# Integer-Valued Quadratic Forms and Quadratic Diophantine Equations

Goro Shimura

Received: September 12, 2006

Communicated by Don Blasius

Abstract. We investigate several topics on a quadratic form $\Phi$ over an algebraic number field including the following three: (A) an equation $\xi\Phi \cdot {}^t\xi = \Psi$ for another form $\Psi$ of a smaller size; (B) classification of $\Phi$ over the ring of algebraic integers; (C) ternary forms. In (A) we show that the "class" of such a $\xi$ determines a "class" in the orthogonal group of a form $\Theta$ such that $\Phi \approx \Psi \oplus \Theta$. Such was done in [S3] when $\Psi$ is a scalar. We will treat the case of nonscalar $\Psi$, and prove a class number formula and a mass formula, both of new types. In [S5] we classified all genera of **Z**-valued $\Phi$. We generalize this to the case of an arbitrary number field, which is topic (B). Topic (C) concerns some explicit forms of the formulas in (A) when $\Phi$ is of size 3 and $\Psi$ is a scalar.

2000 Mathematics Subject Classification: 11E12 (primary), 11D09, 11E41 (secondary)

## Introduction

A quadratic Diophantine equation in the title means an equation of the form $\xi\Phi \cdot {}^t\xi = \Psi$, where $\Phi$ and $\Psi$ are symmetric matrices of size $n$ and $m$, and $\xi$ is an $(m \times n)$-matrix. We assume that $n > m$, $\det(\Phi)\det(\Psi) \neq 0$, and all these matrices have entries in an algebraic number field $F$. The purpose of this paper is to present various new ideas and new results on such an equation. In the simplest case $m = 1$, we take a vector space $V$ of dimension $n$ over $F$, take also a nondegenerate symmetric $F$-bilinear form $\varphi : V \times V \to F$, and put $\varphi[x] = \varphi(x, x)$ for $x \in V$. Then the equation can be written $\varphi[x] = q$ with $q \in F$, $\neq 0$. In our recent book [S3] we formulated a new arithmetic framework of such an equation. In the present paper we attempt to extend the theory so that equations of the type $\xi\Phi \cdot {}^t\xi = \Psi$ can be treated along the same line of ideas, and give essential improvements on the results in [S3], as well as some new results.

Let us first recall the basic ideas of [S3] on this topic. Let $\mathfrak{g}$ denote the ring of algebraic integers in $F$. For a $\mathfrak{g}$-lattice $L$ in $V$ and a fractional ideal $\mathfrak{b}$ in $F$ we put

$$L[q, \mathfrak{b}] = \{\, x \in V \mid \varphi[x] = q,\ \varphi(x, L) = \mathfrak{b}\,\},$$
$$\Gamma(L) = \{\, \gamma \in SO^{\varphi}(V) \mid L\gamma = L\},$$
$$SO^{\varphi}(V) = \{\, \alpha \in SL(V, F) \mid \varphi[x\alpha] = \varphi[x] \quad \text{for every} \quad x \in V\}.$$

We call $L$ *integral* if $\varphi[x] \in \mathfrak{g}$ for every $x \in L$, and call an integral lattice *maximal* if it is the only integral lattice containing itself.

Given $h \in L[q, \mathfrak{b}]$, put $G = SO^{\varphi}(V)$, $W = (Fh)^{\perp}$, that is,

$$W = \{x \in V \mid \varphi(x, h) = 0\},$$

and $H = SO^{\varphi}(W)$, where we use $\varphi$ also for its restriction to $W$. Then in [S3] we proved, for a maximal $L$, that

(1a) *There is a bijection of* $\bigsqcup_{i\in I} \{L_i[q, \mathfrak{b}]/\Gamma(L_i)\}$ *onto* $H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)$, *and consequently*

(1b) $$\sum_{i\in I} \#\{L_i[q, \mathfrak{b}]/\Gamma(L_i)\} = \#\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)\}.$$

Here the subscript $\mathbf{A}$ means adelization, $C = \{x \in G_{\mathbf{A}} \mid Lx = L\}$, and $\{L_i\}_{i\in I}$ is a complete set of representatives for the classes in the genus of $L$ with respect to $G$. If $F = \mathbf{Q}$, $\mathfrak{g} = \mathfrak{b} = \mathbf{Z}$, $L = \mathbf{Z}^3$, and $\varphi$ is the sum of three squares, then the result is a reformulation of the result of Gauss that connects the number of primitive representations of an integer $q$ as sums of three squares with the class number of primitive binary forms of discriminant $-q$. This result can be formulated as a statement about $\#L[q, \mathbf{Z}]$ for such $\varphi$ and $L$ as Gauss did, and also as another statement concerning $\#\{L[q, \mathfrak{b}]/\Gamma(L)\}$ as in (1b), which Gauss did not present in a clear-cut form. Though Eisenstein and Minkowski investigated $\#L[q, \mathbf{Z}]$ when $\varphi$ is the sum of five squares, neither (1a) nor (1b) appears in their work. It seems that the idea of $L[q, \mathfrak{b}]/\Gamma(L)$ was taken up for the first time in [S3].

