \sum_{a=1}^c \chi(a)\zeta^{ap} = \chi(p)\tau$  by (3.8a). Now by Lemma 16.12,  $\sigma$  gives  $\left(\frac{F/\mathbf{Q}}{p\mathbf{Z}}\right)$ , and so  $\left(\frac{F/\mathbf{Q}}{p\mathbf{Z}}\right) = 1$  if and only if  $\chi(p) = 1$ . Since  $\left(\frac{F/\mathbf{Q}}{p\mathbf{Z}}\right) = 1$  if and only if  $p$  splits into the product of two prime ideals in  $F$ , from (10.13) we obtain  $\chi(p) = \left(\frac{m}{p}\right)$  for odd  $p$ . This gives a conceptual interpretation of Theorem 3.7. The crucial point is that  $\mathbf{Q}(\sqrt{m}) \subset \mathbf{Q}(\zeta)$ . Suppose  $m - 1 \in 4\mathbf{Z}$ ; then we can consider  $\sigma = \left(\frac{F/\mathbf{Q}}{2\mathbf{Z}}\right)$  and obtain  $\tau^\sigma = \chi(2)\tau$ . Thus the behavior of the prime 2 in  $F$  is determined by  $\chi(2)$ , as stated in (10.15).

It should also be noted that the proof of Theorem 3.4 is essentially the same as what we are explaining here, except that the Frobenius automorphism does not appear explicitly there.

The same method is applicable to other subfields of  $\mathbf{Q}(\zeta)$ :  $\mathbf{Q}(\zeta + \zeta^{-1})$ , for example. But we leave the details of the discussion in this case to the reader.

## ALGEBRAS OVER A FIELD

## 18. Semisimple and simple algebras

**18.1.** Let us first recall the notion of an algebra over a field that we introduced in §11.1. By an **algebra** over a field  $F$ , or simply by an  **$F$ -algebra**, we understand an associative ring  $A$  which is also a vector space over  $F$  such that  $(ax)(by) = abxy$  for  $a, b \in F$  and  $x, y \in A$ . If  $A$  has an identity element, we denote it by  $1_A$ , or simply by  $1$ . Identifying  $a$  with  $a1_A$  for every  $a \in F$ , we can view  $F$  as a subring of  $A$ . In such a case the identity element of  $F$  can be identified with  $1_A$ , and we denote it simply by  $1$ . An  $F$ -algebra  $A$  with identity element is called a **division algebra** if every nonzero element of  $A$  is invertible. For example,  $F$  itself is a division algebra. A subring of  $A$  that is a vector subspace of  $A$  over  $F$  is called a **subalgebra**. In this book we always assume that *an  $F$ -algebra is of finite dimension over  $F$  unless otherwise stated*. In fact, an arbitrary field extension of  $F$  is an  $F$ -algebra, and such will be the only type of  $F$ -algebra we need in this book that is not necessarily of finite dimension over  $F$ .

Hereafter in this section  $A$  denotes an  $F$ -algebra with identity element. Let  $W$  be a right or left  $A$ -module. Since  $F \subset A$ ,  $W$  is a vector space over  $F$ . Clearly  $W$  is finite-dimensional over  $F$  if and only if  $W$  is finitely generated over  $A$ .

Given a right or left  $A$ -module  $W$ , we denote by  $\text{End}_A(W)$  the ring consisting of all  $A$ -endomorphisms of  $W$  into itself. Clearly  $\text{End}_A(W)$  is an  $F$ -algebra, provided  $W$  is finitely generated over  $A$ . We can view  $A$  as a right  $A$ -module by right multiplication. We will often denote this right  $A$ -module by  $A_{[r]}$ . For every  $a \in A$  left multiplication by  $a$  defines an element of  $\text{End}_A(A_{[r]})$ . Conversely, given  $f \in \text{End}_A(A_{[r]})$ , put  $a = f(1)$ . Then for  $x \in A_{[r]}$  we have  $f(x) = f(1)x = ax$ . This means that  $\text{End}_A(A_{[r]})$  consists of the endomorphisms obtained from left multiplication by the elements of  $A$ , and we easily see that  $\text{End}_A(A_{[r]})$  is isomorphic to  $A$ .

We call a right  $A$ -module  $V$  **irreducible** if  $V \neq \{0\}$  and  $V$  has no nontrivial  $A$ -submodule other than  $V$  itself. Take a nonzero element  $x$  of such a  $V$ . Since  $xA$  is an  $A$ -submodule of  $V$  other than  $\{0\}$ , we have  $V = xA$ . We can similarly

discuss an irreducible left  $A$ -module. Thus a right or left irreducible  $A$ -module is of finite dimension over  $F$ .

**Lemma 18.2.** *Let  $V_1$  and  $V_2$  be irreducible right  $A$ -modules. Then an  $A$ -homomorphism of  $V_1$  into  $V_2$  is either 0 or a bijection.*

PROOF. Let  $\alpha$  be a nonzero  $A$ -homomorphism of  $V_1$  into  $V_2$ . Then  $\alpha(V_1)$  is an  $A$ -submodule of  $V_2$  other than  $\{0\}$ , and so  $\alpha(V_1) = V_2$ , as  $V_2$  is irreducible. Thus  $\alpha$  is surjective. Also,  $\text{Ker}(\alpha)$  is an  $A$ -submodule of  $V_1$ , which is different from  $V_1$ , as  $\alpha \neq 0$ , and so the irreducibility of  $V_1$  implies that  $\text{Ker}(\alpha) = \{0\}$ . Thus  $\alpha$  is injective. This proves our lemma.

**Lemma 18.3.** *If  $V$  is an irreducible right  $A$ -module, then  $\text{End}_A(V)$  is a division algebra.*

PROOF. We first observe that  $\text{End}_A(V) \neq \{0\}$ , as it contains the identity map of  $V$  onto itself, which is not 0. By Lemma 18.2, every nonzero element of  $\text{End}_A(V)$  is invertible, and so our lemma holds.

**Lemma 18.4.** *Let  $V$  be a right  $A$ -module such that  $V = \sum_{i \in I} W_i$  with a family of irreducible right  $A$ -modules  $\{W_i\}$  indexed by a finite set  $I$ . Given an  $A$ -submodule  $U$  of  $V$ , we can find a subset  $J$  of  $I$  such that  $V$  is the direct sum of  $U$  and the modules  $W_i$  for  $i \in J$ .*

PROOF. Take any subset  $J$  of  $I$  such that  $U$  and the modules  $W_i$  for  $i \in J$  form a direct sum. Denote that direct sum by  $X$ . If  $V = X$ , the matter is settled. Suppose  $V \neq X$ ; then  $W_k \not\subset X$  for some  $k \in I$ . Then  $W_k \cap X$  is an  $A$ -submodule of  $W_k$  different from  $W_k$ , and so  $W_k \cap X = \{0\}$ , as  $W_k$  is irreducible. Then  $X$  and  $W_k$  form a direct sum. Replacing  $J$  by  $J \cup \{k\}$ , repeat the same argument. Since  $V = \sum_{i \in I} W_i$  and  $I$  is finite, we eventually reach our desired conclusion.

**18.5.** Given a right  $A$ -module  $V$ , put  $B = \text{End}_A(V)$  and  $C = \text{End}_B(V)$ . We write the action of the elements of  $B$  on  $V$  always on the left, and the action of those of  $C$  on the right. Thus, for  $\beta \in B$ ,  $\gamma \in C$ , and  $x \in V$ , the image of  $x$  under  $\beta$  is written  $\beta x$ , and the image of  $x$  under  $\gamma$  is  $x\gamma$ . Put

$$(18.1) \quad Y = \{\alpha \in A \mid V\alpha = 0\}.$$

It can easily be seen that  $Y$  is a two-sided ideal of  $A$ . Then  $A/Y$  has a structure of an  $F$ -algebra and  $V$  can be viewed as a right  $A/Y$ -module, or rather  $A/Y$  can be viewed as a subalgebra of  $C$ . Consequently every  $C$ -submodule of  $V$  is an  $A$ -submodule. Notice that  $B = \text{End}_C(V)$ . To prove this, let  $\alpha \in \text{End}_C(V)$ . Since  $A/Y \subset C$ , we have  $\alpha \in \text{End}_A(V) = B$ . On the other hand,  $C = \text{End}_B(V)$ , and so  $B \subset \text{End}_C(V)$ , which proves the desired fact.

We call a right  $A$ -module  $V$  **completely reducible** if  $V$  is the sum of finitely many irreducible right  $A$ -modules. We include  $\{0\}$  in this class of modules.

**18.6.** An  $F$ -algebra  $A$  with identity element is called **right semisimple** (resp. **left semisimple**) if every right (resp. left)  $A$ -module is completely reducible. We will eventually show in Corollary 18.17 that  $A$  is right semisimple if and only if it is left semisimple. A right ideal of  $A$  can be viewed as a right  $A$ -module. It is called **minimal** if it is irreducible as a right  $A$ -module. In the following lemmas what we prove in terms of right  $A$ -modules and right ideals are valid also with the word *left* in place of *right*.

An  $F$ -algebra  $A$  with identity element is called **simple** if  $A$  has no two-sided ideal other than  $\{0\}$  and  $A$ .

**Lemma 18.7.** *An  $F$ -algebra  $A$  with identity element is right semisimple if  $A$  as a right  $A$ -module is completely reducible.*

PROOF. Suppose  $A$  is completely reducible. Let  $V$  be a right  $A$ -module. Take elements  $x_1, \dots, x_r$  of  $V$  so that  $V = x_1A + \dots + x_rA$ . Let  $X$  be the direct sum of  $r$  copies of  $A$  viewed as a right  $A$ -module. Clearly  $X$  is completely reducible. Define  $\varphi : X \rightarrow V$  by  $\varphi(a_1, \dots, a_r) = \sum_{i=1}^r x_i a_i$  for  $(a_1, \dots, a_r) \in X$  with  $a_i \in A$  and let  $N = \text{Ker}(\varphi)$ . Then  $N$  is an  $A$ -submodule of  $X$  and  $V$  is  $A$ -isomorphic to  $X/N$ . Applying Lemma 18.4 to  $X$  and  $N$ , we have  $X = N \oplus M$  with an  $A$ -submodule  $M$  of  $X$  that is completely reducible. Thus  $V$ , being isomorphic to  $M$ , is completely reducible, which proves our lemma.

**18.8.** Let  $V$  be a right  $A$ -module and  $W$  the direct sum of  $r$  copies of  $V$ . Then  $W$  consists of all  $(v_1, \dots, v_r)$  with  $v_i \in V$ . Let  $B = \text{End}_A(V)$ . We are going to show that  $\text{End}_A(W)$  is isomorphic to  $M_r(B)$ . For that purpose denote by  $\omega_i$  the map  $V \rightarrow W$  that identifies  $V$  with the  $i$ -th summand of  $W$ , and by  $\pi_i$  the map  $W \rightarrow V$  that is the projection to the  $i$ -th summand of  $W$ . Given  $\alpha \in \text{End}_A(W)$ , put  $\alpha_{ij} = \pi_i \circ \alpha \circ \omega_j$ . Then  $\alpha_{ij} \in B$ . We see that  $\alpha(0, \dots, 0, x_j, 0, \dots, 0) = (\alpha_{1j}x_j, \dots, \alpha_{rj}x_j)$ , and so  $\alpha(x_1, \dots, x_r) = (y_1, \dots, y_r)$  with  $y_i = \sum_{j=1}^r \alpha_{ij}x_j$ . Assigning the matrix  $(\alpha_{ij}) \in M_r(B)$  to  $\alpha$ , we easily see that  $\text{End}_A(W)$  is isomorphic to  $M_r(B)$ . For instance, since  $\text{id}_W = \sum_{k=1}^r \omega_k \circ \pi_k$ , for  $\alpha, \beta \in \text{End}_A(W)$  corresponding to  $(\alpha_{ij})$  and  $(\beta_{ij})$  we have

$$\begin{aligned} (\alpha\beta)_{ij} &= \pi_i \circ \alpha\beta \circ \omega_j = \pi_i \circ \alpha \circ \left(\sum_{k=1}^r \omega_k \circ \pi_k\right) \circ \beta \circ \omega_j \\ &= \sum_{k=1}^r \pi_i \circ \alpha \circ \omega_k \circ \pi_k \circ \beta \circ \omega_j = \sum_{k=1}^r \alpha_{ik} \circ \beta_{kj}. \end{aligned}$$

Also, given  $\alpha_{ij} \in B$ , put  $\gamma = \sum_{i,j=1}^r \omega_i \circ \alpha_{ij} \circ \pi_j$ . Then  $\pi_k \circ \gamma \circ \omega_\ell = \alpha_{k\ell}$ .

A special case of our setting is worthy of a separate statement as follows.

**Lemma 18.9.** *Let  $D$  be a division  $F$ -algebra and let  $D_r^1$  denote the set of all  $(1 \times r)$ -matrices  $[d_1 \ \cdots \ d_r]$  with  $d_i \in D$ , viewed as a left  $D$ -module. Then the following assertions hold.*

- (i) *Every (nontrivial) left  $D$ -module (which is finite-dimensional over  $F$  by our convention made in §18.1) is isomorphic to  $D_r^1$  for some  $r$ .*
- (ii) *Let  $A = M_r(D)$ , and let  $A$  act on  $D_r^1$  by right matrix multiplication. Then  $\text{End}_D(D_r^1) = A$  and  $\text{End}_A(D_r^1) = D$ .*
- (iii)  *$D_r^1$  is an irreducible right  $A$ -module.*

PROOF. Let  $V$  be a left  $D$ -module and let  $0 \neq y \in V$ . Then  $Dy$  is an irreducible left  $D$ -submodule of  $V$ . Indeed, if  $0 \neq z \in Dy$  we have  $z = dy$  with  $d \in D$ ,  $d \neq 0$ , and so  $Dz = Ddy = Dy$ , which proves the desired fact. Now  $V = Dx_1 + \cdots + Dx_s$  with some  $x_i \in V$ . Applying Lemma 18.4 to  $V$ , we find that  $V = De_1 \oplus \cdots \oplus De_r$  with a suitable subset  $\{e_1, \dots, e_r\}$  of  $\{x_1, \dots, x_s\}$ . Clearly  $[d_1 \ \cdots \ d_r] \mapsto \sum_{i=1}^r d_i e_i$  gives a  $D$ -isomorphism of  $D_r^1$  onto  $V$ . This proves (i). Though the equality  $\text{End}_D(D_r^1) = A$  of (ii) is a special case of what we did in §18.8, this case is much simpler. Indeed, given  $\alpha \in \text{End}_D(D_r^1)$ , let  $e_i \alpha = \sum_{j=1}^r a_{ij} e_j$  with  $a_{ij} \in D$ . Then  $(\sum_{i=1}^r d_i e_i) \alpha = \sum_{j=1}^r (\sum_{i=1}^r d_i a_{ij}) e_j$ , and so  $\alpha$  corresponds to right multiplication by the matrix  $[a_{ij}]$ , from which we easily obtain  $\text{End}_D(D_r^1) = A$ . To prove (iii), let  $0 \neq u_1 \in D_r^1$ . Then  $Du_1$  is an irreducible left  $D$ -module, and so by Lemma 18.4,  $D_r^1 = Du_1 \oplus \cdots \oplus Du_t$  with suitable  $u_2, \dots, u_t$ . Looking at the dimension of  $D_r^1$  over  $F$ , we find that  $t = r$ . For each  $i \leq r$  and  $0 \neq d \in D$  we can find an element  $\beta_i \in A$  such that  $u_1 \beta_i = de_i$ . Thus  $de_i \in u_1 A$ , and so  $D_r^1 = u_1 A$ , which proves (iii). Finally let  $E = \text{End}_A(D_r^1)$ . Let  $V_k$  be the subset of  $A$  consisting of the matrices whose  $j$ -th row is 0 if  $j \neq k$ . Then  $A = V_1 \oplus \cdots \oplus V_r$  and each  $V_i$  is isomorphic to  $D_r^1$ . Taking  $A$  to be  $W$  of §18.8, we obtain  $\text{End}_A(A_{[r]}) \cong M_r(E)$ . As noted in §18.1,  $A \cong \text{End}_A(A_{[r]})$ . Thus  $M_r(D) \cong M_r(E)$ . Clearly  $D \subset E$ , and so  $D = E$ , which completes the proof.

**Lemma 18.10.** *Let  $A$  be a right semisimple algebra and let  $A = \bigoplus_{i \in I} W_i$  with minimal right ideals  $W_i$  of  $A$  (see Lemma 18.7). Then every irreducible right  $A$ -module is isomorphic to  $W_i$  for some  $i$ .*

PROOF. Let  $V$  be an irreducible right  $A$ -module. Then  $V = xA$  with some  $x \in V$ , and the map  $a \mapsto xa$  for  $a \in A$  is an  $A$ -homomorphism of  $A$  onto  $V$ , whose kernel is  $\{a \in A \mid xa = 0\}$ . Denote this kernel by  $N$ . Then  $N$  is a right ideal of  $A$ . By Lemma 18.4,  $A = N \oplus M$ ,  $M = \bigoplus_{i \in J} W_i$  with a subset  $J$  of  $I$ . Then  $V \cong A/N \cong M$  and  $M = W_i$  for some  $i$ , as  $V$  is irreducible. This proves our lemma.

**Theorem 18.11.** *The following conditions on an  $F$ -algebra  $A$  with identity element are mutually equivalent:*

- (i)  $A$  is right semisimple and all irreducible right  $A$ -modules are isomorphic.
- (ii)  $A$  can be decomposed to a direct sum of finitely many minimal right ideals that are  $A$ -isomorphic to each other.
- (iii)  $A$  is isomorphic to a matrix algebra  $M_r(D)$  with a division algebra  $D$ .

PROOF. Let  $A = M_r(D)$  as in (iii). Define  $V_k$  as in the proof of Lemma 18.9. Clearly  $V_k$  is a right ideal of  $A$  isomorphic to  $D_r^1$ , which is an irreducible right  $A$ -module by Lemma 18.9(iii). Since  $A = V_1 \oplus \cdots \oplus V_r$ , this proves that (iii)  $\Rightarrow$  (ii). Clearly (i)  $\Rightarrow$  (ii). If we assume (ii), then  $A$  is right semisimple by Lemma 18.7, and (i) holds by Lemma 18.10. Suppose  $A_{[r]}$  is isomorphic to the direct sum of  $r$  copies of an irreducible right  $A$ -module  $V$ . Let  $D = \text{End}_A(V)$ . By Lemma 18.3,  $D$  is a division algebra. As shown in §18.8,  $\text{End}(A_{[r]}) \cong M_r(D)$ . Since  $A \cong \text{End}(A_{[r]})$  as noted in §18.1, this proves (ii)  $\Rightarrow$  (iii), and completes the proof.

**Theorem 18.12.** *An  $F$ -algebra  $A$  with identity element is simple if and only if  $A$  is isomorphic to a matrix algebra  $M_r(D)$  with a division algebra  $D$ . Moreover, the isomorphism class of  $D$  and  $r$  are determined by  $A$ .*

PROOF. Suppose  $A$  is simple, that is,  $A$  has no two-sided ideal other than  $\{0\}$  and  $A$  itself. Take a minimal right ideal  $R$  of  $A$ , and let  $E = \text{End}_A(R)$ . By Lemma 18.3,  $E$  is a division algebra. We can put  $R = Ee_1 \oplus \cdots \oplus Ee_r$  with some elements  $e_i$ . Let  $W$  be the direct sum of  $r$  copies of  $R$  and let  $g = (e_1, \dots, e_r) \in W$ . Consider the map  $\alpha \mapsto g\alpha$ , defined for  $\alpha \in A$ , of  $A$  into  $W$ . If  $g\alpha = 0$ , then  $e_i\alpha = 0$  for every  $i$ , and so  $R\alpha = \{0\}$ . All such  $\alpha$  form a two-sided ideal of  $A$ , which is clearly different from  $A$ , as we cannot have  $\alpha = 1$ . Thus  $g\alpha = 0$  only if  $\alpha = 0$ . Therefore our map gives an isomorphism of  $A_{[r]}$  onto the submodule  $gA$  of  $W$ . By Lemma 18.4,  $gA$  is isomorphic to the direct sum of  $s$  copies of  $R$  with an integer  $s \leq r$ . Thus  $A$  satisfies (ii) of Theorem 18.11, and (iii) of the same theorem shows that  $A$  is isomorphic to a matrix algebra over a division algebra. If  $A = M_r(D)$ , then by (ii) and (iii) of Lemma 18.9,  $D$  is determined as  $\text{End}_A(V)$  with an irreducible right  $A$ -module  $V$ , and  $V$  must be isomorphic to  $D_r^1$ . Thus  $D$  and  $r$  are determined by  $A$ . That  $M_r(D)$  for any division algebra  $D$  is simple can be shown by taking  $D$  to be  $Z$  of the following lemma.

**Lemma 18.13.** *Let  $Z$  be an associative ring with identity element, and let  $S = M_n(Z)$ . Then every two-sided ideal of  $S$  is of the form  $M_n(Y)$  with a two-sided ideal  $Y$  of  $Z$ .*

PROOF. For  $x = \sum_{i,j} a_{ij}e_{ij} \in M_n(Z)$  with  $a_{ij} \in Z$  and the standard matrix units  $e_{ij}$  write  $a_{ij} = p_{ij}(x)$ . Given a two-sided ideal  $X$  of  $S$ , put  $Y_{ij} = p_{ij}(X)$ . Since  $e_{ii}xe_{jj} = p_{ij}(x)e_{ij}$ , we see that  $Y_{ij}e_{ij} \subset X$ . Also, we have



$Y_{ij} = Y_{11}$  for all  $(i, j)$ , since  $e_{1i}e_{ij}e_{j1} = e_{11}$  and  $e_{i1}e_{11}e_{1j} = e_{ij}$ . Clearly  $Y_{11}$  is a two-sided ideal of  $Z$ , which proves our lemma.

**Lemma 18.14.** *Let  $A$  be a simple  $F$ -algebra. Then every two right  $A$ -modules of the same dimension over  $F$  are  $A$ -isomorphic.*

PROOF. This is because  $A$  has property (i) of Theorem 18.11.

**Lemma 18.15.** *Let  $A = M_r(D)$  with a division algebra  $D$ , and let  $e$  be a nonzero element of  $A$  such that  $e^2 = e$ . Then  $eAe \cong M_s(D)$  with  $0 < s \leq r$ .*

PROOF. Let  $V = D_r^1$ . Then  $D = \text{End}_A(V)$  and  $A = \text{End}_D(V)$  by Lemma 18.9(ii). Put  $f = 1 - e$ . Then  $ef = fe = 0$ ,  $f^2 = f$ , and  $V = Ve \oplus Vf$ . Clearly  $eAe \subset \text{End}_D(Ve)$ . Let  $\alpha \in \text{End}_D(Ve)$ . Define  $\beta \in \text{End}_F(V)$  by  $\beta = \alpha$  on  $Ve$  and  $\beta = 0$  on  $Vf$ . Then  $\beta \in \text{End}_D(V) = A$  and  $\alpha = e\beta e \in eAe$ . This proves that  $eAe = \text{End}_D(Ve)$ . By Lemma 18.9,  $\text{End}_D(Ve) \cong M_s(D)$  with  $s = [Ve : F]/[D : F]$ , which proves our lemma.

**Theorem 18.16.** *An  $F$ -algebra  $A$  with identity element is right semisimple if and only if  $A$  is a direct sum of a finite number of simple algebras.*

PROOF. Suppose  $A = A_1 \oplus \cdots \oplus A_s$  with simple algebras  $A_i$ . We can put  $A_i = \bigoplus_{j=1}^{r_i} N_{ij}$  with minimal right ideals  $N_{ij}$  of  $A_i$ . Since  $A_i A_k = \{0\}$  for  $i \neq k$ , we see that each  $N_{ij}$  is a right ideal of  $A$ , which is clearly minimal. We have  $A = \bigoplus_{i=1}^s (\bigoplus_{j=1}^{r_i} N_{ij})$ , and so by Lemma 18.7,  $A$  is right semisimple. Conversely suppose  $A$  is right semisimple. We can put  $A_{[r]} = \bigoplus_{i=1}^t W_i$ , where  $W_i$  is isomorphic to the direct sum of  $s_i$  copies of an irreducible right  $A$ -module  $V_i$  such that  $V_i$  is not isomorphic to  $V_k$  if  $i \neq k$ . By Lemma 18.2 every  $A$ -homomorphism of  $W_i$  into  $W_k$  is 0 if  $i \neq k$ . Therefore  $\text{End}_A(A_{[r]})$  can be identified with  $\bigoplus_{i=1}^t \text{End}_A(W_i)$ , and  $\text{End}_A(W_i) \cong M_{s_i}(D_i)$  with  $D_i = \text{End}_A(V_i)$ , as shown in §18.8. Since  $V_i$  is irreducible,  $D_i$  is a division algebra. We have seen in §18.1 that  $A \cong \text{End}_A(A_{[r]})$ , and so  $A \cong \bigoplus_{i=1}^t M_{s_i}(D_i)$ , which completes the proof.

**Corollary 18.17.** *An  $F$ -algebra  $A$  with identity element is right semisimple if and only if it is left semisimple.*

PROOF. Using the word *left* instead of *right*, we can show that  $A$  is a direct sum of a finite number of simple algebras if and only if  $A$  is left semisimple, and so we obtain our corollary.

Hereafter an algebra  $A$  is called **semisimple** if it is right or left semisimple. A simple  $F$ -algebra is commutative if and only if it is a finite algebraic extension of  $F$ , and therefore a semisimple  $F$ -algebra is commutative if and only if it is the direct sum of a finite number of finite algebraic extensions of  $F$ .

**Lemma 18.18.** (i) Let  $D$  be a division algebra over  $F$ . Given  $\alpha \in D$ , let  $F[\alpha]$  denote the set of all elements of  $D$  of the form  $c_0 + c_1\alpha + \cdots + c_n\alpha^n$  with  $c_i$  in  $F$  and  $0 \leq n \in \mathbf{Z}$ . Then  $F[\alpha]$  is a finite algebraic extension of  $F$ .

(ii) If  $F$  is an algebraically closed field, then  $F$  is the only division algebra over  $F$ .

(iii) If  $F$  is as in (ii), then every simple algebra over  $F$  is a matrix algebra  $M_n(F)$ .

PROOF. Let  $F[X]$  be the polynomial ring in one indeterminate  $X$  over  $F$ , and let  $I = \{g \in F[X] \mid g(\alpha) = 0\}$ . Then the map  $h(X) \mapsto h(\alpha)$  gives an isomorphism of  $F[X]/I$  onto  $F[\alpha]$ . Since  $D$  is a division ring and finite-dimensional over  $F$ , the ideal  $I$  must be a prime ideal other than  $\{0\}$ , and so  $F[\alpha]$  is a field. This proves (i). If  $F$  is algebraically closed, we have  $F[\alpha] = F$ , which means that  $D = F$ . This proves (ii). The last assertion follows from this combined with Theorem 18.12.

**18.19.** Let  $G$  be a finite group and  $F$  a field. We denote by  $F[G]$  the set of all formal sums  $\sum_{\gamma \in G} a_\gamma \gamma$  with  $a_\gamma \in F$ . This set has a structure of a vector space over  $F$  with respect to formal addition and multiplication by elements of  $F$ . We can make it an  $F$ -algebra by defining

$$\left(\sum_{\gamma \in G} a_\gamma \gamma\right) \left(\sum_{\delta \in G} b_\delta \delta\right) = \sum_{\gamma, \delta} a_\gamma b_\delta \gamma\delta = \sum_{\varepsilon \in G} c_\varepsilon \varepsilon \quad \text{with} \quad c_\varepsilon = \sum_{\gamma \in G} a_\gamma b_{\gamma^{-1}\varepsilon}.$$

This algebra is called the **group algebra** of  $G$  over  $F$ . In fact we do not need this in our later treatment, but we prove its semisimplicity as stated in the following theorem, since the result is very basic and its proof is nontrivial.

**Theorem 18.20.** If  $G$  is of order  $h$  and  $h1_F \neq 0$  (that is, if the characteristic of  $F$  is 0 or does not divide  $h$ ), then  $F[G]$  is semisimple.

PROOF. Put  $A = F[G]$ . Let  $V$  be a left  $A$ -module. Our task is to show that  $V$  is completely reducible. Let  $U$  be an  $A$ -submodule of  $V$ . Take a vector subspace  $X$  of  $V$  such that  $V = U \oplus X$ . For every  $x \in X$  and  $\alpha \in G$  there is a unique element  $y \in X$  such that  $\alpha x - y \in U$ . Put  $y = T_\alpha x$ . Then  $T_\alpha$  gives an element of  $\text{End}_F(X)$  and  $\alpha x - T_\alpha x \in U$  for every  $x \in X$ . Moreover, we easily see that  $T_{\alpha\beta} = T_\alpha T_\beta$  for  $\alpha, \beta \in G$ . Assuming that  $h1_F \neq 0$ , put  $Rx = h^{-1} \sum_{\alpha \in G} \alpha^{-1} T_\alpha x$  for  $x \in X$ . Then  $R$  is an  $F$ -linear map of  $X$  into  $V$ . For every  $x \in X$  we have  $x - \alpha^{-1} T_\alpha x \in U$ , and so  $Rx - x \in U$ . Put  $Y = RX$ . Then  $x \in U + Y$  for every  $x \in X$ , and so  $V = U + X \subset U + Y$ . Since  $\dim(Y) \leq \dim(X)$ , we have  $V = U \oplus Y$ . Besides, for  $\beta \in G$  and  $x \in X$  we have  $\beta Rx = h^{-1} \sum_{\alpha \in G} \beta \alpha^{-1} T_\alpha x = h^{-1} \sum_{\alpha \in G} \beta \alpha^{-1} T_{\alpha\beta^{-1}} T_\beta x = h^{-1} \sum_{\gamma \in G} \gamma^{-1} T_\gamma (T_\beta x) = R T_\beta x \in Y$ . Thus  $\beta Y \subset Y$ , that is,  $Y$  is an  $A$ -submodule. If we start from an irreducible  $A$ -submodule  $U$  of  $V$ , then we repeat the same procedure on  $Y$ , and eventually we can show that  $V$  is completely reducible as expected.

## 19. Central simple algebras

**19.1.** Given an associative ring  $A$  with identity element, put

$$(19.1) \quad Z = \{a \in A \mid ax = xa \text{ for every } x \in A\}.$$

Then  $Z$  is a subring of  $A$  containing the identity element of  $A$ . We call  $Z$  the **center** of  $A$ . We state here seven easy facts on the center of a ring.

(19.2) If  $A = A_1 \oplus \cdots \oplus A_s$  with rings  $A_i$  and  $Z_i$  is the center of  $A_i$ , then  $Z_1 \oplus \cdots \oplus Z_s$  is the center of  $A$ .

(19.3) If  $Z$  is the center of  $A$ , then the center of  $M_n(A)$  consists of the matrices  $z1_n$  with  $z \in Z$ .

(19.4) If  $D$  is a division ring, then the center of  $D$  is a field.

(19.5) If  $A$  is an  $F$ -algebra, then the center of  $A$  is an  $F$ -algebra.

(19.6) If  $A$  is a simple  $F$ -algebra, then the center of  $A$  is a field that is a finite algebraic extension of  $F$ .

(19.7) If  $A$  is a semisimple  $F$ -algebra, then the center of  $A$  is a direct sum of a finite number of finite algebraic extensions of  $F$ .

(19.8) If  $A$  is a semisimple  $F$ -algebra and the center of  $A$  is a field, then  $A$  is simple.

These can easily be verified. Take (19.6), for example. If  $A$  is simple, then by Theorem 18.12,  $A = M_n(D)$  with a division algebra  $D$ . By (19.3), the center of  $A$  can be identified with the center of  $D$ , which is clearly a field. We leave the details of the proof of the other statements to the reader.

An  $F$ -algebra is called **central** over  $F$  if its center is  $F$ . Every central simple algebra over  $F$  is of the form  $M_n(D)$  with a central division algebra  $D$  over  $F$ . In particular,  $M_n(F)$  is a central simple algebra over  $F$ .

**19.2.** Given two  $F$ -algebras  $A$  and  $B$  not necessarily of finite dimension over  $F$ , put  $C = A \otimes_F B$ . We can make  $C$  an  $F$ -algebra in such a way that  $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$  for  $a, a' \in A$  and  $b, b' \in B$ . To show this, we first define a map  $f_{a,b} : A \times B \rightarrow C$  for fixed  $a \in A$  and  $b \in B$  by  $f_{a,b}(x, y) = ax \otimes by$  for  $x \in A$  and  $y \in B$ . Then  $f_{a,b}$  is an  $F$ -bilinear map, and so there is an  $F$ -linear map  $\varphi_{a,b}$  of  $C$  into  $C$  such that  $\varphi_{a,b}(x \otimes y) = f_{a,b}(x, y)$ . Then  $\varphi_{a,b}(x \otimes y) = ax \otimes by$ . We easily see that  $(a, b) \mapsto \varphi_{a,b}$  is an  $F$ -bilinear map of  $A \times B$  into  $\text{Hom}(C, C)$ , and so there is an  $F$ -linear map  $\psi : C \rightarrow \text{Hom}(C, C)$  such that  $\psi(a \otimes b) = \varphi_{a,b}$  for every  $(a, b) \in A \times B$ . Now we define the law of multiplication  $(z, w) \mapsto zw$  in  $C$  by  $zw = \psi(z)(w)$ . It is an easy exercise to show that  $C$  is indeed an  $F$ -algebra with respect to this multiplication-law, and clearly  $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ . Hereafter we understand that  $A \otimes_F B$  means this  $F$ -algebra, and write simply  $A \otimes B$  for  $A \otimes_F B$  whenever  $F$  is clear from the context.

We easily see that the map  $a \mapsto a \otimes 1_B$  is an  $F$ -linear ring-injection of  $A$  into  $A \otimes B$ . Let  $A'$  denote the image of this map. Similarly the map  $b \mapsto 1_A \otimes b$  is an  $F$ -linear ring-injection of  $B$  into  $A \otimes B$ . Let  $B'$  denote the image of this map. Then  $xy = yx$  for every  $x \in A'$  and every  $y \in B'$ , and  $A \otimes B = A'B'$ .

Conversely, suppose we have an  $F$ -algebra  $C$  and two subalgebras  $A$  and  $B$  of  $C$  that have the following properties: (i)  $A$ ,  $B$ , and  $C$  have the same identity element; (ii)  $xy = yx$  for every  $x \in A$  and every  $y \in B$ ; (iii)  $C = AB$ ; (iv)  $[C : F] = [A : F][B : F]$ . Then there is an isomorphism of  $A \otimes B$  onto  $C$  that maps  $x \otimes y$  to  $xy$  for every  $x \in A$  and  $y \in B$ . We leave the proof to the reader. Thus if conditions (i), (ii), (iii), and (iv) are satisfied, we often identify  $C$  with  $A \otimes B$  with respect to that isomorphism.

We can easily show that  $M_r(A) \cong M_r(F) \otimes A$  for every  $F$ -algebra  $A$  and  $M_{rs}(F) \cong M_r(F) \otimes M_s(F) \cong M_r(M_s(F))$ .

As a special case, take an arbitrary field extension  $K$  of  $F$  (not necessarily of finite dimension over  $F$ ) as  $B$ . Then we can form  $A \otimes_F K$ , which we will often write  $A_K$ , and call it the **scalar extension** of  $A$  from  $F$  to  $K$ . Clearly  $A_K$  is a  $K$ -algebra.

**Lemma 19.3.** *For an  $F$ -algebra  $A$  denote by  $Z(A)$  the center of  $A$ . Then the following assertions hold:*

- (i)  $Z(A \otimes_F B) = Z(A) \otimes_F Z(B)$  for every  $F$ -algebra  $B$ .
- (ii) If  $K$  is an arbitrary field extension of  $F$ , then  $Z(A_K) = Z(A)_K$ .

PROOF. Here we do not assume that  $A$  and  $B$  are of finite dimension over  $F$ . Let  $\{x_i\}_{i \in I}$  be an  $F$ -basis of  $A$ . Then  $A \otimes B = \sum_{i \in I} x_i \otimes B$ . Let  $z = \sum_{i \in I} x_i \otimes b_i \in Z(A \otimes B)$ . The commutativity of  $z$  with  $1_A \otimes u$  for every  $u \in B$  shows that  $b_i \in Z(B)$  for every  $i$ , and so  $Z(A \otimes B) \subset A \otimes Z(B)$ . Let  $\{y_j\}_{j \in J}$  be an  $F$ -basis of  $Z(B)$ . Since  $A \otimes Z(B) = \sum_{j \in J} A \otimes y_j$ , we can put  $z = \sum_{j \in J} a_j \otimes y_j$  with  $a_j \in A$ . The commutativity of  $z$  with  $v \otimes 1_B$  for every  $v \in A$  shows that  $a_j \in Z(A)$  for every  $j$ . Thus  $Z(A \otimes B) \subset Z(A) \otimes Z(B)$ , which proves (i), as the opposite inclusion is obvious. Taking  $K$  as  $B$ , we obtain (ii).

**Lemma 19.4.** *Let  $B$  be a central simple algebra over  $F$  and  $A$  an  $F$ -algebra with identity element, not necessarily of finite dimension over  $F$ . Then every two-sided ideal of  $A \otimes B$  is of the form  $I \otimes B$  with a two-sided ideal  $I$  of  $A$ , and vice versa.*

PROOF. It is sufficient to prove the direct part. Let  $J$  be a two-sided ideal of  $A \otimes B$  different from  $\{0\}$ , and let  $I = J \cap A$ . Clearly  $I$  is a two-sided ideal of  $A$  and  $I \otimes B \subset J$ . We can find an  $F$ -basis  $\{x_\nu\}_{\nu \in N}$  of  $A$  such that  $\{x_\mu\}_{\mu \in M}$  is an  $F$ -basis of  $I$  with a subset  $M$  of  $N$ . Then  $A \otimes B = \sum_{\nu \in N} x_\nu \otimes B$  and  $I \otimes B = \sum_{\mu \in M} x_\mu \otimes B$ . Let  $L$  be the complement of  $M$  in  $N$ . Suppose  $J$  has

an element  $w$  not contained in  $I \otimes B$ . Put  $w = \sum_{\nu \in N} x_\nu b_\nu$  with  $b_\nu \in B$ . Then  $b_\nu \neq 0$  for some  $\nu \in L$ . Modifying  $w$  by a suitable element of  $I \otimes B$ , we may assume that  $w = \sum_{\nu \in L} x_\nu b_\nu$ . Let  $L_w = \{\nu \in L \mid b_\nu \neq 0\}$ . Then  $L_w$  is a nonempty finite set. Take  $w$  so that  $\#(L_w)$  is the smallest. Fix an element  $\kappa$  of  $L_w$  and put

$$H = \{c_\kappa \mid \sum_{\nu \in L_w} x_\nu c_\nu \in J \text{ with } c_\nu \in B\}.$$

We easily see that  $H$  is a two-sided ideal of  $B$ . Since  $0 \neq b_\kappa \in H$  and  $B$  is simple, we have  $H = B$ . Thus  $1 \in H$ , and so  $J$  has an element  $z = \sum_{\nu \in L_w} x_\nu c_\nu$  with  $c_\nu \in B$  such that  $c_\kappa = 1$ . Let  $d \in B$ . Then  $J \ni dz - zd = \sum_{\nu \in L_w} x_\nu (dc_\nu - c_\nu d)$ . Since the coefficient of this element for  $x_\kappa$  is 0, our assumption on  $w$  implies that  $dz - zd = 0$ , that is,  $dc_\nu = c_\nu d$  for every  $\nu \in L_w$ . Since this is so for every  $d \in B$ , we have  $c_\nu \in F$ , and so  $z \in A \cap J = I$ . This is a contradiction, as  $c_\kappa = 1$  and  $\kappa \notin M$ . Thus  $I \otimes B = J$  as expected.

**Theorem 19.5.** *Let  $B$  be a central simple algebra over  $F$ . Then the following assertions hold.*

- (i) *If  $A$  is simple, then  $A \otimes B$  is simple.*
- (ii) *If  $A$  is semisimple, then  $A \otimes B$  is semisimple.*
- (iii) *If  $A$  is central simple over  $F$ , then  $A \otimes B$  is central simple over  $F$ .*

PROOF. Assertion (i) follows from Lemma 19.4. Next, if  $A$  is semisimple, then  $A = A_1 \oplus \cdots \oplus A_s$  with simple algebras  $A_i$ , and so  $A \otimes B = (A_1 \otimes B) \oplus \cdots \oplus (A_s \otimes B)$ . Thus (ii) follows from (i). Finally, (iii) follows from (i) and Lemma 19.3(i).

**Theorem 19.6.** *Let  $K$  be an arbitrary (not necessarily finite) field extension of  $F$ , and  $B$  an  $F$ -algebra. Then  $B$  is central simple over  $F$  if and only if  $B_K$  is central simple over  $K$ .*

PROOF. From Lemma 19.3(ii) we see that  $Z(B) = F$  if and only if  $Z(B_K) = K$ . Thus our question is whether the algebras in question are simple. Suppose  $B$  is central simple over  $F$ . Then taking  $K$  as  $A$  in Theorem 19.5 (i), we see that  $B_K$  is simple. Conversely, suppose  $B_K$  is central simple over  $K$ . Let  $I$  be a two-sided ideal of  $B$  different from  $\{0\}$ . Then  $I \otimes K$  is a two-sided ideal of  $B_K$  different from  $\{0\}$ , and so  $I \otimes K = B_K$ . Thus  $I = B$ , which shows that  $B$  is simple, and our proof is complete.

**Theorem 19.7.** *Let  $\bar{F}$  be an algebraic closure of  $F$ . Then an  $F$ -algebra  $A$  is central simple over  $F$  if and only if  $A \otimes \bar{F}$  is isomorphic to a matrix algebra  $M_n(\bar{F})$  with some  $n$ .*

PROOF. This follows from Theorem 19.6 combined with Lemma 18.18(iii).

**Theorem 19.8.** *If  $A$  is a central simple algebra over  $F$ , then  $[A : F]$  is the square of an integer.*

PROOF. This follows immediately from Theorem 19.7.

**19.9.** By an **anti-isomorphism** of a ring  $A$  to a ring  $B$  we mean an additive bijection  $x \mapsto x^\alpha$  of  $A$  onto  $B$  such that  $(xy)^\alpha = y^\alpha x^\alpha$  for every  $x, y \in A$ . We call such an  $\alpha$  an **anti-automorphism** of  $A$  if  $A = B$ . We also call  $\alpha$  an **involution** of  $A$  if  $A = B$  and  $(x^\alpha)^\alpha = x$  for every  $x \in A$ . For example, if  $A = M_n(F)$ , then the transpose map  $x \mapsto {}^t x$  is an involution of  $A$ . If the rings are  $F$ -algebras and  $\alpha$  is  $F$ -linear, we call  $\alpha$  an anti-isomorphism or an anti-automorphism **over**  $F$ .

If  $A$  has an identity element and  $Z$  is the center of  $A$ , then every anti-automorphism of  $A$  induces an automorphism of  $Z$ .

Given an  $F$ -algebra  $A$  with identity element, we can construct an  $F$ -algebra  $A'$  that is anti-isomorphic to  $A$  over  $F$  as follows. We take  $A'$  as a vector space over  $F$  to be a copy of  $A$ ; then we define a law of multiplication on  $A'$  to be  $(a, b) \mapsto ba$ , where  $ba$  is the product considered in the algebra  $A$ . Then  $x \mapsto x$  of  $A$  onto  $A'$  is an anti-isomorphism of  $A$  onto  $A'$  over  $F$ . (Traditionally  $A'$  is called the **reciprocal** of  $A$ , but for simplicity we dispense with that terminology.)

**Theorem 19.10.** *Let  $A$  be a central simple algebra over  $F$ , and  $B$  a simple  $F$ -algebra. Suppose there exist two  $F$ -linear ring-injections  $\sigma$  and  $\tau$  of  $B$  into  $A$  that send  $1_B$  to  $1_A$ . Then there is an element  $\gamma$  of  $A^\times$  such that  $z^\tau = \gamma z^\sigma \gamma^{-1}$  for every  $z \in B$ .*

PROOF. We prove this for two  $F$ -linear anti-isomorphisms  $\sigma$  and  $\tau$  of  $B$  onto subalgebras of  $A$  that send  $1_B$  to  $1_A$ . This reformulation is valid, as we can replace  $B$  by an algebra anti-isomorphic to  $B$  over  $F$ , which can be obtained as in §19.9. Put  $C = A \otimes B$ , which is simple by Theorem 19.5(i). We define a right action of  $C$  on  $A$  by putting  $x(a \otimes b) = b^\sigma xa$  for  $x, a \in A$  and  $b \in B$ . Since  $(b_1 b_2)^\sigma = b_2^\sigma b_1^\sigma$ , the action defines a structure of a right  $C$ -module on  $A$ . (More precisely, we put  $x(\sum_i a_i \otimes b_i) = \sum_i b_i^\sigma x a_i$ , and we have to prove that this is indeed a well-defined action, but we leave the details to the reader.) We denote this right  $C$ -module by  $A_\sigma$ . Taking  $\tau$  in place of  $\sigma$ , we obtain another right  $C$ -module  $A_\tau$ . By Lemma 18.14,  $A_\sigma$  and  $A_\tau$  are  $C$ -isomorphic, that is, there exists an  $F$ -linear bijection  $f$  of  $A$  onto  $A$  such that  $f(b^\sigma xa) = b^\tau f(x)a$  for every  $a, x \in A$  and every  $b \in B$ . Taking  $x = 1_A$  and  $b = 1_B$ , we obtain  $f(a) = f(1_A)a$ . Put  $\gamma = f(1_A)$ . Then  $A = f(A) = \gamma A$ , and so  $\gamma \in A^\times$ . Also, we have  $\gamma b^\sigma = f(b^\sigma) = b^\tau \gamma$  for every  $b \in B$ , which proves our theorem.

Taking  $A = B$  and  $\tau$  to be the identity map of  $A$  to itself, we obtain the

following result.

**Corollary 19.11.** *Let  $A$  be a central simple algebra over  $F$ , and let  $\sigma$  be an  $F$ -linear automorphism of  $A$ . Then there exists an element  $\gamma$  of  $A^\times$  such that  $x^\sigma = \gamma x \gamma^{-1}$  for every  $x \in A$ .*

**Theorem 19.12.** *Let  $A$  be a central simple algebra over  $F$ , and  $A'$  an  $F$ -algebra anti-isomorphic to  $A$  over  $F$ ; let  $r = [A : F]$ . Then  $A \otimes A' \cong M_r(F)$ .*

PROOF. Put  $C = A \otimes A'$ . Let  $x \mapsto x^t$  be an  $F$ -linear anti-isomorphism of  $A'$  onto  $A$ . We can view  $A$  as a right  $C$ -module by the action  $x(a \otimes b) = b^t x a$  for  $a, x \in A$  and  $b \in A'$ . (This is a special case of what was done in the proof of Theorem 19.10.) By Theorem 19.5(iii),  $C$  is a central simple algebra over  $F$ . Now, the action of  $C$  on  $A$  defines an  $F$ -linear homomorphism  $\varphi$  of  $C$  into  $\text{End}_F(A)$ . Then  $\text{Ker}(\varphi)$  is a two-sided ideal of  $C$ , which cannot be  $C$ , as  $\varphi$  is nontrivial. Since  $C$  is simple, we have  $\text{Ker}(\varphi) = \{0\}$ , and so  $\varphi$  is injective. We have  $[C : F] = r^2 = [\text{End}_F(A) : F]$ . Consequently,  $C \cong \text{End}_F(A) \cong M_r(F)$  as expected.

**Lemma 19.13.** *Let  $A = M_r(D)$  with a division algebra  $D$  over  $F$ ,  $W$  a finitely generated  $A$ -module, and let  $B = \text{End}_A(W)$ . Then  $B \cong M_s(D)$  with some  $s$  and  $[W : F]^2 = [A : F][B : F]$ .*

PROOF. Let  $V = D_r^1$ . By Lemma 18.9,  $V$  is an irreducible right  $A$ -module and  $\text{End}_A(V) = D$ . By Theorem 18.11,  $W$  is isomorphic to the direct sum of  $s$  copies of  $V$  for some  $s$ . As explained in §18.8,  $B \cong M_s(D)$ . Then  $[W : F]^2 = s^2 r^2 [D : F]^2 = r^2 [D : F] s^2 [D : F] = [A : F][B : F]$ . This proves our lemma.

**Theorem 19.14.** *Let  $A$  be a central simple algebra over  $F$ ,  $B$  a simple subalgebra of  $A$  such that  $1_B = 1_A$ , and let  $C = \{x \in A \mid xb = bx \text{ for every } b \in B\}$ . (This set  $C$  is called **the commutor of  $B$  in  $A$** .) Then the following assertions hold:*

- (i)  $C$  is a simple algebra;
- (ii)  $B$  is the commutor of  $C$  in  $A$ ;
- (iii)  $[A : F] = [B : F][C : F]$ .
- (iv) Let  $B'$  be an algebra anti-isomorphic to  $B$  and let  $A \otimes_F B' \cong M_\mu(P)$  with a division algebra  $P$  and some  $\mu$ . Then  $C \cong M_\nu(P)$  with some  $\nu$ .

PROOF. We can put  $A = M_r(D)$  with a central division algebra  $D$  over  $F$ . Let  $V = D_r^1$ . Then  $V$  is an irreducible right  $A$ -module and  $D = \text{End}_A(V)$  by Lemma 18.9. With  $B'$  as in (iv), we can view  $V$  as a left  $(D \otimes B')$ -module by putting  $(d \otimes e')w = dwe$  for  $d \in D$  and  $e \in B$ , where  $e \mapsto e'$  is an anti-isomorphism of  $B$  onto  $B'$ . We easily see that  $C = \text{End}_{D \otimes B'}(V)$ . By Theorem 19.5(i),  $D \otimes B'$  is simple. Taking  $D \otimes B'$  and  $V$  to be  $A$  and  $W$  in Lemma

19.13, we find that  $C$  (which corresponds to  $B$  of that lemma) is simple, and  $[V : F]^2 = [C : F][D : F][B : F]$ , and so  $[A : F] = r^2[D : F] = [C : F][B : F]$ . Let  $E$  be the commutator of  $C$  in  $A$ . Then  $B \subset E$  and  $[A : F] = [C : F][E : F]$ , and so  $[B : F] = [E : F]$ . Thus  $B = E$ , which gives (ii). Let  $P$  be as in (iv). Then  $D \otimes_F B' \cong M_{\mu/r}(P)$ . Thus, when we view  $D \otimes B'$  as  $A$  of Lemma 19.13,  $P$  becomes  $D$  of that lemma, and so  $C \cong M_\nu(P)$  with some  $\nu$  by that lemma. This proves (iv) and completes the proof.

**Theorem 19.15.** *Let  $A$  be a central simple algebra over  $F$  and let  $[A : F] = m^2$ . Let  $K$  be a subalgebra of  $A$  that is a field and such that  $1_K = 1_A$ . Further let  $B$  be the commutator of  $K$  in  $A$ . Then  $B$  is a central simple algebra over  $K$  and  $[B : K] = s^2$  with an integer  $s$  such that  $m = s[K : F]$ . In particular,  $[K : F] = m$  if and only if  $K$  is the commutator of  $K$  in  $A$ , in which case  $A \otimes_F K \cong M_m(K)$ .*

PROOF. Clearly  $K \subset B$ . By Theorem 19.14,  $B$  is simple and  $K$  is the commutator of  $B$  in  $A$ . Thus  $B$  is a central simple algebra over  $K$ . Put  $[B : K] = s^2$ . Then  $m^2 = [A : F] = [K : F][B : F] = [K : F]^2 s^2$ , which proves the main part of our theorem. If  $[K : F] = m$ , then  $B = K$ , and vice versa. In such a case, take  $B = C = K$  in Theorem 19.14. Then both  $B'$  and  $P$  there coincide with  $K$ , and so  $A \otimes_F K \cong M_m(K)$ , which completes the proof.

**Lemma 19.16.** *If  $D$  is a central division algebra over  $F$  different from  $F$ , then  $D$  contains a separable extension of  $F$  different from  $F$ .*

PROOF. Let  $z \in D$ ,  $z \notin F$ . By Lemma 18.18(i),  $F[z]$  is an algebraic extension of  $F$  different from  $F$ , and so there is no problem if the characteristic of  $F$  is 0. Suppose  $F$  has characteristic  $p$  with a prime number  $p$ . If  $F[z]$  is not purely inseparable over  $F$ , then  $F[z]$  contains a nontrivial separable extension of  $F$ . So, assume that  $F[z]$  is purely inseparable over  $F$ . Then  $[F[z] : F] = q$  and  $z^q \in F$  with a power  $q = p^e$ ,  $0 < e \in \mathbf{Z}$ . Put  $u = z^{p^{e-1}}$ . Then  $u^p \in F$  and  $[F[u] : F] = p$ . Define an  $F$ -linear automorphism  $\sigma$  of  $D$  by  $\sigma(x) = uxu^{-1}$ . We view  $\sigma$  as an element of  $\text{End}_F(D)$ . We easily see that  $\sigma^p = 1$ ; also  $\sigma \neq 1$ , as  $u \notin F$ . Thus  $(\sigma - 1)^p = 0$  and  $\sigma - 1 \neq 0$ . Take the largest integer  $r$  such that  $(\sigma - 1)^r \neq 0$ ; then  $1 \leq r < p$ . Take  $y \in D$  so that  $(\sigma - 1)^r y \neq 0$ , and put  $a = (\sigma - 1)^{r-1} y$  and  $b = (\sigma - 1)^r y$ . Then  $0 \neq b = \sigma(a) - a$  and  $\sigma(b) - b = (\sigma - 1)^{r+1} y = 0$ , because of our choice of  $r$ . Put  $c = b^{-1}a$ . Then  $\sigma(c) = \sigma(b)^{-1}\sigma(a) = b^{-1}(b+a) = c+1$ . This means that  $\sigma$  gives a nontrivial automorphism of  $F[c]$ , so that  $F[c]$  is not purely inseparable over  $F$ . Thus we can find a nontrivial separable extension of  $F$  contained in  $D$ .

**Theorem 19.17.** *Let  $D$  be a central division algebra over  $F$ . Then  $D$  contains a separable extension  $M$  of  $F$  such that  $[D : F] = [M : F]^2$ .*



PROOF. Let  $[D : F] = m^2$ . Our assertion is obvious if  $m = 1$ , and so we assume  $m > 1$ . By Lemma 19.16,  $D$  contains a separable extension  $K$  of  $F$  different from  $F$ . Take such a  $K$  with the maximum value of  $[K : F]$ , and suppose  $[K : F] \neq m$ . Let  $B$  be the commutator of  $K$  in  $A$ . By Theorem 19.15,  $B$  is a central simple algebra over  $K$  and  $[B : K] = s^2$  with an integer  $s$  such that  $m = s[K : F]$ . Since  $B \subset D$ ,  $B$  is a division algebra. Now we have  $s > 1$ , and so by Lemma 19.16,  $B$  contains a separable extension  $L$  of  $K$  different from  $K$ . Then  $L$  is a separable extension of  $F$  and  $[L : F] > [K : F]$ , a contradiction. Therefore  $[K : F] = m$  and we obtain our theorem.

**19.18.** Let  $A$  be an  $F$ -algebra with identity element. An  $F$ -linear homomorphism  $\rho : A \rightarrow M_r(F)$  such that  $\rho(1_A) = 1_r$  is called a **representation** of  $A$  of degree  $r$ . We call  $\rho$  **faithful** if it is injective. Two  $F$ -linear representations  $\rho$  and  $\rho'$  of  $A$  are said to be **equivalent** over  $F$  if they are of the same degree, say  $r$ , and there exists an element  $T$  of  $GL_r(F)$  such that  $\rho'(\alpha) = T\rho(\alpha)T^{-1}$  for every  $\alpha \in A$ .

In general, every right or left  $A$ -module  $V$  produces a ring-homomorphism  $A \rightarrow \text{End}_F(V)$ . Identifying  $\text{End}_F(V)$  with  $M_n(F)$ , where  $n = [V : F]$ , we obtain a representation of  $A$ . Conversely, from a representation of  $A$  we can construct a right or left  $A$ -module.

Define a right  $A$ -module  $A_{[r]}$  as in §18.1 and put  $n = [A : F]$ . Then right multiplication by the elements of  $A$  defines an  $F$ -linear ring-homomorphism  $A \rightarrow \text{End}_F(A_{[r]})$ . This is certainly injective, as we are assuming that  $A$  has an identity element. Since  $\text{End}_F(A_{[r]}) \cong M_n(F)$ , we thus obtain a faithful representation  $\rho_r : A \rightarrow M_n(F)$ , which we call a **right regular representation** of  $A$ . This depends on the choice of an  $F$ -basis of  $A$ , but it is determined up to equivalence. Similarly let  $A_{[l]}$  denote the vector space  $A$  viewed as a left  $A$ -module. Then left multiplication defines an  $F$ -linear ring-injection  $A \rightarrow \text{End}_F(A_{[l]})$ , and consequently we obtain a representation  $\rho_l : A \rightarrow M_n(F)$ , which we call a **left regular representation** of  $A$ .

**Theorem 19.19.** (i) *Every two representations of a simple algebra of the same degree are equivalent.*

(ii) *If  $A$  is semisimple, then a right regular representation of  $A$  over  $F$  is equivalent to a left regular representation of  $A$  over  $F$ .*

PROOF. In view of what we said in §19.18 about the correspondence between representations and  $A$ -modules, (i) follows from Lemma 18.14. As for (ii), we can reduce the problem to the case where  $A$  is simple by means of Theorem 18.16. For simple  $A$ , the result follows from (i).

**Theorem 19.20.** *Let  $A$  be a simple algebra over  $F$  and  $Z$  the center of  $A$ . Suppose that  $Z$  is separable over  $F$ ; let  $[Z : F] = m$  and  $[A : Z] = n^2$  (see*

*Theorem 19.8).* Further let  $\rho$  be a right or left regular representation of  $A$  over  $F$  and  $\bar{F}$  an algebraic closure of  $Z$ . Then there exists a representation  $\tau : A \rightarrow M_{mn}(\bar{F})$  such that  $\rho$  is equivalent over  $\bar{F}$  to the direct sum of  $n$  copies of  $\tau$ . Moreover, put, for  $\alpha \in A$ ,

$$(19.9) \quad h_\alpha(x) = \det [x1_{mn} - \tau(\alpha)]$$

with an indeterminate  $x$ . Then  $h_\alpha$  has coefficients in  $F$  and  $h_\alpha(x)^n = \det [x1_t - \rho(\alpha)]$ ,  $t = mn^2$ , for every  $\alpha \in A$ .

This will be proved in §19.23.

**19.21.** Let  $A$  be a simple algebra over  $F$ . Taking a representation  $\tau$  of  $A$  as in the above theorem, we define a multiplicative map  $N_{A/F} : A \rightarrow F$  and an  $F$ -linear map  $\text{Tr}_{A/F} : A \rightarrow F$  by

$$(19.10) \quad N_{A/F}(\alpha) = \det [\tau(\alpha)], \quad \text{Tr}_{A/F}(\alpha) = \text{tr}[\tau(\alpha)] \quad (\alpha \in A).$$

We call these the **reduced norm** and the **reduced trace** of  $\alpha$ . That these are indeed the numbers belonging to  $F$  follows from the fact that  $h_\alpha$  of (19.9) has coefficients in  $F$ . Clearly  $N_{A/F}(c) = c^{mn}$  and  $\text{Tr}_{A/F}(c) = mnc$  for  $c \in F$ .

If  $A = M_n(F)$  in particular, then  $N_{A/F}(\alpha) = \det(\alpha)$  and  $\text{Tr}_{A/F}(\alpha) = \text{tr}(\alpha)$  for every  $\alpha \in M_n(F)$ . Indeed, in this case we have  $m = 1$  and we can take  $\tau$  to be the identity map of  $M_n(F)$  onto itself.

If  $K$  is a finite separable extension of  $F$ , then  $N_{K/F}$  and  $\text{Tr}_{K/F}$  of (19.10) (with  $K$  as  $A$ ) coincide with those of (7.1). Indeed, take  $A = Z = K$  in Theorem 19.20. Then  $\rho = \tau$  and  $h_\alpha(x) = \det[x1_m - \rho(\alpha)]$  for every  $\alpha \in K$ . Therefore the desired fact is already proved in Theorem 7.8(iv).

**Lemma 19.22.** *Let  $A$  be a simple algebra over  $F$  and  $Z$  the center of  $A$ . Then  $Z$  is a finite algebraic extension of  $F$ . Suppose that  $Z$  is separable over  $F$ . Then  $A \otimes_F L$  is semisimple for any finite or infinite extension  $L$  of  $F$ .*

**PROOF.** The first assertion is already stated as (19.6). Let  $\Omega$  be a Galois extension of  $L$  that contains an  $F$ -linear isomorphic image of  $Z$ . Take  $Z$  as  $K$  in the setting of Theorem 11.3. Thus we let  $S = \text{Inj}_F(Z, \Omega)/G$  with  $G = \text{Gal}(\Omega/L)$  and  $U_\sigma = Z^\sigma L$ . Then  $Z \otimes_F L \cong \bigoplus_{\sigma \in S} U_\sigma$ . Take a  $Z$ -basis  $\{x_\nu\}_{\nu=1}^t$  of  $A$ . Then  $A \otimes_F L = \bigoplus_{\nu=1}^t x_\nu(Z \otimes_F L) = \bigoplus_{\sigma \in S} \bigoplus_{\nu=1}^t x_\nu U_\sigma$ . We view  $Z$  as a subfield of  $U_\sigma$  under the map  $z \mapsto z^\sigma \in U_\sigma$ . Then  $A \otimes_Z U_\sigma = \sum_{\nu=1}^t U_\sigma$ , and so  $A \otimes_F L = \bigoplus_{\sigma \in S} (A \otimes_Z U_\sigma)$ . Since  $A \otimes_Z U_\sigma$  is central simple over  $U_\sigma$ , we see that  $A \otimes_F L$  is semisimple. This proves our lemma.

**19.23. Proof of Theorem 19.20.** We can put  $A = M_r(D)$  with a central division algebra  $D$  over  $Z$ . Put also  $[D : Z] = s^2$ ,  $[Z : F] = m$ , and  $n = rs$ . Then  $[A : F] = mn^2$ . By Theorem 19.17,  $D$  contains a separable extension  $L$  of  $Z$  such that  $[L : Z] = s$ . Then  $L$  is separable over  $F$  and  $[L : F] = ms$ . Let

$Y$  be a Galois extension of  $F$  containing an  $F$ -linear isomorphic image of  $L$ . We then consider  $A_Y = A \otimes_F Y$ , whose center is  $Z_Y = Z \otimes_F Y$  by Lemma 19.3(ii). We apply Theorem 11.3 to  $Z \otimes_F Y$  by taking  $(Z, Y)$  as  $(K, L)$  there. Then  $G = \text{Gal}(Y/Y) = \{1\}$  and  $S = \text{Inj}_F(Z, Y) = \text{Gal}(Y/Z) \setminus \text{Gal}(Y/F)$ , which has  $m$  elements. By that theorem there exists an isomorphism  $\psi : Z_Y \rightarrow \bigoplus_{\sigma \in S} U_\sigma$ ,  $U_\sigma = Z^\sigma Y$ , such that  $\psi(a \otimes b) = (a^\sigma b)_{\sigma \in S}$  for  $a \in Z$  and  $b \in Y$ . Since  $U_\sigma = Y$ , we see that  $\bigoplus_{\sigma \in S} U_\sigma$  is the direct sum of  $m$  copies of  $Y$ . We have  $A_Y = M_r(D_Y)$  with  $D_Y = D \otimes_F Y$ . Now  $\psi$  can be extended to a  $Y$ -linear isomorphism

$$(19.11) \quad \varphi : A_Y \rightarrow \bigoplus_{\sigma \in S} M_n(U_\sigma).$$

Indeed, as shown in the proof of Lemma 19.22,  $A_Y = \bigoplus_{\sigma \in S} (A \otimes_Z U_\sigma)$ , where  $Z$  is identified with the subfield  $Z^\sigma$  of  $U_\sigma$ . We have  $A = M_r(D)$ , and so  $A \otimes_Z U_\sigma = M_r(D \otimes_Z U_\sigma)$ . Since  $U_\sigma = Y$ , which contains an isomorphic image of the field  $L$  such that  $[D : Z] = [L : Z]^2$ , the last statement of Theorem 19.15 shows that  $D \otimes_Z U_\sigma \cong M_s(U_\sigma)$ . Thus  $A \otimes_Z U_\sigma \cong M_{rs}(U_\sigma)$ , which establishes the isomorphism of (19.11).

Let  $\rho$  be a regular representation of  $A$  over  $F$ . This can be extended naturally to a regular representation of  $A_Y$  over  $Y$ . Since  $U_\sigma = Y$ , the isomorphism of (19.11) shows that  $\rho$  is equivalent to  $\text{diag}[\rho_\sigma]_{\sigma \in S}$  with a regular representation of  $M_n(U_\sigma) = M_n(Y)$  over  $Y$ . Now a regular representation of  $M_n(Y)$  over  $Y$  is equivalent to the direct sum of  $n$  copies of the identity map of  $M_n(Y)$  onto itself. Therefore  $\rho_\sigma$  is equivalent to the direct sum of  $n$  copies of the identity map of  $M_n(U_\sigma)$  combined with the projection map of  $A_Y$  to that factor. Define  $\tau : A_Y \rightarrow \bigoplus_{\sigma \in S} M_n(U_\sigma)$  by  $\tau = \text{diag}[\tau_\sigma]_{\sigma \in S}$ , where  $\tau_\sigma$  is the identity map of  $M_n(U_\sigma)$  onto itself, and define  $h_\alpha$  by (19.9). Then  $h_\alpha$  has coefficients in  $Y$  and  $h_\alpha(x)^n = \det[x1_t - \rho(\alpha)]$ . Take any  $\alpha \in A$ . Then  $\rho(\alpha)$  has entries in  $F$ . Therefore for every  $\sigma \in \text{Gal}(Y/F)$  we have  $(h_\alpha^\sigma)^n = h_\alpha^n$ , and so  $h_\alpha^\sigma = h_\alpha$ , as  $h_\alpha$  is monic. Thus  $h_\alpha$  has coefficients in  $F$ . This completes the proof.

**Theorem 19.24.** *Let  $A$ ,  $Z$ , and  $F$  be as in Theorem 19.20, still under the condition that  $Z$  is separable over  $F$ . Then the  $F$ -bilinear form*

$$(19.12) \quad (x, y) \mapsto \text{Tr}_{A/F}(xy)$$

*is nondegenerate.*

PROOF. We consider the isomorphism  $\varphi$  of (19.11), using also the symbols  $U_\sigma$  and  $\tau = \text{diag}[\tau_\sigma]_{\sigma \in S}$  as in §19.23. We recall that  $U_\sigma = Y$  and  $\tau_\sigma$  is essentially the projection to  $M_n(U_\sigma) = M_n(Y)$ . If  $\varphi(\alpha) = (\alpha_\sigma)_{\sigma \in S}$  for  $\alpha \in A$ , then  $\tau_\sigma(\alpha) = \alpha_\sigma$  and  $\text{Tr}_{A/F}(\alpha) = \sum_{\sigma \in S} \text{tr}(\alpha_\sigma)$ . To prove that the bilinear form of (19.12) is nondegenerate, it is sufficient to show that its  $Y$ -bilinear extension to  $A_Y \times A_Y$  is nondegenerate, which is so if  $(z, w) \mapsto \text{tr}(zw)$

on  $M_n(U_\sigma) \times M_n(U_\sigma) = M_n(Y) \times M_n(Y)$  is nondegenerate. Since the last statement is clearly the case, we obtain our theorem.

**Lemma 19.25.** *Let  $A$  be an  $F$ -algebra whose center is a separable extension of  $F$ . If  $A \otimes_F L$  is semisimple for an extension  $L$  of  $F$ , then  $A$  is simple.*

PROOF. We use the symbols of the proof of Lemma 19.22. Without assuming  $A$  to be simple, we obtain  $A \otimes_F L = \bigoplus_{\sigma \in S} (A \otimes_Z U_\sigma)$ . Our assumption that  $A \otimes_F L$  is semisimple implies that  $A \otimes_Z U_\sigma$  is semisimple. By Lemma 19.3(ii),  $U_\sigma$  is the center of  $A \otimes_Z U_\sigma$ , and so  $A \otimes_Z U_\sigma$  is simple by (19.8). Therefore, by Theorem 19.6,  $A$  must be simple.

## 20. Quaternion algebras

**20.1.** Let  $B$  be an  $F$ -algebra with identity element equipped with an  $F$ -linear automorphism  $x \mapsto x'$ . Given an element  $\gamma \in F$ , we can construct an  $F$ -algebra  $A$  which contains  $B$  as a subalgebra and which has an element  $e \neq 0$  such that

$$(20.1) \quad A = B \oplus Be, \quad e^2 = \gamma, \quad be = eb' \quad \text{for every } b \in B.$$

Indeed, we consider  $M_2(B)$  and its subset  $A$  consisting of the matrices of the form

$$(20.2) \quad \begin{bmatrix} a & b \\ \gamma b' & a' \end{bmatrix} \quad \text{with } a, b \in B.$$

We easily see that  $A$  is a subalgebra of  $M_2(B)$ . Identify an element  $a$  of  $B$  with  $\text{diag}[a, a']$  and put  $e = \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix}$ . Then  $a + be$  is the matrix of (20.2), and so we have (20.1). Here we do not assume  $\gamma \neq 0$ .

There is an important special case in which  $B$  is a field. Changing the notation, take a separable quadratic extension  $K$  of  $F$  and an element  $\gamma \in F^\times$ . Let  $a \mapsto a^\sigma$  be the nontrivial automorphism of  $K$  over  $F$ . Then the above discussion produces an  $F$ -algebra  $A$  such that

$$(20.3) \quad A = K \oplus Kw, \quad w^2 = \gamma, \quad aw = wa^\sigma \quad \text{for every } a \in K.$$

We can easily show that

$$(20.4) \quad K = \{a \in A \mid ax = xa \text{ for every } x \in K\},$$

and also that  $F$  is the center of  $A$ . In this case the above embedding of  $A$  into  $M_2(B)$  becomes the map

$$(20.5) \quad a + bw \mapsto \begin{bmatrix} a & b \\ \gamma b^\sigma & a^\sigma \end{bmatrix},$$

which is an  $F$ -linear ring-injection of  $A$  into  $M_2(K)$ .

To show that  $A$  is simple, take a two-sided ideal  $J$  of  $A$  different from  $\{0\}$  and  $A$ . We can let  $K \otimes K$  act on  $J$  by  $(\sum_i a_i \otimes b_i)x = \sum_i a_i x b_i$  for  $a_i, b_i \in K$

and  $x \in J$ . Then  $J$  is a left  $(K \otimes K)$ -module. Let  $V$  be an irreducible  $(K \otimes K)$ -submodule of  $J$ . Since  $K \otimes K$  is the direct sum of two copies of  $K$  (see §11.4),  $V$  must be of dimension 2 over  $F$ , and so if we fix a nonzero element  $v$  of  $V$ , then  $Kv = vK = V$ . Thus, for  $a \in K$  there is a unique element  $a^\tau$  of  $K$  such that  $av = va^\tau$ , and clearly  $\tau$  gives an automorphism of  $K$  over  $F$ . If  $\tau$  is the identity map of  $K$ , then  $v \in K$  by (20.4), which implies that  $1 = v^{-1}v \in V$ , and so  $J = A$ . Thus  $\tau = \sigma$ , and so  $avw^{-1} = vw^{-1}a$  for every  $a \in K$ . Again by (20.4),  $vw^{-1} \in K$ , and so  $v$  is invertible, which means that  $J = A$ , a contradiction. This proves that  $A$  is simple.

**20.2.** We call an  $F$ -algebra  $A$  a **quaternion algebra** if  $A$  is central simple over  $F$  and  $[A : F] = 4$ . From Theorem 18.12 we see that a quaternion algebra is either isomorphic to  $M_2(F)$  or a central division algebra  $D$  over  $F$  such that  $[D : F] = 4$ . Given a separable quadratic extension  $K$  of  $F$  and an element  $\gamma \in F^\times$ , we can construct an algebra  $A$  by (20.3). Since it is central simple over  $F$ , it is a quaternion algebra. We denote this quaternion algebra by  $\{K, \gamma\}$ . We note an easy fact:

$$(20.6) \quad \{K, 1\} \cong M_2(F).$$

Indeed, if  $\gamma = 1$  in (20.3), then we have  $0 = 1 - w^2 = (1 + w)(1 - w)$  and  $1 \pm w \neq 0$ , as  $Kw \cap K = \{0\}$ . Thus  $\{K, 1\}$  is not a division algebra, and so we obtain (20.6).

As a special case we obtain the **Hamilton quaternion algebra**

$$(20.7) \quad \mathbf{H} = \mathbf{R} + \mathbf{R}\mathbf{i} + \mathbf{R}\mathbf{j} + \mathbf{R}\mathbf{k}.$$

Indeed, take  $F = \mathbf{R}$ ,  $K = \mathbf{C}$ , and  $\gamma = -1$ ; identify  $\mathbf{R} + \mathbf{R}\mathbf{i}$  with  $\mathbf{C}$  by putting  $\mathbf{i} = \sqrt{-1}$ ; put also  $w = \mathbf{j}$  and  $\mathbf{k} = \mathbf{i}\mathbf{j}$ . Then we rediscover the standard multiplication table of the quaternion units  $\mathbf{i}, \mathbf{j}, \mathbf{k}$ . Thus we can put  $\mathbf{H} = \{\mathbf{C}, -1\}$ .

Instead of a quadratic extension of  $F$ , we can take  $K = F \oplus F$ . Define an automorphism  $\sigma$  in this case by  $(a, b)^\sigma = (b, a)$  for  $(a, b) \in F \oplus F$ . The base field  $F$  is the subalgebra of  $F \oplus F$  consisting of the elements  $(c, c)$  with  $c \in F$ . Taking  $K = F \oplus F$  as  $B$  in (20.1), we obtain a subalgebra of  $M_2(K)$  consisting of  $\begin{bmatrix} (x, y) & (z, w) \\ (\gamma w, \gamma z) & (y, x) \end{bmatrix}$  with  $x, y, z, w$  in  $F$ . If we identify  $M_2(K)$  with  $M_2(F) \oplus M_2(F)$ , the subalgebra in question consists of  $\left( \begin{bmatrix} x & z \\ \gamma w & y \end{bmatrix}, \begin{bmatrix} y & w \\ \gamma z & x \end{bmatrix} \right)$ . Taking the projection to the first summand  $M_2(F)$ , we see that the algebra is isomorphic to  $M_2(F)$ . Thus we use the symbol  $\{K, \gamma\}$  also for  $K = F \oplus F$ . This will naturally appear when we extend the base number field to its completion at a prime.

**Theorem 20.3.** *Let  $A$  be a quaternion algebra over  $F$  and  $K$  a quadratic extension of  $F$ . Then  $A_K \cong M_2(K)$  if and only if there is an  $F$ -linear ring-injection of  $K$  into  $A$ .*

PROOF. The “if”-part is a special case of Theorem 19.15. Conversely, suppose  $A_K \cong M_2(K)$ . Let  $V$  be the vector space consisting of all the two-dimensional row vectors with components in  $K$ , viewed as a right  $A$ -module with respect to right matrix multiplication. Since  $A$  is simple and  $[V : F] = 4 = [A : F]$ , by Lemma 18.14,  $V$  is  $A$ -isomorphic to  $A_{[r]}$  of §18.1. Then, as noted there,  $A \cong \text{End}_A(A_{[r]})$ . Now left multiplication by the elements of  $K$  on  $V$  defines elements of  $\text{End}_A(V)$ , which means that there is an  $F$ -linear ring-injection of  $K$  into  $\text{End}_A(V)$ . This completes the proof, as  $\text{End}_A(V) \cong \text{End}_A(A_{[r]}) \cong A$ .

**Lemma 20.4.** *Let  $A$  be a quaternion algebra over  $F$ , and  $K$  a separable extension of  $F$  contained in  $A$  different from  $F$ . (Such a  $K$  always exists if  $A$  is a division algebra; see Lemma 19.16.) Then  $[K : F] = 2$  and  $A = \{K, \gamma\}$  with a suitable  $\gamma \in F^\times$ . Consequently every division quaternion algebra over  $F$  can be given as  $\{K, \gamma\}$  with suitable  $K$  and  $\gamma$ .*

PROOF. Clearly  $[K : F] \mid 4$ . The center of  $A$  is  $F$ , and so  $A \neq K$ . Thus  $[K : F] = 2$ . Let  $\sigma$  be a nontrivial automorphism of  $K$  over  $F$ . By Theorem 19.10, there exists an element  $w$  of  $A^\times$  such that  $a^\sigma = w^{-1}aw$  for every  $a \in K$ . Then  $K + Kw$  is a subalgebra of  $A$  different from  $K$ , and clearly  $A = K + Kw$ . Now  $aw^2 = w^2a$  for every  $a \in K$  and  $w^2$  commutes with  $w$ , and so  $w^2$  belongs to the center of  $A$ , that is,  $w^2 \in F$ . Putting  $\gamma = w^2$ , we find that  $A = \{K, \gamma\}$ .

**20.5.** Define a bijection  $\iota$  of  $M_2(F)$  onto itself by

$$(20.8) \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^\iota = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Then we can easily verify that  $\iota$  has the following properties, in which  $x$  denotes an arbitrary element of  $M_2(F)$ :

$$(20.9) \quad xx^\iota = \det(x), \quad x + x^\iota = \text{tr}(x),$$

$$(20.10) \quad (x^\iota)^\iota = x,$$

$$(20.11) \quad x^\iota = j \cdot {}^t x j^{-1} \quad \text{with} \quad j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

From (20.10) and (20.11) we see that  $\iota$  is an  $F$ -linear involution of  $M_2(F)$ . (See §19.9 for the definition of an involution.)

**Theorem 20.6.** *Every quaternion algebra  $A$  over  $F$  has a unique  $F$ -linear involution  $\iota$  such that  $\xi + \xi^\iota \in F$  and  $\xi\xi^\iota \in F$  for every  $\xi \in A$ . Moreover,*

$\xi + \xi^\iota = \text{Tr}_{A/F}(\xi)$  and  $\xi\xi^\iota = N_{A/F}(\xi)$  with the symbols  $\text{Tr}_{A/F}$  and  $N_{A/F}$  of (19.10).

PROOF. For  $A = M_2(F)$  we have such an involution as shown above. Suppose  $A$  is a division algebra. By Lemma 20.4 we can put  $A = \{K, \gamma\} = K + Kw$  as in (20.3) with a separable quadratic extension  $K$  of  $F$  and  $\gamma \in F^\times$ . Observe that the map of (20.5) sends  $a^\sigma - bw$  to  $\begin{bmatrix} a^\sigma & -b \\ -\gamma b^\sigma & a \end{bmatrix} = \begin{bmatrix} a & b \\ \gamma b^\sigma & a^\sigma \end{bmatrix}^\iota$ . This means that if we view  $A$  as a subset of  $M_2(K)$  by means of the injection of (20.5), then the involution  $\iota$  of  $M_2(K)$  defined by (20.8) sends  $A$  onto itself, and so we obtain an involution of  $A$ , which we also denote by  $\iota$ . If  $\xi = a + bw$ , then  $\xi^\iota = a^\sigma - bw$ ,  $\xi + \xi^\iota = a + a^\sigma \in F$ , and  $\xi\xi^\iota = aa^\sigma - \gamma bb^\sigma \in F$ . This proves the existence of an involution with the stated properties. To prove the uniqueness, let  $\tau$  be an  $F$ -linear involution of  $A$  such that  $\xi + \xi^\tau \in F$  and  $\xi\xi^\tau \in F$  for every  $\xi \in A$ . Since  $\xi^\tau = \xi$  for every  $\xi \in F$ , our aim is to show that  $\xi^\tau$  is uniquely determined for  $\xi$  when  $\xi \notin F$ . Let  $b = \xi + \xi^\tau$ ,  $c = \xi\xi^\tau$ , and  $f(x) = x^2 - bx + c$ . Then  $f(x) = (x - \xi)(x - \xi^\tau)$ . Suppose  $A$  is a division algebra and  $\xi \notin F$ . Then  $F[\xi]$  is an algebraic extension of  $F$  different from  $F$ . Since  $f$  has coefficients in  $F$  and  $f(\xi) = 0$ ,  $f$  must be the minimal polynomial for  $\xi$  over  $F$ . Thus  $\xi^\tau$ , the other root of  $f$ , is the image of  $\xi$  under the nontrivial automorphism of  $F[\xi]$ , and is uniquely determined. Next suppose  $A = M_2(F)$ . We again assume  $\xi \notin F$ . Then the characteristic polynomial of  $\xi$  is the unique monic polynomial  $g(x)$  of degree 2 such that  $g(\xi) = 0$ , and so  $g = f$ . This means that  $\xi + \xi^\tau = \text{tr}(\xi)$ . Thus  $\xi^\tau$  is uniquely determined as  $\text{tr}(\xi) - \xi$  when  $A = M_2(F)$ . Let  $h_\xi$  be the polynomial determined by (19.9) with  $\xi$  as  $\alpha$ . Then  $h_\xi(\xi) = 0$ , since  $\tau$  is injective and  $h_\xi(\tau(\xi)) = 0$ . We have  $h_\xi(x) = (x - \xi)^2$  if  $\xi \in F$ . Suppose  $\xi \notin F$ . If  $A$  is a division algebra, then  $h_\xi$  must be the minimal polynomial for  $\xi$  over  $F$ , and so  $h_\xi = f$ . The same is true for  $A = M_2(F)$  for the reason explained above. Since  $h_\xi(x) = x^2 - \text{Tr}_{A/F}(\xi)x + N_{A/F}(\xi)$ , we obtain the last statement of our theorem. This completes the proof.

**20.6a.** We call the involution of a quaternion algebra  $A$  over  $F$  uniquely determined as in the above theorem the **main involution** of  $A$ , and denote it by  $\iota$  if there is no fear of confusion. We can easily verify that

$$(20.12) \quad (\alpha\xi\alpha^{-1})^\iota = \alpha\xi^\iota\alpha^{-1} \quad \text{for every } \alpha \in A^\times, \xi \in A.$$

Let  $A_L = A \otimes_F L$  with any extension  $L$  of  $F$ . Then the  $L$ -linear extension of the main involution of  $A$  to  $A_L$  is the main involution of  $A_L$ . This follows, for example, from the first assertion of Theorem 20.6. The main involution of  $\mathbf{H}$  coincides with the standard quaternion conjugation, and so  $N_{\mathbf{H}/\mathbf{R}}(w) = |w|^2$  for every  $w \in \mathbf{H}$ , where  $|w| = (ww^\iota)^{1/2}$ .

**Lemma 20.7.** *Let  $A$  be a quaternion algebra over a field  $F$  of characteristic different from 2, and let  $A^\circ = \{\alpha \in A \mid \alpha^\iota = -\alpha\}$ . Then  $A = F \oplus A^\circ$ ,  $F = \{\alpha \in A \mid \alpha^\iota = \alpha\}$ , and  $A^\circ = \{\alpha \in A \mid \alpha^2 \in F, \alpha \notin F^\times\}$ .*

PROOF. For  $\alpha \in A$  we have  $2\alpha = (\alpha + \alpha^\iota) + (\alpha - \alpha^\iota)$ ,  $\alpha + \alpha^\iota \in F$ , and  $\alpha - \alpha^\iota \in A^\circ$ . Thus  $A = F \oplus A^\circ$ , as  $2 \neq 0$ . We have clearly  $F = \{\alpha \in A \mid \alpha^\iota = \alpha\}$  and  $A^\circ \cap F^\times = \emptyset$ . If  $\alpha \in A^\circ$ , then  $\alpha^2 = -\alpha\alpha^\iota \in F$ . Conversely, suppose  $\alpha^2 \in F$  and  $\alpha \notin F^\times$ ; put  $\alpha^2 = e$ ,  $b = \alpha + \alpha^\iota$ , and  $c = \alpha\alpha^\iota$ . Suppose  $\alpha \notin A^\circ$ . Then  $b \neq 0$ . Since  $\alpha$  is a root of both  $x^2 - bx + c$  and  $x^2 = e$ , we have  $b\alpha = c + e$ , and so  $\alpha \in F$ . Thus  $\alpha = 0 \in A^\circ$ , a contradiction. This completes the proof.

**Theorem 20.8.** *Let  $K$  be a separable quadratic extension of  $F$  and let  $\alpha, \beta \in F^\times$ . Then the following assertions hold:*

- (i) *There is an  $F$ -linear isomorphism of  $\{K, \alpha\}$  onto  $\{K, \beta\}$  if and only if  $\alpha/\beta \in N_{K/F}(K^\times)$ .*
- (ii) *In particular,  $\{K, \alpha\} \cong M_2(F)$  if and only if  $\alpha \in N_{K/F}(K^\times)$ .*
- (iii)  *$\{K, \alpha\} \otimes \{K, \beta\} \cong M_2(\{K, \alpha\beta\})$ .*

PROOF. Let  $\{K, \gamma\} = K + Kw$  as in (20.3). Take any  $s \in K^\times$  and put  $z = sw$ . Then  $z^2 = ss^\sigma w^2 = N_{K/F}(s)\gamma$  and  $az = za^\sigma$  for every  $a \in K$ . Since  $K + Kw = K + Kz$ , we see that  $\{K, \gamma\} = \{K, N_{K/F}(s)\gamma\}$ , which proves the “if”-part of (i). Next, put  $A = \{K, \alpha\}$  and  $B = \{K, \beta\}$ ; let  $\varphi$  be an  $F$ -linear isomorphism of  $A$  onto  $B$ . We can put  $A = K + Ku$  and  $B = K + Kv$  with  $u$  and  $v$  such that  $u^2 = \alpha$ ,  $v^2 = \beta$ , and  $u^{-1}au = v^{-1}av = a^\sigma$  for every  $a \in K$ . Applying Theorem 19.10 to  $\varphi : K \rightarrow B$  and the natural injection  $K \rightarrow B$ , we can find an element  $y$  of  $B^\times$  such that  $\varphi(a) = yay^{-1}$  for every  $a \in K$ . Put  $t = y^{-1}\varphi(u)y$ . Then for  $a \in K$  we have  $at = ay^{-1}\varphi(u)y = y^{-1}\varphi(au)y = y^{-1}\varphi(ua^\sigma)y = y^{-1}\varphi(u)yy^{-1}\varphi(a^\sigma)y = ta^\sigma$ , and so  $atv^{-1} = tv^{-1}a$ . Thus  $tv^{-1} \in K$  by (20.4). Putting  $tv^{-1} = d$ , we have  $t^2 = v^2dd^\sigma = \beta dd^\sigma$ . Also,  $t^2 = y^{-1}\varphi(u^2)y = y^{-1}\varphi(\alpha)y = \alpha$ , and so  $\alpha/\beta = dd^\sigma \in N_{K/F}(K^\times)$ , which proves the “only if”-part of (i), and completes the proof of (i). Then (ii) follows from (i) and (20.6).

To prove (iii), we use the same symbols  $A, B, u$ , and  $v$ . We view  $K \otimes K$  as a subset of  $A \otimes B$ . There is an isomorphism  $\psi : K \otimes K \rightarrow K \oplus K$  such that  $\psi(a \otimes b) = (ab, a^\sigma b)$ ; see §11.4. For  $x, y \in K$  denote by  $[x, y]$  the element of  $K \otimes K$  such that  $\psi([x, y]) = (x, y) \in K \oplus K$ . Let  $e = [1, 0]$  and  $f = [0, 1]$ . Then  $e^2 = e$ ,  $f^2 = f$ , and  $ef = fe = 0$ . Now  $(u \otimes 1)^{-1}(a \otimes b)(u \otimes 1) = a^\sigma \otimes b$  for  $a, b \in K$ , and so  $(u \otimes 1)^{-1}[ab, a^\sigma b](u \otimes 1) = [a^\sigma b, ab]$ . Thus  $(u \otimes 1)^{-1}[x, y](u \otimes 1) = [y, x]$ . Similarly we obtain  $(1 \otimes v)^{-1}[x, y](1 \otimes v) = [y^\sigma, x^\sigma]$ , and  $(u \otimes v)^{-1}[x, y](u \otimes v) = [x^\sigma, y^\sigma]$ . Consequently  $(u \otimes 1)^{-1}e(u \otimes 1) = (1 \otimes v)^{-1}e(1 \otimes v) = f$  and  $(u \otimes v)^{-1}e(u \otimes v) = e$ . Now  $A \otimes B = K \otimes K + (K \otimes K)(u \otimes 1) + (K \otimes K)(1 \otimes v) + (K \otimes K)(u \otimes v)$ . Put  $K' = (K \otimes K)e$  and



$w = e(u \otimes v)e$ . Then  $K' = \{[x, 0] \mid x \in K\}$ , which is isomorphic to  $K$ . We have  $e(A \otimes B)e = K' + K'w$ ,  $w^2 = \alpha\beta e$ , and  $w[x, 0] = [x^\sigma, 0]w$ . Therefore  $e(A \otimes B)e \cong \{K', \alpha\beta\} \cong \{K, \alpha\beta\}$ . If  $\{K, \alpha\beta\}$  is a division algebra, then Lemma 18.15 shows that  $A \otimes B \cong M_2(\{K, \alpha\beta\})$ . If  $\{K, \alpha\beta\} \cong M_2(F)$ , then the same lemma shows that  $A \otimes B \cong M_4(F)$ . This proves (iii).

**Lemma 20.9.** *Let  $A$  be a quaternion algebra over a field  $F$  of characteristic different from 2. Let  $A^c$  be the commutator subgroup of  $A^\times$  and  $A^1 = \{x \in A^\times \mid xx^t = 1\}$ . Then  $A^c = A^1$ .*

PROOF. Clearly  $A^c \subset A^1$  and  $A^1 \cap F^\times = \{\pm 1\}$ . We first consider the case  $A = M_2(F)$ . Then  $A^1 = SL_2(F)$ . Let  $\delta = \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix}$  and  $\varepsilon = \text{diag}[c, -c]$  with  $\gamma, c \in F^\times$ . Then  $\delta\varepsilon = -\varepsilon\delta$ , and so  $-1 \in A^c$ . (This is valid even when  $A$  is a division algebra, since we can take  $A$  to be the set of elements  $\begin{bmatrix} a & b \\ \gamma b^\sigma & a^\sigma \end{bmatrix}$  with  $a, b$  in a quadratic extension  $K$  of  $F$  as in §20.1, and find an element  $a$  of  $K^\times$  such that  $a^\sigma = -a$ .) Now every element of  $A^1$  is conjugate either to  $\pm \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$  or to  $\beta = \text{diag}[a, a^{-1}]$ . Since  $-1 \in A^c$ , we consider  $\alpha = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ . Let  $\xi = \text{diag}[1, -1]$  and  $\eta = \begin{bmatrix} 1 & b/2 \\ 0 & 1 \end{bmatrix}$ . Then  $\alpha = \xi^{-1}\eta^{-1}\xi\eta \in A^c$ . As for  $\beta$ , we have  $\beta = \zeta\omega\zeta^{-1}\omega^{-1}$  with  $\zeta = \text{diag}[a, 1]$  and  $\omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ . This proves that  $A^c = A^1$  when  $A = M_2(F)$ . Next suppose  $A$  is a division algebra; let  $\beta \in A^1, \notin F^\times$ . Then  $F[\beta]$  is a quadratic extension of  $F$  and  $\iota$  gives a nontrivial automorphism of  $F[\beta]$ , and so there exists an element  $\gamma$  of  $A^\times$  such that  $\xi^t = \gamma^{-1}\xi\gamma$  for every  $\xi \in F[\beta]$ ; see Theorem 19.10 or Lemma 20.4. By Lemma 1.8,  $\beta = \alpha^t\alpha^{-1}$  with  $\alpha \in F[\beta]^\times$ . Then  $\beta = \gamma^{-1}\alpha\gamma\alpha^{-1} \in A^c$ . This completes the proof.

## 21. Arithmetic of semisimple algebras

**21.1.** Let  $F$  be the field of quotients of an integral domain  $\mathfrak{g}$ . We are interested only in the following two cases: (i)  $F$  is an algebraic number field of finite degree and  $\mathfrak{g}$  is the ring of all algebraic integers in  $F$ ; (ii)  $F$  is a finite algebraic extension of  $\mathbf{Q}_p$  and  $\mathfrak{g}$  is the integral closure of  $\mathbf{Z}_p$  in  $F$ . We call a field of type (i) a **global field**, and that of type (ii) a **local field**. In this section, we employ the terms global and local fields only in these senses. Thus, a local field always means a nonarchimedean one. (This is essentially the same setting as in Section 14, in which we used  $J$  for the maximal order in  $F$ . For a certain technical reason we use  $\mathfrak{g}$  in this section instead of  $J$ .) In §4.1 we defined the notion of a  $\mathfrak{g}$ -lattice. In the local case,  $\mathfrak{g}$  is a principal

ideal domain; in the global case  $\mathfrak{g}$  satisfies (4.1), as shown in §10.1, and also in Lemma 10.6. Thus Lemma 4.2 holds in both cases.