Now the major portion of this paper consists of several types of new results, which are the fruits of the ideas developed from (1a) and (1b). More explicitly, they can be described as follows.

I. The main theorems about $\#\{L[q, \mathfrak{b}]/\Gamma(L)\}$ in [S3], formula (1b) in particular, were proved under the following condition: if $n$ is odd, then $\det(\varphi)\mathfrak{g}$ is a square ideal. We will show that this condition is unnecessary.

II. The same types of problems about the equation $\xi\Phi\cdot{}^t\xi = \Psi$ for $m > 1$ were discussed in [S3] to some extent, but mainly restricted to the case $m = n-1$. In Theorem 2.2 we will prove more general results for an arbitrary $m$ formulated from a new viewpoint. Namely, we present the principle that the class of a solution $\xi$ determines a class in the orthogonal group in dimension $n - m$, which is complementary to that of $\Psi$. We then obtain generalizations of (1a) and (1b).

III. In [S3] we proved a certain mass formula which connects the "mass" of the set $L[q,\, \mathfrak{b}]$ with the mass of $H$ with respect to a subgroup of $H_{\mathbf{A}}$. If $F$ is totally real and $\varphi$ is totally definite, this can be given in the form

$$\sum_{i\in I} \#L_i[q,\, \mathfrak{b}]/\#\Gamma(L_i) = \sum_{\varepsilon\in E} [H \cap \varepsilon C\varepsilon^{-1} : 1]^{-1}, \tag{2}$$

where $E$ is a subset of $H_{\mathbf{A}}$ such that $H_{\mathbf{A}} = \bigsqcup_{\varepsilon\in E} H\varepsilon(H_{\mathbf{A}}\cap C)$. The right-hand side may be called the mass of $H$ with respect to $H_{\mathbf{A}} \cap C$. In Theorem 3.2 we will generalize this to the case of $\xi\Phi \cdot {}^t\xi = \Psi$ with $m \geq 1$ and definite or indefinite $\varphi$. Our formulas are different from any of the mass formulas of Siegel. See the remark at the end of Section 3 for more on this point.

IV. For $n = 3$, the right-hand side of (1b) can be written $[H_{\mathbf{A}} : H(H_{\mathbf{A}}\cap C)]$. In [S3] we gave an explicit formula for this index under the condition mentioned in I. In Theorem 5.7 of the present paper we prove the result without that condition. In general it is difficult to determine when $L[q,\, \mathfrak{b}] \neq \emptyset$. We will investigate this problem for a ternary form.

Every ternary space is isomorphic to a space of type $(B^\circ,\, \beta)$ obtained from a quaternion algebra $B$ over $F$ as follows. Denote by $\iota$ the main involution of $B$ and put $B^\circ = \{x \in B \,|\, x^\iota = -x\}$ and $\beta[x] = dxx^\iota$ for $x \in B^\circ$ with $d \in F^\times$. Then we will determine for a maximal $L$ exactly when $L[q,\, \mathbf{Z}] \neq \emptyset$ and give an explicit formula for $\#L[q,\, \mathbf{Z}]$ for $(B^\circ,\, \beta)$ over $\mathbf{Q}$ under the following conditions: (i) $B$ is definite and the genus of maximal lattices in $B^\circ$ consists of a single class; (ii) the discriminant $e$ of $B$ is a prime number; (iii) $d$ is one of the following four types: $d = 1$, $d = e$, $d$ is a prime $\neq e$, $d/e$ is a prime $\neq e$ (Theorems 6.6 and 6.7). In fact there are exactly 30 positive definite ternary forms over $\mathbf{Q}$ satisfying these three conditions, including of course the case of the sum of three squares. If we drop conditions (ii) and (iii), then there are exactly 64 ternary quadratic spaces over $\mathbf{Q}$ of type (i). Though our methods are applicable to those 64 spaces, we impose the last two conditions in order to avoid complicated analysis.

Indeed, though the results about $L[q,\, \mathbf{Z}]$ are not so complicated, they are not of the type one can easily guess, even under all three conditions. Also, to make transparent statements, it is better to consider an equation $\xi\cdot\lambda\Phi^{-1}\cdot{}^t\xi = s = \lambda q$ with a suitable $\lambda$, where $\Phi$ is the matrix representing $\varphi$ with respect to a $\mathbf{Z}$-basis of $L$. Take, for example, a ternary form $2x^2 + 3y^2 - yz + z^2$. Then we consider the equation $\xi \cdot \lambda\Phi^{-1} \cdot {}^t\xi = s$ for $s \in \mathbf{Z}$ with $\lambda = 22$, which can be written

$$11x^2 + 8(y^2 + yz + 3z^2) = s. \tag{3}$$

We can show that there is a bijection of $L[s/22,\, \mathbf{Z}]$ for this $\varphi$ onto the set of solutions $(x,\, y,\, z)$ of (3) such that $x\mathbf{Z} + y\mathbf{Z} + z\mathbf{Z} = \mathbf{Z}$. Moreover, such a solution exists if and only if $s = r^2m$ with a squarefree positive integer $m$ such that $m - 3 \in 8\mathbf{Z}$ and an odd positive integer $r$ such that $11|r$ if 11 remains prime in $K$, where $K = \mathbf{Q}(\sqrt{-m}\,)$. Thus $\#L[s/22,\, \mathbf{Z}]$ equals the number of such solutions of (3), and can be given as

$$\frac{2^{3-\mu_0-\mu_1}c}{w}\cdot r\prod_{p|r}\left\{1-\left(\frac{-m}{p}\right)\right\}. \tag{4}$$

Here $\mu_0 = 0$ if 2 is unramified in $K$ and $\mu_0 = 1$ otherwise; $\mu_1 = 0$ if $11|r$ or $11\nmid m$, and $\mu_1 = 1$ otherwise; $c$ is the class number of $K$; $w$ is the number of roots of unity in $K$; $\prod_{p|r}$ is the product over all prime factors $p$ of $r$. We can state similar results in the 30 cases mentioned above, and the same can be said, in principle, even in the 64 cases too, though we will not do so in the present paper. The condition that the class number is 1 is necessary, as the left-hand side of (2) has more than one term otherwise.

A much smaller portion of this paper, Section 4, is devoted to the classification of $\Phi$ over $\mathfrak{g}$. In [S5] we classified the genera of matrices that represent reduced **Z**-valued quadratic forms. Here a quadratic form is called *reduced* if it cannot be represented nontrivially over **Z** by another **Z**-valued quadratic form. This is different from Eisenstein's terminology for ternary forms. We will treat the same type of problem over the ring of algebraic integers of an arbitrary algebraic number field. For this we first have to define the genus of a symmetric matrix in a proper way, so that every genus of maximal lattices can be included. The formulation requires new concepts, and the classification has some interesting features. It should be noted that the obvious definition of a genus employed by Siegel applies only to a special case.

As a final remark we mention the article [S6], in which the reader will find a historical perspective of this topic that we do not include here. For example, [S6] contains a more detailed account of the work of Gauss and his predecessors, Lagrange and Legendre, and also comparisons of our formulas with Siegel's mass formulas. Therefore, [S6] is complementary to the present paper in that sense.

## 1. Basic symbols and a crucial local result

1.1. Throughout the paper we denote by $V$ a finite-dimensional vector space over a field $F$ and by $\varphi$ a nondegenerate $F$-bilinear symmetric form $V\times V \to F$; we put then $\varphi[x] = \varphi(x, x)$ for $x \in V$, $n = \dim(V)$, and

$$O^\varphi(V) = \{\alpha \in GL(V) \mid \varphi[x\alpha] = \varphi[x] \text{ for every } x \in V\},$$
$$SO^\varphi(V) = O^\varphi(V) \cap SL(V).$$

For every subspace $U$ of $V$ on which $\varphi$ is nondegenerate, we denote the restriction of $\varphi$ to $U$ also by $\varphi$, and use the symbols $O^\varphi(U)$ and $SO^\varphi(U)$. We denote by $A(V)$ the Clifford algebra of $(V, \varphi)$, and define the *canonical automorphism* $\alpha \mapsto \alpha'$ and the *canonical involution* $\alpha \mapsto \alpha^*$ of $A(V)$ by the condition $-x' = x^* = x$ for every $x \in V$. We then put

$$A^+(V) = A^+(V, \varphi) = \{\alpha \in A(V) \mid \alpha' = \alpha\},$$
$$G^+(V) = \{\alpha \in A^+(V)^\times \mid \alpha^{-1}V\alpha = V\}.$$

We can define a homomorphism $\nu : G^+(V) \to F^\times$ by $\nu(\alpha) = \alpha\alpha^*$ and also a surjective homomorphism $\tau : G^+(V) \to SO^\varphi(V)$ by $x\tau(\alpha) = \alpha^{-1}x\alpha$ for $\alpha \in G^+(V)$ and $x \in V$. Then $\mathrm{Ker}(\tau) = F^\times$. We denote by $\delta(\varphi)$ the coset of $F^\times/F^{\times 2}$ represented by $(-1)^{n(n-1)/2}\det(\varphi)$, where $F^{\times 2} = \{a^2 \mid a \in F^\times\}$.