In both local and global cases we call a  $\mathfrak{g}$ -lattice in  $F$  a  **$\mathfrak{g}$ -ideal**. If  $F$  is global, this is the same as a fractional ideal in  $F$ . A  $\mathfrak{g}$ -ideal is called **integral** if it is contained in  $\mathfrak{g}$ . We call a  $\mathfrak{g}$ -lattice simply a lattice if there is no fear of confusion. Let  $A$  be a semisimple  $F$ -algebra. By an **order** in  $A$  we mean a subring of  $A$  containing  $\mathfrak{g}$  that is a  $\mathfrak{g}$ -lattice in  $A$ . An order  $\mathfrak{o}$  is called **maximal** if there is no order, other than  $\mathfrak{o}$  itself, containing  $\mathfrak{o}$ . For two  $\mathfrak{g}$ -lattices  $\mathfrak{a}$  and  $\mathfrak{b}$  in  $A$  we denote by  $\mathfrak{a}\mathfrak{b}$  the  $\mathfrak{g}$ -lattice spanned by the products  $xy$  with  $x \in \mathfrak{a}$  and  $y \in \mathfrak{b}$ . Given an order  $\mathfrak{o}$  in  $A$ , we call a  $\mathfrak{g}$ -lattice  $\mathfrak{a}$  in  $A$  a **right** (resp. **left** or **two-sided**)  **$\mathfrak{o}$ -ideal** if  $\mathfrak{a}\mathfrak{o} \subset \mathfrak{a}$  (resp.  $\mathfrak{o}\mathfrak{a} \subset \mathfrak{a}$  or  $\mathfrak{o}\mathfrak{a}\mathfrak{o} \subset \mathfrak{a}$ ). An  $\mathfrak{o}$ -ideal is not necessarily contained in  $\mathfrak{o}$ , but it always contains an invertible element of  $A$ .

**21.2.** We can extend the notion of integrality introduced in §8.1 to the elements of an  $F$ -algebra  $A$  with identity element with a local or global  $F$ . We call an element  $\alpha$  of  $A$  **integral over  $\mathfrak{g}$**  if

$$(21.1) \quad \alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$$

with  $c_i \in \mathfrak{g}$  and  $n > 0$ . In that case we have  $\mathfrak{g}[\alpha] = \sum_{i=0}^{n-1} \mathfrak{g}\alpha^i$ , for the same reason as in the proof of Lemma 8.3. (Here we understand that  $\alpha^0 = 1$ . This causes some confusion when  $A$  is not a division ring, but later we consider integral elements only when  $A$  is a division algebra.) Conversely if  $\alpha$  belongs to a subring  $B$  of  $A$  that is a finitely generated  $\mathfrak{g}$ -module, then  $\alpha$  is integral over  $\mathfrak{g}$ . Indeed, suppose  $\alpha \in B$  with a subring  $B$  of the form  $B = \sum_{i=1}^k \mathfrak{g}\beta_i$  of  $A$ . Put  $C = \bigcup_{\nu=1}^{\infty} \left( \sum_{i=0}^{\nu} \mathfrak{g}\alpha^i \right)$ . This is a  $\mathfrak{g}$ -submodule of  $B$ , and so by Lemma 4.2, we can put  $C = \sum_{i=1}^m \mathfrak{g}\gamma_i$  with suitable  $\gamma_i$ . All these  $\gamma_i$  are contained in  $\sum_{i=0}^{\nu} \mathfrak{g}\alpha^i$  for a sufficiently large  $\nu$ . Then  $\alpha^{\nu+1}$  is a  $\mathfrak{g}$ -linear combination of  $\{\alpha^i\}_{i=0}^{\nu}$ , which shows that  $\alpha$  is integral over  $\mathfrak{g}$ .

Consequently, if  $\alpha$  is an element of an order  $\mathfrak{o}$ , then  $\alpha$  is integral over  $\mathfrak{g}$  since the powers of  $\alpha$  are contained in a finitely generated  $\mathfrak{g}$ -module.

If  $A$  is a field, then it is a finite algebraic extension of  $F$ , and all the elements of  $A$  integral over  $\mathfrak{g}$  form a ring. In the global case, the ring is the set of all algebraic integers in  $A$ , which we called the maximal order of  $A$  in §8.9, which is indeed maximal in the sense we defined in §21.1. If  $F$  is local, then, as shown in Theorem 9.5(5), the integral closure of  $\mathfrak{g}$  is the valuation ring of  $A$ , which is a free  $\mathfrak{g}$ -module of rank  $[A : F]$ . Thus  $A$  has a unique maximal order, which is the valuation ring of  $A$ .

**Lemma 21.3.** *Given a  $\mathfrak{g}$ -lattice  $\mathfrak{x}$  in a semisimple algebra  $A$  over  $F$ , let  $\mathfrak{o}_1 = \{\alpha \in A \mid \alpha\mathfrak{x} \subset \mathfrak{x}\}$  and  $\mathfrak{o}_2 = \{\alpha \in A \mid \mathfrak{x}\alpha \subset \mathfrak{x}\}$ . Then  $\mathfrak{o}_1$  and  $\mathfrak{o}_2$  are orders in  $A$ . (These are called **the left order** and **the right order** of  $\mathfrak{x}$ .)*

PROOF. Put  $[A : F] = n$  and take any free  $\mathfrak{g}$ -module  $\mathfrak{a}$  of rank  $n$  in  $A$ . We can find elements  $c$  and  $d$  of  $F^\times$  such that  $c\mathfrak{a} \subset \mathfrak{x} \subset d\mathfrak{a}$ . Let  $\rho$  be a left regular representation of  $A$  defined with respect to a  $\mathfrak{g}$ -basis of  $\mathfrak{a}$ . Then  $\alpha \in \mathfrak{o}_1 \Rightarrow cd^{-1}\rho(\alpha) \in M_n(\mathfrak{g})$  and  $\rho(\alpha) \in M_n(\mathfrak{g}) \Rightarrow cd^{-1}\alpha \in \mathfrak{o}_1$ . From this we see that  $\mathfrak{o}_1$  is a  $\mathfrak{g}$ -lattice in  $A$ . Clearly  $\mathfrak{o}_1$  is a subring of  $A$  containing  $\mathfrak{g}$ , and so it is an order in  $A$ . The case of  $\mathfrak{o}_2$  is similar.

**Lemma 21.4.** *For a semisimple  $F$ -algebra  $A$  the following two assertions hold:*

- (i) *Every order in  $M_n(A)$  containing the standard matrix units of  $M_n(A)$  can be written  $M_n(S)$  with an order  $S$  in  $A$ .*
- (ii) *Such an order  $M_n(S)$  is maximal if and only if  $S$  is maximal.*

PROOF. For  $x = \sum_{i,j} a_{ij}e_{ij} \in M_n(A)$  with  $a_{ij} \in A$  and the standard matrix units  $e_{ij}$  write  $a_{ij} = p_{ij}(x)$ . Given an order  $R$  in  $M_n(A)$  containing the  $e_{ij}$ , put  $S_{ij} = p_{ij}(R)$ . Since  $e_{ii}xe_{jj} = a_{ij}e_{ij}$ , we see that  $S_{ij}e_{ij} \subset R$ . Also, we have  $S_{ij} = S_{11}$  for all  $(i, j)$ , since  $e_{1i}e_{ij}e_{j1} = e_{11}$  and  $e_{i1}e_{11}e_{1j} = e_{ij}$ . Clearly  $S_{11}$  is an order in  $A$ , and  $R = M_n(S_{11})$ . If  $S_{11}$  is contained in a larger order  $T$ , then  $R \subsetneq M_n(T)$ , which means that  $S_{11}$  is maximal if  $R$  is maximal. Next, given a maximal order  $S$  in  $A$ , let  $R$  be an order containing  $M_n(S)$ . By (i) we have  $R = M_n(Q)$  with an order  $Q$  in  $A$ . Then  $S \subset Q$ , and hence  $S = Q$ , as  $S$  is maximal. Thus  $M_n(S) = R$ , which completes the proof.

**21.5.** We now assume that  $F$  is an algebraic number field of finite degree. We denote by  $\mathbf{a}$  and  $\mathbf{h}$  the sets of archimedean primes and nonarchimedean primes of  $F$  respectively, and put  $\mathbf{v} = \mathbf{a} \cup \mathbf{h}$  as we did in Section 15. Further we denote by  $\mathfrak{g}$  the maximal order of  $F$ . For every  $v \in \mathbf{v}$  we denote by  $F_v$  the  $v$ -completion of  $F$ . In particular, for  $v \in \mathbf{h}$  and a  $\mathfrak{g}$ -ideal  $\mathfrak{a}$  we denote by  $\mathfrak{a}_v$  the  $v$ -closure of  $\mathfrak{a}$  in  $F_v$ , which coincides with the  $\mathfrak{g}_v$ -linear span of  $\mathfrak{a}$  in  $F_v$ . If  $F = \mathbf{Q}$ , there is only one archimedean prime, which we often denote by  $\infty$ . Thus  $\mathbf{v} = \{\infty\} \cup \mathbf{h}$  if  $F = \mathbf{Q}$ , and  $\mathbf{Q}_\infty = \mathbf{R}$ .

Given a finite-dimensional vector space  $X$  over  $F$  and a  $\mathfrak{g}$ -lattice  $L$  in  $X$ , we put  $X_v = X \otimes_F F_v$  for every  $v \in \mathbf{v}$ , and denote by  $L_v$  the  $\mathfrak{g}_v$ -linear span of  $L$  in  $X_v$  if  $v \in \mathbf{h}$ . In particular, if  $A$  is an  $F$ -algebra and  $S$  is an order in  $A$ , then  $S_v$  is an order in  $A_v$ . Since  $X_v$  is isomorphic to  $F_v^n$  for some  $n$ , Lemma 6.9 shows that  $X_v$  has a structure of a locally compact additive group, and also that every  $\mathfrak{g}_v$ -lattice in  $X_v$  is an open compact subgroup of  $X_v$ . For a  $\mathfrak{g}$ -lattice  $L$  in  $X$ , we see that  $L_v$  is a  $\mathfrak{g}_v$ -lattice in  $X_v$ , and is the closure of  $L$  in  $X_v$ .

**Lemma 21.6.** *With  $F$  and  $X$  as above, let  $L$  be an arbitrarily fixed  $\mathfrak{g}$ -lattice in  $X$ . Then the following assertions hold:*

- (i) *If  $M$  is a  $\mathfrak{g}$ -lattice in  $X$ , then  $L_v = M_v$  for almost all  $v$ . Moreover,  $L \subset M$  (resp.  $L = M$ ) if  $L_v \subset M_v$  (resp.  $L_v = M_v$ ) for every  $v \in \mathbf{h}$ .*

(ii) Given a  $\mathfrak{g}_v$ -lattice  $N_v$  in  $X_v$  for each  $v \in \mathbf{h}$  such that  $N_v = L_v$  for almost all  $v$ , there exists a  $\mathfrak{g}$ -lattice  $M$  in  $X$  such that  $M_v = N_v$  for every  $v \in \mathbf{h}$ .

(iii) If  $Y$  is a subspace of  $X$  and  $L$  is a  $\mathfrak{g}$ -lattice in  $X$ , then  $(L \cap Y)_v = L_v \cap Y_v$  for every  $v \in \mathbf{h}$ .

(iv) Let  $x \in X$ . If  $x \in L_v$  for every  $v \in \mathbf{h}$ , then  $x \in L$ .

PROOF. To prove (i), take an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $X$  contained in  $L \cap M$  and take  $c \in \mathfrak{g}$ ,  $c \neq 0$ , so that  $c(L + M) \subset \sum_{i=1}^n \mathfrak{g}e_i$ . Put  $H = \sum_{i=1}^n \mathfrak{g}c^{-1}e_i$ . Then  $cH \subset L \cap M \subset L + M \subset H$ . Clearly  $L_v = M_v$  if  $v \nmid c$ , which is the first part of (i). Since  $\mathfrak{g}/c\mathfrak{g}$  is isomorphic to  $\prod_{v|c}(\mathfrak{g}_v/c\mathfrak{g}_v)$ , we easily see that the map  $x \pmod{cH} \mapsto (x \pmod{cH_v})_{v|c}$  for  $x \in H$  gives an isomorphism of  $H/cH$  onto  $\prod_{v|c}(H_v/cH_v)$ . We can also find  $u_v \in \mathfrak{g}$  for each  $v|c$  such that  $u_v - 1 \in c\mathfrak{g}_v$  and  $u_v \in c\mathfrak{g}_w$  for  $v \neq w|c$ . Assume now  $L_v \subset M_v$  for every  $v \in \mathbf{h}$ . Let  $x \in L$ . Since  $x \in L_v \subset M_v$  and  $M$  is dense in  $M_v$ , we can find an element  $y_v$  of  $M$  for each  $v|c$  such that  $x - y_v \in cH_v$ . Put  $z = \sum_{v|c} u_v y_v$ . Then  $z \in M$  and  $x - z \in cH_v$  for every  $v|c$ . In view of the above isomorphism, this means that  $x - z \in cH \subset M$ , so that  $x \in M$ . Thus  $L \subset M$ . If  $L_v = M_v$  for every  $v \in \mathbf{h}$ , then exchanging  $L$  and  $M$ , we obtain  $M \subset L$ , and hence  $L = M$ . To prove (ii), changing  $L$  suitably, we may assume that  $L$  is isomorphic to  $\mathfrak{g}_n^1$  with some  $n$ . Put  $\mathbf{p} = \{v \in \mathbf{h} \mid N_v \neq L_v\}$ . Take  $b \in \mathfrak{g}$ ,  $b \neq 0$ , so that  $bN_v \subset L_v$  for every  $v \in \mathbf{p}$ . Changing  $N_v$  for  $bN_v$ , we may assume that  $N_v \subset L_v$  for every  $v \in \mathbf{h}$ . Defining  $\mathbf{p}$  for this new  $\{N_v\}_{v \in \mathbf{h}}$ , take  $c \in \mathfrak{g}$ ,  $c \neq 0$ , so that  $cL_v \subset N_v$  for every  $v \in \mathbf{p}$ . Then  $cL_v \subset N_v$  for every  $v \in \mathbf{h}$ , and the map  $x \pmod{cL} \mapsto (x \pmod{cL_v})_{v|c}$  for  $x \in L$  gives an isomorphism of  $L/cL$  onto  $\prod_{v|c}(L_v/cL_v)$ . Let  $M$  be the  $\mathfrak{g}$ -submodule of  $L$  containing  $cL$  such that  $M/cL$  is sent to  $\prod_{v|c}(N_v/cL_v)$ . Clearly  $cL_v \subset M_v \subset N_v$  for every  $v|c$ , and  $M_v = N_v$  if  $v \nmid c$ . Given  $v|c$  and  $y \in N_v$ , we can find, in view of the above isomorphism, an element  $x$  of  $M$  such that  $x - y \in cL_v$ . Then  $y \in M + cL_v \subset M_v$ , which shows that  $M_v = N_v$  as expected. As for (iii), take an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $X$  so that  $Y = \sum_{i=m}^n Fe_i$ . By Theorem 10.19(i) we have  $L = \sum_{i=1}^n A_i g_i$  with fractional ideals  $A_i$  and an  $F$ -basis  $\{g_i\}_{i=1}^n$  of  $X$  such that  $g_i \in \sum_{k=i}^n Fe_k$ . Then  $Y = \sum_{i=m}^n Fg_i$  and  $L \cap Y = \sum_{i=m}^n A_i g_i$ , from which we obtain (iii). Applying (i) to  $L$  and  $\mathfrak{g}x + L$ , we obtain (iv). This completes the proof.

**Lemma 21.7.** *Let  $A$  be a semisimple algebra over a local or global field  $F$ . Then the following assertions hold:*

(i)  *$A$  has an order. Moreover, given an order  $R$  in  $A$ , there exists a maximal order  $S$  in  $A$  containing  $R$ .*

(ii) *If  $F$  is global, then an order  $S$  in  $A$  is maximal if and only if  $S_v$  is maximal for every  $v \in \mathbf{h}$ .*

(iii) Suppose  $F$  is global; let  $\Lambda$  be a  $\mathfrak{g}$ -lattice in  $A$ . Given an order  $R_v$  in  $A_v$  for each  $v \in \mathbf{h}$ , suppose that  $R_v = \Lambda_v$  for almost all  $v$ . Then there exists an order  $S$  in  $A$  such that  $S_v = R_v$  for every  $v \in \mathbf{h}$ .

(iv) If  $A$  is commutative ( $F$  local or global), then  $A$  has a unique maximal order.

PROOF. Take an  $F$ -basis  $\{\varepsilon_i\}_{i=1}^n$  of  $A$ . Then  $\varepsilon_i \varepsilon_j = \sum_{k=1}^n c_{ijk} \varepsilon_k$  with  $c_{ijk} \in F$ . Take  $b \in \mathfrak{g}$ ,  $b \neq 0$ , so that  $bc_{ijk} \in \mathfrak{g}$  for every  $\{i, j, k\}$ . Put  $T = \mathfrak{g} + \sum_{i=1}^n \mathfrak{g} b \varepsilon_i$ . Then clearly  $T$  is an order in  $A$ . To prove the remaining part of (i), let  $A = A_1 \oplus \cdots \oplus A_r$  with simple algebras  $A_i$  and  $1_A = e_1 + \cdots + e_r$  with the identity element  $e_i$  of  $A_i$ . Given an order  $R$  in  $A$ , put  $R' = \sum_{i=1}^r R e_i$ . We easily see that  $R e_i$  is an order in  $A_i$ ,  $R'$  is an order in  $A$ , and  $R \subset R'$ . If  $S_i$  is a maximal order in  $A_i$  containing  $R e_i$ , then  $\sum_{i=1}^r S_i$  is a maximal order containing  $R$ . Thus it is sufficient to prove the existence of  $S$  in (i) when  $A$  is simple. Assuming  $A$  to be simple, denote by  $K$  the center of  $A$  and by  $\mathfrak{r}$  the maximal order of  $K$ . Let  $R$  be an order in  $A$  and let  $U = \mathfrak{r}R$ . Then  $U$  is an order in  $A$  containing both  $R$  and  $\mathfrak{r}$ . Therefore replacing  $F$  and  $\mathfrak{g}$  by  $K$  and  $\mathfrak{r}$ , we may assume that  $A$  is central simple over  $F$ . Let  $R$  be an order in  $A$  and  $R'$  an order in  $A$  containing  $R$ . Take an  $F$ -basis  $\{\varepsilon_i\}_{i=1}^n$  of  $A$  contained in  $R$ . Since  $(x, y) \mapsto \text{Tr}_{A/F}(xy)$  is nondegenerate, we can find  $\{\eta_i\}_{i=1}^n$  in  $A$  such that  $\text{Tr}_{A/F}(\varepsilon_i \eta_j) = \delta_{ij}$ . Given  $\alpha \in R'$ , put  $c_i = \text{Tr}_{A/F}(\alpha \varepsilon_i)$ . Then  $c_i \in \mathfrak{g}$  by Lemma 21.9 below. Clearly  $\alpha = \sum_{i=1}^n c_i \eta_i$ , and so  $R' \subset \sum_{i=1}^n \mathfrak{g} \eta_i$ . Thus every order containing  $R$  is contained in  $\sum_{i=1}^n \mathfrak{g} \eta_i$ . Therefore in view of Lemma 4.2, there must be a maximal order containing  $R$ .

In the setting of (iii), by Lemma 21.6(ii) there exists a  $\mathfrak{g}$ -lattice  $S$  in  $A$  such that  $S_v = R_v$  for every  $v \in \mathbf{h}$ . For  $x, y \in S$  we have  $(S + \mathfrak{g}xy)_v = S_v + \mathfrak{g}_v xy \subset R_v = S_v$  for every  $v$ , so that  $S + \mathfrak{g}xy \subset S$ , that is,  $xy \in S$ . Similarly  $1 \in S$ . Thus  $S$  is an order in  $A$ . This proves (iii). To prove (ii), take an order  $S$  in  $A$ . Suppose  $S \subsetneq T$  with an order  $T$  in  $A$ . By Lemma 21.6(i),  $S_v \neq T_v$  for some  $v$ , so that  $S_v$  is not maximal. Conversely, suppose  $S_u$  is not maximal for some  $u \in \mathbf{h}$ . Then  $S_u \subsetneq Y_u$  with an order  $Y_u$  in  $A_u$ . By (iii), there exists an order  $Z$  in  $A$  such that  $Z_v = S_v$  for every  $v \in \mathbf{h}$ ,  $v \neq u$ , and  $Z_u = Y_u$ . Clearly  $S \subsetneq Z$ , so that  $S$  is not maximal. This proves (ii).

To prove (iv), take  $A = A_1 \oplus \cdots \oplus A_r$  as before, assuming  $A$  to be commutative. Then  $A_i$  is a finite algebraic extension of  $F$ , which has a unique maximal order  $S_i$ , as explained in the last paragraph of §21.2. We have seen that every order in  $A$  is contained in  $\bigoplus_{i=1}^r S_i$ . Thus  $\bigoplus_{i=1}^r S_i$  is the unique maximal order in  $A$ . This proves (iv) and completes the proof.

**21.8.** Let us now prove (14.7). We take  $K$  there to be  $A$  in the above lemma. By (iv) above,  $K_P$  has a unique maximal order, which must be the right-hand side of (14.7), since  $J_{Q_i}$  is the maximal order of  $K_{Q_i}$ . On the other

hand, by Lemma 21.7(ii),  $J_K \otimes J_P$  is maximal in  $K_P$ . Therefore we obtain (14.7).

**Lemma 21.9.** *Let  $A$  be a simple algebra over a local or global field  $F$ , and  $R$  an order in  $A$ . Then  $\text{Tr}_{A/F}(\alpha) \in \mathfrak{g}$  for every  $\alpha \in R$ .*

PROOF. Given  $0 \neq \alpha \in R$ , put  $S = \bigcup_{m=1}^{\infty} (\sum_{i=1}^m \mathfrak{g}\alpha^i)$ . Then  $S$  is a  $\mathfrak{g}$ -submodule of  $R$ , and so by Lemma 4.2,  $S = \sum_{j=1}^s \mathfrak{g}\beta_j$  with some  $\beta_j$ . Then we can find  $n$  such that  $\beta_j \in \sum_{i=1}^n \mathfrak{g}\alpha^i$  for every  $j$ . Then  $\alpha^{n+1} \in \sum_{i=1}^n \mathfrak{g}\alpha^i$ . Thus we obtain a monic polynomial  $p(x)$  of degree  $n+1$  in  $\mathfrak{g}[x]$  such that  $p(\alpha) = 0$ . Define  $h_\alpha$  by (19.9). Let  $\rho$  be a regular representation of  $A$  over  $F$  and  $q(x)$  the minimal polynomial of  $\alpha$  over  $F$ , which is clearly the minimal polynomial of  $\rho(\alpha)$  over  $F$ . Then  $q$  divides  $p$ , and so  $q \in \mathfrak{g}[x]$  by Theorem 8.6. Now the characteristic polynomial of  $\rho(\alpha)$  is a power of  $h_\alpha$  as shown in Theorem 19.20, and also it divides a power of  $q$ . Thus  $h_\alpha$  divides a power of  $q$ , and so  $h_\alpha \in \mathfrak{g}[x]$  again by Theorem 8.6. Since  $\text{Tr}_{A/F}(\alpha)$  is a coefficient of  $h_\alpha$ , we obtain our lemma.

**21.10.** Hereafter we consider  $F$  and  $\mathfrak{g}$  in the local case. We denote by  $\mathfrak{p}$  and  $\mu$  the maximal ideal of  $\mathfrak{g}$  and the normalized order function of  $F$ , and put  $q = \#(\mathfrak{g}/\mathfrak{p})$ .

Let  $X$  be a finite-dimensional vector space over  $F$ . Then  $X$ , being isomorphic to the product of a finite number of copies of  $F$ , has a natural structure of a locally compact topological group, in which every  $\mathfrak{g}$ -lattice is an open compact subset. If  $X$  is of dimension  $n$ , then every  $\mathfrak{g}$ -lattice is a free  $\mathfrak{g}$ -module of rank  $n$ . If  $A$  is an  $F$ -algebra and  $\mathfrak{o}$  is an order in  $A$ , then  $A^\times$ , with the topology induced from that of  $A$ , has a natural structure of a locally compact topological group. Let  $U_m = \{1 + x \mid x \in \mathfrak{p}^m \mathfrak{o}\}$  for  $0 < m \in \mathbf{Z}$ . This is clearly a subgroup of  $\mathfrak{o}^\times$ , and compact, as it is homeomorphic to the compact set  $\mathfrak{p}^m \mathfrak{o}$ . Since  $U_m$  is of finite index in  $\mathfrak{o}^\times$ , we see that  $\mathfrak{o}^\times$  is compact. Also, since the  $\mathfrak{p}^m \mathfrak{o}$  for  $0 < m \in \mathbf{Z}$  form a base of open neighborhoods of 0 in  $A$ , the groups  $U_m$  form a base of open neighborhoods of 1 in  $A^\times$ .

**Lemma 21.11.** *If  $X$  is a finite-dimensional vector space over a local field  $F$ , then every compact subset of  $X$  is contained in a  $\mathfrak{g}$ -lattice in  $X$ .*

PROOF. Let  $Y$  be a compact subset of  $X$ . Take any  $\mathfrak{g}$ -lattice  $L$  in  $X$ . Then  $Y \subset \bigcup_{y \in Y} (y + L)$ . Since  $y + L$  is open, we have  $Y \subset \bigcup_{p \in P} (p + L)$  with a finite subset  $P$  of  $Y$ . Then  $\sum_{p \in P} (\mathfrak{g}p + L)$  is a  $\mathfrak{g}$ -lattice containing  $Y$ .

We insert here three elementary lemmas.

**Lemma 21.12.** *Put  $F^{\times 2} = \{x^2 \mid x \in F^\times\}$ ,  $\mathfrak{g}^{\times 2} = \{x^2 \mid x \in \mathfrak{g}^\times\}$ , and  $1 + \mathfrak{a} = \{x \in \mathfrak{g} \mid x - 1 \in \mathfrak{a}\}$  for a  $\mathfrak{g}$ -ideal  $\mathfrak{a}$ . Then the following assertions hold:*

- (i)  $1 + 4\mathfrak{p}^m = \{a^2 \mid a \in 1 + 2\mathfrak{p}^m\}$  for  $0 < m \in \mathbf{Z}$ ; in particular,  $1 + 4\mathfrak{p} \subset \mathfrak{g}^{\times 2}$ .
- (ii)  $F^{\times 2}$  is an open and closed subgroup of  $F^\times$ .
- (iii)  $\mathfrak{g}^\times = \{u^2 + x \mid u \in \mathfrak{g}^\times, x \in \mathfrak{p}\} = \mathfrak{g}^{\times 2}(1 + \mathfrak{p})$  if  $2 \in \mathfrak{p}$ .

PROOF. Clearly  $1 + 4\mathfrak{p}^m \supset \{a^2 \mid a \in 1 + 2\mathfrak{p}^m\}$ . Conversely, let  $c \in \mathfrak{p}^m$ ,  $m > 0$ . By Hensel's lemma, there exists an element  $d \in \mathfrak{g}$  such that  $d^2 - d - c = 0$ . Changing  $d$  for  $1 - d$  if necessary, we may assume that  $d \notin \mathfrak{p}$ . Then  $(1 + 2d^{-1}c)^2 = 1 + 4c$ , which proves the equality of (i). Taking  $m = 1$ , we obtain the last part of (i). Since  $1 + 4\mathfrak{p}$  is open in  $F^\times$ , (ii) follows from (i). Suppose  $2 \in \mathfrak{p}$ ; then  $(\mathfrak{g}/\mathfrak{p})^\times$  is of odd order, and so  $x \mapsto x^2$  is a surjective map of  $(\mathfrak{g}/\mathfrak{p})^\times$  onto itself. From this we obtain (iii).

**Lemma 21.13.** *Let  $K$  be a quadratic extension of  $F$ ,  $\mathfrak{r}$  the valuation ring of  $K$ ,  $\mathfrak{q}$  the maximal ideal of  $\mathfrak{r}$ ,  $\rho$  the generator of  $\text{Gal}(K/F)$ , and  $\mathfrak{d} = d(K/F) = \mathfrak{q}^e$  with  $0 \leq e \in \mathbf{Z}$ . Put*

$$U = \{u \in \mathfrak{r}^\times \mid uu^\rho = 1\}, \quad U_0 = \{u^\rho/u \mid u \in \mathfrak{r}^\times\}.$$

*Then the following assertions hold:*

- (i) *For  $v \in \mathfrak{r}$  we have  $\mathfrak{r} = \mathfrak{g}[v]$  if and only if  $\mathfrak{d} = (v - v^\rho)\mathfrak{r}$ .*
- (ii)  *$[U : U_0] = 1$  or  $2$  according as  $K$  is unramified or ramified over  $F$ .*
- (iii)  *$U_0 = \{a \in U \mid a - 1 \in \mathfrak{d}\}$ .*
- (iv)  *$x \in U, x \notin U_0 \implies (x - 1)\mathfrak{q} = \mathfrak{d}$ .*
- (v) *If  $\mathfrak{d} \neq \mathfrak{r}$ , then  $(1 + \mathfrak{p}^s) \cap N_{K/F}(\mathfrak{r}^\times) \subset N_{K/F}(1 + \mathfrak{q}^s)$  for  $0 < s \in \mathbf{Z}$ , and  $(1 + \mathfrak{p}^s) \cap N_{K/F}(\mathfrak{r}^\times) = N_{K/F}(1 + \mathfrak{q}^s)$  if  $0 < s \leq e$ .*

PROOF. Assertion (i) is already given in (14.9). To prove (ii), define a homomorphism  $g : K^\times \rightarrow U$  by  $g(a) = a^\rho/a$ . By Lemma 1.8 this is surjective and  $g^{-1}(U_0) = F^\times \mathfrak{r}^\times$ , and so we have  $[U : U_0] = [K^\times : F^\times \mathfrak{r}^\times]$ , from which we obtain (ii). If  $\mathfrak{d} = \mathfrak{r}$ , (iii) follows from (ii). Suppose  $\mathfrak{d} \neq \mathfrak{r}$ ; let  $a = u^\rho/u$  with  $u \in \mathfrak{r}^\times$ . Then  $a - 1 = (u^\rho - u)/u \in \mathfrak{d}$ . Therefore, to prove (iii), it is sufficient to show that  $U$  is different from the right-hand side of (iii). Since  $U = g(K^\times)$ ,  $U$  is generated by  $U_0$  and  $\pi^\rho/\pi$  with a prime element  $\pi$  of  $K$ . By Theorem 9.9(ii),  $\mathfrak{r} = \mathfrak{g}[\pi]$ . If  $\pi^\rho/\pi - 1 \in \mathfrak{d}$ , then  $\mathfrak{d} = (\pi^\rho - \pi)\mathfrak{r} \subset \pi\mathfrak{d}$ , a contradiction. This proves (iii). If  $x \in U$  and  $x \notin U_0$  as in (iv), then  $\mathfrak{d} \neq \mathfrak{r}$  and  $x = (\pi^\rho/\pi)(u^\rho/u)$  with  $u \in \mathfrak{r}^\times$ . Putting  $y = \pi u$ , we have  $(x - 1)\mathfrak{q} = (y^\rho - y)y^{-1}\mathfrak{q} = \mathfrak{d}$ , as  $\mathfrak{r} = \mathfrak{g}[\pi u]$ . This proves (iv).

To prove (v), write simply  $N$  for  $N_{K/F}$  and take  $y \in K^\times$  so that  $yy^\rho - 1 \in \mathfrak{p}^s$  with  $s > 0$ . Then  $y \in \mathfrak{r}^\times$ . Since  $y - y^\rho \in \mathfrak{d}$ , we have  $y^2 - 1 \in \mathfrak{q}$ , so that  $\pm y - 1 \in \mathfrak{q}$ . Put  $x = \pm y - 1$  and  $x\mathfrak{r} = \mathfrak{q}^m$  with  $m \in \mathbf{Z}$ . If  $m \geq s$ , then  $yy^\rho = N(1 + x) \in N(1 + \mathfrak{q}^s)$  as expected. If  $m < s$ , then  $x + x^\rho + xx^\rho = yy^\rho - 1 \in \mathfrak{q}^{2s}$ . Put  $z = \mp x^\rho/x$ . Then  $zz^\rho = 1$  and  $1 - zy = (x + x^\rho + xx^\rho)/x \in \mathfrak{q}^{2s-m} \subset \mathfrak{q}^s$ , so that  $N(y) = N(zy) \in N(1 + \mathfrak{q}^s)$ , which proves the first part

of (v). If  $0 < s \leq e \neq 0$ , then  $\text{Tr}_{K/F}(\mathfrak{q}^{-s}) \subset \text{Tr}_{K/F}(\mathfrak{q}^{-e}) = \mathfrak{g}$  by (14.1a), and so  $\text{Tr}_{K/F}(\mathfrak{q}^s) \subset \mathfrak{p}^s$ . From this we easily obtain  $N(1 + \mathfrak{q}^s) \subset 1 + \mathfrak{p}^s$ , which combined with the first part proves the second part of (v). This completes the proof.

**Lemma 21.14.** *The symbols  $K$ ,  $\mathfrak{r}$ , and  $\rho$  being as in Lemma 21.13, suppose that  $K$  is unramified over  $F$ . Then there exists an element  $u$  of  $\mathfrak{r}$  such that  $uu^\rho = 1$ ,  $\mathfrak{r} = \mathfrak{g}[u]$ , and  $u - u^\rho$  is a unit.*

PROOF. Let  $\mathfrak{q}$  be the maximal ideal of  $\mathfrak{r}$ . Then  $\mathfrak{r}/\mathfrak{q}$  is a quadratic extension of  $\mathfrak{g}/\mathfrak{p}$ . We can find an element  $\alpha$  of  $\mathfrak{r}/\mathfrak{q}$ , not contained in  $\mathfrak{g}/\mathfrak{p}$ , whose norm to  $\mathfrak{g}/\mathfrak{p}$  is 1, since there are  $q + 1$  elements in  $\mathfrak{r}/\mathfrak{q}$  with norm 1 if  $q = \#(\mathfrak{g}/\mathfrak{p})$ . Then the equation for  $\alpha$  over  $\mathfrak{g}/\mathfrak{p}$  can be written in the form  $x^2 + ax + 1 \equiv 0$  with  $a \in \mathfrak{g}$ . By Hensel's lemma,  $K$  contains an element  $u$  such that  $u^2 + au + 1 = 0$ . Then  $uu^\rho = 1$  and  $u - u^\rho$  is a unit, as the equation is separable over  $\mathfrak{g}/\mathfrak{p}$ . By Lemma 21.13(i) we have  $\mathfrak{r} = \mathfrak{g}[u]$ .

**Theorem 21.15.** *We have  $[F^\times : N_{K/F}(K^\times)] = 2$  for a quadratic extension  $K$  of a local field  $F$ .*

PROOF. If  $K$  is unramified over  $F$ , this is a special case of Theorem 9.10(ii), which we already proved. Therefore we assume  $K$  to be ramified over  $F$ , and use the symbols  $\mathfrak{q}$ ,  $e$ ,  $U$ , and  $N$  of Lemma 21.13 and its proof. We first prove

$$(21.2a) \quad \mathfrak{g}^\times \neq N_{K/F}(\mathfrak{r}^\times) \text{ if } K \text{ is ramified over } F.$$

Suppose  $2 \notin \mathfrak{p}$ . By Theorem 9.9(ii),  $\mathfrak{r} = \mathfrak{g}[\pi]$  with a prime element  $\pi$  of  $K$ . Then for  $a, b \in \mathfrak{g}$  we have  $N(a + b\pi) - a^2 \in \mathfrak{p}$ . Since  $a \mapsto a^2$  is not a surjective map of  $(\mathfrak{g}/\mathfrak{p})^\times$  onto itself, this proves (21.2a). Next suppose  $2 \in \mathfrak{p}$ ; then  $e \geq 2$  by Theorem 14.7. Suppose  $\mathfrak{g}^\times = N(\mathfrak{r}^\times)$ . Then  $N(1 + \mathfrak{q}^{e-1}) = 1 + \mathfrak{p}^{e-1}$  and  $N(1 + \mathfrak{q}^e) = 1 + \mathfrak{p}^e$  by Lemma 21.13(v). Thus  $N$  gives a surjective homomorphism of  $1 + \mathfrak{q}^{e-1}$  onto  $1 + \mathfrak{p}^{e-1}$ . By Lemma 21.13(iii, iv),  $U \subset 1 + \mathfrak{q}^{e-1}$ . Therefore the inverse image of  $1 + \mathfrak{p}^e$  is  $U(1 + \mathfrak{q}^e)$ , and so  $[1 + \mathfrak{q}^{e-1} : U(1 + \mathfrak{q}^e)] = [1 + \mathfrak{p}^{e-1} : 1 + \mathfrak{p}^e] = q$ , where  $q = [\mathfrak{g} : \mathfrak{p}]$ . On the other hand  $[1 + \mathfrak{q}^{e-1} : 1 + \mathfrak{q}^e] = q$ , and  $U(1 + \mathfrak{q}^e) \neq 1 + \mathfrak{q}^e$ , in view of Lemma 21.13(ii, iv). This is a contradiction, and so we obtain (21.2a). We complete the proof of our theorem after the proof of Theorem 21.23. At the same time we will prove

$$(21.2b) \quad [\mathfrak{g}^\times : N_{K/F}(\mathfrak{r}^\times)] = 2 \text{ if } K \text{ is ramified over } F.$$

In general, a semisimple algebra  $A$  over  $F$  may have many maximal orders, but if it is a division algebra, the matter is simpler. Indeed, every division algebra over  $F$  has a unique maximal order, say  $\mathfrak{O}$ , and every one-sided  $\mathfrak{O}$ -ideal is two-sided and principal as will be shown in Theorem 21.17 below. We first prove:



**Theorem 21.16.** *Let  $D$  be a central division algebra over  $F$  and let  $n = [D : F]^{1/2}$ . Then there is a map  $\lambda : D \rightarrow \mathbf{Z} \cup \{\infty\}$  with the following properties:*

- (1)  $\lambda = n\mu$  on  $F$ .
- (2)  $\lambda(xy) = \lambda(x) + \lambda(y)$ .
- (3)  $\lambda(x + y) \geq \min\{\lambda(x), \lambda(y)\}$ .
- (4)  $\text{Tr}_{D/F}(z) \in \mathfrak{g}$  if  $\lambda(z) \geq 0$ .

PROOF. Put  $\lambda(x) = \mu(N_{D/F}(x))$  for  $x \in D$ , where  $N_{D/F}$  is the reduced norm map; see §19.21. Clearly we have (1) and (2). To prove (3), we may assume that  $xy \neq 0$ . Assuming  $\lambda(x) \leq \lambda(y)$ , put  $z = x^{-1}y$  and  $K = F[z]$ . Then  $\lambda(z) \geq 0$  and  $K$  is a subfield of  $D$ . For  $b \in K$  such that  $K = F[b]$  let  $g_b(x)$  denote the minimal polynomial of  $b$  over  $F$ , which coincides with the characteristic polynomial of  $b$  as an element of  $\text{End}_F(K)$ . Define  $\rho$  and  $h_b$  as in Theorem 19.20 by taking  $D$  as  $A$  there. Viewing  $D$  as a left  $K$ -module, we see that the characteristic polynomial of  $\rho(b)$  is a power of  $g_b$ , and so  $h_b = g_b^s$  with a positive integer  $s$ . Then  $N_{D/F}(b) = N_{K/F}(b)^s$ . Taking  $z$  as  $b$ , we find that  $\mu(N_{K/F}(z)) = s^{-1}\lambda(z) \geq 0$ . Let  $\mathfrak{r}$  be the valuation ring of  $K$ . As shown in the proof of Theorem 9.5, an element  $y$  of  $K$  belongs to  $\mathfrak{r}$  if and only if  $\mu(N_{K/F}(y)) \geq 0$ . (The symbol  $\nu$  there is  $\mu$  here.) Thus  $z \in \mathfrak{r}$ , and so  $1 + z \in \mathfrak{r}$ . Then  $\lambda(1 + z) = s \cdot \mu(N_{K/F}(1 + z)) \geq 0$ . Therefore  $\lambda(x + y) = \lambda(x(1 + z)) = \lambda(x) + \lambda(1 + z) \geq \lambda(x)$ , which proves (3). We see also that  $\text{Tr}_{D/F}(z) = s \cdot \text{Tr}_{K/F}(z) \in \mathfrak{g}$  if  $\lambda(z) \geq 0$ , which is (4).

**Theorem 21.17.** *The notation being as in Theorem 21.16, put*

$$\mathfrak{D} = \{x \in D \mid \lambda(x) \geq 0\} \quad \text{and} \quad \mathfrak{P} = \{x \in D \mid \lambda(x) > 0\}.$$

*Then the following assertions hold:*

- (1)  $\mathfrak{D}$  is a unique maximal order of  $D$  and consists of all the elements of  $D$  integral over  $\mathfrak{g}$ .
- (2) Given  $k \in \mathbf{Z}$ , put  $\mathfrak{X}_k = \{x \in D \mid \lambda(x) \geq k\}$ . Then  $\mathfrak{X}_k$  is a two-sided  $\mathfrak{D}$ -ideal and  $\mathfrak{X}_k = \mathfrak{D}c = c\mathfrak{D}$  with any element  $c$  of  $D$  such that  $\lambda(c) = k$ . Moreover, every right or left  $\mathfrak{D}$ -ideal is a two-sided  $\mathfrak{D}$ -ideal of the form  $\mathfrak{X}_k$  with an integer  $k$ . Write  $\mathfrak{X}_k = \mathfrak{P}^k$ . (This notation will be justified in the proof.)
- (3)  $\mathfrak{D}/\mathfrak{P}$  is a finite field containing  $\mathfrak{g}/\mathfrak{p}$ .
- (4)  $[\lambda(D^\times) : \lambda(F^\times)] = [\mathfrak{D}/\mathfrak{P} : \mathfrak{g}/\mathfrak{p}] = n$ ; consequently  $\lambda(D^\times) = \mathbf{Z}$ .
- (5)  $\mathfrak{p}\mathfrak{D} = \mathfrak{P}^n$ .
- (6)  $\text{Tr}_{D/F}(\mathfrak{D}) = \mathfrak{g}$ .
- (7)  $\mathfrak{P}^{1-n} = \{a \in D \mid \text{Tr}_{D/F}(a\mathfrak{D}) \subset \mathfrak{g}\}$  and  $\text{Tr}_{D/F}(\mathfrak{P}^{1-n}) = \mathfrak{g}$ .
- (8)  $D$  has a subfield which is an unramified extension of  $F$  of degree  $n$ .

PROOF. Clearly  $\mathfrak{O}$  is a subring of  $D$  containing  $\mathfrak{g}$ . Given  $z \in D$ , put  $K = F[z]$ . Since the restriction of  $\lambda$  to  $K$  is an order function of  $K$ , we see that  $z \in \mathfrak{O}$  if and only if  $z$  belongs to the valuation ring of  $K$ , which is so if and only if  $z$  is integral over  $\mathfrak{g}$ . This proves the second part of (1). Since every element of  $D$  times a suitable nonzero element of  $\mathfrak{g}$  belongs to  $\mathfrak{O}$ , we can find an  $F$ -basis  $\{y_i\}$  of  $D$  contained in  $\mathfrak{O}$ . By Theorem 19.24, we can find another  $F$ -basis  $\{x_i\}$  of  $D$  such that  $\text{Tr}_{D/F}(x_i y_j) = \delta_{ij}$ . Let  $\mathfrak{Y} = \{a \in D \mid \text{Tr}_{D/F}(a\mathfrak{O}) \subset \mathfrak{g}\}$ . Then we easily see that  $\mathfrak{O} \subset \mathfrak{Y} \subset \sum_i \mathfrak{g} x_i$ . Therefore  $\mathfrak{O}$  is finitely generated over  $\mathfrak{g}$ . Thus  $\mathfrak{O}$  is an order in  $D$ . Since every element contained in any order in  $D$  is integral over  $\mathfrak{g}$ , we obtain (1).

Clearly  $\mathfrak{X}_k$  of (2) is a two-sided  $\mathfrak{O}$ -ideal. Given a right  $\mathfrak{O}$ -ideal  $\mathfrak{A}$ , let  $c$  be an element of  $\mathfrak{A}$  with the smallest value of  $\lambda$ . If  $\lambda(y) \geq \lambda(c)$  with  $y \in D$ , then  $\lambda(c^{-1}y) \geq 0$ , so that  $c^{-1}y \in \mathfrak{O}$ . Thus  $y \in c\mathfrak{O} \subset \mathfrak{A}$ . This shows that  $\mathfrak{A} = c\mathfrak{O} = \{x \in D \mid \lambda(x) \geq \lambda(c)\}$ . Since the last set is a two-sided  $\mathfrak{O}$ -ideal, we obtain (2) except the fact that  $\text{Min}\{\lambda(x) \mid x \in \mathfrak{X}_k\} = k$ , which follows from the equality  $\lambda(D^\times) = \mathbf{Z}$  given in (4). Assuming that fact, we have  $\mathfrak{P} = \mathfrak{X}_1$ . If  $k > 0$ , clearly  $\mathfrak{X}_k$  is the  $k$ -th power of  $\mathfrak{P}$  in the ordinary sense; of course  $\mathfrak{X}_0 = \mathfrak{O}$ . If  $k < 0$ , we easily see that  $\mathfrak{X}_k = \{x \in D \mid x\mathfrak{P}^{|k|} \subset \mathfrak{O}\}$ . This justifies the symbol  $\mathfrak{P}^k$  for  $\mathfrak{X}_k$ .

Next, from (2) we see that  $\mathfrak{O}/\mathfrak{P}$  has no nontrivial proper one-sided ideals, so that  $\mathfrak{O}/\mathfrak{P}$  is a division ring. Clearly  $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{g}$ , and so  $\mathfrak{g}/\mathfrak{p}$  can be viewed as a subfield of  $\mathfrak{O}/\mathfrak{P}$ . By (2) we have  $\mathfrak{P} = z\mathfrak{O}$  with some  $z \in \mathfrak{O}$ . Put  $K = F[z]$ ,  $\mathfrak{r} = \mathfrak{O} \cap K$ , and  $\mathfrak{q} = \mathfrak{P} \cap K$ . Then  $\mathfrak{q} = z\mathfrak{r}$ , and  $\mathfrak{p}\mathfrak{r} = \mathfrak{q}^e$  with a positive integer  $e$ . Then  $\mathfrak{p}\mathfrak{O} = z^e\mathfrak{O} = \mathfrak{P}^e$ . Now  $e \leq [K : F] \leq n$ . (From the equality  $h_b = g_b^s$  in the proof of Theorem 21.16 we see that  $[K : F]$  divides  $n$  for every subfield  $K$  of  $D$  containing  $F$ .) Let  $\{b_i\}$  be a  $\mathfrak{g}$ -basis of  $\mathfrak{O}$ . Then  $\mathfrak{P}^e = \mathfrak{p}\mathfrak{O} = \sum_i \mathfrak{p}b_i$ , so that  $[\mathfrak{O} : \mathfrak{P}^e] = q^{n^2}$ . On the other hand, from (2) we see that  $\mathfrak{P}^k/\mathfrak{P}^{k+1}$  is isomorphic to  $\mathfrak{O}/\mathfrak{P}$ , and hence  $[\mathfrak{O} : \mathfrak{P}^e] = [\mathfrak{O} : \mathfrak{P}]^e$ , so that  $[\mathfrak{O} : \mathfrak{P}] = q^{n^2/e}$ . In particular this shows that  $\mathfrak{O}/\mathfrak{P}$  is finite and so commutative. Take an element  $s$  of  $\mathfrak{O}$  so that the class of  $s$  modulo  $\mathfrak{P}$  generates  $\mathfrak{O}/\mathfrak{P}$  over  $\mathfrak{g}/\mathfrak{p}$ . Put  $M = F[s]$ ,  $\mathfrak{o} = \mathfrak{O} \cap M$ , and  $\mathfrak{h} = \mathfrak{P} \cap M$ . Then we easily see that  $\mathfrak{o}/\mathfrak{h}$  can be identified with  $\mathfrak{O}/\mathfrak{P}$ , so that  $n^2/e = [\mathfrak{o}/\mathfrak{h} : \mathfrak{g}/\mathfrak{p}] \leq [M : F] \leq n$ . Since  $e \leq n$ , we thus obtain  $e = n = [\mathfrak{o}/\mathfrak{h} : \mathfrak{g}/\mathfrak{p}] = [\mathfrak{O}/\mathfrak{P} : \mathfrak{g}/\mathfrak{p}]$ . Since  $z^n \in \pi\mathfrak{O}^\times$  with a prime element  $\pi$  of  $F$ , we have  $n\lambda(z) = \lambda(\pi) = n$ , so that  $\lambda(z) = 1$ , which implies that  $\lambda(D^\times) = \mathbf{Z}$ . We also note that  $[M : F] = n$ , and so  $M$  is unramified over  $F$ , which proves (8). We have  $\mathfrak{g} = \text{Tr}_{M/F}(\mathfrak{o}) \subset \text{Tr}_{D/F}(\mathfrak{O})$ . Combining this with Theorem 21.16(4), we obtain (6).

Finally, to prove (7), let  $b \in \mathfrak{P}$ . Then  $\lambda(b) > 0$  and it is a well-known fact (see Exercise 1, (c) at the end of Section 9) that the minimal polynomial of  $b$  over  $F$  (that is,  $g_b$  in the proof of Theorem 21.16) has coefficients in  $\mathfrak{p}$  except for the highest one, and hence the same is true with  $h_b$ . Therefore  $\text{Tr}_{D/F}(\mathfrak{P}) \subset$

$\mathfrak{p}$ . This means that  $\mathfrak{P}^{1-n} = \mathfrak{p}^{-1}\mathfrak{P} \subset \mathfrak{Y}$ . Clearly  $\mathfrak{Y}$  is a right  $\mathfrak{D}$ -ideal, so that  $\mathfrak{Y} = \mathfrak{P}^k$  with  $k \leq 1 - n$ . Now  $\mathfrak{p}^{-1} = \text{Tr}_{D/F}(\mathfrak{p}^{-1}\mathfrak{D}) = \text{Tr}_{D/F}(\mathfrak{P}^{-n})$ , and therefore  $k > -n$ , so that  $k = 1 - n$ . This proves the first equality of (7). The second one follows from (6), since  $\mathfrak{D} \subset \mathfrak{P}^{1-n}$  and  $\text{Tr}_{D/F}(\mathfrak{Y}) \subset \mathfrak{g}$ . This completes the proof.

**Lemma 21.18.** *Let  $D$  and  $\mathfrak{D}$  be as in Theorem 21.17; let  $V$  be a free left  $D$ -module of rank  $r$ , and  $H$  an  $\mathfrak{D}$ -submodule of  $V$  that is a  $\mathfrak{g}$ -lattice in  $V$ . Then  $H$  is a free  $\mathfrak{D}$ -module of rank  $r$ .*

PROOF. Let  $L = \sum_{i=1}^r \mathfrak{D}e_i$  with a  $D$ -basis  $\{e_i\}$  of  $V$ . Then  $L$  is a  $\mathfrak{g}$ -lattice in  $V$ , and so we can find a nonzero element  $c$  of  $\mathfrak{g}$  such that  $cH \subset L$ . Therefore we may assume that  $H \subset L$ . Define  $p: L \rightarrow \mathfrak{D}$  by  $p(\sum_{i=1}^r a_i e_i) = a_1$  for  $a_i \in \mathfrak{D}$ . Then  $p(H)$  is a left ideal of  $\mathfrak{D}$ . If this ideal is  $\{0\}$ , then  $H \subset \sum_{i=2}^r \mathfrak{D}e_i$ , which is impossible, since  $H$  is a  $\mathfrak{g}$ -lattice in  $V$ . Thus  $p(H) \neq \{0\}$ , and by Theorem 21.17(2), we can put  $p(H) = \mathfrak{D}b$  with  $0 \neq b \in \mathfrak{D}$ . If  $r=1$ , then this shows that  $H = \mathfrak{D}be_1$ , which is the desired result. If  $r > 1$ , we can find an element  $f$  of  $H$  such that  $p(f) = b$ . Given  $x \in H$ , put  $p(x) = ab$  with  $a \in \mathfrak{D}$ , and put also  $y = x - af$ . Then  $y \in H$  and  $p(y) = 0$ . Put  $J = H \cap (\sum_{i=2}^r \mathfrak{D}e_i)$ . Then  $y \in J$ , and hence we easily see that  $H = \mathfrak{D}f \oplus J$ . Applying induction to  $J$ , we obtain our lemma.

**Lemma 21.19.** *Let  $A$  be a semisimple  $F$ -algebra. Given two maximal orders  $\mathfrak{R}$  and  $\mathfrak{S}$  in  $A$ , there always exists an element  $\alpha$  of  $A^\times$  such that  $\alpha\mathfrak{R}\alpha^{-1} = \mathfrak{S}$ .*

PROOF. Let  $A = \bigoplus_{i=1}^m A_i$  with simple algebras  $A_i$ . As shown in the proof of Lemma 21.7, every maximal order of  $A$  is of the form  $\bigoplus_{i=1}^m \mathfrak{R}_i$  with a maximal order  $\mathfrak{R}_i$  of  $A_i$  for each  $i$ . Therefore it is sufficient to prove our lemma when  $A$  is simple, in which case  $A$  is isomorphic to  $M_r(D)$  with a division algebra  $D$ . Take the unique maximal order  $\mathfrak{D}$  in  $D$ . Let  $\mathfrak{R}$  be a maximal order in  $M_r(D)$ . Put  $V = D_r^1$ , and let  $D$  resp.  $M_r(D)$  act on  $V$  by left resp. right multiplication. Then  $M_r(D)$  coincides with the ring of all  $D$ -linear endomorphisms of  $V$ . Let  $L = \mathfrak{D}_r^1$ ,  $H = L\mathfrak{R}$ , and  $\mathfrak{T} = \{\xi \in M_r(D) \mid H\xi \subset H\}$ . Then  $L$  and  $H$  are  $\mathfrak{g}$ -lattices in  $V$ , and  $\mathfrak{T}$  is a ring containing  $\mathfrak{R}$ . Now,  $H$  is a left  $\mathfrak{D}$ -module, and hence, by Lemma 21.18,  $H = \bigoplus_{i=1}^r \mathfrak{D}f_i$  with elements  $f_i$  of  $H$ . Let  $\{e_i\}_{i=1}^r$  be the standard  $D$ -basis of  $V = D_r^1$ . We can then define an element  $\alpha$  of  $M_r(D)$  by  $e_i\alpha = f_i$  for every  $i$ . Then  $L\alpha = H$ . Since  $H\mathfrak{R} \subset H$ , we see that  $L\alpha\mathfrak{R}\alpha^{-1} \subset L$ , which means that  $\alpha\mathfrak{R}\alpha^{-1} \subset M_r(\mathfrak{D})$ . Since  $\mathfrak{R}$  is a maximal order, we obtain  $\alpha\mathfrak{R}\alpha^{-1} = M_r(\mathfrak{D})$ . This proves our lemma.

**Lemma 21.20.** *If  $R = M_n(D)$  and  $S = M_n(\mathfrak{D})$  with  $D$  and  $\mathfrak{D}$  as in Theorem 21.17, then every two-sided  $S$ -ideal is of the form  $cS$  with  $c \in D^\times$ .*

PROOF. Take  $Z = \mathfrak{D}$  and  $S = M_n(\mathfrak{D})$  in Lemma 18.13. Given a two-sided  $S$ -ideal  $W$ , we can find an element  $b \in F^\times$  such that  $bW \subset S$ . By Lemma 18.13,  $bW = M_n(Y)$  with a two-sided ideal  $Y$  of  $\mathfrak{D}$ . By Theorem 21.17(2),  $Y = d\mathfrak{D}$  with  $d \in \mathfrak{D}$ . Then  $W = cS$  with  $c = b^{-1}d$ . This proves our lemma.

Let us now specialize our discussion to the quaternion case.

**Theorem 21.21.** *The notation being as in Theorem 21.17, suppose that  $D$  is a division quaternion algebra; let  $\iota$  be the main involution of  $D$ . Then  $\mathfrak{D}/\mathfrak{P}$  is a field with  $q^2$  elements, and*

$$\begin{aligned} \mathfrak{D} &= \{\alpha \in D \mid \alpha\alpha^\iota \in \mathfrak{g}\}, \quad \mathfrak{P}^m = \{\alpha \in D \mid \alpha\alpha^\iota \in \mathfrak{p}^m\} \quad (m \in \mathbf{Z}), \\ \mathfrak{p}\mathfrak{D} &= \mathfrak{P}^2, \quad \mathfrak{P}^{-1} = \{\alpha \in D \mid \text{Tr}_{D/F}(\alpha\mathfrak{D}) \subset \mathfrak{g}\}, \quad \text{Tr}_{D/F}(\mathfrak{P}^{-1}) = \mathfrak{g}. \end{aligned}$$

Moreover  $D$  has a subfield  $J$  which is an unramified quadratic extension of  $F$  and an element  $\omega$  such that  $D = J + J\omega$ ,  $\mathfrak{D} = \mathfrak{r} + \mathfrak{r}\omega$ ,  $\mathfrak{P} = \mathfrak{D}\omega$ ,  $\omega a = a^\iota\omega$  for every  $a \in J$ , and  $\omega^2$  is a prime element of  $F$ , where  $\mathfrak{r} = \mathfrak{D} \cap J$ .

PROOF. The first half up to the equality  $\text{Tr}_{D/F}(\mathfrak{P}^{-1}) = \mathfrak{g}$  consists of special cases of the assertions of Theorem 21.17. Now Theorem 21.17(8) guarantees an unramified quadratic extension  $J$  of  $F$  as a subfield of  $D$ . By Lemma 20.4 we can find an element  $\omega$  of  $D$  such that  $D = J + J\omega$ ,  $\omega a = a^\iota\omega$  for every  $a \in J$ , and  $\omega^2 \in F^\times$ . By Theorem 20.8(i) the isomorphism-class of  $\{J, \gamma\}$  with  $\gamma \in F^\times$  is determined by the coset  $\gamma N_{J/F}(J^\times)$  in  $J^\times / N_{J/F}(J^\times)$ . Since  $J$  is unramified over  $F$  and  $\{J, 1\} \cong M_2(F)$  by (20.6), Theorem 9.10(ii) allows us to assume that  $\omega^2$  is a prime element of  $F$ . Put  $\mathfrak{r} = \mathfrak{D} \cap J$ ,  $\mathfrak{A} = \mathfrak{r} + \mathfrak{r}\omega$ , and  $\mathfrak{B} = \{\alpha \in D \mid \text{Tr}_{D/F}(\alpha\mathfrak{A}) \subset \mathfrak{g}\}$ . Then  $\mathfrak{A} \subset \mathfrak{D} \subset \mathfrak{P}^{-1} \subset \mathfrak{B}$ . Now every element of  $D$  can be written  $c + \omega^{-1}d$  with  $c$  and  $d$  in  $J$ . This belongs to  $\mathfrak{B}$  if and only if  $\text{Tr}_{J/F}(\mathfrak{r}c) \subset \mathfrak{g}$  and  $\text{Tr}_{J/F}(\mathfrak{r}d) \subset \mathfrak{g}$ , which is the case if and only if  $c, d \in \mathfrak{r}$  since  $J$  is unramified over  $F$ . Thus  $\mathfrak{B} = \mathfrak{r}\omega^{-1} + \mathfrak{r}$ , and hence  $[\mathfrak{B} : \mathfrak{A}] = q^2 = [\mathfrak{D} : \mathfrak{P}]$ . This shows that  $\mathfrak{A} = \mathfrak{D}$  and  $\mathfrak{P}^{-1} = \mathfrak{B}$ , which completes the proof.

**Theorem 21.22.** *Let  $F$  be either  $\mathbf{R}$  or a finite algebraic extension of  $\mathbf{Q}_p$  with a prime number  $p$ . Then there exists only one division quaternion algebra over  $F$  up to isomorphism. It is represented by  $\mathbf{H}$  if  $F = \mathbf{R}$ ; for a nonarchimedean local field  $F$ , it is given as  $\{J, \pi\}$  with an unramified quadratic extension  $J$  of  $F$  and a prime element  $\pi$  of  $F$ .*

PROOF. Let  $A$  be a division quaternion algebra over  $\mathbf{R}$ . Take any  $z \in A$ ,  $z \notin \mathbf{R}$ . Then  $\mathbf{R}[z]$  is an algebraic extension of  $\mathbf{R}$  by Lemma 18.18(i), and so  $\mathbf{R}[z] \cong \mathbf{C}$ . By Lemma 20.4,  $A \cong \{\mathbf{C}, \gamma\}$  with  $\gamma \in \mathbf{R}^\times$ . Now  $N_{\mathbf{C}/\mathbf{R}}(\mathbf{C}^\times)$  consists of all positive real numbers. Thus, by Theorem 20.8(i),  $A \cong M_2(\mathbf{R})$  if  $\gamma > 0$ . If  $\gamma < 0$ , then  $A \cong \{\mathbf{C}, -1\} = \mathbf{H}$ . Suppose  $F$  is local. That a division quaternion algebra over  $F$  can be given as  $\{J, \pi\}$  is proved in Theorem 21.21.

If  $\pi'$  is another prime element of  $F$ , then  $\pi'/\pi \in \mathfrak{g}^\times$ , which is contained in  $N_{J/F}(J^\times)$  by Theorem 9.10(ii), and so  $\{J, \pi'\} \cong \{J, \pi\}$  by Theorem 20.8(i). This completes the proof.

**Theorem 21.23.** *Let  $B$  be a quaternion algebra over a local field  $F$ . Then the following assertions hold:*

(i)  $N_{B/F}(B^\times) = F^\times$ .

(ii) *Every quadratic extension of  $F$  can be  $F$ -linearly embedded into  $B$ .*

PROOF. These are obvious if  $B$  is a matrix algebra; so we take  $B$  to be  $D$  of Theorem 21.21. Take  $J$  and  $\omega$  as in that theorem. Then  $\omega\omega^\iota = -\omega^2$ , which is a prime element of  $F$ . Now  $F^\times$  is generated by  $\mathfrak{g}^\times$  and any prime element. By Theorem 9.10(ii),  $\mathfrak{g}^\times = N_{J/F}(J^\times) \subset N_{B/F}(B^\times)$ , and so we obtain (i). Next let  $K$  be a quadratic extension of  $F$ . If  $K$  is ramified over  $F$ , then  $N_{K/F}(K^\times) \neq F^\times$ . Indeed suppose  $N_{K/F}(K^\times) = F^\times$ ; then for every  $a \in \mathfrak{g}^\times$  there is an element  $b$  of  $K^\times$  such that  $N_{K/F}(b) = a$ . Then  $b \in \mathfrak{r}^\times$ , and so  $\mathfrak{g}^\times = N_{K/F}(\mathfrak{r}^\times)$ , which contradicts (21.2a). Therefore  $N_{K/F}(K^\times) \neq F^\times$ . The same holds also when  $K$  is unramified over  $F$  in view of Theorem 9.10(ii). Therefore in either case we can find an element  $\gamma \in F^\times$  not contained in  $N_{K/F}(K^\times)$ . Then  $\{K, \gamma\}$  is a division quaternion algebra, and must be isomorphic to  $B$  by Theorem 21.22. This proves (ii).

Returning to Theorem 21.15, suppose  $K$  is ramified over  $F$ . By (ii) above and Theorem 20.8(i) the isomorphism classes of quaternion algebras over  $F$  correspond to  $F^\times/N_{K/F}(K^\times)$ . Since we have exactly two isomorphism classes, we obtain Theorem 21.15. Let  $\pi$  be a prime element of  $K$ . Then  $N_{K/F}(\pi)$  is a prime element of  $F$ , and so  $F^\times = \bigcup_{n \in \mathbf{Z}} N_{K/F}(\pi)^n \mathfrak{g}^\times$ . Since  $N_{K/F}(K^\times) = \bigcup_{n \in \mathbf{Z}} N_{K/F}(\pi)^n N_{K/F}(\mathfrak{r}^\times)$ , we obtain (21.2b).

**Lemma 21.24.** *Let  $D$  be a division algebra over a local field,  $\mathfrak{D}$  its unique maximal order, and  $T$  the group consisting of all upper triangular elements of  $GL_n(D)$ ; put  $\mathfrak{E} = \mathfrak{E}^n = GL_n(\mathfrak{D})$ . Then  $GL_n(D) = T\mathfrak{E}$ .*

PROOF. This is obvious if  $n = 1$ . We prove the general case by induction on  $n$ . We let  $D$  resp.  $M_n(D)$  act on  $D_n^1$  by left resp. right multiplication. Suppose  $n > 1$ ; let  $\{e_i\}_{i=1}^n$  be the standard basis of  $D_n^1$ . Given  $\alpha \in GL_n(D)$ , put  $x = e_n \alpha = \sum_{i=1}^n x_i e_i$ . Then  $x$  is the last row of  $\alpha$ . By Theorem 21.17(2) we have  $\sum_{i=1}^n x_i \mathfrak{D} = x_k \mathfrak{D}$  with some  $k$ . Put  $x_k = d$  and  $y = d^{-1}x$ . We easily see that  $\mathfrak{D}y + \sum_{k \neq i} \mathfrak{D}e_i = \mathfrak{D}_n^1$ , and so we can find an element  $\varepsilon$  of  $GL_n(\mathfrak{D})$  such that  $e_n \varepsilon = y$ . Then  $e_n \alpha \varepsilon^{-1} = d e_n$ , which means that  $\alpha \varepsilon^{-1} = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$  with  $a \in GL_{n-1}(D)$  and  $b \in D_1^{n-1}$ . By induction we can put  $a = \beta \gamma$  with an upper triangular  $\beta$  and  $\gamma \in \mathfrak{E}^{n-1}$ . Put  $\zeta = \text{diag}[\gamma, 1]$ . Then  $\alpha \varepsilon^{-1} \zeta^{-1} \in T$ , which proves our lemma, as  $\zeta \varepsilon \in \mathfrak{E}^n$ .

**21.25.** Let  $V$  be a finite-dimensional vector space over a local or global field  $F$ . Given  $\mathfrak{g}$ -lattices  $L$  and  $M$  in  $V$ , we can associate a  $\mathfrak{g}$ -ideal  $[L/M]$  with the following properties:

$$(21.3a) \quad [L/M][M/N] = [L/N],$$

$$(21.3b) \quad [L/M]_v = [L_v/M_v] \text{ for every } v \in \mathbf{h} \text{ if } L \text{ and } M \text{ are } \mathfrak{g}\text{-lattices in the global case,}$$

$$(21.3c) \quad [L/L\alpha] = \det(\alpha)\mathfrak{g} \text{ if } \alpha \in GL_F(V),$$

$$(21.3d) \quad [L/M] \subset \mathfrak{g} \text{ if } M \subset L,$$

$$(21.3e) \quad [L : M] = N([L/M]) \text{ if } M \subset L,$$

$$(21.3f) \quad [L/M]L \subset M \text{ if } M \subset L.$$

To show these, put  $n = [V : F]$ . Given  $L$  and  $M$  in the local case, we can find an element  $\alpha \in GL(V)$  such that  $L\alpha = M$ , since both  $L$  and  $M$  are free  $\mathfrak{g}$ -modules of rank  $n$ ; see Theorem 5.3. If  $L\beta = M$  with another  $\beta \in GL(V)$ , then both  $\alpha\beta^{-1}$  and  $\beta\alpha^{-1}$  can be represented by elements of  $M_n(\mathfrak{g})$ , and so  $\alpha\beta^{-1} \in GL_n(\mathfrak{g})$ . Thus  $\det(\alpha)\mathfrak{g}$  depends only on  $L$  and  $M$ . Therefore we define  $[L/M]$  in the local case by (21.3c) and define it in the global case by (21.3b). Then (21.3a) and (21.3d) are clear. As for (21.3e) and (21.3f), it is sufficient to prove it in the local case. Then Theorem 5.1 reduces the problem to the one-dimensional case, and we easily obtain the desired result.

**Lemma 21.26.** *Let  $A$  be a central simple algebra over a local or global field  $F$ , and  $\mathfrak{a}$  a  $\mathfrak{g}$ -lattice in  $A$ . Then  $[\mathfrak{a}/\mathfrak{a}\beta] = N_{A/F}(\beta)^n\mathfrak{g}$ , where  $n = [A : F]^{1/2}$ .*

PROOF. Let  $\rho$  be a right regular representation of  $A$  over  $F$ . Then (21.3c) shows that  $[\mathfrak{a}/\mathfrak{a}\beta] = \det[\rho(\beta)]\mathfrak{g}$  for every  $\beta \in A^\times$ . Since  $\det[\rho(\beta)] = N_{A/F}(\beta)^n$  as can be seen from (19.9) and (19.10), we obtain our lemma.

**Theorem 21.27.** *Let  $A$  be a quaternion algebra over a global field  $F$  and  $\mathfrak{o}$  an order in  $A$ . Let  $d(A/F)$  be the product of all the prime ideals in  $F$  corresponding to the primes  $v \in \mathbf{h}$  such that  $A_v$  is a division algebra. For a  $\mathfrak{g}$ -lattice  $\mathfrak{a}$  in  $A$  put*

$$(21.4) \quad \tilde{\mathfrak{a}} = \{x \in A \mid \text{Tr}_{A/F}(x\mathfrak{a}) \subset \mathfrak{g}\}.$$

*Then  $\mathfrak{o}$  is maximal if and only if  $[\tilde{\mathfrak{o}}/\mathfrak{o}] = d(A/F)^2$ .*

PROOF. We easily see that  $\tilde{\mathfrak{a}}_v = \{x \in A_v \mid \text{Tr}_{A_v/F_v}(x\mathfrak{a}_v) \subset \mathfrak{g}_v\}$  for every  $v \in \mathbf{h}$ . Suppose  $\mathfrak{o}$  is maximal; then by Lemma 21.7(ii),  $\mathfrak{o}_v$  is a maximal order in  $A_v$ . By Theorem 21.21, if  $A_v$  is a division algebra, then  $[\tilde{\mathfrak{o}}_v/\mathfrak{o}_v] = \pi_v^2\mathfrak{g}_v$  with a prime element  $\pi_v$  of  $F_v$ . If  $A_v$  is not a division algebra, Lemmas 21.4 and 21.19 allow us to put  $A_v = M_2(F_v)$  and  $\mathfrak{o}_v = M_2(\mathfrak{g}_v)$ . Then we easily see that  $[\tilde{\mathfrak{o}}_v/\mathfrak{o}_v] = \mathfrak{g}_v$ . From these and (21.3b) we obtain  $[\tilde{\mathfrak{o}}/\mathfrak{o}] = d(A/F)^2$ . Given an arbitrary order  $\mathfrak{o}_1$  in  $A$ , take a maximal order  $\mathfrak{o}$  containing  $\mathfrak{o}_1$ .

Then  $\mathfrak{o}_1 \subset \mathfrak{o} \subset \tilde{\mathfrak{o}} \subset \tilde{\mathfrak{o}}_1$ , and so if  $[\tilde{\mathfrak{o}}_1/\mathfrak{o}_1] = [\tilde{\mathfrak{o}}/\mathfrak{o}]$ , then  $\mathfrak{o}_1 = \mathfrak{o}$ , that is,  $\mathfrak{o}_1$  is maximal. This completes the proof.

We call  $d(A/F)$  the **discriminant ideal** of  $A$ .

## QUADRATIC FORMS

## 22. Algebraic theory of quadratic forms

**22.1.** We take a base field  $F$  and consider a finite-dimensional vector space  $V$  over  $F$  and an  $F$ -valued  $F$ -bilinear form  $\varphi : V \times V \rightarrow F$ . We call, as usual,  $\varphi$  **symmetric** if  $\varphi(x, y) = \varphi(y, x)$  for every  $x, y \in V$ . We put then

$$(22.1) \quad \varphi[x] = \varphi(x, x) \quad (x \in V).$$

In this book we make the convention that *whenever we speak of  $\varphi$  of this type, the characteristic of  $F$  is not 2*. Traditionally  $\varphi[x]$  is called **the quadratic form** associated to the symmetric form  $\varphi(x, y)$ , but we use the same letter  $\varphi$  for both objects, since one determines the other uniquely, because of the formula

$$(22.2) \quad 2\varphi(x, y) = \varphi[x + y] - \varphi[x] - \varphi[y].$$

We call the pair  $(V, \varphi)$  a **quadratic space over  $F$** . We call  $\varphi$  or  $(V, \varphi)$  **isotropic** if  $\varphi[x] = 0$  for some  $x \in V, x \neq 0$ ; we call  $\varphi$  or  $(V, \varphi)$  **anisotropic** if  $\varphi[x] = 0$  only for  $x = 0$ . (This means that  $\varphi$  is anisotropic if  $V = \{0\}$ .) We call a subspace  $U$  of  $V$  **totally  $\varphi$ -isotropic** if  $\varphi(x, y) = 0$  for every  $x, y \in U$ . We also call  $\varphi$  **nondegenerate** on  $V$  if there is no nonzero element  $x \in V$  such that  $\varphi(x, V) = 0$ . We call then  $(V, \varphi)$  **nondegenerate**. Whenever we speak of a nondegenerate quadratic space  $(V, \varphi)$ , we assume that  $V \neq \{0\}$ . For a subspace  $X$  of  $V$  on which  $\varphi$  is nondegenerate, we put

$$(22.3) \quad X^\perp = \{y \in V \mid \varphi(y, x) = 0 \text{ for every } x \in X\}.$$

This is a subspace of  $V$ , and is naturally called the **orthogonal complement** of  $X$  in  $V$  with respect to  $\varphi$ . We use this symbol  $X^\perp$  whenever  $V$  and  $\varphi$  are clear from the context.

For a vector space  $W$  over  $F$  and an  $F$ -linear map  $\alpha$  of  $V$  into  $W$  we denote by  $x\alpha$  the image of  $x \in V$  under  $\alpha$ . If  $\beta$  is an  $F$ -linear map of  $W$  into a vector space  $X$  over  $F$ , then the image of  $x\alpha$  under  $\beta$  is  $(x\alpha)\beta$ , and so the composite map of  $\alpha$  and  $\beta$  is  $\alpha\beta$ . Thus we have  $(x\alpha)\beta = x(\alpha\beta)$ .

Assuming  $\varphi$  to be nondegenerate, we define groups  $O^\varphi$  and  $SO^\varphi$  by



$$O^\varphi = O(\varphi) = O^\varphi(V) = \{\alpha \in GL_F(V) \mid \varphi[x\alpha] = \varphi[x] \text{ for every } x \in V\},$$

$$SO^\varphi = SO(\varphi) = SO^\varphi(V) = \{\alpha \in O^\varphi(V) \mid \det(\alpha) = 1\},$$

where  $GL_F(V)$  denotes the group of all  $F$ -linear automorphisms of  $V$ . These are called the **orthogonal group** of  $\varphi$  and the **special orthogonal group** of  $\varphi$  respectively. From (22.2) we see that  $\varphi(x\alpha, y\alpha) = \varphi(x, y)$  for every  $\alpha \in O^\varphi(V)$  and every  $x, y \in V$ . We have  $[O^\varphi : SO^\varphi] = 2$ , as  $O^\varphi$  contains an element of determinant  $-1$ , which can be shown as follows. Since  $\varphi$  is nondegenerate,  $\varphi[x] \neq 0$  for some  $x \in F$ . (Otherwise (22.2) shows that  $\varphi = 0$ .) Then  $V = Fx \oplus (Fx)^\perp$ . Define an element  $\gamma$  of  $GL_F(V)$  by  $x\gamma = -x$  and  $y\gamma = y$  for every  $y \in (Fx)^\perp$ . Then  $\gamma \in O^\varphi$  and  $\det(\gamma) = -1$ .

Let  $X$  be a subspace of  $V$  and  $\psi$  the restriction of  $\varphi$  to  $X$ . If  $\psi$  is nondegenerate, the symbols  $O^\psi(X)$  and  $SO^\psi(X)$  are meaningful. In our later treatment, however, we will often write these  $O^\varphi(X)$  and  $SO^\varphi(X)$  without introducing the symbol  $\psi$ .

Given two quadratic spaces  $(V, \varphi)$  and  $(V', \varphi')$  over  $F$ , we say that  $(V, \varphi)$  is *isomorphic* to  $(V', \varphi')$  if  $\varphi[x] = \varphi'[xf]$  for every  $x \in V$  with an  $F$ -linear bijection  $f$  of  $V$  onto  $V'$ . We also denote by  $(V, \varphi) \oplus (V', \varphi')$  the quadratic space  $(V \oplus V', \varphi \oplus \varphi')$  given by  $(\varphi \oplus \varphi')(x + x', y + y') = \varphi(x, y) + \varphi'(x', y')$  for  $x, y \in V$  and  $x', y' \in V'$ . Clearly  $\varphi \oplus \varphi'$  is nondegenerate if and only if both  $\varphi$  and  $\varphi'$  are nondegenerate. In such a case, we can view  $O^\varphi \times O^{\varphi'}$  as a subgroup of  $O^{\varphi \oplus \varphi'}$ . The element  $(\alpha, \beta)$  of  $O^\varphi \times O^{\varphi'}$  viewed as an element of  $O^{\varphi \oplus \varphi'}$  will be denoted by  $\alpha \times \beta$  or by  $(\alpha, \beta)$ .

**Theorem 22.2.** *Let  $(V, \varphi) = (S, \sigma) \oplus (T, \tau) = (S', \sigma') \oplus (T', \tau')$  with nondegenerate  $\varphi$ . If  $(S, \sigma)$  is isomorphic to  $(S', \sigma')$ , then  $(T, \tau)$  is isomorphic to  $(T', \tau')$ .*

PROOF. If there is an element  $f$  of  $O^\varphi$  such that  $Sf = S'$ , then  $f$  gives an isomorphism of  $(T, \tau)$  to  $(T', \tau')$ , since  $T = S^\perp$  and  $T' = (S')^\perp$ . We prove the existence of such an  $f$  by induction on  $\dim(S)$ . Suppose  $\dim(S) = 1$ ; then we can put  $S = Fx$  and  $S' = Fy$  with elements  $x$  and  $y$  such that  $\varphi[x] = \varphi[y] \neq 0$ . Since  $\varphi[x + y] + \varphi[x - y] = 4\varphi[x] \neq 0$ , we have  $\varphi[x + y] \neq 0$  or  $\varphi[x - y] \neq 0$ . Changing  $y$  for  $-y$  if necessary, we may assume that  $\varphi[x + y] \neq 0$ . Let  $U = (F(x + y))^\perp$ . Define  $f \in GL_F(V)$  by  $uf = -u$  for  $u \in U$  and  $(x + y)f = x + y$ . Clearly  $f \in O^\varphi$ . Since  $x - y \in U$ , we have  $(x - y)f = y - x$ , so that  $xf = y$ , which proves the case  $\dim(S) = 1$ . Next suppose  $\dim(S) = m > 1$ . Let  $h$  be an isomorphism of  $(S, \sigma)$  to  $(S', \sigma')$ . Take any  $x \in S$  such that  $\varphi[x] \neq 0$ ; put  $y = xh$ ,  $R = S \cap (Fx)^\perp$ , and  $R' = Rh$ . Then  $S = Fx \oplus R$  and  $S' = Fy \oplus R'$ . By the above result we can find an element  $g$  of  $O^\varphi$  such that  $Fyg = Fx$ . Now both  $R$  and  $R'g$  are contained in  $(Fx)^\perp$ , and  $hg$  gives a bijection of  $R$  onto  $R'g$  that leaves  $\varphi$  invariant. Since  $\dim(R) = m - 1$ , by induction  $O^\varphi((Fx)^\perp)$  has an element  $k$  that maps

$R$  onto  $R'g$ . Extend  $k$  to an element  $\ell$  of  $GL_F(V)$  by putting  $x\ell = x$ . Then  $\ell \in O^\varphi$  and we see that  $S\ell g^{-1} = S'$ , which completes the proof.

This is called **Witt's theorem**. It can be generalized to the case of a hermitian form over a division algebra with an involution; see [S97, Theorem 1.2 and Lemma 1.3], for example.

**Lemma 22.3.** *Given  $(V, \varphi)$  with a nondegenerate  $\varphi$  as above, let  $I$  be a totally isotropic subspace of  $V$  of dimension  $m$ , and let  $\{e_i\}_{i=1}^m$  be an  $F$ -basis of  $I$ . Then we can find a subspace  $Z$  of  $V$  and a set of elements  $\{f_i\}_{i=1}^m$  such that*

$$(22.4a) \quad V = Z + \sum_{i=1}^m (Fe_i + Ff_i),$$

$$(22.4b) \quad \varphi(e_i, e_j) = \varphi(f_i, f_j) = 0, \quad 2\varphi(e_i, f_j) = \delta_{ij} \quad \text{for every } i \text{ and } j,$$

$$(22.4c) \quad Z = \{v \in V \mid \varphi(e_i, v) = \varphi(f_i, v) = 0 \quad \text{for every } i\}.$$

*Conversely suppose that  $V$  has  $2m$  elements  $e_i, f_i$  satisfying (22.4b); put  $I = \sum_{i=1}^m Fe_i$  and  $I' = \sum_{i=1}^m Ff_i$ ; define  $Z$  by (22.4c); let  $\zeta$  denote the restriction of  $\varphi$  to  $Z$ . Then  $I$  and  $I'$  are totally isotropic subspaces of  $V$  of dimension  $m$ ,  $V = Z \oplus I' \oplus I$ , and  $\zeta$  is nondegenerate.*

**PROOF.** The converse part can easily be verified. We prove the first part by induction on  $m$ . Let  $e_1$  be a nonzero element of  $V$  such that  $\varphi[e_1] = 0$ . Since  $\varphi$  is nondegenerate, we can find an element  $x$  such that  $\varphi(e_1, x) = 1$ . Put  $f_1 = x - 2^{-1}\varphi[x]e_1$ . Then  $\varphi[f_1] = 0$  and  $\varphi(e_1, f_1) = 1$ . Given such  $\{e_1, f_1\}$ , define  $Z$  by (22.4c) with  $m = 1$ . Then the converse part of our lemma gives (22.4a) in the case  $m = 1$ . If we have  $I = \sum_{i=1}^m Fe_i$  with  $m > 1$ , then the  $e_i$  for  $i > 1$  belong to the subspace  $Z$  just defined for  $\{e_1, f_1\}$ . Applying our induction to  $Z$  and its subspace  $\sum_{i=2}^m Fe_i$ , we obtain our lemma.

In the setting of the above lemma we call the expression of (22.4a) with  $0 \leq m \in \mathbf{Z}$  a **weak Witt decomposition** (of  $V$  with respect to  $\varphi$ ); we call it a **Witt decomposition** if the restriction of  $\varphi$  to  $Z$  is anisotropic. In particular, if  $Z = \{0\}$ , we call it a **split Witt decomposition** and say that  $(V, \varphi)$  is **split**. If (22.4a) is a Witt decomposition, we call  $Z$  a **core subspace** of  $V$  with respect to  $\varphi$ , and call  $\dim(Z)$  the **core dimension** of  $(V, \varphi)$ , or simply of  $\varphi$ .

**Lemma 22.4.** *For a nondegenerate quadratic space  $(V, \varphi)$  the following assertions hold:*

(i)  *$V$  has a Witt decomposition.*

(ii) *If (22.4a) is a Witt decomposition and  $\zeta$  is the restriction of  $\varphi$  to  $Z$ , then the integer  $m$  and the isomorphism class of  $(Z, \zeta)$  are completely determined by the isomorphism class of  $(V, \varphi)$ .*

(iii) *Every totally isotropic subspace of  $V$  is contained in a totally isotropic subspace of  $V$  of dimension  $m$  with the integer  $m$  determined as in (ii).*

PROOF. There is no problem if  $\varphi$  is anisotropic. Suppose  $V$  has a nontrivial totally isotropic subspace  $X$ . Clearly  $X$  is contained in a maximal totally isotropic subspace  $I$  of  $V$ . By Lemma 22.3, we can find a weak Witt decomposition (22.4a) with  $I$  in place of  $\sum_{i=1}^m Fe_i$ . If  $Z$  contains a nonzero vector  $g$  such that  $\varphi[g] = 0$ , then  $Fg + I$  is totally isotropic, which is a contradiction as  $I$  is maximal. Therefore  $\varphi$  is anisotropic on  $Z$ , so that (22.4a) is a Witt decomposition. This proves (i). Let  $V = Z' + \sum_{i=1}^n (Fe'_i + Ff'_i)$  be another Witt decomposition; suppose  $n \geq m$ . Then, by Theorem 22.2, we can find an  $F$ -linear bijection  $f$  of  $Z$  onto  $Z' + \sum_{i=1}^{n-m} (Fe'_i + Ff'_i)$  such that  $\varphi[xf] = \varphi[x]$  for every  $x \in Z$ . Since  $\varphi$  is anisotropic on  $Z$ , we have  $m = n$ , and at the same time we obtain (ii). Assertion (iii) is also proved, as we have seen that  $X \subset I$ .

**Lemma 22.5.** (i) *Given  $(V, \varphi)$  with nondegenerate  $\varphi$ , let  $\alpha$  and  $\beta$  be  $F$ -linear injections of a vector space  $W$  into  $V$  such that  $\varphi[x\alpha] = \varphi[x\beta]$  for every  $x \in W$ . Suppose that  $\varphi$  is nondegenerate on  $W\alpha$ . Then there exists an element  $\gamma$  of  $O^\varphi$  such that  $\alpha\gamma = \beta$ . Moreover, such a  $\gamma$  can be taken from  $SO^\varphi$  if  $\dim(V) > \dim(W)$ .*

(ii) *Given  $(V, \varphi)$  as in (i), let  $h$  and  $k$  be nonzero elements of  $V$  such that  $\varphi[h] = \varphi[k]$ . Then there exists an element  $\gamma$  of  $O^\varphi$  such that  $h\gamma = k$ . Moreover such a  $\gamma$  can be taken from  $SO^\varphi$  if  $\varphi[h] \neq 0$  and  $\dim(V) > 1$ , or if  $\varphi[h] = 0$  and  $\dim(V) > 2$ .*

(iii) *With  $(V, \varphi)$  as in (i), suppose that  $\varphi$  is isotropic and  $V$  has core dimension  $t$ ; let  $U = (Fy)^\perp$  with an element  $y$  of  $V$  such that  $\varphi[y] \neq 0$ . Then  $U$  has core dimension  $\leq t + 1$ .*

PROOF. We can find an  $F$ -linear bijection  $\xi$  of  $W\alpha$  to  $W\beta$  by  $(x\alpha)\xi = x\beta$  for  $x \in W$ . Then  $\varphi[y\xi] = \varphi[y]$  for every  $y \in W\alpha$ . Applying Theorem 22.2 to  $V = (W\alpha) + (W\alpha)^\perp = (W\beta) + (W\beta)^\perp$ , we can extend  $\xi$  to an element  $\gamma$  of  $O^\varphi$ . Then  $\alpha\gamma = \beta$ . If  $\dim(V) > \dim(W)$ , we can modify  $\gamma$  by a suitable element of  $O^\varphi((W\alpha)^\perp)$  so that  $\det(\gamma) = 1$ . This proves (i).

As for (ii), suppose  $\varphi[h] \neq 0$ ; define  $\alpha, \beta : F \rightarrow V$  by  $x\alpha = xh$  and  $x\beta = xk$  for  $x \in F$ . Then our assertion follows from (i). Suppose  $\varphi[h] = 0$ . Then, by Lemma 22.3,  $V$  has weak Witt decompositions  $V = X + Fh + Fg = Y + Fk + F\ell$  with subspaces  $X, Y$  and elements  $g, \ell$ . By Theorem 22.2 we can find an element  $\gamma$  of  $O^\varphi$  such that  $X\gamma = Y$ ,  $h\gamma = k$ , and  $g\gamma = \ell$ . If  $X \neq \{0\}$ , then we can take  $\gamma$  from  $SO^\varphi$  by modifying it by a suitable element of  $O^\varphi(X)$ .

To prove (iii), let the notation be as in (22.4a, b, c). Let  $z = e_1 + \varphi[y]f_1$ . Then  $\varphi[z] = \varphi[y]$ , and so  $z = y\gamma$  with  $\gamma \in O^\varphi$  by (ii). Then  $U\gamma = (Fz)^\perp$ ,

and clearly the core dimension of  $(Fz)^\perp$  is  $\leq t + 1$ . This completes the proof.

**22.6.** Let us now express various things by matrices. Given  $(V, \varphi)$  with degenerate or nondegenerate  $\varphi$ , take an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $V$ . For  $x = \sum_{i=1}^n \xi_i e_i \in V$  with  $\xi_i \in F$ , let  $x_0$  be the element of  $F_n^1$  whose components are  $\xi_1, \dots, \xi_n$ . Let  $\Phi$  be the  $n \times n$ -matrix  $[\varphi(e_i, e_j)]_{i,j=1}^n$ . Then  ${}^t\Phi = \Phi$  and  $\varphi(x, y) = x_0 \Phi \cdot {}^t y_0$ . We call  $\Phi$  the matrix that represents  $\varphi$  with respect to  $\{e_i\}_{i=1}^n$ , or simply a matrix representing  $\varphi$  when the basis is not specified. Clearly  $\varphi$  is nondegenerate if and only if  $\det(\Phi) \neq 0$ . Hereafter, we will often (but not always) use the same letter for a quadratic form and the matrix representing it when the basis is fixed. If we change the basis, then  $\Phi$  is changed into  $\alpha \Phi \cdot {}^t \alpha$  with  $\alpha \in GL_n(F)$ . We can define an isomorphism  $\alpha \mapsto \alpha_0$  of  $GL_F(V)$  onto  $GL_n(F)$  by  $(x\alpha)_0 = x_0 \alpha_0$ . If  $\varphi$  is nondegenerate, the map  $\alpha \mapsto \alpha_0$  gives an isomorphism of  $O^\varphi$  onto the group

$$(22.5) \quad O(\Phi) = \{\beta \in GL_n(F) \mid \beta \Phi \cdot {}^t \beta = \Phi\}.$$

Naturally we put  $SO(\Phi) = Q(\Phi) \cap SL_n(F)$ . If  $(W, \psi) = (V, \varphi) \oplus (V', \varphi')$  and  $\varphi$  resp.  $\varphi'$  is represented by  $\Phi$  resp.  $\Phi'$ , then  $\psi$  is represented by  $\text{diag}[\Phi, \Phi']$ .

It is an easy exercise to show that every degenerate or nondegenerate  $\varphi$  can be represented by a diagonal matrix. In particular, we have a diagonal representation of a nondegenerate  $\varphi$  with respect to a basis  $\{h_i\}_{i=1}^n$  if and only if  $\varphi(h_i, h_j) = c_i \delta_{ij}$  for every  $i$  and  $j$  with  $c_i \in F^\times$ . In such a case we call  $\{h_i\}_{i=1}^n$  an **orthogonal basis** of  $V$  with respect to  $\varphi$ .

If  $V = \sum_{i=1}^m (Ff_i + Fe_i)$  is a split Witt decomposition, we will often use the expression  $(H_m, 2^{-1}\eta_m)$  instead of  $(V, \varphi)$ , where

$$(22.6) \quad \eta_m = \begin{bmatrix} 0 & 1_m \\ 1_m & 0 \end{bmatrix}.$$

Thus  $2^{-1}\eta_m$  is the matrix representing  $\varphi$  with respect to the basis  $\{f_1, \dots, f_m, e_1, \dots, e_m\}$ . Also we will often put  $I' = \sum_{i=1}^m Ff_i$  and  $I = \sum_{i=1}^m Fe_i$ , so that  $H_m = I' \oplus I$ . More generally, let the notation be as in (22.4a) and let  $\zeta_0$  be the matrix representing  $\zeta$  with respect to an  $F$ -basis of  $Z$ ; then both

$$(22.6a) \quad \begin{bmatrix} 0 & 0 & 1_m \\ 0 & \zeta_0 & 0 \\ 1_m & 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \zeta_0 & 0 & 0 \\ 0 & 0 & 1_m \\ 0 & 1_m & 0 \end{bmatrix}$$

represent  $\varphi$ .

Suppose now  $\varphi$  is nondegenerate; put  $F^{\times 2} = \{a^2 \mid a \in F^\times\}$ . Take  $\Phi$  as above. Since  $\det(\alpha \Phi \cdot {}^t \alpha) \in \det(\Phi) F^{\times 2}$ , the coset  $(-1)^{n(n-1)/2} \det(\Phi) F^{\times 2}$  in  $F^\times / F^{\times 2}$  is completely determined by  $\varphi$ . We call this coset the **discriminant** (coset) of  $\varphi$ , or of  $(V, \varphi)$ , and denote it by  $\delta_0(\varphi)$  or  $\delta_0(V, \varphi)$ . The factor  $(-1)^{n(n-1)/2}$  may look artificial, but it merely means  $(-1)^{n/2}$  if  $n \in 2\mathbb{Z}$  and  $(-1)^{(n-1)/2}$  if  $n \notin 2\mathbb{Z}$ . We easily see that

$$(22.7a) \quad 1 \in \delta_0(\eta_m),$$

$$(22.7b) \quad \delta_0(\varphi \oplus \varphi') = \delta_0(\varphi)\delta_0(\varphi') \quad \text{if } \dim(V) \text{ (that is, the size of } \varphi) \text{ is even.}$$

Notice that for  $c \in F^\times$  we have  $\delta_0(c\varphi) = \delta_0(\varphi)$  if  $n$  is even, and  $\delta_0(c\varphi) = c\delta_0(\varphi)$  if  $n$  is odd.