We note here an easy fact [S3, Lemma 1.5 (ii)]:

$$\{k \in V \mid \varphi[k] = q\} = h \cdot SO^\varphi(V) \quad \text{if} \quad n > 1,\ h \in V, \text{and } \varphi[h] = q \in F^\times. \tag{1.1}$$

1.2. We now consider symbols $F$ and $\mathfrak{g}$ in the following two cases: (i) $F$ is an algebraic number field of finite degree and $\mathfrak{g}$ is its maximal order; (ii) $F$ and $\mathfrak{g}$ are the completions of those in Case (i) at a nonarchimedean prime. We call a field of type (i) a *global field,* and that of type (ii) a *local field.* In this paper, we employ the terms global and local fields only in these senses. If $F$ is a local field, we denote by $\mathfrak{p}$ the maximal ideal of $\mathfrak{g}$. In both local and global cases, by a $\mathfrak{g}$-*lattice* (or simply a *lattice*) in a finite-dimensional vector space $V$ over $F$, we mean a finitely generated $\mathfrak{g}$-module in $V$ that spans $V$ over $F$. When $F$ is a global field, we denote by $\mathbf{a}$ and $\mathbf{h}$ the sets of archimedean primes and nonarchimedean primes of $F$ respectively, and put $\mathbf{v} = \mathbf{a} \cup \mathbf{h}$. For each $v \in \mathbf{v}$ we denote by $F_v$ the $v$-completion of $F$. Given an algebraic group $G$ defined over $F$, we define an algebraic group $G_v$ over $F_v$ for each $v \in \mathbf{v}$ and the adelization $G_\mathbf{A}$ as usual, and view $G$ and $G_v$ as subgroups of $G_\mathbf{A}$. We then denote by $G_\mathbf{a}$ and $G_\mathbf{h}$ the archimedean and nonarchimedean factors of $G_\mathbf{A}$, respectively. In particular, $F_\mathbf{A}^\times$ is the idele group of $F$. For $v \in \mathbf{v}$ and $x \in G_\mathbf{A}$ we denote by $x_v$ the $v$-component of $x$.

Given a $\mathfrak{g}$-lattice $L$ in $V$ and another $\mathfrak{g}$-lattice $M$ contained in $L$ in both local and global cases, we can find a finite set $\{\mathfrak{a}\}$ of integral ideals $\mathfrak{a}$ such that $L/M$ as a $\mathfrak{g}$-module is isomorphic to $\bigoplus_{\mathfrak{a}\in\{\mathfrak{a}\}} \mathfrak{g}/\mathfrak{a}$. We then put $[L/M] = \prod_{\mathfrak{a}\in\{\mathfrak{a}\}} \mathfrak{a}$. For $x \in G_\mathbf{A}$ with $G$ acting on $V$ in the global case, we denote by $Lx$ the $\mathfrak{g}$-lattice in $V$ such that $(Lx)_v = L_v x_v$ for every $v \in \mathbf{h}$. We call the set of all such $Lx$ the $G$-*genus* of $L$, and call the set of $L\alpha$ for all $\alpha \in G$ the $G$-*class* of $L$.

In our later treatment we will often use a quaternion algebra over a local or global field $F$. Whenever we deal with such an algebra $B$, we always denote by $\iota$ the main involution of $B$; we then put

$$B^\circ = \{\, x \in B \mid x^\iota = -x \,\}, \tag{1.2}$$

$\mathrm{Tr}_{B/F}(x) = x + x^\iota$, and $N_{B/F}(x) = xx^\iota$ for $x \in B$.