We now consider a field  $K_0$  given by

$$(22.8) \quad K_0 = F(\delta^{1/2}), \quad \delta \in \delta_0(\varphi),$$

and call  $K_0$  the **discriminant field** of  $\varphi$ , or of  $(V, \varphi)$ . This is either  $F$  itself or a quadratic extension of  $F$ ; clearly it does not depend on the choice of  $\delta$ . We then define the **discriminant algebra**  $K$  of  $\varphi$ , or of  $(V, \varphi)$ , by

$$(22.9) \quad K = \begin{cases} K_0 & \text{if } K_0 \neq F, \\ F \oplus F & \text{if } K_0 = F. \end{cases}$$

For such a  $K$ , we always denote by  $\rho$  the nontrivial automorphism of  $K$  over  $F$ ; in particular,  $(x, y)^\rho = (y, x)$  for  $(x, y) \in F \oplus F$ .

If  $\zeta$  is the restriction of  $\varphi$  to a core subspace  $Z$  of  $V$ , then from (22.7a, b) we see that  $\delta_0(\varphi) = \delta_0(\zeta)$ , and so the discriminant field and algebra of  $\zeta$  coincide with those of  $\varphi$ .

**Lemma 22.7.** *Suppose that  $\dim(V) = 2$  and  $\varphi$  is nondegenerate. Then  $\varphi$  is isotropic if and only if  $\delta_0(\varphi) = 1$ .*

PROOF. If  $\varphi$  is isotropic, then by Lemma 22.3,  $\eta_1$  represents  $\varphi$ , and so  $\delta_0(\varphi) = 1$ . To prove the converse, take an orthogonal basis  $\{x, y\}$  of  $V$ ; put  $a = \varphi[x]$  and  $b = \varphi[y]$ . Suppose  $\delta_0(\varphi) = 1$ ; then  $ab = -c^2$  with  $c \in F^\times$ , and  $\varphi[bx + cy] = 0$ , so that  $\varphi$  is isotropic. This proves our lemma.

**22.8.** As we defined in §19.9, an involution of an  $F$ -algebra  $A$  is a bijection  $\rho$  of  $A$  onto itself such that  $(x + y)^\rho = x^\rho + y^\rho$ ,  $(xy)^\rho = y^\rho x^\rho$ , and  $(x^\rho)^\rho = x$ , where  $x^\rho$  denotes the image of  $x$  under  $\rho$ . We do not necessarily assume that  $\rho$  is  $F$ -linear. The restriction of  $\rho$  to  $F$  is an automorphism of  $F$  of order 1 or 2. Given an involution  $\rho$  of  $A$ , we can define an involution  $x \mapsto {}^t x^\rho$  of  $M_n(A)$  by  $({}^t x^\rho)_{ij} = (x_{ji})^\rho$ .

We also defined in §20.6a the *main involution* of a quaternion algebra. Throughout the book we make the following convention: *Whenever the letter  $\iota$  appears as a superscript, it means the main involution of the quaternion algebra in question.* The letter may be used with a different meaning, but in that case it is not a superscript.

## 23. Clifford algebras

**23.1.** Let  $V$  be a finite-dimensional vector space over a field  $F$  of characteristic different from 2, and let  $(V, \varphi)$  be a quadratic space over  $F$ . We do not

assume that  $\varphi$  is nondegenerate, though we will later assume that condition for the most part of our treatment. As will be proven in §23.3 below, there exists a pair  $(A, p)$  consisting of an  $F$ -algebra  $A$  and an  $F$ -linear map  $p$  of  $V$  into  $A$  with the following four properties:

- (1)  $A$  has an identity element; we denote it by  $1_A$ .
- (2)  $A$  as a ring is generated by  $p(V)$  and  $1_A$  over  $F$ .
- (3)  $p(x)^2 = \varphi[x]1_A$  for every  $x \in V$ .
- (4) If  $(A_1, p_1)$  is another pair satisfying (1) and (3), then there exists an  $F$ -linear ring-homomorphism  $f$  of  $A$  into  $A_1$  such that  $p_1 = f \circ p$  and  $f(1_A) = 1_{A_1}$ .

From (4) we easily see that such a pair  $(A, p)$  is unique up to isomorphism. Moreover,  $p$  is injective, as will be proven in §23.3. We then call  $A$  the **Clifford algebra** of  $\varphi$ . Identifying  $x$  with  $p(x)$  for every  $x \in V$ , we view  $V$  as a subspace of  $A$ , so that  $x^2 = \varphi[x]$  for  $x \in V$ , as we view  $F$  as a subring of  $A$  by identifying  $b$  with  $b1_A$  for every  $b \in F$ . We denote this algebra  $A$  by  $A(V, \varphi)$ , and also by  $A(V)$  or  $A(\varphi)$ , when  $\varphi$  or  $V$  is clear from the context.

An element  $x$  of  $V$  is invertible in the ring  $A$  if and only if  $\varphi[x] (= x^2) \neq 0$ . Indeed, if  $x^2 \neq 0$ , then  $(x^2)^{-1}$  is meaningful as an element of  $F$ , and  $x^{-1} = (x^2)^{-1}x$ ; conversely, if  $x$  is invertible, clearly we cannot have  $x^2 = 0$ . When  $\varphi$  is clear from the context, we call an element  $x$  of  $V$  **invertible** if  $\varphi[x] (= x^2) \neq 0$ .

If  $\dim(V) = n$  and  $\{e_i\}_{i=1}^n$  is an  $F$ -basis of  $V$ , then the  $2^n$  elements  $e_{i_1} \cdots e_{i_s}$  for  $i_1 < \cdots < i_s$ ,  $0 \leq s \leq n$ , (with the understanding that the product means 1 if  $s = 0$ ) form an  $F$ -basis of  $A$ ; see §23.3 for the proof. If  $V = \{0\}$ , then naturally  $\varphi = 0$ , and we have clearly  $A(V) = F$ .

Once we know that  $[A(V) : F] = 2^n$ , then from (4) we can easily derive:

- (23.1) *If  $(A, p)$  satisfies (1), (2), and (3), and  $A$  has dimension  $\geq 2^n$  over  $F$ , where  $n = \dim(V)$ , then  $A$  is the Clifford algebra of  $\varphi$ .*

Since  $x^2 + y^2 + xy + yx = (x + y)^2 = \varphi[x + y] = \varphi[x] + \varphi[y] + 2\varphi(x, y)$ , we obtain a basic equality

$$(23.2) \quad xy + yx = 2\varphi(x, y) \quad \text{for every } x, y \in V.$$

We say that  $x$  is *orthogonal* to  $y$  with respect to  $\varphi$  if  $\varphi(x, y) = 0$ , which is the case if and only if  $xy = -yx$ .

If  $\varphi = 0$  on the whole  $V$ , then we easily see that  $A(V)$  is the exterior algebra of  $V$ .

**23.2.** Apply (4) to  $(A_1, p_1)$  with  $A_1 = A$  and  $p_1 : V \rightarrow A$  given by  $p_1(u) = -u$ . Then we can find an  $F$ -linear ring-homomorphism  $f$  of  $A$  into itself such that  $f(u) = -u$  for every  $u \in V$ . We write  $a' = f(a)$ . Since  $V$  and  $F$  generate  $A$ , clearly  $a \mapsto a'$  is an  $F$ -linear ring-automorphism of  $A$ , which

we call the **canonical automorphism** of  $A(V)$ . Similarly we can define an  $F$ -linear involution (see §22.8)  $a \mapsto a^*$  of  $A(V)$  such that  $u^* = u$  for every  $u \in V$ . This means  $(x_1 \cdots x_s)^* = x_s \cdots x_1$  for  $x_1, \dots, x_s \in V$ . We call it the **canonical involution** of  $A(V)$ .

We now put

$$(23.3) \quad A^+(V) = \{a \in A(V) \mid a' = a\}, \quad A^-(V) = \{a \in A(V) \mid a' = -a\}.$$

We denote these by  $A^\pm(V, \varphi)$ , and also by  $A^\pm(\varphi)$ , according to the context. For  $m$  elements  $x_1, \dots, x_m \in V$  we have  $(x_1 \cdots x_m)' = (-1)^m x_1 \cdots x_m$ . Therefore the product  $x_1 \cdots x_m$  belongs to  $A^+(V)$  or  $A^-(V)$  according as  $m$  is even or odd. In particular, if  $n = \dim(V)$  and  $\{e_i\}_{i=1}^n$  is an  $F$ -basis of  $V$ , then the elements  $e_{i_1} \cdots e_{i_s}$  for  $i_1 < \cdots < i_s$ ,  $0 \leq s \leq n$ , with even (resp. odd)  $s$  form a basis of  $A^+(V)$  (resp.  $A^-(V)$ ). Thus both  $A^+(V)$  and  $A^-(V)$  are of dimension  $2^{n-1}$  over  $F$ , provided  $n > 0$ . Clearly both  $A^+(V)$  and  $A^-(V)$  are stable under the canonical involution. Also,  $A^+(V)$  is a subalgebra of  $A(V)$ , which we call the **even Clifford algebra** of  $\varphi$ . If  $V = \{0\}$ , then  $A(V) = A^+(V) = F$  and  $A^-(V) = \{0\}$ .

**23.3.** Let us now prove the existence of  $(A, p)$  satisfying the four conditions of §23.1 by induction on  $n = \dim(V)$ . First, assuming that  $n = 1$ , put  $V = Fe$  and  $\varphi[e] = \gamma$ . We can then define an algebra  $A = F \oplus Fe$  with the law of multiplication determined in an obvious way by the rule  $e^2 = \gamma$ . It can easily be seen that  $A$  satisfies the required conditions.

Suppose  $n > 1$ . Then we can put  $V = X + Fe$  with an element  $e$  of  $V$  and a subspace  $X$  of dimension  $n - 1$  such that  $\varphi(e, x) = 0$  for every  $x \in X$ . (This can be done, for example, by taking a basis of  $V$  with respect to which  $\varphi$  is represented by a diagonal matrix. We do not assume that  $\varphi[e] \neq 0$ .) By our induction assumption we have the Clifford algebra  $B = A(X, \psi)$ , where  $\psi$  is the restriction of  $\varphi$  to  $X$ . Then we can define an  $F$ -linear automorphism  $a \mapsto a'$  of  $B$  such that  $x' = -x$  for every  $x \in X$ . Put  $\varphi[e] = \gamma$  and

$$(23.4) \quad q(a, b) = \begin{bmatrix} a & b \\ \gamma b' & a' \end{bmatrix} \quad \text{for } a, b \in B.$$

Let  $A$  be the set of all such  $q(a, b)$ . We easily see that  $A$  is a subalgebra of  $M_2(B)$  containing the identity element  $1_2$ . (This was already observed in §20.1.) Define  $p : V \rightarrow A$  by  $p(x + ce) = q(x, c)$  for  $x + ce \in V$  with  $x \in X$  and  $c \in F$ . Then  $p(x + ce)^2 = (x^2 + \gamma c^2)1_2 = \varphi[x + ce]1_2$ . Since  $X$  and  $F$  generate  $B$ , it can easily be verified that  $p(V)$  and  $F$  generate  $A$ . Thus  $(A, p)$  has properties (1), (2), and (3). Identifying  $\text{diag}[b, b']$  with  $b \in B$ , we can view  $B$  as a subalgebra of  $A$ . Then identifying  $p(e)$  with  $e$ , we can put  $A = B + Be$  and  $q(a, b) = a + be$ ; in particular,  $p(w) = w$  for  $w \in V$ . We easily see that  $be = eb'$  for every  $b \in B$ . Let  $(A_1, p_1)$  be a pair satisfying (1) and (3). Since  $B$  satisfies (4) for  $X$ , there is an  $F$ -linear ring-homomorphism  $g$  of  $B$  into

$A_1$  such that  $g(x) = p_1(x)$  for every  $x \in X$  and  $g(1_B) = 1_{A_1}$ . For  $x \in X$  we have  $p_1(x)p_1(e) + p_1(e)p_1(x) = 2\varphi(x, e) = 0$  by (23.2), since the proof of (23.2) shows that it is true even for  $(A_1, p_1)$ . Thus  $p_1(x)p_1(e) = p_1(e)p_1(-x)$ , from which we can derive that

$$(23.5) \quad g(b)p_1(e) = p_1(e)g(b') \quad \text{for every } b \in B,$$

as  $X$  and  $F$  generate  $B$ . Define  $f : A \rightarrow A_1$  by  $f(a + be) = g(a) + g(b)p_1(e)$  for  $a, b \in B$ . Clearly  $f(w) = p_1(w)$  for  $w \in V$ . Since  $be = eb'$ , from (23.5) we see that  $f$  is an  $F$ -linear ring-homomorphism. Thus  $A$  satisfies (4). This completes the proof of the existence. At the same time, our induction shows the injectivity of the map  $p : V \rightarrow A$ , as well as the fact that  $\dim(A) = 2^n$ .

Next, given an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $V$ , let us prove that the  $2^n$  elements  $e_{i_1} \cdots e_{i_s}$  for  $i_1 < \cdots < i_s$ ,  $0 \leq s \leq n$ , form an  $F$ -basis of  $A$ . This is clear if  $n = 1$ . If  $n > 1$ , take  $V = X + Fe$  and  $B$  as above; take also an  $F$ -basis  $\{f_i\}_{i=1}^{n-1}$  of  $X$  and put  $f_n = e$ . Applying induction to  $B$  and  $\{f_i\}_{i=1}^{n-1}$ , we easily see that the elements  $f_{i_1} \cdots f_{i_s}$  for  $i_1 < \cdots < i_s$ ,  $0 \leq s \leq n$ , form an  $F$ -basis of  $A$ . Given  $\{e_i\}_{i=1}^n$ , we can easily verify that every product  $u_1 \cdots u_r$  with  $u_i \in V$  and  $r \leq n$  is an  $F$ -linear combination of  $e_{i_1} \cdots e_{i_s}$  of the above type, because of the relations  $e_i e_j = 2\varphi(e_i, e_j) - e_j e_i$ . Since the elements  $f_{i_1} \cdots f_{i_s}$  span  $A$  over  $F$ , the elements  $e_{i_1} \cdots e_{i_s}$  must span  $A$  over  $F$ . They must be linearly independent over  $F$ , as  $\dim(V) = 2^n$ . This proves the desired fact.

Given a vector subspace  $X$  of  $V$ , let  $C$  be the subalgebra of  $A(V)$  generated by the elements of  $X$  and  $F$ . Taking an  $F$ -basis of  $X$  as a subset of  $\{e_i\}_{i=1}^n$ , we see that  $\dim(C) \geq 2^{\dim(X)}$ , and so by (23.1),  $C$  can be viewed as the Clifford algebra of the restriction of  $\varphi$  to  $X$ , and therefore we can put  $C = A(X)$ . In our later treatment we consider  $A(X)$  for various subspaces  $X$  of  $V$  with the same  $\varphi$ , which is why we use  $A(V)$  instead of  $A(\varphi)$ .

**23.4.** Hereafter we fix a nondegenerate quadratic space  $(V, \varphi)$ . We first assume that  $\varphi$  is isotropic, and consider a weak Witt decomposition of the simplest type:

$$(23.6a) \quad V = U + Fe + Ff, \quad ef + fe = 1, \quad e^2 = f^2 = 0,$$

$$(23.6b) \quad U = (Fe + Ff)^\perp = \{x \in V \mid xe = -ex, xf = -fx\}.$$

Notice that in view of (23.2), equality  $2\varphi(e_i, f_j) = \delta_{ij}$  in (22.4b) can be written  $e_i f_j + f_j e_i = \delta_{ij}$ .

We are going to define an  $F$ -linear isomorphism

$$(23.7) \quad \Psi : A(V) \xrightarrow{\cong} M_2(A(U)).$$

We first define an  $F$ -linear map  $\Psi : V \rightarrow M_2(A(U))$  by



$$(23.8) \quad \Psi(u + re + sf) = \begin{bmatrix} u & r \\ s & -u \end{bmatrix} \quad (u \in U, r \in F, s \in F).$$

For  $x = u + re + sf$  we have  $\Psi(x)^2 = (u^2 + rs)1_2 = \varphi[u + re + sf]1_2$ . Thus  $\Psi(x)^2 = \varphi[x]1_2$  for every  $x \in V$ , and so  $\Psi$  can be extended to an  $F$ -linear ring-homomorphism of  $A(V)$  into  $M_2(A(U))$ . Observing that

$$(23.9) \quad \Psi(e) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \Psi(f) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad \Psi(e f) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \Psi(f e) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

we can easily verify that  $\Psi(V)$  generates the whole  $M_2(A(U))$ . Since the algebras  $M_2(A(U))$  and  $A(V)$  have the same dimension over  $F$ , we can conclude that  $\Psi$  gives an isomorphism of  $A(V)$  onto  $M_2(A(U))$ .

For  $\xi = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  with  $a, b, c, d \in A(U)$ , put  $\xi^* = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$ , where  $*$  is the canonical involution of  $A(U)$ . Then  $\xi \mapsto \xi^*$  is an involution of  $M_2(A(U))$ . We note two easy formulas:

$$(23.10) \quad \Psi(\alpha^*) = J\Psi(\alpha')^*J^{-1} \quad \text{for every } \alpha \in A(V), \quad J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$(23.11) \quad \Psi(b) = \text{diag}[b, b'] \quad \text{for every } b \in A(U).$$

Indeed, (23.10) and (23.11) follow from (23.8) if  $\alpha \in V$  and  $b \in U$ ; consequently they hold for every monomial of elements of  $V$  or  $U$ . Thus they are valid as stated.

Put  $\ell = e - f$ . Then  $\ell^2 = -1$ , and  $\ell u \ell^{-1} = -u = u'$  for every  $u \in U$ , so that  $\ell a \ell^{-1} = a'$  for every  $a \in A(U)$ . Put  $\Lambda = \text{diag}[\ell, -\ell]$ . Then

$$(23.12) \quad \Lambda\Psi(\xi)\Lambda^{-1} = \Psi(\xi') \quad \text{for every } \xi \in A(V).$$

This follows from (23.8) if  $\xi \in V$ ; consequently it holds for every monomial of elements of  $V$ ; thus it is valid as stated. Let us now prove

$$(23.13) \quad \Psi(A^\pm(V)) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, d \in A^\pm(U); b, c \in A^\mp(U) \right\}.$$

Indeed, for  $\Psi(\xi) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  we have  $\Psi(\xi') = \begin{bmatrix} a' & -b' \\ -c' & d' \end{bmatrix}$  by (23.12). Thus  $\xi \in A^\pm(V)$  if and only if  $a' = \pm a$ ,  $b' = \mp b$ ,  $c' = \mp c$ , and  $d' = \pm d$ . This proves (23.13).

**23.5.** The above discussion is valid even when  $U = \{0\}$ . Then we have  $A(U) = F$ ,  $\Psi(A(V)) = M_2(F)$ , and  $\Psi(A^+(V))$  consists of  $\text{diag}[a, d]$  with  $a, d \in F$ .

If  $U \neq \{0\}$ , we can define another representation that is often more convenient than  $\Psi$ , which is as follows. Take an element  $g$  of  $U$  such that  $g^2 \neq 0$ , and put

$$(23.14) \quad \Xi(\alpha) = \Delta^{-1}\Psi(\alpha)\Delta, \quad \Delta = \text{diag}[g, 1].$$

Then  $\Xi$  is a ring-bijection of  $A(V)$  onto  $M_2(A(U))$ ; besides, since  $g^{-1}A^-(U) = A^-(U)g = A^+(U)$  and  $g^{-1}A^+(U)g = A^+(U)$ , from (23.13) we obtain

$$(23.15) \quad \Xi(A^+(V)) = M_2(A^+(U)) \quad \text{if } U \neq \{0\}.$$

**Theorem 23.6.** *Let  $V = X + \sum_{i=1}^s (Fe_i + Ff_i)$  be a weak Witt decomposition, and let  $m = 2^s$ . Then  $A(V)$  is isomorphic to  $M_m(A(X))$ . Moreover,  $A^+(V)$  is isomorphic to  $M_m(A^+(X))$  if  $X \neq \{0\}$ , and to  $M_{m/2}(F) \oplus M_{m/2}(F)$  if  $X = \{0\}$ .*

PROOF. The discussion of §§23.4 and 23.5 proves the case  $s = 1$ . To prove the general case by induction on  $s$ , assume that  $s > 1$  and put  $U = X + \sum_{i=1}^{s-1} (Fe_i + Ff_i)$ . Then  $V = U + Fe_s + Ff_s$ , and so  $A(V)$  is isomorphic to  $M_2(A(U))$  and  $A^+(V)$  is isomorphic to  $M_2(A^+(U))$ . Applying induction to  $A(U)$  and  $A^+(U)$ , we obtain our theorem.

**Lemma 23.7.** *Given an orthogonal basis  $\{h_i\}_{i=1}^n$  of  $V$ , put  $z = h_1 \cdots h_n$ . Then the following assertions hold:*

- (i)  $z^{-1}xz = (-1)^{n-1}x$  for every  $x \in V$ ;
- (ii)  $z^2 = (-1)^{(n-1)n/2}h_1^2 \cdots h_n^2$  and  $z^* = (-1)^{(n-1)n/2}z$ ;
- (iii)  $Fz$  is independent of the choice of  $\{h_i\}_{i=1}^n$ ;
- (iv)  $F + Fz$  is the center of  $A(V)$  or  $A^+(V)$  according as  $n$  is odd or even.
- (v)  $F + Fz$  is isomorphic to the discriminant algebra of  $\varphi$ . Moreover, if  $n$  is even, then the canonical involution gives the nontrivial automorphism of  $F + Fz$  over  $F$ , and

$$(23.16) \quad ax = xa^* \quad \text{for every } a \in F + Fz \text{ and every } x \in V.$$

PROOF. We easily see that  $h_i z = (-1)^{n-1} z h_i$  for every  $i$ . Since the  $h_i$  span  $V$  over  $F$ , we obtain (i). Assertion (ii) is an easy exercise. We prove (iv) in the proof of the next theorem. Since  $z^2 \in F$  and  $z \notin F$ , we see that if  $x \in F + Fz$ ,  $x \notin F$ , and  $x^2 \in F$ , then  $x \in Fz$ . Assertion (iii) follows from this fact and (iv). The first part of (v) follows easily from (ii). If  $n$  is even, then  $z^* = -z$  by (ii), and  $zx = -xz$  for every  $x \in V$  by (i), and so we obtain (23.16).

**Theorem 23.8.** *Let  $\mathfrak{C}$  be the center of  $A(V)$  and  $\mathfrak{C}^+$  the center of  $A^+(V)$ .*

(i) *Suppose  $\dim(V)$  is even and  $> 0$ . Then  $A(V)$  is a central simple algebra over  $F$  and  $\mathfrak{C}^+ = F + Fz$  with  $z$  as in Lemma 23.7.  $A^+(V)$  is a central simple algebra over  $\mathfrak{C}^+$  if  $\mathfrak{C}^+$  is a field; otherwise  $A^+(V)$  is the direct sum of two central simple algebras over  $F$  of the same degree.*

(ii) *Suppose  $\dim(V)$  is odd. Then  $A^+(V)$  is a central simple algebra over  $F$ ,  $\mathfrak{C} = F + Fz$  with  $z$  as in Lemma 23.7, and  $A(V) = A^+(V) \otimes_F \mathfrak{C}$ .*

PROOF. Let  $\overline{F}$  be the algebraic closure of  $F$ ; let  $\overline{V} = V \otimes_F \overline{F}$ ; extend  $\varphi$  naturally to  $\overline{V}$ . Suppose  $\dim(V) = 2r + 1$  with  $r \in \mathbf{Z}$ . Then  $\overline{V}$  has a Witt de-

composition  $\overline{V} = \overline{F}g + \sum_{i=1}^r (\overline{F}e_i + \overline{F}f_i)$ , and  $A^+(\overline{F}g) = \overline{F}$ . By Theorem 23.6,  $A^+(V)$  is isomorphic to  $M_m(\overline{F})$ , where  $m = 2^r$ . Since  $A^+(\overline{V}) = A^+(V) \otimes_F \overline{F}$ , we can conclude from Theorem 19.7 that  $A^+(V)$  is central simple over  $F$ . Take  $z$  as in Lemma 23.7; then by (i) of that lemma,  $zx = xz$  for every  $x \in V$ , and so  $z \in \mathfrak{C}$ . Since  $z \in A^-(V)$ , we have  $A(V) = A^+(V) \oplus A^+(V)z$ . Now  $F + Fz$  is a commutative algebra of rank 2, and so  $A(V) = A^+(V) \otimes_F (F + Fz)$ . Since the center of  $A^+(V)$  is  $F$ , we have clearly  $\mathfrak{C} = F + Fz$ .

Next suppose  $\dim(V) = 2r$  with  $r \in \mathbf{Z}$ . Then  $\overline{V}$  has a Witt decomposition  $\overline{V} = \sum_{i=1}^r (\overline{F}e_i + \overline{F}f_i)$ , and  $A(\overline{V})$  is isomorphic to  $M_m(\overline{F})$ , where  $m = 2^r$ . Thus by Theorem 19.7,  $A(V)$  is central simple over  $F$ . By Theorem 23.6,  $A^+(\overline{V})$  is isomorphic to  $M_{m/2}(\overline{F}) \oplus M_{m/2}(\overline{F})$ , whose center is  $\overline{F} \oplus \overline{F}$ . Therefore  $[\mathfrak{C}^+ : F] = 2$  in view of Lemma 19.3(ii). From (i) of Lemma 23.7 we see that  $z\alpha = \alpha z$  for every  $\alpha \in A^+(V)$ , and so  $\mathfrak{C}^+ = F + Fz$ , since  $z \notin F$ . If  $\mathfrak{C}^+$  is a field, then  $A^+(V)$  is central simple over  $\mathfrak{C}^+$  by Lemma 19.25. Otherwise there is an element  $c$  of  $F$  such that  $z^2 = c^2$ . Put  $\varepsilon = (1 + c^{-1}z)/2$  and  $\delta = (1 - c^{-1}z)/2$ . Then  $1 = \varepsilon + \delta$ ,  $\varepsilon^2 = \varepsilon$ ,  $\delta^2 = \delta$ , and  $\varepsilon\delta = 0$ . Therefore  $\mathfrak{C}^+$  is isomorphic to  $F \oplus F$ , and  $A^+(V)$  is the direct sum of two subalgebras  $A^+(V)\varepsilon$  and  $A^+(V)\delta$ . Since these become  $M_{m/2}(\overline{F})$  over  $\overline{F}$ , they must be central simple over  $F$  by Theorem 19.7. This completes the proof, and proves also (iv) of Lemma 23.7.

**Corollary 23.9.** *An element  $\alpha$  of  $A^+(V)$  commutes with every element of  $V$  if and only if  $\alpha \in F$ .*

PROOF. Since  $V$  generates  $A(V)$ , if an element  $\alpha$  of  $A^+(V)$  commutes with every element of  $V$ , then  $\alpha \in \mathfrak{C} \cap \mathfrak{C}^+$ . By Theorem 23.8,  $\mathfrak{C} \cap \mathfrak{C}^+ = F$ , which gives our assertion.

**Lemma 23.10.** *With  $(V, \varphi)$ ,  $n$ , and  $z$  as in Lemma 23.7, let  $(V', \varphi')$  be another quadratic space and let  $\delta = z^2$ . Define a vector subspace  $C$  of  $A(\varphi \oplus \varphi')$  by  $C = A^+(\varphi') + zA^-(\varphi')$ . Then  $C$  is a subalgebra of  $A(\varphi \oplus \varphi')$  and the following assertions hold:*

- (i) *There is an isomorphism of  $C$  onto  $A((-1)^n \delta \varphi')$  that maps  $A^+(\varphi')$  onto  $A^+((-1)^n \delta \varphi')$ .*
- (ii)  *$A(\varphi \oplus \varphi') = A(\varphi) \otimes_F C$  if  $n \in 2\mathbf{Z}$ , and  $A^+(\varphi \oplus \varphi') = A^+(\varphi) \otimes_F C$  if  $n \notin 2\mathbf{Z}$ .*
- (iii) *The canonical involution of  $A(\varphi \oplus \varphi')$  restricted to  $A^+(\varphi')$  coincides with the canonical involution of  $A((-1)^n \delta \varphi')$  restricted to  $A^+((-1)^n \delta \varphi')$ .*

PROOF. Notice that if  $u = x_1 \cdots x_r$  with  $x_i \in V$  and  $v = y_1 \cdots y_s$  with  $y_j \in V'$ , then  $uv = (-1)^{rs}vu$ . We can easily verify that  $C$  is a subalgebra of  $A(\varphi \oplus \varphi')$ . Define  $p : V' \rightarrow C$  by  $p(y) = zy$  for  $y \in V'$ . Then  $p(y)^2 = (-1)^n \delta \varphi'[y]$ , and we easily see that  $F$  and  $p(V')$  generate  $C$ , and so we see that

$C \cong A((-1)^n \delta \varphi')$ . Also, for  $y_j \in V'$ , we have  $(zy_1) \cdots (zy_s) \in A^+(\varphi')$  if  $s \in 2\mathbf{Z}$ , and so  $A^+((-1)^n \delta \varphi')$  as a set coincides with  $A^+(\varphi')$ . If  $n$  is even,  $A(\varphi)$  commutes elementwise with  $C$ ; also we easily see that  $A(\varphi)C = A(\varphi \oplus \varphi')$ , and so we obtain (ii) for  $n \in 2\mathbf{Z}$ . For  $n$  odd, taking  $A^+(\varphi \oplus \varphi')$  and  $A^+(\varphi)$  in place of  $A(\varphi \oplus \varphi')$  and  $A(\varphi)$ , we obtain the desired result. Assertion (iii) can easily be verified.

## 24. Clifford groups and spin groups

**24.1.** Still assuming that  $\varphi$  is nondegenerate, let us now put

$$(24.1a) \quad G(V) = \{\alpha \in A(V)^\times \mid \alpha^{-1}V\alpha = V\},$$

$$(24.1b) \quad G^+(V) = G(V) \cap A^+(V), \quad G^-(V) = G(V) \cap A^-(V).$$

Clearly  $G(V)$  resp.  $G^+(V)$  is a subgroup of  $A(V)^\times$  resp.  $A^+(V)^\times$ , and  $F^\times \subset G^+(V)$ . We denote these by  $G(V, \varphi)$  and  $G^\pm(V, \varphi)$ , and also by  $G(\varphi)$  and  $G^\pm(\varphi)$  according to the context. We call  $G(V, \varphi)$  the **Clifford group** of  $\varphi$ , and  $G^+(V, \varphi)$  the **even Clifford group** of  $\varphi$ . (See the remark after the proof of Theorem 24.6.)

For  $\alpha \in G(V)$  we can define  $\tau(\alpha) \in GL_F(V)$  by

$$(24.1c) \quad x\tau(\alpha) = \alpha^{-1}x\alpha \quad (x \in V).$$

Clearly  $\varphi[x\tau(\alpha)] = (\alpha^{-1}x\alpha)^2 = x^2 = \varphi[x]$ , and so  $\tau(\alpha)$  belongs to the orthogonal group  $O^\varphi$  of  $\varphi$ . Thus  $\tau$  gives a homomorphism of  $G(V)$  into  $O^\varphi$ . Notice that  $\alpha^{-1}V\alpha = V$  if and only if  $\alpha^{-1}V\alpha \subset V$ , as  $\alpha^{-1}V\alpha$  has the same dimension as  $V$  over  $F$ .

**24.2.** For a subspace  $X$  of  $V$  on which  $\varphi$  is nondegenerate, the orthogonal complement of  $X$  defined by (22.3) can be given in the form

$$X^\perp = \{y \in V \mid xy = -yx \text{ for every } x \in X\}.$$

Then  $\varphi$  is nondegenerate on  $X^\perp$ . Put  $Y = X^\perp$ . Taking  $F$ -bases of  $X$  and  $Y$ , we easily see that  $A(X) \cap A(Y) = F$  and  $A(X) \cap V = X$ . Let  $\alpha \in A(X)$  and  $\beta \in A(Y)$  for such  $X$  and  $Y$ . Then we can easily verify that  $\alpha\beta = \beta\alpha$  if  $\alpha \in A^+(X)$  or  $\beta \in A^+(Y)$ ;  $\alpha\beta = -\beta\alpha$  if  $\alpha \in A^-(X)$  and  $\beta \in A^-(Y)$ . In particular, for  $\alpha \in A^+(X)^\times$  we have  $\alpha^{-1}y\alpha = y$  for every  $y \in Y$ , and  $\alpha^{-1}X\alpha = X$  if and only if  $\alpha^{-1}V\alpha = V$ . Therefore we can view an element of  $G^+(X)$  as an element of  $G^+(V)$ ; then  $\tau(\alpha)$  defined as an element of  $O^\varphi(V)$  gives the identity map on  $Y$ . In fact,  $\tau(\alpha) \in SO^\varphi(V)$  as will be shown in Theorem 24.6 below. Hereafter, whenever we have a subspace  $X$  of  $V$  on which  $\varphi$  is nondegenerate, we always view  $G^+(X)$  as a subgroup of  $G^+(V)$ . This injection  $G^+(X) \rightarrow G^+(V)$  maps  $F^\times$  onto itself. If  $\alpha \in G^+(X)$  and  $\beta \in G^+(Y)$ , then  $\tau(\alpha\beta)$  gives the element of  $SO^\varphi(V)$  that can be identified with  $(\tau(\alpha), \tau(\beta))$  of  $SO^\varphi(X) \times SO^\varphi(Y)$ .

**Lemma 24.3.** *For  $x, y \in V$  we have  $xyx \in V$ . Moreover, if  $x^2 \neq 0$ , then  $x \in G^-(V)$  and  $x^{-1} \in V$ .*

PROOF. Both  $x^2$  and  $xy+yx$  belong to  $F$ , and so  $xyx = (xy+yx)x-yx^2 \in V$ . Suppose  $x^2 \neq 0$ ; then  $x$  is invertible and  $x^{-1} = (x^2)^{-1}x \in V$ , and  $x^{-1}Vx = (x^2)^{-1}xVx \subset V$ , so that  $x \in G(V)$ . Since  $x \in A^-(V)$ , we obtain  $x \in G^-(V)$ .

**24.4.** If elements  $x_i$  of  $V$  are invertible, then Lemma 24.3 shows that the product  $x_1 \cdots x_m$  belongs to  $G^+(V)$  or  $G^-(V)$  according as  $m$  is even or odd. To obtain a more precise result, let us now take a hyperplane  $H = \{x \in V \mid \varphi(v, x) = 0\}$  defined with a fixed  $v \in V$  such that  $v^2 \neq 0$ . This is the orthogonal complement  $(Fv)^\perp$  of  $Fv$  in  $V$  with respect to  $\varphi$ ; thus

$$V = Fv \oplus H \quad \text{with} \quad H = (Fv)^\perp = \{x \in V \mid vx = -xv\}.$$

Let  $\gamma$  be the element of  $GL_F(V)$  such that  $v\gamma = -v$  and  $x\gamma = x$  for every  $x \in H$ . Clearly  $\gamma \in O^\varphi$ ,  $\det(\gamma) = -1$ , and  $\gamma$  has order 2. We call  $\gamma$  the **symmetry of  $V$  with respect to  $H$** . We easily see that it coincides with  $-\tau(v)$ . (We are considering here only those hyperplanes defined with the elements  $v$  such that  $v^2 \neq 0$ .) Thus, for an invertible element  $v \in V$  we have

$$(24.2) \quad -\tau(v) \text{ is the symmetry with respect to } (Fv)^\perp \text{ and } \det[-\tau(v)] = -1.$$

We hereafter put  $n = \dim(V)$ .

**Theorem 24.5.** *Every element of  $O^\varphi$  is a product of symmetries of the above type.*

PROOF. If  $n=1$ , then  $O^\varphi = \{\pm 1\}$  and  $-1$  is a symmetry, and our theorem is true. We prove the general case by induction on  $n$ . Suppose  $n > 1$ ; take an element  $v \in V$  such that  $v^2 \neq 0$ , and put  $H = (Fv)^\perp$  as above. Let  $\alpha \in O^\varphi$ .

Special case 1: Suppose  $v\alpha = v$ ; then  $H\alpha = H$ . Let  $\beta$  be the restriction of  $\alpha$  to  $H$ . By induction,  $\beta = \gamma_1 \cdots \gamma_m$  with symmetries  $\gamma_i$  of  $H$ . We can extend each  $\gamma_i$  to a symmetry  $\delta_i$  of  $V$  such that  $v\delta_i = v$ . Then  $\alpha = \delta_1 \cdots \delta_m$ , which is the desired result.

Special case 2: Suppose  $v\alpha = -v$ . Let  $\varepsilon = -\tau(v)$ . Then  $v\alpha\varepsilon = v$ , and we can apply the result of Special case 1 to  $\alpha\varepsilon$ , and obtain the desired fact, since  $\alpha = \alpha\varepsilon\varepsilon$  and  $\varepsilon$  is a symmetry.

General case: Let  $u = v\alpha$ . Then  $u^2 = v^2$ . Since  $0 \neq 4v^2 = (v+u)^2 + (v-u)^2$ , we see that  $(v+u)^2 \neq 0$  or  $(v-u)^2 \neq 0$ . Suppose  $(v+u)^2 \neq 0$ ; put  $x = v+u$  and  $\xi = -\tau(x)$ . Then  $-xu - ux = (u-x)^2 - u^2 - x^2 = -x^2$ , and so  $v\alpha\xi = u\xi = -x^{-1}ux = x^{-1}(xu - x^2) = u - x = -v$ ; thus we can apply the result of Special case 2 to  $\alpha\xi$ . Suppose  $(v-u)^2 \neq 0$ ; put  $y = v-u$  and  $\eta = -\tau(y)$ . Then  $yu + uy = (u+y)^2 - u^2 - y^2 = -y^2$ , and so  $v\alpha\eta = u\eta =$

$-y^{-1}uy = y^{-1}(yu + y^2) = u + y = v$ ; thus we can apply the result of Special case 1 to  $\alpha\eta$ . This completes the proof.

Let us now put

$$(24.3) \quad G^*(V) = G^+(V) \cup G^-(V).$$

This is a subgroup of  $G(V)$ , as will be shown in Theorems 24.6 and 24.7 below.

**Theorem 24.6.** (i) *If  $n$  is odd, then  $\tau(G^+(V)) = \tau(G(V)) = SO^\varphi$  and  $G(V) = \mathfrak{C}^\times G^+(V)$ , where  $\mathfrak{C}$  is the center of  $A(V)$ .*

(ii) *If  $n$  is even and  $> 0$ , then  $G(V) = G^*(V)$ ,  $[G(V) : G^+(V)] = 2$ ,  $\tau(G(V)) = O^\varphi$ ,  $\tau(G^+(V)) = SO^\varphi$ , and  $\tau(G^-(V)) = \{\xi \in O^\varphi \mid \det(\xi) = -1\}$ . Moreover, let  $\mathfrak{C}^+$  be the center of  $A^+(V)$  and  $z$  be as in Lemma 23.7. Then*

$$\mathfrak{C}^+ \cap G^+(V) = \begin{cases} (\mathfrak{C}^+)^\times = G^+(V) & \text{if } n = 2, \\ F^\times \cup F^\times z & \text{if } n > 2. \end{cases}$$

(iii) *For both even and odd  $n$ ,  $\tau$  gives an isomorphism of  $G^+(V)/F^\times$  onto  $SO^\varphi$ ; for even  $n$ ,  $\tau$  gives an isomorphism of  $G(V)/F^\times$  onto  $O^\varphi$ .*

(iv) *If  $Y = X^\perp$  as in §24.2, then*

$$(24.3a) \quad G^+(X) = \{\alpha \in G^+(V) \mid y\tau(\alpha) = y \text{ for every } y \in Y\}.$$

PROOF. Let  $\xi \in O^\varphi$ . By Theorem 24.5,  $\xi = (-\tau(v_1)) \cdots (-\tau(v_k))$  with invertible  $v_i \in V$ . Since each symmetry  $-\tau(v_i)$  has determinant  $-1$ , we have  $\det(\xi) = (-1)^k$ . If  $\xi \in SO^\varphi$ , then  $k$  is even, so that  $\xi = \tau(v_1 \cdots v_k)$ . This shows that  $SO^\varphi \subset \tau(G^+(V))$ . Clearly,  $\tau(G^+(V)) \subset \tau(G(V)) \subset O^\varphi$ .

Suppose  $0 < n \in 2\mathbb{Z}$ . Then, for every invertible  $v$  of  $V$ , we have  $\det(\tau(v)) = -1$ . Since  $v \in G(V)$  and  $[O^\varphi : SO^\varphi] = 2$ , we see that  $\tau(G(V)) = O^\varphi$ . Suppose  $\tau(v) = \tau(\alpha)$  with  $\alpha \in G^+(V)$ . Then  $\alpha^{-1}v$  commutes with every element of  $V$ . Since  $V$  generates  $A(V)$ ,  $\alpha^{-1}v$  must belong to the center of  $A(V)$ , which is  $F$  by Theorem 23.8(i). Therefore  $v = c\alpha$  with  $c \in F$ , which is a contradiction, since  $c\alpha \in A^+(V)$  and  $0 \neq v \in A^-(V)$ . Thus  $\tau(v) \notin \tau(G^+(V))$ , and so  $\tau(G^+(V)) = SO^\varphi$ . We easily see that  $G^-(V) = vG^+(V)$ , and so  $\tau(G^-(V)) = \{\xi \in O^\varphi \mid \det(\xi) = -1\}$ . Next, let  $\gamma \in G(V)$ . For  $\det(\tau(\gamma)) = \pm 1$  we have  $\tau(\gamma) = \tau(\beta)$  with  $\beta \in G^\pm(V)$ . Then  $\beta^{-1}\gamma \in F^\times$ , so that  $\gamma \in G^\pm(V)$ . This proves that  $G(V) = G^*(V)$ , and so  $[G(V) : G^+(V)] = 2$ . Next, let  $\lambda \in \mathfrak{C}^+ \cap G^+(V)$ . By Lemma 23.7(iv) we have  $\mathfrak{C}^+ = F + Fz$ , and by (23.16),  $\lambda^0 v = v\lambda$  for every  $v \in V$ . Thus  $\lambda^{-1}\lambda^0 v = \lambda^{-1}v\lambda \in V$ . Put  $\lambda^{-1}\lambda^0 = c + dz$  with  $c, d \in F$ . Suppose  $d \neq 0$ ; then  $zv \in V$  for every  $v \in V$ , which is the case if and only if  $n = 2$ , as can easily be verified. Thus if  $n > 2$ , then  $d = 0$ , so that  $\lambda^{-1}\lambda^0 = c$ , which can happen only if  $c = \pm 1$ . Therefore  $\lambda \in F^\times \cup F^\times z$  if  $n > 2$ . We also see that  $(\mathfrak{C}^+)^\times = G^+(V)$  if  $n = 2$ , and  $F^\times \cup F^\times z \subset G^+(V)$  for  $n \geq 2$ . This completes the proof of (ii).

Suppose  $n$  is odd. Consider the element  $-1$  of  $O^\varphi$ ; suppose  $-1 = \tau(\alpha)$  with  $\alpha \in G(V)$ . Then  $\alpha^{-1}x\alpha = -x$  for every  $x \in V$ , so that  $\alpha^{-1}y\alpha = y'$  for every  $y \in A(V)$ . Let  $z$  be as in Lemma 23.7. Then  $z' = -z$  and  $z$  belongs to the center  $\mathfrak{C}$  of  $A(V)$ , so that  $z = \alpha^{-1}z\alpha = z' = -z$ , a contradiction. Thus  $-1 \notin \tau(G(V))$ , so that  $\tau(G(V)) = \tau(G^+(V)) = SO^\varphi$ . Take any  $\gamma \in G(V)$ . Then  $\tau(\gamma) = \tau(\beta)$  with  $\beta \in G^+(V)$ , and so  $\beta^{-1}\gamma \in \mathfrak{C}$ , so that  $\gamma \in \mathfrak{C}^\times G^+(V)$ . Clearly  $\mathfrak{C}^\times \subset G(V)$ , and so  $G(V) = \mathfrak{C}^\times G^+(V)$ . Finally, as for (iii), if  $\alpha \in G^+(V)$  and  $\tau(\alpha) = 1$ , then  $\alpha \in F^\times$  by Corollary 23.9; if  $n$  is even, the same is true even for  $\alpha \in G(V)$ , since  $F$  is the center of  $A(V)$ . This proves (iii).

As for (iv), we have seen in §24.2 that  $G^+(X)$  is contained in the right-hand side of (24.3a). Suppose  $\alpha \in G^+(V)$  and  $\tau(\alpha)$  gives the identity map on  $Y$ . Then  $\tau(\alpha)$  gives an element of  $SO^\varphi(X)$ , and so by (i) and (ii) it coincides with  $\tau(\beta)$  with  $\beta \in G^+(X)$ . Then  $\beta$  is an element of  $G^+(V)$  belonging to the right-hand side of (24.3a). Thus we have  $\tau(\alpha) = \tau(\beta)$ , and so  $\alpha = c\beta$  with  $c \in F^\times$ . Therefore  $\alpha \in G^+(X)$ , which proves (24.3a). This completes the proof.

Let us insert here a historical remark. The algebra  $A(V, \varphi)$  for  $V = \mathbf{R}^n$  and  $\varphi = -1_n$  was first defined by Clifford, but the idea of (24.1a, b, c) and the fact that  $\tau(G^+(V)) = SO^\varphi$  are due to Lipschitz; see [Ano]. Therefore the terminology “Clifford group” may be a misnomer, but we use it for expediency.

Now, with the canonical involution  $\xi \mapsto \xi^*$  of  $A(V)$  as in §23.2, put

$$(24.4) \quad \nu(\alpha) = \alpha\alpha^* \quad \text{for } \alpha \in G(V).$$

**Theorem 24.7.** (i)  $G^+(V)$  (resp.  $G^-(V)$ ) consists of all the products of an even (resp. odd) number of elements of  $V$  that are invertible in  $A(V)$ .

(ii)  $G^-(V)$  is a subgroup of  $G(V)$ ,  $[G^-(V) : G^+(V)] = 2$ , and  $\nu$  gives a homomorphism of  $G^-(V)$  into  $F^\times$ . Moreover,  $\nu(\alpha^*) = \nu(\alpha') = \nu(\alpha)$  for every  $\alpha \in G^-(V)$ .

PROOF. We have  $G^-(V) = xG^+(V)$  with any invertible  $x \in V$ . Therefore it is sufficient to prove (i) only for  $G^+(V)$ . If  $w_1, \dots, w_k$  are elements of  $V$  and invertible, then each  $w_i$  belongs to  $G(V)$  by Lemma 24.3, and so  $w_1 \cdots w_k \in G^+(V)$  if  $k$  is even. To prove the converse, let  $\alpha \in G^+(V)$ ; then  $\tau(\alpha) = \tau(v_1 \cdots v_m)$  with  $v_1, \dots, v_m \in V \cap A(V)^\times$  and even  $m$ , as shown in the proof of Theorem 24.6. By (iii) of the same theorem,  $\alpha = cv_1 \cdots v_m$  with  $c \in F^\times$ . Since  $cv_1 \in V$ , this proves (i). Once we have (i), then clearly  $G^-(V)$  is a subgroup of  $G(V)$  and  $[G^-(V) : G^+(V)] = 2$ . Next, if  $\alpha = x_1 \cdots x_k$  with  $x_i \in V \cap A(V)^\times$ , then

$$(24.4a) \quad \nu(\alpha) = \alpha\alpha^* = x_1 \cdots x_k \cdot x_k \cdots x_1 = x_1^2 \cdots x_k^2.$$

The remaining part of (ii) follows immediately from this and (i).

**24.8.** Let  $X$  be a subspace of  $V$  on which  $\varphi$  is nondegenerate, and let  $Y = X^\perp$ . From Theorem 24.7 we see that  $G(X)$  is a subgroup of  $G(V)$ . Moreover,  $\tau(\alpha)$  for  $\alpha \in G^\pm(X)$  gives  $\pm 1_Y$  on  $Y$ .

Notice that for an element  $\alpha$  of  $A^\pm(V)$  we have

$$(24.5) \quad [\alpha\alpha^* \in F^\times \quad \text{and} \quad \alpha V\alpha^* \subset V] \iff \alpha \in G^\pm(V).$$

This is because  $\alpha^* = \alpha^{-1} \cdot \alpha\alpha^*$ . We define a subgroup  $G^1(V)$  of  $G^+(V)$  by

$$(24.6) \quad G^1(V) = \{\alpha \in G^+(V) \mid \nu(\alpha) = 1\}.$$

Since  $F^\times \cap G^1(V) = \{\pm 1\}$ , from Theorem 24.6(iii) we see that  $\tau$  gives an injection of  $G^1(V)/\{\pm 1\}$  into  $SO^\varphi$ . We call  $G^1(V)$  the **spin group** of  $\varphi$ .

We define a homomorphism

$$(24.7) \quad \sigma : O^\varphi(V) \longrightarrow F^\times / F^{\times 2}, \quad F^{\times 2} = \{a^2 \mid a \in F^\times\},$$

as follows. By Theorem 24.5 every element  $\alpha$  of  $O^\varphi(V)$  is of the form  $\alpha = (-1)^r \tau(x_1 \cdots x_r)$  with invertible  $x_i \in V$ . We then put  $\sigma(\alpha) = x_1^2 \cdots x_r^2 F^{\times 2}$ . To show that this is independent of the choice of  $x_i$ , let  $\alpha = (-1)^s \tau(y_1 \cdots y_s)$  with invertible  $y_j$ . Then  $(-1)^{r+s} \tau(x_1 \cdots x_r y_s \cdots y_1) = 1$ . Since  $\det[-\tau(x)] = -1$  for any invertible  $x$ , we see that  $r+s \in 2\mathbf{Z}$ . Thus  $\tau(x_1 \cdots x_r y_s \cdots y_1) = 1$ . By Theorem 24.6(iii),  $x_1 \cdots x_r y_s \cdots y_1 = c$  with  $c \in F^\times$ , and so  $x_1^2 \cdots x_r^2 y_s^2 \cdots y_1^2 \in F^{\times 2}$ , which proves that  $\sigma$  is well defined.

Clearly  $\sigma$  is a homomorphism. We call  $\sigma(\alpha)$  the **spinor norm** of  $\alpha$ . In particular, if  $\alpha \in SO^\varphi(V)$ , we take an element  $\xi$  of  $G^+(V)$  such that  $\tau(\xi) = \alpha$ , and find that  $\sigma(\alpha) = \nu(\xi)F^{\times 2}$ . We easily see that

$$(24.7a) \quad \tau(G^1(V)) = \{\alpha \in SO^\varphi(V) \mid \sigma(\alpha) = 1\}.$$

For simplicity we will often denote by  $c$  the coset  $cF^{\times 2}$  for  $c \in F^\times$ . Thus

$$(24.7b) \quad \sigma(\tau(x_1) \cdots \tau(x_m)) = x_1^2 \cdots x_m^2 \quad \text{if} \quad x_i \in V, x_i^2 \neq 0, \text{ and } m \in 2\mathbf{Z}.$$

**Lemma 24.9.** (i) For every  $c \in F^\times$  there exists an  $F$ -linear ring-isomorphism  $f$  of  $A^+(V, c\varphi)$  onto  $A^+(V, \varphi)$  such that  $f(G^+(V, c\varphi)) = G^+(V, \varphi)$  and  $f(\xi)^* = f(\xi^*)$  for every  $\xi \in A^+(V, \varphi)$ ; further  $\tau(\alpha) = \tau(f(\alpha))$  and  $\nu(\alpha) = \nu(f(\alpha))$  for every  $\alpha \in G^+(V, \varphi)$ .

(ii) Given an  $F$ -linear bijection  $\gamma : V \rightarrow W$ , define a quadratic form  $\psi$  on  $W$  by  $\psi[x\gamma] = \varphi[x]$  for  $x \in V$ . Then the map  $x \mapsto x\gamma$  of  $V$  to  $W$  can be extended to an  $F$ -linear ring-isomorphism of  $A(V, \varphi)$  to  $A(W, \psi)$ , written  $\alpha \mapsto \alpha^\gamma$ , such that  $\tau(\alpha^\gamma) = \gamma^{-1}\tau(\alpha)\gamma$  for every  $\alpha \in G(V)$ . Moreover,  $G^+(V)$  and  $G^-(V)$  are mapped onto  $G^+(W)$  and  $G^-(W)$  under this isomorphism, and  $\nu(\alpha^\gamma) = \nu(\alpha)$  for every  $\alpha \in G(V)$ ; further,  $\sigma(\gamma^{-1}\xi\gamma) = \sigma(\xi)$  for every  $\xi \in SO^\varphi(V)$ . In particular, if  $(V, \varphi) = (W, \psi)$  and  $\gamma \in O^\varphi(V)$ , then  $\alpha \mapsto \alpha^\gamma$  is an automorphism of  $A(V)$ .



PROOF. Take an algebraic extension  $E = F(d)$  of  $F$  with an element  $d$  such that  $d^2 = c$ , and let  $Y = V \otimes_F E$ . We extend  $\varphi$  to an  $E$ -bilinear form  $Y \times Y \rightarrow E$ , and denote it again by  $\varphi$ . Clearly  $A(Y, \varphi) = A(V, \varphi) \otimes_F E$ . Since  $\varphi[dx] = c\varphi[x]$  for  $x \in Y$ , the map  $x \mapsto dx$  for  $x \in Y$  can be extended to a ring-isomorphism  $f$  of  $A(Y, c\varphi)$  onto  $A(Y, \varphi)$ . We easily see that  $f$  maps  $A^+(V, c\varphi)$  onto  $A^+(V, \varphi)$  and  $G^+(V, c\varphi)$  onto  $G^+(V, \varphi)$ . Clearly  $SO^{c\varphi}(V) = SO^\varphi(V)$  and  $f(y\beta) = f(y)\beta$  for  $\beta \in SO^\varphi(V)$  and  $y \in Y$ . Now, for  $\alpha \in G^+(V, c\varphi)$  we have  $f(y)\tau(\alpha) = f(y\tau(\alpha)) = f(\alpha^{-1}y\alpha) = f(\alpha)^{-1}f(y)f(\alpha) = f(y)\tau(f(\alpha))$ , and so  $\tau(\alpha) = \tau(f(\alpha))$ . The formulas  $f(\xi)^* = f(\xi^*)$  and  $\nu(\alpha) = \nu(f(\alpha))$  can easily be verified.

Next, given  $\gamma : V \rightarrow W$  as in (ii), we can view  $\gamma$  as an injection of  $V$  into  $A(W)$ . Then we find an  $F$ -linear ring-homomorphism  $f$  of  $A(V)$  into  $A(W)$  such that  $f(x) = x\gamma$  for every  $x \in V$ . Clearly  $f$  is a bijection. Put  $f(\alpha) = \alpha^\gamma$  for  $\alpha \in G(V)$ . Then for  $x \in V$  we have  $x\tau(\alpha)\gamma = (\alpha^{-1}x\alpha)^\gamma = (\alpha^\gamma)^{-1}x^\gamma\alpha^\gamma = x^\gamma\tau(\alpha^\gamma)$ ; thus  $\tau(\alpha)\gamma = \gamma\tau(\alpha^\gamma)$ . If  $\alpha = x_1 \cdots x_m \in G^\pm(V)$  with  $x_i \in V$ , then  $\alpha^\gamma = (x_1\gamma) \cdots (x_m\gamma)$ , and so  $\alpha^\gamma \in G^\pm(W)$ , and  $\nu(\alpha^\gamma) = \psi[x_1\gamma] \cdots \psi[x_m\gamma] = \varphi[x_1] \cdots \varphi[x_m] = \nu(\alpha)$ . From this we immediately obtain  $\sigma(\gamma^{-1}\xi\gamma) = \sigma(\xi)$  for  $\xi = \tau(\alpha)$ . The case  $(V, \varphi) = (W, \psi)$  is merely a special case.

**24.10.** Given  $(V, \varphi)$  as before, we denote by  $G^c(V)$  the commutator subgroup of  $O^\varphi(V)$ . We investigate this group in connection with the group

$$(24.8) \quad S^\circ(V, \varphi) = S^\circ(V) = \{\alpha \in SO^\varphi(V) \mid \sigma(\alpha) = 1\},$$

where  $\sigma$  is the map of (24.7). Clearly  $G^c(V) \subset SO^\varphi(V)$  and  $\sigma(G^c(V)) = 1$ , and so  $G^c(V) \subset S^\circ(V)$ . For every  $c \in F^\times$  we have  $SO^{c\varphi}(V) = SO^\varphi(V)$  and  $S^\circ(V, c\varphi) = S^\circ(V, \varphi)$ , as can be seen from Lemma 24.9(i).

**Lemma 24.11.** *The group  $G^c(\varphi)$  is generated by the elements of the form  $\tau(xyxy)$  with invertible  $x, y \in V$ .*

PROOF. Since  $\tau(x) = \tau(x)^{-1}$ , we see that  $\tau(xyxy) \in G^c(V)$ . Let  $H$  be the subgroup of  $O^\varphi$  generated by such elements  $\tau(xyxy)$ . Then  $H \subset G^c(V)$ . For every  $\gamma \in O^\varphi$  we have, by Lemma 24.9(ii),  $\gamma^{-1}\tau(xyxy)\gamma = \tau(x^\gamma y^\gamma x^\gamma y^\gamma)$ , where  $z^\gamma = z\gamma$ . Thus  $H$  is a normal subgroup of  $O^\varphi$ . Since  $\tau(xyxy) \in H$  and  $O^\varphi$  is generated by the elements of the form  $-\tau(x)$ , we see that  $O^\varphi/H$  is commutative. Thus  $G^c(V) \subset H$ , and so  $G^c(V) = H$  as expected.

**Lemma 24.12.** *Let  $U$  be a subspace of  $V$ . If  $\varphi[U] = \varphi[V]$  and  $G^c(U) = S^\circ(U)$ , then  $G^c(V) = S^\circ(V)$ .*

PROOF. Given  $\alpha \in S^\circ(V)$ , we can put  $\alpha = \xi_1 \cdots \xi_r$ ,  $\xi_i = \tau(x_i)$ , with  $x_i \in V$ . Take  $y_i \in U$  so that  $y_i^2 = x_i^2$  and put  $\beta = \eta_1 \cdots \eta_r$  with  $\eta_i = \tau(y_i)$ . Let  $f$  denote the natural map of  $O^\varphi(V)$  onto  $O^\varphi(V)/G^c(V)$ . Since the last group is commutative,  $f(\alpha\beta^{-1}) = f(\xi_1 \cdots \xi_r \eta_r \cdots \eta_1) = f(\xi_1 \eta_1 \cdots \xi_r \eta_r)$ . We have

$\xi_i \eta_i = \tau(x_i y_i)$ . Since  $x_i^2 = y_i^2$ , by Lemma 22.5(ii),  $x_i = y_i \gamma$  with some  $\gamma \in O^\varphi(V)$ . Then  $\tau(x_i) = \gamma^{-1} \tau(y_i) \gamma$  by Lemma 24.9(ii), and so  $\xi_i \eta_i = \tau(x_i y_i) = \gamma^{-1} \tau(y_i) \gamma \tau(y_i) \in G^c(V)$ . This shows that  $\alpha \in \beta G^c(V)$ . Since  $\sigma(\alpha) = 1$ , we have  $x_1^2 \cdots x_r^2 \in F^{\times 2}$ , and so  $y_1^2 \cdots y_r^2 \in F^{\times 2}$ . Thus  $\beta \in S^\circ(U) = G^c(U)$ . Viewing an element  $\omega$  of  $O^\varphi(U)$  as an element of  $O^\varphi(V)$  by defining the action of  $\omega$  on  $U^\perp$  to be the identity map, we find that  $\beta \in G^c(V)$ , and so  $\alpha \in G^c(V)$ , which proves our lemma.

**Lemma 24.13.** *If  $1 \leq n \leq 3$  or  $\varphi$  is isotropic, then  $G^c(V) = S^\circ(V)$ .*

PROOF. The case  $n = 1$  is trivial, since  $SO(\varphi) = \{1\}$ . The case  $n$  is 2 or 3 will be proven in Lemma 25.2 below. Suppose  $\varphi$  is isotropic. Then  $V$  has a two-dimensional subspace  $U$  on which  $\varphi$  is nondegenerate and isotropic. Then  $\varphi[U] = F$  and  $G^c(U) = S^\circ(U)$  by virtue of the result in the case  $n = 2$ . Therefore, by Lemma 24.12,  $G^c(V) = S^\circ(V)$ .

**Remark 24.14.** In this book we are interested only in the algebraic and arithmetic aspects of quadratic forms and orthogonal groups, not in their Lie-theoretical aspects, nor in the symmetric spaces associated with them. Here we content ourselves with merely mentioning a few basic facts on such topics.

Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $\mathbf{R}$ . Then  $SO^\varphi(V)$  is connected if  $\varphi$  is positive or negative definite; otherwise  $SO^\varphi(V)$  has two connected components. If  $\varphi$  is definite and  $\dim(V) > 2$ , then  $G^1(V)$  is simply connected and the map  $\tau : G^1(V) \rightarrow SO^\varphi(V)$  is the covering map.

For these the reader is referred to standard textbooks on Lie groups; some easy related facts are proved in [S04b]. For instance, the symmetric spaces associated with  $SO^\varphi(V)$  are explicitly described in Section 16 of the book; also the spin representations and the structure of the Lie algebra of  $SO^\varphi(V)$  are discussed in Section A5 of the book.

## 25. Lower-dimensional cases

**25.1.** As will be proven in Theorem 25.5 below, a quadratic form on a space of dimension  $> 4$  over a local field (in the sense of §21.1) is always isotropic. Thus, over a local field, we have a Witt decomposition (1.2a) with an anisotropic space  $Z$  of dimension  $\leq 4$ . Therefore it is important to investigate the Clifford algebra and spin group of such a  $Z$ . First we consider the problem with an arbitrary field  $F$  of characteristic  $\neq 2$ . We fix a vector space  $V$  over  $F$  of dimension  $\leq 4$  and a nondegenerate quadratic form  $\varphi$  defined on  $V$ , which may or may not be anisotropic for the moment. We also denote by  $x \mapsto x^*$  the canonical involution of  $A(\varphi)$ .

As we said in §23.2,  $A(V) = A^+(V) = F$  if  $V = \{0\}$ .

Suppose  $\dim(V) = 1$ ; put  $V = Fh$ . Then  $A(V) = F + Fh$ ,  $A^+(V) = F$ , and  $A^-(V) = Fh$ . We easily see that  $G^+(V) = F^\times$ ,  $G^1(V) = \{\pm 1\}$ ,  $G^-(V) = F^\times h$ ,

and  $G(V) = A(V)^\times$ ;  $O^\varphi(V) = \{\pm 1\}$  and  $SO^\varphi(V) = \{1\}$ .

Before discussing  $(V, \varphi)$  of general types, we mention special forms of quadratic spaces of dimension  $\leq 4$ . We first take a couple  $(K, \rho)$  consisting of an  $F$ -algebra  $K$  of rank 2 and an  $F$ -linear automorphism  $\rho$  of  $K$  belonging to the following two types:

(25.1a)  $K$  is a quadratic extension of  $F$  and  $\rho$  is the generator of  $\text{Gal}(K/F)$ ;

(25.1b)  $K = F \oplus F$  and  $(a, b)^\rho = (b, a)$  for  $(a, b) \in F \oplus F$ .

In both cases we obtain a quadratic space  $(K, \kappa)$  of dimension 2 by putting  $\kappa[x] = xx^\rho$  for  $x \in K$ ; we have  $2\kappa(x, y) = \text{Tr}_{K/F}(xy^\rho)$  for  $x, y \in K$ . We call  $\kappa$  the **norm form** of  $K$ . Clearly  $\kappa$  is anisotropic if and only if  $K$  is a field. For every  $c \in F^\times$  the discriminant algebra of  $(K, c\kappa)$  is  $K$  itself.

Next we take a quaternion algebra  $B$  over  $F$  and consider its main involution  $\iota$ . We recall that  $\text{Tr}_{B/F}(x) = x + x^\iota$  and  $N_{B/F}(x) = xx^\iota$  for  $x \in B$ . We have  $F = \{x \in B \mid x^\iota = x\}$ , and so we have a direct sum decomposition

$$(25.2) \quad B = F \oplus B^\circ \quad \text{with} \quad B^\circ = \{x \in B \mid x^\iota = -x\};$$

see Theorem 20.6 and Lemma 20.7. Given  $B$ , we always define  $B^\circ$  in this way. An element of  $B^\circ$  is traditionally called a **pure quaternion**. Putting  $\beta[x] = xx^\iota$  for  $x \in B$ , we call  $\beta$  the **norm form** of  $B$ . Then  $(B, \beta)$  is a quadratic space of dimension 4. Denoting by  $\beta^\circ$  the restriction of  $\beta$  to  $B^\circ$ , we obtain a quadratic space  $(B^\circ, \beta^\circ)$  of dimension 3. We easily see that

$$(25.3) \quad B \text{ is a division algebra} \iff \beta \text{ is anisotropic} \iff \beta^\circ \text{ is anisotropic}.$$

We also see that  $2\beta(x, y) = \text{Tr}_{B/F}(xy^\iota)$  for  $x, y \in B$ , since  $2\beta(x, y) = \beta[x + y] - \beta[x] - \beta[y]$ . If  $B = \{K, \gamma\} = K + Kw$  with  $\gamma \in F^\times$ , an element  $w$  such that  $w^2 = \gamma$ , and  $K$  as in (25.1a, b), then  $\beta[x + yw] = N_{K/F}(x) - \gamma N_{K/F}(y)$  for  $x, y \in K$ . Thus

$$(25.3a) \quad (B, \beta) \cong (K, \kappa) \oplus (K, -\gamma\kappa).$$

From this we easily see that  $1 \in \delta_0(\beta) = \delta_0(-\beta^\circ)$ . Thus  $F$  is the discriminant field of both  $(B, \beta)$  and  $(B^\circ, -\beta^\circ)$ .

**Lemma 25.2.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space of dimension  $n$ , and  $K$  the discriminant algebra of  $\varphi$ , which we view as a subalgebra of  $A(\varphi)$ ; see Lemma 23.7(v). Let  $G^c(V)$  and  $S^\circ(V)$  be as in §24.10. Then the following assertions hold.*

(i) *If  $n = 2$ ,  $(V, \varphi)$  is isomorphic to  $(K, c\kappa)$  with some  $c \in F^\times$ , where  $\kappa$  is the norm form of  $K$ . Moreover,  $A(\varphi)$  is a quaternion algebra  $\{K, c\}$  in the sense of §20.2,  $A^+(\varphi) = K$ ,  $SO^\varphi(V) = \{b \in K^\times \mid bb^\rho = 1\}$ ,  $G^+(\varphi) = K^\times$ ,  $G(\varphi) = K^\times \cup K^\times h$  for any  $h \in V$ ,  $h \neq 0$ ,  $\alpha^* = \alpha^\rho$ ,  $\tau(\alpha) = \alpha^{-1}\alpha^\rho$ ,  $\nu(\alpha) = N_{K/F}(\alpha)$  for  $\alpha \in G^+(\varphi)$ , and  $G^c(V) = S^\circ(V)$ .*

(ii) If  $n = 3$ , there exists a quaternion algebra  $B$  over  $F$  such that  $(V, \varphi)$  is isomorphic to  $(B^\circ, -\delta\beta^\circ)$  with  $\delta \in \delta_0(\varphi)$ . Moreover,  $A(\varphi) = A^+(\varphi) \otimes_F K$ ,  $A^+(\varphi) \cong B$ ,  $G^+(\varphi) \cong B^\times$ ,  $x\tau(b) = b^{-1}xb$  for  $x \in B^\circ$  and  $b \in B^\times = G^+(\varphi)$ , and the canonical involution of  $A(\varphi)$  restricted to  $A^+(\varphi)$  corresponds to the main involution of  $B$ . Furthermore,  $G^c(V) = S^\circ(V)$ .

PROOF. Suppose  $n = 2$ ; let  $V = Fg + Fh$  with elements  $g$  and  $h$  such that  $\varphi(g, h) = 0$ . Put  $b = g^2$ ,  $c = h^2$ , and  $z = gh$ . Then  $\varphi[xg + yh] = bx^2 + cy^2$  for  $x, y \in F$ ,  $z^2 = -bc$ ,  $A^+(\varphi) = K = F + Fz$ ,  $V = Kh$ , and  $A(\varphi) = K + Kh$ . Since  $z^* = -z$ , we see that  $\alpha^* = \alpha^\rho$  for  $\alpha \in K$ . We have  $\varphi[\xi h] = cN_{K/F}(\xi)$  for  $\xi \in K$ , and so  $\xi \mapsto \xi h$  gives an isomorphism of  $(K, c\kappa)$  onto  $(V, \varphi)$ . Since  $h\xi = \xi^*h$  for  $\xi \in K$ , we see that  $A(\varphi) = \{K, c\}$ . We easily see that  $K^\times = A^+(\varphi)^\times \subset G(\varphi)$  and  $h \in G^-(\varphi)$ , and so, by Theorem 24.6(ii),  $K^\times = G^+(\varphi)$  and  $G(\varphi) = K^\times \cup K^\times h$ .

Next let  $\alpha \in K^\times = G^+(\varphi)$  and  $x = \xi h \in V$  with  $\xi \in K$ . Then  $x\tau(\alpha) = \alpha^{-1}\xi h\alpha = \alpha^{-1}\alpha^\rho x$ . Thus  $\tau(\alpha)$  as an element of  $\text{End}_F(Kh)$  is multiplication by  $\alpha^{-1}\alpha^\rho$ . Therefore  $SO^\circ = \tau(G^+(\varphi)) = \{\eta \in K^\times \mid \eta\eta^\rho = 1\}$  by Lemma 1.8, which is valid even when  $K = F \oplus F$ . Also,  $\tau(h)^{-1}\tau(\alpha)\tau(h) = \tau(\alpha^\rho)$  for  $\alpha \in K^\times$ . For  $\eta = \alpha^{-1}\alpha^\rho = \tau(\alpha) \in SO^\circ$  we have  $\sigma(\eta) = \alpha\alpha^\rho$ , and so  $\eta \in S^\circ$  if and only if  $\alpha\alpha^\rho = s^2$  with  $s \in F^\times$ . Put  $\zeta = s^{-1}\alpha$ . Then  $\zeta\zeta^\rho = 1$  and  $\zeta^{-2} = \eta$ . By Lemma 1.8,  $\zeta = \gamma^{-1}\gamma^\rho$  with  $\gamma \in K^\times$ . Then  $\eta = \zeta^{-1}\zeta^\rho = \tau(\zeta) = \tau(\gamma^{-1}\gamma^\rho) = \tau(\gamma)^{-1}\tau(h)^{-1}\tau(\gamma)\tau(h) \in G^c(V)$ . Thus  $G^c(V) = S^\circ(V)$ .

Next suppose  $n = 3$ . Let  $\{h_i\}_{i=1}^3$  be an  $F$ -basis of  $V$  such that  $\varphi(h_i, h_j) = c_i\delta_{ij}$  with  $c_i \in F^\times$ . Put

$$\begin{aligned} g_1 &= h_2h_3, & g_2 &= h_3h_1, & g_3 &= h_1h_2, & z &= h_1h_2h_3, \\ d &= c_1c_2c_3, & T &= Fg_1 + Fg_2 + Fg_3, & B &= F + T. \end{aligned}$$

Then  $z^2 = -d \in \delta_0(\varphi)$ ,  $A^+(\varphi) = B$ ,  $K = F + Fz$ , and  $A(\varphi) = B + Bz$ . By Theorem 23.8(ii),  $A(\varphi) = B \otimes_F K$ , and  $B$  is a quaternion algebra over  $F$ . Since  $g_i^* = -g_i$ , we see that  $\alpha \mapsto \alpha^*$  coincides with the main involution of  $B$ , and so  $T = B^\circ$ . Since  $V = B^\circ z$  and  $\varphi[xz] = dxx^*$  for  $x \in B^\circ$ ,  $(V, \varphi)$  is isomorphic to  $(B^\circ, d\beta^\circ)$ . We have  $b^{-1}B^\circ b = B^\circ$  for every  $b \in B^\times$ , and so  $G^+(\varphi) = B^\times$ .

As for  $S^\circ(V)$ , we have  $SO(\varphi) = \tau(G^+(\varphi)) = \tau(B^\times)$ , and  $x\tau(\beta) = b^{-1}xb$  for  $b \in B^\times$  and  $x \in B^\circ$ . Thus, from (24.7a) we obtain

$$(25.3b) \quad S^\circ(V) = \tau(B^1), \quad G^1(\varphi) = B^1 = \{\gamma \in B^\times \mid \gamma\gamma^\iota = 1\}.$$

Therefore Lemma 20.9 shows that  $S^\circ(V) = G^c(V)$ . This completes the proof.

**25.3.** Let us now discuss the case  $n = 4$ . The structure of  $(V, \varphi)$  depends on  $\delta_0(\varphi)$  and also on whether or not  $\varphi$  is isotropic. We first prove easy facts applicable to all cases:

$$(25.4a) \quad V = \{x \in A^-(V) \mid x^* = x\} \quad \text{if } \dim(V) = 4,$$

$$(25.4b) \quad F + Fz = \{x \in A^+(V) \mid x^* = x\} \quad \text{if } \dim(V) = 4,$$

$$(25.4c) \quad G^\pm(V) = \{x \in A^\pm(V) \mid \alpha\alpha^* \in F^\times\} \quad \text{if } \dim(V) = 4,$$

where  $z$  is as in Lemma 23.7. We can easily derive (25.4a) from the fact that  $A^-(V) = V + \sum_{i < j < k} F e_i e_j e_k$  with an orthogonal basis  $\{e_i\}_{i=1}^4$  of  $V$ ; (25.4b) is similar. Clearly  $G^\pm(V)$  is contained in the right-hand side of (25.4c). Conversely, let  $\alpha \in A(V)^\times \cap A^\pm(V)$ . Then for  $x \in V$  we have  $\alpha^* x \alpha \in A^-(V)$  and  $(\alpha^* x \alpha)^* = \alpha^* x \alpha$ , so that  $\alpha^* x \alpha \in V$  by (25.4a). If  $\alpha\alpha^* \in F^\times$ , then  $\alpha^{-1} x \alpha \in V$ , so that  $\alpha \in G(V)$ . This proves (25.4c).

(A) Let us now consider the case of isotropic  $\varphi$ . We can then put  $V = U + Fe + Ff$  with a subspace  $U$  of dimension 2 and  $e, f$  as in (23.6a). Then by Theorem 23.6,  $A(V)$  resp.  $A^+(V)$  is isomorphic to  $M_2(A(U))$  resp.  $M_2(A^+(U))$ . Let  $K$  be the discriminant algebra of  $(V, \varphi)$ , which is also the discriminant algebra of  $(U, \varphi)$ . By Lemma 25.2(i) and its proof we can put  $A^+(U) = K$  and  $U = Kh$  with an element  $h$  such that  $ha = a^*h$  for every  $a \in K$ . Define  $\Xi : A(V) \rightarrow M_2(A(U))$  by (23.14) with  $h$  as  $g$  there. Then from (23.10) we can easily derive that

$$(25.4d) \quad \Xi(\alpha^*) = J^{-1} \cdot {}^t \Xi(\alpha') J \quad \text{for every } \alpha \in A(V).$$

Now  $\xi \mapsto J^{-1} \cdot {}^t \xi J$  is the main involution of  $M_2(K)$ ; see (20.11). Therefore if we identify  $A^+(V)$  with  $M_2(K)$ , then (25.4d) shows that  $\alpha \mapsto \alpha^*$  is the main involution of  $M_2(K)$ . Thus (25.4c) for  $G^+(V)$  can be written

$$(25.4e) \quad \begin{aligned} \Xi(G^+(V)) &= \{\xi \in GL_2(K) \mid \det(\xi) \in F^\times\} \quad \text{and} \\ \nu(\alpha) &= \det(\xi) \quad \text{if } \xi = \Xi(\alpha) \quad \text{with } \alpha \in G^+(V). \end{aligned}$$

(B) Let us next treat the situation which will become necessary for our later local analysis. We take a quaternion algebra  $B$  over  $F$  and put  $(V, \varphi) = (B, d\beta)$  with  $\beta$  as in §25.1 and  $d \in F^\times$ . We consider a map

$$(25.5a) \quad p : B \longrightarrow M_2(B) \quad \text{given by} \quad p(x) = \begin{bmatrix} 0 & dx \\ x^t & 0 \end{bmatrix} \quad \text{for } x \in B.$$

Observe that  $p(x)^2 = dx x^t 1_2 = \varphi[x] 1_2$ . Now  $p(B)$  generates  $M_2(B)$  over  $F$ . Indeed, take two elements  $x$  and  $y$  of  $B$  such that  $xy = -yx \in B^\times$ . Then  $p(xy)p(1) = d \cdot \text{diag}[xy, y^t x^t]$  and  $p(x)p(y^t) = d \cdot \text{diag}[xy, -y^t x^t]$ , so that  $p(xy)p(1) + p(x)p(y^t) = \text{diag}[2dxy, 0]$ . In this way we can easily verify that the whole  $M_2(B)$  can be generated by  $p(B)$  over  $F$ . By (23.1) we can thus put  $M_2(B) = A(V)$  with  $V = p(B)$ , that is,

$$(25.5b) \quad V = \left\{ \begin{bmatrix} 0 & dx \\ x^t & 0 \end{bmatrix} \mid x \in B \right\}.$$

Then  $A^+(V) = \{\text{diag}[a, b] \mid a, b \in B\} \cong B \oplus B$ . For  $\alpha = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in M_2(B) =$

$A(V)$ , we have  $\alpha^* = \begin{bmatrix} p^t & dr^t \\ d^{-1}q^t & s^t \end{bmatrix}$ , since this is so for every  $\alpha \in V$ . If we identify  $A^+(V)$  with  $B \times B$  in an obvious fashion, then

$$(25.6a) \quad G^+(V) = \{(a, b) \in B^\times \times B^\times \mid aa^t = bb^t\},$$

$$(25.6b) \quad G^1(V) = \{(a, b) \in B^\times \times B^\times \mid aa^t = bb^t = 1\},$$

$\nu((a, b)) = aa^t$  for  $(a, b) \in G^+(V)$ , and  $p(x)\tau(\alpha) = p(a^{-1}xb)$  for  $x \in B$  and  $\alpha = (a, b) \in G^+(V)$ . Furthermore,  $G(V) = G^+(V) \cup G^+(V)\eta$  with  $\eta = \begin{bmatrix} 0 & d \\ 1 & 0 \end{bmatrix}$  and  $p(x)\tau(\eta) = p(x^t)$  for every  $x \in V$ . The main involution  $\iota$  of  $B$  belongs to  $O^\varphi$  and has determinant  $-1$ . Thus  $O^\varphi$  is generated by  $SO^\varphi$  and  $\iota$ .

**Theorem 25.4.** (i) *Given a nondegenerate quadratic space  $(V, \varphi)$  over a field  $F$  of characteristic different from 2, suppose that  $\dim(V) = 4$  and  $1 \in \delta_0(\varphi)$ . Then there exists a quaternion algebra  $B$  over  $F$  such that  $(V, \varphi)$  is isomorphic to  $(B, d\beta)$  with  $d \in F^\times$ , where  $\beta$  is the norm form of  $B$ .*

(ii) *Given  $(V, \varphi)$  over a local field  $F$ , suppose  $\dim(V) = 4$  and  $\varphi$  is anisotropic. Then  $1 \in \delta_0(\varphi)$  and  $(V, \varphi)$  is isomorphic to  $(B, \beta)$  with a division quaternion algebra  $B$  over  $F$ , whose uniqueness is established in Theorem 21.22.*

(iii) *For a division quaternion algebra  $B$  over a local field  $F$  we have*

$$\{y^2 \mid 0 \neq y \in B^\circ\} = \{s \in F^\times \mid s \notin F^{\times 2}\}.$$

(iv) *If  $(V, \varphi) = (B, d\beta)$ , then  $G^c(V) = S^\circ(V)$ , where the symbols are as in §24.10.*

PROOF. To prove (i), take a decomposition  $V = U + Fe$  with an element  $e$  such that  $e^2 \neq 0$  and  $U = (Fe)^\perp$ . By Lemma 25.2(ii) there exist a quaternion algebra  $B$  over  $F$  and an isomorphism  $f$  of  $(B^\circ, d\beta^\circ)$  onto  $(U, \varphi)$  with  $-d \in \delta_0(U, \varphi)$ . Since  $1 \in \delta_0(V, \varphi)$ , we see that  $\varphi[e] = db^2$  with  $b \in F^\times$ . Define  $\alpha : B \rightarrow V$  by  $(a + x)\alpha = ab^{-1}e + xf$  for  $a \in F$  and  $x \in B^\circ$ . Then  $\varphi[(a + x)\alpha] = a^2b^{-2}\varphi[e] + dxx^t = dN_{B/F}(a + x)$ , and so  $\alpha$  is an isomorphism of  $(B, d\beta)$  onto  $(V, \varphi)$ . This proves (i).

To prove (iii), given  $0 \neq y \in B^\circ$ , put  $J = F[y]$ . Since  $y \notin F$ ,  $J$  is a quadratic extension of  $F$ , and so  $y^2 \notin F^{\times 2}$ . Conversely, let  $s \in F$  and  $s \notin F^{\times 2}$ . By Theorem 21.23(ii),  $B$  contains a quadratic extension  $F[x]$  with an element  $x$  such that  $x^2 = s$ . Then  $x^t = -x$ , so that  $x \in B^\circ$ . This proves (iii).

To prove (ii), take  $e, B, B^\circ, d$ , and  $f$  as in the proof of (i), without assuming that  $1 \in \delta_0(\varphi)$ . Put  $c = \varphi[e]$ . Since  $\varphi$  is anisotropic,  $B$  is a division algebra by (25.3). Suppose  $c/d \notin F^{\times 2}$ ; then by (iii),  $B^\circ$  contains an element  $z$  such that  $z^2 = c/d$ . Then  $\varphi[e + zf] = c + dzz^t = 0$ , a contradiction, since  $\varphi$  is anisotropic. Therefore  $c/d \in F^{\times 2}$ , so that  $1 \in \delta_0(\varphi)$ . By (i),  $(V, \varphi)$  is isomorphic to  $(B_1, d_1\beta_1)$  with a quaternion algebra  $B_1$  and  $d_1 \in F^\times$ , where

$\beta_1$  is the norm form of  $B_1$ . By Theorem 21.23(i),  $d_1 = bb'$  with some  $b \in B_1^\times$ . Then  $x \mapsto b^{-1}x$  gives the desired isomorphism.

To prove (iv), we first note that  $\tau(G^1(V)) = S^\circ(V)$  as noted in (24.7a). Thus, from (25.6b) we obtain

$$S^\circ(V) = \{\tau(a, b) \mid a, b \in B^1\}, \quad B^1 = \{x \in B^\times \mid xx^t = 1\}.$$

Since  $O^\circ(V)$  contains  $\tau(a, b)$  for  $(a, b) \in B^\times \times B^\times$  and  $\tau(a, 1)\tau(1, b) = \tau(a, b)$ , our assertion of (iv) follows from Lemma 20.9.

**Theorem 25.5.** *For a nondegenerate quadratic space  $(V, \varphi)$  over a local field  $F$  the following assertions hold:*

(i) *If  $\dim(V) \geq 4$ , then every element of  $F$  can be written  $\varphi[x]$  with some  $x \in V$ .*

(ii) *If  $\dim(V) > 4$ , then  $\varphi$  is isotropic.*

PROOF. Take any subspace  $W$  of  $V$  of dimension 4 on which  $\varphi$  is nondegenerate. If  $\varphi$  is isotropic on  $W$ , then the conclusions of both (i) and (ii) are true; so assume that  $\varphi$  is anisotropic on  $W$ . By Theorem 25.4(ii),  $\varphi$  on  $W$  is isomorphic to the norm form on a division quaternion algebra  $B$  over  $F$ . Therefore, by Theorem 21.23(i), given any  $a \in F$ , we can find an element  $x$  of  $W$  such that  $\varphi[x] = a$ , which proves (i). Assuming  $\dim(V) > 4$ , take  $a = -\varphi[y]$  with any nonzero element  $y$  of  $W^\perp$ . Then  $\varphi[x + y] = 0$ . Since  $x + y \neq 0$ , this shows that  $\varphi$  is isotropic on  $V$ .

**25.6.** We have seen that

$$(25.7) \quad G^1(V) = \{\alpha \in A^+(V)^\times \mid \alpha\alpha^* = 1\}$$

at least for  $1 \leq n \leq 4$ . Indeed, this is trivial for  $n = 1$ ; the case  $n = 2$  or  $3$  is shown in Lemma 25.2, since  $G^+(V) = A^+(V)^\times$  then; the formula in the case  $n = 4$  follows from (25.4c). Actually (25.7) is true also for  $n = 5$  and  $6$ . The proof is given in [S06b, (7.5a) and (7.10)].

Before proceeding further, we note easy facts. Let  $B$  and  $C$  be quaternion algebras over a field  $F$  and let  $\beta$  and  $\gamma$  be their norm forms. Then

$$(25.8) \quad B \cong C \iff (B, \beta) \cong (C, \gamma) \iff (B^\circ, \beta^\circ) \cong (C^\circ, \gamma^\circ).$$

Here the first  $\cong$  is an isomorphism between  $F$ -algebras, and the latter two  $\cong$  are isomorphisms of quadratic spaces. The first  $\implies$  is obvious. The next  $\implies$  follows from the fact that  $B^\circ = (F\varepsilon)^\perp$  with an element  $\varepsilon$  such that  $\beta[\varepsilon] = 1$ . Finally  $A^+(B^\circ, \beta^\circ) \cong B$ , and so the last  $\cong$  implies the first  $\cong$ .

**25.7.** We now assume that  $F$  is a global field, that is, an algebraic number field of finite degree, and use the symbols  $\mathbf{a}$ ,  $\mathbf{h}$ , and  $\mathbf{v}$  as in §§15.1 and 21.5. For a nondegenerate quadratic space  $(V, \varphi)$  over  $F$  and  $v \in \mathbf{v}$  we define a quadratic space  $(V, \varphi)_v = (V_v, \varphi_v)$  over  $F_v$  by putting  $V_v = V \otimes_F F_v$  and

denoting by  $\varphi_v$  the  $F_v$ -bilinear extension of  $\varphi$  to  $V_v \times V_v$ . For simplicity we will often write  $\varphi[y]$  for  $\varphi_v[y]$  with  $y \in V_v$ . We will eventually show that the structures  $(V, \varphi)_v$  for all  $v \in \mathbf{v}$  determine  $(V, \varphi)$ . In particular,  $(V, \varphi)$  is isotropic if  $(V, \varphi)_v$  is isotropic for every  $v \in \mathbf{v}$ . In the rest of this section we prove the special case in which  $F = \mathbf{Q}$  and  $\dim(V) = 3$ . For this we need an elementary result:

**Lemma 25.8.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $\mathbf{Q}$  of dimension  $n$  and let  $L = \sum_{i=1}^n \mathbf{Z}e_i$  with a  $\mathbf{Q}$ -basis  $\{e_i\}_{i=1}^n$  of  $V$ . Suppose  $\varphi$  as a real quadratic form on  $V \otimes_{\mathbf{Q}} \mathbf{R}$  has  $r$  positive and  $s$  negative eigenvalues. Then  $L$  has a nonzero element  $x$  such that  $|\varphi[x]| \leq \text{Max}(r, s)|\det(\Phi)|^{1/n}$ , where  $\Phi = (\varphi(e_i, e_j))_{i,j=1}^n$ .*

PROOF. We have  $\Phi = A \cdot \text{diag}[1_r, -1_s] \cdot {}^t A$  with  $A \in GL_n(\mathbf{R})$ . Then  $|\det(A)|^2 = |\det(\Phi)|$ . Let  $b = |\det(A)|^{1/n}$ . Then by Theorem 12.5(ii) there exists  $\xi \in \mathbf{Z}_n^1, \neq 0$ , such that  $|(\xi A)_i| \leq b$ . Then  $|\xi \Phi \cdot {}^t \xi| = |\sum_{i=1}^r (\xi A)_i^2 - \sum_{j=r+1}^b (\xi A)_i^2| \leq \text{Max}(r, s)b^2$ , and so we obtain our lemma.

**Theorem 25.9.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $\mathbf{Q}$  of dimension 3 such that  $\varphi_v$  is isotropic for every  $v \in \mathbf{v}$ . Then  $\varphi$  is isotropic.*

PROOF. By Lemma 25.2,  $(V, \varphi) \cong (B^\circ, c\beta^\circ)$  with a quaternion algebra  $B$  over  $\mathbf{Q}$  and  $c \in \mathbf{Q}^\times$ . Our condition on  $\varphi_v$  means that  $B_\infty \cong M_2(\mathbf{R})$  and  $B_p \cong M_2(\mathbf{Q}_p)$  for every prime number  $p$ ; see (25.3). Thus our aim is to show that  $B \cong M_2(\mathbf{Q})$ . Replacing  $\varphi$  by  $c^{-1}\varphi$ , we may assume that  $c = 1$ . Let  $L = B^\circ \cap \mathfrak{o}$  with a maximal order  $\mathfrak{o}$  in  $B$ . By Lemma 21.7(ii),  $\mathfrak{o}_p$  is a maximal order in  $B_p$ , and so by Lemmas 21.4 and 21.9,  $\mathfrak{o}_p = \alpha_p^{-1}M_2(\mathbf{Z}_p)\alpha_p$  with  $\alpha_p \in GL_2(\mathbf{Q}_p)$ . Thus  $\alpha_p L_p \alpha_p^{-1} = \{x \in M_2(\mathbf{Z}_p) \mid \text{tr}(x) = 0\}$ , and so  $\beta^\circ$  on  $L_p$  can be represented by  $\text{diag}\left[2^{-1} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, -1\right]$ . Define  $\Phi$  as in Lemma 25.8 for the present  $L$ . Then  $\det(\Phi)\mathbf{Z}_p = 4^{-1}\mathbf{Z}_p$  for every  $p$  and  $\det(\Phi) > 0$ , and so  $\det(\Phi) = 4^{-1}$ . Therefore that lemma guarantees an element  $y \in L, \neq 0$ , such that  $|\varphi[y]| \leq 2 \cdot 4^{-1/3} < 2$ . Since  $xx^t \in \mathbf{Z}$  for every  $x \in \mathfrak{o}$ , we have  $\varphi[y] = 0$  or  $\pm 1$ . The matter is settled if  $\varphi[y] = 0$ . Suppose  $\varphi[y] = -1$ . Since  $y^t = -y$ , we have  $y^2 = 1$ , and so  $(y-1)(y+1) = 0$ . if  $B$  is a division algebra, then  $y \pm 1 \neq 0$ , a contradiction. Thus  $B \cong M_2(\mathbf{Q})$  in the case  $\varphi[y] = -1$ .

Suppose  $\varphi[y] = 1$ ; let  $W = (\mathbf{Q}y)^\perp$  and let  $\psi$  be the restriction of  $\varphi$  to  $W$ . Since  $\det(\Phi) = 4^{-1}$ , we see that  $-1 \in \delta_0(\psi)$ . Thus, by Lemma 25.2(i),  $(W, \psi) \cong (K, -d^{-1}\kappa)$  with  $K = \mathbf{Q}(\sqrt{-1})$  and  $d \in \mathbf{Q}^\times$ . We see that  $d > 0$ . Replacing  $d$  by its suitable multiple, we may assume that  $d$  is a square-free integer. Since  $d$  can be replaced by  $bd$  with any  $b \in N_{K/\mathbf{Q}}(K^\times)$ , we may assume that  $d = 1$  or  $d$  is the product of prime numbers  $p$  such that  $p+1 \in 4\mathbf{Z}$ . If  $d = 1$ , then  $\psi[z] = -1$  for some  $z \in W$ , and so  $\varphi[y+z] = 0$ . Thus



$\varphi$  is isotropic as desired. Suppose  $d$  has a prime factor  $p$  such that  $p+1 \in 4\mathbf{Z}$ . Then  $K_p$  is unramified over  $\mathbf{Q}_p$ , and  $\kappa[x] \neq dc^2$  for every  $x \in K_p^\times$  and every  $c \in \mathbf{Q}_p^\times$  by Theorem 9.10(ii), which means that  $(V, \varphi)_p$  is anisotropic, a contradiction. This completes the proof.