Given $(V, \varphi)$ as in §1.1 over a local or global $F$, we call a $\mathfrak{g}$-lattice $L$ in $V$ *integral* if $\varphi[x] \in \mathfrak{g}$ for every $x \in L$, and call such an $L$ *maximal* if $L$ is the only integral lattice containing $L$. For an integral lattice $L$ in $V$ we denote by $A(L)$ the subring of $A(V)$ generated by $\mathfrak{g}$ and $L$, and put $A^+(L) = A(L) \cap A^+(V)$. For a $\mathfrak{g}$-lattice $\Lambda$ in $V$, an element $q$ in $F^\times$, and a fractional ideal $\mathfrak{b}$ in $F$, we put

$$\widetilde{\Lambda} = \{\, y \in V \mid 2\varphi(y, \Lambda) \subset \mathfrak{g} \,\}, \tag{1.3a}$$

$$\Lambda[q, \mathfrak{b}] = \{\, x \in V \mid \varphi[x] = q,\ \varphi(x, \Lambda) = \mathfrak{b} \,\}, \tag{1.3b}$$

(1.3c) $D(\Lambda) = \{\gamma \in O^{\varphi}(V) \mid \Lambda\gamma = \Lambda\}$, $C(\Lambda) = D(\Lambda) \cap SO^{\varphi}(V)$ ($F$ local).

THEOREM 1.3. *If $F$ is local, $L$ is a maximal lattice in $V$, and $n > 2$, then* $\#\{L[q, \mathfrak{b}]/C(L)\} \le 1$.

This was given in [S3, Theorem 10.5] under the condition that *if $n$ is odd, then $\delta(\varphi) \cap \mathfrak{g}^{\times} \neq \emptyset$*; see [S3, (8.1)]. Our theorem says that this condition is unnecesary. It is sufficient to prove the case $\mathfrak{b} = 2^{-1}\mathfrak{g}$, since $cL[q, \mathfrak{b}] = L(c^2q, c\mathfrak{b}]$ for every $c \in F^{\times}$. We devote §§1.4 and 1.5 to the proof. To avoid possible misunderstandings, we note that a result which looks similar to the above theorem was stated in [E1, Satz 10.4]. This result of Eichler has no relevance to our theory, as it does not consider the set $\varphi(x, L)$, an essential ingredient of our theorem. Besides, we have $\#\{L[q, \mathfrak{b}]/C(L)\} = 2$ for certain nonmaximal $L$; see [S7, Theorem 4.2 and (4.3)].

1.4. Given $(V, \varphi)$ over a local field $F$ and a maximal lattice $L$ in $V$, by Lemma 6.5 of [S3] we can find decompositions

$$V = Z \oplus U, \quad U = \sum_{i=1}^{r}(Fe_i + Ff_i), \quad \varphi(Z, U) = 0, \tag{1.4a}$$

$$L = M \oplus R, \quad R = \sum_{i=1}^{r}(\mathfrak{g}e_i + \mathfrak{g}f_i), \quad M = \{z \in Z \mid \varphi[z] \in \mathfrak{g}\}, \tag{1.4b}$$

$$2\varphi(e_i, f_j) = \delta_{ij}, \quad \varphi(e_i, e_j) = \varphi(f_i, f_j) = 0, \quad \varphi[z] \neq 0 \text{ for } 0 \neq z \in Z. \tag{1.4c}$$

We put $t = \dim(Z)$, and call it *the core dimension* of $(V, \varphi)$. To prove Theorem 1.3, we assume hereafter until the end of §1.6 that $n$ is odd and $\delta(\varphi)$ contains a prime element of $F$. Then $t$ is 1 or 3. We denote by $\pi$ any fixed prime element of $F$. We first note a few auxiliary facts:

(1.5) $\{x \in \mathfrak{g} \mid x - 1 \in 4\mathfrak{p}^m\} = \{a^2 \mid a - 1 \in 2\mathfrak{p}^m\}$ *if* $0 < m \in \mathbf{Z}$.

(1.6) *If $k \in U$ and $2\varphi(k, R) = \mathfrak{g}$, then $k\alpha = e_1 + sf_1$ with some $\alpha \in D(R)$ and $s \in \mathfrak{g}$; $\alpha$ can be taken from $C(R)$ if $r > 1$.*

(1.7) *If $h \in L[q, 2^{-1}\mathfrak{g}]$, $\notin Z$, then there exists an element $\alpha$ of $C(L)$ such that $h\alpha = \pi^m(e_1 + sf_1) + z$ with $0 \le m \in \mathbf{Z}$, $s \in \mathfrak{g}$, and $z \in M$.*

The first of these is [S3, Lemma 5.5 (i)]; (1.6) is proven in [S3, §10.7, (A1), (A2)]. Notice that the proof there is valid even when $\varphi[k] = 0$. Now let $h = k + w \in L[q, 2^{-1}\mathfrak{g}]$ with $k \in U$ and $w \in Z$. If $h \notin Z$, then $k \neq 0$, and we can put $2\varphi(k, R) = \mathfrak{p}^m$ with $0 \le m \in \mathbf{Z}$. By (1.6), there exists an element $\alpha_0 \in D(R)$ such that $\pi^{-m}k\alpha_0 = e_1 + sf_1$ with $s \in \mathfrak{g}$. Since $D(M)$ contains an element of determinant $-1$, we can extend $\alpha_0$ to an element $\alpha$ of $C(L)$ such that $M\alpha = M$. This proves (1.7).

1.5. By virtue of (1.7), it is sufficient to prove Theorem 1.3 when $r \le 1$. If $r = 0$, then $L = M$ and $SO^{\varphi}(V) = C(L)$ by [S3, Lemma 6.4]. Therefore, if $n = t = 3$ and $\varphi[z] = \varphi[w]$ with $z, w \in V$, then by (1.1), $z = w\alpha$ with $\alpha \in C(L)$, which gives the desired fact. For this reason we hereafter assume that

$r = 1$, and write $e$ and $f$ for $e_1$ and $f_1$. We represent the elements of $O^\varphi(V)$ by $(n \times n)$-matrices with respect to $\{e,\, g_1,,\, \dots,\, g_t,\, f\}$, where $\{g_1,,\, \dots,\, g_t\}$ is a $\mathfrak{g}$-basis of $M$.

(A) Case $t = 1$. In this case $M = \mathfrak{g}g$ with an element $g$ such that $\varphi[g]$ is a prime element of $F$. Thus we can take $\varphi[g]$ as $\pi$.

(a1) Suppose $L[q,\, 2^{-1}\mathfrak{g}] \cap Z \neq \emptyset$; let $w \in L[q,\, 2^{-1}\mathfrak{g}] \cap Z$ and $h \in L[q,\, 2^{-1}\mathfrak{g}]$. Then we can put $w = [0 \;\; c \;\; 0]$ with $c \in F$ such that $2c\mathfrak{p} = \mathfrak{g}$. By (1.1), $h = w\alpha$ with $\alpha \in SO^\varphi(V)$. Now $SO^\varphi(V) = PC(L)$ with the subgroup $P$ of $SO^\varphi(V)$ consisting of the upper triangular elements; see [S3, Theorem 6.13 (ii)]. Put $\alpha = \beta\gamma$ with $\beta \in P$ and $\gamma \in C(L)$. The second row of $\beta$ is of the form $[0 \;\; 1 \;\; j]$ with $j \in F$. Thus $h\gamma^{-1} = w\beta = [0 \;\; c \;\; cj]$, and so $cj \in \mathfrak{g}$. Since $2c\mathfrak{p} = \mathfrak{g}$, we can find an element $p$ of $\mathfrak{g}$ such that $2c\pi p = cj$. Take the matrix

$$\eta = \begin{bmatrix} 1 & -p & -\pi p^2 \\ 0 & 1 & 2\pi p \\ 0 & 0 & 1 \end{bmatrix}. \tag{1.8}$$

Then $\eta \in C(L)$ and $w\eta = w\beta = h\gamma^{-1}$, which gives the desired fact.

(a2) Thus we assume that $L[q,\, 2^{-1}\mathfrak{g}] \cap Z = \emptyset$. Let $h \in L[q,\, 2^{-1}\mathfrak{g}]$. By (1.7) we can put $h = \pi^m(e + sf) + cg$ with $0 \leq m \in \mathbf{Z}$ and $s, c \in \mathfrak{g}$. Then $q = \pi^{2m}s + \pi c^2$ and $\mathfrak{p}^m + 2c\mathfrak{p} = \mathfrak{g}$. Put $d = 2\pi c$. Suppose $d \in \mathfrak{g}^\times$. Then by (1.5), we can put $d^2 + 4\pi^{2m+1}s = d_1^2$ with $d_1 \in \mathfrak{g}^\times$. We easily see that $(2\pi)^{-1}d_1 g \in L[q,\, 2^{-1}\mathfrak{g}]$, a contradiction, as $g \in Z$. Thus $d \in \mathfrak{p}$, so that $m = 0$ and $h = e + sf + (2\pi)^{-1}dg$, and $q = s + (4\pi)^{-1}d^2$. Suppose we have another element $h_1 = e + s_1 f + (2\pi)^{-1}d_1 g$ with $s_1 \in \mathfrak{g}$ and $d_1 \in \mathfrak{p}$ such that $\varphi[h_1] = q$. Then $d_1^2 - d^2 = 4\pi(s - s_1) \in 4\mathfrak{p}$, and so $d_1 - d \in 2\mathfrak{p}$ or $d_1 + d \in 2\mathfrak{p}$. Since $-2d \in 2\mathfrak{p}$, we have $d_1 - d \in 2\mathfrak{p}$ in both cases. Let $\alpha$ be the element of (1.8) with $p = (d_1 - d)/(2\pi)$. Then $\alpha \in C(L)$ and $h = h_1\alpha \in h_1 C(L)$. This completes the proof when $t = 1$.