## 26. The Hilbert reciprocity law

**26.1.** We consider a number field  $F$  and its completion  $F_v$  at a fixed  $v \in \mathbf{v}$ . Here  $\mathbf{v} = \mathbf{a} \cup \mathbf{h}$  with  $\mathbf{a}$  and  $\mathbf{h}$  as in §21.5. Given  $b, c \in F_v^\times$ , we consider a ternary form  $f(x, y, z) = x^2 - by^2 - cz^2$ . We call an element  $(x, y, z) \neq (0, 0, 0)$  of  $F_v^3$  such that  $f(x, y, z) = 0$  a **nontrivial zero** of  $f$ ; we use the same terminology with  $F$  as the base field in place of  $F_v$ . We now define a symbol  $(b, c)_v$  as follows:

$$(26.0) \quad \begin{aligned} (b, c)_v &= 1 && \text{if } x^2 - by^2 - cz^2 \text{ has a nontrivial zero in } F_v^3, \\ (b, c)_v &= -1 && \text{otherwise.} \end{aligned}$$

This is called the **Hilbert symbol** and satisfies

$$(26.1) \quad (b, c)_v = (c, b)_v,$$

$$(26.2) \quad (b, c)_v = 1 \iff c \in N_{K/F_v}(K^\times), \quad K = F_v(\sqrt{b}).$$

The first fact is trivial. If  $\sqrt{b} \in F_v$ , then  $b$  is a square in  $F_v$ , and clearly  $(b, c)_v = 1$ . Suppose  $K = F_v(\sqrt{b}) \neq F_v$ . Suppose also  $(\xi, \eta, \zeta)$  is a nontrivial zero of  $x^2 - by^2 - cz^2$  in  $F_v^3$ . Then  $\zeta \neq 0$  as  $b$  is not a square in  $F_v$ , and  $c = N_{K/F_v}((\xi + \eta\sqrt{b})/\zeta)$ . Conversely, if  $c \in N_{K/F_v}(K^\times)$ , then we easily see that  $(b, c)_v = 1$ . This proves (26.2). We also have

$$(26.3) \quad (b, cc')_v = (b, c)_v(b, c')_v,$$

$$(26.4) \quad (bb', c)_v = (b, c)_v(b', c)_v.$$

These can be proved as follows. If  $v$  is an imaginary archimedean prime, then  $F_v = \mathbf{C}$  and  $(b, c)_v$  is always 1. If  $v$  is a real archimedean prime or a nonarchimedean prime, then  $[F_v^\times : N_{K/F_v}(K^\times)] = 2$  for every quadratic extension  $K$  of  $F_v$ . This is trivial if  $v$  is real. For  $v$  nonarchimedean the fact is given in Theorem 9.10(i). Therefore (26.3) follows from (26.2); (26.4) follows from this and (26.1).

**Theorem 26.2.** *Let  $F$  be a global field and let  $b, c \in F^\times$ . Then  $(b, c)_v = 1$  for almost all  $v \in \mathbf{v}$ .*

PROOF. Let  $K = F(\sqrt{b})$ . There is no problem if  $K = F$ , and so we assume  $K \neq F$ . Let  $v \in \mathbf{h}$ . If  $v$  splits in  $K$ , then  $F_v(\sqrt{b}) = F_v$ , and so  $(b, c)_v = 1$ . Suppose  $v$  is unramified and does not split in  $K$ ; put  $K_v = K \otimes_F F_v$ . Then  $K_v = F_v(\sqrt{b})$ , which is an unramified quadratic extension of  $F_v$ . Suppose also  $c$  is a  $v$ -unit; then by Theorem 9.10(ii),  $c \in N_{K_v/F_v}(K_v^\times)$ , and so  $(b, c)_v = 1$ .

Since there are only finitely many  $v \in \mathbf{h}$  such that  $v$  is ramified in  $K$  or  $c$  is not a  $v$ -unit, we obtain our theorem.

**Theorem 26.3.** *Let  $F$  be a global field and let  $b, c \in F^\times$ ; also, let  $K = F(\sqrt{b})$  and  $K_v = K \otimes_F F_v$  for  $v \in \mathbf{v}$ . Then the following assertions hold:*

- (i)  $x^2 - by^2 - cz^2$  has a nontrivial zero in  $F^3$  if  $(b, c)_v = 1$  for all  $v \in \mathbf{v}$ .
- (ii) If  $c \in N_{K/F}(K_v^\times)$  for all  $v \in \mathbf{v}$ , then  $c \in N_{K/F}(K^\times)$ .

We easily see that  $x^2 - by^2 - cz^2$  has a nontrivial zero in  $F^3$  if and only if  $c \in N_{K/F}(K^\times)$ . (If the form has a nontrivial zero of the form  $(\xi, \eta, 0)$ , then  $K = F$ , and vice versa.) Therefore, in view of (26.2), (i) is equivalent to (ii). In fact, let  $H$  be a cyclic extension of  $F$  of an arbitrary degree, and let  $H_v = H \otimes_F F_v$ . Then for  $c \in F^\times$  we have

$$(26.5) \quad c \in N_{H/F}(H^\times) \quad \text{if} \quad c \in N_{H/F}(H_v^\times) \quad \text{for every } v \in \mathbf{v}.$$

This is called the **Hasse norm theorem** and (ii) is a special case of (26.5).

We have proved (i) in Theorem 25.9 when  $F = \mathbf{Q}$ , and consequently (ii) is established when  $F = \mathbf{Q}$ . Without proving either of them in the general case, we will derive other facts from them. Thus our book is self-contained only when  $F = \mathbf{Q}$ . Also, we will eventually state a more general result in Theorem 27.2(i) below of which (i) is a special case. For a detailed discussion of the Hasse norm theorem and the Hilbert reciprocity law stated below, the reader is referred to any textbook on class field theory, [CF] for example.

**Theorem 26.4.** *Let  $F$  be a global field and let  $b, c \in F^\times$ . Then*

$$(26.6) \quad \prod_{v \in \mathbf{v}} (b, c)_v = 1.$$

The infinite product is meaningful because of Theorem 26.2. This formula is called the **Hilbert reciprocity law**. Here we prove it only when  $F = \mathbf{Q}$ .

**PROOF.** In view of (26.3) and (26.4) it is sufficient to prove (26.6) when  $b$  or  $c$  is a prime number or  $-1$ . Also, we can exchange  $b$  and  $c$ . Thus there are four cases to be discussed: (A)  $b = c = -1$ ; (B)  $b = -1$  and  $c$  is a prime number; (C)  $b$  is a prime number and  $c = b$ ; (D)  $b$  and  $c$  are prime numbers and  $b \neq c$ . To find  $(b, c)_v$  in each case, we check whether  $c \in N_{K/\mathbf{Q}_v}(K^\times)$ , where  $K = \mathbf{Q}_v(\sqrt{b})$ . We invoke Theorem 9.10(ii), (9.2), (9.3), and the table below (9.3), which we will call table T.

Case (A):  $b = c = -1$ . Clearly  $(-1, -1)_v = -1$  for archimedean  $v$ . By Theorem 9.10(ii),  $-1 \in N_{K/\mathbf{Q}_p}(K^\times)$  for  $K = \mathbf{Q}_p(\sqrt{-1})$  if  $p$  is an odd prime number, and so  $(-1, -1)_p = 1$  for such a  $p$ . Also from table T we see that  $(-1, -1)_2 = -1$ , which settles this case.

Case (B):  $b = -1$  and  $c$  is a prime number. If  $c = 2$ , then  $x^2 - by^2 - cz^2 = x^2 + y^2 - 2z^2$ , which has  $(1, 1, 1)$  as a zero. Thus we assume that  $c \neq 2$ . By

Theorem 9.10(ii),  $(-1, c)_p = 1$  if  $p$  is an odd prime number and  $p \neq c$ . If  $c - 1 \in 4\mathbf{Z}$ , then  $c$  splits in  $\mathbf{Q}(\sqrt{-1})$ , and so  $(-1, c)_c = 1$ . If  $c + 1 \in 4\mathbf{Z}$ , then  $\mathbf{Q}_c(\sqrt{-1})$  is an unramified quadratic extension of  $\mathbf{Q}_c$ , and so  $(-1, c)_c = -1$  by Theorem 9.10(ii). From table T we see that  $(-1, c)_2 = -1$  if and only if  $c + 1 \in 4\mathbf{Z}$ . Thus we obtain the desired result.

Case (C):  $b$  is a prime number and  $b = c$ . In this case we have  $(b, b)_v = (-b, b)_v(-1, b)_v$ , and  $(-b, b)_v = 1$ , as  $(0, 1, 1)$  is a zero of  $x^2 + by^2 - bz^2$ . Thus  $\prod_v (b, b)_v = \prod_v (-1, b)_v$ , which is reduced to Case (B).

Case (D):  $b$  and  $c$  are prime numbers and  $b \neq c$ . Clearly  $(b, c)_v = 1$  for archimedean  $v$ . Suppose  $b = 2$ . Then  $c \neq 2$  and table T shows that  $(2, c)_2 = -1$  if and only if  $c \pm 3 \in 8\mathbf{Z}$ , in which case  $\left(\frac{2}{c}\right) = -1$  by (3.3), and so  $c$  remains prime in  $\mathbf{Q}(\sqrt{2})$ ; thus  $(2, c)_c = -1$ . By Theorem 9.10(ii),  $(2, c)_p = 1$  for an odd prime number  $p \neq c$ , and so our problem is settled when  $b = 2$ . Finally suppose both  $b$  and  $c$  are odd and  $b \neq c$ . By Theorem 9.10(ii),  $(b, c)_p = 1$  for an odd prime number  $p$  different from  $b$  and  $c$ . Taking  $b$  to be  $p$  of (9.2), we see that  $(b, c)_b = \left(\frac{c}{b}\right)$ . Similarly  $(b, c)_c = (c, b)_c = \left(\frac{b}{c}\right)$ . Thus

$$\prod_{v \in \mathbf{v}} (b, c)_v = (b, c)_2 (b, c)_b (b, c)_c = (b, c)_2 \left(\frac{c}{b}\right) \left(\frac{b}{c}\right).$$

The first three lines of table T determine  $N_{K/\mathbf{Q}_2}(K^\times)$  for  $K = \mathbf{Q}_2(\sqrt{b})$ . We then find that  $(b, c)_2 = -1$  if and only if  $b \equiv c \equiv 3 \pmod{4}$ . Combining this with the quadratic reciprocity law (3.5), we obtain the desired result. This completes the proof.

**26.5.** Given a local or global field  $F$  and  $b, c \in F^\times$ , we define a quaternion algebra  $\{b, c\}$  over  $F$  as follows:

$$(26.7) \quad \{b, c\} = \begin{cases} \{F(\sqrt{b}), c\} & \text{if } [F(\sqrt{b}) : F] = 2, \\ M_2(F) & \text{otherwise.} \end{cases}$$

For a quaternion algebra  $A$  over a global  $F$  and  $v \in \mathbf{v}$  we put  $A_v = A \otimes_v F_v$ . Then we define  $\varepsilon_v(A)$  by

$$(26.8) \quad \varepsilon_v(A) = \begin{cases} 1 & \text{if } A_v \cong M_2(F_v), \\ -1 & \text{otherwise.} \end{cases}$$

We say that  $A$  is **ramified** at  $v$  if  $\varepsilon_v(A) = -1$ ; otherwise we say that  $A$  is **unramified** at  $v$ . By Theorem 21.22,  $\varepsilon_v(A) = -1$  can happen exactly in the following two cases: (a)  $v$  is real archimedean and  $A_v \cong \mathbf{H}$ ; (b)  $v$  is nonarchimedean and  $A_v$  is the unique division quaternion algebra over  $F_v$  specified in Theorem 21.22. In all cases,  $\varepsilon_v(A)$  determines the isomorphism class of  $A_v$  over  $F_v$ . We also say that a prime ideal  $\mathfrak{p}$  in  $F$  is **ramified** in  $A$

if  $A$  is ramified at the prime  $v$  determined by  $\mathfrak{p}$ ; otherwise we say that  $\mathfrak{p}$  is unramified in  $A$ .

**Theorem 26.6.** (i) *If  $A$  is a quaternion algebra over a global field  $F$ , then  $\varepsilon_v(A) = 1$  for almost all  $v \in \mathbf{v}$ , and  $\prod_{v \in \mathbf{v}} \varepsilon_v(A) = 1$ .*

(ii) *For  $A$  as in (i),  $A \cong M_2(F)$  if  $\varepsilon_v(A) = 1$  for every  $v \in \mathbf{v}$ .*

PROOF. By Lemma 20.4 every quaternion algebra over  $F$  can be given as  $\{b, c\}$  with some  $b, c \in F^\times$ . We now note that

$$(26.9) \quad \varepsilon_v(\{b, c\}) = (b, c)_v.$$

Indeed, let  $A = \{b, c\}$ . If  $\varepsilon_v(A) = 1$ , then  $\sqrt{b} \in F_v$  or  $\{F_v(\sqrt{b}), c\} \cong M_2(F_v)$ , which means that  $c \in N_{K/F_v}(K^\times)$  with  $K = F_v(\sqrt{b})$ ; thus  $(b, c)_v = 1$ . Conversely, following our argument in the opposite direction, we find that  $\varepsilon_v(A) = 1$  if  $(b, c)_v = 1$ . This proves (26.9). Therefore (i) of our theorem follows from Theorems 26.2 and 26.4.

As for (ii), there is no problem if  $A \cong M_2(F)$ . Otherwise by Lemma 20.4 we can put  $A = \{K, c\}$  with a quadratic extension  $K$  of  $F$  and  $c \in F^\times$ . Then (ii) follows from Theorem 26.3 combined with Theorem 20.8(ii).

## 27. The Hasse principle

**27.1.** We now assume that  $F$  is a global field, that is, an algebraic number field of finite degree, and use the symbols  $\mathbf{a}$ ,  $\mathbf{h}$ , and  $\mathbf{v}$  as before. We consider a nondegenerate quadratic space  $(V, \varphi)$  over  $F$ ; we put  $n = \dim(V)$ . For each  $v \in \mathbf{v}$  we define a quadratic space  $(V, \varphi)_v = (V_v, \varphi_v)$  over  $F_v$  as in §25.7

Though we state the results for an arbitrary number field, our exposition is self-contained only when  $F = \mathbf{Q}$ , since we invoke Theorems 26.3 and 26.6, which we proved only for  $F = \mathbf{Q}$ . There is one more basic fact:

(27.1) *If an element of  $F$  is square in  $F_v$  for every  $v \in \mathbf{v}$ , then it is a square in  $F$ .*

This is clearly true if  $F = \mathbf{Q}$ . In general, let  $K = F(\sqrt{c})$  with an element  $c$  of  $F^\times$  that is not a square in  $F$ . Then there are infinitely many prime ideals in  $F$  that remain prime in  $K$ . This implies (27.1), and follows from an easy case of class field theory. Thus we employ (27.1) in addition to Theorems 26.3 and 26.4. Once we assume Theorem 26.4, then we obtain Theorem 26.6 as a consequence.

In the rest of this section we show that the structure of  $(V, \varphi)$  is completely determined by those of  $(V_v, \varphi_v)$  for all  $v \in \mathbf{v}$ . We begin with

**Theorem 27.2.** (i) *For  $(V, \varphi)$  as above,  $\varphi$  is isotropic if and only if  $\varphi_v$  is isotropic for every  $v \in \mathbf{v}$ .*

(ii) *If  $n \geq 3$ , then  $\varphi_v$  is anisotropic only for finitely many  $v \in \mathbf{v}$ .*

PROOF. (I) We naturally assume  $n > 1$ . Clearly it is sufficient to prove the “if”-part. Thus we assume that  $\varphi_v$  is isotropic for every  $v \in \mathbf{v}$ . Then our task is to show that  $\varphi$  is isotropic. Suppose  $n = 2$ ; then by Lemma 22.7,  $-\det(\varphi) \in F_v^{\times 2}$  for every  $v \in \mathbf{v}$ , and so  $-\det(\varphi) \in F^{\times 2}$  by (27.1). By Lemma 22.7,  $\varphi$  is isotropic as expected.

(II) Suppose  $n = 3$ ; take  $B$  as in Lemma 25.2(ii) for the present  $(V, \varphi)$ . By (25.3),  $B_v$  is not a division algebra for every  $v \in \mathbf{v}$ . By Theorem 26.6(ii),  $B \cong M_2(F)$ , and consequently  $\varphi$  is isotropic, which proves the desired fact.

(III) Clearly it is sufficient to prove (ii) when  $n = 3$ . Take  $B$  as above. Then by Theorem 26.6(i),  $B_v \cong M_2(F_v)$  for almost all  $v$ , and  $\varphi_v$  is isotropic for such a  $v$ .

(IV) Suppose  $n = 4$  and  $1 \in \delta_0(\varphi)$ . Then by Theorem 25.4(i), we can put  $(V, \varphi) = (B, d\beta)$  with a quaternion algebra  $B$  over  $F$  and  $d \in F^\times$ . For every  $v \in \mathbf{v}$ ,  $\varphi_v$  is isotropic, so that  $B_v \cong M_2(F_v)$ . By Theorem 26.6(ii),  $B \cong M_2(F)$ , and so  $\varphi$  is isotropic as desired.

(V) Suppose  $n = 4$  and  $1 \notin \delta_0(\varphi)$ ; let  $K$  be the discriminant field of  $\varphi$ . Then  $K = F(\delta)$  with  $\delta^2 \in \delta_0(\varphi)$ ; thus  $[K : F] = 2$ . Put  $Y = V \otimes_F K$  and denote by  $\psi$  the  $K$ -bilinear extension of  $\varphi$  to  $Y \times Y$ . From our assumption on  $\varphi_v$ , we see that the localizations of  $\psi$  are all isotropic. Since  $1 \in \delta_0(\psi)$ , we can apply the result of (IV) to  $\psi$  to find that  $\psi$  is isotropic. Thus  $Y$  has an isotropic element  $x + \delta y$  with  $x, y \in V$ . Then  $\varphi[x] + \delta^2 \varphi[y] + 2\delta\varphi(x, y) = 0$ , so that  $\varphi[x] = -\delta^2 \varphi[y]$  and  $\varphi(x, y) = 0$ . Suppose  $\varphi$  is anisotropic. If  $\varphi[x] = 0$ , then  $x = y = 0$ , a contradiction. Therefore  $\varphi[x] \neq 0$ , and so  $\dim(Fx + Fy) = 2$ . Put  $U = (Fx + Fy)^\perp$ . Then  $\delta^2 \varphi[y]^2 \delta_0(U, \varphi) = -\varphi[x]\varphi[y] \delta_0(U, \varphi) = \delta_0(V, \varphi)$ , which contains  $\delta^2$ , so that  $1 \in \delta_0(U, \varphi)$ . By Lemma 22.7,  $\varphi$  is isotropic on  $U$ , a contradiction. This settles the case  $n = 4$ .

(VI) Let us finally prove the case  $n \geq 5$  by induction on  $n$ . Assuming  $n \geq 5$ , take a decomposition  $V = X \oplus Y$ ,  $Y = X^\perp$ , with a 2-dimensional subspace  $X$  of  $V$  on which  $\varphi$  is nondegenerate. Let  $\mathbf{p}$  be the set of all  $v \in \mathbf{v}$  such that  $\varphi_v$  is anisotropic on  $Y_v$ . Since  $\dim(Y) \geq 3$ ,  $\mathbf{p}$  is a finite set by (ii). If  $\mathbf{p} = \emptyset$ , then by induction,  $\varphi$  is isotropic on  $Y$ ; so assume that  $\mathbf{p} \neq \emptyset$ . Since  $\varphi_v$  is isotropic on  $V_v$ , we can find, for each  $v \in \mathbf{p}$ , elements  $x \in X_v$  and  $y \in Y_v$  such that  $x + y \neq 0$  and  $\varphi[x] + \varphi[y] = 0$ . We may assume that  $\varphi[x] \neq 0$ . (This is clear if  $\varphi$  is anisotropic on  $X_v$ . Otherwise take any  $y \in Y_v, \neq 0$ , and take  $x \in X_v$  so that  $\varphi[x] = -\varphi[y]$ .) Put  $a_v = \varphi[x]$  for any choice of such an  $x$ . Now  $F_v^{\times 2}$  is open in  $F_v^\times$  for every  $v \in \mathbf{h}$  by Lemma 21.12(ii), and also for every  $v \in \mathbf{a}$ , as can easily be seen. By Lemma 15.3(ii),  $X$  is dense in  $\prod_{v \in \mathbf{p}} X_v$ , and so we can find  $z \in X$  such that  $\varphi[z] \in a_v F_v^{\times 2}$  for every  $v \in \mathbf{p}$ . Then  $-\varphi[z] \in \varphi[F_v^\times y]$ , so that  $\varphi_v$  is isotropic on  $F_v z + Y_v$  for every  $v \in \mathbf{p}$ , and for every  $v \notin \mathbf{p}$  as well, as  $\varphi_v$  is isotropic on  $Y_v$  for  $v \notin \mathbf{p}$ . Applying our induction to  $Fz + Y$ , we find that  $\varphi$  is isotropic on  $Fz + Y$ . This

completes the proof.

**Remark.** As we said at the beginning, once we assume (27.1) and Theorems 26.3 and 26.6, then we obtain Theorem 27.2 and all the results stated in this section. Though we established (27.1) and Theorems 26.3 and 26.6 for  $F = \mathbf{Q}$ , that is not enough for the proof of Theorem 27.2 when  $F = \mathbf{Q}$ , because we considered in (V) above a quadratic extension  $K$  of  $F$ . However, we can give a proof without such an extension when  $F = \mathbf{Q}$ . The fact that requires a proof is: *Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $\mathbf{Q}$  of dimension 4 such that  $(V, \varphi)_v$  is isotropic for every  $v \in \mathbf{v}$ . Then  $(V, \varphi)$  itself is isotropic.* The proof of this fact will be given at the end of Section 29. Once this is done, this book becomes self-contained when the base field is  $\mathbf{Q}$ , at least up to Section 32.

**Theorem 27.3.** *Let  $(V, \varphi)$  and  $(W, \psi)$  be nondegenerate quadratic spaces over a global field  $F$ . Then the following assertions hold:*

(i) *There exists an  $F$ -linear injection  $\alpha$  of  $W$  into  $V$  such that  $\varphi[x\alpha] = \psi[x]$  for every  $x \in W$  if and only if there exists, for every  $v \in \mathbf{v}$ , an  $F_v$ -linear injection  $\beta_v$  of  $W_v$  into  $V_v$  such that  $\varphi_v[y\beta_v] = \psi_v[y]$  for every  $y \in W_v$ .*

(ii) *Given  $c \in F$ , there exists an element  $z \in V$  such that  $\varphi[z] = c$  if and only if  $c = \varphi[w]$  with some  $w \in V_v$  for every  $v \in \mathbf{v}$ .*

PROOF. Clearly it is sufficient to prove the “if”-part of each assertion. Suppose  $\dim(W) = 1$ ; take a nonzero element  $e$  of  $W$ . If there exists an  $F$ -linear injection  $\alpha$  of  $W$  into  $V$  such that  $\varphi[e\alpha] = \psi[e]$ , then  $(W, -\psi) \oplus (V, \varphi)$  is isotropic and vice versa; the same is true with  $(V_v, W_v, F_v)$  in place of  $(V, W, F)$ . (If  $\varphi$  is isotropic, then  $V$  has elements  $g, f$  such that  $g^2 = f^2 = 0$  and  $gf + fg = 1$ , and so  $\varphi[cg + f] = c$  for every  $c \in F$ . Thus  $(W, \psi)$  can be embedded in  $(V, \varphi)$ .) Therefore our assertion follows from Theorem 27.2.

To prove (ii), we may assume that  $c \neq 0$ . Define  $(W, \psi)$  of dimension 1 by  $W = Fx$  and  $\psi[x] = c$ . If  $\varphi_v[w] = c$  with  $w \in V_v$ , then we define  $\beta_v : W_v \rightarrow V_v$  by  $x\beta_v = w$ . Clearly  $\varphi_v[y\beta_v] = \psi_v[y]$  for every  $y \in W_v$ . Thus we obtain (ii) from (i) with  $\dim(W) = 1$ .

We prove the general case of (i) by induction on  $\dim(W)$ . We assume the existence of  $\beta_v$  as in our theorem for every  $v \in \mathbf{v}$ . Take  $w \in W$  such that  $\psi[w] \neq 0$ . Then  $\psi[w] = \varphi[w\beta_v] \in \varphi[V_v]$  for every  $v \in \mathbf{v}$ , and so there exists an element  $z \in V$  such that  $\varphi[z] = \psi[w]$ , by virtue of (ii). Let  $X = \{x \in V \mid \varphi(z, x) = 0\}$  and  $Y = \{y \in W \mid \psi(w, y) = 0\}$ . Then  $V = Fz \oplus X$  and  $W = Fw \oplus Y$ , so that  $W_v\beta_v = F_vw\beta_v \oplus Y_v\beta_v$ . Since  $\varphi[w\beta_v] = \psi[w] = \varphi[z]$ , Witt’s theorem says that  $(X, \varphi)_v$  is isomorphic to the orthogonal complement of  $F_vw\beta_v$  in  $V_v$ , which contains  $Y_v\beta_v$ . This means that for each  $v \in \mathbf{v}$  there exists an  $F_v$ -linear injection  $\gamma_v$  of  $Y_v$  into  $X_v$  such that  $\varphi[w\gamma_v] = \psi[u]$  for every  $u \in Y_v$ . By induction, there exists an  $F$ -linear

injection  $\delta$  of  $Y$  into  $X$  such that  $\varphi[y\delta] = \psi[y]$  for every  $y \in Y$ . Extending  $\delta$  to  $W$  by  $w\delta = z$ , we can complete the proof.

**Corollary 27.4.** *Let  $(V, \varphi)$  and  $(W, \psi)$  be defined over a global field  $F$  with nondegenerate  $\varphi$  and  $\psi$ . Then  $(V, \varphi)$  and  $(W, \psi)$  are isomorphic if and only if  $(V, \varphi)_v$  and  $(W, \psi)_v$  are isomorphic for every  $v \in \mathbf{v}$ .*

This is merely a special case of Theorem 27.3(i) in which  $\dim(V) = \dim(W)$ .

The above theorem and corollary are due to Minkowski when  $F = \mathbf{Q}$ , and Hasse in the general case. For simplicity we call either of them the **Hasse principle**.

**Corollary 27.5.** *Let  $(V, \varphi)$  be defined over a global field  $F$ ; suppose  $n \geq 4$ ; let  $\mathbf{c}_+$  resp.  $\mathbf{c}_-$  be the set of all real archimedean primes  $v$  such that  $\varphi_v$  is positive resp. negative definite. Then, for  $a \in F^\times$  there exists an element  $x$  of  $V$  such that  $\varphi[x] = a$  if and only if  $a$  is positive at every  $v \in \mathbf{c}_+$  (if  $\mathbf{c}_+ \neq \emptyset$ ) and negative at every  $v \in \mathbf{c}_-$  (if  $\mathbf{c}_- \neq \emptyset$ ).*

PROOF. The “only if”-part is clear. The “if”-part follows from Theorem 27.3(ii), Theorem 25.5(i), and an obvious fact about the values of  $\varphi$  at archimedean primes.

**Lemma 27.6.** *Let  $B$  be a quaternion algebra over an algebraic number field  $F$ , and  $K$  a quadratic extension of  $F$ . If there is an  $F_v$ -linear ring-injection of  $K_v$  into  $B_v$  for every  $v \in \mathbf{v}$ , then there is an  $F$ -linear ring-injection of  $K$  into  $B$ .*

PROOF. Define  $(B^\circ, \beta^\circ)$  as in §25.1. We have  $K = F(\alpha)$ ,  $\alpha^2 = b \in F^\times$ , with a suitable  $b$ . Let  $f_v$  be an  $F_v$ -linear ring-injection of  $K_v$  into  $B_v$ . Put  $\xi_v = f_v(\alpha)$ . Then  $\xi_v^2 = b \in F^\times$  and  $\xi_v \notin F_v$ , as  $\alpha \notin F$ . Therefore  $\xi_v \in B_v^\circ$  by Lemma 20.7, and  $\beta^\circ[\xi_v] = -b$ . By Theorem 27.3(ii) we then have an element  $\xi \in B^\circ$  such that  $\beta^\circ[\xi] = -b$ . Define an  $F$ -linear map  $f$  of  $K$  into  $B$  by  $f(\alpha) = \xi$ . Since  $\xi^2 = -\xi\xi^\iota = b$ , we easily see that  $f$  is a ring-injection. This proves our lemma.

**Theorem 27.7.** *Two quaternion algebras  $A$  and  $B$  over a global field  $F$  are isomorphic over  $F$  if and only if  $\varepsilon_v(A) = \varepsilon_v(B)$  for every  $v \in \mathbf{v}$ .*

PROOF. Suppose  $\varepsilon_v(A) = \varepsilon_v(B)$  for every  $v \in \mathbf{v}$ . Then  $A_v \cong B_v$  for every  $v \in \mathbf{v}$ . Now  $A \cong \{K, \gamma\}$  with a quadratic extension  $K$  of  $F$  and  $\gamma \in F^\times$ . This was shown in Lemma 20.4 for a division quaternion algebra. Also, by (20.6),  $M_2(F) \cong \{K, 1\}$  with any quadratic extension  $K$  of  $F$ . Take  $K$  so that  $A \cong \{K, \gamma\}$ . Since  $A_v \cong B_v$  for every  $v \in \mathbf{v}$ , there is an  $F_v$ -linear ring-injection of  $K_v$  into  $B_v$ . By Lemma 27.6 there is an  $F$ -linear ring-injection of

$K$  into  $B$ . Then we can put  $B = \{K, \delta\}$  with  $\delta \in F^\times$ . Since  $A_v \cong B_v$ , we have  $\gamma/\delta \in N_{K_v/F_v}(K_v^\times)$  by Theorem 20.8(i) for every  $v \in \mathbf{v}$ . By Theorem 26.3(ii),  $\gamma/\delta \in N_{K/F}(K^\times)$ , and so  $A \cong B$  by Theorem 20.8(i). This proves our theorem.

**Theorem 27.8.** *Let  $\{\delta_v\}_{v \in \mathbf{v}}$  be a set of numbers indexed by  $v \in \mathbf{v}$  with the following properties: (1)  $\delta_v = \pm 1$ ; (2)  $\delta_v = 1$  for almost all  $v$ ; (3)  $\delta_v = 1$  for every imaginary archimedean  $v$ ; (4)  $\prod_{v \in \mathbf{v}} \delta_v = 1$ , that is, the number of  $v$ 's for which  $\delta_v = -1$  is even. Then there exists a quaternion algebra  $A$  over  $F$  such that  $\varepsilon_v(A) = \delta_v$  for every  $v \in \mathbf{v}$ .*

PROOF. We prove this only when  $F = \mathbf{Q}$ . Let  $P$  be the set of prime numbers  $p$  such that  $\delta_p = -1$ . If  $P = \emptyset$ , then condition (4) shows that  $\delta_\infty = 1$ . Then we can take  $A = M_2(\mathbf{Q})$ . Suppose  $P \neq \emptyset$ . For each odd  $p \in P$  take  $a_p \in \mathbf{Z}$  so that  $\left(\frac{a_p}{p}\right) = -1$ . Then we can find a positive integer  $c$  such that  $\delta_\infty c - a_p \in p\mathbf{Z}$  for every odd  $p \in P$ . We can even take  $c$  so that  $\delta_\infty c - 1 \in 8\mathbf{Z}$  if  $2 \notin P$  and  $\delta_\infty c - 5 \in 8\mathbf{Z}$  if  $2 \in P$ . Now by Dirichlet's theorem on prime numbers in an arithmetic progression, we can take such a  $c$  to be a prime number. Put  $K = \mathbf{Q}(\sqrt{\delta_\infty c})$ . Then every  $p \in P$  remains prime in  $K$ ; see (10.13) and (10.14). Let  $m$  be the product of all  $p$  in  $P$ . Then we take  $A = \{K, m\}$  if  $\delta_\infty = 1$  and  $A = \{K, -m\}$  if  $\delta_\infty = -1$ . Clearly  $\varepsilon_\infty(A) = \delta_\infty$ . If  $p \in P$ , then  $A_p$  is of the type  $\{J, \pi\}$  of Theorem 21.22, and so  $\varepsilon_p(A) = -1 = \delta_p$ . Let  $p$  be a prime number for which  $\delta_p = 1$  and  $p \neq c$ . Then  $p$  is unramified in  $K$  and  $p$  does not divide  $m$ , and so  $\varepsilon_p(A) = 1$ . Thus  $\varepsilon_v(A) = \delta_v$  for every  $v \neq c$ . From Theorem 26.6(i) and our condition (4) we see that  $\varepsilon_c(A) = 1$ . This proves our theorem.

**27.9.** Let us illustrate the above theorem more explicitly when  $F = \mathbf{Q}$ . Let  $B$  be a division quaternion algebra over  $\mathbf{Q}$ . We call  $B$  **definite** or **indefinite** according as its norm form is definite or indefinite as a real quadratic form. Thus  $B$  is definite if  $B \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{H}$  and indefinite if  $B \otimes_{\mathbf{Q}} \mathbf{R} \cong M_2(\mathbf{R})$ . The product of all prime numbers  $p$  such that  $\varepsilon_p(B) = -1$  is called the **discriminant** of  $B$  and written  $D_B$ . The number of such  $p$ 's is even or odd according as  $B$  is indefinite or definite. Using the notation introduced in Theorem 21.27, we have  $d(B/\mathbf{Q}) = D_B\mathbf{Z}$  and  $[\bar{\mathfrak{o}} : \mathfrak{o}] = D_B^2$  for every maximal order  $\mathfrak{o}$  in  $B$ . Let  $B = \{K, \gamma\}$  with a quadratic field  $K$  and  $\gamma \in \mathbf{Q}^\times$ . Then a prime number  $p$  divides  $D_B$  only if  $K_p = K \otimes_{\mathbf{Q}} \mathbf{Q}_p$  is a field and  $\gamma \notin N_{K_p/\mathbf{Q}_p}(K_p^\times)$ . If  $\gamma \in \mathbf{Z}_p^\times$ , then such happens only when  $p$  is ramified in  $K$ ; see Theorem 9.10(ii).

Take for instance  $B = \{\mathbf{Q}(\sqrt{-1}), -1\}$ . Then  $B \otimes_{\mathbf{Q}} \mathbf{R} = \mathbf{H}$ . The only prime number ramified in  $\mathbf{Q}(\sqrt{-1})$  is 2, and so  $D_B = 2$ . Let  $\mathfrak{o}_0 = \mathbf{Z} + \mathbf{Z}\mathbf{i} + \mathbf{Z}\mathbf{j} + \mathbf{Z}\mathbf{k}$  with the standard quaternion units  $\mathbf{i}, \mathbf{j}, \mathbf{k}$  as in (20.7). We can easily verify



that  $\tilde{\mathfrak{o}}_0 = 2^{-1}\mathfrak{o}_0$ , and so  $[\tilde{\mathfrak{o}}_0 : \mathfrak{o}_0] = 2^4$ . Thus  $\mathfrak{o}$  is not maximal. Put  $\mathfrak{o} = \mathbf{Z}\mathbf{f} + \mathfrak{o}_0$  with  $\mathbf{f} = 2^{-1}(1 + \mathbf{i} + \mathbf{j} + \mathbf{k})$ . We easily see that  $\mathfrak{o}$  is an order in  $B$ . Since  $[\mathfrak{o} : \mathfrak{o}_0] = 2$ , we have  $[\tilde{\mathfrak{o}}_0 : \tilde{\mathfrak{o}}] = 2$ , and so  $[\tilde{\mathfrak{o}} : \mathfrak{o}] = 4 = D_B^2$ . Therefore, by Theorem 21.27,  $\mathfrak{o}$  is a maximal order.

**Lemma 27.10.** *Given a finite subset  $\mathbf{x}$  of  $\mathbf{v}$  that contains no imaginary archimedean prime of  $F$ , we can find a quadratic extension of  $F$  in which every prime of  $\mathbf{x}$  is ramified.*

PROOF. We may assume that  $\mathbf{x}$  contains at least one nonarchimedean prime. Let  $\mathfrak{a}$  be the product of the prime ideals in  $F$  corresponding to the nonarchimedean members of  $\mathbf{x}$ . By Lemma 10.5(i) there exists an integral ideal  $\mathfrak{b}$  prime to  $\mathfrak{a}$  such that  $\mathfrak{a}\mathfrak{b} = \gamma\mathfrak{g}$  with  $\gamma \in F$ . Let  $M$  be a positive integer divisible by  $\mathfrak{a}\mathfrak{b}$  and let  $\mathbf{y}$  be the set of all real archimedean primes of  $\mathbf{x}$ . Then we can find an element  $\varepsilon$  such that  $\varepsilon - 1 \in M\mathfrak{g}$  and  $\varepsilon\gamma < 0$  in  $F_v$  for every  $v \in \mathbf{y}$ . Then  $K = F(\sqrt{\varepsilon\gamma})$  has the desired property.

**Theorem 27.11.** *Let  $A$  and  $B$  be quaternion algebras over an algebraic number field  $F$ . Then  $A \otimes B \cong M_2(C)$  with a quaternion algebra  $C$  over  $F$  such that  $\varepsilon_v(C) = \varepsilon_v(A)\varepsilon_v(B)$  for every  $v \in \mathbf{v}$ .*

PROOF. Let  $\mathbf{x}$  be the set of primes  $v \in \mathbf{v}$  such that  $\varepsilon_v(A) = -1$  or  $\varepsilon_v(B) = -1$ . By Lemma 27.10 there exists a quadratic extension  $K$  of  $F$  in which every  $v \in \mathbf{x}$  is ramified. By Theorem 21.23 both  $A_v$  and  $B_v$  contain isomorphic images of  $K_v$  for every  $v \in \mathbf{x} \cap \mathbf{h}$ . This is also true for  $v \in \mathbf{x} \cap \mathbf{a}$ , since  $K_v \cong \mathbf{C}$  for such a  $v$ , and  $\mathbf{C}$  has an isomorphic image in  $\mathbf{H}$  and  $M_2(\mathbf{R})$ . If  $v \notin \mathbf{x}$ , then  $A_v \cong B_v \cong M_2(F_v)$ , which contains an isomorphic image of  $K_v$ . Therefore, by Lemma 27.6,  $K$  can be  $F$ -linearly embedded in  $A$  and  $B$ . Thus, by Lemma 20.4 we have  $A \cong \{K, \alpha\}$  and  $B \cong \{K, \beta\}$  with  $\alpha, \beta \in F^\times$ . Then our theorem follows from Theorem 20.8(iii), since  $\varepsilon_v(\{K, \alpha\beta\})$  is determined by the coset  $\alpha\beta N_{K_v/F_v}(K_v^\times)$ .

**Theorem 27.12.** *Let  $F$  be either an algebraic number field or its completion at a prime  $v \in \mathbf{v}$ , and  $(V, \varphi)$  a nondegenerate quadratic space over  $F$  of dimension  $n$ . If  $0 < n \in 2\mathbf{Z}$ , then  $A(\varphi) \cong M_s(B)$  with a quaternion algebra  $B$  over  $F$ , where  $s = 2^{(n-2)/2}$ . If  $0 < n - 1 \in 2\mathbf{Z}$ , then  $A^+(\varphi) \cong M_t(B)$  with a quaternion algebra  $B$  over  $F$ , where  $t = 2^{(n-3)/2}$ . In either case the isomorphism class of  $B$  over  $F$  is determined by  $(V, \varphi)$ .*

PROOF. For  $n \leq 3$  our assertions follow from Lemma 25.2. We prove the general case when  $F$  is a number field by induction on  $n$ . Take any nondegenerate quadratic space  $(V', \varphi')$  over  $F$  of dimension 2. Suppose  $0 < n \in 2\mathbf{Z}$  and  $A(\varphi) \cong M_s(B)$  as stated above. Then by Lemma 23.10(ii),  $A(\varphi \oplus \varphi') \cong A(\varphi) \otimes_F A(\delta\varphi')$  with  $\delta \in \delta_0(\varphi)$ . By Lemma 25.2(i),  $A(\delta\varphi')$  is a quaternion

algebra over  $F$ , and so by Theorem 27.11,  $B \otimes A(\delta\varphi') \cong M_2(D)$  with a quaternion algebra  $D$  over  $F$ , and so  $A(\varphi \oplus \varphi') \cong M_{2s}(D)$ , which proves the case of dimension  $n + 2$ . The case of odd  $n$  can be proved similarly; also the case where  $F$  is a completion at a prime can be handled in a similar way by means of Theorem 20.8(iii). The last assertion follows from Theorem 18.12.

We add here some classical facts on the quaternion algebra of §27.9.

**Theorem 27.13.** *Let  $B = \{\mathbf{Q}(\sqrt{-1}), -1\}$ ,  $\mathfrak{o}_0 = \mathbf{Z} + \mathbf{Z}\mathbf{i} + \mathbf{Z}\mathbf{j} + \mathbf{Z}\mathbf{k}$ , and  $\mathfrak{o} = \mathfrak{o}_0 + \mathbf{Z}\mathbf{f}$  as in §27.9. Then the following assertions hold:*

(i) *Every right or left  $\mathfrak{o}$ -ideal is principal in the sense that it is of the form  $\alpha\mathfrak{o}$  or  $\mathfrak{o}\alpha$  with  $\alpha \in B^\times$ .*

(ii) *Every maximal order in  $B$  is of the form  $\alpha\mathfrak{o}\alpha^{-1}$  with  $\alpha \in B^\times$ .*

PROOF. To prove (i), take any right  $\mathfrak{o}$ -ideal  $\mathfrak{a}$ . Replacing it by its suitable integer multiple, we may assume that  $\mathfrak{a} \subset \mathfrak{o}$ . Let  $\alpha$  be an element of  $\mathfrak{a}$  with the smallest nonzero value of  $|\alpha|$ , where  $|\alpha| = (\alpha\alpha^\iota)^{1/2}$ . Let  $\xi \in \mathfrak{a}$  and  $\alpha^{-1}\xi = p + q\mathbf{i} + r\mathbf{j} + s\mathbf{k}$  with  $p, q, r, s \in \mathbf{Q}$ . Taking integers closest to  $p, q, r, s$ , we can find an element  $\beta$  of  $\mathfrak{o}_0$  such that  $|\alpha^{-1}\xi - \beta| \leq 1$ . Put  $\gamma = \alpha^{-1}\xi - \beta$ . Then  $\alpha\gamma = \xi - \alpha\beta \in \mathfrak{a}$ . If  $|\gamma| < 1$ , then  $|\alpha\gamma| < |\alpha|$ , and so  $\alpha\gamma = 0$  because of our choice of  $\alpha$ . Then  $\xi = \alpha\beta \in \alpha\mathfrak{o}$ . Suppose  $|\gamma| = 1$ . This can happen only when  $\gamma = \varepsilon_0 + \varepsilon_1\mathbf{i} + \varepsilon_2\mathbf{j} + \varepsilon_3\mathbf{k}$  with  $\varepsilon_j = \pm 1/2$ . Changing  $\beta$  suitably, we may assume that  $\alpha^{-1}\xi - \beta = \mathbf{f}$ . Then  $\xi = \alpha(\beta + \mathbf{f}) \in \alpha\mathfrak{o}$ . This proves that  $\alpha = \alpha\mathfrak{o}$ . The case of a left  $\mathfrak{o}$ -ideal can be handled in a similar way. This proves (i).

Next, let  $\mathfrak{o}'$  be a maximal order in  $B$ . Put  $\mathfrak{a} = \mathfrak{o}'\mathfrak{o}$ . Clearly  $\mathfrak{a}$  is a right  $\mathfrak{o}$ -ideal, and so  $\mathfrak{a} = \alpha\mathfrak{o}$  with some  $\alpha \in B^\times$  by (i). Then

$$\mathfrak{o}' \subset \{\xi \in B \mid \xi\mathfrak{a} \subset \mathfrak{a}\} \subset \{\xi \in B \mid \xi\alpha\mathfrak{o}\alpha^{-1} \subset \alpha\mathfrak{o}\alpha^{-1}\} = \alpha\mathfrak{o}\alpha^{-1}.$$

Since  $\mathfrak{o}'$  is maximal and  $\alpha\mathfrak{o}\alpha^{-1}$  is an order, we obtain  $\mathfrak{o}' = \alpha\mathfrak{o}\alpha^{-1}$ . This proves (ii).

**Theorem 27.14.** (i) *Every natural number is the sum of four squares.*

(ii) *A positive integer  $q$  is the sum of three squares if and only if  $q = r^2s$  with  $r \in \mathbf{Z}$  and a square-free positive integer  $s$  such that  $s + 1 \notin 8\mathbf{Z}$ , which is so if and only if the prime 2 does not split in  $\mathbf{Q}(\sqrt{-q})$ .*

Here a *square* means the square of an integer including zero.

PROOF. Let the notation be as in Theorem 27.13. Since  $N_{B/\mathbf{Q}}$  restricted to  $\mathfrak{o}_0$  is the sum of four squares and  $N_{B/\mathbf{Q}} : B^\times \cap \mathfrak{o}_0 \rightarrow \mathbf{Q}^\times$  is a multiplicative map, to prove (i), it is sufficient to show that every prime number  $p$  is of the form  $p = \alpha\alpha^\iota$  for some  $\alpha \in \mathfrak{o}_0$ . This is so for  $p = 2$ , as  $2 = (1 + \mathbf{i})(1 + \mathbf{i})^\iota$ . Thus we have only to consider an odd prime number  $p$ . Since  $p$  is unramified in  $B$ , there is an isomorphism of  $B_p$  onto  $M_2(\mathbf{Q}_p)$  that maps  $\mathfrak{o}_p$  onto  $M_2(\mathbf{Z}_p)$ , as

observed in the proof of Theorem 21.27. Thus we can find an element  $\alpha_p$  of  $\mathfrak{o}_p$  such that  $\alpha_p \alpha'_p = p$ . By Lemma 21.6, there exists a  $\mathbf{Z}$ -lattice  $\mathfrak{a}$  in  $B$  such that  $\mathfrak{a}_p = \alpha_p \mathfrak{o}_p$  and  $\mathfrak{a}_q = \mathfrak{o}_q$  for every prime number  $q \neq p$ . Then  $\mathfrak{a}$  is a right  $\mathfrak{o}$  ideal, and so by Theorem 27.13(i),  $\mathfrak{a} = \alpha \mathfrak{o}$  with  $\alpha \in B^\times$ . By Lemma 21.26,  $\alpha \alpha' = [\mathfrak{o} : \mathfrak{a}]^{1/2} = p$ . Since  $\mathfrak{o} = \mathfrak{o}_0 + \mathbf{Z}\mathbf{f}$ , we can put  $\alpha = \delta + c\mathbf{f}$  with  $\delta \in \mathfrak{o}_0$  and  $c \in \mathbf{Z}$ . If  $c$  is even, then  $\alpha \in \mathfrak{o}_0$ , and the matter is settled. Suppose  $c$  is odd. Then we have  $2\alpha = m_0 + m_1\mathbf{i} + m_2\mathbf{j} + m_3\mathbf{k}$  with odd integers  $m_i$ . We can put  $m_i = 4b_i + \varepsilon_i$  with  $b_i \in \mathbf{Z}$  and  $\varepsilon_i = \pm 1$ . Put  $\beta = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$  and  $\gamma = (1/2)(\varepsilon_0 + \varepsilon_1\mathbf{i} + \varepsilon_2\mathbf{j} + \varepsilon_3\mathbf{k})$ . Then  $\alpha = 2\beta + \gamma$ , and so  $\alpha\gamma' = 2\beta\gamma' + \gamma\gamma'$ . Since  $\gamma\gamma' = 1$  and  $2\beta\gamma' \in \mathfrak{o}_0$ , we have  $\alpha\gamma' \in \mathfrak{o}_0$  and  $N_{B/\mathbf{Q}}(\alpha\gamma') = p$ . Thus  $p$  is the sum of four squares. This proves (i).

As for (ii), we consider  $(B^\circ, \beta^\circ)$ . We observe that  $\mathfrak{o} \cap B^\circ = \mathfrak{o}_0 \cap B^\circ = \mathbf{Z}\mathbf{i} + \mathbf{Z}\mathbf{j} + \mathbf{Z}\mathbf{k}$ , and  $\beta^\circ$  restricted to  $\mathfrak{o}_0 \cap B^\circ$  is the sum of three squares. Thus our question is whether a given positive integer  $q$  belongs to  $\beta^\circ[\mathfrak{o}_0 \cap B^\circ]$ . Put  $K = \mathbf{Q}(\sqrt{-q})$ . Suppose  $q = \gamma\gamma'$  with  $\gamma \in B^\circ$ ; then  $q = -\gamma^2$ , and so  $\mathbf{Q}[\gamma]$  is isomorphic to  $K$ . Conversely, suppose  $K$  has an isomorphic image in  $B$ . Then  $B$  contains an element  $\xi$  such that  $\xi^2 = -q$ . By Lemma 20.7,  $\xi \in B^\circ$ . We can find an order in  $B$  containing  $\mathbf{Z}[\xi]$ , a fact whose proof we leave to the reader as an easy exercise. Thus, by Lemma 21.7(i),  $\mathbf{Z}[\xi]$  is contained in a maximal order, which, by Theorem 27.13, is of the form  $\alpha\mathfrak{o}\alpha^{-1}$  with  $\alpha \in B^\times$ . Put  $\eta = \alpha^{-1}\xi\alpha$ . Then  $\eta \in \mathfrak{o} \cap B^\circ = \mathbf{Z}\mathbf{i} + \mathbf{Z}\mathbf{j} + \mathbf{Z}\mathbf{k}$  and  $q = \eta\eta'$ . Thus  $q$  is the sum of three squares if and only if  $K$  has an isomorphic image in  $B$ , which, by Lemma 27.6, is so if and only if  $K_p$  can be embedded in  $B_p$  for every prime number  $p$ . (Notice that  $K \otimes_{\mathbf{Q}} \mathbf{R} = \mathbf{C}$ , which is embedded in  $B \otimes_{\mathbf{Q}} \mathbf{R} = \mathbf{H}$ .) If  $p \neq 2$ , then  $B_p = M_2(\mathbf{Q}_p)$ , and this imposes no condition on  $q$ . If  $p = 2$ , however,  $B_2$  is a division algebra, and  $K_2$  must be a field. If  $K_2$  is a field, it has an isomorphic image in  $B_2$  by Theorem 21.23(ii). Thus the condition on  $q$  is that 2 does not split in  $K = \mathbf{Q}(\sqrt{-q})$ . Let  $q = r^2s$  with  $r \in \mathbf{Z}$  and a square-free positive integer  $s$ . Then 2 splits in  $K$  if and only if  $s+1 \in 8\mathbf{Z}$  by (10.14), since there is  $-s$ . Thus the condition for  $q$  is that  $s+1 \notin 8\mathbf{Z}$ . This proves (ii) and completes the proof.

**Corollary 27.15.** *Every positive integer is the sum of three triangular numbers.* (Here a **triangular number** means an integer of the form  $m(m+1)/2$  with  $0 \leq m \in \mathbf{Z}$ .)

PROOF. Given  $n \in \mathbf{Z}$ ,  $> 0$ , put  $8n+3 = r^2s$  with  $r \in \mathbf{Z}$  and a square-free positive integer  $s$ . Then  $r$  is odd, and so  $s-3 \in 8\mathbf{Z}$ . By Theorem 27.14(ii) we can put  $8n+3 = \sum_{i=1}^3 k_i^2$  with  $0 \leq k_i \in \mathbf{Z}$ . Then  $k_i$  is odd for every  $i$ . Indeed, suppose  $k_3 \in 2\mathbf{Z}$ . Then  $k_1^2 + k_2^2 - 3 \in 4\mathbf{Z}$ , which is impossible. Thus  $k_i = 2m_i + 1$  with  $m_i \in \mathbf{Z}$  for  $1 \leq i \leq 3$ . Then  $n = \sum_{i=1}^3 m_i(m_i+1)/2$ , which gives the desired result.

We note that Theorem 27.14(i) is due to Lagrange; Theorem 27.14(ii) and Corollary 27.15 were proved by Gauss. We will discuss more about the sums of three squares in §34.3 and Theorem 37.5.

We mention here a result due to the author [S04a, Theorem 5.4] with the hope that future researchers will find an elementary proof. The original proof requires a rather involved analysis.

**Theorem 27.16.** *Every positive integer is the sum of three integers each of which is of the form  $(3m^2 - m)/2$  with  $m \in \mathbf{Z}$ .*

Traditionally a number of the form  $(3m^2 - m)/2$  with  $0 < m \in \mathbf{Z}$  is called a **pentagonal number**, but the case  $m \leq 0$  is included in the above theorem.



## DEEPER ARITHMETIC OF QUADRATIC FORMS

### 28. Classification of quadratic spaces over local and global fields

**28.1.** Let  $F$  be either an algebraic number field or its completion at a prime  $v \in \mathbf{v}$ , and  $(V, \varphi)$  a nondegenerate quadratic space over  $F$  of dimension  $n$ . We then define **the characteristic (quaternion) algebra** of  $(V, \varphi)$  as follows. This is a quaternion algebra  $Q(\varphi)$  over  $F$  such that

$$(28.1a) \quad A(\varphi) \cong M_s(Q(\varphi)) \quad \text{if } 0 < n \in 2\mathbf{Z},$$

$$(28.1b) \quad A^+(\varphi) \cong M_s(Q(\varphi)) \quad \text{if } 1 < n \notin 2\mathbf{Z},$$

with  $0 < s \in \mathbf{Z}$ . The existence and uniqueness of such a  $Q(\varphi)$  were proved in Theorem 27.12. We put  $Q(\varphi) = M_2(F)$  if  $n = 1$ . In view of Theorem 23.6,  $Q(\varphi)$  depends only on the isomorphism class of core subspaces of  $(V, \varphi)$ .

If we start from  $(V, \varphi)$  over a global field and define  $(V, \varphi)_v = (V_v, \varphi_v)$  for each  $v \in \mathbf{v}$  as in §§25.7 and 27.1, then clearly  $A(\varphi_v) = A(\varphi)_v$  and  $A^+(\varphi_v) = A^+(\varphi)_v$ , and so  $Q(\varphi_v) = Q(\varphi)_v$ , where we put  $R_v = R \otimes_F F_v$  for any  $F$ -algebra  $R$ . Also, if  $K$  is the discriminant algebra of  $(V, \varphi)$ , then  $K_v$  is the discriminant algebra of  $(V, \varphi)_v$ .

To simplify our notation, given a field  $F$  and a symmetric element  $\Phi \in GL_n(F)$ , we denote by  $\langle F, \Phi \rangle$  the quadratic space  $(F_n^1, \varphi)$  with  $\varphi$  defined by  $\varphi[x] = x\Phi \cdot {}^t x$  for  $x \in F_n^1$ . We then put  $Q(\Phi) = Q(\varphi)$ .

**28.2.** Let us now determine the discriminant algebra and characteristic algebra when  $F$  is a local field in the sense of §21.1, that is, the completion of an algebraic number field at a nonarchimedean prime. Given  $(V, \varphi)$  over such an  $F$ , denote by  $t$  its core dimension, and by  $K_0$  resp.  $K$  its discriminant field resp. algebra. By Theorem 25.5(ii) we have  $t \leq 4$ . Also, by Theorem 21.22, there is only one isomorphism class of division quaternion algebras over a fixed  $F$ . Thus  $Q(\varphi)$  is either this unique division quaternion algebra, or  $M_2(F)$ .

We have  $n = 2r + t$  with  $0 \leq r \in \mathbf{Z}$  and  $(V, \varphi) = \langle F, 2^{-1}\eta_r \rangle \oplus (Z, \zeta)$  with  $\eta_r$  as in (22.6) and a core subspace  $Z$  of dimension  $t$ . Then  $K$  is the discriminant algebra of  $(Z, \zeta)$ , and  $Q(\varphi) = Q(\zeta)$ .

Let us now determine  $Q(\varphi)$  for a given  $(V, \varphi)$  of dimension  $n \leq 4$ , without assuming that  $\varphi$  is anisotropic. We first consider the case of even  $n$ . If  $n = 0$ , then  $A(\varphi) = F$ ; thus we have  $Q(\varphi) = M_2(F)$  and  $K = F \oplus F$ .

If  $n = 2$ , then by Lemma 25.2(i),  $(V, \varphi) \cong (K, s\kappa)$  with  $s \in F^\times$ ; also,  $A(\varphi) \cong \{K, s\}$ . Thus  $Q(\varphi) = \{K, s\}$ ;  $\varphi$  is anisotropic if and only if  $K$  is a field. If  $K = F \oplus F$ , then  $Q(\varphi) \cong M_2(F)$ ; if  $K$  is a field, then by Theorem 20.8(ii),  $\{K, s\} \cong M_2(F)$  if and only if  $s \in N_{K/F}(K^\times)$ . Thus, for  $n = 2$  we have

$$(28.2) \quad \begin{aligned} Q(\varphi) = M_2(F) &\iff 1 \in \varphi[V] \\ &\iff (V, \varphi) \cong \langle F, \text{diag}[a, 1] \rangle \text{ with } a \in F^\times. \end{aligned}$$

Suppose  $n = 4$ ; then  $t = 0, 2$ , or  $4$ . The case  $t = 0$  or  $2$  can be reduced to the case  $n = 0$  or  $2$  we already discussed. Let us now assume that  $1 \in \delta_0(\varphi)$ , with no condition on  $t$ . This is the case if  $t = 4$ , in view of Theorem 25.4(ii). By Theorem 25.4(i),  $(V, \varphi) \cong (B, d\beta)$  with  $d \in F^\times$  and a quaternion algebra  $B$  over  $F$ . By Theorem 21.23(i) we can find an element  $\alpha \in B$  such that  $\alpha\alpha^t = d$ . Then the map  $x \mapsto x\alpha^{-1}$  gives an isomorphism of  $(B, \beta)$  onto  $(B, d\beta)$ . Thus  $(V, \varphi) \cong (B, \beta)$  if  $1 \in \delta_0(\varphi)$ . As shown in §25.3 (B),  $A(\varphi) \cong M_2(B)$ . Thus  $Q(\varphi) = B$ .

Next suppose  $n \notin 2\mathbf{Z}$ . If  $n = 1$ , then  $(V, \varphi) \cong \langle F, c \rangle$  with  $c \in F^\times$ , and  $A^+(\varphi) = F$ . Thus  $Q(\varphi) = M_2(F)$  and  $K_0 = F(c^{1/2})$ .

If  $n = 3$ , then by Lemma 25.2(ii),  $A^+(\varphi)$  is a quaternion algebra  $B$  over  $F$ , and  $(V, \varphi) \cong (B^\circ, -\delta\beta^\circ)$  with  $\delta \in \delta_0(\varphi)$ . Thus  $Q(\varphi) = B$  and  $K_0 = F(\delta^{1/2})$ ;  $\varphi$  is anisotropic if and only if  $B$  is a division algebra.

**Theorem 28.3.** (i) *The isomorphism class of a nondegenerate quadratic space  $(V, \varphi)$  over a nonarchimedean local field  $F$  is completely determined by  $K_0$ ,  $Q(\varphi)$ , and  $n$ .*

(ii) *Suppose  $n > 2$ ; then for each  $\delta \in F^\times$  and a quaternion algebra  $B$  over  $F$ , there exists a quadratic space  $(V, \varphi)$  of dimension  $n$  over  $F$  such that  $\delta \in \delta_0(\varphi)$  and  $Q(\varphi) = B$ . The same holds for  $n = 2$  under the assumption that  $B = M_2(F)$  if  $\delta \in F^{\times 2}$ .*

PROOF. Let  $(Z, \zeta)$  be a core subspace of  $(V, \varphi)$  and  $t = \dim(Z)$  as in §28.2. Since the isomorphism class of  $(V, \varphi)$  is determined by  $(Z, \zeta)$  and  $n$ , it is sufficient to show that  $(Z, \zeta)$  is determined by  $K_0$ ,  $Q(\zeta)$ , and  $t \pmod{2}$ . Suppose  $t \in 2\mathbf{Z}$ . Then  $K_0 \neq F$  if and only if  $t = 2$ , in which case  $(Z, \zeta) \cong (K, s\kappa)$  as in §28.2. The isomorphism class of  $(K, s\kappa)$  is determined by  $sN_{K/F}(K^\times)$ . Now  $Q(\zeta) = \{K, s\}$ , whose isomorphism class is determined by  $sN_{K/F}(K^\times)$ . Thus, if  $K_0 = K$ , then  $Q(\zeta)$  determines  $(Z, \zeta)$ , and vice versa. Suppose  $K_0 = F$  still with  $t \in 2\mathbf{Z}$ . Then  $t = 0$  or  $t = 4$  according as  $Q(\zeta) \cong M_2(F)$  or  $Q(\zeta) \not\cong M_2(F)$ . In the latter case,  $(Z, \zeta) \cong (B, \beta)$  with  $B = Q(\zeta)$  as

explained in §28.2. Thus  $(Z, \zeta)$  is determined by  $Q(\zeta)$  and  $K_0$  if  $t \in 2\mathbf{Z}$ . Next suppose  $t \notin 2\mathbf{Z}$ . Then  $t = 1$  or  $t = 3$  according as  $Q(\zeta) \cong M_2(F)$  or  $Q(\zeta) \not\cong M_2(F)$ . Then  $(Z, \zeta)$  is determined by  $K_0$  as explained in §28.2. Thus we obtain (i).

To prove (ii), let a quaternion algebra  $B$  over  $F$  and  $\delta \in F^\times$  be given. First suppose  $n$  is odd; put  $n - 3 = 2r$  and  $(V, \varphi) = \langle F, \eta_r \rangle \oplus (Z, \zeta)$  with  $(Z, \zeta) = (B^\circ, -\delta\beta^\circ)$ . As shown in §28.2,  $\delta \in \delta_0(\zeta)$  and  $B = Q(\zeta)$ , which settles the question, as  $\delta_0(\zeta) = \delta_0(\varphi)$  and  $Q(\varphi) = Q(\zeta)$ . Next, suppose  $0 < n \in 2\mathbf{Z}$ . For a given  $\delta$  define  $K_0$  and  $K$  by (22.8) and (22.9). If  $K$  is a field, then put  $(V, \varphi) = \langle F, \eta_r \rangle \oplus (K, c\kappa)$  with  $r = (n - 2)/2$  and the norm form  $\kappa$  of  $K$ ; we take  $c \in F^\times$  so that  $B = \{K, c\}$ , which is feasible. Then  $\delta \in \delta_0(c\kappa) = \delta_0(\varphi)$  and  $Q(\varphi) = Q(c\kappa) = \{K, c\} = B$ . Suppose  $K = F \oplus F$ . If  $n = 2$ , then  $\langle F, \eta_1 \rangle$  gives the desired space. If  $n > 2$ , put  $(V, \varphi) = \langle F, \eta_s \rangle \oplus (B, \beta)$ , where  $s = (n - 4)/2$ . Then  $1 \in \delta_0(\beta) = \delta_0(\varphi)$  and  $Q(\varphi) = Q(\beta) = B$  as expected. This completes the proof.

**28.4.** The isomorphism class of nondegenerate quadratic spaces over  $\mathbf{C}$  is completely determined by the dimension, and the characteristic quaternion algebra is always  $M_2(\mathbf{C})$ .

The problem with  $\mathbf{R}$  as the base field is not so trivial. Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $\mathbf{R}$  of dimension  $n$ . Then  $(V, \varphi)$  is isomorphic to  $\langle \mathbf{R}, \text{diag}[1_p, -1_q] \rangle$  with two nonnegative integers  $p$  and  $q$  such that  $p + q = n$ ; we naturally ignore  $1_0$ . We then put  $s(\varphi) = p - q$ . Clearly  $|s(\varphi)| \leq n$  and  $n - s(\varphi) \in 2\mathbf{Z}$ , and so  $\delta/|\delta|$  for  $\delta \in \delta_0(\varphi)$  equals  $(-1)^{s(\varphi)/2}$  if  $n \in 2\mathbf{Z}$ , and  $(-1)^{(s(\varphi)-1)/2}$  if  $n \notin 2\mathbf{Z}$ . The isomorphism class of  $(V, \varphi)$  over  $\mathbf{R}$  is completely determined by  $n$  and  $s(\varphi)$ .

There are exactly two isomorphism classes of quaternion algebras over  $\mathbf{R}$ , represented by  $M_2(\mathbf{R})$  and the division ring  $\mathbf{H}$  of Hamilton quaternions.

**Theorem 28.5.** *For  $(V, \varphi)$  over  $\mathbf{R}$  as above, we have*

$$(28.3a) \quad Q(\varphi) = \begin{cases} M_2(\mathbf{R}) & \text{if } n \in 2\mathbf{Z} \text{ and } s(\varphi) \equiv 0 \text{ or } 2 \pmod{8}, \\ \mathbf{H} & \text{if } n \in 2\mathbf{Z} \text{ and } s(\varphi) \equiv 4 \text{ or } 6 \pmod{8}, \end{cases}$$

$$(28.3b) \quad Q(\varphi) = \begin{cases} M_2(\mathbf{R}) & \text{if } n \notin 2\mathbf{Z} \text{ and } s(\varphi) \equiv \pm 1 \pmod{8}, \\ \mathbf{H} & \text{if } n \notin 2\mathbf{Z} \text{ and } s(\varphi) \equiv \pm 3 \pmod{8}. \end{cases}$$

PROOF. The structure of  $Q(\varphi)$  can be reduced to the case of anisotropic  $\varphi$ . Indeed,  $Q(\varphi) = Q(1_{s(\varphi)})$  if  $s(\varphi) > 0$  and  $Q(\varphi) = Q(-1_{|s(\varphi)|})$  if  $s(\varphi) < 0$ ;  $Q(\varphi) = M_2(\mathbf{R})$  if  $s(\varphi) = 0$ . Therefore it is sufficient to determine  $Q(\varphi)$  for  $\varphi = \pm 1_n$ . For  $(V, \varphi) = \langle \mathbf{Q}, \varepsilon 1_n \rangle$  with  $\varepsilon = \pm 1$  let  $K$  be its discriminant algebra. Our task is to determine  $Q(\varphi)_\mathbf{a}$ . We do this by investigating  $Q(\varphi)_p = Q(\varphi) \otimes_{\mathbf{Q}} \mathbf{Q}_p$  for each prime number  $p$ . Then from Theorem 26.6(i) we obtain  $Q(\varphi)_\mathbf{a}$ . We first observe that  $K = \mathbf{Q} \oplus \mathbf{Q}$  if  $n \in 4\mathbf{Z}$  or  $n - \varepsilon \in 4\mathbf{Z}$ , and



$K = \mathbf{Q}(\sqrt{-1})$  otherwise. Let  $t_p$  be the core dimension of  $(V, \varphi)_p$ . Clearly  $t_p$  depends only on  $n$  and  $p$ , and not on  $\varepsilon$ . There are several easy facts.

$\langle \mathbf{Q}, 1_2 \rangle \cong (K, \kappa)$  with  $K = \mathbf{Q}(\sqrt{-1})$  and its norm form  $\kappa$ ;  $(K, \kappa)_p$  is split if and only if  $p - 1 \in 4\mathbf{Z}$ .

$\langle \mathbf{Q}_p, 1_4 \rangle \cong (B, \beta)_p \cong \langle \mathbf{Q}_p, c1_4 \rangle$  for every  $c \in \mathbf{Q}_p^\times$ , where  $B$  is the quaternion algebra over  $\mathbf{Q}$  whose norm form  $\beta$  is the sum of four squares; see §27.9 and Theorem 21.23(i).

As noted in §27.9,  $D_B = 2$  for the above  $B$ , and so  $B_p$  is a division algebra if and only if  $p = 2$ . Clearly  $\langle \mathbf{Q}, 1_3 \rangle = (B^\circ, \beta^\circ)$  with the same  $B$ . Thus the core dimension of  $\langle \mathbf{Q}_p, c1_3 \rangle$  is 1 for every  $c \in \mathbf{Q}_p^\times$  if  $p \neq 2$ ;  $\langle \mathbf{Q}_2, c1_3 \rangle$  is anisotropic for every  $c \in \mathbf{Q}^\times$  if  $p = 2$ .

If  $n = 4s + r$  with  $0 \leq r \leq 3$  and  $p \neq 2$ , then  $Q(1_n)_p = Q(1_r)_p$ . We also observe that  $\langle \mathbf{Q}_p, 1_4 \rangle \cong \langle \mathbf{Q}_p, -1_4 \rangle$ , and so  $\langle \mathbf{Q}_p, 1_8 \rangle \cong \langle \mathbf{Q}_p, \text{diag}[1_4, -1_4] \rangle$ , which is split for every  $p$ . For  $4 < a < 8$  and  $a - 4 = b$  we have

$$\langle \mathbf{Q}_p, 1_a \rangle \cong \langle \mathbf{Q}_p, \text{diag}[1_b, -1_4] \rangle \cong \langle \mathbf{Q}_p, \text{diag}[1_b, -1_b] \rangle \oplus \langle \mathbf{Q}_p, -1_{8-a} \rangle,$$

and so  $Q(1_a)_p = Q(-1_{8-a})$  for  $4 < a < 8$  and every  $p$ .

From these observations we can easily derive that

$$(28.4a) \quad p \neq 2: \quad t_p = \begin{cases} 1 & \text{if } n \notin 2\mathbf{Z}, \\ 2 & \text{if } n - 2 \in 4\mathbf{Z} \text{ and } p - 3 \in 4\mathbf{Z}, \\ 0 & \text{otherwise,} \end{cases}$$

$$(28.4b) \quad p = 2: \quad t_p = a \quad \text{if } n \pm a \in 8\mathbf{Z}, \ 0 \leq a \leq 4.$$

If  $n - 2 \in 4\mathbf{Z}$  and  $p \neq 2$ , then  $(V, \varphi)_p$  can be reduced to  $(K, \varepsilon\kappa)_p$  with  $K = \mathbf{Q}(\sqrt{-1})$ , and so  $Q(\varphi)_p = Q(\varepsilon\kappa)_p = \{K_p, \varepsilon\} = M_2(\mathbf{Q}_p)$ , as  $\varepsilon \in N_{K_p/\mathbf{Q}_p}(K_p^\times)$ . Similarly if  $p = 2$  and  $n - 2 \in 8\mathbf{Z}$ , then  $K = \mathbf{Q}(\sqrt{-1})$  and  $Q(\varphi)_2 = Q(\varepsilon 1_2)_2 = \{K, \varepsilon\}_2$ , which is  $M_2(\mathbf{Q}_2)$  if and only if  $\varepsilon = 1$ . Suppose  $p = 2$  and  $n - 6 \in 8\mathbf{Z}$ . We have seen that  $Q(\varepsilon 1_6) = Q(-\varepsilon 1_2)$ , and so  $Q(\varphi)_2 = \{K, -\varepsilon\}_2$ , which is  $M_2(\mathbf{Q}_2)$  if and only if  $\varepsilon = -1$ .

To sum up,  $Q(\varphi)_p$  is a division algebra exactly when  $p = 2$  and  $n \equiv \pm 3, 4$ , or  $-2\varepsilon \pmod{8}$ . Thus  $Q(\varphi)$  is unramified at every  $p \neq 2$ , and so by Theorem 26.8(i) (or as explained in §27.9)  $Q(\varphi)_\mathbf{a} = \mathbf{H}$  if and only if  $Q(\varphi)_2$  is a division algebra, that is, if and only if  $n \equiv \pm 3, 4$ , or  $-2\varepsilon \pmod{8}$ . From this we obtain (28.3a, b) when  $|s(\varphi)| = n$ , from which we can easily derive the general case as we said at the beginning. This completes the proof.

We can also give a proof more directly and inductively by means of Lemma 23.10. There is one more type of proof given in [S04b, Section A3].

**28.6.** We now consider a nondegenerate quadratic space  $(V, \varphi)$  over a global field  $F$ . We denote by  $\mathbf{r}$  the subset of  $\mathbf{a}$  consisting of all the *real* archimedean primes. For each  $v \in \mathbf{r}$  we put  $s_v(\varphi) = s(\varphi_v)$ , where  $s(\varphi_v)$  is

determined as in §28.4. Namely,  $s_v(\varphi) = p_v - q_v$  when  $(V, \varphi)_v$  is isomorphic to  $(\mathbf{R}, \text{diag}[1_{p_v}, -1_{q_v}])$ . We call  $s_v(\varphi)$  the **index** of  $\varphi$  at  $v$ .

**Theorem 28.7.** (i) *Two nondegenerate quadratic spaces over  $F$  of dimension  $n$  and  $n'$  have isomorphic core subspaces if and only if  $n - n' \in 2\mathbf{Z}$  and they have the same discriminant field, the same characteristic algebra, and the same index at every  $v \in \mathbf{r}$ .*

(ii) *The isomorphism class of a nondegenerate quadratic space  $(V, \varphi)$  over  $F$  is determined by its dimension, discriminant field, characteristic algebra  $Q(\varphi)$ , and  $s_v(\varphi)$  for all  $v \in \mathbf{r}$ .*

PROOF. Once the dimension, the discriminant field, and  $Q(\varphi)$  are given, then by Theorem 28.3, the isomorphism class of  $(V_v, \varphi_v)$  for every  $v \in \mathbf{h}$  is determined. This together with the index at each  $v \in \mathbf{r}$  determines  $(V, \varphi)$  over  $F$  by the Hasse principle, which proves (ii). Next, the “only if”-part of (i) is obvious. Let  $(V, \varphi)$  and  $(V', \varphi')$  be nondegenerate quadratic spaces over  $F$  of dimension  $n$  and  $n'$  with the same set of data as in (i); suppose  $0 \leq n' - n \in 2\mathbf{Z}$ . Let  $(V'', \varphi'') = (V, \varphi) \oplus \langle F, \eta_r \rangle$  with  $r = (n' - n)/2$ . Then, by (ii),  $(V'', \varphi'')$  must be isomorphic to  $(V', \varphi')$ . This proves the “if”-part of (i).

**28.8.** We are going to show the existence of  $(V, \varphi)$  with a given set of data  $(n, K_0, B, \{\sigma_v\}_{v \in \mathbf{r}})$  consisting of the following objects:

(28.5a)  $0 < n \in \mathbf{Z}$ ; an extension  $K_0 = F(\delta^{1/2})$  of  $F$  with  $\delta \in F^\times$ ; a quaternion algebra  $B$  over  $F$ ; an integer  $\sigma_v$  such that  $|\sigma_v| \leq n$  and  $\sigma_v - n \in 2\mathbf{Z}$  for each  $v \in \mathbf{r}$ .

We also put

$$(28.5b) \quad K = K_0 \text{ if } [K_0 : F] = 2, \quad K = F \oplus F \text{ if } K_0 = F,$$

and  $K_v = K \otimes_F F_v$  for  $v \in \mathbf{v}$ .

Our task is to find a quadratic space  $(V, \varphi)$  over  $F$  of dimension  $n$  such that  $K$  is its discriminant algebra,  $B = Q(\varphi)$ , and  $\sigma_v = s_v(\varphi)$ . These data cannot be arbitrary. Indeed, let  $B = Q(\varphi)$  and  $\sigma_v = s_v(\varphi)$  for  $v \in \mathbf{r}$ . In view of Theorem 28.5, we have to assume:

$$(28.6a) \quad n \text{ even : } B_v = \begin{cases} M_2(\mathbf{R}) & \text{if } \sigma_v \equiv 0 \text{ or } 2 \pmod{8}, \\ \mathbf{H} & \text{if } \sigma_v \equiv 4 \text{ or } 6 \pmod{8}, \end{cases}$$

$$(28.6b) \quad n \text{ odd : } B_v = \begin{cases} M_2(\mathbf{R}) & \text{if } \sigma_v \equiv \pm 1 \pmod{8}, \\ \mathbf{H} & \text{if } \sigma_v \equiv \pm 3 \pmod{8}. \end{cases}$$

If  $n = p_v + q_v$  and  $\sigma_v = p_v - q_v$ , then  $(-1)^{(n/2)+q_v} = (-1)^{\sigma_v/2}$ . Therefore, for  $\delta$  as in (28.5a), we have obvious conditions:

$$(28.7a) \quad n \text{ even : } (-1)^{\sigma_v/2} \delta > 0 \quad \text{at each } v \in \mathbf{r},$$

$$(28.7b) \quad n \text{ odd : } (-1)^{(\sigma_v-1)/2} \delta > 0 \quad \text{at each } v \in \mathbf{r}.$$

Now the main theorem of the existence of a quadratic space with a given set of data can be stated as follows.

**Theorem 28.9.** *Given a set of data as in (28.5a, b) with  $n > 2$ , there exists a quadratic space  $(V, \varphi)$  over  $F$  of dimension  $n$  such that  $K$  is the discriminant algebra of  $\varphi$ ,  $B = Q(\varphi)$ , and  $\sigma_v = s_v(\varphi)$  for every  $v \in \mathbf{r}$ , if and only if (28.6a, b) and (28.7a, b) are satisfied. Such a  $(V, \varphi)$  exists even for  $n = 1$  or  $2$  if and only if condition (28.8a) or (28.8b) below is satisfied in addition to (28.6a, b) and (28.7a, b):*

$$(28.8a) \quad B = M_2(F) \text{ if } n = 1;$$

$$(28.8b) \text{ if } n = 2, v \in \mathbf{h}, \text{ and } B_v \text{ is a division algebra, then } K_v \text{ is a field.}$$

We have to prove only the “if”-part. We devote §§28.11 and 28.12 to the proof. We first insert here an auxiliary result.

**Lemma 28.10.** *Given a quaternion algebra  $B$  over an arbitrary field  $F$  of characteristic different from 2,  $h \in F^\times$ , and  $\delta \in F^\times$ , put  $K_0 = F(\delta^{1/2})$  and define  $(V, \varphi)$  so that  $(V, h\varphi) = \langle F, 1 \rangle \oplus (B^\circ, \delta\beta^\circ)$ . Then the discriminant field of  $\varphi$  is  $K_0$  and  $A(\varphi) \cong B \otimes_F \{K, h\}$ , where  $K$  is as in (28.5b).*

**PROOF.** We easily see that  $K_0$  is the discriminant field of  $\varphi$  and  $K$  is the discriminant algebra of  $\varphi$ . Let  $f$  be the element 1 in  $\langle F, 1 \rangle$  viewed as an element of  $V$ . Put  $e = hf$ . Since  $h\varphi[f] = 1$ , we have  $\varphi[e] = h$ . Also, since  $\varphi(e, B^\circ) = 0$ ,  $e$  commutes with every element of  $A^+(\delta B^\circ)$ . Put  $w = g_1 g_2 g_3$  and  $z = ew$  with an orthogonal basis  $\{g_i\}_{i=1}^3$  of  $(B^\circ, \delta\beta^\circ)$ . Then we can take  $z$  to be the element  $z$  of Lemma 23.7 for  $(V, \varphi)$ . Taking  $\delta\beta^\circ$  and 1 to be  $\varphi$  and  $\varphi'$  of Lemma 23.10, we obtain  $A^+(h\varphi) = A^+(\delta\beta^\circ) \otimes C$  with  $C = F + Fz$ . (Observe that  $A^+(\varphi') = F$  and  $A^-(\varphi') = Fe$ , and  $w$  here gives  $z$  there.) We have  $ez = -ze$  and  $z^* = -z$ . Thus  $C + Ce \cong \{C, h\}$ . Put  $D = A^+(\delta\beta^\circ)$ . By Lemma 24.9 we have  $A^+(h\varphi) \cong A^+(\varphi)$ , and so  $A(\varphi) = A^+(\varphi) = A^+(\varphi)e \cong D \otimes (C + Ce) = D \otimes \{C, h\}$ . Since  $D \cong B$  and  $C \cong K$ , we obtain our lemma.

**28.11.** We first prove Theorem 28.9 for  $n \leq 4$ . If  $n = 1$ , we have  $(V, \varphi) = \langle F, \delta \rangle$  and  $Q(\varphi) = M_2(F)$ . Clearly (28.6b), (28.7b), and (28.8a) are necessary and sufficient.

Suppose  $n = 2$ ; then the discussion of §28.2 shows that  $K$  must be embeddable in  $Q(\varphi)$ , and so (28.8b) is necessary. Conversely, suppose (28.6a), (28.7a), and (28.8b) are satisfied; suppose also that  $K_0 = F$ . Then  $\sigma_v = 0$  for  $v \in \mathbf{r}$  by (28.7a), and so  $B_v = M_2(\mathbf{R})$  for  $v \in \mathbf{r}$  by (28.6a). Also, (28.8b)

implies that  $B_v = M_2(F_v)$  for every  $v \in \mathbf{h}$ . Therefore  $B \cong M_2(F)$  by Theorem 26.8(ii). We take  $(V, \varphi)$  to be the split space  $\langle F, \eta_1 \rangle$ . Clearly this gives the desired space.

Next suppose  $K_0 \neq F$ . If  $v \in \mathbf{r}$  and  $B_v = \mathbf{H}$ , then (28.6a) shows that  $\sigma_v = -2$ , and so  $K_v = \mathbf{C}$  by (28.7a). This combined with (28.8b) and Lemma 27.6 means that  $K$  can be  $F$ -linearly embedded into  $B$ . Thus, by Lemma 20.4,  $B = \{K, r\}$  with some  $r \in F^\times$ . Take  $(V, \varphi) = (K, r\kappa)$ . Then, as shown in §28.2,  $K$  is the discriminant algebra and  $Q(\varphi) = B$ . Comparing conditions (28.6a) and (28.7a) with (28.3a), we see that  $\sigma_v = s_v(\varphi)$  for every  $v \in \mathbf{r}$  as expected.

If  $n = 3$ , we take  $(V, \varphi) = (B^\circ, -\delta\beta^\circ)$ . Then, as shown in Lemma 25.2(ii),  $A^+(\varphi) \cong B$  and  $K_0$  is its discriminant field. From (28.6b), (28.7b), and (28.3b) we see that  $s_v(\varphi) = \sigma_v$  for every  $v \in \mathbf{r}$ . This settles the case  $n = 3$ .

In the case  $n = 4$  we determine  $(V, \varphi)$  by

$$(28.9) \quad (V, h\varphi) = \langle F, 1 \rangle \oplus (B^\circ, \delta\beta^\circ).$$

Here we take  $h \in N_{K/F}(K^\times)$  so that  $h < 0$  at every  $v \in \mathbf{r}$  such that  $\sigma_v = -4$  and  $h > 0$  at all other  $v \in \mathbf{r}$ . Such an  $h$  exists, because  $K_v = \mathbf{R} \oplus \mathbf{R}$  if  $\sigma_v = -4$  and  $K$  is dense in  $K \otimes_{\mathbf{Q}} \mathbf{R}$ . We can easily verify that  $s_v(\varphi) = \sigma_v$  for every  $v \in \mathbf{r}$ . Moreover,  $K$  is the discriminant algebra of  $\varphi$  and  $A(\varphi) \cong M_2(B)$  by Lemma 28.10.

**28.12.** Let us now prove the case  $6 \leq n \in 2\mathbf{Z}$  by induction on  $n$ . Take a quadratic extension  $K_1 = F(\varepsilon^{1/2})$  of  $F$ , different from  $K_0$ , with  $\varepsilon \in F^\times$  such that  $\varepsilon < 0$  at every  $v \in \mathbf{r}$ . Take also  $r \in F^\times$  so that  $r > 0$  or  $r < 0$  at  $v \in \mathbf{r}$  according as  $\sigma_v \geq 4 - n$  or  $\sigma_v < 4 - n$ . (If  $\mathbf{r} = \emptyset$ , we take  $K_1$  to be a quadratic extension  $F(\varepsilon^{1/2})$  of  $F$  different from  $K_0$ , and  $r = 1$ .) Put  $\tau_v = 2 - \sigma_v$  if  $\sigma_v \geq 4 - n$  and  $\tau_v = -2 - \sigma_v$  if  $\sigma_v < 4 - n$ . Then  $\tau_v \in 2\mathbf{Z}$  and  $|\tau_v| \leq n - 2$ . By Theorem 27.11 there exists a quaternion algebra  $D$  over  $F$  such that  $\varepsilon_v(D) = \varepsilon_v(\{K_1, r\})\varepsilon_v(B)$  for every  $v \in \mathbf{v}$ . By the same theorem,  $D \otimes \{K_1, r\} \cong M_2(B')$  with a quaternion algebra  $B'$  over  $F$  such that  $\varepsilon_v(B') = \varepsilon_v(\{K_1, r\})\varepsilon_v(D)$  for every  $v \in \mathbf{v}$ . Then  $\varepsilon_v(B) = \varepsilon_v(B')$  for every  $v \in \mathbf{v}$ , and so  $B \cong B'$  by Theorem 27.7. Thus  $D \otimes \{K_1, r\} \cong M_2(B)$ . Now we observe that the set  $(n - 2, F((\varepsilon\delta)^{1/2}), D, \{\tau_v\})$  satisfies conditions (28.6a) and (28.7a). By the induction assumption we can find a quadratic space  $(W, \psi)$  over  $F$  corresponding to this set. Put  $(V, \varphi) = (K_1, r\kappa_1) \oplus (W, \varepsilon\psi)$ , where  $\kappa_1$  is the norm form of  $K_1$ . Clearly  $K$  is the discriminant algebra of  $\varphi$ , and we easily see that  $s_v(\varphi) = \sigma_v$  for every  $v \in \mathbf{r}$ . By Lemma 23.10(ii),  $A(\varphi) \cong \{K_1, r\} \otimes A(\psi)$ , and so  $Q(\varphi) = B$  as expected.

It remains to prove the case  $4 \leq n - 1 \in 2\mathbf{Z}$ . By Lemma 24.9,  $A^+(c\varphi) \cong A^+(\varphi)$  for every  $c \in F^\times$ ; also, conditions (28.6b) and (28.7b) are consistent with the change of  $\varphi$  for  $c\varphi$ . Therefore it is sufficient to prove the existence

of  $\varphi$  when  $\sigma_v \neq -n$  for every  $v \in \mathbf{r}$ . Put  $\tau_v = 1 - \sigma_v$  for every  $v \in \mathbf{r}$  and observe that  $\tau_v \in 2\mathbf{Z}$ ,  $|\tau_v| \leq n - 1$ , and the set  $(n - 1, K_0, B, \{\tau_v\})$  satisfies conditions (28.6a) and (28.7a). Since we have proved the case of even  $n$ , there exists a quadratic space  $(W, \psi)$  corresponding to that set. Put  $(V, \varphi) = \langle F, 1 \rangle \oplus (W, -\psi)$ . Then  $K_0$  is the discriminant field of  $\varphi$  and  $s_v(\varphi) = \sigma_v$  for every  $v \in \mathbf{r}$ . Taking  $\langle F, 1 \rangle$  as  $\varphi$  of Lemma 23.10(ii), we find that  $A^+(\varphi) \cong F \otimes_F A(\psi)$ , and so  $Q(\varphi) = Q(\psi) = B$ . This proves the case of odd  $n$  and completes the proof of Theorem 28.9.

**28.13.** Let us now present a short history of classification of quadratic forms over an algebraic number field  $F$ , or rather, of the question of how one can associate some invariants to a given form  $\varphi$  so that  $\varphi$  can be determined by those invariants. The dimension, discriminant, and indices (signatures) of  $\varphi$  at real archimedean primes  $v \in \mathbf{r}$  as defined above are obvious invariants. In addition, to a form  $\varphi = \sum_{i=1}^n a_i x_i^2$  and a prime  $v \in \mathbf{v}$  Hasse associated a number  $\alpha_v(\varphi)$ , which is either 1 or  $-1$ , and defined by

$$\alpha_v(\varphi) = \prod_{i \leq j} (a_i, a_j)_v,$$

where  $(a, b)_v$  is the Hilbert symbol defined in §26.1. He then showed in [Has] that the equivalence class of  $\varphi$  over  $F$  corresponds to the set consisting of these numbers  $\{\alpha_v(\varphi)\}$  and the above “obvious invariants” satisfying certain conditions, and the correspondence is one-to-one; namely he constructed a unique quadratic form for a given set of such data.

This was followed by a work of Witt [W]. Given a form  $\varphi$  of  $n$  variables, he considered the form  $\varphi^*$  of  $2n$  variables which is the direct sum of  $\varphi$  and the form  $-\sum_{i=1}^n y_i^2$ , and denoted by  $S(\varphi)$  the Clifford algebra of  $\varphi^*$ . Now  $S(\varphi)$  is a central simple algebra over  $F$ . He showed that  $\alpha_v(\varphi)$  is actually the invariant of  $S(\varphi)$  at  $v$  in the standard sense.

Some later authors chose  $\alpha'_v(\varphi) = \prod_{i < j} (a_i, a_j)_v$  instead of  $\alpha_v(\varphi)$ , but this together with the discriminant gives an equivalent set of invariants. Though we can develop a reasonable theory of classification of quadratic forms with these invariants  $\alpha_v(\varphi)$  and  $\alpha'_v(\varphi)$ , it must be pointed out that they have some features which do not look so natural. Indeed, if  $\varphi$  is the hyperbolic form  $x_1 x_2 + x_3 x_4$  of four variables  $\{x_i\}_{i=1}^4$  over  $\mathbf{Q}$ , then both  $\alpha_v(\varphi)$  and  $\alpha'_v(\varphi)$  are  $-1$  for  $v = 2$ . On the other hand, they are 1 for every prime  $v$  if  $\varphi$  is the sum of  $n$  squares over any number field  $F$ . This is a matter of perspective, but it is more natural to assign a *trivial* quantity to a hyperbolic form. Besides, one might say, it is too pedestrian to define invariants in terms of a diagonal matrix that represents the form.

In fact, better invariants were introduced by Eichler in [E52b]. He associated with  $\varphi$  a set of invariants  $\{\chi_v(\varphi)\}$  different from  $\{\alpha_v(\varphi)\}$  and  $\{\alpha'_v(\varphi)\}$ ,

and proved a result of the same type as what Hasse proved. This set  $\{\chi_v(\varphi)\}$  is conceptually more natural than  $\{\varepsilon_v(\varphi)\}$ , as  $\chi_v(\varphi)$  is more closely connected with the structure of  $\varphi$  at  $v$ .

In fact, it can be shown that  $\chi_v(\varphi) = \varepsilon_v(Q(\varphi))$  with the symbol  $\varepsilon_v$  of (26.8); namely  $\chi_v(\varphi) = 1$  or  $-1$  according as  $Q(\varphi)_v$  is isomorphic to  $M_2(F_v)$  or is a division algebra. However, this is not the way Eichler defined  $\chi_v(\varphi)$  in [E52b]. He defined the invariant in each case according to the type of  $\varphi_v$ , without using Clifford algebras. The fact that it is the invariant of  $Q(\varphi)$  at  $v$  can easily be seen for  $v \in \mathbf{h}$ . The fact for  $v \in \mathbf{a}$  follows from formulas (28.3a, b), which is nontrivial. In Satz 23.2 of [E52b] he constructed a space  $(V', \varphi')$  corresponding to  $(m, K_0, B, \{\sigma_v\})$  with some  $m$  such that  $m - n \in 2\mathbf{Z}$ , and proved the product formula  $\prod_{v \in \mathbf{v}} \chi_v(\varphi) = 1$  at the end of the proof. Then he derived a theorem equivalent to Theorem 28.9 in Satz 23.3 of [E52b] by establishing the desired  $(V, \varphi)$  as a subspace of  $(V', \varphi')$ .

In the present book we employed  $Q(\varphi)$  instead of  $\{\chi_v(\varphi)\}$ , as we think this approach is clearer and easier. In fact, it allows us to present the desired  $(V, \varphi)$  more directly without using an auxiliary space of an unspecified dimension. In addition, our methods enable us to classify integer-valued quadratic forms to the extent we will discuss in Section 31.

## 29. Lattices in a quadratic space

**29.1.** Our next problem is to investigate quadratic forms over the ring of integers. We do this by considering lattices in a given quadratic space. We take our setting to be that of §21.1. We use the symbols  $F$ ,  $\mathbf{g}$ , and the same terminology. Thus  $F$  is either a global field, which means an algebraic number field of finite degree, or a local field, which means the completion of a global field at a nonarchimedean prime. In this section we will often call a  $\mathbf{g}$ -lattice in a vector space over  $F$  simply a lattice.