(B) Case $t = 3$. As shown in [S3, §§7.3 and 7.7 (III)], there is a division quaternion algebra $B$ over $F$ with which we can put $Z = B^\circ$ and $2\varphi(x,\, y) = d\mathrm{Tr}_{B/F}(xy^\iota)$ for $x, y \in Z$, where $d$ is an element of $F^\times$ that represents the determinant of the restriction of $\varphi$ to $Z$. Thus we can take a prime element $\pi$ of $F$ as $d$; then $M = \{x \in Z \,|\, \pi x x^\iota \in \mathfrak{g}\}$. Let $K$ be an unramified quadratic extension of $F$, $\mathfrak{r}$ the maximal order of $K$, and $\rho$ the generator of $\mathrm{Gal}(K/F)$. We can put $B = K + K\eta$ with an element $\eta$ such that $\eta^2 = \pi$ and $x\eta = \eta x^\rho$ for every $x \in K$. Take $u \in \mathfrak{r}$ so that $\mathfrak{r} = \mathfrak{g}[u]$ and put $\sigma = u - u^\rho$. Then $M = \mathfrak{g}\sigma + \mathfrak{r}\eta^{-1}$ and $\widetilde{M} = (2\mathfrak{p})^{-1}\sigma + \mathfrak{r}\eta^{-1}$. Since $r = 1$, $\varphi$ is represented by a matrix

$$\begin{bmatrix} 0 & 0 & 2^{-1} \\ 0 & \zeta & 0 \\ 2^{-1} & 0 & 0 \end{bmatrix},$$

where $\zeta$ is an element of $\mathfrak{g}_3^3$ that represents the restriction of $\varphi$ to $Z$. Define $\lambda = (\lambda_{ij}) \in \mathfrak{g}_3^3$ by $\lambda_{ii} = \zeta_{ii}$, $\lambda_{ij} = 2\zeta_{ij}$ if $i < j$ and $\lambda_{ij} = 0$ if $i > j$. Then $\lambda + {}^t\lambda = 2\zeta$. Let $P$ be the subgroup of $SO^\varphi(V)$ consisting of the elements that send $Ff$ onto itself, Then $SO^{\varphi}(V) = PC(L)$; see [S3, Theorem 6.13 (ii)].

(b1) Suppose $L[q,\, 2^{-1}\mathfrak{g}] \cap Z \neq \emptyset$. Let $h \in L[q,\, 2^{-1}\mathfrak{g}]$ and $w \in L[q,\, 2^{-1}\mathfrak{g}] \cap Z$. Identify $w$ with a row vector $w = [0 \quad y \quad 0]$, where $y = (y_i)_{i=1}^3$ with $y_i \in \mathfrak{g}$. By (1.1), $h = w\alpha$ with $\alpha \in SO^{\varphi}(V)$. Put $\alpha = \beta\gamma$ with $\beta \in P$ and $\gamma \in C(L)$. The middle three rows of $\beta$ can be written in the form $[0 \quad \varepsilon \quad j]$ with $\varepsilon \in SO^{\varphi}(Z)$ and a column vector $j$. Replacing $\gamma$ by $\mathrm{diag}[1,\, \varepsilon,\, 1]\gamma$, we may assume that $\varepsilon = 1$. Then $h\gamma^{-1} = w\beta = [0 \quad y \quad yj]$ and $yj \in \mathfrak{g}$. Since $w \in L[q,\, 2^{-1}\mathfrak{g}]$, we see that $2y\zeta$ is primitive, and so we can find $p \in \mathfrak{g}_3^1$ such that $-2y\zeta \cdot {}^tp = yj$. Let

$$\psi = \begin{bmatrix} 1 & p & -p\lambda \cdot {}^tp \\ 0 & 1 & -2\zeta \cdot {}^tp \\ 0 & 0 & 1 \end{bmatrix}. \tag{1.9}$$

Then $\psi \in C(L)$ and $w\psi = w\beta = h\gamma^{-1}$, and so $h \in wC(L)$ as expected.