Let  $(V, \varphi)$  be a nondegenerate quadratic space over a local or global field  $F$ . Given a  $\mathbf{g}$ -lattice  $L$  in  $V$ , we denote by  $\mu(L)$  the  $\mathbf{g}$ -ideal generated by the elements  $\varphi[x]$  for all  $x \in L$ , and by  $\mu_0(L)$  the  $\mathbf{g}$ -ideal generated by the elements  $\varphi(x, y)$  for all  $x, y \in L$ . We call  $L$   $\varphi$ -**integral**, or simply **integral**, if  $\mu(L) \subset \mathbf{g}$ . We call an integral lattice  $L$   $\varphi$ -**maximal**, or simply **maximal**, if  $L$  is the only integral lattice containing  $L$ . Similarly we call  $L$   $\varphi^*$ -**integral** if  $\mu_0(L) \subset \mathbf{g}$ , and call a  $\varphi^*$ -integral lattice  $L$   $\varphi^*$ -**maximal** if it is the only  $\varphi^*$ -integral lattice containing it. If  $\alpha \in O^\varphi$ , we have clearly  $\mu(L\alpha) = \mu(L)$  and  $\mu_0(L\alpha) = \mu_0(L)$ ; if  $L$  is maximal, so is  $L\alpha$ . Since  $2\varphi(x, y) = \varphi[x + y] - \varphi[x] - \varphi[y]$ , we have

$$(29.1) \quad 2\mu_0(L) \subset \mu(L) \subset \mu_0(L).$$

For a  $\mathbf{g}$ -lattice  $L$  in  $V$  we put

$$(29.2) \quad \varphi[L] = \{\varphi[x] \mid x \in L\},$$

$$(29.3a) \quad L^\varphi = \{x \in V \mid \varphi(x, L) \subset \mathfrak{g}\},$$

$$(29.3b) \quad \tilde{L} = L^\sim = \{y \in V \mid 2\varphi(y, L) \subset \mathfrak{g}\},$$

$$(29.3c) \quad d(L) = [L^\varphi/L],$$

where the symbol  $[ \ / ]$  is as in §21.25. Then  $\tilde{L} = L^{2\varphi}$  and  $L^\varphi = 2\tilde{L}$ . Clearly  $L^\varphi$  is a  $\mathfrak{g}$ -lattice in  $V$ , and  $L \subset \tilde{L}$  if  $\mu(L) \subset \mathfrak{g}$ . Also,  $\tilde{L} \subset \tilde{M}$  if  $M \subset L$ ,  $(cL)^\sim = c^{-1}\tilde{L}$  for every  $c \in F^\times$ ;  $(L\gamma)^\sim = \tilde{L}\gamma$  and  $d(L\gamma) = d(L)$  for every  $\gamma \in O^\varphi(V)$ . We call  $d(L)$  the **discriminant ideal** of  $L$ . In the simplest case in which  $F = \mathbf{Q}$ ,  $\mathfrak{g} = \mathbf{Z}$ ,  $(V, \varphi) = \langle \mathbf{Q}, \Phi \rangle$  with  $\Phi = {}^t\Phi \in GL_n(\mathbf{Q})$  (see §28.1), and  $L = \mathbf{Z}_n^1$ , we have  $L^\varphi = L\Phi^{-1}$  and  $d(L) = \det(\Phi)\mathbf{Z}$ .

If  $L$  is defined in the global case, for every  $v \in \mathbf{h}$  we have

$$(29.4) \quad \mu(L_v) = \mu(L)_v, \quad \mu_0(L_v) = \mu_0(L)_v, \quad (L_v)^\sim = (\tilde{L})_v, \quad \text{and} \quad d(L_v) = d(L)_v,$$

where  $L_v$  is the  $\mathfrak{g}_v$ -linear span of  $L$  in  $V_v$ ; see §21.5. The latter three equalities are easy. As for the first one, we have clearly  $\mu(L)_v \subset \mu(L_v)$ . If  $a_i \in \mathfrak{g}_v$  and  $x_i \in L$ , then  $\varphi[\sum_i a_i x_i] = \sum_i a_i^2 \varphi[x_i] + \sum_{i < j} 2a_i a_j \varphi(x_i, x_j)$ , which is contained in  $\mu(L)_v$  by virtue of (29.1). Thus  $\mu(L_v) \subset \mu(L)_v$ , and so  $\mu(L_v) = \mu(L)_v$ .

Now  $(\tilde{L})^\sim = L$  for any  $\mathfrak{g}$ -lattice  $L$ . To prove this, first assume  $F$  to be local, take a  $\mathfrak{g}$ -basis  $\{x_i\}$  of  $L$ , and take also a basis  $\{y_i\}$  of  $V$  so that  $2\varphi(x_i, y_j) = \delta_{ij}$ . Then  $\tilde{L} = \sum_{i=1}^n \mathfrak{g}y_i$ , from which we can derive  $(\tilde{L})^\sim = L$ . The global case follows from this combined with Lemma 21.6(i).

**Lemma 29.2.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over a local or global field  $F$ . Then the following assertions hold.*

(1) *Given an integral resp.  $\varphi^*$ -integral lattice  $M$  in a subspace  $X$  of  $V$  on which  $\varphi$  is nondegenerate, there exists a maximal resp.  $\varphi^*$ -maximal lattice in  $V$  containing  $M$ .*

(2) *Let  $L$  and  $M$  be lattices in  $V$ . If  $M$  is maximal,  $M \subset L$ , and  $c\mu(L) \subset \mu(M)$  with  $c \in \mathfrak{g}$ , then  $cL \subset M$ .*

(3) *If  $L$  is maximal,  $h \in \tilde{L}$ , and  $\varphi[h] \in \mathfrak{g}$ , then  $h \in L$ .*

(4) *Let  $h$  be an element of  $V$  such that  $\varphi[h] \neq 0$  and  $L$  a lattice in  $V$ ; let  $\mathfrak{a}$  be a  $\mathfrak{g}$ -ideal such that  $2\mathfrak{a}\tilde{L} \subset L$ . Then  $\varphi[h]\varphi(h, L)^{-2}\mathfrak{a}$  is an integral  $\mathfrak{g}$ -ideal that depends only on  $L$ ,  $\mathfrak{a}$ , and  $F^\times h$ .*

(5) *Suppose  $F$  is global; let  $L$  be a lattice in  $V$ . Then  $L$  is maximal resp.  $\varphi^*$ -maximal if and only if  $L_v$  is maximal resp.  $\varphi^*$ -maximal for every  $v \in \mathbf{h}$ .*

**PROOF.** To prove (i), put  $Y = X^\perp$ . We can easily find an integral lattice  $N$  in  $Y$ . Then  $M + N$  is an integral lattice in  $V$ . Therefore we may assume that  $X = V$  and  $M$  is a lattice in  $V$ . Take an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $V$  contained in  $M$ ; let  $H = (\sum_{i=1}^n \mathfrak{g}e_i)^\sim$ . Then  $H$  is a lattice in  $V$ . Let  $L$  be an integral

lattice in  $V$  containing  $M$ . By (29.1) we have  $2\varphi(L, e_i) \subset \mathfrak{g}$ , so that  $L \subset H$ . Since  $[H : M] < \infty$  by (21.3c), we can find a maximal one among the integral lattices  $L$  containing  $M$ . The same type of argument is applicable to  $\varphi^*$ -integral lattices. This proves (1). Given  $L, M$ , and  $c$  as in (2), put  $N = M + cL$  and take  $u = x + cy \in N$  with  $x \in M$  and  $y \in L$ . Then  $\varphi[u] = \varphi[x] + 2c\varphi(x, y) + c^2\varphi[y] \in \mu(M)$  by our assumption and (29.1). Therefore  $\mu(N) = \mu(M)$ . Since  $M$  is maximal, we have  $N = M$ , so that  $cL \subset M$ . This proves (2). Let  $h$  and  $L$  be as in (3). Then we easily see that  $\varphi[x] \in \mathfrak{g}$  for every  $x \in L + \mathfrak{g}h$ . Since  $L$  is maximal,  $h$  must be contained in  $L$ . This proves (3). As for (4), that  $\varphi[h]\varphi(h, L)^{-2}\mathfrak{a}$  depends only on  $L, \mathfrak{a}$ , and  $F^\times h$  is obvious. To show that it is integral, put  $\mathfrak{x} = \varphi(h, L)$ . Then  $2^{-1}\mathfrak{x}^{-1}h \in \tilde{L}$ . By our choice of  $\mathfrak{a}$ , we have  $\mathfrak{a}\mathfrak{x}^{-1}h \subset L$ , and so  $\varphi[h]\mathfrak{a}\mathfrak{x}^{-2} = \varphi(h, \mathfrak{a}\mathfrak{x}^{-2}h) \subset \mathfrak{x}^{-1}\varphi(h, L) = \mathfrak{g}$ , which proves (4). The “if”-part of (5) is obvious, since if  $L \subsetneq M$ , then  $L_v \subsetneq M_v$  for some  $v \in \mathbf{h}$ . Conversely, suppose  $L$  is maximal and  $L_u$  is not maximal for some  $u \in \mathbf{h}$ . Take a maximal lattice  $M'$  in  $V_u$  containing  $L_u$ . By Lemma 21.6(i) there exists a lattice  $M$  in  $V$  such that  $M_u = M'$  and  $M_v = L_v$  for every  $v \in \mathbf{h}, v \neq u$ . Then  $L \subsetneq M$  and  $\mu(M)_v \subset \mathfrak{g}_v$  for every  $v \in \mathbf{h}$ , and so  $M$  is integral, a contradiction, since  $L$  is maximal. This proves the “only if”-part of (5) for maximal lattices. The case of  $\varphi^*$ -maximal lattices can be proved in the same way. This completes the proof.

**Lemma 29.3.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over a local or global field  $F$ , and  $L$  a maximal lattice in  $V$ . Suppose  $V$  has a weak Witt decomposition  $V = Fx + Fy + W$  with  $x, y$ , and  $W$  such that  $\varphi[x] = \varphi[y] = 0$ ,  $2\varphi(x, y) = 1$ , and  $W = (Fx + Fy)^\perp$ . Then there exists a  $\mathfrak{g}$ -ideal  $\mathfrak{a}$  such that  $L = \mathfrak{a}x + \mathfrak{a}^{-1}y + (L \cap W)$ .*

PROOF. Let  $\mathfrak{a} = \{a \in F \mid ax \in L\}$  and  $\mathfrak{b} = \{a \in F \mid ax \in \tilde{L}\}$ . Then  $2\varphi(\mathfrak{a}x, L) \subset 2\mu_0(L) \subset \mu(L) \subset \mathfrak{g}$ . Thus  $\mathfrak{a}x \subset \tilde{L}$ , and so  $\mathfrak{a} \subset \mathfrak{b}$ . Since  $\mathfrak{b}x \subset \tilde{L}$ , we have  $2\varphi(\mathfrak{b}x, L) \subset \mathfrak{g}$ , and so we have  $\varphi[\mathfrak{b}x + z] \subset \mathfrak{g}$  for every  $z \in L$ . Then the maximality of  $L$  shows that  $\mathfrak{b}x + L = L$ , and so  $\mathfrak{b} = \mathfrak{a}$ . Take an  $F$ -basis  $\{e_i\}_{i=1}^{n-2}$  of  $W$  and put  $e_{n-1} = y$  and  $e_n = x$ . By Theorem 10.19(i) there exists an  $F$ -basis  $\{g_i\}_{i=1}^n$  of  $V$  such that  $g_i \in \sum_{k=i}^n Fe_k$  and  $\tilde{L} = \sum_{i=1}^n \mathfrak{c}_i g_i$  with  $\mathfrak{g}$ -ideals  $\mathfrak{c}_i$ . Then  $\mathfrak{c}_n = \mathfrak{a}$  and  $\tilde{L} \cap Fx = \mathfrak{a}x$ . Since  $\varphi(y, W) = \varphi(y, y) = 0$ , we have  $\varphi(y, \tilde{L}) = \varphi(y, \tilde{L} \cap (Fx + Fy)) = \varphi(y, \tilde{L} \cap Fx) = \varphi(y, \mathfrak{a}x)$ . Therefore  $2\varphi(\mathfrak{a}^{-1}y, \tilde{L}) = 2\varphi(\mathfrak{a}^{-1}y, \mathfrak{a}x) = \mathfrak{g}$ , and so  $\mathfrak{a}^{-1}y \subset (\tilde{L})^\sim = L$ . Thus  $\mathfrak{a}x + \mathfrak{a}^{-1}y \subset L$ . Let  $h \in L$  and  $h = ax + by + w$  with  $a, b \in F$  and  $w \in W$ . Then  $\mathfrak{a}a^{-1} = 2\varphi(h, \mathfrak{a}^{-1}y) \subset \mathfrak{g}$ , and so  $a \in \mathfrak{a}$ , and similarly  $b \in \mathfrak{a}^{-1}$ . Thus  $w = h - ax - by \in L \cap W$ , which leads to the desired conclusion.

**29.4.** Let  $(V, \varphi)$  be a nondegenerate quadratic space over a local or global field  $F$ . Given an integral lattice  $\Lambda$  in  $V$ , we denote by  $A(\Lambda)$  the subring of  $A(V)$



generated by  $\mathfrak{g}$  and  $\Lambda$ , and put  $A^\pm(\Lambda) = A(\Lambda) \cap A^\pm(V)$ . If  $\{\ell_i\}_{i=1}^n$  is a  $\mathfrak{g}$ -basis of  $\Lambda$ , then  $A(\Lambda)$  is spanned over  $\mathfrak{g}$  by the products  $\ell_{i_1} \cdots \ell_{i_s}$ ,  $i_1 < \cdots < i_s$  for  $0 \leq s \leq n$ , as considered in §23.3. This can easily be verified because  $x^2 \in \mathfrak{g}$  and  $xy + yx \in \mathfrak{g}$  for every  $x, y \in \Lambda$ . Similarly  $A^+(\Lambda)$  is spanned over  $\mathfrak{g}$  by such products with even  $s$ . Therefore  $A(\Lambda)$  and  $A^+(\Lambda)$  are orders in  $A(V)$  and  $A^+(V)$ , respectively, which are stable under the canonical automorphism and involution of  $A(V)$ .

**Lemma 29.5.** *In the setting of §29.4 let  $L$  be an integral lattice in  $V$ . Then  $L\tau(x) = L$  for every  $x \in L$  such that  $x^2 \in \mathfrak{g}^\times$ . Moreover,  $A(L) \cap V = L$  if  $L$  is maximal.*

PROOF. Suppose  $x \in L$  and  $x^2 = c \in \mathfrak{g}^\times$ ; let  $y \in L$ . Then  $y\tau(x) = c^{-1}xyx = c^{-1}(xy + yx)x - y \in L$ , since  $xy + yx \in \mathfrak{g}$ . Thus  $L\tau(x) \subset L$ , and so  $L\tau(x) = L$ , since  $\tau(x)^2 = 1$ . Next, assuming  $L$  to be maximal, put  $M = A(L) \cap V$ . This is a lattice in  $V$  containing  $L$ . For  $x \in M$  we have  $x^2 \in A(L) \cap F = \mathfrak{g}$ , and so  $M$  is integral. Since  $L$  is maximal, we have  $L = M$ . This completes the proof.

Hereafter in this section, until Lemma 29.12, we assume that  $F$  is local. We let  $\mathfrak{p}$  denote the maximal ideal of  $\mathfrak{g}$  and  $\pi$  an unspecified prime element of  $F$ . We fix a nondegenerate quadratic space  $(V, \varphi)$  over  $F$ , put  $n = \dim(V)$ , and denote by  $K$  its discriminant algebra. We denote by  $\mathfrak{r}$  the maximal order of  $K$ , which is  $\mathfrak{g} \oplus \mathfrak{g}$  if  $K = F \oplus F$ . We also denote by  $\mathfrak{d}$  the different of  $K$  relative to  $F$ , which we define to be  $\mathfrak{r}$  if  $K = F \oplus F$ . We define  $N_{K/F}(\mathfrak{d})$  to be  $\mathfrak{g}$  if  $K = F \oplus F$ .

**Lemma 29.6.** *For every lattice  $L$  in  $V$ , there exists an element  $\sigma$  of  $O(\varphi)$  such that  $\det(\sigma) = -1$  and  $L\sigma = L$ .*

PROOF. Take  $y \in L$  so that  $\mu(L) = \varphi[y]\mathfrak{g}$ . Define  $\sigma \in GL(V)$  so that  $y\sigma = -y$  and  $z\sigma = z$  for every  $z \in (Fy)^\perp$ . Then  $\sigma \in O^\varphi$  and  $\det(\sigma) = -1$ . (Actually  $\sigma = -\tau(y)$ ; see §24.4.) Given  $x \in L$ , put  $a = \varphi(x, y)/\varphi[y]$  and  $z = x - ay$ . Then  $\varphi(z, y) = 0$  and  $2a \in \mathfrak{g}$ , since by (29.1),  $2\varphi(x, y) \in \mu(L) = \varphi[y]\mathfrak{g}$ . Therefore  $x\sigma = z\sigma + ay\sigma = z - ay = x - 2ay \in L$ , so that  $L\sigma \subset L$ . Then  $L\sigma = L$  since  $\det(\sigma) = -1$ .

**Lemma 29.7.** *Suppose that  $\varphi$  is anisotropic. Let*

$$(29.5) \quad L = \{x \in V \mid \varphi[x] \in \mathfrak{g}\}.$$

*Then  $L$  is a maximal lattice,  $L\alpha = L$  for every  $\alpha \in O^\varphi$ , and there is no other maximal lattice in  $V$ .*

PROOF. Clearly  $\mathfrak{g}x \subset L$  if  $x \in L$ . To show that  $L$  is closed under addition, suppose that  $x, y \in L$  and  $x+y \notin L$ ; put  $W = Fx + Fy$ . Then  $\varphi[x+y] \notin \mathfrak{g}$  and

we easily see that  $\dim(W) = 2$ . Put  $b = \varphi[x]$ ,  $c = \varphi[y]$ , and  $d = \varphi(x, y)$ . Then  $2d = \varphi[x + y] - b - c \notin \mathfrak{g}$ , and so  $d \neq 0$  and  $(2d)^{-1} \in \mathfrak{p}$ . Now  $bc - d^2 = -d^2(1 - d^{-2}bc)$ . Since  $b, c \in \mathfrak{g}$ , we have  $d^{-2}bc \in 4\mathfrak{p}^2$ , and so, by Lemma 21.12(i),  $1 - d^{-2}bc$  is a square in  $F$ . This means that if  $\psi$  is the restriction of  $\varphi$  to  $W$ , then  $1 \in \delta_0(\psi)$ , and so  $\psi$  is isotropic by Lemma 22.7, a contradiction. Thus  $L$  is a  $\mathfrak{g}$ -module. Clearly  $L$  contains every integral lattice in  $V$ , and so  $L$  is maximal. The remaining points of our lemma are obvious.

**Lemma 29.8.** *Let  $L$  be a maximal lattice in  $V$ . Then there exists a Witt decomposition  $V = \sum_{i=1}^r (Fx_i + Fy_i) + Z$  such that  $L = \sum_{i=1}^r (\mathfrak{g}x_i + \mathfrak{g}y_i) + M$  with  $M = \{u \in Z \mid \varphi[u] \in \mathfrak{g}\}$ . Conversely, given a Witt decomposition  $V = \sum_{i=1}^r (Ff_i + Fe_i) + Z$ , put*

$$L = \sum_{i=1}^r (\mathfrak{g}f_i + \mathfrak{g}e_i) + N, \quad N = \{v \in Z \mid \varphi[v] \in \mathfrak{g}\}.$$

*Then  $L$  is maximal; moreover,  $\mu(L) = \mathfrak{g}$  if  $r > 0$ .*

PROOF. We prove the direct part by induction on  $n$ . If  $\varphi$  is anisotropic, it is included in Lemma 29.7; so we assume that  $\varphi$  is isotropic. Then  $V$  has a weak Witt decomposition  $V = Fx + Fy + W$  with  $x, y$ , and  $W$  such that  $\varphi[x] = \varphi[y] = 0$ ,  $2\varphi(x, y) = 1$ , and  $W = (Fx + Fy)^\perp$ . By Lemma 29.3 we have  $L = \mathfrak{a}x + \mathfrak{a}^{-1}y + L'$  with  $L' = L \cap W$  and a  $\mathfrak{g}$ -ideal  $\mathfrak{a}$ . Replacing  $x$  and  $y$  by their suitable scalar multiples, we may assume that  $\mathfrak{a} = \mathfrak{g}$ . Clearly  $L'$  is maximal. Applying our induction to  $L'$ , we obtain the desired expression for  $L$ . Next, define  $L$  as in the converse part. Clearly  $L$  is integral. If  $r = 0$ , then  $L$  is maximal by Lemma 29.7. Assuming that  $r > 0$ , take an integral lattice  $H$  containing  $L$ ; let  $w = \sum_{i=1}^r (a_i f_i + b_i e_i) + z \in H$  with  $a_i, b_i \in F$  and  $z \in Z$ . Then  $a_i = 2\varphi(w, e_i) \in 2\mu_0(H) \subset \mathfrak{g}$ , and similarly  $b_i \in \mathfrak{g}$ . Consequently  $\sum_{i=1}^r (a_i f_i + b_i e_i) \in L$ , and so  $z \in H$  and  $\varphi[z] \in \mathfrak{g}$ . Thus  $z \in N$ , and consequently  $w \in L$ , which shows that  $L$  is maximal as expected. That  $\mu(L) = \mathfrak{g}$  if  $r > 0$  is obvious. This completes the proof.

**Lemma 29.9.** *Let  $L$  and  $L'$  be maximal lattices in  $V$ . Then  $L\alpha = L'$  with some  $\alpha \in SO(\varphi)$ .*

PROOF. If  $\varphi$  is anisotropic, then  $L = L'$  by Lemma 29.7. If  $\varphi$  is isotropic, then by Lemma 29.8, there exists a Witt decomposition  $V = \sum_{i=1}^r (Fx_i + Fy_i) + Z$  such that  $L = \sum_{i=1}^r (\mathfrak{g}x_i + \mathfrak{g}y_i) + M$  with  $M = \{u \in Z \mid \varphi[u] \in \mathfrak{g}\}$ . Similarly we have a Witt decomposition  $V = \sum_{i=1}^r (Fx'_i + Fy'_i) + Z'$  such that  $L' = \sum_{i=1}^r (\mathfrak{g}x'_i + \mathfrak{g}y'_i) + M'$  with  $M' = \{u \in Z' \mid \varphi[u] \in \mathfrak{g}\}$ . By Witt's theorem, there exists an isomorphism  $\gamma$  of  $(Z, \varphi)$  onto  $(Z', \varphi)$ . Then clearly  $M\gamma = M'$ . Extend  $\gamma$  to an element  $\beta$  of  $GL_F(V)$  by putting  $x_i\beta = x'_i$  and  $y_i\beta = y'_i$ . Then  $\beta \in O(\varphi)$  and  $L\beta = L'$ . This combined with Lemma 29.6 proves our lemma.

**29.10.** Let us now determine  $\mu(L)$ ,  $\mu(\tilde{L})$ , and  $[\tilde{L}/L]$  for a maximal lattice  $L$  in  $V$ . These do not depend on the choice of  $L$  in view of Lemma 29.9. Since  $L^\varphi = 2\tilde{L}$ , we have  $[\tilde{L}/L] = 2^n d(L)$ , and so we will eventually determine  $d(L)$ . We take a Witt decomposition  $V = \sum_{i=1}^r (Fx_i + Fy_i) + Z$  and put  $t = \dim(Z)$ . Then  $\delta_0(\varphi) = \delta_0(\zeta)$ , and so  $K$  is the discriminant algebra of both  $\varphi$  and  $\zeta$ . By Lemma 29.8, we can put  $L = \sum_{i=1}^r (\mathfrak{g}x_i + \mathfrak{g}y_i) + M$  with  $M = \{u \in Z \mid \varphi[u] \in \mathfrak{g}\}$ . We easily see that

$$(29.6) \quad \tilde{L} = \sum_{i=1}^r (\mathfrak{g}x_i + \mathfrak{g}y_i) + \tilde{M},$$

and so  $[\tilde{L}/L] = [\tilde{M}/M]$ ; thus  $2^{2r}d(L) = d(M)$ . Therefore the problem can be reduced to the investigation of a maximal lattice  $M$  in  $Z$ .

If  $t = 1$ , then  $(Z, \zeta) = \langle F, \delta \rangle$  with  $\delta \in \delta_0(\zeta)$ . We may assume that  $\mathfrak{p} \subset \delta\mathfrak{g} \subset \mathfrak{g}$ . Then clearly  $M = \mathfrak{g}$ ,  $\mu(M) = \delta\mathfrak{g}$ ,  $\tilde{M} = (2\delta)^{-1}M$ ,  $\mu(\tilde{M}) = (4\delta)^{-1}\mathfrak{g}$ ,  $M$  is  $\zeta^*$ -maximal, and  $[\tilde{M}/M] = 2\delta\mathfrak{g}$ .

If  $t = 2$ , then  $(Z, \zeta) = (K, s\kappa)$  with  $s \in F^\times$ ;  $K$  must be a field, as  $\zeta$  is anisotropic. If  $K$  is ramified over  $F$ , then  $N_{K/F}(K^\times)$  contains a prime element of  $F$ , and so choosing  $s$  suitably, we can assume that  $s \in \mathfrak{g}^\times$ . Then  $M = \mathfrak{r}$ ,  $\mu(M) = \mathfrak{g}$ ,  $\tilde{M} = \mathfrak{d}^{-1}$ ,  $\mu(\tilde{M}) = N_{K/F}(\mathfrak{d})^{-1}$ , and  $[\tilde{M}/M] = N_{K/F}(\mathfrak{d})$ .

If  $t = 2$  and  $K$  is unramified, then we may assume that  $\mathfrak{p} \subset s\mathfrak{g} \subset \mathfrak{g}$ . We have  $M = \mathfrak{r}$ ,  $\mu(M) = s\mathfrak{g}$ ,  $\tilde{M} = s^{-1}\mathfrak{r} = \mu(M)^{-1}\mathfrak{r}$ ,  $\mu(\tilde{M}) = s^{-1}\mathfrak{g}$ , and  $[\tilde{M}/M] = \mu(M)^2$ . Since  $Q(\varphi) = Q(\zeta) = \{K, s\}$ , we have  $s\mathfrak{g} = \mathfrak{p}$  if and only if  $Q(\varphi)$  is a division algebra.

Suppose  $t = 4$ . By Theorem 25.4(ii),  $1 \in \delta_0(\varphi)$  and  $(Z, \zeta) = (B, \beta)$  with a division quaternion algebra  $B$  over  $F$ ;  $2\beta(x, y) = \text{Tr}_{B/F}(xy^t)$ . Let  $\mathfrak{o}$  be the maximal order in  $B$  which is uniquely determined by  $\mathfrak{o} = \{\alpha \in B \mid \alpha\alpha^t \in \mathfrak{g}\}$ ; see Theorem 21.21. Therefore  $M = \mathfrak{o}$ ,  $\mu(M) = \mathfrak{g}$ , and  $\tilde{M} = \xi^{-1}\mathfrak{o}$  with an element  $\xi$  of  $\mathfrak{o}$  such that  $\xi\xi^t\mathfrak{g} = \mathfrak{p}$ , as can be seen from the same theorem. Thus  $\mu(\tilde{M}) = \mathfrak{p}^{-1}$  and  $[\tilde{M}/M] = \mathfrak{p}^2$ .

Finally suppose  $t = 3$ . Let  $B$  and  $\mathfrak{o}$  be as in the case  $t = 4$ . By Theorem 25.2(ii),  $(Z, \zeta) = (B^\circ, -\delta\beta^\circ)$  with  $\delta \in \delta_0(\zeta)$ . Replacing  $\delta$  by a suitable element of  $\delta F^{\times 2}$ , we may assume that  $\mathfrak{p} \subset \delta\mathfrak{g} \subset \mathfrak{g}$ . By Theorem 21.21 we can put  $B = J + J\omega$  with an unramified quadratic extension  $J$  of  $F$  and an element  $\omega$  such that  $\omega a = a^t\omega$  for every  $a \in J$  and  $\omega^2$  is a prime element of  $F$ ;  $\mathfrak{o} = \mathfrak{r} + \mathfrak{r}\omega$ , where  $\mathfrak{r}$  is the maximal order of  $J$ . Take  $u \in \mathfrak{r}$  so that  $\mathfrak{r} = \mathfrak{g} + \mathfrak{g}u$  and put  $y = u - u^t$ . Then  $y \in \mathfrak{r}^\times$  by (14.9),  $B^\circ = Fy + J\omega$ , and  $\tilde{M} = \{z \in B^\circ \mid \delta \text{Tr}_{B/F}(zM) \subset \mathfrak{g}\}$ . If  $\delta\mathfrak{g} = \mathfrak{g}$ , then  $M = \mathfrak{g}y + \mathfrak{r}\omega$ ,  $\mu(M) = \mathfrak{g}$ , and  $\tilde{M} = 2^{-1}\mathfrak{g}y + \mathfrak{r}\omega^{-1}$ . If  $\delta\mathfrak{g} = \mathfrak{p}$ , then  $M = \mathfrak{g}y + \mathfrak{r}\omega^{-1}$ ,  $\mu(M) = \mathfrak{g}$ , and  $\tilde{M} = (2\mathfrak{p})^{-1}y + \mathfrak{r}\omega^{-1}$ . Thus  $[\tilde{M}/M] = 2\delta^{-1}\mathfrak{p}^2$  and  $\mu(\tilde{M})^{-1} = 4\delta\mathfrak{g} \cap \mathfrak{p}$  in both cases.

To sum up, for a maximal lattice  $L$  we obtain

$$(29.7) \quad [\tilde{L}/L] = \begin{cases} 2\delta\mathfrak{g} & \text{if } t = 1, \\ 2\delta^{-1}\mathfrak{p}^2 & \text{if } t = 3, \\ \mathfrak{p}^2 & \text{if } t \in 2\mathbf{Z}, \mathfrak{d} = \mathfrak{r}, \text{ and } Q(\varphi) \not\cong M_2(F), \\ N_{K/F}(\mathfrak{d}) & \text{otherwise,} \end{cases}$$

where  $\mathfrak{r}$  is the maximal order in  $K$ ,  $\mathfrak{d}$  is the different of  $K$  relative to  $F$ , and  $\delta$  is an element of  $\delta_0(\varphi)$  such that  $\mathfrak{p} \subset \delta\mathfrak{g} \subset \mathfrak{g}$ .

As for  $\mu(L)$  and  $\mu(\tilde{L})$ , we have

$$(29.8) \quad \mu(L) = \begin{cases} \delta\mathfrak{g} & \text{if } n = 1, \\ \mathfrak{p} & \text{if } n = t = 2, \mathfrak{d} = \mathfrak{r}, \text{ and } Q(\varphi) \not\cong M_2(F), \\ \mathfrak{g} & \text{otherwise,} \end{cases}$$

$$(29.9) \quad \mu(\tilde{L})^{-1} = \begin{cases} 4\delta\mathfrak{g} & \text{if } t = 1, \\ 4\delta\mathfrak{g} \cap \mathfrak{p} & \text{if } t = 3, \\ \mathfrak{p} & \text{if } t \in 2\mathbf{Z}, \mathfrak{d} = \mathfrak{r}, \text{ and } Q(\varphi) \not\cong M_2(F), \\ N_{K/F}(\mathfrak{d}) & \text{otherwise.} \end{cases}$$

We have already determined  $\mu(M)$  and  $\mu(\tilde{M})$ . Thus (29.8) is easy. As for (29.9), we see that  $\mathfrak{g} \subset \mu(\tilde{M})$ , and so (29.6) shows that  $\mu(\tilde{L}) = \mu(\tilde{M})$ . Therefore we obtain (29.9).

**Lemma 29.11.** *Let  $L$  be a maximal lattice in  $V$ . If  $\varphi$  is isotropic,  $L$  has a  $\mathfrak{g}$ -basis  $\{u_i\}$  such that  $\varphi[u_i] = 0$  for every  $i$ .*

PROOF. Take an expression  $L = \sum_{i=1}^r (\mathfrak{g}x_i + \mathfrak{g}y_i) + M$  as in Lemma 29.8. Let  $A$  be a  $\mathfrak{g}$ -basis of  $M$  and let  $z \in A$ ; put  $c = \varphi[z]$  and  $w = x_1 - cy_1 + z$ . Then  $\varphi[w] = 0$ . Since  $c \in \mathfrak{g}$ , we have  $w \in L$ . Replacing  $z$  by  $w$ , we obtain our lemma.

**Theorem 29.12.** *Let  $L$  and  $M$  be maximal lattices in  $V$ . Then there exist a Witt decomposition  $V = \sum_{i=1}^r (Fx_i + Fy_i) + W$  and elements  $a_i, b_i$  of  $F$  such that*

$$\begin{aligned} L &= \sum_{i=1}^r (\mathfrak{g}x_i + \mathfrak{g}y_i) + N, & M &= \sum_{i=1}^r (\mathfrak{g}a_i x_i + \mathfrak{g}b_i y_i) + N, \\ N &= \{w \in W \mid \varphi[w] \in \mathfrak{g}\}, \\ a_1 b_1 &= \cdots = a_r b_r = 1, & \mathfrak{g}a_1 &\supset \cdots \supset \mathfrak{g}a_r \supset \mathfrak{g} \supset \mathfrak{g}b_r \supset \cdots \supset \mathfrak{g}b_1. \end{aligned}$$

PROOF. We prove this by induction on  $n$ . For anisotropic  $\varphi$  our assertion follows immediately from Lemma 29.7. Suppose that  $\varphi$  is isotropic. By Lemma 29.11 we can find a  $\mathfrak{g}$ -basis  $\{u_i\}$  of  $L$  such that  $\varphi[u_i] = 0$  for every  $i$ . Put  $\mathfrak{c}_i = \{a \in F \mid au_i \in M\}$ . We arrange the  $u_i$  so that  $\mathfrak{c}_1 \subset \mathfrak{c}_i$  for every  $i$ , write  $y_1$  for  $u_1$ , and put  $\mathfrak{c}_1 = \mathfrak{g}b_1$  with  $b_1 \in F$ . Then  $\{a \in F \mid aL \subset M\} = \mathfrak{g}b_1$  and  $\{a \in F \mid ay_1 \in L\} = \mathfrak{g}$ . Since  $\mu(L) = \mu(M) = \mathfrak{g}$ , we see that  $b_1 \in \mathfrak{g}$ . By

Lemma 22.3 we have a weak Witt decomposition  $V = Fx_1 + Fy_1 + U$ , and so, by Lemma 29.3,  $L = \mathfrak{a}x_1 + \mathfrak{a}^{-1}y_1 + (L \cap U)$  and  $M = \mathfrak{b}x_1 + \mathfrak{b}^{-1}y_1 + (M \cap U)$  with  $\mathfrak{g}$ -ideals  $\mathfrak{a}$  and  $\mathfrak{b}$ . Clearly  $\mathfrak{a} = \mathfrak{g}$  and  $\mathfrak{b}^{-1} = \mathfrak{g}b_1$ ; also  $L \cap U$  and  $M \cap U$  are maximal. If  $\varphi$  is anisotropic on  $U$ , our question is settled. Otherwise, applying our induction to  $L \cap U$  and  $M \cap U$ , we find a Witt decomposition  $U = \sum_{i=2}^r (Fx_i + Fy_i) + W$  and elements  $a_i, b_i$  of  $F$  such that  $a_i b_i = 1$ ,  $\mathfrak{g}b_2 \subset \cdots \subset \mathfrak{g}b_r \subset \mathfrak{g}$ ,  $L \cap U = \sum_{i=2}^r (\mathfrak{g}x_i + \mathfrak{g}y_i) + N$ , and  $M \cap U = \sum_{i=2}^r (\mathfrak{g}a_i x_i + \mathfrak{g}b_i y_i) + N$ , with  $N$  as in our theorem. Since  $b_1 L \subset M$ , we have  $b_1 y_2 \in M$ , and so  $b_1 \in \mathfrak{g}b_2$ . Therefore we obtain our theorem.

**Lemma 29.13.** *Let  $(V, \varphi)$  be defined over a global field  $F$ . Let  $L$  be a maximal lattice  $L$  in  $V$ ; define  $A(L)$  as in §29.4 and put*

$$C_v = \{\alpha \in SO_v^\varphi \mid L_v \alpha = L_v\} \quad \text{and} \quad X_v = A(L)_v^\times \cap G^+(V)_v$$

for  $v \in \mathbf{h}$ . Then  $\tau(X_v) \subset C_v$  for every  $v \in \mathbf{h}$  and  $\tau(X_v) = C_v$  for almost all  $v \in \mathbf{h}$ .

PROOF. Let  $x \in X_v$  with any  $v \in \mathbf{h}$ . Then  $L_v \tau(x) = x^{-1} L_v x \subset A(L)_v \cap V_v = L_v$  by Lemma 29.5. Since  $\det(\tau(x)) = 1$ , we have  $L_v \tau(x) = L_v$ , and so  $\tau(X_v) \subset C_v$ . Thus we have to prove that  $C_v \subset \tau(X_v)$  for almost all  $v \in \mathbf{h}$ . Suppose  $n$  is even; then for almost all  $v \in \mathbf{h}$ ,  $A(L)_v$  is a maximal order in  $A(V)_v$  and  $Q(\varphi)_v \cong M_2(F_v)$ . Thus  $A(V)_v \cong M_r(F_v)$  with  $r = 2^{n/2}$  for such a  $v$ . Let  $\alpha \in C_v$ . Then  $\alpha = \tau(z)$  with  $z \in G^+(V)_v$ , and so  $z^{-1} L_v z = L_v \alpha = L_v$ . We have therefore  $z^{-1} A(L)_v z = A(L)_v$ , and so  $z A(L)_v$  is a two-side ideal of  $A(L)_v$ . By Lemma 21.4,  $M_r(\mathfrak{g}_v)$  is a maximal order in  $A(V)_v$ , and by Lemma 21.19,  $A(L)_v$  is conjugate to  $M_r(\mathfrak{g}_v)$ . Therefore, by Lemma 21.20,  $z A(L)_v = c A(L)_v$  with  $c \in F_v^\times$ . Put  $w = c^{-1} z$ . Then  $w \in X_v$  and  $\tau(w) = \alpha$ , which proves the case of even  $n$ . Suppose  $n$  is odd; then for almost all  $v \in \mathbf{h}$ ,  $A^+(L)_v$  is a maximal order in  $A^+(V)_v$  and  $Q(\varphi)_v \cong M_2(F_v)$ , and so  $A^+(V)_v \cong M_s(F_v)$  with  $s = 2^{(n-1)/2}$ . Let  $\tau(z) = \alpha \in C_v$  with  $z \in G^+(V)_v$ . Then we have  $z^{-1} A^+(L)_v z = A^+(L)_v$ , and so looking at  $z A^+(L)_v$  instead of  $z A(L)_v$ , we obtain our assertion for odd  $n$ .

The rest of this section is devoted to the proof of the fact stated in the remark after Theorem 27.2. We first prove two theorems that are special cases of Theorems 27.7 and 27.3(ii), in order to make our exposition self-contained when the base field is  $\mathbf{Q}$ .

**Theorem 29.14.** *Let  $B$  and  $C$  be quaternion algebras over  $\mathbf{Q}$ . If  $B_v \cong C_v$  for every  $v \in \mathbf{v}$ , then  $B \cong C$ .*

PROOF. Put  $(V, \varphi) = (B^\circ, \beta^\circ) \oplus (C^\circ, -\gamma^\circ)$ , assuming that  $B_v \cong C_v$  for every  $v \in \mathbf{v}$ . By (25.8),  $(B^\circ, \beta^\circ)_v \cong (C^\circ, \gamma^\circ)_v$  for every  $v \in \mathbf{v}$ , and so we see that  $(V, \varphi)_v$  has a split Witt decomposition for every  $v \in \mathbf{v}$ . Let  $L$  be a

maximal lattice in  $V$  and  $\Phi$  the matrix representing  $\varphi$  with respect to a  $\mathbf{Z}$ -basis of  $L$ . Then  $L_p^\varphi = 2\tilde{L}_p = 2L_p$  for every prime number  $p$ ; see (29.6). Thus  $\det(\Phi)\mathbf{Z} = [L^\varphi/L] = 2^{-6}\mathbf{Z}$ . Since  $\Phi$  has 3 positive and 3 negative eigenvalues, we have  $\det(\Phi) = -2^{-6}$ .

Suppose we could prove that  $\varphi$  is isotropic. Then we have a weak Witt decomposition  $V = \mathbf{Q}e + \mathbf{Q}f + Y$ . If  $\eta$  is the restriction of  $\varphi$  to  $Y$ , then we easily see that  $1 \in \delta_0(\eta)$ , and so by Theorem 25.4,  $(Y, \eta) \cong (A, d\alpha)$  with  $d \in \mathbf{Q}^\times$  and a quaternion algebra  $A$  over  $\mathbf{Q}$ , where  $\alpha$  is the norm form of  $A$ . Since  $V_v$  has a split Witt decomposition for every  $v \in \mathbf{v}$ . The same is true for  $Y_v$  in view of Witt's theorem. Thus  $\varepsilon_v(A) = 1$  for every  $v \in \mathbf{v}$ , and so  $A \cong M_2(\mathbf{Q})$  by Theorem 26.6(ii). Therefore  $V$  has a split Witt decomposition over  $\mathbf{Q}$ . This means that

$$(B^\circ, \beta^\circ) \oplus (C^\circ, -\gamma^\circ) = (V, \varphi) \cong (C^\circ, \gamma^\circ) \oplus (C^\circ, -\gamma^\circ),$$

and so by Witt's theorem,  $(B^\circ, \beta^\circ) \cong (C^\circ, \gamma^\circ)$ . Thus by (25.8),  $B \cong C$  as desired. Therefore our aim is to show that  $\varphi$  is isotropic.

Now applying Lemma 25.8 to  $L$  and  $\Phi$ , we find a nonzero element  $y$  of  $L$  such that  $|\varphi[y]| \leq 3/2$ . Since  $\varphi[L] \subset \mathbf{Z}$ , we have  $\varphi[y] = 0$  or  $\pm 1$ . The matter is settled if  $\varphi[y] = 0$ , and so we assume that  $\varphi[y] = \pm 1$ . Let  $U = (\mathbf{Q}y)^\perp$  and let  $\psi$  be the restriction of  $\varphi$  to  $U$ . Clearly  $-\varphi[y] \in \delta_0(\psi)$ . By Lemma 22.5(iii),  $U_p$  has core dimension 1 for every  $p$ . Let  $M$  be a maximal lattice in  $U$ . By (29.7),  $[M_p^\psi/M_p] = [2\tilde{M}_p/M_p] = 2^{-4}\mathbf{Z}_p$  for every  $p$ . Thus if  $\Psi$  is the matrix representing  $\psi$  on  $M$ , then  $|\det(\Psi)| = 2^{-4}$ . By Lemma 25.8,  $M$  contains a nonzero element  $z$  such that  $|\psi[z]| \leq 3 \cdot 2^{-4/5} < 2$ . Therefore  $\psi[z] = 0$  or  $\pm 1$ . So we assume that  $\psi[z] = \pm 1$  for the same reason as before. If  $\psi[z] = -\varphi[y]$ , then  $\varphi[y+z] = 0$  and  $y+z \neq 0$ , and so  $\varphi$  is isotropic. Thus we consider only the case  $\varphi[y] = \varphi[z] = 1$  or  $\varphi[y] = \varphi[z] = -1$ .

Let  $X = (\mathbf{Q}y + \mathbf{Q}z)^\perp$  and let  $N$  be a maximal lattice in  $X$ ; let  $\Xi$  be the matrix representing  $\varphi$  on  $N$ . Then  $\Xi$  as a real symmetric matrix is equivalent to  $\pm \text{diag}[1_3, -1]$  and  $-1 \in \delta_0(\Xi)$ , and so  $\mathbf{Q}(\sqrt{-1})$  is the discriminant field of  $\Xi$ . By Lemma 22.5(iii) the core dimension of  $X_p$  is 0 or 2 for every  $p$ . For  $p$  odd and  $x \in L_p$  we have  $\varphi(x, L_p) \subset \mathbf{Z}_p$ , and so we see that  $x - \varphi[y]\varphi(x, y)y - \varphi[z]\varphi(x, z)z \in L_p \cap U_p$ . This shows that  $L_p = \mathbf{Z}_p y + \mathbf{Z}_p z + N'_p$  with  $N'_p = L_p \cap U_p$ . Clearly  $N'_p$  is maximal, and so  $\det(\Xi)\mathbf{Z}_p = [2\tilde{N}_p/N_p] = [2\tilde{N}'_p/N'_p] = \mathbf{Z}_p$  for odd  $p$ . If  $p = 2$ , from (29.7) we see that  $\det(\Xi)\mathbf{Z}_2 = [2\tilde{N}_2/N_2] = 2^{-2}\mathbf{Z}_2$ . Thus  $\det(\Xi) = -2^{-2}$ . By Lemma 25.8,  $N$  has a nonzero element  $w$  such that  $|\varphi[w]| \leq 3 \cdot 2^{-1/2} < 3$ . Thus  $|\varphi[w]|$  is 0, 1, or 2. We are interested only in nonzero values of  $\varphi[w]$ . Also, replacing  $\varphi$  by  $-\varphi$  if necessary, we may assume that  $\varphi[y] = \varphi[z] = 1$ . If  $\varphi[w] = -1$ , then  $\varphi[y+w] = 0$ ; if  $\varphi[w] = -2$ , then  $\varphi[y+z+w] = 0$ . Thus we may assume that  $\varphi[w]$  is 1 or 2. Let  $S = \mathbf{Q}y + \mathbf{Q}z + \mathbf{Q}w$  and  $T = S^\perp$ . Let  $H$  be a maximal lattice in  $T$  and

let  $\tau$  be the matrix representing  $\varphi$  on  $H$ .

First suppose  $\varphi[w] = 1$ ; then  $1 \in \delta_0(\tau)$ . From (29.7) we see that  $[H^\tau/H]_p = \mathbf{Z}_p$  for odd  $p$  and  $[H^\tau/H]_2$  is  $\mathbf{Z}_2$  or  $2^{-2}\mathbf{Z}_2$ . Thus  $|\det(\tau)| \leq 1$ . By Lemma 25.8,  $H$  has a nonzero element  $x$  such that  $|\varphi[x]| \leq 3$ . Since  $\varphi$  is negative definite on  $T$ , we have  $0 \leq -\varphi[x] \leq 3$ . The case  $\varphi[x] = 0$  gives the desired conclusion, and so we assume  $1 \leq -\varphi[x] \leq 3$ . We can easily find an element  $u \in S$  such that  $\varphi[u] = -\varphi[x]$ . Then  $\varphi[u+x] = 0$ , which settles the problem.

Next suppose  $\varphi[w] = 2$ ; then  $2 \in \delta_0(\tau)$ . From (29.7) we see that  $[H^\tau/H]_p = 2^{-1}\mathbf{Z}_p$  for every  $p$ . Thus  $|\det(\tau)| = 2^{-1}$ . By Lemma 25.8,  $H$  has a nonzero element  $x$  such that  $|\varphi[x]| \leq 3 \cdot 2^{-1/3} < 3$ . Thus  $0 \leq -\varphi[x] \leq 2$  and we can settle the matter in the same manner as in the case  $\varphi[w] = 1$ . This completes the proof.

**Theorem 29.15.** *Let  $B$  be a quaternion algebra over  $\mathbf{Q}$  and  $P = \{v \in \mathbf{h} \mid \varepsilon_v(B) = -1\}$ . Given  $c \in \mathbf{Q}^\times$ , equation  $-\beta^\circ[x] = c$  has a solution in  $B^\circ$  if it has a solution in  $B_v^\circ$  for every  $v \in P$ .*

PROOF. Clearly we may assume that  $c$  is a square-free positive or negative integer. Since the problem is trivial if  $B \cong M_2(\mathbf{Q})$ , we assume that  $B$  is a division algebra, and so  $P \neq \emptyset$  by Theorem 26.6. Put  $\delta_\infty = \varepsilon_\infty(B)$ . We assume that  $-\beta^\circ[x] = c$  has a solution in  $B_v^\circ$  for every  $v \in P$ . Since  $-\beta^\circ[x] = x^2$ , from Theorem 25.4(iii) we obtain

$$(*) \quad c \notin \mathbf{Q}_v^{\times 2} \text{ for every } v \in P.$$

In particular,  $c < 0$  if  $\delta_\infty = -1$ ; also,  $c - 1 \notin 8\mathbf{Z}$  if  $2 \in P$ .

Now, we have prime numbers  $p_1, \dots, p_r$  such that  $P = \{p_1, \dots, p_r\}$  if  $\delta_\infty = 1$  and  $P = \{p_1, \dots, p_r, \infty\}$  if  $\delta_\infty = -1$ . Put  $p_1 \cdots p_r = de$  with square-free positive integers  $d$  and  $e$  such that  $d|c$  and  $e$  is prime to  $c$ . Put also  $K = \mathbf{Q}(\sqrt{\delta_\infty eq})$  and  $C = \{K, c\}$  with a prime number  $q$  that does not divide  $2ce$ . We easily see that  $C_\infty \cong \mathbf{H}$  if and only if  $\delta_\infty = -1$ . We choose  $q$  so that  $\varepsilon_p(C_p) = -1$  for a prime number  $p$  if and only if  $p \in P$ . We do this by imposing the following conditions on  $q$ :

$$\begin{aligned} \left( \frac{\delta_\infty eq}{p} \right) &= -1 \quad \text{if } p|d \text{ and } p \neq 2, \\ \delta_\infty eq - 5 &\in 8\mathbf{Z} \quad \text{if } 2|d, \\ \delta_\infty eq - 1 &\in p\mathbf{Z} \quad \text{if } p|c \text{ and } p \nmid 2de, \\ \delta_\infty eq - 1 &\in 8\mathbf{Z} \quad \text{if } 2 \nmid de, \\ \delta_\infty eq + 2 &\in 16\mathbf{Z} \quad \text{if } 2|e \text{ and } c+1 \in 8\mathbf{Z}, \\ \delta_\infty eq - 2 &\in 16\mathbf{Z} \quad \text{if } 2|e \text{ and } c \pm 3 \in 8\mathbf{Z}. \end{aligned}$$

Such a  $q$  exists by virtue of Dirichlet's theorem concerning the prime numbers in an arithmetic progression. From the first two conditions we see that  $K_p$  is

an unramified quadratic extension of  $\mathbf{Q}_p$  and  $c$  is a prime element of  $\mathbf{Q}_p$  if  $p|d$ , and so  $\varepsilon_p(C) = -1$ . If  $p|e$  and  $p \neq 2$ , then from (9.2), (9.3), and (\*) we see that  $c \notin N_{K_p/\mathbf{Q}_p}(K_p^\times)$ . The same is true for  $p = 2$  if  $2|e$ , as can be seen from the last two conditions and the fact about  $\mathbf{Q}_2(\sqrt{\pm 2})$  stated in the table below (9.3). (As already noted,  $c - 1 \notin 8\mathbf{Z}$  if  $2 \in P$ .) Thus  $\varepsilon_p(C) = -1$  if  $p|e$ . Let  $p$  be a prime number that does not divide  $2qde$ . Then  $p$  is unramified in  $K$ , and  $p$  splits in  $K$  if  $p|c$ . Thus  $\varepsilon_p(C) = 1$  if  $p \nmid 2qde$ . If  $2 \nmid de$ , from the fourth condition we see that  $\varepsilon_2(C) = 1$ . We thus find that  $\varepsilon_v(C) = \varepsilon_v(B)$  for every  $v \neq q$ . Then by Theorem 26.6(i) we obtain  $\varepsilon_q(C) = \varepsilon_q(B)$ . By Theorem 29.14, we have  $B \cong C$ . Since  $C = \{K, c\}$ , we have  $c = z^2$  with  $z \in C^\circ$ . Therefore  $c = w^2 = -\beta_0[w]$  with  $w \in B^\circ$ . This proves our theorem.

**29.16.** Returning to the question stated in the remark after Theorem 27.2, we take a nondegenerate quadratic space  $(V, \varphi)$  over  $\mathbf{Q}$  of dimension 4 such that  $(V, \varphi)_v$  is isotropic for every  $v \in \mathbf{v}$ . Our task is to show that  $(V, \varphi)$  itself is isotropic. Take any  $\xi \in V$  such that  $\varphi[\xi] \neq 0$ , put  $W = (\mathbf{Q}\xi)^\perp$ , and denote by  $\psi$  the restriction of  $\varphi$  to  $W$ . By Lemma 25.2(ii),  $(W, \psi) \cong (B^\circ, c\beta^\circ)$  with  $c \in \mathbf{Q}^\times$  and a quaternion algebra  $B$  over  $\mathbf{Q}$ . Put  $P = \{v \in \mathbf{v} \mid \varepsilon_v(B) = -1\}$ . If  $v \notin P$ , then  $(B^\circ, \beta^\circ)_v$  is isotropic and we can find  $y_v \in B_v^\circ$  such that  $c\beta^\circ[y_v] = -\varphi[\xi]$ . Suppose  $v \in P$ ; since  $(V, \varphi)_v$  is isotropic, we can find  $a_v \in \mathbf{Q}_v$  and  $z_v \in B_v^\circ$  such that  $a_v\xi + z_v \neq 0$  and  $\varphi[a_v\xi + z_v] = 0$ . If  $a_v = 0$ , then  $z_v \neq 0$  and  $\beta^\circ[z_v] = 0$ , a contradiction, since  $\varepsilon_v(B) = -1$ . Thus  $a_v \neq 0$  and  $c\beta^\circ[a_v^{-1}z_v] = -\varphi[\xi]$ . This means that the equation  $c\beta^\circ[x] = -\varphi[\xi]$  has a solution  $x$  in  $B_v^\circ$  for every  $v \in \mathbf{v}$ . Therefore by Theorem 29.15 it has a solution in  $B^\circ$ , which means that  $(V, \varphi)$  is isotropic as expected.

### 30. The genus and class of a lattice and a matrix

**30.1.** Let  $(V, \varphi)$  be a nondegenerate quadratic space over a global field  $F$ . Then we can define the orthogonal and special orthogonal groups  $O(\varphi)$  and  $SO(\varphi)$ , and also  $O(\varphi_v)$  and  $SO(\varphi_v)$  for each  $v \in \mathbf{v}$ . The latter groups act on  $V_v$ . To simplify our exposition, we let  $G$  denote either  $O(\varphi)$  or  $SO(\varphi)$ , and  $G_v$  the group  $O(\varphi_v)$  or  $SO(\varphi_v)$ . Given a  $\mathfrak{g}$ -lattice  $L$  in  $V$ , by the **class** of  $L$  with respect to  $G$  (or the  **$G$ -class** of  $L$ ) we mean the set of all lattices of the form  $L\alpha$  with  $\alpha \in G$ . Next, by the **genus** of  $L$  with respect to  $G$  (or the  **$G$ -genus** of  $L$ ) we mean the set of all lattices  $M$  in  $V$  such that  $M_v = L_v\alpha_v$  with some  $\alpha_v \in G_v$  for every  $v \in \mathbf{h}$ . These definitions of  $G$ -class and  $G$ -genus are applicable to any algebraic subgroup  $G$  of  $GL_F(V)$  for which  $G_v$  is well defined. For instance, if  $G = GL_F(V)$ , then  $G_v = GL_{F_v}(V_v)$ .

In view of Lemma 29.6 we see that the  $O(\varphi)$ -genus of a lattice  $L$  is the  $SO(\varphi)$ -genus of  $L$ . Therefore we call it the  **$\varphi$ -genus** of  $L$ . Also, Lemmas 29.2(5) and 29.9 show that *all the maximal lattices in  $V$  form a single  $\varphi$ -*



*genus*. The principal purpose of this section is to prove that the  $\varphi$ -genus of any fixed  $\mathfrak{g}$ -lattice consists of a finite number of classes with respect to  $SO(\varphi)$ .

We first note a few formulas about the discriminant ideal of a lattice  $L$  defined in (29.3c). If  $F$  is local, we have clearly  $d(L) = \det [\varphi(x_i, x_j)]_{i,j=1}^n \mathfrak{g}$  for every  $\mathfrak{g}$ -basis  $\{x_i\}_{i=1}^n$  of  $L$ . If  $F$  is global, then by Theorem 10.19, we can find an  $F$ -basis  $\{e_i\}_{i=1}^n$  of  $V$  and  $\mathfrak{g}$ -ideals  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  such that  $L = \sum_{i=1}^n \mathfrak{a}_i e_i$ . Then we have

$$(30.1) \quad d(L) = \det [\varphi(e_i, e_j)]_{i,j=1}^n \mathfrak{a}_1^2 \cdots \mathfrak{a}_n^2.$$

Indeed, if we take this to be a new definition of  $d(L)$ , then clearly  $d(L)_v = d(L_v)$  for every  $v \in \mathbf{h}$ , and so it must coincide with the previous  $d(L)$ . We note two more easy facts on  $d(L)$ :

$$(30.2) \quad d(L) \subset \mu_0(L)^n \quad \text{if } n = \dim(V),$$

$$(30.3) \quad d(M) = [L/M]^2 d(L),$$

where  $[L/M]$  is as in §21.25. The first fact is obvious. As for (30.3), it is sufficient to prove it in the local case. If  $F$  is local, we can take  $\alpha \in GL_F(V)$  so that  $M = L\alpha$ . Then  $d(M) = \det(\alpha)^2 d(L)$  and  $[L/M] = \det(\alpha)\mathfrak{g}$ , from which we obtain (30.3).

**Lemma 30.2.** *Given a global field  $F$ , there is a constant  $B$  depending only on  $F$  with the following property: given  $\alpha \in GL_m(F)$  such that  $\det(\alpha) \in \mathfrak{g}^\times$ , there exists a nonzero vector  $\xi \in \mathfrak{g}_m^1$  such that  $|(\xi\alpha)_i|_v \leq B$  for every  $i \leq m$  and every  $v \in \mathbf{a}$ , where  $(\xi\alpha)_i$  is the  $i$ -th coordinate of  $\xi\alpha$ .*

PROOF. Let  $X = (F_{\mathbf{a}})_m^1$  and  $d = [F : \mathbf{Q}]$ . For a positive number  $b$  let  $Y_b$  denote the set of all  $x \in X$  such that  $|(x\alpha)_i|_v \leq b$  for every  $i$  and every  $v \in \mathbf{a}$ . Since  $\det(\alpha) \in \mathfrak{g}^\times$ , we have  $|N_{F/\mathbf{Q}}(\det(\alpha))| = 1$ , and so  $\text{vol}(Y_b) = 2^{mr}\pi^{ms}b^{md}$ , where  $r$  resp.  $s$  is the number of real resp. imaginary primes of  $F$ . By Theorem 12.5(i), if  $\text{vol}(Y_b) > 2^{md}\text{vol}(X/\mathfrak{g}_m^1)$ , then  $Y_b \cap \mathfrak{g}_m^1$  contains a nonzero element. Taking  $B$  so that  $2^r\pi^s B^d > 2^d\text{vol}(F_{\mathbf{a}}/\mathfrak{g})$ , we obtain our lemma.

**Lemma 30.3.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over a global field  $F$ , and  $\mathfrak{r}$  an integral ideal in  $F$ . Then there exists a finite subset  $S$  of  $F^\times$  such that  $\varphi[L] \cap S \neq \emptyset$  for every  $\mathfrak{g}$ -lattice  $L$  such that  $\mu_0(L) \subset \mathfrak{g}$  and  $\mathfrak{r} \subset d(L)$ .*

PROOF. By (30.2) we have  $\mathfrak{r} \subset d(L) \subset \mu_0(L) \subset \mathfrak{g}$  for such an  $L$ . There are only finitely many ideals  $\mathfrak{a}$  such that  $\mathfrak{r} \subset \mathfrak{a} \subset \mathfrak{g}$ , and so we can replace the condition  $\mathfrak{r} \subset d(L)$  by  $\mathfrak{r} = d(L)$ . Suppose  $d(L) = \mathfrak{r}$  and  $\mu_0(L) \subset \mathfrak{g}$ ; then we can find a maximal lattice  $L_1$  containing  $L$ . By (30.3),  $\mathfrak{r} = [L_1/L]^2 d(L_1)$ .

We first assume that  $\varphi$  is isotropic. Since  $d(L)$  depends only on the  $\varphi$ -genus of  $L$  and all the maximal lattices form a single  $\varphi$ -genus, we see that  $d(L_1)$  is determined independently of the choice of  $L_1$ . We are going to prove:

(30.4) *There is an element of  $F^\times$  that is contained in  $\varphi[M]$  for every maximal lattice  $M$  in  $V$ .*

Suppose this is so; let  $z$  be that element of  $F^\times$ . In the above setting  $d(L_1)^{-1}\mathfrak{r}$  is the square of an integral ideal  $[L_1/L]$ . Pick and fix a nonzero element  $c$  in  $[L_1/L]$ . By (21.3f),  $cL_1 \subset L$ , and so  $c^2z \in \varphi[L]$ . Since  $[L_1/L]$  is determined by  $\mathfrak{r}$ , our problem can be reduced to (30.4).

Since  $\varphi$  is isotropic, by Lemma 22.3 we can find a weak Witt decomposition  $V = Fx + Fy + W$  with elements  $x, y$  such that  $\varphi[x] = \varphi[y] = 0$  and  $2\varphi(x, y) = 1$ . Let  $M$  be a maximal lattice in  $V$ . By Lemma 29.3,  $M = \mathfrak{a}x + \mathfrak{a}^{-1}y + (M \cap W)$  with a  $\mathfrak{g}$ -ideal  $\mathfrak{a}$ . Let  $\{\mathfrak{a}_1, \dots, \mathfrak{a}_h\}$  be a set of ideals that represents the ideal class group of  $F$ . Replacing  $x$  and  $y$  by their suitable scalar multiples, we may assume that  $\mathfrak{a} = \mathfrak{a}_i$  for some  $i$ . Take a nonzero element  $g$  in  $\bigcap_{i=1}^h (\mathfrak{a}_i \cap \mathfrak{a}_i^{-1})$ . Then  $g^2 = \varphi[gx + gy] \in \varphi[M]$ , which proves (30.4).

Next we assume that  $\varphi$  is anisotropic. Let  $L$  be a lattice in  $V$  such that  $d(L) = \mathfrak{r}$  and  $\mu_0(L) \subset \mathfrak{g}$ . By Theorem 10.19 we can put  $L = \mathfrak{b}x_1 + \mathfrak{g}x_2 + \dots + \mathfrak{g}x_n$  with an  $F$ -basis  $\{x_i\}_{i=1}^n$  of  $V$  and a  $\mathfrak{g}$ -ideal  $\mathfrak{b}$ . Replacing  $x_1$  by its suitable scalar multiple, we may assume that  $\mathfrak{g} \subset \mathfrak{b}$ , and  $\mathfrak{b}$  belongs to a fixed finite set  $\mathfrak{B}$  of ideals that represents the ideal class group of  $F$ . Let  $\mathcal{L}(\mathfrak{b})$  denote the set of all lattices  $L$  of this type such that  $d(L) = \mathfrak{r}$  and  $\mu_0(L) \subset \mathfrak{g}$ . For each  $\mathfrak{b} \in \mathfrak{B}$  we take and fix a member  $L_0$  of  $\mathcal{L}(\mathfrak{b})$ , written  $L_0 = \mathfrak{b}y_1 + \mathfrak{g}y_2 + \dots + \mathfrak{g}y_n$  with an  $F$ -basis  $\{y_i\}_{i=1}^n$  of  $V$ . For  $L$  as above define  $\alpha \in GL_F(V)$  by  $y_i\alpha = x_i$  for  $1 \leq i \leq n$ . Then  $L_0\alpha = L$ . Put  $y_i\alpha = \sum_{j=1}^n a_{ij}y_j$ . By (30.3),  $\mathfrak{r} = d(L) = \det(\alpha)^2 d(L_0) = \det(\alpha)^2 \mathfrak{r}$ , and so  $\det(a_{ij}) = \det(\alpha) \in \mathfrak{g}^\times$ . By Lemma 30.2 there exists a nonzero element  $\xi = (\xi_1, \dots, \xi_n)$  of  $\mathfrak{g}_n^1$  such that  $|\sum_{i=1}^n \xi_i a_{ij}|_v \leq B$  for every  $j$  and every  $v \in \mathfrak{a}$  with a constant  $B$  depending only on  $F$ . Put  $w = \sum_{i=1}^n \xi_i y_i$  and  $\eta_j = \sum_{i=1}^n \xi_i a_{ij}$ . Then  $w \in L_0$  and  $w\alpha = \sum_{j=1}^n \eta_j y_j \in L$ ,  $0 \neq \varphi[w\alpha] \in \mu_0(L) \subset \mathfrak{g}$ , and  $|\eta_j|_v \leq B$  for every  $j$  and every  $v \in \mathfrak{a}$ . Now  $\varphi[w\alpha] = \varphi(\sum_j \eta_j y_j, \sum_k \eta_k y_k) = \sum_{j,k} \eta_j \eta_k \varphi(y_j, y_k)$ , and so  $|\varphi[w\alpha]|_v \leq 2^{n^2} n^2 B^2 E$  for every  $v \in \mathfrak{a}$ , where  $E = \text{Max}_{j,k} |\varphi(y_j, y_k)|_v$ . (The factor  $2^{n^2}$  is necessary only if  $v$  is imaginary.) Take  $x \in F_{\mathbf{A}}^\times$  so that  $x\mathfrak{g} = \mathfrak{g}$  and  $|x|_v = 2^{n^2} n^2 B^2 E$  for every  $v \in \mathfrak{a}$ . Then  $\varphi[w\alpha]$  belongs to the set  $S(x)$  defined in (15.10). The set  $S(x)$  depends on the choice of  $L_0 \in \mathcal{L}(\mathfrak{b})$ . Put  $S_{\mathfrak{b}} = S(x)$  with any fixed choice of  $L_0$ . Since  $\varphi[w\alpha] \in \varphi[L] \cap S_{\mathfrak{b}}$ , we can take  $\bigcup_{\mathfrak{b} \in \mathfrak{B}} S_{\mathfrak{b}}$  as  $S$  of our lemma. Our proof is now complete.

**Theorem 30.4.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over a global field  $F$ . Given an integral  $\mathfrak{g}$ -ideal  $\mathfrak{r}$ , let  $\Lambda_V(\mathfrak{r})$  denote the set of all*

$\mathfrak{g}$ -lattices  $L$  in  $V$  such that  $\mathfrak{x} \subset d(L)$  and  $\mu_0(L) \subset \mathfrak{g}$ . Then there exists a finite number of  $\mathfrak{g}$ -lattices  $L_1, \dots, L_h$  in  $V$  such that every member of  $\Lambda_V(\mathfrak{x})$  is the image of  $L_i$  for some  $i$  under an element of  $SO(\varphi)$ .

PROOF. Since  $[O^\varphi : SO^\varphi] = 2$ , it is sufficient to prove our theorem with  $O^\varphi$  in place of  $SO^\varphi$ . Let  $n = \dim(V)$ . If  $n = 1$ , then we can put  $(V, \varphi) = \langle F, c \rangle$  with  $c \in F^\times$ . Thus  $L$  is a  $\mathfrak{g}$ -ideal and  $d(L) = cL^2$ , and so  $\Lambda_V(\mathfrak{x})$  consists of the  $\mathfrak{g}$ -ideals  $L$  such that  $\mathfrak{x} \subset cL^2 \subset \mathfrak{g}$ , and so the finiteness is obvious. Let us therefore prove the case  $n > 1$  by induction on  $n$ . Fixing  $\xi \in F^\times \cap \mathfrak{g}$ , denote by  $\Lambda_V(\mathfrak{x}, \xi)$  the subset of  $\Lambda_V(\mathfrak{x})$  consisting of all  $L \in \Lambda_V(\mathfrak{x})$  such that  $\xi \in \varphi[L]$ . In view of Lemma 30.3 it is sufficient to prove the finiteness of  $\Lambda_V(\mathfrak{x}, \xi)$  modulo  $O(\varphi)$ . (Replacing  $\xi$  by  $c^2\xi$  with a suitable  $c \in F^\times$ , we may assume that  $\xi \in \mathfrak{g}$ .) We may of course assume that  $\xi = \varphi[z]$  for some  $z \in V$ . Fixing such a  $z$ , put  $U = (Fz)^\perp$ . By the induction assumption, there exist lattices  $M_1, \dots, M_k$  in  $U$  such that  $\Lambda_U(\xi^{2n}\mathfrak{x})$  consists of the images of the  $M_i$  under  $O^\varphi(U)$ .

Let  $L \in \Lambda_V(\mathfrak{x}, \xi)$ . Then  $\xi = \varphi[w]$  with some  $w \in L$ . By Lemma 22.5(ii),  $z = w\gamma$  with some  $\gamma \in O^\varphi(V)$ . Then  $z \in L\gamma$ . Replacing  $L$  by  $L\gamma$ , we may assume that  $z \in L$ . Put  $N = \{\xi x - \varphi(x, z)z \mid x \in L\}$  and  $L' = \mathfrak{g}z + N$ . Then  $N$  is a lattice in  $U$  and  $L'$  is a lattice in  $V$ . For  $x \in L$  we see that  $\xi x \in N + \mathfrak{g}z = L'$ . Thus  $\xi L \subset L' \subset L$ , and so  $\xi^{2n}\mathfrak{x} \subset d(\xi L) \subset d(L') = \xi d(N) \subset d(N)$ . Also,  $\mu_0(N) \subset \mu_0(L) \subset \mathfrak{g}$ . Therefore  $N \in \Lambda_U(\xi^{2n}\mathfrak{x})$ , and so  $N\alpha = M_i$  for some  $\alpha \in O^\varphi(U)$  and some  $i$ . Extend  $\alpha$  to an element  $\beta$  of  $O^\varphi(V)$  by putting  $z\beta = z$ ; put also  $L_i = \mathfrak{g}z + M_i$  for  $1 \leq i \leq k$ . Then  $L_i = L'\beta \subset L\beta$ , and so  $\varphi(L\beta, L_i) \subset \varphi(L\beta, L\beta) \subset \mu_0(L) \subset \mathfrak{g}$ . Thus  $L_i \subset L\beta \subset 2\tilde{L}_i$ . There are only a finite number of lattices between  $L_i$  and  $2\tilde{L}_i$ . We have proved that  $L$  is the image of one of them under an element of  $O^\varphi(V)$ . This completes the proof.

**Corollary 30.5.** *With  $(V, \varphi)$  as in Theorem 30.4, let  $L$  be a  $\mathfrak{g}$ -lattice in  $V$ . Then the  $\varphi$ -genus of  $L$  consists of a finite number of  $SO(\varphi)$ -classes.*

PROOF. As we already noted,  $d(L)$  and  $\mu_0(L)$  depend only on the  $\varphi$ -genus of  $L$ . Replacing  $L$  by  $cL$  with a suitable element  $c$  of  $F^\times$ , we may assume that  $\mu_0(L) \subset \mathfrak{g}$ . Then our assertion immediately follows from Theorem 30.4.

**30.6.** We now define the adelization of the orthogonal and special orthogonal groups. We begin with a finite-dimensional vector space  $V$  over  $F$  and  $GL(V)$ . We define the adelizations of  $V$  and  $GL(V)$ , written  $V_{\mathbf{A}}$  and  $GL(V)_{\mathbf{A}}$ , by

$$(30.5) \quad V_{\mathbf{A}} = \left\{ x \in \prod_{v \in \mathbf{V}} X_v \mid x_v \in L_v \text{ for almost all } v \in \mathbf{h} \right\},$$

$$(30.6) \quad GL(V)_{\mathbf{A}} = \left\{ \alpha \in \prod_{v \in \mathbf{V}} GL(V_v) \mid L_v \alpha_v = L_v \text{ for almost all } v \in \mathbf{h} \right\}.$$

Here  $L$  is an arbitrarily fixed  $\mathfrak{g}$ -lattice in  $V$ . In view of Lemma 21.6(i) these do not depend on the choice of  $L$ . Also  $V_{\mathbf{A}}$  is an additive group with respect to componentwise addition, and similarly  $GL(V)_{\mathbf{A}}$  is a group with respect to componentwise multiplication. We can view  $V$  (resp.  $GL(V)$ ) as a subset of  $V_{\mathbf{A}}$  (resp.  $GL(V)_{\mathbf{A}}$ ) by identifying each  $\alpha \in V$  resp.  $\alpha \in GL(V)$  with the element of  $V_{\mathbf{A}}$  resp.  $GL(V)_{\mathbf{A}}$  whose  $v$ -component is  $\alpha$  for every  $v$ . If  $V = F$ , then  $GL(V) = F^{\times}$ , and we see that  $F_{\mathbf{A}}$  and  $GL(V)_{\mathbf{A}}$  are exactly the adèle-ring and the idele-group of  $F$  defined in (15.2) and (15.3).

We easily see that  $V_{\mathbf{A}}$  has a natural structure of an  $F_{\mathbf{A}}$ -module. If  $V$  has a structure of an  $F$ -algebra, then  $V_{\mathbf{A}}$  becomes an associative ring with respect to componentwise multiplication. It is also easy to see that  $GL(V)_{\mathbf{A}}$  can be identified with all the  $F_{\mathbf{A}}$ -linear automorphisms of  $V_{\mathbf{A}}$ . If we identify  $V$  with  $F_n^1$  and  $GL(V)$  with  $GL_n(F)$ , then we naturally obtain  $GL_n(F)_{\mathbf{A}}$ , which can be identified with  $GL_n(F_{\mathbf{A}})$ . We put

$$(30.7) \quad V_{\mathbf{a}} = \prod_{v \in \mathbf{a}} V_v, \quad V_{\mathbf{h}} = \{x \in V_{\mathbf{A}} \mid x_v = 0 \text{ for every } v \in \mathbf{a}\},$$

$$(30.8) \quad GL_n(F)_{\mathbf{a}} = \prod_{v \in \mathbf{a}} GL_n(F_v),$$

$$(30.9) \quad GL_n(F)_{\mathbf{h}} = \{\alpha \in GL_n(F)_{\mathbf{A}} \mid \alpha_v = 1 \text{ for every } v \in \mathbf{a}\}.$$

To make our formulas short, for a  $\mathfrak{g}$ -ideal  $\mathbf{a}$  and an element  $x = (x_v) \in \prod_{v \in \mathbf{v}} (F_v)_n^m$  we write

$$(30.10) \quad x \prec \mathbf{a} \quad \text{if} \quad x_v \in (\mathbf{a}_v)_n^m \quad \text{for every } v \in \mathbf{h}.$$

**30.7.** Given a  $\mathfrak{g}$ -lattice  $L$  in  $V$  and an element  $\alpha \in GL(V)_{\mathbf{A}}$ , we denote by  $L\alpha$  the  $\mathfrak{g}$ -lattice such that  $(L\alpha)_v = L_v\alpha_v$  for every  $v \in \mathbf{h}$ . Such a  $\mathfrak{g}$ -lattice is guaranteed by Lemma 21.6(ii). In particular, for a  $\mathfrak{g}$ -ideal  $\mathfrak{r}$  and  $t \in F_{\mathbf{A}}^{\times}$  we can define a  $\mathfrak{g}$ -ideal  $t\mathfrak{r}$  so that  $(t\mathfrak{r})_v = t_v\mathfrak{r}_v$  for every  $v \in \mathbf{h}$ . (This was already defined in §15.5.) When  $\alpha \in GL(V)$  and  $t \in F^{\times}$ , these symbols  $L\alpha$  and  $t\mathfrak{r}$  are consistent with what we already have.

Now, given an algebraic subgroup  $G$  of  $GL(V)$  (or  $GL_n(F)$ ) for which  $G_v$  is defined, we define the adelization  $G_{\mathbf{A}}$  of  $G$  by

$$(30.11) \quad G_{\mathbf{A}} = GL(V)_{\mathbf{A}} \cap \prod_{v \in \mathbf{v}} G_v \\ = \left\{ x \in \prod_{v \in \mathbf{v}} G_v \mid L_v x_v = L_v \text{ for almost all } v \in \mathbf{h} \right\},$$

where  $L$  is an arbitrarily fixed  $\mathfrak{g}$ -lattice in  $V$ . An algebraic subgroup  $G$  of  $GL_n(F)$ , roughly speaking, is a subgroup of  $GL_n(F)$  that is defined by polynomial equations for the matrix entries, but there is a technical problem of how to define  $G_v$  for each  $v \in \mathbf{v}$ , which is nontrivial. Therefore in this book we consider only the cases in which  $G_v$  can be defined in an obvious way.

In fact, we consider  $G_{\mathbf{A}}$  only for  $G = SL(V)$ ,  $O^\varphi(V)$ ,  $SO^\varphi(V)$ ,  $G^+(V)$ , and  $G^1(V)$ , and a few more groups such as the subgroup of  $GL_n(F)$  consisting of the upper triangular matrices. For more on this point, the reader is referred to [S97, Section 8].

Restricting the injection of  $GL(V)$  into  $GL(V)_{\mathbf{A}}$  to  $G$ , we can view  $G$  as a subgroup of  $G_{\mathbf{A}}$ . Also, for each  $v \in \mathbf{v}$  we can view  $G_v$  as a subgroup of  $G_{\mathbf{A}}$  by means of the standard injection  $G_v \rightarrow \prod_{v \in \mathbf{v}} G_v$ . We put

$$(30.12) \quad G_{\mathbf{a}} = \{x \in G_{\mathbf{A}} \mid x_v = 1 \text{ for every } v \in \mathbf{h}\},$$

$$(30.13) \quad G_{\mathbf{h}} = \{x \in G_{\mathbf{A}} \mid x_v = 1 \text{ for every } v \in \mathbf{a}\}.$$

Then  $G_{\mathbf{A}} = G_{\mathbf{a}}G_{\mathbf{h}}$  and  $G_{\mathbf{a}} = \prod_{v \in \mathbf{a}} G_v$ . For every  $x \in G_{\mathbf{A}}$  we can define uniquely  $x_{\mathbf{a}} \in G_{\mathbf{a}}$  and  $x_{\mathbf{h}} \in G_{\mathbf{h}}$  by  $x = x_{\mathbf{a}}x_{\mathbf{h}}$ .

To define a topology on  $G_{\mathbf{A}}$ , we first observe that  $M_n(F_v)$  for each  $v \in \mathbf{v}$  has a natural topology. Since  $F_v$  is locally compact,  $M_n(F_v)$  is a locally compact additive group, and its subset  $GL_n(F_v)$  has a natural structure of a locally compact topological group. Now  $x \mapsto \det(x)$  is a continuous map of  $M_n(\mathfrak{g}_v)$  into  $\mathfrak{g}_v$ , and  $GL_n(\mathfrak{g}_v)$  is the inverse image of  $\mathfrak{g}_v^\times$ . Since  $\mathfrak{g}_v^\times$  is open and compact in  $\mathfrak{g}_v$ ,  $GL_n(\mathfrak{g}_v)$  must be open and compact. Thus, for a  $\mathfrak{g}$ -lattice  $L$  in  $V$  and  $v \in \mathbf{h}$  the group  $\{y \in GL(V)_v \mid L_v y = L_v\}$  is an open and compact subgroup of  $GL(V)_v$ . If  $G$  is as above, then  $G_v$  is clearly a closed subgroup of  $GL(V)_v$ , and so it has a natural structure of a locally compact group. Now put

$$(30.14) \quad U = G_{\mathbf{a}} \prod_{v \in \mathbf{h}} U_v, \quad U_v = \{y \in G_v \mid L_v y = L_v\},$$

with a fixed  $\mathfrak{g}$ -lattice  $L$ . (If  $L = \mathfrak{g}_n^1$ , then  $U_v = G_v \cap GL_n(\mathfrak{g}_v)$ .) Clearly  $U = \{x \in G_{\mathbf{A}} \mid Lx = L\}$ , where  $Lx$  is defined at the beginning of this subsection; also  $U_v$  is an open compact subgroup of  $G_v$ . We then make  $U$  a topological group with respect to the product topology. Since  $\prod_{v \in \mathbf{h}} U_v$  is compact and  $G_{\mathbf{a}}$  is a locally compact group,  $U$  becomes a locally compact group. Now we define a topology on  $G_{\mathbf{A}}$  by taking  $U$  to be its open subgroup. In other words, a subset of  $G_{\mathbf{A}}$  is defined to be open if it is a union of sets of the form  $xB$  with  $x \in G_{\mathbf{A}}$  and open subsets  $B$  of  $U$ . We easily see that this topology does not depend on the choice of  $L$ , and  $G_{\mathbf{A}}$  becomes a locally compact topological group.

Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $F$  and  $L$  a  $\mathfrak{g}$ -lattice in  $V$ . Then the  $\varphi$ -genus of  $L$  is the set of all lattices of the form  $Lx$  with  $x \in O(\varphi)_{\mathbf{A}}$ . Therefore, if  $U = \{y \in O(\varphi)_{\mathbf{A}} \mid Ly = L\}$ , then the map  $x \mapsto Lx$  gives a bijection of  $U \backslash O(\varphi)_{\mathbf{A}}$  onto the set of all lattices in the  $\varphi$ -genus of  $L$ , and consequently each double coset of the double orbit space  $U \backslash O(\varphi)_{\mathbf{A}} / O(\varphi)$  determines an  $O(\varphi)$ -class in the  $\varphi$ -genus of  $L$ . Therefore the number of  $O(\varphi)$ -classes in the  $\varphi$ -genus of  $L$  is exactly  $\#(U \backslash O(\varphi)_{\mathbf{A}} / O(\varphi))$ ; similarly the num-

ber of  $SO(\varphi)$ -classes in the  $\varphi$ -genus of  $L$  is exactly  $\#(U' \backslash SO(\varphi)_{\mathbf{A}} / SO(\varphi))$ , where  $U' = U \cap SO(\varphi)_{\mathbf{A}}$ .

**Theorem 30.8.** *Given  $(V, \varphi)$  as above, let  $X$  be an open subgroup of  $SO(\varphi)_{\mathbf{A}}$  containing  $SO(\varphi)_{\mathbf{a}}$ . Then  $X \backslash SO(\varphi)_{\mathbf{A}} / SO(\varphi)$  is a finite set.*

PROOF. Put  $G = SO(\varphi)$  and  $D = \{x \in G_{\mathbf{A}} \mid Lx = L\}$  with a lattice  $L$  in  $V$ . Put also  $Y = X \cap D$ ,  $Y_v = Y \cap G_v$ , and  $D_v = D \cap G_v$  for  $v \in \mathbf{h}$ . Then  $Y$  is an open subgroup of  $G_{\mathbf{A}}$ , and so  $D_v = Y_v$  for almost all  $v$ . Thus  $[D : Y] = \prod_{v \in \mathbf{p}} [D_v : Y_v]$  with a finite subset  $\mathbf{p}$  of  $\mathbf{h}$ . Since  $D_v$  and  $Y_v$  are open and compact, we see that  $[D_v : Y_v] < \infty$ , and so  $[D : Y] < \infty$ . By Corollary 30.5 and the statement at the end of §30.7,  $D \backslash G_{\mathbf{A}} / G$  is a finite set, and consequently  $X \backslash G_{\mathbf{A}} / G$  is finite. This proves our theorem.

**Theorem 30.9.** (i) *Put  $G^1 = SL_n(F)$ . Then we have  $G_{\mathbf{A}}^1 = G^1 Y$  for every open subgroup  $Y$  of  $G_{\mathbf{A}}^1$  containing  $G_{\mathbf{a}}^1$ .*

(ii) *If  $G = GL_n(F)$  and  $D$  is an open subgroup of  $G_{\mathbf{A}}$  containing  $G_{\mathbf{a}}$ , then  $GD$  is a normal subgroup of  $G_{\mathbf{A}}$ , and for every  $y \in G_{\mathbf{A}}$  we have*

$$GyD = \{x \in G_{\mathbf{A}} \mid \det(y^{-1}x) \in F^{\times} \det(D)\}.$$

PROOF. Put  $L = \mathfrak{g}_n^1$  and  $U = \{y \in G_{\mathbf{A}}^1 \mid Ly = L\}$ . Then  $U = G_{\mathbf{a}}^1 \cdot \prod_{v \in \mathbf{h}} SL_n(\mathfrak{g}_v)$ . Let  $M = L\xi$  with  $\xi \in G_{\mathbf{A}}^1$ . Then  $[L/M]_v = [L_v/M_v] = \det(\xi_v)\mathfrak{g}_v = \mathfrak{g}_v$  for every  $v \in \mathbf{h}$ , and so  $[L/M] = \mathfrak{g}$ . By Theorem 10.19 we can put  $L = \mathfrak{a}e_1 + \sum_{i=2}^n \mathfrak{g}e_i$  and  $M = \mathfrak{b}f_1 + \sum_{i=2}^n \mathfrak{g}f_i$  with  $\mathfrak{g}$ -ideals  $\mathfrak{a}$ ,  $\mathfrak{b}$ , and  $F$ -bases  $\{e_i\}_{i=1}^n$  and  $\{f_i\}_{i=1}^n$  of  $F_n^1$ . Define  $\alpha \in GL_n(F)$  by  $e_i\alpha = f_i$  for every  $i$ . Then  $\mathfrak{g} = [L/M] = [L/L\alpha][L\alpha/M] = \det(\alpha)\mathfrak{a}^{-1}\mathfrak{b}$ , and so  $\mathfrak{b} = \det(\alpha)^{-1}\mathfrak{a}$ . Define  $\beta \in GL_n(F)$  by  $f_1\beta = \det(\alpha)^{-1}f_1$  and  $f_i\beta = f_i$  for  $i > 1$ . Then  $\det(\alpha\beta) = 1$ ,  $L\alpha\beta = M = L\xi$ , and so  $\xi(\alpha\beta)^{-1} \in U$ . This proves that  $G_{\mathbf{A}}^1 = UG^1$ . Given an integral ideal  $\mathfrak{a}$ , put  $A = \{x \in U \mid x - 1 \prec \mathfrak{a}\}$ , using the notation of (30.10). Given an open subgroup  $Y$  of  $G_{\mathbf{A}}^1$ , we can take  $\mathfrak{a}$  so that  $A \subset Y$ . Since  $G_{\mathbf{A}}^1 = G^1 U$ , it is sufficient to show that  $U \subset G^1 A$ . Let  $\alpha \in U$ . Then we can find an element  $\beta$  of  $M_n(\mathfrak{g})$  such that  $\beta - \alpha \prec \mathfrak{a}$ . Then  $\det(\beta) - 1 \in \mathfrak{a}$ . By Theorem 10.21, there exists an element  $\gamma$  of  $SL_n(\mathfrak{g})$  such that  $\gamma - \beta \prec \mathfrak{a}$ . Then  $\gamma - \alpha \prec \mathfrak{a}$ , and so  $\gamma^{-1}\alpha \in A$ . Thus  $\alpha \in G^1 A$ , which shows that  $U \subset G^1 A$ , and we obtain (i).

To prove (ii), suppose  $\det(y^{-1}x) = c \cdot \det(d)$  with  $c \in F^{\times}$  and  $d \in D$ . We can find  $\alpha \in G$  such that  $\det(\alpha) = c$ . Then  $y^{-1}\alpha^{-1}xd^{-1} \in G_{\mathbf{A}}^1$ . Taking  $G_{\mathbf{A}}^1 \cap yDy^{-1}$  as  $Y$  in (i), we obtain  $G_{\mathbf{A}}^1 \subset G^1 yDy^{-1} \subset GyDy^{-1}$ . Therefore  $x \in \alpha y G_{\mathbf{A}}^1 D = \alpha G_{\mathbf{A}}^1 yD \subset GyD$ . This proves the last equality of (ii). Taking  $y = 1$ , we easily see that  $GD$  is a normal subgroup of  $G_{\mathbf{A}}$ . This completes the proof.

In general we say that **strong approximation** holds in an algebraic group  $G$  of  $G_{\mathbf{A}}$  if  $G_{\mathbf{A}} = GX$  for every open subgroup  $X$  of  $G_{\mathbf{A}}$  containing  $G_{\mathbf{a}}$ . Thus

the above theorem says that strong approximation holds in  $SL_n(F)$ . This result is included in the theorem of Eichler in [E38] similar to Theorem 10.21 concerning  $A^\times$  for a central simple algebra over an algebraic number field, which is the origin of strong approximation.

**30.10.** We defined the genus and class of a *lattice* with respect to an orthogonal group. Since the genus and class of a quadratic form were traditionally defined in terms of *matrices*, let us now explain the relationship between these two kinds of definitions.

Given an integral domain  $R$ , we denote by  $S_n(R)$  the set of all symmetric elements of  $M_n(R)$  with nonzero determinant. We fix a nondegenerate quadratic space  $(V, \varphi)$  over a global field  $F$ , isomorphic to  $\langle F, \varphi_0 \rangle$  with  $\varphi_0 \in S_n(F)$ , so that  $O^\varphi(V)$  can be identified with  $O(\varphi_0)$  of (22.5). Put  $L = \mathfrak{g}_n^1$  and define several local and global groups as follows:

$$(30.15) \quad \Delta = \{\gamma \in GL_n(\mathfrak{g}) \mid \det(\gamma) = \pm 1\}, \quad \Delta^1 = SL_n(\mathfrak{g}),$$

$$(30.16) \quad \Delta_v = \{\gamma \in GL_n(\mathfrak{g}_v) \mid \det(\gamma) = \pm 1\}, \quad \Delta_v^1 = SL_n(\mathfrak{g}_v) \quad (v \in \mathbf{h}),$$

$$(30.17) \quad \Delta_v = GL_n(F_v) \quad (v \in \mathbf{a}).$$

Now we consider the set  $\Phi$  of all  $\psi \in S_n(F)$  such that  $\psi = \gamma_v \varphi_0 \cdot {}^t \gamma_v$  with  $\gamma_v \in \Delta_v$  for every  $v \in \mathbf{v}$ . This  $\Phi$  is called the **genus** of  $\varphi_0$ . Here we can take  $\Delta_v^1$  in place of  $\Delta_v$  if  $v \in \mathbf{h}$  without changing  $\Phi$ , because  $\Delta_v \cap O(\varphi_0)_v$  has an element of determinant  $-1$ ; see Lemma 29.6. For  $\psi \in \Phi$ , by the ***O*-class** resp. the ***SO*-class** of  $\psi$  we understand the set of  $\delta \psi \cdot {}^t \delta$  for all  $\delta \in \Delta$  resp.  $\delta \in \Delta^1$ . Given  $\psi \in \Phi$ , we have an element  $\gamma$  of  $\prod_{v \in \mathbf{v}} \Delta_v$  such that  $\psi = \gamma \varphi_0 \cdot {}^t \gamma$ . Then by Corollary 27.4,  $\psi = \alpha \varphi_0 \cdot {}^t \alpha$  with  $\alpha \in GL(V)$ . Clearly  $\det(\psi) = \det(\varphi_0)$ , and so  $\det(\alpha) = \pm 1$ . Thus we can take such an  $\alpha$  from  $SL(V)$ , as  $O(\varphi_0)$  has an element of determinant  $-1$ . We assign the lattice  $L\alpha$  to  $\psi$ . Then  $L\alpha$  belongs to the  $\varphi$ -genus of  $L$ . Indeed, put  $\varepsilon = \gamma^{-1}\alpha$ ; then  $\varepsilon \in O(\varphi_0)_{\mathbf{A}}$  and  $L\alpha = L\varepsilon$ , which shows the desired fact.

Let  $\psi' \in \Phi$ ; then  $\psi' = \beta \varphi_0 \cdot {}^t \beta$  with  $\beta \in GL(V)$ . Suppose  $\psi' = \sigma \psi \cdot {}^t \sigma$  with  $\sigma \in \Delta$ ; put  $\tau = \beta^{-1} \sigma \alpha$ . Then  $\tau \in O(\varphi_0)$  and  $(L\beta)\tau = L\alpha$ , that is,  $L\beta$  belongs to the  $O(\varphi_0)$ -class of  $L\alpha$ . This means that the  $O(\varphi_0)$ -class of  $L\alpha$  depends only on the  $O$ -class of  $\psi$ . We can take  $\alpha, \beta \in SL(V)$ , so that if  $\sigma \in \Delta^1$ , then  $\tau \in SO(\varphi_0)$ , and so the  $SO(\varphi_0)$ -class of  $L\alpha$  depends only on the  $SO$ -class of  $\psi$ .

Conversely, let  $M$  be a lattice belonging to the  $\varphi$ -genus of  $L$ . Then  $M = L\xi$  with  $\xi \in SO(\varphi_0)_{\mathbf{A}}$ . By Theorem 30.9 we can find an element  $\alpha \in SL(V)$  such that  $(\xi \alpha^{-1})_{\mathbf{h}} \in \prod_{v \in \mathbf{h}} \Delta_v^1$ . Put  $\gamma = \alpha \xi^{-1}$  and  $\psi = \alpha \varphi_0 \cdot {}^t \alpha$ . Then  $\psi \in \Phi$ , since  $\psi = \gamma_v \varphi_0 \cdot {}^t \gamma_v$  for every  $v \in \mathbf{v}$ , and  $M = L\alpha$ , which corresponds to  $\psi$ . Thus the correspondence  $\psi \mapsto L\alpha$  gives a surjection of  $\Phi$  onto the  $\varphi$ -genus of  $L$ .

Finally, given  $\psi = \alpha\varphi_0 \cdot {}^t\alpha \in \Phi$  and  $\psi' = \beta\varphi_0 \cdot {}^t\beta \in \Phi$  with  $\alpha, \beta \in SL(V)$ , suppose  $L\beta = L\alpha\eta$  with  $\eta \in O(\varphi_0)$ ; put  $\zeta = \alpha\eta\beta^{-1}$ . Then  $\zeta \in \Delta$  and  $\psi = \zeta\psi' \cdot {}^t\zeta$ , so that  $\psi'$  belongs to the  $O$ -class of  $\psi$ . If  $\eta \in SO(\varphi_0)$ , then  $\zeta \in \Delta^1$ , and so  $\psi'$  belongs to the  $SO$ -class of  $\psi$ . In this way we find a bijection of the set of  $O$ -classes of matrices onto the set of  $O(\varphi_0)$ -classes of lattices, and also a bijection with  $SO$ -classes instead of  $O$ -classes.

It should be noted that we can take  $GL_n(\mathfrak{g})$  and  $GL_n(\mathfrak{g}_v)$  in place of  $\Delta$  and  $\Delta_v$ . Indeed, define  $\Phi'$  to be the set of all  $\psi \in S_n(F)$  such that  $\psi = \gamma_v\varphi_0 \cdot {}^t\gamma_v$  with  $\gamma_v \in GL_n(\mathfrak{g}_v)$  for  $v \in \mathbf{h}$  and  $\gamma_v \in GL_n(F_v)$  for  $v \in \mathbf{a}$ . For such a  $\psi$  we have  $\psi = \alpha\varphi_0 \cdot {}^t\alpha$  with  $\alpha \in GL(V)$ . Then  $\det(\alpha) = \pm \det(\gamma_v)$  for every  $v \in \mathbf{h}$ , so that  $\det(\alpha) \in \mathfrak{g}^\times$ . Put  $\varepsilon = \text{diag}[\det(\alpha)^{-1}, 1_{n-1}]$  and  $\psi' = \varepsilon\psi \cdot {}^t\varepsilon$ . Then  $\varepsilon \in GL_n(\mathfrak{g})$ ,  $\varepsilon\gamma_v \in \Delta_v$  for every  $v \in \mathbf{h}$  and so  $\psi' \in \Phi$ . From this we see that

$$(30.18) \quad \Phi' = \{\delta\psi \cdot {}^t\delta \mid \psi \in \Phi, \delta \in GL_n(\mathfrak{g})\}, \quad \Phi = \{\psi \in \Phi' \mid \det(\psi) = \det(\varphi_0)\}.$$

Then we find that the set of  $O$ -classes in  $\Phi$  is a complete set of representatives for  $\Phi'$  modulo the equivalence under  $GL_n(\mathfrak{g})$ .

What we explained here is applicable only to the lattices  $L$  that are isomorphic to  $\mathfrak{g}_n^1$ . In general each isomorphism class of  $\mathfrak{g}$ -lattices as  $\mathfrak{g}$ -modules is determined by an ideal class of  $F$  as described in Theorem 10.19. Therefore the genus and class of a matrix must be formulated according to the choice of that ideal class. We can give a clear-cut formulation, but it is somewhat involved, and so for a detailed exposition, we refer the reader to Section 4 of [S06c].

### 31. Integer-valued quadratic forms

**31.1.** Let  $F$  be a local or global field and  $\mathfrak{g}$  its maximal order as in §§21.1 and 29.1, and  $(V, \varphi)$  a nondegenerate quadratic space over  $F$ . We put

$$(31.1) \quad T_n(\mathfrak{g}) = \{(c_{ij}) \in S_n(\mathfrak{g}) \mid c_{ii} \in 2\mathfrak{g} \text{ for every } i\},$$

where  $S_n(\mathfrak{g})$  is the set of symmetric elements of  $M_n(\mathfrak{g}) \cap GL_n(F)$ , as defined in §30.10. Assuming for the moment  $\mathfrak{g}$  to be a principal ideal domain (which is so if  $F$  is local), take a  $\mathfrak{g}$ -lattice  $L$  in  $V$ . Let  $\varphi_0$  be the matrix representing  $\varphi$  with respect to a  $\mathfrak{g}$ -basis of  $L$ . Then  $\mu_0(L) \subset \mathfrak{g}$  if and only if  $\varphi_0 \in S_n(\mathfrak{g})$ , and  $\mu(L) \subset \mathfrak{g}$  if and only if  $2\varphi_0 \in T_n(\mathfrak{g})$ . Thus the discussion of integral lattices is essentially the discussion of  $2^{-1}T_n(\mathfrak{g})$ . An element of  $S_n(\mathfrak{g})$  defines a  $\mathfrak{g}$ -valued *symmetric form* on a lattice, and is different from a  $\mathfrak{g}$ -valued *quadratic form*, which is represented by an element of  $2^{-1}T_n(\mathfrak{g})$ . The distinction between these two kinds of  $\mathfrak{g}$ -valued forms is nontrivial. In this section we classify  $\mathfrak{g}$ -valued quadratic forms; the classification of  $\mathfrak{g}$ -valued symmetric forms will be done in Section 33.



Now pick and fix  $\varphi_0 \in 2^{-1}T_n(\mathfrak{g})$  in the global case; let  $(V, \varphi) = \langle F, \varphi_0 \rangle$  and  $L = \mathfrak{g}_n^1$ . Then  $\tilde{L} = L(2\varphi_0)^{-1}$ ,  $[\tilde{L}/L] = \det(2\varphi_0)\mathfrak{g}$ , and  $d(L) = \det(\varphi_0)\mathfrak{g}$ . Let  $\psi$  be an element of  $S_n(F)$  belonging to the genus of  $\varphi_0$  in the sense of §30.10. Then  $\langle F, \psi \rangle$  is isomorphic to  $\langle F, \varphi_0 \rangle$ , but the isomorphism-class of  $\langle F, \varphi_0 \rangle$  does not necessarily determine the genus of  $\varphi_0$ . However, as noted in §30.1, all the maximal lattices in  $V$  form a single  $\varphi$ -genus, and so the genus of a matrix corresponding to a maximal lattice is determined by the isomorphism-class of quadratic spaces. This point becomes clearer if  $F = \mathbf{Q}$ , as will be explained in §31.3. We first state a global result concerning  $[\tilde{L}/L]$  and  $\mu(\tilde{L})$  with no condition on  $F$ .

**Theorem 31.2.** *Given  $(V, \varphi)$  over a global field  $F$ , let  $K_0 = F(\delta^{1/2})$  be the discriminant field of  $(V, \varphi)$ , and  $L$  a maximal lattice in  $V$ . Let  $\mathfrak{e}$  be the product of the prime ideals ramified in  $Q(\varphi)$ , and  $\mathfrak{e}_1$  the product of the prime factors of  $\mathfrak{e}$  that do not ramify in  $K_0$ ; also let  $\mathfrak{d}_0 = N_{K_0/F}(d(K_0/F))$ , where  $d(K_0/F)$  is the different of  $K_0$  relative to  $F$ . Then the following assertions hold:*

- (i)  $\mu(L) = \mathfrak{g}$  if  $n > 2$ .
- (ii) If  $n$  is even, then  $[\tilde{L}/L] = \mathfrak{d}_0\mathfrak{e}_1^2$  and  $\mu(\tilde{L})^{-1} = \mathfrak{d}_0\mathfrak{e}_1$ .
- (iii) Suppose  $n$  is odd; let  $\delta\mathfrak{g} = \mathfrak{a}\mathfrak{b}^2$  with a square-free integral ideal  $\mathfrak{a}$  and a fractional ideal  $\mathfrak{b}$ . Then  $[\tilde{L}/L] = 2\mathfrak{a}^{-1}\mathfrak{e}^2 \cap 2\mathfrak{a}$  and  $\mu(\tilde{L})^{-1} = 4\mathfrak{a} \cap \mathfrak{e}$ .

PROOF. We gave formulas for  $[\tilde{L}/L]$ ,  $\mu(L)$ , and  $\mu(\tilde{L})^{-1}$  for a local lattice  $L$  in (29.7), (29.8), and (29.9). For a global lattice  $L$  we have  $\mu(L)_v = \mu(L_v)$ . Thus (i) follows from (29.8). Similarly (ii) and (iii) follow from (29.7) and (29.9).

We will comment on  $\mu(\tilde{L})^{-1}$  in §31.11.

**31.3.** By Theorems 28.7 and 28.9 we can enumerate all the isomorphism classes of  $(V, \varphi)$  with given  $n$ ,  $K$ ,  $B$ , and  $\{\sigma_v\}$ . We can express the results in connection with  $[\tilde{L}/L]$  and  $\mu(\tilde{L})$  by virtue of Theorem 31.2. For simplicity we do so in this book only when  $F = \mathbf{Q}$ , in which case we can give a list according to the nature of a symmetric matrix representing  $\varphi$  with respect to a  $\mathbf{Z}$ -basis of  $L$ .

We first consider more generally a local or global field  $F$  and its maximal order  $\mathfrak{g}$ , and note that both  $S_n(\mathfrak{g})$  and  $T_n(\mathfrak{g})$  are stable under the map  $\varphi \mapsto \alpha\varphi \cdot {}^t\alpha$  for every  $\alpha \in GL_n(\mathfrak{g})$ . We call an element  $\varphi$  of  $2^{-1}T_n(\mathfrak{g})$   **$q$ -reduced** (that is, reduced as a quadratic form) if it satisfies the following condition:

$$(31.2) \quad \varphi = \alpha\psi \cdot {}^t\alpha, \quad \alpha \in M_n(\mathfrak{g}), \text{ and } \psi \in 2^{-1}T_n(\mathfrak{g}) \implies \alpha \in GL_n(\mathfrak{g}).$$

Similarly we call an element  $\varphi$  of  $S_n(\mathfrak{g})$   **$s$ -reduced** (reduced as a symmetric form) if it satisfies

$$(31.3) \quad \varphi = \alpha\psi \cdot {}^t\alpha, \alpha \in M_n(\mathfrak{g}), \text{ and } \psi \in S_n(\mathfrak{g}) \implies \alpha \in GL_n(\mathfrak{g}).$$

If an element of  $S_n(\mathfrak{g})$  is  $q$ -reduced, then it is  $s$ -reduced, but the converse is false. For example,  $\eta_r$  of (22.6) is  $s$ -reduced, but not  $q$ -reduced if  $2 \notin \mathfrak{g}^\times$ , as  $\eta_r = \alpha(2^{-1}\eta_r) \cdot {}^t\alpha$  with  $\alpha = \text{diag}[1, 2 \cdot 1_r]$ ;  $2^{-1}\eta_r$  is  $q$ -reduced.

Let  $(V, \varphi)$  be a quadratic space over  $F$ . Suppose  $\mathfrak{g}$  is a principal ideal domain; let  $\psi$  be the matrix representing  $\varphi$  with respect to a  $\mathfrak{g}$ -basis of a lattice  $L$  in  $V$ . Then we see that  $\psi$  is  $q$ -reduced resp.  $s$ -reduced if and only if  $L$  is  $\varphi$ -maximal resp.  $\varphi^*$ -maximal in the sense of §29.1. Indeed, let  $L = \mathfrak{g}_n^1$  and  $\varphi \in 2^{-1}T_n(\mathfrak{g})$ ; suppose  $L$  is  $\varphi$ -maximal and  $\varphi = \alpha\psi \cdot {}^t\alpha$  with  $\alpha \in M_n(\mathfrak{g})$  and  $\psi \in 2^{-1}T_n(\mathfrak{g})$ . Then  $L \subset L\alpha^{-1}$  and  $L\alpha^{-1}$  is  $\varphi$ -integral, and so the  $\varphi$ -maximality of  $L$  implies that  $L = L\alpha^{-1}$ . Thus  $\alpha \in GL_n(\mathfrak{g})$ , which means that  $\varphi$  is  $q$ -reduced. The converse and the statement about the  $s$ -reducibility can be verified in a similar way.

**31.4.** Now, instead of trying to classify all  $\mathbf{Z}$ -valued quadratic forms or symmetric forms, we restrict ourselves to the  $q$ -reduced or  $s$ -reduced elements. This idea seems perfectly reasonable for the following reason. In algebraic number theory, without considering an arbitrary ring of algebraic integers, we take the maximal order, and discuss everything in relation with it. For instance, the class number of an algebraic number field is the number of ideal classes with respect to the maximal order. Likewise, it is natural to define the **class number of a quadratic space** to be the number of classes in the genus of maximal lattices, which amounts to the number of classes in the genus of a  $q$ -reduced matrix. It should also be noted that there are few previous investigations on classification for an arbitrary value of the discriminant of the form beyond the unimodular case. It can easily be seen that if  $\varphi \in 2^{-1}T_n(\mathfrak{g})$  resp.  $S_n(\mathfrak{g})$  and  $\det(2\varphi)$  resp.  $\det(\varphi)$  is square-free, then  $\varphi$  is  $q$ -reduced resp.  $s$ -reduced. Therefore we will eventually classify all  $\mathbf{Z}$ -valued quadratic and symmetric forms with square-free determinant.

Before proceeding further, let us introduce a generalization of a traditional terminology. We say that an element  $\varphi$  of  $S_n(\mathfrak{g})$  is of **Type 1** if  $x\varphi \cdot {}^tx \notin 2\mathfrak{g}$  for some  $x \in \mathfrak{g}_n^1$ , and of **Type 2** if  $x\varphi \cdot {}^tx \in 2\mathfrak{g}$  for every  $x \in \mathfrak{g}_n^1$ . Clearly  $\varphi$  is of Type 2 if and only if  $\varphi \in T_n(\mathfrak{g})$ . Given  $\varphi$  and  $\psi$  of  $S_n(F)$  let us write

$$(31.4) \quad \varphi \sim \psi \quad \text{if} \quad \varphi = \alpha\psi \cdot {}^t\alpha \quad \text{with} \quad \alpha \in GL_n(F),$$

$$(31.5) \quad \varphi \approx \psi \quad \text{if} \quad \varphi = \alpha\psi \cdot {}^t\alpha \quad \text{with} \quad \alpha \in GL_n(\mathfrak{g}).$$

If  $\varphi \approx \psi$  for  $\varphi, \psi \in S_n(\mathfrak{g})$ , then clearly  $\varphi$  and  $\psi$  are of the same type.

**31.5.** Let us again take  $F = \mathbf{Q}$  and  $\mathfrak{g} = \mathbf{Z}$ . Given  $\varphi \in 2^{-1}T_n(\mathbf{Z})$ , let  $N$  be the smallest positive integer such that  $N(2\varphi)^{-1} \in T_n(\mathbf{Z})$ . We put  $N = \ell(T)$  and call it the **level** of  $T$ . We let  $\mathfrak{S}_n^0$  denote the subset of  $2^{-1}T_n(\mathbf{Z})$  consisting

of the  $q$ -reduced elements of  $2^{-1}T_n(\mathbf{Z})$ . Clearly if  $T \in 2^{-1}T_n(\mathbf{Z})$  and  $\det(2T)$  is square-free, then  $T \in \mathfrak{S}_n^0$ .

Given  $(V, \varphi)$  over  $\mathbf{Q}$ , take a maximal lattice  $L$  in  $V$  and let  $\Phi$  be the matrix that represents  $\varphi$  with respect to a  $\mathbf{Z}$ -basis of  $L$ . Then  $\tilde{L} = L(2\Phi)^{-1}$ ,  $\det(2\Phi)\mathbf{Z} = [\tilde{L}/L]$ ,  $\Phi \in \mathfrak{S}_n^0$ , and every matrix in  $\mathfrak{S}_n^0$  can be obtained in this fashion from a maximal lattice. Since all the maximal lattices form one genus, we see that the genus of  $\Phi$  in the sense explained in §30.10 is determined by the isomorphism class of  $(V, \varphi)$ , and vice versa. Also, we can easily verify that  $\mu(\tilde{L})^{-1} = \ell(\Phi)\mathbf{Z}$ . If  $n > 2$ , then  $\mu(L) = \mathbf{Z}$  by Theorem 31.2(i), and hence the greatest common divisor of  $2\varphi_{ij}$  and  $\varphi_{ii}$  for all  $i, j$  is 1.

Now the classification of all  $\Phi$  in  $\mathfrak{S}_n^0$  can be stated in the following two theorems.

**Theorem 31.6** (The case of even  $n$ ). *Let three integers  $n, \sigma, \delta$ , and two square-free positive integers  $e_0, e_1$  be given as follows:  $4 \leq n \in 2\mathbf{Z}$ ,  $|\sigma| \leq n$ ,  $\sigma \in 2\mathbf{Z}$ ;  $\delta = 1$  or  $\delta$  is the discriminant of a quadratic extension  $K_0$  of  $\mathbf{Q}$ ;  $e_0$  divides  $\delta$  and  $e_1$  is prime to  $\delta$ . Let  $r$  be the number of prime factors of  $e_0e_1$ , and let  $B$  be the quaternion algebra over  $\mathbf{Q}$  such that  $D_B = e_0e_1$  (see §27.9). Suppose that  $(-1)^{\sigma/2}\delta > 0$  and  $\sigma - 4r \equiv 0$  or  $2 \pmod{8}$ . Then there exists an element  $\Phi$  of  $\mathfrak{S}_n^0$  such that*

$$|\det(2\Phi)| = |\delta|e_1^2, \quad s(\Phi) = \sigma, \quad Q(\Phi) = B, \quad \ell(\Phi) = |\delta|e_1.$$

Moreover,  $K_0$  is the discriminant field of  $\Phi$ , every element of  $\mathfrak{S}_n^0$  is of this type, and its genus is determined by  $(\sigma, \delta, e_0, e_1)$ , where we put  $K_0 = \mathbf{Q}$  if  $\delta = 1$ . These statements are true even for  $n = 2$  under the following additional condition on  $e_1$ : if  $e_1 \neq 1$ , then  $\delta \neq 1$  and every prime factor of  $e_1$  remains prime in  $K_0$ .

PROOF. Take  $F = \mathbf{Q}$  in Theorems 28.9 and 31.2; put  $\mathfrak{e} = e_0e_1\mathbf{Z}$ . We have  $\mathfrak{d}_0 = \delta\mathbf{Z}$ . As observed in §27.9,  $B_{\mathbf{a}} \cong M_2(\mathbf{R})$  if and only if  $r \in 2\mathbf{Z}$ . Therefore from (28.6a) we see that  $\sigma - 4r \equiv 0$  or  $2 \pmod{8}$ . Since  $B$  is determined by  $e$ , and  $(V, \varphi)$  by  $(n, \sigma, \delta, B)$ , we obtain our theorem.

**Theorem 31.7** (The case of odd  $n$ ). *Let two integers  $n$  and  $\sigma$  be given as follows:  $0 < n - 1 \in 2\mathbf{Z}$ ,  $|\sigma| \leq n$ , and  $\sigma - 1 \in 2\mathbf{Z}$ ; also let  $m$  and  $e$  be square-free positive integers. Further let  $r$  be the number of prime factors of  $e$ , and let  $B$  be the quaternion algebra over  $\mathbf{Q}$  such that  $D_B = e$  (see §27.9). Suppose that  $\sigma \equiv 4r \pm 1 \pmod{8}$ . Then there exists an element  $\Phi$  of  $\mathfrak{S}_n^0$  such that*

$$|\det(2\Phi)| = 2(m \cap e)^2/m, \quad s(\Phi) = \sigma, \quad Q(\Phi) = B, \quad \ell(\Phi) = 4m \cap e,$$

where  $x \cap y$  denotes the least common multiple of  $x$  and  $y$ . Moreover, the discriminant field of  $\Phi$  is  $\mathbf{Q}(\delta^{1/2})$  with  $\delta = (-1)^{(\sigma-1)/2}m$ , every element of  $\mathfrak{S}_n^0$  is of this type, and its genus is determined by  $(\sigma, m, e)$ .

PROOF. For the same reason as in the proof of Theorem 31.6, we see that (28.6b) holds if and only if  $\sigma \equiv 4r \pm 1 \pmod{8}$ . Given  $m$  and  $e$ , take  $\delta = (-1)^{(\sigma-1)/2}m$  and  $\mathfrak{e} = e\mathbf{Z}$  in Theorems 28.9 and 31.2(iii). Then  $\mathfrak{a} = m\mathbf{Z}$ , and we immediately obtain the desired results.

**31.8.** As one of the easiest special cases let us now discuss  $\Phi \in 2^{-1}T_n(\mathbf{Z})$  such that  $\det(2\Phi)$  is square-free. Though we will state results in more general cases in Theorem 31.9 below, we first treat this simpler case, since the arguments in the general case are complicated and it may not be so easy to understand what the main points of the proof are.

Thus we take a square-free positive integer  $f$  with exactly  $\nu$  prime factors; the case  $f = 1$  is included. We also take an integer  $\sigma$  such that  $|\sigma| \leq n$  and  $\sigma - n \in 2\mathbf{Z}$ . We look for an element  $\Phi$  of  $2^{-1}T_n(\mathbf{Z})$  such that

$$(31.6) \quad |\det(2\Phi)| = f \quad \text{and} \quad s(\Phi) = \sigma.$$

Since  $f$  is square-free, such a  $\Phi$  is  $q$ -reduced. Before discussing this problem, we note an easy fact. For a positive square-free integer  $m$  let  $\kappa(m)$  denote the number of prime factors of  $m$ . Then we have:

(31.7) *Given such an  $m > 1$  and  $\varepsilon = 0$  or  $1$ , the number of positive divisors  $e$  of  $m$  such that  $\kappa(e) - \varepsilon \in 2\mathbf{Z}$  is  $2^{\kappa(m)-1}$ .*

This is because  $\sum_{i=0}^{[k/2]} \binom{k}{2i} = \sum_{i=0}^{[(k-1)/2]} \binom{k}{2i+1} = 2^{k-1}$ .

Now take  $\Phi$  as in (31.6).

(I) Suppose  $n \in 2\mathbf{Z}$ . Let the symbols be as in Theorem 31.6. Then  $|\delta|e_1^2 = f$ , and so  $e_1 = 1$ ,  $|\delta| = f$ ,  $e_0|f$ , and  $r \leq \nu$ . The nature of  $\delta$  can be seen from (10.11); namely,  $4|\delta|$  or  $\delta - 1 \in 4\mathbf{Z}$ . If  $\delta > 0$ , then  $\sigma \in 4\mathbf{Z}$ , and  $\delta = 1$  or  $1 < \delta = f \equiv 1 \pmod{4}$ ; if  $\delta < 0$ , then  $\sigma - 2 \in 4\mathbf{Z}$  and  $-\delta = f \equiv 3 \pmod{4}$ . Therefore we see that  $\sigma - f + 1 \in 4\mathbf{Z}$  in both cases. Now there are  $2^\nu$  factors  $e_0$  of  $f$ , but the number of prime factors  $r$  of  $e_0$  must be taken so that  $\sigma - 4r \in 8\mathbf{Z}$  if  $f - 1 \in 4\mathbf{Z}$  and  $\sigma - 4r - 2 \in 8\mathbf{Z}$  if  $f - 3 \in 4\mathbf{Z}$ .

Therefore if  $\delta = 1$ , then  $\nu = 0$ , and  $r = 0$  is the only choice, so that we must have  $\sigma \in 8\mathbf{Z}$ . If  $\delta \neq 1$ , then  $\nu > 0$  and we have to assume that  $\sigma - f + 1 \in 4\mathbf{Z}$ . Once this is satisfied, we can find  $r$ , and  $r \pmod{2}$  is determined. Thus by (31.7) there are  $2^{\nu-1}$  choices of  $e_0$ . Notice that the case  $n = 2$  can be included.

(II) Suppose  $0 < n - 1 \in 2\mathbf{Z}$ ; let the symbols be as in Theorem 31.7. Then we easily see that  $e|m$ ,  $f = 2m$ ,  $m \notin 2\mathbf{Z}$ , and  $r \leq \nu - 1$ . If  $\nu = 1$ , then  $f = 2$  and  $\sigma \pm 1 \in 8\mathbf{Z}$ . Otherwise  $m > 1$ , and we have to take  $r$  so that  $\sigma \equiv 4r \pm 1 \pmod{8}$ , which is feasible and there exist  $2^{\nu-2}$  choices of  $e$ .

To sum up, *given a square-free positive integer  $f$  and an integer  $\sigma$  such that  $|\sigma| \leq n$  and  $\sigma - n \in 2\mathbf{Z}$ , there exists an element  $\Phi$  of  $2^{-1}T_n(\mathfrak{g})$  satisfying (31.6) if and only if one of the following conditions is satisfied:*

$$(31.8a) \quad f = 1 \quad \text{and} \quad \sigma \in 8\mathbf{Z},$$

$$(31.8b) \quad f = 2 \quad \text{and} \quad \sigma \pm 1 \in 8\mathbf{Z},$$

$$(31.8c) \quad 0 < f - 1 \in 2\mathbf{Z}, \quad n \in 2\mathbf{Z}, \quad \text{and} \quad \sigma - f + 1 \in 4\mathbf{Z},$$

$$(31.8d) \quad f = 2m, \quad 1 < n - 1 \in 2\mathbf{Z} \quad \text{with} \quad 0 < m - 1 \in 2\mathbf{Z}.$$

The genus of such a  $\Phi$  is unique in the first two cases, and there are exactly  $2^{\nu-1}$  genera of such  $\Phi$  in case (31.8c) and  $2^{\nu-2}$  genera in case (31.8d), where  $\nu$  is the number of prime factors of  $f$ .

It should be noted that case (31.8a) is well known. Namely, *there exists*  $\Psi \in T_n(\mathbf{Z})$  (that is,  $\Psi$  of Type 2) such that  $|\det(\Psi)| = 1$  if and only if  $s(\Psi) \in 8\mathbf{Z}$ . For the original proof of this classical result, the reader is referred to van der Blij [V]. Let us now state more general results derived from the above two theorems.

**Theorem 31.9.** *In the following statements  $\sigma$  is an integer such that  $|\sigma| \leq n$  and  $\sigma - n \in 2\mathbf{Z}$ .*

(i) *Let  $f$  and  $g$  be square-free positive integers whose greatest common divisor is 2 if both  $n$  and  $f$  are even, and 1 otherwise. Let  $\Phi \in \mathfrak{S}_n^0$ . Then  $|\det(2\Phi)| = fg^2$  with such  $f$  and  $g$  if  $n$  is even, and  $|\det(2\Phi)| = 2fg^2$  with such  $f$  and  $g$  if  $n$  is odd.*

(ii) *There is no  $\Phi \in 2^{-1}T_n(\mathbf{Z})$  for even  $n$  such that  $2^{-1}\det(2\Phi)$  is an odd integer.*

(iii) *Let  $g$  be the product of  $t$  ( $\geq 0$ ) different prime numbers and let  $2 < n \in 2\mathbf{Z}$ . Then  $\mathfrak{S}_n^0$  contains an element  $\Phi$  such that  $|\det(2\Phi)| = g^2$  and  $s(\Phi) = \sigma$  if and only if  $\sigma - g \in 4\mathbf{Z}$  or  $\sigma - 4t \in 8\mathbf{Z}$ , and the genus of such a  $\Phi$  is determined by  $(\sigma, g)$ .*

(iv) *For  $g$  as in (iii) and  $0 < n - 1 \in 2\mathbf{Z}$  the set  $\mathfrak{S}_n^0$  contains an element  $\Phi$  such that  $|\det(2\Phi)| = 2g^2$  and  $s(\Phi) = \sigma$  if and only if  $\sigma \equiv 4t \pm 1 \pmod{8}$ , and the genus of such a  $\Phi$  is determined by  $(\sigma, g)$ .*

(v) *Let  $f$  and  $g$  be as in (i) and let  $s$  be the number of prime factors of  $f$ ; suppose that  $s > 0$  and  $2 < n \in 2\mathbf{Z}$ . Then the number of genera of  $\Phi \in \mathfrak{S}_n^0$  such that  $|\det(2\Phi)| = fg^2$  and  $s(\Phi) = \sigma$  is  $2^s$  if  $f - \sigma + 1 \in 4\mathbf{Z}$  and  $2^{s-1}$  otherwise. Moreover,  $g \in 2\mathbf{Z}$  if  $f - \sigma + 1 \in 4\mathbf{Z}$ .*

(vi) *Let  $f, g$ , and  $s$  be as in (v). Then for  $1 < n - 1 \in 2\mathbf{Z}$  the number of genera of  $\Phi \in \mathfrak{S}_n^0$  such that  $|\det(2\Phi)| = 2fg^2$  and  $s(\Phi) = \sigma$  is  $2^{s-1}$ .*

(vii) *There exists  $\Phi \in 2^{-1}T_n(\mathbf{Z})$  such that  $|\det(2\Phi)| = 2$  and  $s(\Phi) = \sigma$  if and only if  $\sigma \equiv \pm 1 \pmod{8}$ , and such a  $\Phi$  determines a unique genus for each  $(n, \sigma)$ .*

PROOF. We can derive (i) from Theorems 31.6 and 31.7 in the same manner as in §31.8, using (10.11); (ii) follows easily from (i). Suppose  $2 < n \in 2\mathbf{Z}$  and  $|\det(2\Phi)| = g^2$  with  $g$  as in (iii). Then in Theorem 31.6 we have  $(\delta, e_1) =$

$(1, g)$  or  $(-4, g/2)$ , which is so according as  $\sigma \in 4\mathbf{Z}$  or  $\sigma - 2 \in 4\mathbf{Z}$ . If  $\sigma \in 4\mathbf{Z}$ , then  $t = r$ , and so  $\sigma - 4t \in 8\mathbf{Z}$ ; if  $\sigma - 2 \in 4\mathbf{Z}$ , then  $e_1$  is odd, and so  $\sigma - g \in 4\mathbf{Z}$ . In the latter case we take  $e = e_1$  or  $2e_1$  according to the parity of  $t$  and  $\sigma \pmod{8}$ . Thus we obtain (iii). The proof of (iv) is similar and simpler.

As for (v), we have  $|\delta| = f$  or  $4f$ , and  $(\sigma, \delta)$  determines  $(\sigma, f)$  and vice versa. Now  $\delta$  has exactly  $s + 1$  prime factors if and only if  $f$  is odd and  $|\delta| = 4f$ , which can happen if and only if  $f - \sigma + 1 \in 4\mathbf{Z}$ . Otherwise  $\delta$  has exactly  $s$  prime factors. Once  $(\sigma, \delta, e_1)$  is fixed, the genus of  $\Phi$  is determined by a factor  $e_0$  of  $\delta$ , and the number of the prime factors of  $e_0$  must have the parity determined by  $r$  and  $e_1$ . Since  $\sigma$  determines  $r \pmod{2}$ , we obtain (v) in view of (31.7). The proof of (vi) is similar and simpler. Finally, (vii) is trivially true if  $n = 1$ . For  $n > 1$ , it follows immediately from (ii) and (iv).

**31.10. Remark.** (A) If  $n = 2$ , we can easily classify all  $\Phi \in 2^{-1}T_2(\mathbf{Z})$  without assuming  $\Phi$  to be reduced. In the higher-dimensional case, however, no clear-cut results seem obtainable without the assumption that  $\Phi$  is reduced, and therefore we believe that our restriction of  $\Phi$  to  $\mathfrak{S}_n^0$  is more than natural.

(B) When  $F \neq \mathbf{Q}$ , analogues of the statements of Theorem 31.9 are not so simple. See [S06b, p. 1540, Remark (B)] and [S06c].

(C) We can state results about  $s$ -reduced elements of  $S_n(\mathbf{Z})$  similar to the above theorems as we will indeed do in Section 3Z. However, before doing so we investigate various things such as strong approximation.

(D) We have so far considered the *genus* of  $\Phi$ , not the *class* of  $\Phi$ , since the nature of the latter is completely different from and far more complex than the former. However, we can make a clear-cut statement about the class, provided  $\varphi$  is indefinite and  $\dim(V) \geq 3$ , as will be shown in Theorem 32.19 and §32.20.

**31.11.** Let us now explain the meaning of  $\ell(\Phi)$  in terms of the theta series associated with  $\Phi$ , which is given by

$$(31.9) \quad \theta(z, \Phi) = \sum_g \exp(2\pi iz \cdot g\Phi \cdot {}^t g).$$

Here  $\Phi$  is a positive definite element of  $2^{-1}T_n(\mathbf{Z})$ ,  $g$  runs over the elements of  $\mathbf{Z}_n^1$ , and  $z$  is a variable on the complex half plane  $H = \{z \in \mathbf{C} \mid \operatorname{Im}(z) > 0\}$ . This is a modular form of weight  $n/2$  and of level  $\ell(\Phi)$ , which is why we call  $\ell(\Phi)$  the level of  $\Phi$ . To be precise, put  $N = \ell(\Phi)$ . Then for every  $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbf{Z})$  such that  $c \in N\mathbf{Z}$  we have

$$(31.10a) \quad \theta(\gamma(z), \Phi) = \left(\frac{\Delta}{d}\right)(cz + d)^{n/2}\theta(z, \Phi) \quad \text{if } n \in 2\mathbf{Z},$$

$$(31.10b) \quad \theta(\gamma(z), \Phi) = \left( \frac{\Delta}{d} \right) h_\gamma(z) (cz + d)^{(n-1)/2} \theta(z, \Phi) \quad \text{if } n \notin 2\mathbf{Z}.$$

Here  $\gamma(z) = (az + b)(cz + d)^{-1}$ ,  $\Delta = (-1)^{n/2} \det(2\Phi)$  if  $n \in 2\mathbf{Z}$ , and  $\Delta = (-1)^{(n-1)/2} 2 \det(2\Phi)$  if  $n \notin 2\mathbf{Z}$ ;  $h_\gamma(z)$  is the standard factor of automorphy of weight  $1/2$ , which was written  $j(\gamma, z)$  in [S73]. Clearly  $\Delta$  can be replaced by the discriminant of the discriminant field of the quadratic form represented by  $\Phi$ .

To obtain (31.10a, b), we consider the theta series  $\theta(z; h, A, N, P)$  of [S73, (2.0)] with  $h = 0$ ,  $A = 2\Phi$ , and  $P = 1$ . Then it gives our series of (31.9), and so we obtain (31.10a, b) as special cases of Proposition 2.1 of [S73].

We can similarly associate a theta series in the Hilbert modular case with an integral lattice  $L$  in  $(V, \varphi)$  when  $F$  is totally real and  $\varphi$  is totally positive. Then we can derive transformation formulas similar to (31.10a, b) from [S93, Theorem 3.5, Proposition 3b.2]. The ideal  $\mu(\tilde{L})^{-1}$  is the level of the series in the same sense.

### 32. Strong approximation in the indefinite case

**32.1.** The principal purpose of this section is to prove a kind of strong approximation on an indefinite orthogonal group. As a preliminary step we take a nondegenerate quadratic space  $(V, \varphi)$  over a local field  $F$  and prove several lemmas concerning lattices in  $V$  and symmetric matrices. We use symbols  $\mathfrak{g}, \mathfrak{p}$  as before and also  $S_n(\ )$  and  $\approx$  as in §30.10 and (31.5). From §32.7 on, however, we consider objects over a global field.

**Lemma 32.2.** *Let  $L$  be a lattice in  $V$ . If  $L(\alpha - \beta) \subset \mathfrak{p}L\alpha$  for  $\alpha, \beta \in GL(V)$ , then  $L\alpha = L\beta$ .*

PROOF. Put  $L\alpha = M$  and  $L\beta = N$ . For  $x \in L$  we have  $x\alpha - x\beta \in \mathfrak{p}M$  and  $x\alpha \in M$ , and so  $N \subset M$ . Similarly  $M \subset N + \mathfrak{p}M$ , and we can show inductively that  $M \subset N + \mathfrak{p}^k M$  for every  $k \in \mathbf{Z}, > 0$ . We have  $\mathfrak{p}^k M \subset N$  for some  $k$ , and so  $M \subset N$ . Thus  $M = N$  as expected.

**Lemma 32.3.** *Suppose  $(V, \varphi) = \langle F, \varphi_0 \rangle$  with  $\varphi_0 \in S_n(F)$ ; let  $L = \mathfrak{g}_n^1$ . Then  $L^\varphi = L$  if and only if  $\varphi_0 \in GL_n(\mathfrak{g})$  and  $\tilde{L} = L$  if and only if  $2\varphi_0 \in GL_n(\mathfrak{g})$ .*

PROOF. This is because  $2\tilde{L} = L^\varphi = L\varphi_0^{-1}$ , as observed in §29.1.

**Lemma 32.4.** (i) *Let  $\psi \in S_n(\mathfrak{g})$  and  $\varepsilon \in S_r(\mathfrak{g}) \cap GL_r(\mathfrak{g})$ ,  $r < n$ . If  $\psi \approx \begin{bmatrix} \varepsilon & * \\ * & * \end{bmatrix}$ , then  $\psi \approx \text{diag}[\varepsilon, \xi]$  with  $\xi \in S_{n-r}(\mathfrak{g})$ .*

(ii) *Let  $L$  be a lattice in  $V$  such that  $\mu_0(L) \subset \mathfrak{g}$ ; let  $M$  be a  $\mathfrak{g}$ -submodule of  $L$  and  $X$  the  $F$ -linear span of  $M$ . Suppose  $\varphi$  is nondegenerate on  $X$  and  $M = \{x \in X \mid \varphi(x, M) \subset \mathfrak{g}\}$ . Then  $L = M \oplus (L \cap X^\perp)$ .*

PROOF. Given  $\psi$  as in (i), we can put  $\psi = \begin{bmatrix} \varepsilon & {}^t\beta \\ \beta & \omega \end{bmatrix}$  with  $\beta \in \mathfrak{g}_r^{n-r}$  and  $\omega \in \mathfrak{g}_{n-r}^{n-r}$ . Put  $\gamma = \begin{bmatrix} 1 & 0 \\ -\beta\varepsilon^{-1} & 1 \end{bmatrix}$ . Then  $\gamma\psi \cdot {}^t\gamma = \text{diag}[\varepsilon, \xi]$  with  $\xi \in S_{n-r}(\mathfrak{g})$ . This proves (i). In the setting of (ii) we easily see that  $M = L \cap X$ . Take a  $\mathfrak{g}$ -basis  $\{e_i\}_{i=1}^r$  of  $M$ . Then  $(\varphi(e_i, e_j))_{i,j=1}^r \in GL_r(\mathfrak{g})$  by Lemma 32.3. Therefore, given  $z \in L$ , we can take  $c_i \in \mathfrak{g}$  so that  $\sum_{i=1}^r c_i \varphi(e_i, e_j) = \varphi(z, e_j)$  for every  $j$ . Then  $z - \sum_{i=1}^r c_i e_i \in L \cap X^\perp$ , which proves (ii). In fact, (ii) is merely a reformulation of (i).

**Lemma 32.5.** *Given  $\sigma = {}^t\sigma \in M_n(F)$ , we have  $\sigma \approx \text{diag}[\sigma_1, \dots, \sigma_r]$  with  $\sigma_i$  of size 1 or 2, where each  $\sigma_i$  of size 2 is of the form  $\sigma_i = \begin{bmatrix} a & b \\ b & d \end{bmatrix}$ ,  $a\mathfrak{g} + d\mathfrak{g} \subsetneq b\mathfrak{g} \neq \{0\}$ , and is necessary only if  $2 \in \mathfrak{p}$ .*

PROOF. We prove this by induction on  $n$ . Multiplying  $\sigma$  by a suitable element of  $\mathfrak{g}$ , we may assume that  $\sigma \in M_n(\mathfrak{g})$ ; we may also assume that  $\sigma \neq 0$ . Put  $\sigma = (s_{ij})$ . Let  $\mathfrak{a}$  be the  $\mathfrak{g}$ -ideal generated by the  $s_{ij}$ . Suppose that  $\mathfrak{a} = s_{ii}\mathfrak{g}$  for some  $i$ ; we may then assume that  $i = 1$ , and we can put  $\sigma = \begin{bmatrix} a & b \\ {}^tb & d \end{bmatrix}$  with  $a = s_{11}$ . Put  $\gamma = \begin{bmatrix} 1 & -a^{-1}b \\ 0 & 1_{n-1} \end{bmatrix}$  and observe that  $a^{-1}b \in \mathfrak{g}_{n-1}^1$ . Thus  $\gamma \in GL_n(\mathfrak{g})$ , and  ${}^t\gamma\sigma\gamma = \text{diag}[a, d - {}^tba^{-1}b]$ . Applying induction to  $d - {}^tba^{-1}b$ , we obtain the desired conclusion. Next suppose  $\mathfrak{a} = s_{ij}\mathfrak{r}$  with  $i \neq j$  and  $\mathfrak{a} \neq s_{kk}\mathfrak{r}$  for every  $k$ ; we may assume that  $\mathfrak{a} = s_{12}\mathfrak{r}$ . Put  $a = \begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix}$  and  $\sigma = \begin{bmatrix} a & b \\ {}^tb & d \end{bmatrix}$ . Then  $\det(a)\mathfrak{r} = \mathfrak{a}^2$  and  $a^{-1}$  has entries in  $\mathfrak{a}^{-1}$ . Therefore, putting  $\gamma = \begin{bmatrix} 1_2 & -a^{-1}b \\ 0 & 1_{n-2} \end{bmatrix}$ , we see that  $\gamma \in GL_n(\mathfrak{g})$ , and  ${}^t\gamma\sigma\gamma = \text{diag}[a, d - {}^tba^{-1}b]$ . Thus again induction gives the desired fact. To see when  $\sigma_i$  of size 2 is necessary, suppose  $2 \in \mathfrak{g}^\times$ ; take the above  $a$  of size 2; put  $e = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ . Then  $ea \cdot {}^te = \begin{bmatrix} f & g \\ g & h \end{bmatrix}$  with  $f = s_{11} + s_{22} + 2s_{12}$ , and so  $f\mathfrak{g} = \mathfrak{a}$ . Therefore we can reduce our problem to the case of  $a$  of size 1. This completes the proof.

**Lemma 32.6.** (i) *If  $L$  is an integral lattice in  $V$  and  $\widetilde{L} = L$ , then  $L$  is maximal.*

(ii) *If in addition  $n \geq 3$  or  $\varphi$  is isotropic, then  $\varphi[L] = \mathfrak{g}$ ; if  $n = 2$ , then  $\mathfrak{g}^\times \subset \varphi[L]$ .*

(iii) *Let  $M$  be a maximal lattice in  $V$ . If  $n \geq 4$ , then  $\varphi[M] = \mathfrak{g}$ . If  $n = 3$ , then there is a nonzero element  $c$  of  $\mathfrak{g}$  such that  $c\mathfrak{g}^\times \subset \varphi[M]$ .*

PROOF. In the setting of (i) if  $L \subset M$  and  $M$  is integral, then  $L \subset M \subset \widetilde{M} \subset \widetilde{L}$ , and so  $L = M$ . Thus  $L$  is maximal and its nature was studied in Lemma 29.8 and §29.10. Clearly  $\mathfrak{g} = \varphi[L]$  if  $\varphi$  is isotropic. Suppose  $\varphi$  is



anisotropic. Then  $n \leq 4$ . If  $n = 4$ , then  $(V, \varphi) = (B, \beta)$  and  $L = \mathfrak{o}$  with a quaternion algebra  $B$  over  $F$  and the maximal order  $\mathfrak{o}$  in  $B$ . From Theorems 21.21 and 21.23 we see that  $\varphi[L] = \mathfrak{g}$ . Suppose  $n = 3$ . By (29.7) we have  $2\mathfrak{p}^2 = \delta\mathfrak{g}$ , which is impossible, as  $\mathfrak{p} \subset \delta\mathfrak{g} \subset \mathfrak{g}$ . Thus we obtain the first part of (ii). Suppose  $n = 2$  and  $\varphi$  is anisotropic. By (29.7) we have  $(V, \varphi) = (K, \kappa)$  with an unramified quadratic extension  $K$  of  $F$  and  $L$  is the maximal order of  $K$ , and so  $\mathfrak{g}^\times \subset \varphi[L]$  by Theorem 9.10(ii). As for (iii), if  $\varphi$  is isotropic, then  $\varphi[M] = \mathfrak{g}$ . Suppose  $\varphi$  is anisotropic. If  $n = 4$ , then  $\varphi[M] = \mathfrak{g}$  as already seen in the proof of (ii). Suppose  $n = 3$ ; then we can put  $\varphi[x] = -\delta xx^\iota$  for  $x \in M$  as in the case  $t = 3$  in §29.10, where  $\delta\mathfrak{g}$  is  $\mathfrak{g}$  or  $\mathfrak{p}$ . If  $\delta\mathfrak{g} = \mathfrak{g}$ , then  $M = \mathfrak{g}y + \tau\omega$  with the symbols in that subsection. Let  $x = a\omega$  with  $a \in \mathfrak{r}$ . Then  $\varphi[x] = \delta\omega^2 N_{K/F}(a)$ . By Theorem 9.10(ii) we have  $\mathfrak{g}^\times = N_{K/F}(\mathfrak{r}^\times)$ , and so  $c\mathfrak{g}^\times \subset \varphi[M]$  with  $c = \delta\omega^2$ . If  $\delta\mathfrak{g} = \mathfrak{p}$ , then  $M = \mathfrak{g}y + \tau\omega^{-1}$ , and we similarly obtain  $\mathfrak{g}^\times \subset \varphi[M]$ . This completes the proof.

**32.7.** Until the end of this section we assume  $F$  to be a global field and take  $(V, \varphi) = \langle F, \varphi \rangle$  with  $\varphi \in S_n(F)$ . Thus  $SO(\varphi) \subset SL_n(F)$ . We will be considering the group  $SO(\varphi)_{\mathbf{A}}$  defined in §30.7. We denote by  $\mathbf{r}$  (as we did in §28.6) the set of all real archimedean primes of  $F$ .

**Lemma 32.8.** *Let  $\mathfrak{a}$  be an integral  $\mathfrak{g}$ -ideal and let  $x \in SO(\varphi)_{\mathbf{A}}$ . Then there exists an element  $\alpha$  of  $SO(\varphi)$  such that  $\alpha - x \prec \mathfrak{a}$ . (See (30.10) for the symbol  $\prec$ .)*

PROOF. Let  $\mathbf{p}$  be the set of all prime factors of  $\mathfrak{a}$ . For each  $v \in \mathbf{p}$ , we have, by Theorem 24.6,  $x_v = \tau(u_{v1} \cdots u_{vr})$  with invertible  $u_{vi} \in V_v$  and  $r \in 2\mathbf{Z}$ . The integer  $r$  may depend on  $v$ , but we can take the same  $r$  for all  $v \in \mathbf{h}$ , since  $\tau(w^2) = 1$  for every invertible  $w \in V$ . Put  $L = \mathfrak{g}_n^1$ . Then for  $k \in \mathbf{Z}$ ,  $k > 0$ , we can find invertible  $y_i \in V$  such that  $y_i - u_{vi} \prec \mathfrak{a}_v^k L_v$  for every  $v \in \mathbf{p}$ . Since the map  $\tau : G(V)_v \rightarrow O(\varphi)_v$  is continuous, by taking a sufficiently large  $k$ , we find that  $\tau(y_1 \cdots y_r) - x \prec \mathfrak{a}$ . This proves our lemma.

**Lemma 32.9.** *Given lattices  $L$  and  $M$  belonging to the same  $\varphi$ -genus and a finite subset  $\mathbf{p}$  of  $\mathbf{h}$ , we can find a lattice  $N$  belonging to the  $SO(\varphi)$ -class of  $M$  such that  $N_v = L_v$  for every  $v \in \mathbf{p}$ .*

PROOF. We can put  $L = Mx$  with  $x \in SO(\varphi)_{\mathbf{A}}$ . By Lemma 32.8 we can find an element  $\alpha$  of  $SO(\varphi)$  such that  $M_v(\alpha - x_v) \subset \pi_v L_v$  for every  $v \in \mathbf{p}$ , where  $\pi_v$  is a prime element of  $F_v$ . Then  $M_v\alpha = M_v x_v$  by Lemma 32.2, and so  $(M\alpha)_v = L_v$  for every  $v \in \mathbf{p}$ . Thus  $M\alpha$  gives the desired  $N$ .

**Lemma 32.10.** *Let  $\{L_i\}_{i=1}^h$  be a complete set of representatives for the  $SO(\varphi)$ -classes in the  $\varphi$ -genus of a lattice  $L$  in  $V$ . If  $a \in \varphi[V]$  and  $a \in \varphi[L_v]$  for every  $v \in \mathbf{h}$ , then  $a \in \varphi[L_i]$  for some  $i$ .*

PROOF. Suppose  $0 \neq a = \varphi[x]$  with  $x \in V$  and  $a \in \varphi[L_v]$  for every  $v \in \mathbf{h}$ . Let  $\mathbf{p} = \{v \in \mathbf{h} \mid x \notin L_v\}$ . Then  $\mathbf{p}$  is a finite set. Since  $a \in \varphi[L_v]$ , by Lemma 22.5(ii) we can find, for each  $v \in \mathbf{p}$ , an element  $\alpha_v$  of  $O(\varphi_v)$  such that  $x \in L_v \alpha_v$ . By Lemma 21.6(ii) we can define a lattice  $M$  so that  $M_v = L_v \alpha_v$  for every  $v \in \mathbf{p}$  and  $M_v = L_v$  for  $v \notin \mathbf{p}$ . Then  $M$  belongs to the  $\varphi$ -genus of  $L$ , and so  $M = L_i \beta$  for some  $i$  and some  $\beta \in SO(\varphi)$ . We see that  $x \in M_v$  for every  $v \in \mathbf{h}$ , and so  $x \in M$  by Lemma 21.6(iv). Thus  $\varphi[x] \in \varphi[M] = \varphi[L_i]$ , which proves our lemma.

**Lemma 32.11.** *Suppose  $n \geq 3$ ; let  $\mathbf{p}$  be a finite subset of  $\mathbf{h}$  and  $L$  a lattice in  $V$ . Then there exists an element  $\lambda$  of  $\mathfrak{g}$  such that  $\lambda \in \mathfrak{g}_v^\times$  for every  $v \in \mathbf{p}$  and*

$$(*) \quad a \in \varphi[V] \cap \lambda \mathfrak{g} \text{ and } a \in \varphi[L_v] \text{ for every } v \in \mathbf{h} \implies a \in \varphi[L].$$

PROOF. If this holds for  $\mathbf{p}'$  in place of  $\mathbf{p}$  and  $\mathbf{p} \subset \mathbf{p}'$ , then it holds for  $\mathbf{p}$ . Thus we may assume that  $\tilde{L}_v = L_v$  for every  $v \notin \mathbf{p}$  and  $\mathbf{p}$  contains every prime factor of 2. Then for  $v \notin \mathbf{p}$ ,  $L_v$  is integral and maximal, and  $\varphi[L_v] = \mathfrak{g}_v$  by Lemma 32.6. Take  $\{L_i\}_{i=1}^h$  as in Lemma 32.10. By Lemma 32.9 we may assume that  $(L_i)_v = L_v$  for every  $i$  and for every  $v \in \mathbf{p}$ . Let  $\mathbf{q} = \{v \in \mathbf{h} \mid (L_i)_v \neq L_v \text{ for some } i\}$ . Then  $\mathbf{q}$  is finite and  $\mathbf{p} \cap \mathbf{q} = \emptyset$ . Take  $c \in \mathfrak{g}$ ,  $\neq 0$ , so that  $cL_i \subset L$  for every  $i$ . By Theorem 1.3 we can find  $d \in \mathfrak{g}$  such that  $d \in \mathfrak{g}_v^\times$  for every  $v \in \mathbf{p}$  and  $d \in c\mathfrak{g}_v$  for every  $v \in \mathbf{q}$ . Then  $(dL_i)_v = L_v$  for every  $v \in \mathbf{p}$  and  $(dL_i)_v \subset L_v$  for every  $v \in \mathbf{q}$ . For  $v \notin \mathbf{p} \cup \mathbf{q}$  we have  $(dL_i)_v \subset (L_i)_v = L_v$ . Thus  $dL_i \subset L$  for every  $i$ . Let  $a$  be as in the left-hand side of  $(*)$  with  $\lambda = d^2$ . Then  $a = d^2 b$  with  $b \in \mathfrak{g}$ . For  $v \notin \mathbf{p}$  we have  $b \in \mathfrak{g}_v = \varphi[L_v]$ . If  $v \in \mathbf{p}$ , then  $a \in \varphi[L_v]$  and  $d \in \mathfrak{g}_v^\times$ , and so  $b \in \varphi[L_v]$ . Therefore, by Lemma 32.10,  $b \in \varphi[L_i]$  for some  $i$ . Thus  $a = d^2 b \in \varphi[dL_i] \subset \varphi[L]$ . This proves our lemma.

**Theorem 32.12.** *Suppose  $n \geq 4$  and there is a prime  $u \in \mathbf{a}$  such that  $\varphi_u$  is indefinite (that is,  $|s_u(\varphi)| \neq n$ ); let  $L$  be a lattice in  $V$ . Let  $\mathfrak{a}$  be an integral  $\mathfrak{g}$ -ideal and  $\mathbf{p}$  a finite subset of  $\mathbf{h}$ . Further let  $a$  be a nonzero element of  $\varphi[V]$  and  $x$  an element of  $V_{\mathbf{A}}$  such that  $a = \varphi[x]$  and  $x_v \in L_v$  for every  $v \in \mathbf{h}$ ,  $\notin \mathbf{p}$ . Then there exists an element  $y$  of  $V$  such that  $a = \varphi[y]$ ,  $y - x_v \in \mathfrak{a}_v L_v$  for every  $v \in \mathbf{p}$ , and  $y \in L_v$  for every  $v \in \mathbf{h}$ ,  $\notin \mathbf{p}$ . (Notice that  $y \in L$  if  $x_v \in L_v$  for every  $v \in \mathbf{p}$ .)*

PROOF. Suppose our lemma holds for  $L$ . Given a lattice  $M$  in  $V$  and a finite subset  $\mathbf{p}$  of  $\mathbf{h}$ , put  $\mathbf{p}' = \mathbf{p} \cup \{v \in \mathbf{h} \mid L_v \neq M_v\}$ . Let  $0 \neq a \in \varphi[V]$  and let  $x \in V_{\mathbf{A}}$ ; assume that  $a = \varphi[x]$  and  $x_v \in M_v$  for every  $v \in \mathbf{h}$ ,  $\notin \mathbf{p}$ . Then  $x_v \in L_v$  for every  $v \in \mathbf{h}$ ,  $\notin \mathbf{p}'$ . There exists an element  $y$  of  $V$  such that  $y \in L_v$  for every  $v \in \mathbf{h}$ ,  $\notin \mathbf{p}'$ ,  $a = \varphi[y]$ , and  $y - x_v \in \mathfrak{a}'_v L_v$  for every  $v \in \mathbf{p}'$ , where we take  $\mathfrak{a}'$  so that  $\mathfrak{a}'L \subset \mathfrak{a}M$ . Then for  $v \in \mathbf{p}$  we have  $y - x_v \in \mathfrak{a}M_v$ ;

for  $v \notin \mathbf{p}$  we have  $v \in \mathbf{p}'$  or  $v \notin \mathbf{p}'$ . In the former case  $y - x_v \in \mathfrak{a}M_v$  and  $x_v \in M_v$  and so  $y \in M_v$ ; in the latter case  $y \in L_v = M_v$ . Thus our lemma holds for  $M$ .

Therefore we can change  $L$ . Thus we may assume that  $L = \mathfrak{g}_n^1$  and  $x_v \in L_v$  for every  $v \in \mathbf{h}$ . Also, replacing  $\varphi$  by  $a^{-1}\varphi$ , we may assume that  $a = 1$ . Replacing  $\mathbf{p}$  by a larger set, we may assume that  $\mathbf{p}$  contains every prime factor of 2 and  $\tilde{L}_v = L_v$  for  $v \in \mathbf{h}, \notin \mathbf{p}$ . Further replacing  $\mathfrak{a}$  by its suitable multiple, we may assume that  $\mathfrak{a}_v \neq \mathfrak{g}_v$  for  $v \in \mathbf{p}$ . Take an element  $z$  of  $V$  such that  $\varphi[z] = 1$ . By Lemma 22.5(ii),  $SO(\varphi_v)$  has an element  $\alpha_v$  such that  $x_v = z\alpha_v$ . By Lemma 32.8,  $SO(\varphi)$  has an element  $\beta$  such that  $z\beta - x_v = z(\beta - \alpha_v) \in \mathfrak{a}L_v$  for every  $v \in \mathbf{p}$ . Put  $f = z\beta$ . Then  $\varphi[f] = 1$  and  $f - x_v \in \mathfrak{a}L_v$  for every  $v \in \mathbf{p}$ . Take  $c \in \mathfrak{g}, \neq 0$  so that  $cf \in L$ . We can find  $\mu \in \mathfrak{g}$  such that  $\mu - 1 \in \mathfrak{a}_v$  for  $v \in \mathbf{p}$  and  $\mu \in c\mathfrak{g}_v$  for  $v \notin \mathbf{p}$ . Put  $w = \mu f$ . Then for every  $v \in \mathbf{p}$ ,  $w - x_v \in \mathfrak{a}L_v$ , and so  $w \in L_v$ , since  $x_v \in L_v$ . We have also  $w \in L_v$  for  $v \notin \mathbf{p}$ , since  $cf \in L$ . Thus  $w \in L$ ,  $\varphi[w] = \mu^2$ , and  $\mu \in \mathfrak{g}_v^\times$  for  $v \in \mathbf{p}$ .

Put  $\mathbf{q}_1 = \{v \in \mathbf{h} \mid \mu \notin \mathfrak{g}_v^\times\}$  and  $U = (Fw)^\perp$ . Then  $\mathbf{q}_1 \cap \mathbf{p} = \emptyset$  and  $V = Fw \oplus U$ . By Lemma 21.6(iii),  $(L \cap U)_v = L_v \cap U_v$  for every  $v \in \mathbf{h}$ . Also, by Lemma 21.6(ii) there exists a lattice  $M$  in  $U$  such that  $M_v = L_v \cap U_v$  for  $v \notin \mathbf{p}$  and  $M_v = \mathfrak{a}_v L_v \cap U_v$  for  $v \in \mathbf{p}$ . Then  $M \subset L \cap U$ . Since  $\varphi[w] \in \mathfrak{g}_v^\times$  if  $v \notin \mathbf{q}_1$ , by Lemma 32.4(ii),  $L_v = \mathfrak{g}_v w \oplus M_v$  for  $v \notin \mathbf{p} \cup \mathbf{q}_1$ . We have  $\tilde{L}_v = L_v$  for  $v \notin \mathbf{p}$ , and so  $\tilde{M}_v = M_v$  for  $v \notin \mathbf{p} \cup \mathbf{q}_1$ . Since  $\dim(U) \geq 3$ , we have  $\mathfrak{g}_v = \varphi[M_v]$  for  $v \notin \mathbf{p} \cup \mathbf{q}_1$  by Lemma 32.6(ii).

Let  $v \in \mathbf{q}_1$ . Then  $v \notin \mathbf{p}$ , and so  $v \nmid 2$ ,  $\tilde{L}_v = L_v$ , and  $\mu(L_v) = \mathfrak{g}_v$ . We can find a  $\mathfrak{g}_v$ -basis  $\{e_i\}_{i=1}^n$  of  $L_v$  such that  $Fe_1 = Fw$  by the local version of Theorem 10.19. Then  $w \in \mathfrak{g}_v e_1$  and  $U_v = (F_v e_1)^\perp$ . Since  $\tilde{L}_v = L_v$  and  $2 \in \mathfrak{g}_v^\times$ , we see that  $(\varphi(e_i, e_j))_{i,j=1}^n \in GL_n(\mathfrak{g}_v)$ , and so  $\varphi(e_1, e_j) \in \mathfrak{g}_v^\times$  for some  $j$ . If  $\varphi[e_1] \in \mathfrak{g}_v^\times$ , then  $L_v = \mathfrak{g}_v e_1 \oplus M_v$  by Lemma 32.4, and  $\tilde{M}_v = M_v$ . Thus  $\mathfrak{g}_v \subset \varphi[M_v]$  by Lemma 32.6(ii). If  $\varphi[e_1] \notin \mathfrak{g}_v^\times$ , then  $\varphi(e_1, e_j) \in \mathfrak{g}_v^\times$  for some  $j > 1$ , and  $\begin{bmatrix} \varphi(e_1, e_1) & \varphi(e_1, e_j) \\ \varphi(e_1, e_j) & \varphi(e_j, e_j) \end{bmatrix} \in GL_2(\mathfrak{g}_v)$ . By Lemma 32.4 we have  $L_v = S_v \oplus T_v$  with  $S_v = \mathfrak{g}_v e_1 + \mathfrak{g}_v e_j$  and  $T_v$  orthogonal to  $S_v$ . Then  $\tilde{T}_v = T_v$ ,  $w \in S_v$ , and  $T_v \subset M_v$ , since  $\varphi(w, T_v) = 0$ . By Lemma 32.6(ii),  $\mathfrak{g}_v^\times \subset \varphi[T_v] \subset \varphi[M_v]$ . Thus  $\mathfrak{g}_v^\times \subset \varphi[M_v]$  for every  $v \in \mathbf{q}_1$ .

Next, let  $v \in \mathbf{p}$ . Let  $N$  be a maximal lattice in  $U_v$ . Then  $cN \subset M_v$  for some  $c \in \mathfrak{g}_v, \neq 0$ . By Lemma 32.6(iii),  $c'\mathfrak{g}_v^\times \subset \varphi[N]$  for some  $c' \in \mathfrak{g}_v, \neq 0$ . Then  $c^2 c' \mathfrak{g}_v^\times \subset \varphi[M_v]$ . Therefore, multiplying this by a suitable square, we can find an element  $e_v$  of  $\mathfrak{g}_v$  such that

$$(1) \quad e_v \mathfrak{g}_v^\times \subset \varphi[M_v] \quad \text{and} \quad 0 \neq e_v \in 4\mathfrak{a}_v.$$

This is for every  $v \in \mathbf{p}$ .

By Lemma 32.11 there exists an element  $\lambda$  of  $\mathfrak{g}$  such that  $\lambda \in \mathfrak{g}_v^\times$  for

every  $v \in \mathbf{p} \cup \mathbf{q}_1$  and

$$(2) \quad a \in \varphi[U] \cap \lambda \mathbf{g} \quad \text{and} \quad a \in \varphi[M_v] \quad \text{for every } v \in \mathbf{h} \implies a \in \varphi[M].$$

Put  $\mathbf{q}_2 = \{v \in \mathbf{h} \mid \lambda \notin \mathbf{g}_v^\times\}$ . Then  $\mathbf{q}_2 \cap (\mathbf{p} \cup \mathbf{q}_1) = \emptyset$ . By Lemma 15.10 we can find an element  $d$  of  $F$  such that:

$$(3) \quad d \in \mathbf{g}_v \text{ for } v \in \mathbf{h}, \notin \mathbf{p} \cup \mathbf{q}_2; \quad d - \mu^{-1}(1 - e_v/2) \in e_v \mathbf{a}_v \text{ for } v \in \mathbf{p}; \\ 1 - d^2 \mu^2 \in \lambda \mathbf{g}_v \text{ for } v \in \mathbf{q}_2; \quad |d|_u > 1/\varepsilon; \quad |d|_v < \varepsilon \text{ if } u \neq v \in \mathbf{r} \text{ and } 1 \in \varphi[U_v]; \\ |d|_v > 1/\varepsilon \text{ if } u \neq v \in \mathbf{r} \text{ and } 1 \notin \varphi[U_v].$$

Here  $\varepsilon$  is a small positive number. Since  $\varphi_u$  is indefinite and  $\varphi[w] = \mu^2$ ,  $\varphi$  cannot be positive definite on  $U_u$ . With a sufficiently small  $\varepsilon$  we see that  $1 - d^2 \mu^2 \in \varphi[U_v]$  for every  $v \in \mathbf{a}$ . Also  $1 - d^2 \mu^2 \in \mathbf{g}_v = \varphi[M_v]$  for  $v \in \mathbf{h}, \notin \mathbf{p} \cup \mathbf{q}_1$ ;  $1 - d^2 \mu^2 \in \mathbf{g}_v^\times \subset \varphi[M_v]$  for  $v \in \mathbf{q}_1$ . For  $v \in \mathbf{p}$  we have  $\mu - 1 \in \mathbf{a}_v$ , and so  $\mu \in \mathbf{g}_v^\times$ . Thus  $d - 1 \in \mathbf{a}_v$  and  $1 - d^2 \mu^2 - e_v \in e_v \mathbf{a}_v$ , so that  $(1 - d^2 \mu^2) \mathbf{g}_v = e_v \mathbf{g}_v$ . We easily see that  $d \in \mathbf{g}$ . Therefore we can take  $1 - d^2 \mu^2$  as  $a$  of (2) to find that  $1 - d^2 \mu^2 = \varphi[k]$  with  $k \in M$ . Put  $y = dw + k$ . Then  $y \in L$  and  $\varphi[y] = 1$ . For  $v \in \mathbf{p}$  we have  $k \in M_v \subset \mathbf{a}_v L_v$ ,  $w \in L_v$ , and  $d - 1 \in \mathbf{a}_v$ , and so  $y - x_v \in \mathbf{a}_v L_v$ . Thus  $y$  gives the desired element of our theorem.

**Corollary 32.13.** *Let  $B$  be a quaternion algebra over a global field  $F$  such that  $B_u \cong M_2(F_u)$  for some  $u \in \mathbf{a}$ , and  $\beta$  the norm form on  $B$ . Then the following assertions hold.*

(i) *Let  $\mathfrak{o}$  be an order in  $B$ ,  $\mathbf{a}$  an integral  $\mathbf{g}$ -ideal, and  $\mathbf{p}$  the set of the prime factors of  $\mathbf{a}$ ; let  $a$  be an element of  $F^\times \cap \beta[B]$  such that  $a \in \beta[\mathfrak{o}_v]$  for every  $v \in \mathbf{h}, \notin \mathbf{p}$ . Given  $(\xi_v) \in \prod_{v \in \mathbf{p}} B_v$  such that  $\beta[\xi_v] = a$ , there exists an element  $\alpha$  of  $B$  such that  $\beta[\alpha] = a$ ,  $\alpha \in \mathfrak{o}_v$  for every  $v \in \mathbf{h}, \notin \mathbf{p}$ , and  $\alpha - \xi_v \in \mathbf{a}_v \mathfrak{o}_v$  for every  $v \in \mathbf{p}$ .*

(ii) *Let  $B^1 = \{\gamma \in B^\times \mid \gamma\gamma^t = 1\}$ . Then  $B_{\mathbf{A}}^1 = DB^1$  for every open subgroup of  $B_{\mathbf{A}}^1$  containing  $B_{\mathbf{a}}^1$ . (See §30.7 for the notation.)*

PROOF. Take  $(V, \varphi)$  of Theorem 32.12 to be  $(B, \beta)$ . Then we immediately obtain (i). To prove (ii), put  $U = \{y \in B_{\mathbf{A}}^1 \mid \mathfrak{o}y = \mathfrak{o}\}$  and  $W = \{w \in U \mid w_v - 1 \in \mathfrak{a}\mathfrak{o}_v \text{ for every } v \in \mathbf{h}\}$ . Given  $D$  as in (ii), we can take  $\mathbf{a}$  so that  $W \subset D$ , and so it is sufficient to prove that  $B_{\mathbf{A}}^1 = WB^1$ . Let  $\zeta \in U$ . By (i), we can find  $\alpha \in B^1$  such that  $\alpha \in \mathfrak{o}_v$  for every  $v \in \mathbf{h}, \notin \mathbf{p}$ , and  $\alpha - \zeta_v \in \mathfrak{a}\mathfrak{o}_v$  for every  $v \in \mathbf{p}$ . Then  $\alpha \in \mathfrak{o}_v$  for every  $v \in \mathbf{h}$ , and so  $\alpha \in \mathfrak{o}$ . Since  $\alpha\alpha^t = 1$ , we have  $\alpha \in \mathfrak{o}^\times$ . Put  $\eta = \zeta\alpha^{-1}$ . Then  $\eta \in W$ . Thus  $\zeta = \eta\alpha \in WB^1$ . This shows that  $U \subset WB^1$ . Therefore we have only to prove that  $B_{\mathbf{A}}^1 \subset UB^1$ . Given  $\xi \in B_{\mathbf{A}}^1$ , take an integral ideal  $\mathbf{a}$  such that  $\mathfrak{a}\mathfrak{o}_v \subset \mathfrak{o}_v \xi_v$  for every  $v \in \mathbf{h}$ , and let  $\mathbf{p}$  be the set of the prime factors of  $\mathbf{a}$ . If  $v \notin \mathbf{p}$ , we have  $\mathfrak{o}_v \subset \mathfrak{o}_v \xi_v$ , and so  $\xi_v^t \in \mathfrak{o}_v \xi_v^t \subset \mathfrak{o}_v$ , which means that  $\xi_v \in \mathfrak{o}_v$ . Thus  $\mathfrak{o}_v = \mathfrak{o}_v \xi_v$  for  $v \notin \mathbf{p}$ . By (i) there exists an element  $\gamma \in B^1$  such that  $\gamma - \xi_v \in \mathbf{a}^2 \mathfrak{o}_v$  if  $v \in \mathbf{p}$  and  $\gamma \in \mathfrak{o}_v$  if  $v \notin \mathbf{p}$ . By Lemma 32.2, we have  $\mathfrak{o}_v \gamma = \mathfrak{o}_v \xi_v$  if  $v \in \mathbf{p}$  and  $\gamma \in \mathfrak{o}_v^\times$  if  $v \notin \mathbf{p}$ .

Thus  $\mathfrak{o}_v\gamma = \mathfrak{o}_v\xi_v$  for every  $v \in \mathbf{h}$ , and so  $\xi\gamma^{-1} \in U$ . Therefore,  $\xi \in U\gamma$ , which shows that  $B_{\mathbf{A}}^1 \subset UB^1$  as expected. This completes the proof.

**32.14.** Notice that (i) of the above corollary is similar to Theorem 10.21, and (ii) to Theorem 30.9. Thus the above corollary shows that *strong approximation holds for  $B^1$  with a quaternion algebra  $B$  over  $F$  such that  $B_u \cong M_2(F_u)$  for some  $u \in \mathbf{a}$* . We now prove strong approximation for  $S^\circ(V, \varphi)$  with an indefinite  $\varphi$  in the sense stated in the following theorem, where  $S^\circ$  is defined in (24.8). The theorem as well as the above corollary are due to Eichler.

Before stating the result, we note that the map  $\tau : G^+(V) \rightarrow SO^\varphi(V)$  is defined by rational expressions in matrix entries, and so defines a continuous map of  $G^+(V)_v$  to  $SO^\varphi(V)_v$  for every  $v \in \mathbf{v}$ . This is so for every homomorphism of an algebraic group into another defined by rational expressions. To be explicit, fix  $v \in \mathbf{h}$  and a lattice  $L$  in  $V$ . Let  $R$  be an order in  $A(V)$ . Then the continuity of  $\tau : G^+(V)_v \rightarrow SO^\varphi(V)_v$  can be stated as follows: *Given  $\alpha, \beta \in G^+(V)_v$  and an integral  $\mathfrak{g}$ -ideal  $\mathfrak{a}$  such that  $\mathfrak{a}_v \neq \mathfrak{g}_v$ , there exists a positive integer  $\nu$  such that*

$$(32.1) \quad \alpha - \beta \in \mathfrak{a}^\nu R_v \implies L_v(\tau(\alpha) - \tau(\beta)) \subset \mathfrak{a}L_v.$$

The following theorem and Theorem 32.17 below are called **strong approximation** in  $S^\circ(V)$  and  $SO^\varphi(V)$ ; they are due to Eichler; see [E52a] and [K].

**Theorem 32.15.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space of dimension  $n \geq 3$  over a global field  $F$  such that  $\varphi_u$  is indefinite for some  $u \in \mathbf{a}$ . Let  $L$  be a lattice in  $V$ ,  $\mathfrak{a}$  an integral  $\mathfrak{g}$ -ideal, and  $\mathbf{p}$  the set of the prime factors of  $\mathfrak{a}$ . Given  $(\xi_v) \in \prod_{v \in \mathbf{p}} S^\circ(V_v)$ , there exists an element  $\alpha$  of  $S^\circ(V)$  such that  $L_v\alpha = L_v$  for every  $v \in \mathbf{h}, \notin \mathbf{p}$ , and  $L_v(\alpha - \xi_v) \subset \mathfrak{a}L_v$  for every  $v \in \mathbf{p}$ .*

PROOF. We first note that  $G^c(V_v) = S^\circ(V_v)$  for every  $v \in \mathbf{h}$ , where  $G^c(\ )$  is defined in §24.10. Indeed, if  $\varphi_v$  is isotropic or  $n = 3$ , the fact is proved in Lemma 24.13. If  $n > 3$  and  $\varphi_v$  is anisotropic, then by Theorem 25.4(ii),  $(V, \varphi)_v$  is isomorphic to  $(B, \beta)$  with a division quaternion algebra  $B$  over  $F_v$ , and so (iv) of the same theorem gives the equality.

To prove our theorem, we naturally assume that  $\mathfrak{a} \neq \mathfrak{g}$  and denote by  $\mathfrak{a}_1, \mathfrak{a}_2, \dots$ , etc., sufficiently high powers of  $\mathfrak{a}$  chosen suitably in each instance so that the continuity property similar to (32.1) holds, so that we will eventually obtain the desired result at the end. We may also assume that  $L$  is maximal.

We first assume that  $n \geq 4$  and consider  $\zeta_v = \tau(x_v y_v x_v y_v)$  with invertible  $x_v, y_v \in V_v$  given for each  $v \in \mathbf{h}$ . We can find invertible  $x, y \in V$  such that

$x - x_v \in \mathfrak{a}_1 L_v$  and  $y - y_v \in \mathfrak{a}_1 L_v$  for every  $v \in \mathbf{p}$ . (Since  $V \cong F_n^1$ , this follows from Lemma 15.3(ii), or even from Theorem 1.3.) Put  $w = x\tau(y)$ . Then  $\tau(x)\tau(w) = \tau(x)\tau(y)\tau(x)\tau(y)$ ,  $\varphi[x] = \varphi[w]$ , and  $L_v(\tau(xw) - \zeta_v) \subset \mathfrak{a}_2 L_v$  for every  $v \in \mathbf{p}$ . We are going to find  $\alpha \in S^\circ(V)$  such that

$$(1) \quad L_v \alpha = L_v \text{ if } v \in \mathbf{h}, \notin \mathbf{p}, \text{ and } L_v(\alpha - \tau(\zeta_v)) \subset \mathfrak{a}_2 L_v \text{ if } v \in \mathbf{p}.$$

Replacing  $x$  and  $w$  by their suitable scalar multiples, we may assume that  $x, w \in L$ , and still with  $\varphi[x] = \varphi[w]$ . Put  $\mathbf{p}' = \{v \in \mathbf{h} \mid v \notin \mathbf{p}, \varphi[x] \notin \mathfrak{g}_v^\times\}$ . By Theorem 32.12, there exists an element  $z$  of  $V$  such that  $\varphi[z] = \varphi[x]$ ,  $z \in L_v$  for  $v \in \mathbf{h}, \notin \mathbf{p} \cup \mathbf{p}'$ ,  $z - w \in \mathfrak{a}_3 L_v$  for  $v \in \mathbf{p}$ , and  $z - x \in \mathfrak{a}_3 L_v$  for  $v \in \mathbf{p}'$ . Then  $z \in L$ ,  $L_v(\tau(z) - \tau(w)) \subset \mathfrak{a}_4 L_v$  for  $v \in \mathbf{p}$  and  $L_v(\tau(z) - \tau(x)) \subset \mathfrak{a}_4 L_v$  for  $v \in \mathbf{p}'$ . Put  $\alpha = \tau(x)\tau(z)$ . Then  $\sigma(\alpha) = \varphi[x]^2$ , and so  $\alpha \in S^\circ(V)$ . Also,  $L_v(\alpha - \tau(xw)) \subset \mathfrak{a}_2 L_v$  for  $v \in \mathbf{p}$  and  $L_v(\alpha - 1) \subset \mathfrak{a}_2 L_v$  for  $v \in \mathbf{p}'$  (if we choose  $\mathfrak{a}_3$  and  $\mathfrak{a}_4$  so that  $\mathfrak{a}_4 L \tau(x) \subset \mathfrak{a}_2 L$ ). Then  $L_v(\alpha - \tau(\zeta_v)) \subset \mathfrak{a}_2 L_v$  for  $v \in \mathbf{p}$ . By Lemma 32.2,  $L_v \alpha = L_v$  for  $v \in \mathbf{p}'$ . For  $v \notin \mathbf{p} \cup \mathbf{p}'$  we have  $\varphi[x] \in \mathfrak{g}_v^\times$ , and so  $L_v \tau(x) = L_v \tau(w) = L_v$  by Lemma 29.5. Thus  $L_v \alpha = L_v$  for every  $v \in \mathbf{h}, \notin \mathbf{p}$ , and  $\alpha$  as in (1) has been obtained.

Now, given  $\xi_v$  as in our theorem, we express  $\xi_v$  for each  $v \in \mathbf{p}$  as a product  $\zeta_{v1} \cdots \zeta_{vr}$  of commutators  $\zeta_{vi}$ , each of which is of the type  $\tau(x_v y_v x_v y_v)$  discussed above, since  $S^\circ(V_v) = G^c(V_v)$ ; see Lemma 24.11. The number  $r$  may depend on  $v$ , but we may assume that  $r$  is the same for all  $v \in \mathbf{p}$ , since we can insert  $1 = \tau(xxxx)$  as many as we like. Then by (1), for  $1 \leq i \leq r$  we can find  $\alpha_i \in S^\circ(V)$  such that  $L_v \alpha_i = L_v$  for every  $v \in \mathbf{h}, \notin \mathbf{p}$ , and  $L_v(\alpha_i - \zeta_{vi}) \subset \mathfrak{a}_2 L_v$  for every  $v \in \mathbf{p}$ . Then  $\alpha_1 \cdots \alpha_r$  gives the element  $\alpha$  of  $S^\circ(V)$  with the required properties of our theorem. This completes the proof in the case  $n \geq 4$ .

Let us finally consider the case  $n = 3$ . By lemma 25.2(ii), there is a quaternion algebra  $B$  over  $F$  such that  $(V, \varphi) \cong (B^\circ, cB^\circ)$  with  $c \in F^\times$ . Then  $G^+(V) = B^\times$ ,  $x\tau(b) = b^{-1}xb$  for  $x \in V = B^\circ$  and  $b \in B^\times$ , and  $S^\circ(V) = \tau(B^1)$  with  $B^1 = \{\gamma \in B^\times \mid \gamma\gamma^t = 1\}$ , as noted in (25.3b). Given  $(\xi_v) \in \prod_{v \in \mathbf{p}} S^\circ(V_v)$ , take  $\gamma_v \in B_v^1$  so that  $\xi_v = \tau(\gamma_v)$ . Take a maximal order  $\mathfrak{o}$  in  $B$  and put  $L = \mathfrak{o} \cap B^\circ$ . By Corollary 32.13 we can find  $y \in B^1$  such that  $y - \gamma_v \in \mathfrak{a}_5 \mathfrak{o}_v$  for every  $v \in \mathbf{p}$  and  $y \in \mathfrak{o}_v$  for  $v \in \mathbf{h}, \notin \mathbf{p}$ . Since  $yy^t = 1$ , we have  $y \in \mathfrak{o}_v^\times$  for  $v \in \mathbf{h}, \notin \mathbf{p}$ . Put  $\alpha = \tau(y)$ . Then  $\alpha \in S^\circ(B^\circ)$  and  $L_v \alpha = y^{-1}(\mathfrak{o} \cap B^\circ)_v y = (\mathfrak{o} \cap B^\circ)_v = L_v$  for  $v \in \mathbf{h}, \notin \mathbf{p}$ . Also,  $L_v(\alpha - \xi_v) = L_v(\tau(y) - \tau(\gamma_v)) \subset \mathfrak{a}_1 L_v$  for every  $v \in \mathbf{p}$  if  $\mathfrak{a}_5$  is taken suitably. This settles the case  $n = 3$ , and completes the proof of our theorem.

**32.16.** Still with  $(V, \varphi)$  over a global field  $F$ , following the general principle of §30.7, we can define  $V_{\mathbf{A}}$ ,  $A(V)_{\mathbf{A}}$ , and  $A(V)_{\mathbf{A}}^\times$ . Then  $G(V)_{\mathbf{A}}$ ,  $G^+(V)_{\mathbf{A}}$ , and  $G^1(V)_{\mathbf{A}}$  can be defined as subgroups of  $A(V)_{\mathbf{A}}^\times$ . To be explicit, take an arbitrary order  $R$  in  $A(V)$ . Then

$$G^+(V)_{\mathbf{A}} = \left\{ (x_v)_{v \in \mathbf{v}} \in \prod_{v \in \mathbf{v}} G^+(V_v) \mid x_v \in R_v^\times \text{ for almost all } v \in \mathbf{h} \right\}.$$

The topology is defined so that  $G^+(V)_{\mathbf{A}} \prod_{v \in \mathbf{h}} [G^+(V_v) \cap R_v^\times]$  is an open (locally compact) subgroup, whose topology is the product topology; here  $G^+(V)_{\mathbf{A}} = \prod_{v \in \mathbf{A}} G^+(V_v)$ . All these are valid with  $G(V)$  or  $G^1(V)$  in place of  $G^+(V)$ .

We can extend  $\tau : G^+(V) \rightarrow SO^\varphi$  and  $\nu : G^+(V) \rightarrow F^\times$  to the maps

$$(32.2) \quad \tau : G^+(V)_{\mathbf{A}} \rightarrow SO_{\mathbf{A}}^\varphi \quad \text{and} \quad \nu : G^+(V)_{\mathbf{A}} \rightarrow F_{\mathbf{A}}^\times.$$

Indeed, for  $x = (x_v)_{v \in \mathbf{v}} \in G^+(V)_{\mathbf{A}}$  we put formally  $\tau(x) = (\tau(x_v))_{v \in \mathbf{v}}$  and  $\nu(x) = (\nu(x_v))_{v \in \mathbf{v}}$ . The notation being as in Lemma 29.13, we have  $x_v \in X_v$  and  $\tau(x_v) \in C_v$  for almost all  $v \in \mathbf{h}$ , and so  $\tau(x) \in SO_{\mathbf{A}}^\varphi$ . Also, since  $A(L)$  is stable under the canonical involution, we see that  $x_v^* \in A(L)_v^\times$ , and so  $\nu(x_v) = x_v x_v^* \in A(L)_v^\times \cap F_v = \mathfrak{g}_v^\times$ , which shows that  $\nu(x) \in F_{\mathbf{A}}^\times$ .

We now define a homomorphism

$$(32.3) \quad \sigma : SO_{\mathbf{A}}^\varphi \longrightarrow F_{\mathbf{A}}^\times / F_{\mathbf{A}}^{\times 2}$$

as follows. Since  $\tau : G^+(V)_v \rightarrow SO_v^\varphi$  is surjective for every  $v \in \mathbf{v}$ , we see from Lemma 29.13 that  $\tau$  of (32.2) is surjective. Therefore, given  $\alpha \in SO_{\mathbf{A}}^\varphi$ , we can find an element  $\xi \in G^+(V)_{\mathbf{A}}$  such that  $\tau(\xi) = \alpha$ . Then we define  $\sigma(\alpha)$  to be the element of  $F_{\mathbf{A}}^\times / F_{\mathbf{A}}^{\times 2}$  represented by  $\nu(\xi)$ . Clearly this is well defined. For expediency, we will often denote by  $\sigma(\alpha)$  any element of  $F_{\mathbf{A}}^\times$  that represents it. We can view this map as an extension of the homomorphism  $\sigma : SO^\varphi \rightarrow F^\times / F^{\times 2}$  of (24.7). (Since  $F^{\times 2} = F^\times \cap F_{\mathbf{A}}^{\times 2}$ , we can view  $F^\times / F^{\times 2}$  as a subgroup of  $F_{\mathbf{A}}^\times / F_{\mathbf{A}}^{\times 2}$ .) Restricting the map of (32.3) to  $SO_v^\varphi$ , we obtain a map  $SO_v^\varphi \rightarrow F_v^\times / F_v^{\times 2}$  for each  $v \in \mathbf{v}$ . We put

$$(32.4) \quad S^\circ(V)_{\mathbf{A}} = \{\alpha \in SO_{\mathbf{A}}^\varphi \mid \sigma(\alpha) = 1\}.$$

Here we are abusing the notation, since  $S^\circ(V)_{\mathbf{A}}$  is *not* the adelization of the group  $S^\circ(V)$  of (24.8); it is merely defined as a subgroup of  $SO_{\mathbf{A}}^\varphi$  by the last equality.

We will be considering the image  $\sigma(X)$  of a subgroup  $X$  of  $SO^\varphi$ . To simplify our notation, we will denote by  $\sigma(X)$  the subgroup of  $F^\times$  containing  $F^{\times 2}$  such that  $\sigma(X)/F^{\times 2}$  is the image of  $X$  in the strict sense. We understand  $\sigma(X)$  for a subgroup  $X$  of  $SO_v^\varphi$  or  $SO_{\mathbf{A}}^\varphi$  in a similar way.

**Theorem 32.17.** *Suppose that  $n \geq 3$  and  $O_{\mathbf{A}}^\varphi$  is not compact. Let  $D$  be an open subgroup of  $SO_{\mathbf{A}}^\varphi$  containing  $SO_{\mathbf{A}}^\varphi$ . Then  $S^\circ(V)_{\mathbf{A}} \subset S^\circ(V)D$ . Moreover, for every  $y \in SO_{\mathbf{A}}^\varphi$  we have*

$$(32.4a) \quad SO_{\mathbf{A}}^\varphi y D = \{x \in SO_{\mathbf{A}}^\varphi \mid \sigma(y^{-1}x) \in F^\times \sigma(D)\}.$$

PROOF. For simplicity put  $G = SO^\varphi$  and  $S^\circ = S^\circ(V)$ . Clearly it is sufficient to prove the case in which  $D$  is given in the form



$$D = \{y \in G_{\mathbf{A}} \mid \Lambda y = \Lambda, \Lambda_v(y_v - 1) \subset \mathfrak{a}\Lambda_v \text{ for every } v \in \mathbf{h}\}$$

with a  $\mathfrak{g}$ -lattice  $\Lambda$  in  $V$  and an integral ideal  $\mathfrak{a}$ . Given  $x \in S_{\mathbf{A}}^{\circ}$ , put  $\mathbf{p} = \{v \in \mathbf{h} \mid x_v \notin D_v\}$ . This is a finite set. By Theorem 32.15 we can find an element  $\alpha \in S^{\circ}$  such that  $\Lambda_v \alpha = \Lambda_v$  if  $v \notin \mathbf{p}$  and  $\Lambda_v(\alpha - x_v) \subset \pi_v \mathfrak{a} \Lambda_v x_v$  if  $v \in \mathbf{p}$ , where  $\pi_v$  is a prime element of  $F_v$ . Then  $\Lambda_v \alpha = \Lambda_v x_v$  by Lemma 32.2 for  $v \in \mathbf{p}$ , and consequently for every  $v \in \mathbf{h}$ . Thus  $\alpha x^{-1} \in D$ , which proves that  $S_{\mathbf{A}}^{\circ} \subset S^{\circ} D$ .

Next, taking  $yDy^{-1}$  in place of  $D$ , we have  $S_{\mathbf{A}}^{\circ} \subset S^{\circ} yDy^{-1} \subset GyDy^{-1}$ . Suppose  $\sigma(y^{-1}x) \in F^{\times} \sigma(D)$ ; then  $\sigma(y^{-1}xd^{-1}) = aF_{\mathbf{A}}^{\times 2}$  with  $a \in F$  and  $d \in D$ . We see that  $a \in \sigma(G_v)$  for every  $v \in \mathbf{a}$ . The set  $\sigma(G_v)$ , viewed as a subset of  $F_v^{\times}$ , consists of the nonzero products  $\varphi[z_1] \cdots \varphi[z_{2m}]$  with  $z_i \in V_v$ , and so coincides with  $\{t \in \mathbf{R} \mid t > 0\}$  if  $v$  is real and  $\varphi_v$  is definite. Otherwise  $\sigma(G_v) = F_v^{\times}$ . Let us now show that  $a = \nu(\gamma)$  for some  $\gamma \in G^+(\varphi)$ . If  $n = 3$ , then by Lemma 25.2(ii),  $G^+(\varphi) = B^{\times}$  with a quaternion algebra  $B$  over  $F$  such that  $B_v \cong \mathbf{H}$  for  $v \in \mathbf{a}$  if and only if  $v$  is real and  $\varphi_v$  is definite. Applying Corollary 27.5 to  $(B, \beta)$ , we find an element  $\gamma \in B^{\times}$  such that  $\nu(\gamma) = a$ . Next suppose  $n > 3$ . Take any  $\xi \in V$  such that  $\varphi[\xi] \neq 0$ . By Corollary 27.5 there is an element  $\eta \in V$  such that  $\varphi[\eta] = a\varphi[\xi]^{-1}$ . Then  $a = \nu(\gamma)$  with  $\gamma = \xi\eta$ . Thus for  $n \geq 3$  we can put  $a = \nu(\gamma)$  with  $\gamma \in G^+(\varphi)$ . Put  $\alpha = \tau(\gamma)$ . Then  $\alpha \in G$ ,  $\sigma(\alpha) = a$ , and  $\sigma(\alpha^{-1}xd^{-1}y^{-1}) = 1$ . Thus  $\alpha^{-1}xd^{-1}y^{-1} \in S_{\mathbf{A}}^{\circ} \subset GyDy^{-1}$ , and so  $x \in GyD$ . This proves (32.4a), since  $\sigma(y^{-1}GyD) \subset F^{\times} \sigma(D)$ .

**Lemma 32.18.** (i) *Given  $(V, \varphi)$  over a global field  $F$  as before, let  $C = \{x \in SO_{\mathbf{A}}^{\varphi} \mid Lx = L\}$  with a maximal lattice  $L$  in  $V$ . Then  $\prod_{v \in \mathbf{h}} \mathfrak{g}_v^{\times} \subset \sigma(C)$ , provided  $n \geq 3$ .*

(ii) *With  $(V, \varphi)$  as above, suppose  $F = \mathbf{Q}$ ,  $\varphi$  is indefinite, and  $n \geq 3$ . Then  $\sigma(SO^{\varphi}) = \mathbf{Q}^{\times}$  and  $\sigma(SO_{\mathbf{a}}^{\varphi}) = \mathbf{R}^{\times}$ .*

**PROOF.** To prove (i), take  $v \in \mathbf{h}$  and assume that  $\varphi_v$  is isotropic. Then from Lemma 29.8 we see that  $\varphi[L_v] = \mathfrak{g}_v$ . Thus for every  $a \in \mathfrak{g}_v^{\times}$  there exists an element  $x \in L_v$  such that  $\varphi[x] = a$ , and also  $y \in L_v$  such that  $\varphi[y] = 1$ . Then  $\sigma(\tau(xy)) = a$ . Suppose  $\varphi$  is anisotropic and  $n = 4$ . Then by Theorem 25.4(ii),  $(V, \varphi)_v \cong (B, \beta)$  with a division quaternion algebra  $B$  over  $F_v$  and  $L_v = \mathfrak{o}$  with the maximal order  $\mathfrak{o}$  in  $B$  as shown in §29.10. By Theorems 21.21 and 21.23(i) we have  $\mathfrak{g}_v = \varphi[L_v]$  in this case, and so the argument in the isotropic case is applicable. Suppose  $\varphi$  is anisotropic and  $n = 3$ . By Theorem 25.2(ii),  $(V, \varphi)_v \cong (B^{\circ}, d\beta^{\circ})$  with  $d \in F_v^{\times}$  and  $B$  as in the case  $n = 4$ , and  $G^+(V) = B^{\times}$ . Given any  $c \in \mathfrak{g}_v^{\times}$ , by Theorem 21.23(i) there exists an element  $z \in B^{\times}$  such that  $zz^t = c$ ; similarly  $ww^t = 1$  for some  $w \in B^{\times}$ . Then  $L_v \tau(z) = L_v \tau(w) = L_v$  by Lemma 29.7. Since  $\sigma(\tau(zw)) = c$ , we obtain the desired result. This proves (i).



The proof of (ii) is similar. Suppose  $n \geq 4$ . By Corollary 27.5, for every  $a \in \mathbf{Q}^\times$  there exist elements  $x, y \in V$  such that  $\varphi[x] = a$  and  $\varphi[y] = 1$ . Then  $\sigma(\tau(xy)) = a$ . Suppose  $n = 3$ . By Lemma 25.2(ii) we can put  $(V, \varphi) = (B^\circ, -\delta\beta^\circ)$  with a quaternion algebra  $B$  over  $\mathbf{Q}$ , and  $G^+(V) = B^\times$ . Since  $\varphi$  is indefinite,  $B_{\mathbf{A}} \cong M_2(\mathbf{R})$ . Therefore, for every  $c \in \mathbf{Q}^\times$  the Hasse principle (combined with Theorem 21.23(i)) guarantees an element  $z$  of  $B$  such that  $zz^t = c$ . Then  $\sigma(\tau(z)) = zz^t = c$ , and so  $\sigma(SO^\varphi) = \mathbf{Q}^\times$ . That  $\sigma(SO_{\mathbf{A}}^\varphi) = \mathbf{R}^\times$  can be proved in a similar way.

**Theorem 32.19.** (i) *Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $\mathbf{Q}$  of dimension  $n \geq 3$  such that  $\varphi$  is indefinite. Given a lattice  $L$  in  $V$ , let  $D = \{x \in SO_{\mathbf{A}}^\varphi \mid Lx = L\}$ . If  $\mathbf{Z}_p^\times \subset \sigma(D)$  for every prime number  $p$ , then the  $\varphi$ -genus of  $L$  consists of a single  $SO^\varphi$ -class. In particular, the genus of maximal lattices in  $V$  consists of a single  $SO^\varphi$ -class.*

(ii) *Let  $\Phi$  be a  $q$ -reduced element of  $2^{-1}T_n(\mathbf{Z})$  such that  $|s(\Phi)| \neq n \geq 3$ . If  $\Psi \in 2^{-1}T_n(\mathbf{Z})$  and  $\Psi = \alpha\Phi \cdot {}^t\alpha$  with  $\alpha \in GL_n(\mathbf{Q})$ , then such an  $\alpha$  can be taken from  $\alpha \in SL_n(\mathbf{Z})$ .*

PROOF. To prove (i), put  $G = SO^\varphi$ . Suppose  $\mathbf{Z}_p^\times \subset \sigma(D)$  for every  $p$ . Then by Lemma 32.18(ii) we have  $\sigma(DG) \supset \mathbf{Q}^\times \mathbf{R}^\times \prod_p \mathbf{Z}_p^\times = \mathbf{Q}_{\mathbf{A}}^\times$ ; see (15.6a). Let  $y \in G_{\mathbf{A}}$ . Then  $\sigma(y) = \sigma(x\alpha)$  with  $\alpha \in G$  and  $x \in D$ . Thus  $x^{-1}y\alpha^{-1} \in S^\circ(V)_{\mathbf{A}} \subset DS^\circ(V)$  by Theorem 32.17, and so  $y \in xDS^\circ(V)\alpha \subset DG$ , which means that  $G_{\mathbf{A}} = DG$ , that is,  $\#(D \backslash G_{\mathbf{A}}/G) = 1$ . This proves the first part of (i) for the reason explained at the end of §30.7. In view of Lemma 32.18(i), our result is applicable to a maximal lattice, and so we obtain the latter part of (i).

As for (ii), the isomorphism class of  $\langle \mathbf{Q}, \Phi \rangle$  with a  $q$ -reduced  $\Phi$  determines the genus of  $\Phi$  as explained in the second paragraph of §31.1, and so if  $\Psi$  is  $q$ -reduced and  $\Psi = \alpha\Phi \cdot {}^t\alpha$  with  $\alpha \in GL_n(\mathbf{Q})$ , then  $\Psi$  belongs to the genus of  $\Phi$ . Therefore, by (i),  $\Psi$  belongs to the  $SO$ -class of  $\Phi$ . This proves (ii).

**32.20.** As a consequence of the above theorem we see that if  $|\sigma| \neq n \geq 3$ , then the number of genera in Theorem 31.9 is actually the number of  $SO$ -classes of the matrices  $\Phi \in \mathfrak{S}_n^0$  in question. For instance, we obtain the following results, in which a class means an  $SO$ -class and we assume that  $n \geq 3$ ,  $|\sigma| < n$ , and  $\sigma - n \in 2\mathbf{Z}$ :

(32.5a) *If  $\sigma \in 8\mathbf{Z}$ , then there exists a unique class of symmetric matrices  $\psi \in T_n(\mathbf{Z})$  such that  $\det(\psi) = 1$  and  $s(\psi) = \sigma$ .*

(32.5b) *If  $\sigma \pm 1 \in 8\mathbf{Z}$ , then there exists a unique class of symmetric matrices  $\psi \in T_n(\mathbf{Z})$  such that  $\det(\psi) = 2$  and  $s(\psi) = \sigma$ .*

(32.5c) *If  $f$  is an odd prime number,  $n \in 2\mathbf{Z}$ , and  $\sigma - f + 1 \in 4\mathbf{Z}$ , then there exists a unique class of symmetric matrices  $\psi \in T_n(\mathbf{Z})$  such*

that  $\det(\psi) = f$  and  $s(\psi) = \sigma$ .

(32.5d) If  $m$  is an odd prime number and  $n - 1 \in 2\mathbf{Z}$ , then there exists a unique class of symmetric matrices  $\psi \in T_n(\mathbf{Z})$  such that  $\det(\psi) = 2m$  and  $s(\psi) = \sigma$ .

More generally, the number of genera mentioned after (31.8c, d) is actually the number of classes, and the genus of  $\Phi$  in Theorem 31.9 becomes the  $SO$ -class of  $\Phi$ , provided  $|\sigma| \neq n \geq 3$ .

In fact we can state a result about  $\#(D \backslash SO_{\mathbf{A}}^{\varphi} / SO^{\varphi})$  for  $(V, \varphi)$  over an arbitrary global field  $F$  such that  $SO_{\mathbf{a}}^{\varphi}$  is not compact and  $n \geq 3$ . We refer the reader to Theorem 9.26 of [S04b]. In that theorem a certain condition (9.2) is assumed in the last statement of the theorem, but that is actually unnecessary, as explained in [S06c, Remark 2.4, (5)].

### 33. Integer-valued symmetric forms

**33.1.** As we said in §31.1, there is a great difference between quadratic forms and symmetric forms when they are discussed over the ring of integers. We have treated  $q$ -reduced quadratic forms in previous sections, and our next task is the discussion of  $s$ -reduced symmetric forms in the sense of (31.3).

Thus we take a local or global field  $F$  and its maximal order  $\mathfrak{g}$ . We consider  $S_n(\mathfrak{g})$ , that is, the set of all symmetric elements of  $M_n(\mathfrak{g}) \cap GL_n(F)$ . In §31.4 we divided the elements of  $S_n(\mathfrak{g})$  into two types, that is, Type 1 and Type 2. For  $\lambda = 1$  or  $2$  we denote by  $S_n^{\lambda}(\mathfrak{g})$  the set of all  $s$ -reduced elements of  $S_n(\mathfrak{g})$  of Type  $\lambda$ . If  $F$  is local and  $2 \in \mathfrak{g}^{\times}$ , then clearly  $S_n^1(\mathfrak{g}) = \emptyset$  and  $S_n^2(\mathfrak{g})$  consists of all the  $q$ -reduced elements of  $T_n(\mathfrak{g})$ , which correspond to maximal lattices. Therefore the problem about  $s$ -reduced matrices over a local field with  $2 \in \mathfrak{g}^{\times}$  is already settled by what we have done in Sections 29 through 32. If  $2 \in \mathfrak{p}$ , however, the matter is far more complicated. Indeed, we easily see that

$$(33.1) \quad \psi \in S_n^2(\mathfrak{g}) \implies 2^{-1}\psi \text{ is } q\text{-reduced.}$$

But the converse is false if  $2 \in \mathfrak{p}$ . Take for example  $\mathfrak{g} = \mathbf{Z}_2$  (or even  $\mathfrak{g} = \mathbf{Z}$ ), and  $\psi = 2 \cdot 1_2$ . Clearly  $1_2$  is the matrix representing the norm form of  $\mathbf{Q}_2(\sqrt{-1})$  with respect to the basis  $\{1, \sqrt{-1}\}$ , and  $\mathbf{Z}_2 + \mathbf{Z}_2\sqrt{-1}$  is a maximal lattice, and so  $1_2$  is  $q$ -reduced. However, we have

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix},$$

which shows that  $2 \cdot 1_2$  is not  $s$ -reduced. It should also be noted that  $\varphi = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$  is  $s$ -reduced and belongs to  $S_2^1(\mathbf{Z}_2)$ ; also,  $\varphi$  is  $q$ -reduced. Indeed, if  $\varphi = {}^t\alpha\xi\alpha$  with  $\xi \in 2^{-1}T_2(\mathbf{Z}_2)$  and  $\alpha \in M_2(\mathbf{Z}_2)$ ,  $\notin GL_2(\mathbf{Z}_2)$ , then  $\det(2\xi) \in \mathbf{Z}_2^{\times}$ , which contradicts (29.7).

Let us now state more general results in the local case.

**Lemma 33.2.** *Suppose  $F$  is local and  $2 \in \mathfrak{p}$ ; then the following assertions hold:*

- (i) *Let  $\sigma = \text{diag}[\sigma_1, \dots, \sigma_r] \in S_n(\mathfrak{g})$  with  $\sigma_i$  as in Lemma 32.5. Suppose  $\sigma$  is  $s$ -reduced. Then every  $\sigma_i$  of size 2 belongs to  $GL_2(\mathfrak{g})$  and there is at most one  $\sigma_i$  of size 1 not contained in  $\mathfrak{g}^\times$ ; such a  $\sigma_i$  not contained in  $\mathfrak{g}^\times$  is a prime element of  $F$ . Moreover, every  $\sigma_i$  of size 2 belongs to  $T_2(\mathfrak{g})$  if  $\mathfrak{p} = 2\mathfrak{g}$ .*
- (ii) *An element  $\sigma$  of  $S_n(\mathfrak{g})$  is  $s$ -reduced if and only if  $\sigma \in GL_n(\mathfrak{g})$  or  $\det(\sigma)\mathfrak{g} = \mathfrak{p}$ .*

PROOF. Suppose  $\sigma_i = \begin{bmatrix} a & b \\ b & d \end{bmatrix}$  and  $a\mathfrak{g} + d\mathfrak{g} \subsetneq b\mathfrak{g} \neq \{0\}$ . If  $b \in \mathfrak{p}$ , then  $\alpha\sigma_i \cdot {}^t\alpha \in S_n(\mathfrak{g})$  for  $\alpha = \text{diag}[1, \pi^{-1}]$  with a prime element  $\pi$ , and so  $\sigma$  cannot be  $s$ -reduced. Therefore if  $\sigma$  is  $s$ -reduced, then  $b \in \mathfrak{g}^\times$ , and so  $\sigma_i \in GL_2(\mathfrak{g})$ ; clearly  $\sigma_i \in T_2(\mathfrak{g})$  if  $\mathfrak{p} = 2\mathfrak{g}$ . Similarly  $\sigma$  cannot be  $s$ -reduced if  $\sigma_i \in \mathfrak{p}^2$  for some  $i$ . Thus every  $\sigma_i$  of size 1 belongs to  $\mathfrak{g}^\times$  or is a prime element of  $F$ . Suppose  $\sigma_1$  and  $\sigma_2$  are prime elements. By Lemma 21.12(iii) we have  $-\sigma_2/\sigma_1 = u^2 - \sigma_1 a$  with some  $u, a \in \mathfrak{g}$ . Put  $\alpha = \begin{bmatrix} 1 & 0 \\ -u & \sigma_1 \end{bmatrix}$  and  $\psi = \begin{bmatrix} \sigma_1 & u \\ u & a \end{bmatrix}$ . Then  $\alpha\psi \cdot {}^t\alpha = \text{diag}[\sigma_1, \sigma_2]$ , which cannot happen if  $\sigma$  is  $s$ -reduced. Thus we obtain (i), which immediately implies the “only if”-part of (ii). The “if”-part of (ii) follows from (31.3).

**33.3.** Let  $(V, \varphi)$  be a nondegenerate quadratic space over  $\mathbf{Q}$ ,  $L$  a lattice in  $V$ , and  $\Phi$  an element of  $S_n(\mathbf{Q})$  that represents  $\varphi$  with respect to a  $\mathbf{Z}$ -basis of  $L$ . Then  $\Phi \in S_n(\mathbf{Z})$  if and only if  $\mu_0(L) \subset \mathbf{Z}$ , and  $\Phi$  is  $s$ -reduced if and only if  $L$  is  $\varphi^*$ -maximal, as observed in §31.3. Also, by Lemma 29.2(5),  $L$  is  $\varphi^*$ -maximal if and only if  $L_p$  is  $\varphi^*$ -maximal for every prime number  $p$ . Therefore  $\Phi$  is  $s$ -reduced if and only if it is an  $s$ -reduced element of  $S_n(\mathbf{Z}_p)$  for every  $p$ . For  $p \neq 2$  it must be a  $q$ -reduced element of  $T_n(\mathbf{Z}_p)$ .

**Theorem 33.4.** *The set  $S_n^2(\mathbf{Z})$  consists of the elements  $\tau$  of  $T_n(\mathbf{Z})$  such that  $2^{-1}\tau$  is  $q$ -reduced and  $\det(\tau) \notin 4\mathbf{Z}$ .*

PROOF. Take  $\tau \in S_n^2(\mathbf{Z})$ . By Lemma 33.2(ii),  $\det(\tau) \notin 4\mathbf{Z}$ . From (31.2) and (31.3) we easily see that  $2^{-1}\tau$  is  $q$ -reduced. Conversely, suppose  $\tau \in T_n(\mathbf{Z})$  and  $2^{-1}\tau$  is  $q$ -reduced. Put  $L = \mathbf{Z}_n^1$ . Then  $L$  is  $(2^{-1}\tau)$ -maximal, and so  $L_p$  is  $\tau^*$ -maximal for every  $p \neq 2$ . Suppose now  $\det(\tau) \notin 4\mathbf{Z}$ . Then by Lemma 33.2(ii),  $\tau$  is  $s$ -reduced at the prime 2. Thus  $L_2$  is  $\tau^*$ -maximal, and so  $L$  is  $\tau^*$ -maximal. Consequently  $\tau$  is  $s$ -reduced. This proves our theorem.

**33.5.** By means of this theorem, the classification of the elements of  $S_n^2(\mathbf{Z})$  and their genera can be reduced to the classification of the reduced  $\mathbf{Z}$ -valued

quadratic forms represented by the elements  $\Phi$  of  $2^{-1}T_n$ , which was settled in Theorems 31.6, 31.7, and 31.9; see also §31.8. We obtain the desired results on  $S_n^2(\mathbf{Z})$  by simply imposing an additional condition that  $\det(2\Phi) \notin 4\mathbf{Z}$ . For this reason, we restrict our results on the classification of  $s$ -reduced elements to those of Type 1.

In the discussion of  $q$ -reduced matrices, the crucial fact is that all the maximal lattices form a single genus. Thus the main question in the case of  $s$ -reduced matrices is whether all the  $\varphi^*$ -maximal lattices form a single genus. The answer in general is no, but we can give a satisfactory answer if the prime 2 is unramified in the global field  $F$  that is the base field. If  $F = \mathbf{Q}$  in particular, we have a clear-cut answer.

Before stating it, we first make some easy observations. Let  $(V, \varphi)$  be a nondegenerate quadratic space over a local field  $F$  in which  $\mathfrak{p} = 2\mathfrak{g}$ , and  $L$  a  $\varphi^*$ -maximal lattice in  $V$ . Then

$$(33.2a) \quad [L^\varphi/L] = \mathfrak{g} \iff \delta_0(\varphi) \cap \mathfrak{g}^\times \neq \emptyset,$$

$$(33.2b) \quad [L^\varphi/L] = \mathfrak{p} \iff \delta_0(\varphi) \cap \mathfrak{g}^\times = \emptyset.$$

Indeed, let  $\sigma$  be the element of  $S_n(\mathfrak{g})$  that represents  $\varphi$  with respect to a  $\mathfrak{g}$ -basis of  $L$ . Clearly  $[L^\varphi/L] = \det(\sigma)\mathfrak{g}$ . By Lemma 33.2, this is  $\mathfrak{p}$  or  $\mathfrak{g}$ . Since  $\delta_0(\varphi)$  is represented by  $\pm \det(\sigma)$ , we obtain (33.2a, b). We also see that  $\sigma \in S_n^1(\mathfrak{g})$  if and only if  $\mu(L) = \mathfrak{g}$ , and  $\sigma \in S_n^2(\mathfrak{g})$  if and only if  $\mu(L) \subset 2\mathfrak{g}$ . We say that  $L$  is of Type  $\lambda$  if  $\sigma \in S_n^\lambda(\mathfrak{g})$ . Now we have

**Theorem 33.6.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over a local field  $F$  in which  $\mathfrak{p} = 2\mathfrak{g}$ , and let  $L$  and  $M$  be  $\varphi^*$ -maximal lattices in  $V$  of the same type. Then  $L = M\gamma$  for some  $\gamma \in SO^\varphi(V)$ .*

This was given as Theorem 2.4(iii) in [SO8]. Unfortunately the proof is long and involved, and therefore we refer the reader to that paper for details.

**Theorem 33.7.** *Let  $\varphi \in S_n(\mathbf{Q})$  with  $n > 2$ . Then there exists an element  $\psi$  of  $S_n^1(\mathbf{Z})$  such that  $\psi = \alpha\varphi \cdot {}^t\alpha$  with  $\alpha \in GL_n(\mathbf{Q})$ . Moreover, the genus of such a  $\psi$  is uniquely determined by  $\varphi$ .*

PROOF. Let  $(V, \varphi) = \langle \mathbf{Q}, \varphi \rangle$ . By Lemma 29.2(1) we can find a maximal lattice  $L$  in  $V = \mathbf{Q}_n^1$ . Then  $\mu(L_2) = \mathbf{Z}_2$  by (29.8), since  $n > 2$ . By Lemma 29.2(1) there is a  $\varphi^*$ -maximal lattice  $L'$  in  $V_2$  containing  $L_2$ . By Lemma 21.6(ii) there exists a lattice  $M$  in  $V$  such that  $M_p = L_p$  for every  $p \neq 2$  and  $M_2 = L'$ . Then  $M$  is  $\varphi^*$ -maximal. Let  $\psi$  be the matrix that represents  $\varphi$  with respect to a  $\mathbf{Z}$ -basis of  $M$ . Since  $\mu(M_2) = \mathbf{Z}_2$ , we see that  $\psi \in S_n^1(\mathbf{Z})$  and  $\psi \sim \varphi$ . By Theorem 33.6 the genus of  $M$  is determined by  $\varphi$ . This proves our theorem.

**Theorem 33.8.** *Let two integers  $n$  and  $\sigma$  be given as follows:  $3 \leq n \in \mathbf{Z}$ ,  $n - \sigma \in 2\mathbf{Z}$ ,  $|\sigma| \leq n$ ; also let  $m$  and  $e$  be square-free positive integers. Let  $r$  be the number of prime factors of  $e$ , and  $f$  the product of the prime factors of  $e$  prime to  $2m$ . Suppose that  $\sigma - 4r \equiv 0$  or  $2 \pmod{8}$  if  $n$  is even and  $\sigma - 4r \equiv \pm 1 \pmod{8}$  if  $n$  is odd. Then there exists an element  $\psi$  of  $S_n^1(\mathbf{Z})$  such that*

$$|\det(\psi)| = mf^2, \quad s(\psi) = \sigma,$$

*and  $Q(\psi)$  is ramified at a prime number  $p$  if and only if  $p|e$ . Moreover, every element of  $S_n^1(\mathbf{Z})$  is of this type, and its genus is determined by  $(n, \sigma, m, e)$ .*

PROOF. Let  $\delta = (-1)^{[\sigma/2]}m$  and let  $B$  be a quaternion algebra over  $\mathbf{Q}$  that is ramified exactly at the prime factors of  $e$ , and also at the archimedean prime if  $r$  is odd. By Theorem 28.9 we can find a quadratic space  $(V, \varphi)$  over  $\mathbf{Q}$  such that  $Q(\varphi) = B$ ,  $\sigma = s(\varphi)$ , and  $\delta \in \delta_0(\varphi)$ . Indeed, (28.7a) or (28.7b) is satisfied; the condition on  $\sigma - 4r$  implies (28.6a, b). Thus the desired  $(V, \varphi)$  exists. By Theorem 33.7 we can find  $\psi \in S_n^1(\mathbf{Z})$  such that  $\psi \sim \varphi$ . Now for  $L = \mathbf{Z}^n$  we have  $\det(\psi)\mathbf{Z} = [L^\psi/L]$ . From (33.2a, b) we obtain  $[L^\psi/L]_2 = m\mathbf{Z}_2$ . If  $p \neq 2$ , then  $[L^\psi/L]_p$  coincides with  $[\tilde{L}/L]_p$ , which can be given by (29.7). Combining all these, we obtain

$$(33.3) \quad [L^\psi/L] = mf^2\mathbf{Z},$$

and so  $|\det(\psi)| = mf^2$ . This proves the first part of our theorem. Next, given  $\tau \in S_n^1(\mathbf{Z})$ , let  $e$  be the product of the prime numbers ramified in  $Q(\tau)$ ; take a square-free positive integer  $m$  so that  $\pm m \in \delta_0(\tau)$ . Then we find that  $\tau$  is of the type described in our theorem. Now the genus of  $\tau$  is determined by  $n$ ,  $s(\tau)$ ,  $\delta_0(\tau)$ , and  $Q(\tau)$ ; also,  $Q(\tau)$  is determined by  $e$ . Therefore we obtain our assertion about the genus. This proves our theorem.

**Theorem 33.9.** *Let  $n \in \mathbf{Z}$ ,  $> 2$ , and let  $\sigma$  be an integer such that  $|\sigma| \leq n$  and  $\sigma - n \in 2\mathbf{Z}$ . Let  $m$  and  $f$  be two square-free positive integers such that  $f$  is prime to  $2m$ , and let  $\nu$  be the number of different prime factors of  $2m$ . Then there exist exactly  $2^{\nu-1}$  genera of  $\psi \in S_n^1(\mathbf{Z})$  such that  $|\det(\psi)| = mf^2$  and  $s(\psi) = \sigma$ .*

PROOF. Since the genus of  $\psi$  is determined by  $(n, \sigma, m, e)$  as stated in Theorem 33.8, our task is to count the number of possible  $e$ 's. Clearly  $e = fg$  with a square-free factor  $g$  of  $2m$ . Thus we have to count the number of possible  $g$ 's. Let  $\mu$  be the number of prime factors of  $g$ . Then  $\mu \leq \nu$  and  $\sigma - 4r$  modulo 8 must be determined as in Theorem 33.8. We easily see that each  $(\sigma, f)$  determines  $\mu$  modulo 2, and so by (31.7) we have exactly  $2^{\nu-1}$  choices for  $g$ . This proves our theorem.

**Lemma 33.10.** *Let  $F$  be a local field in which  $\mathfrak{p} = 2\mathfrak{g}$ . Given  $\varphi \in S_n^1(\mathfrak{g})$ , put  $C(\varphi) = GL_n(\mathfrak{g}) \cap SO(\varphi)$  and  $\Sigma(\varphi) = \sigma(C(\varphi))$ . Let  $\sigma : SO(\varphi) \rightarrow F^\times / F^{\times 2}$  be the spinor norm map of (24.7). Then  $\mathfrak{g}^\times \subset \Sigma(\varphi)$  provided  $n > 2$ .*

PROOF. This was given as Lemma 2.16 in [S08]. Here we merely explain the basic ideas of the proof in the case in which  $F = \mathbf{Q}_2$ ,  $\mathfrak{g} = \mathbf{Z}_2$ , and  $\varphi = \text{diag}[1, 1, 5]$ . Let  $L = (\mathbf{Z}_2)_3^1$ . Then  $\varphi[L]$  consists of the number  $a^2 + b^2 + 5c^2$  with  $a, b, c \in \mathbf{Z}_2$ . If  $\varphi[x] \in \mathbf{Z}_2^\times$  and  $\varphi[y] \in \mathbf{Z}_2^\times$  with  $x, y \in L$ , then  $\tau(xy) \in C(\varphi)$  by Lemma 29.5 and  $\varphi[x]\varphi[y] = \sigma(\tau(xy)) \in \Sigma(\varphi)$ . We can certainly find  $y \in L$  such that  $\varphi[y] = 1$ . From the fact in the table below (9.3) concerning  $\mathbf{Q}_2(\sqrt{-1})$  we see that every element of  $1 + 4\mathbf{Z}_2$  can be expressed as  $a^2 + b^2$  with  $a, b \in \mathbf{Z}_2$ . Clearly  $7 \in \varphi[L]$ . Thus  $\Sigma(\varphi)$  contains 7 and  $1 + 4\mathbf{Z}_2$ , and so  $\mathbf{Z}_2^\times \subset \Sigma(\varphi)$ , which proves our lemma in this special case. The general case can be handled more or less in a similar way.

**Theorem 33.11.** *Let  $\varphi$  and  $\psi$  be indefinite elements of  $S_n^\lambda(\mathbf{Z})$  with  $n \geq 3$ . Then the following assertions hold:*

(i) *If  $\varphi = \alpha\psi \cdot {}^t\alpha$  with  $\alpha \in GL_n(\mathbf{Q})$ , then such an  $\alpha$  can be taken from  $GL_n(\mathbf{Z})$ .*

(ii) *If  $\lambda = 1$ ,  $s(\varphi) = s(\psi)$ , and  $|\det(\varphi)| = |\det(\psi)| = f^2$  or  $2f^2$  with a square-free odd integer  $f$ , then  $\varphi = \alpha\psi \cdot {}^t\alpha$  with  $\alpha \in GL_n(\mathbf{Z})$ . Such a  $\varphi$  exists for both values  $f^2$  and  $2f^2$  and also for a given value of  $s(\varphi)$ , provided  $|s(\varphi)| \leq n$  and  $s(\varphi) - n \in 2\mathbf{Z}$ .*

PROOF. For  $\lambda = 2$ , (i) follows from Theorems 33.4 and 32.19(ii). Thus we have only to consider the case  $\lambda = 1$ . Let  $(V, \varphi) = \langle \mathbf{Q}, \varphi \rangle$  with an indefinite  $\varphi \in S_n^1(\mathbf{Z})$ ,  $n \geq 3$ . By Theorem 33.7, if  $\psi \in S_n^1(\mathbf{Z})$  and  $\varphi \sim \psi$ , then  $\psi$  belongs to the genus of  $\varphi$ . Combining Lemma 33.10 and Theorem 32.19(i), we see that the genus of  $\varphi$  consists of a single  $SO$ -class, and so we obtain (i). Next, if  $\varphi \in S_n^1(\mathbf{Z})$  and  $\det(\varphi)$  is as in (ii), then the genus of  $\varphi$  is determined by  $\det(\varphi)$  and  $s(\varphi)$ , by virtue of Theorem 33.9. Therefore (ii) follows from (i).

It should be noted that the case  $|\det(\varphi)| = 1$  of (ii) was proved by Milnor in [M].

**33.12.** The case where  $\det(\varphi)$  is square-free is different from the situation of Theorem 33.11(ii). For example, take a prime number  $m$  such that  $m+1 \in 4\mathbf{Z}$ . Put  $\varphi = \text{diag}[1_3, -m]$  and  $\psi = \text{diag}[1_2, m, -1]$ . Clearly these belong to  $S_4^1(\mathbf{Z})$ ,  $\det(\varphi) = \det(\psi) = -m$ , and  $s(\varphi) = s(\psi) = 2$ . However, they define nonisomorphic quadratic spaces. Indeed, suppose  $\langle \mathbf{Q}, \varphi \rangle \cong \langle \mathbf{Q}, \psi \rangle$ . Then by Witt's theorem,  $\text{diag}[1, -m] \sim \text{diag}[-1, m]$ . Put  $K = \mathbf{Q}(\sqrt{m})$  and  $K_m = K \otimes_{\mathbf{Q}} \mathbf{Q}_m$ . Then  $-1 = x^2 - my^2$  with  $x, y \in \mathbf{Q}$ , and  $x + y\sqrt{m}$  must

be an integer of  $K_m$ , and so  $x, y \in \mathbf{Z}_m$ , which means that  $x^2 + 1 \in m\mathbf{Z}_m$ . This is impossible, since  $m + 1 \in 4\mathbf{Z}$ . Therefore  $\varphi \approx \psi$ .

Viewing  $\varphi$  and  $\psi$  in the setting of Theorem 33.9, we have  $\nu = 2$ , and so there exist exactly two genera of the matrices  $\xi \in S_4^1(\mathbf{Z})$  such that  $\det(\xi) = -m$  and  $s(\xi) = 2$ . By Theorem 33.11(i) each genus consists of a single  $SO$ -class. Thus  $\varphi$  and  $\psi$  represent these two different classes of such  $\xi$ .

## QUADRATIC DIOPHANTINE EQUATIONS

### 34. A historical perspective

**34.1.** We take a nondegenerate quadratic space  $(V, \varphi)$  of dimension  $n$  over a local or global field  $F$  in the sense of §21.1. By a **quadratic Diophantine equation** we mean an equation of the type

$$(34.1) \quad \varphi[x] = q$$

with a given  $q \in F^\times$ . Let  $\mathfrak{g}$  denote the maximal order of  $F$  as before. Given a  $\mathfrak{g}$ -lattice  $L$  in  $V$ , put

$$(34.2a) \quad L[q] = \{x \in L \mid \varphi[x] = q\},$$

$$(34.2b) \quad \Gamma(L) = \{\alpha \in SO^\varphi(V) \mid L\alpha = L\}.$$

In particular, in the classical case with  $F = \mathbf{Q}$  and  $V = \mathbf{Q}_n^1$ , we usually take  $L = \mathbf{Z}_n^1$  and assume that  $\varphi$  is  $\mathbf{Z}$ -valued on  $L$  and  $q \in \mathbf{Z}$ . A quadratic form with  $n = 2$  is called a **binary form**. It was an old problem studied by many mathematicians, Fermat and Euler in particular, to find integer solutions  $x$  for a given binary form  $\varphi$  and  $q$ , that is, the elements of  $L[q]$ . They were successful in some special cases, but the case of an arbitrary binary form  $\varphi$  was settled by Lagrange and later reformulated by Gauss.

In this book, however, we do not discuss this problem of finding  $x$  for equation (34.1). To explain what kind of problems we will discuss, we first introduce the notion of primitive solution. Still with  $\mathbf{Z}$ -valued  $\varphi$ ,  $q \in \mathbf{Z}$ , and  $L = \mathbf{Z}_n^1$ , we put

$$(34.3) \quad L^0[q] = \{x \in L[q] \mid \sum_{i=1}^n x_i \mathbf{Z} = \mathbf{Z}\},$$

and call the elements of  $L^0[q]$  **primitive solutions** of (34.1). This condition of primitivity is fundamental in our theory as will be explained later. For the moment, let us just say that the nature of the question about  $L^0[q]$  is quite different from that about  $L[q]$ ; roughly speaking, the former is more conceptual, and the latter more computational. We will eventually explain this difference and present a new interpretation of  $L^0[q]$ , which leads to certain class number formulas for orthogonal groups.



**34.2.** Before proceeding further, let us look more closely at binary forms. A binary form in two variables  $x$  and  $y$  over  $F$  can be given in the form  $ax^2 + bxy + cy^2$  with  $a, b, c \in F$ . This is represented by the matrix  $h = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$ . Employing the notation of §28.1, our two-dimensional quadratic space can be written  $\langle F, h \rangle$ . We have  $\det(2h) = 4ac - b^2$ , and call the number  $b^2 - 4ac$  the **discriminant** of the binary form represented by  $h$ .

We say that another form represented by a similar matrix  $h'$  belongs to the same **class** as  $h$  if

$$(34.4) \quad h' = \det(\alpha)^{-1} \cdot \alpha h \cdot {}^t\alpha \quad \text{with} \quad \alpha \in GL_2(\mathbf{Z}).$$

Here we deviate from the traditional definition  $h' = \alpha h \cdot {}^t\alpha$  with  $\alpha \in SL_2(\mathbf{Z})$ , because (34.4) with  $GL_2(\mathfrak{g})$  in place of  $GL_2(\mathbf{Z})$  is the best definition in the case of an arbitrary number field.

Now Lagrange showed that when  $F = \mathbf{Q}$  and  $\mathfrak{g} = \mathbf{Z}$ , the number of classes of the forms with a given discriminant is finite, which is the easiest case of Theorem 30.4. For an obvious technical reason, it is natural to assume, as Lagrange and later researchers did, that the binary form is **primitive**, which means that the integers  $a, b, c$  have no common divisors other than  $\pm 1$ .

In order to interpret the notion of class in a different way, we consider a *ternary* form  $\varphi$  defined on  $\mathbf{Q}_3^1$  by

$$(34.5) \quad \varphi[(x, y, z)] = 4xy - z^2.$$

If we fix  $q$ , then a primitive binary form of discriminant  $-q$  corresponds to a primitive solution  $h = (a, b, c) \in \mathbf{Z}_3^1$  of the equation  $\varphi[h] = q$  with  $\varphi$  of (34.5), that is, an element of  $L^0[q]$  with  $L = \mathbf{Z}_3^1$ .

This much is trivial, but here is a nontrivial fact:  $\Gamma(L)$  defined by (34.2b) in the present case consists of all the maps  $h \mapsto h'$  of (34.4). (It seems that the previous researchers did not connect  $SO(\varphi)$  for  $\varphi$  of (34.5) with binary forms, and the last fact on  $\Gamma(L)$ , proved in §36.14 below, is not a well-known old result. Indeed, the corresponding fact in the case of an arbitrary number field  $F$  depends on the nature of the ideal class group of  $F$ ; see the comments at the end of §36.14 below.) Therefore the classes of binary forms of discriminant  $-q$  correspond bijectively to  $L^0[q]/\Gamma(L)$  defined with respect to  $\varphi$  of (34.5). Denoting by  $c(q)$  the number of classes of primitive binary forms of discriminant  $-q$ , we thus obtain

$$(34.6) \quad \#\{L^0[q]/\Gamma(L)\} = c(q).$$

Before discussing another ternary form, let us quote here a basic result of Dedekind. Assuming that  $-q$  is not a square in  $\mathbf{Q}$ , define a quadratic extension  $K$  of  $\mathbf{Q}$  by  $K = \mathbf{Q}(\sqrt{-q})$ . Since  $q \in 4\mathbf{Z}$  or  $-q - 1 \in 4\mathbf{Z}$ , we can put  $-q = f^2d$  with  $0 < f \in \mathbf{Z}$  and the discriminant  $d$  of  $K$ . Denote by  $\mathfrak{r}$  the ring

of algebraic integers in  $K$  and define a subring  $\mathfrak{f}$  of  $\mathfrak{r}$  by  $\mathfrak{f} = \mathbf{Z} + f\mathfrak{r}$ . Then Dedekind [DD, §187] showed that there is a bijection from the set of all ideal classes of proper  $\mathfrak{f}$ -ideals (whose definition will be given in §36.1 below) onto the set of all classes of primitive binary forms of discriminant  $-q$ . If  $-q = d$ , then  $f = 1$ ,  $\mathfrak{f} = \mathfrak{r}$ , and a proper  $\mathfrak{f}$ -ideal is a fractional ideal in  $K$ . By virtue of this result,  $c(q)$  is the class number of such an  $\mathfrak{f}$ , and in particular, the class number of  $K$  if  $-q = d$ . We naturally ask whether we can state a theorem that extends this result of Dedekind to the case of an arbitrary algebraic number field. We will give an answer in Theorem 36.13.

**34.3.** Next we turn to a more difficult problem concerning

$$(34.7) \quad \varphi[(x, y, z)] = x^2 + y^2 + z^2.$$

We naturally look for primitive solutions  $h$  of the equation  $\varphi[h] = q$  for a given  $q \in \mathbf{Z}$ ,  $q > 0$ . In this case, the permutations of  $(x, y, z)$  and the diagonal elements of  $GL_3(\mathbf{Z})$  generate a group of order 48 which has  $\Gamma(\mathbf{Z}^3)$  as a subgroup of index 2. In the celebrated book [G] Gauss showed that such a primitive solution exists if and only if  $q = b^2m$  with an odd positive integer  $b$  and a square-free positive integer  $m$  such that  $m \not\equiv 7 \pmod{8}$ . This is a stronger result than Theorem 27.14(ii). Moreover, he proved a far deeper result on  $L^0[q]$  for such a  $q$ , which can be reformulated as follows:

$$(34.8a) \quad \#\{L^0[q]/\Gamma(L)\} = c(q) \cdot \begin{cases} 1 & \text{if } m \equiv 3 \pmod{4} \text{ or } q \leq 2, \\ 2^{-1} & \text{otherwise.} \end{cases}$$

From this we can easily derive a formula valid for  $q = b^2m > 3$ :

$$(34.8b) \quad \#L^0[q] = c(q) \cdot \begin{cases} 24 & \text{if } m \equiv 3 \pmod{4}, \\ 12 & \text{otherwise.} \end{cases}$$

In fact, Gauss stated something equivalent to (34.8b), but did not give a clear-cut statement in the form (34.8a). It should be added that Legendre was the first person who had the insight that binary forms were involved, and Gauss owed much to that idea. The argument of Gauss was long and roundabout. Later Eisenstein and Minkowski investigated the case of five squares, but they never explained why class numbers were involved. Weil's book [We] gives a detailed historical account of what Lagrange and Legendre did, but unfortunately, it does not explain much of the works of Gauss or his successors. We mention Bachmann's book [B], which includes an exposition in that respect.

History aside, our point is that there is an unmistakable parallelism between (34.6) and (34.8a). Therefore we can expect the existence of a general principle of which (34.6) and (34.8a) are special cases. In the above two cases,  $n = 3$  and binary forms have two variables, and so the expected principle for  $\varphi$  of  $n$  variables may be of the following type:

(34.9a)  $\#\{L^0[q]/\Gamma(L)\} = \text{the class number of an object in dimension } n - 1.$

But things are not that simple, though the idea of (34.9a) is basically right. In fact, if  $\#L^0[q]$  is finite, we will eventually find another formula that generalizes (34.8b) and takes the following form in the simplest case:

(34.9b)  $\#L^0[q] = \text{the “mass” of an object in dimension } n - 1.$

This of course requires the definition of the mass. Without going into details here, let us merely say that it is a quantity associated with an orthogonal group and its arithmetic subgroups.

As we said in the introduction, it is one of the main purposes of this book to present a general principle that a *primitive solution of (34.1) of dimension  $n$  determines a class in an  $(n - 1)$ -dimensional orthogonal group*. In other words, we will give a *conceptual interpretation* of each element of  $L^0[q]$ . We will eventually obtain precise versions of (34.9a, b).

### 35. Basic theorems of quadratic Diophantine equations

**35.1.** Let us now develop our theory systematically by considering a more general situation with  $(V, \varphi)$  as in §34.1. To make our exposition smooth, we restate Lemma 22.5(ii) in the following form:

$$(35.1) \quad \{h \in V \mid \varphi[h] = \varphi[k]\} = h \cdot SO^\varphi(V) \quad \text{if } \varphi[h] \neq 0 \text{ and } n > 1.$$

We take  $F$  to be local and use the symbols  $\mathfrak{g}$  and  $\mathfrak{p}$ . Fixing a maximal lattice  $L$  in  $V$ , we put

$$(35.2a) \quad C = \{\alpha \in SO^\varphi(V) \mid L\alpha = L\},$$

$$(35.2b) \quad L^* = \{x \in V \mid 2\varphi(x, L) = \mathfrak{g}\}.$$

Clearly  $L^*\gamma = L^*$  for every  $\gamma \in C$ .

We now state a theorem which plays a crucial role in our theory.

**Theorem 35.2.** *Suppose that  $\dim(V) > 1$ . Let  $h$  and  $k$  be elements of  $V$  such that  $\varphi[h] = \varphi[k] \neq 0$  and  $\varphi(h, L) = \varphi(k, L)$ . Then  $k = h\gamma$  for some  $\gamma \in C$ , except when  $n = 2$ ,  $\varphi$  is isotropic, and  $\varphi[h] \in \mathfrak{p}$ , in which case  $k = h\alpha$  with an element  $\alpha$  of  $O^\varphi$  such that  $L\alpha = L$ .*

This was proved in [S04b, Theorem 10.5] under the following condition:

$$(35.3) \quad \delta_0(\varphi) \cap \mathfrak{g}^\times \neq \emptyset \quad \text{if } n \notin 2\mathbb{Z}.$$

It was shown in [S06c] that this condition was unnecessary. In any case the proof is long and involved, and therefore in this book we prove only the case  $n = 3$  under the following condition:

$$(35.4) \quad \delta_0(\varphi) \cap \mathfrak{g}^\times \neq \emptyset \text{ if } \varphi \text{ is isotropic.}$$

PROOF. First suppose that  $\varphi$  is anisotropic. Then by Lemma 29.7,  $L\alpha = L$  for every  $\alpha \in O^\varphi$ , and so  $C = SO^\varphi$ . Let  $h$  and  $k$  be as in our theorem. Then by (35.1),  $h \in k \cdot SO^\varphi = kC$ , which gives the desired result.

Thus we assume that  $\varphi$  is isotropic. Then we have a Witt decomposition  $V = Fe + Ff + Fg$ ,  $e^2 = f^2 = 0$ ,  $ef + fe = 1$ ,  $g^2 = \delta \in F^\times$ . Our assumption (35.4) allows us to take  $\delta$  so that  $\delta \in \mathfrak{g}^\times$ . Replacing  $\varphi$  by  $\delta^{-1}\varphi$ , we may assume that  $\delta = 1$ . (Indeed, every  $\varphi$ -maximal  $L$  is  $\delta^{-1}\varphi$ -maximal.) We can take  $L = \mathfrak{g}e + \mathfrak{g}f + \mathfrak{g}g$ . Given  $0 \neq h \in V$ , we can find  $c \in F^\times$  such that  $ch \in L^*$ . Therefore, it is sufficient to prove the following statement:

(\*) If  $h, k \in L^*$  and  $\varphi[h] = \varphi[k] \neq 0$ , then  $h \in kC$ .

We note that  $L^* \subset \tilde{L} = \mathfrak{g}e + \mathfrak{g}f + 2^{-1}\mathfrak{g}g$ . Thus let  $h = ae + bf + cg \in L^*$  with  $a, b \in \mathfrak{g}$  and  $c \in 2^{-1}\mathfrak{g}$ . Then  $a\mathfrak{g} + b\mathfrak{g} + 2c\mathfrak{g} = \mathfrak{g}$  and  $\varphi[h] = ab + c^2$ .

We divide our discussion according to the nature of 2.

Case 1:  $2 \in \mathfrak{g}^\times$ ;

Case 2:  $2 \in \mathfrak{p}$ .

In Case 1, we see that  $c \in \mathfrak{g}$  and  $\varphi[h] \in \mathfrak{g}$ . Therefore we have two cases:

Case 1a:  $2 \in \mathfrak{g}^\times$  and  $\varphi[h] \in \mathfrak{g}^\times$ ;

Case 1b:  $2 \in \mathfrak{g}^\times$  and  $\varphi[h] \in \mathfrak{p}$ .

In Case 1a, let  $W_1 = (Fh)^\perp$  and  $W_2 = (Fk)^\perp$  for  $h, k$  as in (\*). Then by Lemma 32.4,  $L = \mathfrak{g}h \oplus (L \cap W_1) = \mathfrak{g}k \oplus (L \cap W_2)$ . Since  $\varphi[h] = \varphi[k]$ , (35.1) guarantees an element  $\alpha$  of  $SO^\varphi(V)$  such that  $h\alpha = k$ . Then  $W_1\alpha = W_2$ . Clearly  $L \cap W_i$  is maximal in  $W_i$ , and so  $(L \cap W_1)\alpha$  is maximal in  $W_2$ . By Lemma 29.9,  $(L \cap W_1)\alpha\beta = L \cap W_2$  for some  $\beta \in SO^\varphi(W_2)$ . We can extend  $\beta$  to an element of  $SO^\varphi(V)$  by putting  $k\beta = k$ . Then  $\alpha\beta \in SO^\varphi(V)$ ,  $h\alpha\beta = k$ , and  $L\alpha\beta = L$ , which gives the desired fact.

Let  $h = ae + bf + cg \in L^*$  as before in both Cases 1 and 2. Since  $\varphi[h] = ab + c^2$ , we have  $\varphi[h] \in \mathfrak{g}$  if and only if  $c \in \mathfrak{g}$ . Thus we divide Case 2 into two cases:

Case 2a:  $2 \in \mathfrak{p}$  and  $\varphi[h] \in \mathfrak{g}$ ;

Case 2b:  $2 \in \mathfrak{p}$  and  $\varphi[h] \notin \mathfrak{g}$ .

Since  $a\mathfrak{g} + b\mathfrak{g} + 2c\mathfrak{g} = \mathfrak{g}$ , we see that  $a \in \mathfrak{g}^\times$  or  $b \in \mathfrak{g}^\times$  in Cases 1b and 2a.

Suppose now  $a \in \mathfrak{g}^\times$  or  $b \in \mathfrak{g}^\times$ . Represent  $GL(V)$  with respect to the basis  $\{f, e, g\}$ . Then  $\text{diag}\left[\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, -1\right] \in C$  and  $\text{diag}[a, a^{-1}, 1] \in C$  for every  $a \in \mathfrak{g}^\times$ . Thus replacing  $h$  by a suitable element of  $hC$ , we may assume that  $h = ae + f + cg$  with  $a \in \mathfrak{g}$  and  $c \in 2^{-1}\mathfrak{g}$ .

Let us next represent  $GL(V)$  with respect to the basis  $\{f, g, e\}$  instead of  $\{f, e, g\}$ , and let  $P$  denote the upper triangular elements of  $SO^\varphi$ . It is easy to verify that  $P$  consists of the matrices of the form

$$(35.5) \quad \begin{bmatrix} d^{-1} & s & -s^2d \\ 0 & 1 & -2sd \\ 0 & 0 & d \end{bmatrix} \quad (d \in F^\times, s \in F).$$

For  $h = ae + f + cg$  we have  $\varphi[h] = a + c^2$ . In Cases 1b and 2a put

$$\alpha = \begin{bmatrix} 1 & -c & -c^2 \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix}.$$

Then  $\alpha \in C$  and  $h\alpha = f + \varphi[h]g$ . Given  $k \in L^*$  such that  $\varphi[k] = \varphi[h]$ , we can similarly find an element  $\beta \in C$  such that  $k\beta = f + \varphi[k]g = h\alpha$ . Thus our problem is settled in Cases 1b and 2a.

Before discussing Case 2b, let us state a basic result:

$$(35.6) \quad SO^\varphi(V) = PC.$$

This will be proved at the end. Still postponing the discussion of Case 2b, we consider any  $h \in L^*$ , with no conditions on  $a, b$ , satisfying

$$(35.7) \quad 4\varphi[h] \in \mathfrak{g}^{\times 2}.$$

In this case we put  $4\varphi[h] = u^2$  with  $u \in \mathfrak{g}^\times$  and  $\ell = 2^{-1}ug$ . Then  $\varphi[\ell] = \varphi[h]$  and  $\ell \in L^*$ . By (35.1) we have  $h = \ell\xi$  with  $\xi \in SO^\varphi(V)$ . By (35.6) we can put  $\xi = \pi\gamma$  with  $\pi \in P$  and  $\gamma \in C$ . Take  $\pi$  in the form (35.5). Then  $\ell\pi$  can be identified with the row vector  $[0 \ 2^{-1}u \ -usd]$ . Since  $\ell\pi = h\gamma^{-1} \in L^*$ , we see that  $-usd \in \mathfrak{g}$ . Put  $x = -sd$  and

$$\eta = \begin{bmatrix} 1 & -x & -x^2 \\ 0 & 1 & 2x \\ 0 & 0 & 1 \end{bmatrix}.$$

Then  $\eta \in C$  and  $\ell\eta = \ell\pi = h\gamma^{-1}$ . Thus  $h \in \ell C$ . Since  $\ell$  depends only on  $\varphi[h]$ , this gives the desired result under (35.7).

Therefore we hereafter assume that  $4\varphi[h] \notin \mathfrak{g}^{\times 2}$ . Let  $h = ae + bf + cg \in L^*$  in Case 2b. Suppose  $a \in \mathfrak{p}$  and  $b \in \mathfrak{p}$ . Then  $2c\mathfrak{g} = \mathfrak{g}$ . Put  $d = 2c$ . Then  $d \in \mathfrak{g}^\times$  and  $4\varphi[h] = 4(ab + c^2) = d^2(1 + 4d^{-2}ab) \in \mathfrak{g}^{\times 2}$  by Lemma 21.12(i), a contradiction. Therefore  $a \in \mathfrak{g}^\times$  or  $b \in \mathfrak{g}^\times$ . For the reason explained in Cases 1b and 2a, we may assume that  $h = f + ae + cg$ . Similarly we may assume that  $k = f + a_1e + c_1g$ . Then  $a + c^2 = \varphi[h] = \varphi[k] = a_1 + c_1^2$ , and so  $(c - c_1)(c + c_1) = c^2 - c_1^2 = a_1 - a \in \mathfrak{g}$ . Therefore  $c - c_1 \in \mathfrak{g}$  or  $c + c_1 \in \mathfrak{g}$ . Since  $2c_1 \in \mathfrak{g}$ , we see that  $c - c_1 \in \mathfrak{g}$ . Put  $r = c - c_1$  and

$$\zeta = \begin{bmatrix} 1 & r & -r^2 \\ 0 & 1 & -2r \\ 0 & 0 & 1 \end{bmatrix}.$$

Then  $\zeta \in C$  and  $k\zeta = h$  as desired. This completes the proof of (\*), except that we have to prove (35.6).

PROOF OF (35.6). We easily see that  $P = \{\alpha \in SO^\varphi \mid e\alpha \in Fe\}$ . Also  $(V, \varphi) \cong (B^\circ, \beta^\circ)$  with  $B = M_2(F)$ ,  $B^\circ = \{x \in B \mid \text{tr}(x) = 0\}$ , and  $\beta^\circ[x] = -xx^t$  for  $x \in B^\circ$ . Indeed, we can put

$$e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad g = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

This is a special case of Lemma 25.2(ii). We have  $G^+(V) = B^\times = GL_2(F)$  and  $x\tau(b) = b^{-1}xb$  for  $x \in B^\circ$  and  $b \in GL_2(F)$ . We have  $L = \mathfrak{g}e + \mathfrak{g}f + \mathfrak{g}g = M_2(\mathfrak{g}) \cap B^\circ$ . Let  $D = GL_2(\mathfrak{g})$  and let  $T$  be the subgroup of  $GL_2(F)$  consisting of the upper triangular matrices. We easily see that  $b^{-1}eb \in Fe$  for  $b \in T$ , and so  $\tau(T) \subset P$ . If  $b \in D$ , then  $L\tau(b) = b^{-1}Lb \subset M_2(\mathfrak{g}) \cap B^\circ = L$ . Thus  $L\tau(b) = L$ , since  $\det(\tau(b)) = 1$ . This means that  $\tau(D) \subset C$ . Now  $GL_2(F) = TD$  by Lemma 21.24. Thus  $SO^\varphi = \tau(GL_2(F)) = \tau(T)\tau(D) \subset PC$ , which proves (35.6).

We note here an easy fact included in the above proof:

(35.7a) *If  $x \in L^*$ , then  $x \in hC$  with  $h$  of the form  $h = ae + f + cg$  or  $h = cg$  with  $a \in \mathfrak{g}$  and  $2c \in \mathfrak{g}$ .*

Indeed, if  $q = \varphi[x] \in \mathfrak{g}$ , then  $x \in hC$  with  $h = qe + f$ . Otherwise  $x$  falls into Case 2b, and the above proof proves (35.7a).

Here we proved (35.6) only for isotropic  $\varphi$  of dimension 3. In fact, equality (35.6) holds for an arbitrary dimension. For this fact the reader is referred to [S04b, Theorem 6.13].

**Theorem 35.3.** *Given  $(V, \varphi)$  over a local field as in §35.1, let  $\Lambda$  be an arbitrary  $\mathfrak{g}$ -lattice in  $V$ , and  $h$  an element of  $\Lambda$  such that  $\varphi[h] \neq 0$ ; let  $D = \{\gamma \in SO^\varphi \mid \Lambda\gamma = \Lambda\}$ . Then there exists a finite subset  $A$  of  $SO^\varphi$  such that*

$$(35.8) \quad \{x \in \Lambda \mid \varphi[x] = \varphi[h]\} = \bigsqcup_{\alpha \in A} h\alpha D.$$

Moreover, we can take  $A = \{1\}$  if  $\dim(V) > 1$ ,  $\Lambda$  is maximal,  $\varphi[h] \in \mathfrak{g}^\times$ , and  $2 \notin \mathfrak{p}$ .

PROOF. This is obvious if  $\dim(V) = 1$ ; so we assume  $\dim(V) > 1$ . Let  $C$  be as in (35.1) with a maximal lattice  $L$  in  $V$ . We have  $[C : C \cap D] < \infty$  and  $a\Lambda \subset L$  for some  $a \in F^\times$ . Thus it is sufficient to prove the case  $\Lambda = L$ . To prove the last assertion, suppose  $h \in L$ ,  $\varphi[h] \in \mathfrak{g}^\times$ , and  $2 \notin \mathfrak{p}$ . Define  $M$  as in Lemma 32.4(ii) for the present  $L$  with  $Fh$  as  $X$ . Clearly  $M = \mathfrak{g}h$ , and so  $L = \mathfrak{g}h \oplus (L \cap X^\perp)$ . If  $k \in L$  and  $\varphi[k] = \varphi[h]$ , then similarly  $L = \mathfrak{g}k \oplus (L \cap Y^\perp)$ , where  $Y = Fk$ . By (35.1),  $k = h\gamma$  with an element  $\gamma$  of  $SO^\varphi$ . Then  $X^\perp\gamma = Y^\perp$ . Since  $L$  is maximal, we easily see that  $L \cap X^\perp$  and  $L \cap Y^\perp$  are maximal. Therefore  $(L \cap X^\perp)\gamma$  is a maximal lattice in  $Y^\perp$ , and so by

Lemma 29.9,  $(L \cap X^\perp)\gamma\beta = L \cap Y^\perp$  with some  $\beta \in SO^\varphi(Y^\perp)$ . We can extend  $\beta$  to an element of  $SO^\varphi(V)$  so that  $k\beta = k$ . Then  $L\gamma\beta = L$  and  $h\gamma\beta = k$ , which proves the last assertion.

Next, if  $x \in L$  and  $\varphi[x] = \varphi[h]$ , then  $2\varphi[h]\mathfrak{g} \subset 2\varphi(x, L) \subset \mathfrak{g}$ . Thus, the set on the left-hand side of (35.8) for  $\Lambda = L$  is contained in  $\bigsqcup_{\mathfrak{b}} \{x \in V \mid \varphi[x] = \varphi[h], 2\varphi(x, L) = \mathfrak{b}\}$ , where  $\mathfrak{b}$  runs over all the integral divisors of  $2\varphi[h]\mathfrak{g}$ . Therefore, by Theorem 35.2, equality (35.8) for  $\Lambda = L$  holds with  $A$  such that  $\#A$  is at most the number of such ideals  $\mathfrak{b}$ . This completes the proof.

For  $h \in V$  and  $z \in O^\varphi(V)_\mathbf{A}$  the element  $hz$  is meaningful as an element of  $V_\mathbf{A}$ , and so  $V \cap hT$  for a subset  $T$  of  $O^\varphi(V)_\mathbf{A}$  is a meaningful subset of  $V$ .

We now prove the global version of Theorem 35.3 as follows.

**Theorem 35.4.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over a global field  $F$  of dimension  $n$ . Let  $L$  be a  $\mathfrak{g}$ -lattice in  $V$ ,  $C = \{\gamma \in SO^\varphi(V)_\mathbf{A} \mid L\gamma = L\}$ , and  $\Gamma = SO^\varphi(V) \cap C$ ; let  $h$  be an element of  $L$  such that  $\varphi[h] \neq 0$  and let  $\mathfrak{X} = \{x \in SO^\varphi(V)_\mathbf{A} \mid hx_v \in L_v \text{ for every } v \in \mathbf{h}\}$ . Then the following assertions hold:*

- (i)  $\{k \in L \mid \varphi[k] = \varphi[h]\} = \bigsqcup_{i=1}^\nu k_i \Gamma$  with a finite set  $\{k_i\}_{i=1}^\nu \subset L$ .
- (ii) Put  $W = (Fh)^\perp$ . Then  $SO^\varphi(W) \backslash \mathfrak{X}/C$  is finite.

PROOF. Since our assertions are trivial if  $n = 1$ , we assume that  $n > 1$ . For simplicity put  $G = SO^\varphi(V)$ ,  $H = SO^\varphi(W)$ , and  $C_v = C \cap G_v$  for  $v \in \mathbf{h}$ . We can identify  $H$  with  $\{\alpha \in G \mid h\alpha = h\}$ . By Theorem 35.3, for each  $v \in \mathbf{h}$  there exists a finite subset  $X_v$  of  $G_v$  such that

$$\{x \in L_v \mid \varphi[x] = \varphi[h]\} = \bigsqcup_{\gamma \in X_v} h\gamma C_v;$$

moreover, we can take  $X_v = \{1\}$  for almost all  $v$ . Therefore we can find a finite subset  $X$  of  $G_\mathbf{h}$  such that  $h\mathfrak{X} = \bigcup_{\xi \in X} h\xi C$ . Thus for every  $x \in \mathfrak{X}$  we have  $hx = h\xi\delta$  with some  $\xi \in X$  and  $\delta \in C$ . Then  $\xi\delta x^{-1} \in H_\mathbf{A}$ , which shows that  $\mathfrak{X} = \bigcup_{\xi \in X} H_\mathbf{A}\xi C$ . Applying Theorem 30.8 to  $H$ , for each  $\xi \in X$  we can find a finite subset  $E_\xi$  of  $H_\mathbf{h}$  such that  $H_\mathbf{A} = \bigsqcup_{\varepsilon \in E_\xi} H\varepsilon(H_\mathbf{A} \cap \xi C\xi^{-1})$ . Then  $H_\mathbf{A}\xi C = \bigcup_{\varepsilon \in E_\xi} H\varepsilon\xi C$ , and so  $\mathfrak{X} = \bigcup_{\varepsilon, \xi} H\varepsilon\xi C$ . This proves (ii). Let  $k$  be an element of  $L$  such that  $\varphi[k] = \varphi[h]$ . By (35.1),  $k = h\alpha$  with  $\alpha \in G$ . Then  $\alpha \in \mathfrak{X}$ , so that  $\alpha \in H\varepsilon\xi C$  with some  $(\varepsilon, \xi)$ . For each  $(\varepsilon, \xi)$  such that  $G \cap \varepsilon\xi C \neq \emptyset$ , pick any  $\beta \in G \cap \varepsilon\xi C$ . Then  $G \cap H\varepsilon\xi C = G \cap H\beta C = H\beta\Gamma$ . Let  $B$  be the set of such  $\beta$ 's chosen for each  $(\varepsilon, \xi)$ . Then  $\alpha \in \bigsqcup_{\beta \in B} H\beta\Gamma$ , and so  $k = h\alpha \in \bigsqcup_{\beta \in B} h\beta\Gamma$ , which proves (i) and completes the proof.

**35.5.** Let  $(V, \varphi)$  be a nondegenerate quadratic space over a global field  $F$  of dimension  $n$ . Given a  $\mathfrak{g}$ -lattice  $L$  in  $V$ ,  $q \in F^\times$ , and a  $\mathfrak{g}$ -ideal  $\mathfrak{b}$ , we put

$$(35.9a) \quad \Gamma(L) = \{\gamma \in SO^\varphi(V) \mid L\gamma = L\},$$

$$(35.9b) \quad C = \{x \in SO^\varphi(V)_\mathbf{A} \mid Lx = L\},$$

$$(35.9c) \quad L[q, \mathfrak{b}] = \{x \in V \mid \varphi[x] = q, \varphi(x, L) = \mathfrak{b}\}.$$

We will later assume that  $L$  is maximal, but for the moment we don't need that condition. Clearly  $\Gamma(L) = C \cap SO^\varphi(V)$ . We have also  $\Gamma(L) = \Gamma(\tilde{L})$ , since  $(L\gamma)^\sim = \tilde{L}\gamma$  for every  $\gamma \in O^\varphi$  as noted in §29.1. We easily see that  $\Gamma(L)$  acts on the right of  $L[q, \mathfrak{b}]$ , and  $L[q, \mathfrak{b}] \subset 2\mathfrak{b}\tilde{L}$ . Therefore, by Theorem 35.4,  $\#(L[q, \mathfrak{b}]/\Gamma(L)) < \infty$ . ( $L[q, \mathfrak{b}]$  is not necessarily contained in  $L$ .)

For an algebraic subgroup  $H$  of  $O^\varphi$ ,  $SO^\varphi$ , or  $G^+(V)$ , we can speak of the  $H$ -genus and  $H$ -class of  $L$  as defined in §30.1. We let  $G^+(V)$  act on  $V$  by the rule  $x\alpha = x\tau(\alpha)$  for  $x \in V$  and  $\alpha \in G^+(V)$ , and so for a subgroup  $J$  of  $G^+(V)$  the  $J$ -genus and  $J$ -class of  $L$  are the same as the  $\tau(J)$ -genus and  $\tau(J)$ -class of  $L$ . As noted in §30.1, the  $SO^\varphi(V)$ -genus of a maximal lattice consists of all the maximal lattices in  $V$ , and it coincides with the  $O^\varphi(V)$ -genus of the lattice. We call it, as we did there, the  $\varphi$ -genus of maximal lattices.

We now state the main theorem of quadratic Diophantine equations.

**Theorem 35.6.** *Let  $(V, \varphi)$  be a nondegenerate quadratic space over a global field  $F$  of dimension  $> 1$ . Define  $C$  by (35.9b) with a fixed lattice  $L$  in  $V$ . Let  $h$  be an element of  $V$  such that  $\varphi[h] \neq 0$ ; put  $W = (Fh)^\perp$ ,  $G = SO^\varphi(V)$ , and  $H = SO^\varphi(W)$ . Let us consider  $H$  a subgroup of  $G$  by defining the action of  $H$  on  $Fh$  to be trivial. Thus  $H = \{\alpha \in G \mid h\alpha = h\}$ . Then the following assertions hold:*

(i) *For  $y \in G_{\mathbf{A}}$  we have  $H_{\mathbf{A}} \cap GyC \neq \emptyset$  if and only if  $V \cap hCy^{-1} \neq \emptyset$ .*

(ii) *Fixing  $y \in G_{\mathbf{A}}$ , take  $\mathcal{E} \subset H_{\mathbf{A}}$  so that  $H_{\mathbf{A}} \cap GyC = \bigsqcup_{\varepsilon \in \mathcal{E}} H\varepsilon(H_{\mathbf{A}} \cap C)$ . For every  $\varepsilon \in \mathcal{E}$  take  $\alpha_\varepsilon \in G$  so that  $\varepsilon \in \alpha_\varepsilon yC$ . Then the map  $\varepsilon \mapsto h\alpha_\varepsilon$  gives a bijection of  $H \backslash (H_{\mathbf{A}} \cap GyC) / (H_{\mathbf{A}} \cap C)$  onto  $(V \cap hCy^{-1}) / \Gamma^y$ , where  $\Gamma^y = G \cap yCy^{-1}$ .*

(iii) *Take  $Y \subset H_{\mathbf{A}}$  so that  $GH_{\mathbf{A}}C = \bigsqcup_{y \in Y} GyC$ . Then*

$$(35.10a) \quad \#\{(V \cap hCy^{-1}) / \Gamma^y\} = \#\{H \backslash (H_{\mathbf{A}} \cap GyC) / (H_{\mathbf{A}} \cap C)\},$$

$$(35.10b) \quad \#\{H \backslash H_{\mathbf{A}} / (H_{\mathbf{A}} \cap C)\} = \sum_{y \in Y} \#\{(V \cap hCy^{-1}) / \Gamma^y\}.$$

(iv) *Let  $\Xi$  be the  $H$ -genus of  $L$  and let  $\Lambda = \{Ly^{-1} \mid y \in Y\}$  with  $Y$  as in (iii). Then  $\Lambda$  is a minimal subset of  $\Xi$  with the property that every member of  $\Xi$  is of the form  $M\alpha$  with some  $M \in \Lambda$  and  $\alpha \in G$ .*

(v) *In particular, suppose  $L$  is maximal and  $n > 2$ ; put  $q = \varphi[h]$  and  $\mathfrak{b} = \varphi(h, L)$ . Then*

$$(35.11) \quad V \cap hCy^{-1} = (Ly^{-1})[q, \mathfrak{b}] \text{ for every } y \in G_{\mathbf{A}},$$

$$(35.12a) \quad \#\{M[q, \mathfrak{b}] / \Gamma(M)\} = \#\{H \backslash (H_{\mathbf{A}} \cap GyC) / (H_{\mathbf{A}} \cap C)\} \\ \text{if } M = Ly^{-1}, y \in H_{\mathbf{A}},$$

$$(35.12b) \quad \#\{H \backslash H_{\mathbf{A}} / (H_{\mathbf{A}} \cap C)\} = \sum_{M \in \Lambda} \#\{M[q, \mathfrak{b}] / \Gamma(M)\}.$$



(vi) Let  $Q$  be an open subgroup of  $G^+(V)_{\mathbf{A}}$  containing  $G^+(V)_{\mathbf{a}}$  and let  $\Delta^x = G^+(V)_{\mathbf{A}} \cap xQx^{-1}$  for  $x \in G^+(V)_{\mathbf{A}}$ . Then (ii) and (iii) are valid with  $\{G^+(V), G^+(W), Q, \Delta^x\}$  in place of  $\{G, H, C, \Gamma^y\}$ . Moreover, if  $L, q$ , and  $\mathbf{b}$  are as in (v) and  $\tau(Q) = C$ , then

$$(35.13a) \quad \begin{aligned} & \# \{G^+(W) \setminus [G^+(W)_{\mathbf{A}} \cap G^+(V)zQ] / [G^+(W)_{\mathbf{A}} \cap Q]\} \\ &= \# \{M[q, \mathbf{b}] / \Delta(M)\} \text{ if } M = L\tau(z^{-1}), z \in G^+(W)_{\mathbf{A}}, \end{aligned}$$

$$(35.13b) \quad \# \{G^+(W) \setminus G^+(W)_{\mathbf{A}} / [G^+(W)_{\mathbf{A}} \cap Q]\} = \sum_M \# \{M[q, \mathbf{b}] / \Delta(M)\},$$

where  $\Delta(M) = \{\alpha \in G^+(V) \mid M\tau(\alpha) = M\}$ , and  $M$  runs over the lattices  $L\tau(z)^{-1}$  with  $z \in G^+(V) \setminus G^+(V)G^+(W)_{\mathbf{A}}Q/Q$ .

*Note:* Since  $G \setminus G_{\mathbf{A}}/C$  and  $H \setminus H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)$  are finite sets by Theorem 30.8, we see that  $Y$  is a finite set, and also from (ii) we see that  $(V \cap hDy^{-1})/\Gamma^y$  is a finite set. Also, we easily see that  $\Gamma(M) = \tau(\Delta(M))$ , since  $\tau(G^+(V)) = SO^{\varphi}(V)$ .

PROOF. Let  $y, \varepsilon$ , and  $\alpha_{\varepsilon}$  be as in (ii); then  $\alpha_{\varepsilon} \in \varepsilon Cy^{-1}$ , and so  $h\alpha_{\varepsilon} \in V \cap hCy^{-1}$ . If  $\eta\varepsilon\zeta \in \beta yC$  with  $\eta \in H, \zeta \in H_{\mathbf{A}} \cap C$ , and  $\beta \in G$ , then  $\beta^{-1}\eta\alpha_{\varepsilon} \in G \cap yCy^{-1} = \Gamma^y$ , and so  $h\alpha_{\varepsilon} = h\eta\alpha_{\varepsilon} \in h\beta\Gamma^y$ . Thus our map of (ii) is well defined. Next let  $k \in V \cap hCy^{-1}$ . Then  $k = h\delta y^{-1}$  with  $\delta \in C$ , and moreover, by (35.1),  $k = h\xi$  with  $\xi \in G$ . Then  $h = h\xi y\delta^{-1}$ , so that  $\xi y\delta^{-1} \in H_{\mathbf{A}}$ . Thus  $\xi y\delta^{-1} \in H_{\mathbf{A}} \cap GyC$ . This shows that  $k$  is the image of an element of  $H_{\mathbf{A}} \cap GyC$ . To prove that the map is injective, suppose  $\varepsilon \in \alpha yC \cap H_{\mathbf{A}}$  and  $\delta \in \beta yC \cap H_{\mathbf{A}}$  with  $\alpha, \beta \in G$ , and  $h\alpha = h\beta\sigma$  with  $\sigma \in \Gamma^y$ . Put  $\omega = \beta\sigma\alpha^{-1}$ . Then  $h\omega = h$ , so that  $\omega \in H$ . Since  $\sigma \in yCy^{-1}$ , we have  $\beta yC = \beta\sigma yC = \omega\alpha yC$ , and so  $\delta \in \beta yC \cap H_{\mathbf{A}} = \omega\alpha yC \cap H_{\mathbf{A}} = \omega(\alpha yC \cap H_{\mathbf{A}}) = \omega(\varepsilon C \cap H_{\mathbf{A}}) = \omega\varepsilon(C \cap H_{\mathbf{A}}) \subset H\varepsilon(C \cap H_{\mathbf{A}})$ . This proves the injectivity, and completes the proof of (ii). At the same time we obtain (i).

We have  $H_{\mathbf{A}} = \bigsqcup_{y \in Y} (H_{\mathbf{A}} \cap GyC)$  with  $Y$  as in (iii), and so (35.10a, b) follow immediately from (ii). To prove (iv), let  $x \in H_{\mathbf{A}}$ . Then  $x \in GyC$  with some  $y \in Y$ , and so  $x \in \alpha yC$  with some  $\alpha \in G$ . Thus  $Lx^{-1} = Ly^{-1}\alpha^{-1}$ . If  $Ly^{-1} = Lz^{-1}\beta$  with  $y, z \in Y$  and  $\beta \in G$ , then  $z^{-1}\beta y \in C$ , and so  $y \in GzC$ . Thus  $y = z$ , which shows that  $\Lambda$  is a minimal subset with the property described in (iv).

As for (v), clearly  $V \cap hC \subset L[q, \mathbf{b}]$ . Conversely, every element of  $L[q, \mathbf{b}]$  belongs to  $hC$  by virtue of Theorem 35.2. Thus

$$(35.14) \quad V \cap hC = L[q, \mathbf{b}].$$

Let  $k \in V \cap hCy^{-1}$  with  $y \in G_{\mathbf{A}}$ ; put  $M = Ly^{-1}$ . Then  $\varphi[k] = q$ ,  $\varphi(k, M) = \varphi(h, L) = \mathbf{b}$ , and  $kyCy^{-1} = hCy^{-1}$ . Taking  $k, M$ , and  $yCy^{-1}$  in place of  $h, L$ , and  $C$  in (35.14), we obtain  $V \cap hCy^{-1} = V \cap kyCy^{-1} = M[q, \mathbf{b}] = (Ly^{-1})[q, \mathbf{b}]$ . This proves (35.11) when  $V \cap hCy^{-1} \neq \emptyset$ . To prove the remaining

case, suppose  $\ell \in (Ly^{-1})[q, \mathfrak{b}]$ ; then  $\varphi(\ell y_v, L_v) = \mathfrak{b}_v = \varphi(h, L)_v$  for every  $v \in \mathbf{h}$ . By Theorem 35.2,  $\ell y \in hC$ , and hence  $\ell \in hCy^{-1}$ . This shows that if  $(Ly^{-1})[q, \mathfrak{b}] \neq \emptyset$ , then  $V \cap hCy^{-1} \neq \emptyset$ , and so (35.11) holds for every  $y \in G_{\mathbf{A}}$ . This combined with (35.10a, b) produces (35.12a, b). Assertion (vi) can be proved by repeating all these arguments with the replaced symbols as specified, since  $G^+(W) = \{\alpha \in G^+(V) \mid h\alpha = h\}$  as noted in (24.3a). This completes the proof.

**Remark 35.7.** (1) Formulas (35.12b) and (35.13b) are precise versions of (34.9a). As explained in §30.7,  $\#\{H \backslash H_{\mathbf{A}} / (H \cap C)\}$  is a generalized class number of  $H$ ; it may or may not be the number of classes in the  $H$ -genus of a lattice in  $W$ . The precise version of (34.9b) will be given in Theorem 37.12.

(2) The set  $Y$  in (35.10) can be replaced by a subset  $X$  of  $G_{\mathbf{A}}$  such that  $G_{\mathbf{A}} = \bigsqcup_{x \in X} GxC$ , which amounts to the addition of several zeros corresponding to the elements  $x$  such that  $H_{\mathbf{A}} \cap GxC = \emptyset$ .

(3) In this book we consider only an equation of type  $\varphi[h] = q$  with a scalar  $q$ . More generally, we can discuss an equation  $\xi \Phi \cdot {}^t\xi = \Psi$  with  $\Psi$  of size  $m > 1$ . For details, the reader is referred to [S04b, Section 13] and [S06c].

### 36. Classification of binary forms

**36.1.** We first recall some basic facts concerning the orders in a quadratic extension of  $F$ . For the moment  $F$  is either local or global. We take symbols  $K$ ,  $\mathfrak{r}$ , and  $\rho$  in the following two cases:

(I)  $K$  is a quadratic extension of  $F$ ,  $\mathfrak{r}$  is the maximal order of  $K$ , and  $\rho$  is the generator of  $\text{Gal}(K/F)$ .

(II)  $K = F \oplus F$ ,  $\mathfrak{r} = \mathfrak{g} \oplus \mathfrak{g}$ , and  $\rho$  is the automorphism of  $K$  given by  $(a, b)^{\rho} = (b, a)$  for  $(a, b) \in F \oplus F$ .

Let  $\mathfrak{f}$  be an order in  $K$  containing  $\mathfrak{g}$  in the sense of §21.1. Since  $\mathfrak{f} \subset \mathfrak{r}$ , we have  $a + a^{\rho} \in \mathfrak{g}$  for every  $a \in \mathfrak{f}$ , and so  $\mathfrak{f}^{\rho} = \mathfrak{f}$ . Put  $\mathfrak{c} = \{\alpha \in \mathfrak{g} \mid \alpha\mathfrak{r} \subset \mathfrak{f}\}$ . Then  $\mathfrak{c}$  is an integral  $\mathfrak{g}$ -ideal, which we call the **conductor** of  $\mathfrak{f}$ .

Let us now show that for every integral  $\mathfrak{g}$ -ideal  $\mathfrak{c}$  there is a unique order in  $K$  of conductor  $\mathfrak{c}$ , and it is given by  $\mathfrak{f} = \mathfrak{g} + \mathfrak{c}\mathfrak{r}$ . Clearly the global case can be reduced to the local case; so assume  $F$  to be local. Take  $u \in \mathfrak{r}$  and  $c \in \mathfrak{g}$  so that  $\mathfrak{r} = \mathfrak{g}[u]$  and  $\mathfrak{c} = c\mathfrak{g}$ . Suppose that  $\mathfrak{c}$  is the conductor of an order  $\mathfrak{f}$ ; then clearly  $\mathfrak{c} = \{\alpha \in \mathfrak{g} \mid \alpha u \in \mathfrak{f}\}$ . If  $a + bu \in \mathfrak{f}$  with  $a, b \in \mathfrak{g}$ , then  $b \in \mathfrak{c}$ . Therefore we have  $\mathfrak{f} = \mathfrak{g} + \mathfrak{c}u = \mathfrak{g} + \mathfrak{g}cu = \mathfrak{g} + \mathfrak{c}\mathfrak{r}$ . Conversely, given an integral  $\mathfrak{g}$ -ideal  $\mathfrak{c}$ , we see that  $\mathfrak{g} + \mathfrak{c}\mathfrak{r} = \mathfrak{g} + \mathfrak{c}u$  and this has conductor  $\mathfrak{c}$ , which proves the desired fact. Also every order  $\mathfrak{f}$  in the local case contains an element  $v$  such that  $\mathfrak{f} = \mathfrak{g}[v]$ . Indeed, we can take  $cu$  above as  $v$ .

In both local and global cases, given an order  $\mathfrak{f}$  in  $K$ , we denote by  $\delta(\mathfrak{f})$  the  $\mathfrak{g}$ -ideal generated by  $(x - x^{\rho})^2$  for all  $x \in \mathfrak{f}$ , and call it the **discriminant**

of  $\mathfrak{f}$ . If  $\mathfrak{c}$  is the conductor of  $\mathfrak{f}$ , then we easily see that  $\delta(\mathfrak{f}) = \mathfrak{c}^2\delta(\mathfrak{r})$ ;  $\delta(\mathfrak{r})$  is the discriminant of  $K$  relative to  $F$ . (In the local case we have  $D(K/F) = (u-u^\rho)^2\mathfrak{r} = \delta(\mathfrak{r})$  with  $u$  such that  $\mathfrak{r} = \mathfrak{g}[u]$ ; see (14.9). In the global case, use Theorem 14.4(ii).) Thus, once  $K$  is fixed,  $\mathfrak{f}$  is completely determined by its discriminant. In the local case if  $\mathfrak{f} = \mathfrak{g}[v]$  with  $v \in \mathfrak{r}$ , then  $\delta(\mathfrak{f}) = (v - v^\rho)^2\mathfrak{g}$ . We note that in both local and global cases we have

$$(36.1) \quad \mathfrak{r}^\times \cap \mathfrak{f} = \mathfrak{f}^\times.$$

Indeed, if  $a \in \mathfrak{r}^\times \cap \mathfrak{f}$ , then  $a^\rho \in \mathfrak{r}^\times \cap \mathfrak{f}$  and  $aa^\rho \in \mathfrak{g}^\times \subset \mathfrak{f}^\times$ , and so  $a^{-1} = a^\rho(aa^\rho)^{-1} \in \mathfrak{f}$ , which proves (36.1).

Now in both local and global cases, for a  $\mathfrak{g}$ -lattice  $\mathfrak{m}$  in  $K$  put

$$(36.2) \quad \mathfrak{m}^* = \{\alpha \in K \mid \text{Tr}_{K/F}(\alpha\mathfrak{m}) \subset \mathfrak{g}\}.$$

Here  $\text{Tr}_{K/F}((a, b)) = a + b$  if  $K = F \oplus F$ . Then  $\mathfrak{m}^*$  is a  $\mathfrak{g}$ -lattice in  $K$  and  $(\mathfrak{m}^*)^* = \mathfrak{m}$ ; if  $\mathfrak{n} \subset \mathfrak{m}$ , then  $\mathfrak{m}^* \subset \mathfrak{n}^*$ . If  $\mathfrak{f} = \mathfrak{g}[v]$ , then  $\mathfrak{f}^* = (v - v^\rho)^{-1}\mathfrak{f}$  because  $((v - v^\rho)^{-1}, (v^\rho - v)^{-1}v^\rho)$  is the dual basis of  $(v, 1)$  with respect to  $(x, y) \mapsto \text{Tr}_{K/F}(xy)$ . Given an order  $\mathfrak{f}$  in  $K$  and a  $\mathfrak{g}$ -lattice  $\mathfrak{m}$  in  $K$ , we call  $\mathfrak{m}$  a **proper  $\mathfrak{f}$ -ideal** if  $\mathfrak{f} = \{\alpha \in K \mid \alpha\mathfrak{m} \subset \mathfrak{m}\}$ .

**Theorem 36.2.** (i) *Let  $\mathfrak{f}$  be an order in  $K$  of the above types over a local or global field  $F$ . Then all the proper  $\mathfrak{f}$ -ideals form a commutative group if we take the product  $\mathfrak{m}\mathfrak{n}$  to be the  $\mathfrak{g}$ -lattice spanned by the products  $xy$  with  $x \in \mathfrak{m}$  and  $y \in \mathfrak{n}$ ; the identity element of this group is  $\mathfrak{f}$ , and  $\mathfrak{m}^{-1} = \{a \in K \mid a\mathfrak{m} \subset \mathfrak{f}\}$ .*

(ii) *In the local case, a  $\mathfrak{g}$ -lattice  $\mathfrak{m}$  in  $K$  is a proper  $\mathfrak{f}$ -ideal if and only if  $\mathfrak{m} = \gamma\mathfrak{f}$  with  $\gamma \in K^\times$ .*

PROOF. Clearly the global case of (i) follows from the local case, which in turn follows from (ii). Thus it is sufficient to prove (ii). The “if”-part of (ii) is obvious. If  $\alpha\mathfrak{m} \subset \mathfrak{m}$  or  $\alpha\mathfrak{m}^* \subset \mathfrak{m}^*$  for  $\alpha \in K$  and a  $\mathfrak{g}$ -lattice  $\mathfrak{m}$  in  $K$ , then  $\text{Tr}_{K/F}(\alpha\mathfrak{m}\mathfrak{m}^*) \subset \text{Tr}_{K/F}(\mathfrak{m}\mathfrak{m}^*) \subset \mathfrak{g}$ , so that  $\alpha\mathfrak{m}^* \subset \mathfrak{m}^*$  and  $\alpha\mathfrak{m} \subset (\mathfrak{m}^*)^* = \mathfrak{m}$ . Take  $\mathfrak{m}$  to be a proper  $\mathfrak{f}$ -ideal. Then we find that  $\mathfrak{f} = \{\alpha \in K \mid \alpha\mathfrak{m}^* \subset \mathfrak{m}^*\}$ . If  $\xi \in (\mathfrak{m}\mathfrak{m}^*)^*$ , then  $\text{Tr}_{K/F}(\xi\mathfrak{m}\mathfrak{m}^*) \subset \mathfrak{g}$ , so that  $\xi\mathfrak{m}^* \subset \mathfrak{m}^*$ ; hence  $\xi \in \mathfrak{f}$ . Thus  $(\mathfrak{m}\mathfrak{m}^*)^* \subset \mathfrak{f}$ , and so  $\mathfrak{f}^* \subset \mathfrak{m}\mathfrak{m}^*$ . On the other hand  $\text{Tr}_{K/F}(\mathfrak{f}\mathfrak{m}\mathfrak{m}^*) = \text{Tr}_{K/F}(\mathfrak{m}\mathfrak{m}^*) \subset \mathfrak{g}$ , and so  $\mathfrak{m}\mathfrak{m}^* \subset \mathfrak{f}^*$ ; thus  $\mathfrak{m}\mathfrak{m}^* = \mathfrak{f}^* = e^{-1}\mathfrak{f}$ , where  $e = v - v^\rho$  with an element  $v$  such that  $\mathfrak{f} = \mathfrak{g}[v]$ . Take  $u \in \mathfrak{r}$  so that  $\mathfrak{r} = \mathfrak{g}[u]$ , and define an  $F$ -linear map  $f : K \rightarrow F$  by  $f(r + su) = r$  for  $r, s \in F$ . Then  $f(e\mathfrak{m}\mathfrak{m}^*) = f(\mathfrak{f}) = \mathfrak{g}$ , so that we can find an element  $\mu$  of  $e\mathfrak{m}^*$  such that  $f(\mu\mathfrak{m}) = \mathfrak{g}$ . Then  $\mu\mathfrak{m} \subset e\mathfrak{m}\mathfrak{m}^* = \mathfrak{f}$ . If  $\alpha \in \mathfrak{f}$ , then  $f(\alpha) = f(\beta)$  with  $\beta \in \mu\mathfrak{m}$ , and  $\alpha - \beta \in \mathfrak{g}u \cap \mathfrak{f} = \mathfrak{c}u$ , where  $\mathfrak{c}$  is the conductor of  $\mathfrak{f}$ . Thus  $\alpha \in \mu\mathfrak{m} + \mathfrak{c}\mathfrak{r}$ . This shows that  $\mathfrak{f} = \mu\mathfrak{m} + \mathfrak{c}\mathfrak{r}$ . Then  $\mathfrak{f} = \mathfrak{f}\mathfrak{f} = (\mu\mathfrak{m} + \mathfrak{c}\mathfrak{r})(\mu\mathfrak{m} + \mathfrak{c}\mathfrak{r}) \subset \mu\mathfrak{m} + \mathfrak{c}^2\mathfrak{r} \subset \mu\mathfrak{m} + \mathfrak{c}\mathfrak{f} \subset \mathfrak{f}$ . Thus  $\mathfrak{f} = \mu\mathfrak{m} + \mathfrak{c}\mathfrak{f}$ . Our theorem is obvious if  $\mathfrak{c} = \mathfrak{g}$ ; so suppose  $\mathfrak{c} \neq \mathfrak{g}$ . Then  $\mathfrak{f} = \mu\mathfrak{m} + \mathfrak{c}(\mu\mathfrak{m} + \mathfrak{c}\mathfrak{f}) = \mu\mathfrak{m} + \mathfrak{c}^2\mathfrak{f}$ . Repeating a similar calculation, we find that

$\mathfrak{f} = \mu\mathfrak{m} + \mathfrak{c}^k\mathfrak{f}$  for every positive integer  $k$ . Taking  $k$  so that  $\mathfrak{c}^k\mathfrak{f} \subset \mu\mathfrak{m}$ , we obtain  $\mathfrak{f} = \mu\mathfrak{m}$ . This completes the proof.

**Lemma 36.3.** *The notation being as in §36.1, assume that  $F$  is local; let  $\{K/F\}$  denote 1,  $-1$ , or 0, according as  $K = F \oplus F$ ,  $K$  is an unramified quadratic extension of  $F$ , or  $K$  is a ramified quadratic extension of  $F$ . Let  $\mathfrak{f}$  be the order in  $K$  of conductor  $\mathfrak{p}^m$ ,  $0 \leq m \in \mathbf{Z}$ , and  $\mathfrak{d}$  the different of  $K$  relative to  $F$ . Put  $\tau(x) = x^\rho/x$  for  $x \in K$ . Then the following assertions hold:*

- (i)  $\tau$  gives an isomorphism of  $\mathfrak{r}^\times/\mathfrak{f}^\times$  onto  $\tau(\mathfrak{r}^\times)/\tau(\mathfrak{f}^\times)$ ;
- (ii)  $\mathfrak{f}^\times = \{a \in \mathfrak{r}^\times \mid a^\rho - a \in \mathfrak{p}^m\mathfrak{d}\}$ ;
- (iii)  $\tau(\mathfrak{f}^\times) = \{y \in \mathfrak{r}^\times \mid yy^\rho = 1, y - 1 \in \mathfrak{p}^m\mathfrak{d}\}$ ;
- (iv)  $[\mathfrak{r}^\times : \mathfrak{f}^\times] = q^m(1 - \{K/F\}q^{-1})$  if  $m > 0$ , where  $q = \#(\mathfrak{g}/\mathfrak{p})$ .

PROOF. To prove (i), suppose  $a \in \mathfrak{r}^\times$  and  $\tau(a) \in \tau(\mathfrak{f}^\times)$ ; then  $\tau(a) = \tau(b)$  with  $b \in \mathfrak{f}^\times$ , and so  $a = cb$  with  $c \in F^\times$ . Clearly  $c \in \mathfrak{g}^\times \subset \mathfrak{f}^\times$ , and so  $a \in \mathfrak{f}^\times$ . This proves (i). To prove (ii), take  $u \in \mathfrak{r}$  so that  $\mathfrak{r} = \mathfrak{g}[u]$ . Then  $\mathfrak{d} = (u - u^\rho)\mathfrak{r}$ . If  $a = b + cu \in \mathfrak{r}$ , then  $a - a^\rho = c(u - u^\rho)$ , which combined with (36.1) proves (ii). To prove (iii), let  $y = \tau(x)$  with  $x \in \mathfrak{f}^\times$ . By (ii),  $x^\rho - x \in \mathfrak{p}^m\mathfrak{d}$ , and so  $y - 1 = (x^\rho - x)/x \in \mathfrak{p}^m\mathfrak{d}$ . Conversely, if  $yy^\rho = 1$  and  $y - 1 \in \mathfrak{p}^m\mathfrak{d}$ , then by Lemma 21.13(iii),  $y = x^\rho/x$  with  $x \in \mathfrak{r}^\times$ . We have then  $x^\rho - x = x(y - 1) \in \mathfrak{p}^m\mathfrak{d}$ , and so  $x \in \mathfrak{f}^\times$  by (ii). This proves (iii). Put  $\mathfrak{c} = \mathfrak{p}^m$  and denote by  $f$  the natural map of  $\mathfrak{r}^\times$  onto  $(\mathfrak{r}/\mathfrak{c}\mathfrak{r})^\times$ . Since  $\mathfrak{f} = \mathfrak{g} + \mathfrak{c}\mathfrak{r}$ , we easily see that  $f(a) \in (\mathfrak{g}/\mathfrak{c})^\times$  for  $a \in \mathfrak{r}^\times$  if and only if  $a \in \mathfrak{f}^\times$ . Thus  $[\mathfrak{r}^\times : \mathfrak{f}^\times] = [(\mathfrak{r}/\mathfrak{c}\mathfrak{r})^\times : (\mathfrak{g}/\mathfrak{c})^\times]$ , from which our formula of (iv) follows immediately.

**36.4.** Given an order  $\mathfrak{f}$  in  $K$ , we can define the class number of  $\mathfrak{f}$  as follows. Let  $\mathcal{I}(\mathfrak{f})$  be the group of all proper  $\mathfrak{f}$ -ideals in the sense of §36.1 and Theorem 36.2, and let  $\mathcal{P}(\mathfrak{f})$  be the subgroup of  $\mathcal{I}(\mathfrak{f})$  consisting of all  $\mathfrak{f}$ -ideals of the form  $\alpha\mathfrak{f}$  with  $\alpha \in K^\times$ . Then we put  $c(\mathfrak{f}) = [\mathcal{I}(\mathfrak{f}) : \mathcal{P}(\mathfrak{f})]$  and call  $c(\mathfrak{f})$  **the class number of  $\mathfrak{f}$** . A coset of  $\mathcal{I}(\mathfrak{f})/\mathcal{P}(\mathfrak{f})$  is called a **class of proper  $\mathfrak{f}$ -ideals**. For  $\mathfrak{f} = \mathfrak{r}$ ,  $c(\mathfrak{r})$  is the class number of  $K$ , which we denote by  $c_K$ . For  $K = F \oplus F$ , we have  $\mathfrak{r} = \mathfrak{g} \oplus \mathfrak{g}$ , and we easily see that  $c(\mathfrak{r})$  is  $c_F^2$ , where  $c_F$  is the class number of  $F$ ; thus we put  $c_K = c_F^2$  for  $K = F \oplus F$ . If  $\mathfrak{c}$  is the conductor of  $\mathfrak{f}$ , then

$$(36.3) \quad c(\mathfrak{f}) = c_K \cdot [\mathfrak{r}^\times : \mathfrak{f}^\times]^{-1} N(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \{1 - [K/F, \mathfrak{p}]N(\mathfrak{p})^{-1}\},$$

which can be proved as follows. Since every proper  $\mathfrak{f}$ -ideal can be written  $x\mathfrak{f}$  with  $x \in K_{\mathbf{A}}^\times$ , we easily see that  $c(\mathfrak{f}) = [K_{\mathbf{A}}^\times : K^\times X(\mathfrak{f})]$ , where  $X(\mathfrak{f}) = K_{\mathbf{A}}^\times \prod_{v \in \mathbf{h}} \mathfrak{f}_v^\times$ . Similarly  $c_K = [K_{\mathbf{A}}^\times : K^\times X(\mathfrak{r})]$ , and so

$$c(\mathfrak{f})/c_K = [K^\times X(\mathfrak{r}) : K^\times X(\mathfrak{f})] = [X(\mathfrak{r}) : X(\mathfrak{r}) \cap K^\times X(\mathfrak{f})].$$

We easily see that  $X(\mathfrak{r}) \cap K^\times X(\mathfrak{f}) = \mathfrak{r}^\times X(\mathfrak{f})$ . Thus

$$c(\mathfrak{f})/c_K = [X(\mathfrak{r}) : \mathfrak{r}^\times X(\mathfrak{f})] = [X(\mathfrak{r}) : X(\mathfrak{f})]/[\mathfrak{r}^\times X(\mathfrak{f}) : X(\mathfrak{f})].$$

Clearly  $\mathfrak{r}^\times \cap X(\mathfrak{f}) = \mathfrak{f}^\times$ , so that  $[\mathfrak{r}^\times X(\mathfrak{f}) : X(\mathfrak{f})] = [\mathfrak{r}^\times : \mathfrak{f}^\times]$ . On the other hand  $[X(\mathfrak{r}) : X(\mathfrak{f})] = \prod_{v|c} [\mathfrak{r}_v^\times : \mathfrak{f}_v^\times]$ , which can be determined by Lemma 36.3(iv). Therefore we obtain (36.3). Notice that the same reasoning proves (36.3) for  $K = F \oplus F$  if we put  $[K/F, \mathfrak{p}] = 1$ .

**36.5.** Let us now consider the genus and classes of maximal lattices for  $(V, \varphi)$  of dimension 2 over a global field  $F$ . As shown in Lemma 25.2(i), we can put  $(V, \varphi) = (K, c\kappa)$  with a suitable  $K$  as in §36.1,  $c \in F^\times$ , and  $\kappa[x] = xx^\rho$  for  $x \in K$ ;  $SO^\varphi(V)$  can be identified with the group

$$(36.4) \quad H = \{\alpha \in K^\times \mid \alpha\alpha^\rho = 1\}.$$

Taking the prime ideal decomposition of  $c\mathfrak{g}$ , we can put  $c\mathfrak{g} = \mathfrak{b}N_{K/F}(\mathfrak{a})$  with a fractional ideal  $\mathfrak{a}$  in  $K$  and a square-free integral ideal  $\mathfrak{b}$  in  $F$  whose prime factors remain prime in  $K$ . Then  $\mathfrak{a}^{-1}\mathfrak{r}$  is a maximal lattice in  $V$ ; see §29.10. Thus every maximal lattice is of the form  $\mathfrak{a}^{-1}\mathfrak{r}x$  with  $x \in H_{\mathbf{A}}$ . Put

$$(36.5) \quad E = \{z \in H_{\mathbf{A}} \mid \mathfrak{r}z = \mathfrak{r}\}.$$

Then  $E \cap H_v = \{a \in \mathfrak{r}_v^\times \mid aa^\rho = 1\}$  for every  $v \in \mathbf{h}$ . Since our group is commutative, each class of maximal lattices corresponds to a coset of  $H_{\mathbf{A}}/HE$ , and so the class number is  $[H_{\mathbf{A}} : HE]$ .

Assuming  $K$  to be a field, put  $\mathfrak{x} = x\mathfrak{r}$  with  $x \in H_{\mathbf{A}}$ ; then  $\mathfrak{x}\mathfrak{r}^\rho = \mathfrak{r}$ . Conversely, if  $\mathfrak{x}$  is an  $\mathfrak{r}$ -ideal such that  $\mathfrak{x}\mathfrak{r}^\rho = \mathfrak{r}$ , then, by a well-known principle, we can put  $\mathfrak{x} = \eta^{-1}\mathfrak{r}^\rho$  with an  $\mathfrak{r}$ -ideal  $\eta$ . Take  $y \in K_{\mathbf{A}}^\times$  so that  $\eta = y\mathfrak{r}$  and put  $x = y^\rho/y$ . Then  $x \in H_{\mathbf{A}}$  and  $\mathfrak{x} = x\mathfrak{r}$ . Thus the genus of maximal lattices consists of all the  $\mathfrak{r}$ -ideals of the form  $\mathfrak{a}^{-1}\mathfrak{x}$  with  $\mathfrak{x}$  such that  $\mathfrak{x}\mathfrak{r}^\rho = \mathfrak{r}$ .

Let  $\mathcal{I}_K$  denote the ideal group of  $K$  and  $\mathcal{I}_{K/F}$  the subgroup of  $\mathcal{I}_K$  generated by all the principal ideals and the ideals  $\mathfrak{z}$  such that  $\mathfrak{z}^\rho = \mathfrak{z}$ . Then it can easily be seen that the map  $\eta \mapsto \mathfrak{a}^{-1}\eta^{-1}\mathfrak{r}^\rho$  for  $\eta \in \mathcal{I}_K$  gives a bijection of  $\mathcal{I}_K/\mathcal{I}_{K/F}$  onto the set of classes in the genus of maximal lattices. Thus

$$(36.6a) \quad [H_{\mathbf{A}} : HE] = [\mathcal{I}_K : \mathcal{I}_{K/F}].$$

Now we have

$$(36.6b) \quad [\mathcal{I}_K : \mathcal{I}_{K/F}] = (c_K/c_F) \cdot 2^{1-\lambda}[\mathfrak{g}^\times : N_{K/F}(\mathfrak{r}^\times)].$$

Here  $c_K$  resp.  $c_F$  is the class number of  $K$  resp.  $F$ , and  $\lambda$  is the number of  $v \in \mathbf{v}$  ramified in  $K$ . This is a special case of a well-known formula for a cyclic extension of an algebraic number field, which can be found in most textbooks on class field theory. Here we cite an earliest reference [C, pp. 402–6]. When  $F = \mathbf{Q}$ , (36.6b) is well known in the so-called genus theory, and its proof will be given in §38.4.

If  $K = F \oplus F$ , we can take  $c = 1$ , and  $\mathfrak{r} = \mathfrak{g} \oplus \mathfrak{g}$ ; the genus of maximal lattices consists of  $\mathfrak{a} \oplus \mathfrak{a}^{-1}$  with all the  $\mathfrak{g}$ -ideals  $\mathfrak{a}$ ;  $SO^\varphi$  is isomorphic to  $F^\times$ .

We easily see that the class number in this case is exactly the class number of  $F^\times$ .

**36.6.** To study the relationship between  $G$  and  $H$  in Theorem 35.6 when  $\dim(V)=3$ , we take  $(V, \varphi) = (B^\circ, -\delta\beta^\circ)$  with a quaternion algebra  $B$  over a local or global  $F$  and  $\delta \in F^\times$  as in Lemma 25.2(ii). Then  $SO^\varphi(V)$  consists of the maps  $x \mapsto b^{-1}xb$  for  $x \in B^\circ$ , where  $b \in B^\times$ . Given  $h \in B^\circ$  such that  $hh^\iota \neq 0$ , put  $W = (Fh)^\perp$  and  $H = SO^\varphi(W)$ , and define a subalgebra  $K$  of  $B$  by  $K = F + Fh$ . (If we start from  $(V, \varphi)$  and define  $B$  as a subset of  $A(\varphi)$  as in the proof of Lemma 25.2(ii), then  $V = B^\circ z$ . Here we start from  $(B^\circ, -\delta\beta^\circ)$  with given  $B$  and  $\delta \in F^\times$ , and put  $(V, \varphi) = (B^\circ, -\delta\beta^\circ)$ , and so  $V = B^\circ$ . We don't need  $A(\varphi)$ ; we have to know only that  $G^+(\varphi) = B^\times$  and  $x\tau(\alpha) = \alpha^{-1}x\alpha$  for  $x \in B^\circ$  and  $\alpha \in B^\times$ .)

It can easily be seen that  $K = \{\alpha \in B \mid \alpha h = h\alpha\}$ ;  $K$  is either a quadratic extension of  $F$ , or isomorphic to  $F \oplus F$ . In either case we have

$$(36.7) \quad B = K + \omega K, \quad \omega^2 = \gamma, \quad \omega h = -h\omega$$

with a suitable  $\gamma \in F^\times$  and  $\omega \in B$ ; see Lemma 20.4 and §20.2. If  $B$  is not a division algebra, then we have  $B = M_2(F)$  and  $B^\circ = \{x \in M_2(F) \mid \text{tr}(x) = 0\}$ .

By (35.1), we can put, without losing generality,  $h = \begin{bmatrix} 0 & p \\ 1 & 0 \end{bmatrix}$  with  $p \in F^\times$ . Then we have (36.7) with  $\omega = \text{diag}[1, -1]$  and  $\gamma = 1$ .

We easily see that  $B^\circ = Fh + \omega K$  and  $\text{Tr}_{B/F}(h^\iota \omega K) = 0$ , and so  $W = \omega K$ . Put  $q = \varphi[h]$ . Since  $h^2 = -hh^\iota = \delta^{-1}q$ ,  $K$  can be determined as follows:

$$(36.8) \quad K = \begin{cases} F \oplus F & \text{if } \delta q \in F^{\times 2}, \\ F((\delta q)^{1/2}) & \text{otherwise.} \end{cases}$$

For  $y = \omega x \in W$  with  $x \in K$  we have  $\varphi[y] = \gamma \delta x x^\iota$ , and so we can put  $(W, \varphi) = (K, \gamma \delta \kappa)$ . Then  $H (= SO^\varphi(W))$  is exactly the group of (36.4). Besides, we easily see that  $H$  consists of the maps  $y \mapsto b^{-1}yb = b^{-1}b^\rho y$  for all  $b \in K^\times$ .

**36.7.** Take  $F$  to be global in the setting of §36.6. We fix a maximal order  $\mathfrak{o}$  in  $B$  and put  $L = \mathfrak{o} \cap B^\circ$ . This is maximal, because each of its localizations is maximal as shown in §29.10. Every maximal lattice is of this form with some maximal order in place of  $\mathfrak{o}$ . Indeed, if  $M$  is a maximal lattice in  $V$ , then  $M = L\tau(\alpha)$  with  $\alpha \in G^+(V)_\mathbf{A} = B_\mathbf{A}^\times$ , as noted in §30.1. Then  $M = \alpha^{-1}\mathfrak{o}\alpha \cap B^\circ$ , and  $\alpha^{-1}\mathfrak{o}\alpha$  is a maximal order in  $B$ . Now  $\mathfrak{o}$  is the unique maximal order containing  $\mathfrak{g}$  and  $\mathfrak{o} \cap B^\circ$ , since the corresponding fact over a local field can easily be verified. (It is sufficient to prove the fact when  $\mathfrak{o} = M_2(\mathfrak{g})$  in the local case.) Therefore the number of classes in the genus of maximal lattices in  $V = B^\circ$  is exactly the type number of  $B$ , that is, the

maximum number of maximal orders in  $B$  that are not mutually conjugate under the inner automorphisms of  $B$ .

We now take  $v \in \mathbf{h}$  such that  $B_v \cong M_2(F_v)$ . Taking a suitable isomorphism, we may assume that  $\mathfrak{o}_v = M_2(\mathfrak{g}_v)$ . Then  $\mathfrak{o}_v^\times = GL_2(\mathfrak{g}_v)$ . We have

$$(36.9) \quad \tau(\mathfrak{o}_v^\times) = \{\alpha \in SO^\varphi(V)_v \mid L_v \alpha = L_v\}, \quad L = \mathfrak{o} \cap B^\circ.$$

Indeed, let  $a \in \mathfrak{o}_v^\times$ . Then  $L_v \tau(a) = a^{-1} L_v a = L_v$ . Conversely, suppose  $L_v \alpha = L_v$  with  $\alpha \in SO^\varphi(V)_v$ . We can put  $\alpha = \tau(b)$  with  $b \in B_v^\times$ . Then  $L_v = b^{-1} L_v b = b^{-1} \mathfrak{o}_v b \cap B_v^\circ$ , and so  $b^{-1} \mathfrak{o}_v b = \mathfrak{o}_v$ , since  $\mathfrak{o}_v \cap B_v^\circ$  determines  $\mathfrak{o}_v$  as explained above. Thus  $b \mathfrak{o}_v$  is a two-sided ideal of  $\mathfrak{o}_v$ . By Lemma 21.20,  $b \mathfrak{o}_v = c \mathfrak{o}_v$  with  $c \in F_v^\times$ , and so  $c^{-1} b \in \mathfrak{o}_v^\times$ . Since  $\alpha = \tau(c^{-1} b)$ , this proves (36.9).

**Lemma 36.8.** *Let  $(V, \varphi) = (B^\circ, -\delta\beta^\circ)$  as in §36.6 with a local field  $F$ ,  $B = M_2(F)$ , and  $\delta \in \mathfrak{g}^\times$ ; put  $\mathfrak{o} = M_2(\mathfrak{g})$  and  $M = B^\circ \cap \mathfrak{o}$ ; further let  $h$  be an element of  $V$  such that  $\varphi[h] \neq 0$ . Put  $K = F[h]$ ,  $\mathfrak{f} = K \cap \mathfrak{o}$ ,  $C = \{\gamma \in SO^\varphi(V) \mid M\gamma = M\}$ , and  $Y = \{y \in V \mid \varphi(h, y) = 0\}$ . Then the following assertions hold:*

- (i)  $\mathfrak{f}$  is the order of  $K$  whose discriminant is  $\varphi[h]\varphi(h, M)^{-2}$ .
- (ii) There exists an element  $\omega$  of  $\mathfrak{o}^\times$  satisfying (36.7).
- (iii)  $A^+(M \cap Y) = \mathfrak{f}$  and  $M \cap Y = \omega \mathfrak{f}$  with any such  $\omega$ .
- (iv)  $SO^\varphi(Y) \cap C = \tau(\mathfrak{f}^\times)$ .
- (v)  $\{\alpha \in SO^\varphi(Y) \mid (M \cap Y)\gamma = M \cap Y\} = \tau(\{a \in K^\times \mid a/a^\rho \in \mathfrak{f}^\times\})$ .
- (vi)  $\omega \mathfrak{f}$  is the only maximal lattice in  $Y$  containing  $M \cap Y$ .

PROOF. As shown in §36.6,  $K$  is given by (36.8). Changing  $h$  for its suitable constant multiple, we may assume that  $2\varphi(h, M) = \mathfrak{g}$ . Take  $\ell \in K$  so that  $\mathfrak{f} = \mathfrak{g}[\ell]$ ; put  $\ell = \begin{bmatrix} u & x \\ y & v \end{bmatrix}$  and  $2h = \begin{bmatrix} c & 2a \\ 2b & -c \end{bmatrix}$ . Then  $a\mathfrak{g} + b\mathfrak{g} + c\mathfrak{g} = \mathfrak{g}$ ,  $h = r + s\ell$  with  $r, s \in F$ , and  $2h = h - h^\iota = s(\ell - \ell^\iota) = s \begin{bmatrix} z & 2x \\ 2y & -z \end{bmatrix}$  with  $z = u - v$ . Since  $\ell \in \mathfrak{o}$ , we can put  $x\mathfrak{g} + y\mathfrak{g} + z\mathfrak{g} = e\mathfrak{g}$  with  $e \in \mathfrak{g}$ . Put  $m = e^{-1} \begin{bmatrix} z & x \\ y & 0 \end{bmatrix}$ ; then  $m = e^{-1}(\ell - v) \in K \cap \mathfrak{o} = \mathfrak{f} = \mathfrak{g}[\ell]$ , so that  $e \in \mathfrak{g}^\times$ . Now  $\mathfrak{g} = a\mathfrak{g} + b\mathfrak{g} + c\mathfrak{g} = s(x\mathfrak{g} + y\mathfrak{g} + z\mathfrak{g}) = se\mathfrak{g} = s\mathfrak{g}$ ; thus  $s \in \mathfrak{g}^\times$ . Since  $s^2(\ell - \ell^\iota)^2 = (h - h^\iota)^2 = \delta^{-1}\varphi[2h]$ , we obtain (i).

We have  $C = \tau(\mathfrak{o}^\times)$  by (36.9). By (35.7a) we can find an element  $\gamma \in C$  such that  $h\gamma = k$  with  $k \in B^\circ$  of the following two types: (1)  $k = \text{diag}[c, -c]$ ; (2)  $k = \begin{bmatrix} c & a \\ 1 & -c \end{bmatrix}$ . Here  $a \in \mathfrak{g}$  and  $2c \in \mathfrak{g}$ . Since  $h\gamma = \alpha h \alpha^{-1}$  with  $\alpha \in \mathfrak{o}^\times$ , in order to prove (ii), we can take  $h$  itself to be one of these two types. Then we can take  $\omega$  of (36.7) as follows:  $\omega = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$  for Type (1) and

$\omega = \begin{bmatrix} -1 & 2c \\ 0 & 1 \end{bmatrix}$  for Type (2). Notice that  $\omega^2 = -1$  for Type (1) and  $\omega^2 = 1$  for Type (2);  $\omega \in \mathfrak{o}^\times$  for both types. This proves (ii). Take any such  $\omega$ . Then  $Y = \omega K$  as noted in §36.6, and  $M \cap Y = \mathfrak{o} \cap B^\circ \cap \omega K = \mathfrak{o} \cap \omega K = \omega(\mathfrak{o} \cap K) = \omega \mathfrak{f}$ . Since  $(\omega a)(\omega b) = \omega^2 a^\rho b$  for  $a, b \in K$  and  $\omega^2 \in \mathfrak{g}^\times$ , we easily see that  $A^+(M \cap Y) = \mathfrak{f}$ . This proves (iii).

Next,  $G^+(Y) = K^\times$  and  $SO^\varphi(Y) = \tau(K^\times)$  as noted in §36.5. For  $x \in K$  and  $a \in K^\times = G^+(Y)$ , we have  $\omega x \tau(a) = \omega b x$ , where  $b = a/a^\rho$ . Clearly  $(M \cap Y)\tau(a) = M \cap Y$  if and only if  $b \in \mathfrak{f}^\times$ , which proves (v). Also,  $\tau(a) \in C$  if and only if  $\tau(a) = \tau(c)$  with  $c \in \mathfrak{o}^\times$ , that is,  $a \in F^\times \mathfrak{o}^\times$ . This is the case if and only if  $a \in F^\times \mathfrak{f}^\times$ , as  $\mathfrak{o}^\times \cap K = \mathfrak{f}^\times$ . This proves (iv). As for (vi), first observe that  $\mathfrak{r}$  is a unique maximal lattice in  $K$  containing  $\mathfrak{f}$  with respect to the quadratic form  $x \mapsto N_{K/F}(x)$  (even when  $K = F \oplus F$ ). Transferring this from  $K$  to  $Y = \omega K$ , we obtain (vi).

**36.9.** We now return to §36.6 with a quaternion algebra  $B$  over a global field  $F$ , and take  $h, q, W$ , and  $K$  as considered there. We take also  $\omega$  and  $\gamma$  as in (36.7). We denote by  $\mathfrak{r}$  the maximal order of  $K$ , by  $\mathfrak{d}$  the different of  $K$  relative to  $F$ , and by  $\rho$  the nontrivial automorphism of  $K$  over  $F$ . We identify  $G^+(W)$  with  $K^\times$ ; then  $SO^\varphi(W) = H = \{\alpha \in K^\times \mid \alpha\alpha^\rho = 1\}$  as shown in §36.5. Since  $H$  is commutative,  $\#[H \backslash H_{\mathbf{A}} / (H_{\mathbf{A}} \cap C)]$  of (35.12b) can be written  $[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)]$ .

**Theorem 36.10.** *The notation being as in §§36.7 and 36.9, suppose  $\delta \in \mathfrak{g}^\times$ . Given  $h \in V$  such that  $\varphi[h] \neq 0$ , let  $K = F + Fh \subset B$  as above and let  $\mathfrak{e}$  be the product of all prime ideals in  $F$  ramified in  $B$ . Then the order  $\mathfrak{f}$  in  $K$  given by  $\mathfrak{f} = K \cap \mathfrak{o}$  has conductor  $\mathfrak{c}$ , which can be determined by the condition that  $\mathfrak{c}_v = \mathfrak{g}_v$  if  $v \nmid \mathfrak{e}$  and  $\mathfrak{c}_v^2 N_{K/F}(\mathfrak{d})_v = \varphi[h]\varphi(h, L)_v^{-2}$  if  $v \mid \mathfrak{e}$ . Moreover, define  $C$  by (35.9b) for the present  $L$ ; suppose  $K$  is a field. Then*

$$(36.10) \quad [H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)] = (c_K/c_F) \cdot 2^{1-\mu-\nu} [\mathfrak{g}^\times : N_{K/F}(\mathfrak{r}^\times)] \\ \cdot [U : U']^{-1} N(\mathfrak{c}) \prod_{\mathfrak{p} \mid \mathfrak{c}} \{1 - [K/F, \mathfrak{p}] N(\mathfrak{p})^{-1}\}.$$

Here  $c_K$  resp.  $c_F$  is the class number of  $K$  resp.  $F$ ;  $\mu$  is the number of prime ideals dividing  $\mathfrak{e}$  and ramified in  $K$ ;  $\nu$  is the number of  $v \in \mathbf{a}$  ramified in  $K$ ;

$$U = \{x \in \mathfrak{r}^\times \mid xx^\rho = 1\}, \quad \text{and} \quad U' = \{x \in U \mid x - 1 \in \mathfrak{c}_v \mathfrak{d}_v \text{ for every } v \nmid \mathfrak{e}\};$$

$\mathfrak{p}$  runs over all prime factors of  $\mathfrak{c}$ ;  $[K/F, \mathfrak{p}]$  denotes 1,  $-1$ , or 0 according as  $\mathfrak{p}$  splits in  $K$ , remains prime in  $K$ , or is ramified in  $K$ .

**PROOF.** We take the localization at  $v \in \mathbf{h}$ . Suppose  $\varphi$  is anisotropic at  $v$ , which is the case if and only if  $v \nmid \mathfrak{e}$ ; see (25.3). From Theorem 21.21 we see that  $\mathfrak{r}_v \subset \mathfrak{o}_v$ , so that  $\mathfrak{f}_v = \mathfrak{r}_v$  for such a  $v$ . Next suppose  $\varphi$  is isotropic at  $v$ ; then



we can put  $B_v = M_2(F_v)$ . By Lemma 36.8(i),  $\mathfrak{c}_v^2 N_{K/F}(\mathfrak{d})_v = \varphi[h]\varphi(h, L)_v^{-2}$ , which proves our assertion concerning  $\mathfrak{c}$ .

To prove (36.10), suppose  $K$  is a field. Then we gave in (36.6b) a formula for the number of classes in the genus of maximal lattices in  $W$ , which equals  $[H_{\mathbf{A}} : HE]$ , where  $E = H_{\mathbf{A}} \prod_{v \in \mathfrak{h}} E_v$  with  $E_v = \mathfrak{r}_v^\times \cap H_v$ . Put  $D = H_{\mathbf{A}} \cap C$  and  $D_v = D \cap H_v$ . If  $v|\mathfrak{e}$ , then  $\varphi_v$  is anisotropic, so that  $C_v = G_v$ ; thus  $D_v = H_v = E_v$  if  $v|\mathfrak{e}$ . If  $v \nmid \mathfrak{e}$ , then, by Lemma 36.8(iv),  $D_v = \tau(\mathfrak{f}_v^\times)$ . Define  $U$  and  $U'$  as above; then  $U = E \cap H$ , and

$$[HE : HD] = [E : E \cap HD] = [E : UD] = [E : D] / [UD : D] = [E : D] / [U : U \cap D].$$

Now  $U \cap D = \{x \in U \mid x \in \tau(\mathfrak{f}_v^\times) \text{ for every } v \nmid \mathfrak{e}\}$ . Therefore, from Lemma 36.3(iii) we obtain  $U \cap D = U'$ . Thus

$$(36.10a) \quad U \cap C = U \cap D = U'.$$

We have also

$$[E : D] = \prod_{v \nmid \mathfrak{e}} [E_v : D_v] = \prod_{v \nmid \mathfrak{e}} [E_v : \tau(\mathfrak{r}_v^\times)] [\tau(\mathfrak{r}_v^\times) : \tau(\mathfrak{f}_v^\times)].$$

By Lemma 21.13(ii),  $[E_v : \tau(\mathfrak{r}_v^\times)] = 2$  if  $v$  is ramified in  $K$ , and  $= 1$  otherwise. This combined with Lemma 36.3(i), (iv) gives

$$[E : D] = 2^b N(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \{1 - [K/F, \mathfrak{p}] N(\mathfrak{p})^{-1}\},$$

where  $b$  is the number of the primes  $v \nmid \mathfrak{e}$  ramified in  $K$ . Now  $[H_{\mathbf{A}} : HD] = [H_{\mathbf{A}} : HE][HE : HD]$ , and as we said,  $[H_{\mathbf{A}} : HE]$  is given by (36.6b). Therefore we obtain the formula of our theorem.

In the above theorem we assumed that  $\delta \in \mathfrak{g}^\times$ . We can actually prove a similar result without that condition; see Theorem 5.7 and Corollary 5.8 of [S06c].

**36.11.** Using (36.3), we can express (36.10) as follows:

$$(36.11) \quad [H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)] = c(\mathfrak{f}) c_F^{-1} 2^{1-\mu-\nu} [\mathfrak{g}^\times : N_{K/F}(\mathfrak{f}^\times)] [U \cap \mathfrak{f}^\times : U']^{-1}.$$

Indeed, observing that the map  $x \mapsto xx^\rho$  gives an isomorphism of  $\mathfrak{r}^\times/U\mathfrak{f}^\times$  onto  $N_{K/F}(\mathfrak{r}^\times)/N_{K/F}(\mathfrak{f}^\times)$ , we have

$$[N_{K/F}(\mathfrak{r}^\times) : N_{K/F}(\mathfrak{f}^\times)] = [\mathfrak{r}^\times : U\mathfrak{f}^\times] = [\mathfrak{r}^\times : \mathfrak{f}^\times] / [U\mathfrak{f}^\times : \mathfrak{f}^\times] = [\mathfrak{r}^\times : \mathfrak{f}^\times] / [U : U \cap \mathfrak{f}^\times].$$

From (36.1) and Lemma 36.3(ii) we obtain

$$(36.12) \quad U \cap \mathfrak{f}^\times = \{x \in U \mid x^\rho - x \in \mathfrak{c}\mathfrak{d}\}.$$

Now  $\mathfrak{c}$  of Theorem 36.10 is prime to  $\mathfrak{e}$ ; so if  $v|\mathfrak{e}$ , then  $x^\rho - x \in \mathfrak{c}_v \mathfrak{d}_v$  for every  $x \in \mathfrak{r}$ . Thus we can replace the condition “ $x^\rho - x \in \mathfrak{c}\mathfrak{d}$ ” in (36.12) by “ $x^\rho - x \in \mathfrak{c}_v \mathfrak{d}_v$  for every  $v \nmid \mathfrak{e}$ .” Since  $x^\rho - x = (1-x)(1+x^\rho)$  for  $x \in U$ , we see that  $U' \subset U \cap \mathfrak{f}^\times$ . Therefore, combining our calculations with (36.10) and (36.3), we obtain (36.11).

**36.12.** Let us next take  $B = M_2(F)$  and  $T = \{x \in M_2(F) \mid \text{tr}(x) = 0\}$ . Thus  $T = B^\circ$ , but we use the letter  $T$  in this subsection. We put

$$(36.13a) \quad j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$(36.13b) \quad S = \{x \in M_2(F) \mid {}^t x = x\},$$

$$(36.13c) \quad \varphi(x, y) = 2^{-1} \text{tr}(xy^t) \quad (x, y \in M_2(F)),$$

$$(36.13d) \quad L = T \cap M_2(\mathfrak{g}) \quad \text{and} \quad \Lambda = S \cap M_2(\mathfrak{g}).$$

We view  $\varphi$  as a symmetric form on  $M_2(F)$ . Clearly  $\varphi[x] = \det(x)$  for  $x \in M_2(F)$ , and the map  $x \mapsto jx$  defines an isomorphism of  $(T, \varphi)$  onto  $(S, \varphi)$ .

As observed in Lemma 25.2(ii) and §36.4, we have  $G^+(T) = GL_2(F)$  and  $x\tau(\alpha) = \alpha^{-1}x\alpha$  for  $x \in T$  and  $\alpha \in GL_2(F)$ , where  $\alpha^{-1}x\alpha$  should be understood within the algebra  $M_2(F)$ . Since  $(S, \varphi)$  is isomorphic to  $(T, \varphi)$ ,  $G^+(S)$  can also be identified with  $GL_2(F)$ . Indeed, denote the projection map  $G^+(S) \rightarrow SO^\varphi(S)$  by  $\tau'$  instead of  $\tau$ ; then using the isomorphism  $x \mapsto jx$ , we can easily verify that

$$(36.14) \quad x\tau'(\alpha) = \det(\alpha)^{-1} \cdot {}^t \alpha x \alpha \quad (x \in S, \alpha \in G^+(S) = GL_2(F)).$$

We easily see that  $L$  resp.  $\Lambda$  is a maximal lattice in  $T$  resp.  $S$ ,  $jL = \Lambda$ , and

$$(36.15) \quad \tilde{\Lambda} = \left\{ \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \mid a, b, c \in \mathfrak{g} \right\}.$$

We now associate a binary form  $ax^2 + bxy + cy^2$  to  $h = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \in S$ . Then  $-\varphi[2h] = b^2 - 4ac$ , which is called the **discriminant** of the binary form. Clearly,  $2\varphi(h, \Lambda) = \mathfrak{g}$  if and only if  $\mathfrak{g}a + \mathfrak{g}b + \mathfrak{g}c = \mathfrak{g}$ . In the classical case in which  $F = \mathbf{Q}$  and  $\mathfrak{g} = \mathbf{Z}$ , we called such a binary form *primitive* in §34.2. In the general case, however, we have to deal with nonprincipal ideals, so that the formulation is not so simple, since  $S$  may have maximal lattices which are not equivalent to  $\Lambda$ .

In order to treat  $(S, \varphi)$ , it is more practical to employ  $G^+(S) = GL_2(F)$  instead of  $SO^\varphi(S)$  with the action of  $GL_2(F)$  on  $S$  defined by (36.14). Of course we can let  $GL_2(F)$  act on  $S$  by the rule  $x \mapsto {}^t \alpha x \alpha$  for  $\alpha \in GL_2(F)$  and  $x \in S$ , but this does not leave  $\det(x)$  invariant, whereas  $\tau'(\alpha)$  belongs to  $SO^\varphi(S)$ . In this case, for a  $\mathfrak{g}$ -lattice  $M$  in  $S$ ,  $q \in F^\times$ , and a  $\mathfrak{g}$ -ideal  $\mathfrak{b}$ , the set of (35.9c) can be written in the form

$$(36.16) \quad M[q, \mathfrak{b}] = \{h \in S \mid \det(h) = q, \text{tr}(h^t M) = 2\mathfrak{b}\}.$$

Also, for  $y \in GL_2(F)_\mathbf{A}$  and  $M = \Lambda\tau'(y)^{-1}$  we put

$$(36.17) \quad \Delta(M) = GL_2(F) \cap yQy^{-1} \quad \text{with} \quad Q = GL_2(F)_\mathbf{a} \prod_{v \in \mathbf{h}} GL_2(\mathfrak{g}_v).$$

From (36.9) we obtain

$$(36.18) \quad \tau(Q) = \{x \in SO^\varphi(T)_{\mathbf{A}} \mid Lx = L\}.$$

**Theorem 36.13.** *Let the notation be as in §36.12. Assuming  $\Lambda[q, \mathfrak{b}] \neq \emptyset$ , for  $h \in \Lambda[q, \mathfrak{b}]$  put  $W = (Fh)^\perp$  and  $K = F + Fjh$  (this is the subalgebra of  $M_2(F)$ ); define  $Y$  as in Theorem 35.6(iii) with  $G = SO^\varphi(S)$ ,  $H = SO^\varphi(W)$ , and  $C = \{x \in G_{\mathbf{A}} \mid \Lambda x = \Lambda\}$ . Let  $\mathfrak{I}$  denote the ideal group of  $F$ , and  $\mathfrak{I}_2$  the subgroup of  $\mathfrak{I}$  generated by all the squares of ideals in  $\mathfrak{I}$  and all the principal ideals. Then the following assertions hold:*

(i)  *$K$  is isomorphic to  $F \oplus F$  if  $-q \in F^{\times 2}$  and to  $F(\sqrt{-q})$  otherwise.*

(ii)

$$\#(Y) = \begin{cases} [\mathfrak{I} : \mathfrak{I}_2]/2 & \text{if } -q \notin F^{\times 2} \text{ and every } v \in \mathbf{v} \text{ is unramified in } K, \\ [\mathfrak{I} : \mathfrak{I}_2] & \text{otherwise.} \end{cases}$$

(iii) *Put  $\mathfrak{f} = K \cap M_2(\mathfrak{g})$ . Then  $\mathfrak{f}$  has discriminant  $q\mathfrak{b}^{-2}$ .*

(iv) *Let  $c_F$  resp.  $c(\mathfrak{f})$  denote the class number of  $F$  resp. the class number of  $\mathfrak{f}$  in the sense of §36.4. Then for every lattice of the form  $M = \Lambda\tau'(y)^{-1}$  with  $y \in K_{\mathbf{A}}^\times$  we have*

$$\begin{aligned} & \# \{M[q, \mathfrak{b}]/\Delta(M)\} \\ &= \begin{cases} 2c(\mathfrak{f})/c_F & \text{if } -q \notin F^{\times 2} \text{ and every } v \in \mathbf{v} \text{ is unramified in } K, \\ c(\mathfrak{f})/c_F & \text{otherwise.} \end{cases} \end{aligned}$$

PROOF. To prove these, we use  $(T, L)$  instead of  $(S, \Lambda)$ . Thus, we take  $h \in L[q, \mathfrak{b}]$ , put  $K = F + Fh$ , and define  $W$  in  $T$  instead of  $S$ . Then our setting is a special case of §36.6; we have  $G^+(W) = K^\times \subset B^\times = G^+(T) = GL_2(F)$  and  $\delta = -1$ . For simplicity put  $R = F_{\mathbf{A}}^\times \prod_{v \in \mathbf{h}} \mathfrak{g}_v^\times$ . We have seen (i) in (36.8). Let  $\mathfrak{r}$  denote the maximal order of  $K$ ,  $\mathfrak{I}_K$  the group of all  $\mathfrak{r}$ -ideals, and  $\mathfrak{I}'$  the subgroup of  $\mathfrak{I}$  generated by  $\mathfrak{I}_2$  and  $N_{K/F}(\mathfrak{r})$  for all  $\mathfrak{r} \in \mathfrak{I}_K$ . Then the map  $x \mapsto x\mathfrak{g}$  gives an isomorphism of  $F_{\mathbf{A}}^\times/R$  onto  $\mathfrak{I}$ , which sends  $F_{\mathbf{A}}^{\times 2}F^\times R$  resp.  $N_{K/F}(K_{\mathbf{A}}^\times)F^\times R$  onto  $\mathfrak{I}_2$  resp.  $\mathfrak{I}'$ . Now, every maximal lattice in  $T$  is of the form  $L\tau(\xi)$  with  $\xi \in B_{\mathbf{A}}^\times$ , and its  $SO^\varphi(T)$ -class is determined by the coset  $\det(\xi)F_{\mathbf{A}}^{\times 2}F^\times R$  by virtue of (32.4a) with  $\tau(Q)$  as  $D$  there, since  $\sigma(\tau(\xi)) = \det(\xi)$  and  $\det(Q) = R$ . Therefore  $L\tau(\xi)$  is equivalent to a lattice belonging to the  $SO^\varphi(W)$ -genus of  $L$  if and only if  $\det(\xi) \in N_{K/F}(\zeta)F_{\mathbf{A}}^{\times 2}F^\times R$  for some  $\zeta \in K_{\mathbf{A}}^\times$ , that is,  $\det(\xi) \in N_{K/F}(K_{\mathbf{A}}^\times)F^\times R$ . This shows that  $\#(Y) = [N_{K/F}(K_{\mathbf{A}}^\times)F^\times R : F_{\mathbf{A}}^{\times 2}F^\times R] = [\mathfrak{I}' : \mathfrak{I}_2] = [\mathfrak{I} : \mathfrak{I}_2]/[\mathfrak{I} : \mathfrak{I}']$ . Since  $[\mathfrak{I} : \mathfrak{I}'] = [F_{\mathbf{A}}^\times : F^\times N_{K/F}(K_{\mathbf{A}}^\times)] = 1$  or  $2$  according as  $K = F \oplus F$  or  $K$  is a field, we have  $[\mathfrak{I} : \mathfrak{I}'] \leq 2$ , and  $[\mathfrak{I} : \mathfrak{I}'] = 2$  if and only if  $K$  is a field and  $R \subset F^\times N_{K/F}(K_{\mathbf{A}}^\times)$ , which is the case if and only if  $K$  is a quadratic extension of  $F$  unramified at every  $v \in \mathbf{v}$ , a well-known fact in class field theory. Otherwise  $\mathfrak{I} = \mathfrak{I}'$ . This proves (ii). Assertion (iii) is included in Theorem 36.10.

Now the left-hand side of (35.13a) is  $\#[(K_{\mathbf{A}}^{\times} \cap B^{\times} zQ)/K^{\times}(K_{\mathbf{A}}^{\times} \cap Q)]$  in the present case. Put  $\mathcal{Y} = \{x \in K_{\mathbf{A}}^{\times} \mid N_{K/F}(x) \in F^{\times} R\}$ . By Theorem 30.9(ii),  $B^{\times} zQ = \{x \in B_{\mathbf{A}}^{\times} \mid \det(z^{-1}x) \in F^{\times} R\}$ , and so we see that  $K_{\mathbf{A}}^{\times} \cap B^{\times} zQ = z\mathcal{Y}$  for every  $z \in K_{\mathbf{A}}^{\times}$ . Consequently the left-hand side of (35.13a) is equal to  $[\mathcal{Y} : K^{\times}(K_{\mathbf{A}}^{\times} \cap Q)]$ , which is independent of  $z$ . Since  $\mathfrak{f} = K \cap M_2(\mathfrak{g})$ , we have  $K_{\mathbf{A}}^{\times} \cap Q = K_{\mathbf{a}}^{\times} \prod_{v \in \mathfrak{h}} \mathfrak{f}_v^{\times}$ , and so

$$(*) \quad c(\mathfrak{f}) = [K_{\mathbf{A}}^{\times} : K^{\times}(K_{\mathbf{A}}^{\times} \cap Q)] = [K_{\mathbf{A}}^{\times} : \mathcal{Y}][\mathcal{Y} : K^{\times}(K_{\mathbf{A}}^{\times} \cap Q)].$$

Let  $\mathcal{J}_K^0$  be the subgroup of  $\mathcal{J}_K$  consisting of the ideals  $\mathfrak{x}$  in  $\mathcal{J}_K$  such that  $N_{K/F}(\mathfrak{x})$  is a principal ideal in  $F$ . Then the map  $x \mapsto x\mathfrak{x}$  gives an isomorphism of  $K_{\mathbf{A}}^{\times}/\mathcal{Y}$  onto  $\mathcal{J}_K/\mathcal{J}_K^0$ . Also,  $\mathfrak{x} \mapsto N_{K/F}(\mathfrak{x})$  gives an isomorphism of  $\mathcal{J}_K/\mathcal{J}_K^0$  onto  $\mathcal{J}'$  modulo the principal ideals. Therefore  $[K_{\mathbf{A}}^{\times} : \mathcal{Y}] = c_F/[\mathcal{J} : \mathcal{J}']$ . This combined with (35.13) and (\*) proves (iv), since we have determined  $[\mathcal{J} : \mathcal{J}']$  in the proof of (i). This completes the proof.

**36.14.** Let us now show that the above theorem gives Dedekind's result on the classes of binary forms over  $\mathbf{Z}$ , as we said in §34.2. Take  $F = \mathbf{Q}$  and  $\mathfrak{g} = \mathbf{Z}$ . Then  $G^+(S) = GL_2(\mathbf{Q})$ . Take  $h = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \in S$  so that  $2h \in \Lambda[q, \mathbf{Z}]$ . Then  $q = 4ac - b^2$  and  $a\mathbf{Z} + b\mathbf{Z} + c\mathbf{Z} = \mathbf{Z}$ . Thus  $h$  represents a primitive binary form of discriminant  $-q$ . By Theorem 30.9(ii),  $G^+(S)_{\mathbf{A}} = GL_2(\mathbf{Q})_{\mathbf{A}} = GL_2(\mathbf{Q})Q$  with  $Q$  of (36.17). Thus  $\#(Y) = 1$ . We have  $\mathfrak{f} = K \cap M_2(\mathbf{Z})$  and so  $K_{\mathbf{A}}^{\times} \cap Q = K_{\mathbf{a}}^{\times} \prod_p \mathfrak{f}_p^{\times}$ , which we denoted by  $X(\mathfrak{f})$  in §36.4.

Since  $\#(Y) = 1$ , Theorem 35.6(ii) combined with (35.11) establishes a bijection of  $K_{\mathbf{A}}^{\times}/[K^{\times}X(\mathfrak{f})]$  onto  $\Lambda[q, \mathbf{Z}]/\Delta(\Lambda)$ . Now  $K_{\mathbf{A}}^{\times}/[K^{\times}X(\mathfrak{f})]$  is the group of ideal classes of proper  $\mathfrak{f}$ -ideals, and  $\Lambda[q, \mathbf{Z}]/\Delta(\Lambda)$  is the classes of primitive binary forms of discriminant  $-q$ . In this way we obtain Dedekind's correspondence. At the same time we obtain (34.6) as a special case of (iv) of the above theorem. However, there is one remaining point: that the group  $\{\gamma \in SO^{\varphi}(S) \mid \Lambda\gamma = \Lambda\}$  consists of the maps  $\tau'(\alpha)$  defined by (36.12) for all  $\alpha \in GL_2(\mathbf{Z})$ . This can be proved as follows. Let us use  $T = B^{\circ}$  instead of  $S$ . Suppose  $\gamma \in G^+(T)$  and  $L\gamma = L$ . Take  $\xi \in GL_2(\mathbf{Q}) = G^+(T)$  so that  $\tau(\xi) = \gamma$ . Then  $\xi^{-1}L\xi = L$  and  $L = \mathfrak{o} \cap T$ , where  $\mathfrak{o} = M_2(\mathbf{Z})$ . For the same reason as in §36.7, we see that  $\xi\mathfrak{o}$  is a two-sided ideal of  $\mathfrak{o}$ , and so  $\xi = c\alpha$  with  $c \in \mathbf{Q}^{\times}$  and  $\alpha \in GL_2(\mathbf{Z})$ . Thus  $\gamma = \tau(\alpha)$  as expected. We can therefore conclude that  $c(\mathfrak{f})$  is the number of classes of primitive binary forms of discriminant  $-q$ .

Here the fact that  $\mathbf{Q}$  has class number 1 makes the matter simpler. In a more general case, the relationship between the stabilizer of  $\Lambda$  in  $SO^{\varphi}(S)$  and that in  $G^+(S)$  is more complicated. Also, when  $F = \mathbf{Q}$ , there is a distinction between real and imaginary quadratic fields. For details, the reader is referred to Lemmas 12.4 and 12.10, and Remark 12.11 of [S04b].

### 37. New mass formulas

**37.1.** Let us now recall the notion of the mass of an algebraic group. The idea of mass for an orthogonal group goes back to Eisenstein, Minkowski, and Siegel, but here we employ the formulation introduced in [S97, §24.1] and [S99a]. Let  $G$  be either  $SO^\varphi(V)$  or  $G^+(V)$  for  $(V, \varphi)$  over a global field. (More generally, we can take  $G$  to be a reductive algebraic group over a number field.) Given an open subgroup  $U$  of  $G_{\mathbf{A}}$  containing  $G_{\mathbf{a}}$  and such that  $U \cap G_{\mathbf{h}}$  is compact, we put  $U^a = aUa^{-1}$  and  $\Gamma^a = G \cap U^a$  for every  $a \in G_{\mathbf{A}}$ . We assume that  $G_{\mathbf{a}}$  acts on a symmetric space  $\mathcal{S}$  and we let  $G$  act on  $\mathcal{S}$  via its projection to  $G_{\mathbf{a}}$ . We also assume that  $\Gamma^a \backslash \mathcal{S}$  has finite measure, written  $\text{vol}(\Gamma^a \backslash \mathcal{S})$ , with respect to a fixed  $G_{\mathbf{a}}$ -invariant measure on  $\mathcal{S}$ . Taking a complete set of representatives  $\mathcal{B}$  for  $G \backslash G_{\mathbf{A}} / U$ , we put

$$(37.1a) \quad \nu(\Gamma) = [\Gamma \cap T : 1]^{-1} \text{vol}(\Gamma \backslash \mathcal{S}),$$

$$(37.1b) \quad \mathbf{m}(G, U) = \mathbf{m}(U) = \sum_{a \in \mathcal{B}} \nu(\Gamma^a).$$

Here  $\Gamma$  is a group of type  $\Gamma^a$ ,  $T$  is the set of all elements of  $G$  which act trivially on  $\mathcal{S}$ , and we assume that  $[\Gamma^a \cap T : 1]$  is finite. We easily see that  $\mathbf{m}(U)$  does not depend on the choice of  $\mathcal{B}$ . We call  $\mathbf{m}(G, U)$  the **mass** of  $G$  relative to  $U$ . If  $G_{\mathbf{a}}$  is compact, we take  $\mathcal{S}$  to be a single point of measure 1 on which  $G_{\mathbf{a}}$  acts trivially. Then we have  $\nu(\Gamma) = [\Gamma : 1]^{-1}$ , and so

$$(37.1c) \quad \mathbf{m}(G, U) = \mathbf{m}(U) = \sum_{a \in \mathcal{B}} [\Gamma^a : 1]^{-1} \quad \text{if } G_{\mathbf{a}} \text{ is compact.}$$

If  $G = SO^\varphi(V)$  and  $G_{\mathbf{a}}$  is not compact, we take  $\mathcal{S}$  to be  $G_{\mathbf{a}}$  modulo its maximal compact subgroup. Given a  $\mathfrak{g}$ -lattice  $\Lambda$  in  $V$ , we can take  $U = \{\xi \in G_{\mathbf{A}} \mid \Lambda x = \Lambda\}$ . Then we put

$$(37.1d) \quad \mathbf{m}(G, \Lambda) = \mathbf{m}(G, U),$$

and call it **the mass of the genus of  $\Lambda$  with respect to  $G$** .

We next take a subset  $S$  of  $V$  that can be given in the form

$$(37.2) \quad S = \bigsqcup_{\beta \in B} h\beta\Gamma(\Lambda)$$

with  $h \in V$  and a finite subset  $B$  of  $SO^\varphi(V)$ . We put  $W = (Fh)^\perp$  and  $H = SO^\varphi(W)$  as before, and define the **mass** of the set  $S$  to be the quantity

$$(37.3) \quad \mathbf{m}(S) = \nu(\Gamma(\Lambda))^{-1} \sum_{\beta \in B} \nu(\Delta_\beta), \quad \Delta_\beta = H \cap \beta\Gamma(\Lambda)\beta^{-1}.$$

Here we define  $\nu(\Delta_\beta)$  for  $\beta \in SO^\varphi(V)$  with respect to a fixed measure on a symmetric space associated with  $SO^\varphi(W)_{\mathbf{a}}$ . We easily see that  $\mathbf{m}(S)$  is independent of the choice of  $B$ . Furthermore we have:

(37.4) *The elements  $h\beta\delta$  with  $\beta \in B$  and  $\delta \in \beta^{-1}\Delta_\beta\beta \setminus \Gamma(\Lambda)$  constitute the set  $S$  without repetition.*

In particular, if  $O^\varphi(V)_{\mathbf{a}}$  is compact, then  $\Gamma(\Lambda)$  and  $\Delta_\beta$  are finite groups. Therefore we obtain

$$(37.5) \quad \mathfrak{m}(S) = \#S \quad \text{if } O^\varphi(V)_{\mathbf{a}} \text{ is compact.}$$

By Theorem 35.4 and what we said in §35.5 we can take  $\Lambda[q]$  and  $\Lambda[q, \mathfrak{b}]$  as  $S$ . The mass can also be defined with respect to invariant measures on  $G_{\mathbf{a}}$  and  $G_{\mathbf{h}}$ . For this and other formulas on the mass the reader is referred to [S06a, Section 5].

We now state a result which may be called the second main theorem of quadratic Diophantine equations.

**Theorem 37.2.** *Let  $(V, \varphi)$ ,  $L$ ,  $C$ ,  $h$ ,  $G$ , and  $H$  be as in Theorem 35.6. Assuming  $L$  to be maximal, take  $y$  and  $\mathcal{E}$  as in (ii),  $Y$  as in (iii),  $q$  and  $\mathfrak{b}$  as in (v) of the same theorem; put  $\Delta_\varepsilon = H \cap \varepsilon C \varepsilon^{-1}$  for  $\varepsilon \in \mathcal{E}$  and  $L^y = L y^{-1}$  for  $y \in Y$ . Then*

$$(37.6a) \quad \mathfrak{m}(L^y[q, \mathfrak{b}]) = \nu(\Gamma(L^y))^{-1} \sum_{\varepsilon \in \mathcal{E}} \nu(\Delta_\varepsilon),$$

$$(37.6b) \quad \sum_{y \in Y} \nu(\Gamma(L^y)) \mathfrak{m}(L^y[q, \mathfrak{b}]) = \mathfrak{m}(H, H_{\mathbf{A}} \cap C).$$

PROOF. From Theorem 35.6(ii) and (35.11) we see that  $L^y[q, \mathfrak{b}]$  is the disjoint union of  $h\alpha_\varepsilon \Gamma(L^y)$  for all  $\varepsilon \in \mathcal{E}$  with  $\alpha_\varepsilon$  defined there, and so we can take  $\{\alpha_\varepsilon \mid \varepsilon \in \mathcal{E}\}$  as the set  $B$  of (37.3) for  $\Lambda = L^y$ . Now  $\alpha_\varepsilon \Gamma(L^y) \alpha_\varepsilon^{-1} = G \cap \alpha_\varepsilon y C y^{-1} \alpha_\varepsilon^{-1} = G \cap \varepsilon C \varepsilon^{-1}$ , and so  $\Delta_\beta = H \cap \varepsilon C \varepsilon^{-1} = \Delta_\varepsilon$  if  $\beta = \alpha_\varepsilon$ . Thus we obtain (37.6a). Next, take  $\mathcal{E}_y \subset H_{\mathbf{A}}$  so that  $H_{\mathbf{A}} \cap G y C = \bigsqcup_{\varepsilon \in \mathcal{E}_y} H \varepsilon (H_{\mathbf{A}} \cap C)$ . Then the union  $\bigsqcup_{y \in Y} \mathcal{E}_y$  gives  $H \setminus H_{\mathbf{A}} / (H_{\mathbf{A}} \cap C)$ , and so  $\sum_{y \in Y} \sum_{\varepsilon \in \mathcal{E}_y} \nu(\Delta_\varepsilon) = \mathfrak{m}(H, H_{\mathbf{A}} \cap C)$ , which combined with (37.6a) gives (37.6b).

It should be emphasized that the right-hand side of (37.6b) is the *mass* of  $H$  relative to  $H_{\mathbf{A}} \cap C$ , which is different from the *class number* of  $H$  relative to  $H_{\mathbf{A}} \cap C$  that appears on the left-hand side of (35.12b). In the next subsection we will discuss more about this difference in connection with Siegel's work.

**37.3.** The formulas of the above theorem may be called the *mass formulas* for the set  $L[q, \mathfrak{b}]$  of “primitive solutions” of the equation  $\varphi[x] = q$ . They are the precise versions of (34.9b) we promised in §34.3. Let us now compare them with Siegel's mass formulas, which have some similarities to, but are quite different from, ours. To make our exposition easier, let us assume that  $SO^\varphi(V)_{\mathbf{a}}$  is compact; then from (37.5) and (37.6b) we obtain

$$(37.7a) \quad \sum_{y \in Y} [\Gamma(L^y) : 1]^{-1} \#L^y[q, \mathfrak{b}] = \mathfrak{m}(H, H_{\mathbf{A}} \cap C).$$

We note here another formula that follows from (35.12b):

$$(37.7b) \quad \sum_{y \in Y} \# \{L^y[q, \mathfrak{b}]/\Gamma(L^y)\} = \# \{H \backslash H_{\mathbf{A}} / (H_{\mathbf{A}} \cap C)\}.$$

If we take  $\#\{x \in L^y \mid \varphi[x] = q\}$  in place of  $\#L^y[q, \mathfrak{b}]$ , then the left-hand side of (37.7a) becomes a quantity similar to the weighted average of the representation numbers of  $q$  by  $\varphi$ , considered by Siegel. He showed that the average is an infinite product of local representation densities; see [Si35] and [Si36]. Though (37.7a) is similar to his formula, there are three kinds of differences: (1) we have  $L^y[q, \mathfrak{b}]$  instead of  $\{x \in L^y \mid \varphi[x] = q\}$ ; (2) the quantity  $\mathfrak{m}(H, H_{\mathbf{A}} \cap C)$  is an infinite product of local representation densities of  $\psi$  by itself, where  $\psi$  is the restriction of  $\varphi$  to  $W$ ; (3) the set  $\{L^y\}_{y \in Y}$  represents only the  $SO^{\varphi}(W)$ -genus of  $L$ , not the  $SO^{\varphi}(V)$ -genus as in his case. The last point is minor, in view of Remark 35.7, (2).

In most of his papers on this topic Siegel considered ordinary solutions of  $\varphi[x] = q$ , not primitive solutions. However, in [Si44] he investigated, when  $F = \mathbf{Q}$  and  $\varphi$  is indefinite, *primitive* representations of  $q$  by  $\varphi$ , whose nature is essentially the same as that of the elements of our  $L[q, \mathfrak{b}]$ . He defined a quantity of type (37.3) or (37.6b), and showed that it can be expressed as an infinite product of local *primitive* representation densities. In such a case, by strong approximation,  $\{L^y\}$  is reduced to  $L$ , and so our formula (37.6b) becomes

$$(37.8) \quad \nu(\Gamma(L))\mathfrak{m}(L[q, \mathfrak{b}]) = \mathfrak{m}(H, H_{\mathbf{A}} \cap C).$$

This time there is only one kind of difference: the right-hand side concerns the representation densities of  $\psi$  by itself, not the representation densities of  $\varphi[h] = q$  in Siegel's formulation. Anyway, (37.6b) covers both definite and indefinite cases over an arbitrary number field, and should not be confused with any of his formulas. We mention [S99a] as to actual computation of  $\mathfrak{m}(H, H_{\mathbf{A}} \cap C)$ . As for (37.7b), its right-hand side is a kind of *class number* of the group  $H$ , and so its nature is fundamentally different from (37.7a), and that kind of quantity does not appear in Siegel's work.

**37.4.** Let us now treat the sums of three squares we mentioned in §34.3. We take  $(V, \varphi) = (B^{\circ}, \beta^{\circ})$  with the quaternion algebra  $B$  over  $\mathbf{Q}$  of §27.9 for which  $\beta$  is the sum of four squares. Let  $\mathfrak{o}$  be the maximal order of  $B$  given there, and let  $L = B^{\circ} \cap \mathfrak{o}$ . Then  $L = \mathbf{Z}\mathbf{i} + \mathbf{Z}\mathbf{j} + \mathbf{Z}\mathbf{k}$ , the form  $\beta^{\circ}$  on  $L$  is the sum of three squares as in (34.7), and  $L^0[q]$  there can be written  $L[q, \mathbf{Z}]$ ; also we observed that  $\Gamma(L)$  is of order 24. Combining Theorem 27.13(ii) with what we explained in §36.7, we see that the genus of  $L$  consists of a single  $SO^{\varphi}$ -class. Therefore we have  $G_{\mathbf{A}} = GC$ , and so we can take  $Y = \{1\}$  in Theorem 37.2 for the present  $(V, \varphi)$ .

**Theorem 37.5.** (i) *In the setting of §37.4,  $L[q, \mathbf{Z}] \neq \emptyset$  for  $q \in \mathbf{Z}$ ,  $> 0$ , if and only if  $q = c^2m$  with an odd integer  $c$  and a square-free positive integer  $m$  such that  $m + 1 \notin 8\mathbf{Z}$ .*

(ii) *Given  $q = c^2m$  as in (i), let  $K = \mathbf{Q}(\sqrt{-q})$  and let  $\mathfrak{f}$  be the order in  $K$  of conductor  $c$ . Then*

$$\#L[q, \mathbf{Z}] = c(\mathfrak{f}) \cdot \begin{cases} 6 & \text{if } q = 1, \\ 8 & \text{if } q = 3, \\ 24 & \text{if } m - 3 \in 4\mathbf{Z} \text{ and } q > 3, \\ 12 & \text{in all other cases.} \end{cases}$$

(iii) *The notation being the same as in (ii), we have*

$$\#\{L[q, \mathbf{Z}]/\Gamma(L)\} = c(\mathfrak{f}) \cdot \begin{cases} 1 & \text{if } q \leq 2 \text{ or } m - 3 \in 4\mathbf{Z}, \\ 2^{-1} & \text{otherwise.} \end{cases}$$

PROOF. For each prime number  $p$  we put  $B_p = B \otimes_{\mathbf{Q}} \mathbf{Q}_p$ ,  $\mathfrak{o}_p = \mathfrak{o} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ , and  $L_p = L \otimes_{\mathbf{Z}} \mathbf{Z}_p$ . Suppose  $L[q, \mathbf{Z}] \neq \emptyset$ ; then by Theorem 27.14(ii),  $q = c^2m$  with  $c \in \mathbf{Z}$  and a square-free positive integer  $m$  such that  $m + 1 \notin 8\mathbf{Z}$ . Let  $h \in L[q, \mathbf{Z}]$  and suppose  $c \in 2\mathbf{Z}$ . Put  $k = 2^{-1}h$ . Then  $\varphi[k] \in \mathbf{Z}$ , and so  $k \in \mathfrak{o}_2$  by Theorem 21.21; thus  $k \in L_2$ . Since  $k \in L_p$  for every  $p \neq 2$ , we see that  $k \in L$ , and so  $h \notin L[q, \mathbf{Z}]$ , a contradiction. Therefore  $c \notin 2\mathbf{Z}$ , which proves the “only if”-part of (i). To prove the “if”-part, let  $q = c^2m$  with  $c$  and  $m$  as in (i). Let  $K = \mathbf{Q}(\sqrt{-q})$  and let  $\mathfrak{f}$  be the order in  $K$  of conductor  $c\mathbf{Z}$ . Take  $\mu \in K$  so that  $\mathbf{Z} + \mu\mathbf{Z}$  is the maximal order of  $K$ . Then  $\mathfrak{f} = \mathbf{Z} + c\mu\mathbf{Z}$ . As shown in the proof of Theorem 27.14(ii), there is a  $\mathbf{Q}$ -linear injection  $g$  of  $K$  into  $B$ . Let  $\mathbf{p}$  be the set of prime numbers  $p$  such that  $g(\mathfrak{f})_p \neq g(K)_p \cap \mathfrak{o}_p$ . Then  $\mathbf{p}$  is a finite set and  $2 \notin \mathbf{p}$ , since  $\mathfrak{f}_2 = \mathfrak{r}_2$  and  $g(\mathfrak{r}_2) \subset \mathfrak{o}_2$ . Thus for every  $p \in \mathbf{p}$  we can identify  $B_p$  and  $\mathfrak{o}_p$  with  $M_2(\mathbf{Q}_p)$  and  $M_2(\mathbf{Z}_p)$ . For such a  $p$  define  $j_p : K_p \rightarrow M_2(\mathbf{Q}_p)$  by  $a[1 \ c\mu] = [1 \ c\mu]j_p(a)$  for  $a \in K_p$ . We easily see that  $a \in \mathfrak{f}_p$  if and only if  $j_p(a) \in M_2(\mathbf{Z}_p)$ , and so  $j_p(\mathfrak{f})_p = j_p(K_p) \cap \mathfrak{o}_p$ . By Theorem 19.10,  $g(x) = \xi_p j_p(x) \xi_p^{-1}$  for every  $x \in K_p$  with some  $\xi_p \in B_p^\times$ . Then  $g(\mathfrak{f})_p = g(K_p) \cap \xi_p \mathfrak{o}_p \xi_p^{-1}$ . Now we can define a maximal order  $\mathfrak{o}'$  in  $B$  such that  $\mathfrak{o}'_p = \mathfrak{o}_p$  for every  $p \notin \mathbf{p}$  and  $\mathfrak{o}'_p = \xi_p \mathfrak{o}_p \xi_p^{-1}$  for every  $p \in \mathbf{p}$ . Then  $g(\mathfrak{f})_p = g(K)_p \cap \mathfrak{o}'_p$  for all  $p$ , and so  $g(\mathfrak{f}) = g(K) \cap \mathfrak{o}'$ . By Theorem 27.13(ii),  $\mathfrak{o}' = \alpha \mathfrak{o} \alpha^{-1}$  with  $\alpha \in B^\times$ . Define  $\theta : K \rightarrow B$  by  $\theta(x) = \alpha^{-1}g(x)\alpha$  for  $x \in K$ . Then  $\theta(\mathfrak{f}) = \theta(K) \cap \mathfrak{o}$ . Put  $k = \theta(\sqrt{-m})$  and  $h = ck$ . Since  $c\sqrt{-m} \in \mathfrak{f}$ , we see that  $h \in L$  and  $\varphi[h] = q$ . By Theorem 36.10,  $q\varphi(h, L)_p^{-2} = c^2m\mathbf{Z}_p$  for  $p \neq 2$ , and so  $\varphi(h, L)_p = \mathbf{Z}_p$  for  $p \neq 2$ . Put  $k = x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$  with  $x, y, z \in \mathbf{Q}$ . Since  $\mathfrak{o}_2$  is the unique maximal order in  $B_2$ , we see that  $x, y, z \in \mathbf{Z}_2$ . Also,  $x^2 + y^2 + z^2 = m$ , which is square-free, and so  $\varphi(k, L)_2 = x\mathbf{Z}_2 + y\mathbf{Z}_2 + z\mathbf{Z}_2 = \mathbf{Z}_2$ . Since  $\varphi(h, L)_2 = \varphi(k, L)_2$ , we have  $\varphi(h, L) = \mathbf{Z}$ . Thus  $h \in L[q, \mathbf{Z}]$ . This completes the proof of (i).



Take  $y = 1$  and  $\mathbf{b} = \mathbf{Z}$  in (37.6a). Since  $H$  is commutative and  $\mathcal{E} \subset H_{\mathbf{A}}$ , we have  $\Delta_{\varepsilon} = H \cap C$  for every  $\varepsilon \in \mathcal{E}$ . Clearly  $H \cap C$  is contained in  $U$  of Theorem 36.10, and so by (36.10a) we have  $\Delta_{\varepsilon} = U'$  for every  $\varepsilon \in \mathcal{E}$ . Thus from (37.6a) we obtain

$$(37.9) \quad \#L[q, \mathbf{Z}] = 24[U' : 1]^{-1}[H_{\mathbf{A}} : (H_{\mathbf{A}} \cap C)H].$$

From (36.11) we obtain  $[H_{\mathbf{A}} : (H_{\mathbf{A}} \cap C)H] = 2^{1-\mu}c(\mathfrak{f})[\mathfrak{f}^{\times} : U']^{-1}$ , and therefore

$$\#L[q, \mathbf{Z}] = 2^{1-\mu}24c(\mathfrak{f})/[\mathfrak{f}^{\times} : 1],$$

where  $\mu = 1$  if 2 is ramified in  $K$  and  $\mu = 0$  otherwise. Since  $K = \mathbf{Q}(\sqrt{-m})$ , we have  $\mu = 0$  if  $m - 3 \in 4\mathbf{Z}$  and  $\mu = 1$  otherwise;  $[\mathfrak{f}^{\times} : 1] = 4$  if  $q = 1$ ,  $[\mathfrak{f}^{\times} : 1] = 6$  if  $q = 3$ , and  $[\mathfrak{f}^{\times} : 1] = 2$  in all other cases. Therefore we obtain (ii).

Since  $Y = \{1\}$  as mentioned in §37.4, from (37.7b) and (37.9) we obtain

$$24\#\{L[q, \mathbf{Z}]/\Gamma(L)\} = 24[H_{\mathbf{A}} : (H_{\mathbf{A}} \cap C)H] = \#L[q, \mathbf{Z}] \cdot [U' : 1].$$

We can easily verify that  $[U' : 1] = 4$  if  $q = 1$ ,  $[U' : 1] = 2$  if  $q = 2$ ,  $[U' : 1] = 3$  if  $q = 3$ , and  $[U' : 1] = 1$  if  $q > 3$ . Therefore we obtain (iii).

We can express the last result also as follows:

$$(37.10) \quad \#L[q, \mathbf{Z}] = 24\#\{L[q, \mathbf{Z}]/\Gamma(L)\} \quad \text{if } q > 3.$$

As explained in §36.14,  $c(\mathfrak{f})$  is exactly the number of classes of primitive binary forms of discriminant  $-q$ , which we denoted by  $c(q)$  in §§34.2 and 34.3. Therefore Theorem 37.5(ii) and (iii) are essentially the same as (34.8b) and (34.8a) respectively.

Here we treated sums of three squares. We can actually discuss sums of  $m$  squares for an arbitrary  $m \in \mathbf{Z}$ ,  $> 1$ . As we said in §34.1, the problem about  $L[q]$  is different from that about  $L^0[q]$ . We refer the reader to [S02] and [S04a] for the former, and to [S04b] and [S06b] for the latter. In particular, it is shown in [S06b] that there are exactly 64 positive definite ternary quadratic spaces over  $\mathbf{Q}$  for which the genus of maximal lattices consists of a single class. Moreover, for each such ternary form we can state a theorem similar to Theorem 37.5; see Theorems 6.6, 6.7, and §6.9 of [S06b]. A short history of the problems concerning sums of squares is given in [Har]; see also remarks [R1] through [R7] at the end of [S06a].

### 38. The theory of genera

**38.1.** In this section we let  $K$  denote a quadratic extension of  $\mathbf{Q}$ ,  $\rho$  the nontrivial automorphism of  $K$  over  $\mathbf{Q}$ ,  $\mathfrak{r}$  the maximal order of  $K$ ,  $\mathcal{I}_K$  the ideal group of  $K$ ,  $\mathfrak{P}_K$  the group of all principal ideals  $\alpha\mathfrak{r}$  with  $\alpha \in K^{\times}$ , and  $\mathfrak{P}_K^{+}$  the subgroup of  $\mathfrak{P}_K$  consisting of all  $\alpha\mathfrak{r}$  such that  $N(\alpha) > 0$ , where we

put  $N(\xi) = N_{K/\mathbf{Q}}(\xi)$  for  $\xi \in K$ . We fix an embedding of  $K$  into  $\mathbf{C}$ . Thus we view  $K$  as a subfield of  $\mathbf{R}$  if  $K$  is real.

Clearly  $\mathfrak{P}_K = \mathfrak{P}_K^+$  if  $K$  is imaginary or  $N(\mathfrak{r}^\times) = \{\pm 1\}$ ;  $[\mathfrak{P}_k : \mathfrak{P}_K^+] = 2$  if  $K$  is real and  $N(\mathfrak{r}^\times) = \{1\}$ .

Let  $\Phi = \mathfrak{I}_K / \mathfrak{P}_K^+$ . This is called *the narrow ideal class group of  $K$* . We call a fractional ideal  $\mathfrak{a}$  in  $K$  **ambiguous** if  $\mathfrak{a}^\rho = \mathfrak{a}$ , and call a coset  $C \in \Phi$  **ambiguous** if  $C^\rho = C$ .

**Lemma 38.2.** *For  $C \in \Phi$  we have*

$$C^2 = 1 \iff C^\rho = C \iff C \text{ contains an ambiguous ideal.}$$

PROOF. Let  $\mathfrak{a} \in C$ . Then  $N(\mathfrak{a})\mathfrak{r} = \mathfrak{a}\mathfrak{a}^\rho \in CC^\rho$ , and so  $CC^\rho = 1$ . Thus  $C^2 = 1$  if  $\mathfrak{a}^\rho = \mathfrak{a}$ . Also,  $C^2 = 1$  if and only if  $C = C^\rho$ . Therefore the only remaining point is the last  $\Rightarrow$ . Suppose  $\mathfrak{a} \in C = C^\rho$ . Then  $\mathfrak{a}^\rho = b\mathfrak{a}$  with  $b \in K^\times$  such that  $N(b) > 0$ . Since  $N(b\mathfrak{r}) = \mathbf{Z}$ , we have  $N(b) = 1$ . By Lemma 1.8,  $b = c/c^\rho$  with some  $c \in K^\times$ . Then  $(c\mathfrak{a})^\rho = c\mathfrak{a}$ . If  $K$  is imaginary, then  $N(c) > 0$ , and so  $c\mathfrak{a} \in C$ . If  $K$  is real, replacing  $b$  by  $-b$  if necessary, we may assume that  $b > 0$ . Then  $cc^\rho = c^2/b > 0$ , and so  $c\mathfrak{a} \in C$ . This proves the last  $\Rightarrow$ , and completes the proof.

**Theorem 38.3.** *Let  $\Psi = \{C \in \Phi \mid C = C^\rho\}$  and let  $t$  be the number of prime factors of  $D_K$ . Then  $[\Psi : 1] = 2^{t-1}$ .*

PROOF. Let  $p_1, \dots, p_t$  be the prime factors of  $D_K$ . Then  $p_i\mathfrak{r} = \mathfrak{p}_i^2$  with a prime ideal  $\mathfrak{p}_i$  of  $\mathfrak{r}$ . Let  $C \in \Psi$ . By Lemma 38.2,  $C$  contains an ideal  $\mathfrak{a}$  such that  $\mathfrak{a}^\rho = \mathfrak{a}$ . We can put  $\mathfrak{a} = b\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$  with  $0 < b \in \mathbf{Q}$  and integers  $e_i$  which are 0 or 1. Therefore  $\Psi$  is generated by the classes of  $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ . Take a square-free positive or negative integer  $m$  so that  $K = \mathbf{Q}(\sqrt{m})$ . Then  $D_K = m$  if  $m - 1 \in 4\mathbf{Z}$  and  $D_K = 4m$  otherwise; see (10.11). Also  $|m| = p_1 \cdots p_t$  if  $m - 3 \notin 4\mathbf{Z}$ , and  $|2m| = p_1 \cdots p_t$  if  $m - 3 \in 4\mathbf{Z}$ . In the latter case we take  $p_t = 2$ . Thus  $\sqrt{m}\mathfrak{r} = \mathfrak{p}_1 \cdots \mathfrak{p}_{t-1}$  if  $m - 3 \in 4\mathbf{Z}$ , and  $\sqrt{m}\mathfrak{r} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$  otherwise.

Suppose  $m < 0$ . Then  $N(\sqrt{m}) > 0$ , and so  $\mathfrak{p}_1 \cdots \mathfrak{p}_t$  or  $\mathfrak{p}_1 \cdots \mathfrak{p}_{t-1}$  belongs to  $\mathfrak{P}_K^+$ . Thus  $[\Psi : 1] \leq 2^{t-1}$ . Suppose  $m > 0$  and  $N(\mathfrak{r}^\times) = \{\pm 1\}$ . Take  $\varepsilon \in \mathfrak{r}^\times$  so that  $N(\varepsilon) = -1$ . Then  $N(\varepsilon\sqrt{m}) > 0$ , and we again obtain  $[\Psi : 1] \leq 2^{t-1}$ . Suppose  $m > 0$  and  $N(\mathfrak{r}^\times) = 1$ . Take a fundamental unit  $\varepsilon$  of  $K$  such that  $\varepsilon > 0$ . Since  $\varepsilon\varepsilon^\rho = 1$ , we see that  $\varepsilon = \beta/\beta^\rho$  with  $\beta \in K^\times$  by Lemma 1.8. We may assume that  $\beta \in \mathfrak{r}$ . Then  $N(\beta) = \varepsilon(\beta^\rho)^2 > 0$ , and so  $\beta\mathfrak{r} \in \mathfrak{P}_K^+$ . Take  $\beta$  so that  $N(\beta)$  is the smallest. Then  $\beta/c \notin \mathfrak{r}$  for every  $c \in \mathbf{Z}, > 1$ . Also,  $\beta\mathfrak{r} \neq \mathfrak{r}$ . (If  $\beta \in \mathfrak{r}^\times$ , then  $\beta\beta^\rho = 1$ , and so  $\varepsilon = \beta^2$ , a contradiction.) Since  $\beta^\rho\mathfrak{r} = \beta\mathfrak{r}$ , we have  $\beta\mathfrak{r} = b\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$  with  $b$  and  $\mathfrak{p}_i^{e_i}$  at the beginning of our proof. Then  $b = 1$  and  $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$  is a nontrivial element of  $\mathfrak{P}_K^+$ . Thus  $[\Psi : 1] \leq 2^{t-1}$  in this case too.

To prove that  $[\Psi : 1] = 2^{t-1}$ , we may assume that  $t > 1$ . This excludes the cases  $m = -1$  and  $m = -3$ . Our task is to show that if  $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s} = \alpha \mathfrak{r} \neq \mathfrak{r}$  with  $s > 0$  and  $N(\alpha) > 0$ , then such a relation is what we already found above. If this is done, our proof is complete. Take such an  $\alpha$ ; then  $\alpha^\rho = \eta \alpha$  with  $\eta \in \mathfrak{r}^\times$ . Then  $N(\eta) = 1$ . Suppose  $m < 0$ . Since the cases  $m = -1$  and  $m = -3$  are excluded, we have  $\eta = \pm 1$ . If  $\eta = 1$ , then  $\alpha \in \mathbf{Z}$ , which is impossible, and so  $\eta = -1$ . Then  $\alpha = c\sqrt{m}$  with  $c \in \mathbf{Z}$ , and clearly  $c = \pm 1$ . Thus the relation is the prime decomposition of  $\sqrt{m}\mathfrak{r}$  we already know.

Next suppose  $m > 0$ . Then  $\eta = \alpha\alpha^\rho/\alpha^2 > 0$  and  $\eta^\rho > 0$ . Let  $\varepsilon$  be a fundamental unit of  $K$ . Suppose  $N(\varepsilon) = -1$ . Then  $\eta = \varepsilon^{2\nu}$  with  $0 \leq \nu \in \mathbf{Z}$ ,  $(\varepsilon^\nu \alpha)^\rho = \pm \varepsilon^\nu \alpha$ , and so  $\varepsilon^\nu \alpha \in \mathbf{Z}$  or  $\varepsilon^\nu \alpha \in \mathbf{Z}\sqrt{m}$ ; also,  $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s} = \varepsilon^\nu \alpha \mathfrak{r}$ . For the same reason as in the case  $m < 0$  we find that this is again the prime decomposition of  $\sqrt{m}\mathfrak{r}$ .

Finally suppose that  $m > 0$  and  $N(\varepsilon) = 1$ . Take  $\beta$  so that  $\varepsilon = \beta/\beta^\rho$  as before. We have  $\eta = \varepsilon^k$  with  $k \in \mathbf{Z}$ . Thus  $\alpha\beta^k = (\alpha\beta^k)^\rho$ , and so  $\alpha\beta^k = c \in \mathbf{Z}$ . Therefore  $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s} = c(\beta\mathfrak{r})^{-k}$ , and consequently, the relation  $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s} \in \mathfrak{P}_K^+$  adds nothing more than the prime decomposition of  $\beta\mathfrak{r}$  we considered above. This completes the proof.

**38.4.** *Proof of (36.6b) when  $F = \mathbf{Q}$ .* Let  $\mathfrak{I}_K$  and  $\mathfrak{I}_{K/F}$  be as in §36.5 and let  $\Psi$  and  $t$  be as in Theorem 38.3. Then  $\Psi$  can be identified with  $\mathfrak{I}_{K/F}/\mathfrak{P}_K^+$ , and therefore

$$[\mathfrak{I}_K : \mathfrak{I}_{K/F}][\Psi : 1] = [\mathfrak{I}_K : \mathfrak{P}_K^+] = [\mathfrak{I}_K : \mathfrak{P}_K][\mathfrak{P}_K : \mathfrak{P}_K^+] = c_K[\mathfrak{P}_K : \mathfrak{P}_K^+],$$

and so  $[\mathfrak{I}_K : \mathfrak{I}_{K/F}] = 2^{1-t}c_K[\mathfrak{P}_K : \mathfrak{P}_K^+]$ . Since  $[\mathfrak{P}_K : \mathfrak{P}_K^+] = 2$  if  $K$  is real and  $N_{K/\mathbf{Q}}(\mathfrak{r}^\times) = \{1\}$ , and  $[\mathfrak{P}_K : \mathfrak{P}_K^+] = 1$  otherwise, we obtain (36.6b).

**38.5.** Put  $\Phi^2 = \{C^2 \mid C \in \Phi\}$ . By Lemma 38.2,  $\Psi = \{C \in \Phi \mid C^2 = 1\}$ , and so  $\Phi/\Psi \cong \Phi^2$ . Thus  $[\Phi : \Phi^2] = [\Psi : 1] = 2^{t-1}$ . Traditionally each coset of  $\Phi/\Phi^2$  is called a **genus** (Geschlecht). Thus there are  $2^{t-1}$  genera. In particular,  $\Phi^2$  itself is called the **principal genus** (Hauptgeschlecht). The term used by Gauss corresponding to this is the origin of the terminology “genus.” Indeed, the set of classes in the genus of maximal lattices in the space  $(K, c\kappa)$  considered in §36.5, when  $F = \mathbf{Q}$ , is essentially the principal genus.

Since  $[\Phi : \Phi^2] = 2^{t-1}$ , we see that  $[\Phi : 1]$  is odd if and only if  $t = 1$ . Therefore we obtain

**Corollary 38.6.** *The index  $[\mathfrak{I}_K : \mathfrak{P}_K^+]$ , which is traditionally called the class number of  $K$  in the narrow sense, is odd if and only if  $K$  is  $\mathbf{Q}(\sqrt{-1})$ ,  $\mathbf{Q}(\sqrt{\pm 2})$ , or  $\mathbf{Q}(\sqrt{\varepsilon q})$  with  $\varepsilon = \pm 1$  and a prime number  $q$  such that  $q - \varepsilon \in 4\mathbf{Z}$ .*

**38.7.** Hereafter we assume that the reader is familiar with class field theory. By class field theory there is an abelian extension  $S$  of  $K$  such that every prime ideal of  $K$  is unramified in  $S$  and the map  $\mathfrak{a} \mapsto \left(\frac{S/K}{\mathfrak{a}}\right)$  for  $\mathfrak{a} \in \mathfrak{I}_K$  gives an isomorphism of  $\mathfrak{I}_K/\mathfrak{P}_K^+$  onto  $\text{Gal}(S/K)$ , where  $\left(\frac{S/K}{\mathfrak{a}}\right)$  is defined by (16.5). Then  $\Phi \cong \text{Gal}(S/K)$ , and therefore there is an extension  $L$  of  $K$  contained in  $S$  such that  $\Phi^2 \cong \text{Gal}(S/L)$ . Thus  $\text{Gal}(L/K) \cong \Phi/\Phi^2$ , and so  $[L : K] = 2^{t-1}$  with  $t$  as in Theorem 38.3.

To present  $L$  explicitly, let  $K = \mathbf{Q}(\sqrt{m})$  with a square-free integer  $m$ . Let  $p_1, \dots, p_r, q_1, \dots, q_s$  be the prime factors of  $m$ , where  $p_i - 1 \in 4\mathbf{Z}$  and  $q_j + 1 \in 4\mathbf{Z}$ . Then there are three cases according to the nature of  $m$ , and we can take  $L$  in each case as follows:

$$(I) \quad m = p_1 \cdots p_r (-q_1) \cdots (-q_s), \quad m - 1 \in 4\mathbf{Z}, \quad t = r + s.$$

$$L = \mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{-q_1}, \dots, \sqrt{-q_s}).$$

$$(II) \quad m = -p_1 \cdots p_r (-q_1) \cdots (-q_s), \quad m + 1 \in 4\mathbf{Z}, \quad t = r + s + 1.$$

$$L = \mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{-q_1}, \dots, \sqrt{-q_s}, \sqrt{-1}).$$

$$(III) \quad m = \delta p_1 \cdots p_r (-q_1) \cdots (-q_s), \quad \delta = \pm 2, \quad t = r + s + 1.$$

$$L = \mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_r}, \sqrt{-q_1}, \dots, \sqrt{-q_s}, \sqrt{\delta}).$$

We can easily verify that  $K \subset L$ ,  $[L : K] = 2^{t-1}$ , and every prime ideal of  $K$  is unramified in  $L$ .

**Theorem 38.8.** *The field  $L$  is maximum among the abelian extensions of  $\mathbf{Q}$  containing  $K$  in which every prime ideal of  $K$  is unramified.*

PROOF. Let  $M$  be such an extension of  $K$ . Suppose  $[M : \mathbf{Q}]$  has an odd prime factor  $p$ . Then there is a subfield  $H$  of  $M$  such that  $[H : \mathbf{Q}] = p$ . Take a prime number  $q$  ramified in  $H$ . Since  $H$  is a cyclic extension of  $\mathbf{Q}$  of degree  $p$ , the prime  $q$  is completely ramified in  $H$ . Then any prime factor of  $q$  in  $K$  must be ramified in  $KH$ , and so it must be ramified in  $M$ , a contradiction. Thus  $[M : \mathbf{Q}] = 2^k$  with  $0 \leq k \in \mathbf{Z}$ . Suppose  $\text{Gal}(M/\mathbf{Q})$  has an element of order 4. Then  $M$  has a subfield  $A$  such that  $\text{Gal}(A/\mathbf{Q})$  is a cyclic group of order 4. Take a prime number  $p$  ramified in  $A$ . Then  $p$  is completely ramified in  $A$ ; see Exercise 2 at the end of Section 16. Since  $[K : \mathbf{Q}] = 2$ , any prime factor of  $p$  in  $K$  must be ramified in  $M$ , a contradiction. Thus  $\text{Gal}(M/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^\nu$  with  $\nu \in \mathbf{Z}$ , and so  $\text{Gal}(M/K) \cong (\mathbf{Z}/2\mathbf{Z})^{\nu-1}$ . Let  $X$  be the subgroup of  $\Phi = \mathfrak{I}_K/\mathfrak{P}_K^+$  corresponding to  $M$ . Then  $\Phi^2 \subset X$ , and so  $M \subset L$ . This proves our theorem.

**Theorem 38.9.** *Let  $S$  and  $L$  be as in §38.7 and  $\mathfrak{r}$  the maximal order of  $K$ ; let  $p$  be a prime number unramified in  $K$ . Then*

$$(38.1) \quad p \in N_{K/\mathbf{Q}}(\mathfrak{r}) \iff p \text{ decomposes completely in } S,$$

$$(38.2) \quad p \in N_{K/\mathbf{Q}}(K) \iff p \text{ decomposes completely in } L.$$

PROOF. Suppose  $p = N(\alpha)$  with  $\alpha \in \mathfrak{r}$ ; let  $\mathfrak{p} = \alpha\mathfrak{r}$ . Then  $p\mathfrak{r} = \mathfrak{p}\mathfrak{p}^\rho$ . Since  $N(\alpha) > 0$ , we have  $\left(\frac{S/K}{\mathfrak{p}}\right) = 1$ , and so  $\mathfrak{p}$  decomposes completely in  $S$ , and so  $p$  decomposes completely in  $S$ . Conversely, suppose  $p$  decomposes completely in  $S$ . Then  $p\mathfrak{r} = \mathfrak{p}\mathfrak{p}^\rho$  with a prime ideal  $\mathfrak{p}$  in  $K$ , and  $\mathfrak{p}$  decomposes completely in  $S$ , and so  $\left(\frac{S/K}{\mathfrak{p}}\right) = 1$ . Thus  $\mathfrak{p} = \alpha\mathfrak{r}$  with  $\alpha \in \mathfrak{r}$  such that  $N(\alpha) > 0$ . Then  $N(\alpha) = p$ . This proves (i).

Next suppose  $p = \beta\beta^\rho$  with  $\beta \in K$ . Clearly  $p$  must split in  $K$ , and so  $p\mathfrak{r} = \mathfrak{p}\mathfrak{p}^\rho$  with a prime ideal  $\mathfrak{p}$  in  $K$ . Put  $\mathfrak{a} = \beta^{-1}\mathfrak{p}$  and  $\mathfrak{b} = \mathfrak{r} + \mathfrak{a}^\rho$ . Then  $\mathfrak{a}\mathfrak{a}^\rho = \mathfrak{r}$ ,  $\mathfrak{a}\mathfrak{b} = \mathfrak{b}^\rho$ , and  $\mathfrak{a} = \mathfrak{b}^{-1}\mathfrak{b}^\rho$ . Since  $\mathfrak{b}\mathfrak{b}^\rho = N(\mathfrak{b})\mathfrak{r} \in \mathfrak{P}_K^+$ , we see that  $\mathfrak{a}\mathfrak{P}_K^+ \in \Phi^2$ , and so  $\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{a}}\right) = 1$ . Thus  $\mathfrak{p}$  decomposes completely in  $L$ , and consequently  $p$  decomposes completely in  $L$ . Conversely, suppose  $p\mathfrak{r} = \mathfrak{p}\mathfrak{p}^\rho$  in  $K$  and  $\mathfrak{p}$  decomposes completely in  $L$ . Then  $\mathfrak{p}\mathfrak{P}_K^+$  belongs to  $\Phi^2$ , and so  $\mathfrak{p} = \alpha\mathfrak{b}^2$  with  $\mathfrak{b} \in \mathfrak{I}_K$  and  $\alpha \in K$ ,  $N(\alpha) > 0$ . We have  $p = N(\alpha)N(\mathfrak{b})^2 = N_{K/\mathbf{Q}}(\alpha N(\mathfrak{b}))$ . This proves (ii) and completes the proof.

From the explicit form of  $L$  in §38.7 we see that  $L$  is contained in the cyclotomic field generated by a primitive  $|D_K|$ -th root of unity. Therefore the above theorem means that we can state a necessary and sufficient condition for  $p \in N_{K/\mathbf{Q}}(K)$  as some congruence conditions on  $p$  modulo  $D_K$ . However, we can state such a necessary and sufficient condition for  $p \in N_{K/\mathbf{Q}}(\mathfrak{r})$  as some congruence conditions on  $p$  modulo  $D_K$  only when  $S = L$ , that is, only when every element of  $\mathfrak{I}_K/\mathfrak{P}_K^+$  is of order 2.

## REFERENCES

- [Ano] Anonymous, Correspondence, *Ann. of Math.* 69 (1959), 247–251.
- [B] P. Bachmann, *Die Arithmetik der Quadratischen Formen*, Leipzig, Teubner, 1898.
- [C] C. Chevalley, Sur la théorie du corps de classes dans les corps finis et les corps locaux, *J. Fac. Sci. Univ. Tokyo* 2 (1933) 365–476.
- [CF] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967.
- [Ch] K.-S. Chang, Diskriminanten und Signaturen gerader quadratischer Formen, *Arch. Math.* 21 (1970), 59–65.
- [DD] L. Dirichlet, *Vorlesungen über Zahlentheorie*, supplement by R. Dedekind, Braunschweig, 1894.
- [E38] M. Eichler, Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre  $L$ -Reihen, *J. Reine u. Angew. Math.* 179 (1938), 227–251.
- [E52a] M. Eichler, Die Ähnlichkeitsklassen indefiniter Gitter, *Math. Z.* 55 (1952), 216–252.
- [E52b] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Springer, Berlin, 1952, 2nd ed. 1974.
- [G] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801, English translation by A. A. Clarke, Yale Univ. Press, 1966.
- [Har] G. H. Hardy, On the representation of a number as the sum of any number of squares, and in particular of five, *Trans. Amer. Math. Soc.* 21 (1920), 255–284.
- [Has] H. Hasse, Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper, *J. für die Reine und Angew. Math.*, 153 (1924), 158–162.
- [K] M. Kneser, Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen, *Arch. d. Math.* 7 (1956), 323–332.
- [M] J. Milnor, On simply connected 4-manifolds, *Symposium Internacional Topologia Algebraica*, Mexico 1958, 122–128.
- [O] O. T. O'Meara, *Introduction to quadratic forms*, Springer, 1963.
- [S73] G. Shimura, On modular forms of half integral weight, *Ann. of Math.*, 97 (1973), 440–481 (=Collected Papers II, 532–573).
- [S93] G. Shimura, On the transformation formulas of theta series, *Amer. J. of Math.*, 115 (1993), 1011–1052 (=Collected Papers IV, 191–232).
- [S97] G. Shimura, *Euler Products and Eisenstein series*, CBMS Regional Conference Series in Math. No. 93, Amer. Math. Soc. 1997.
- [S99a] An exact mass formula for orthogonal groups, *Duke Mathematical Journal*, 97 (1999), 1–66 (=Collected Papers IV, 509–574).

- [S99b] G. Shimura, The number of representations of an integer by a quadratic form, *Duke Mathematical Journal*, 100 (1999), 59–92 (=Collected Papers IV, 575–608).
- [S01] G. Shimura, The relative regulator of an algebraic number field, *Collected Papers IV*, 720–736, 2003.
- [S02] G. Shimura, The representation of integers as sums of squares, *Amer. J. Math.* 124 (2002), 1059–1081.
- [S04a] G. Shimura, Inhomogeneous quadratic forms and triangular numbers, *Amer. J. Math.* 126 (2004), 191–214.
- [S04b] G. Shimura, Arithmetic and analytic theories of quadratic forms and Clifford groups, *Mathematical Surveys and Monographs*, vol. 109, Amer. Math. Soc., 2004.
- [S06a] G. Shimura, Quadratic Diophantine equations, the class number, and the mass formula, *Bull. Amer. Math. Soc.* 43 (2006), 285–304.
- [S06b] G. Shimura, Classification, construction, and similitudes of quadratic forms, *Amer. J. Math.* 128 (2006), 1521–1552.
- [S06c] G. Shimura, Integer-valued quadratic forms and quadratic Diophantine equations, *Documenta Mathematica* 11, (2006), 333–367.
- [S08] G. Shimura, Classification of integer-valued symmetric forms, *Amer. J. Math.* 130 (2008), 685–711.
- [Si35] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, *Ann. of Math.* 36 (1935), 527–606 (=Gesammelte Abhandlungen I, 326–405).
- [Si36] C. L. Siegel, Über die analytische Theorie der quadratischen Formen II, *Ann. of Math.* 37 (1936), 230–263 (=Gesammelte Abhandlungen I, 410–443).
- [Si44] C. L. Siegel, On the theory of indefinite quadratic forms, *Ann. of Math.* 45 (1944), 577–622 (=Gesammelte Abhandlungen, II, 421–466).
- [V] F. van der Blij, An invariant of quadratic forms mod 8, *Indag. Math.* 21 (1959), 291–293.
- [We] A. Weil, *Number Theory*, Birkhäuser, Boston, Basel, Stuttgart, 1984.
- [Wi] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, *J. für die Reine und Angew. Math.*, 176 (1937), 31–44.

# INDEX

## A

Adele ring, 66  
Adelization, 174–175  
Algebra, 47, 79  
Algebraic integer, 27  
Algebraic number field, 27  
Ambiguous ideal, 229  
Ambiguous ideal class, 229  
Anisotropic, 115  
Anti-automorphism, 89  
Anti-isomorphism, 89  
Archimedean prime, 66  
Archimedean valuation, 16

## B

Binary Form, 203

## C

Canonical automorphism, 122  
Canonical involution, 122  
Cauchy sequence, 16  
Center, 86  
Central simple algebra, 86ff  
Central, 86  
Characteristic algebra, 153  
Character (modulo an integer), 7  
Class (of a binary form), 204  
Class (of a lattice), 171  
Class (of a matrix), 178  
Class (of a proper ideal), 215  
Class number (of a number field), 42  
Class number (of an order), 215  
Class number (of a quadratic space), 181  
Clifford algebra, 121  
Clifford group, 127  
Commutator, 90  
Complete, 16  
Completely reducible (module), 81  
Completion, 17, 39  
Conductor (of a character), 9  
Conductor (of an order), 213  
Core dimension, 117  
Core subspace, 117  
Cyclotomic field, 75ff

## D

Decomposition group, 71

Dedekind zeta function, 56  
Definite (quaternion algebra), 147  
Different, 59  
Dirichlet character, 7  
Discrete order function, 15  
Discriminant algebra, 120  
Discriminant field, 120  
Discriminant ideal (of a lattice), 162  
Discriminant ideal (of a quaternion algebra), 114  
Discriminant (of a binary form), 204, 221  
Discriminant (of a field), 39  
Discriminant (of a lattice), 39  
Discriminant (of a quadratic form), 119  
Discriminant (of a quaternion algebra), 147  
Division algebra, 79

## E

Eisenstein equation, 34  
Eisenstein polynomial, 34  
Equivalent (representations), 92  
Equivalent (valuations), 20  
Euler's function, 4  
Even Clifford algebra, 122  
Even Clifford group, 127

## F

Faithful representation, 92  
 $F$ -algebra, 79  
Finite field, 3  
Fractional ideal, 35  
Free module, 11  
Frobenius automorphism, 73  
Fundamental unit, 56

## G

Gauss sum, 7  
Genus (of a lattice), 171  
Genus (of a matrix), 178  
Genus (of ideals), 230  
 $\mathfrak{g}$ -ideal, 101  
Global field, 100  
Group algebra, 85

## H

Hamilton quaternion algebra, 96  
Hasse norm theorem, 141



Hasse principle, 146  
 Hensel's lemma, 23  
 Hilbert reciprocity law, 141  
 Hilbert symbol, 140

## I

Ideal class, 42  
 Ideal class group, 42  
 Ideal group, 36  
 Idele group, 68  
 Idele norm, 67  
 Imaginary archimedean prime, 66  
 Imaginary quadratic field, 40  
 Indecomposable (ring), 3  
 Indefinite (quaternion algebra), 147  
 Inertia group, 72  
 Integral (lattice), 161  
 Integral (over a ring), 25, 101  
 Integral closure, 25  
 Integral ideal, 35  
 Integrally closed, 25  
 Invertible (element of a quadratic space), 121  
 Involution, 89  
 Irreducible (module), 79  
 Isotropic, 115

## L

Lattice (in a real vector space), 50  
 Lattice (in a vector space), 11  
 Left order, 101  
 Left regular representation, 92  
 Left semisimple, 81  
 Level, 181  
 Local field, 100

## M

Main involution, 98  
 Mass, 224  
 Maximal ideal (of a valuation ring), 17  
 Maximal lattice, 161  
 Maximal order, 27  
 Minimal ideal, 81  
 Minimal/minimum polynomial, xi  
 Minkowski's lemma, 52  
 Monic polynomial, xi

## N

Nonarchimedean prime, 66  
 Nonarchimedean valuation, 16  
 Nondegenerate quadratic space, 115

Norm (of an ideal), 35, 38  
 Norm form, 134  
 Normalized order function, 15

## O

Order (in a quadratic extension), 213ff  
 Order (in an algebra), 101  
 Order function, 15  
 Orthogonal basis, 119  
 Orthogonal complement, 115  
 Orthogonal group, 116

## P

$p$ -adic field, 19  
 $p$ -adic integer, 19  
 $p$ -adic number, 19  
 Pentagonal number, 151  
 Prime element, 17  
 Prime ideal, 1, 35  
 Primitive binary form, 204  
 Primitive character, 7, 9  
 Primitive root, 5  
 Primitive solution, 203  
 Principal genus, 230  
 Principal ideal, 1, 35  
 Principal ideal domain, 1  
 Product formula, 22, 50  
 Proper ideal, 214  
 Pure quaternion, 134

## Q

$q$ -reduced, 180  
 Quadratic Diophantine equation, 203  
 Quadratic field, 40  
 Quadratic form, 115  
 Quadratic nonresidue (modulo a prime), 6  
 Quadratic reciprocity law, 6  
 Quadratic residue (modulo a prime), 6  
 Quadratic residue symbol, 6  
 Quadratic space, 115  
 Quaternion algebra, 96

## R

Ramification index, 28  
 Ramified, 28, 30, 40, 57, 66, 142  
 Real archimedean prime, 66  
 Real character, 9  
 Real quadratic field, 40  
 Reciprocal, 89  
 Reduced norm, 93  
 Reduced trace, 93  
 Regular representation, 47  
 Regulator, 55

Relative discriminant, 59  
Representation, 92  
Residue class degree, 28  
Right order, 101  
Right regular representation, 92  
Right semisimple, 81

**S**

Scalar extension, 87  
Semisimple algebra, 84  
Simple algebra, 81  
Special orthogonal group, 116  
Spin group, 131  
Spinor norm, 131  
Split (quadratic space), 117  
Split Witt decomposition, 117  
 $s$ -reduced, 180  
Strong approximation, 177, 192  
Subalgebra, 79  
Symmetry, 128

**T**

Tensor product (of algebras), 86

Tensor product (of fields), 47  
Torsion-free (module), 11  
Totally isotropic, 115  
Totally ramified, 30  
Triangular number, 150  
Type 1, 181  
Type 2, 181

**U**

Unique factorization domain, 1  
Unramified, 28, 30, 40, 57, 66, 142

**V**

Valuation, 15  
Valuation ring, 17

**W**

Weak Witt decomposition, 117  
Witt decomposition, 117  
Witt's theorem, 117