(b2) Let $h \in L[q,\, 2^{-1}\mathfrak{g}], \notin Z$. By (1.7) we may assume that $h = \pi^m(e + sf) + z$ with $0 \leq m \in \mathbf{Z}$, $s \in \mathfrak{g}$, and $z \in Z$. Put $z = (2\pi)^{-1}c\sigma + x\eta^{-1}$ with $c \in F$ and $x \in K$. Then $\mathfrak{g} = \mathfrak{p}^m + c\mathfrak{g} + \mathrm{Tr}_{K/F}(x\mathfrak{r})$, $q = \pi^{2m}s - \pi z^2$, and $\pi z^2 = (4\pi)^{-1}c^2\sigma^2 + xx^{\rho}$. Suppose $m > 0$; then $c \in \mathfrak{g}^{\times}$ or $x \in \mathfrak{r}^{\times}$. If $c \in \mathfrak{g}^{\times}$, then by (1.5) we can put $c^2 - 4\pi^{2m+1}\sigma^{-2}s = b^2$ with $b \in \mathfrak{g}^{\times}$. Put $w = (2\pi)^{-1}b\sigma + x\eta^{-1}$. Then we see that $w \in L[q,\, 2^{-1}\mathfrak{g}] \cap Z$. Next suppose $x \in \mathfrak{r}^{\times}$; then $xx^{\rho} - \pi^{2m}s \in \mathfrak{g}^{\times}$. Since $N_{K/F}(\mathfrak{r}^{\times}) = \mathfrak{g}^{\times}$, we can find $x_1 \in \mathfrak{r}^{\times}$ such that $x_1x_1^{\rho} = xx^{\rho} - \pi^{2m}s$. Put $x = (2\pi)^{-1}c\sigma + x_1\eta^{-1}$. Then $x \in L[q,\, 2^{-1}\mathfrak{g}] \cap Z$. Therefore, if $m > 0$, then the problem can be reduced to case (b1), which has been settled.

(b3) Thus if $L[q,\, 2^{-1}\mathfrak{g}] \cap Z = \emptyset$ and $h \in L[q,\, 2^{-1}\mathfrak{g}]$, then we may assume that $h = e + sf + z$ with $s \in \mathfrak{g}$ and $z \in Z$. Take another element $h_1 = e + s_1f + z_1 \in L[q,\, 2^{-1}\mathfrak{g}]$ with $s_1 \in \mathfrak{g}$ and $z_1 \in Z$. We have $z = (2\pi)^{-1}c\sigma + x\eta^{-1}$ and $z_1 = (2\pi)^{-1}c_1\sigma + x_1\eta^{-1}$ with $c,\, c_1 \in \mathfrak{g}$ and $x,\, x_1 \in \mathfrak{r}$. Since $s - \pi z^2 = s_1 - \pi z_1^2$, we have $(4\pi)^{-1}(c^2 - c_1^2) \in \mathfrak{g}$, so that $c^2 - c_1^2 \in 4\mathfrak{p}$. Then $c - c_1 \in 2\mathfrak{p}$ or $c + c_1 \in 2\mathfrak{p}$. Now the map $x\sigma + y\eta^{-1} \mapsto -x\sigma + y^{\rho}\eta^{-1}$ is an element of $C(M)$. Therefore, replacing $z_1$ by its image under this map if necessary, we may assume that $c - c_1 \in 2\mathfrak{p}$, which implies that $z - z_1 \in M$. Define $\psi$ by (1.9) by taking $p$ to be the vector that represents $z - z_1$. Then $h_1\psi = h$, which gives the desired fact.

1.6. We can now remove condition (8.1) from [S3, Lemma 10.8], which concerns the case where $t = 1$ and $r > 0$. To be precise, that lemma can be restated, without condition (8.1), as follows:

*Let $L = \mathfrak{g}e_1 + \mathfrak{g}f_1 + \mathfrak{g}g$ with $g$ such that $\mathfrak{p} \subset \varphi[g]\mathfrak{g} \subset \mathfrak{g}$, and let $h \in L[q,\, 2^{-1}\mathfrak{g}]$ with $q \in F^{\times}$. Then there exists an element $\gamma$ of $C(L)$ such that $h\gamma = cg$ with $c$ satisfying $2c\varphi[g]\mathfrak{g} = \mathfrak{g}$ or $h\gamma = ae_1 + f_1 + cg$ with $a \in \mathfrak{g}$ and $c \in 2^{-1}\mathfrak{g}$.*

This follows from the discussions of (a1) and (a2) combined with (1.7).

1.7. Still asssuming $F$ to be local, take the symbols as in (1.4a, b, c) with even or odd $n$, put $C = C(L)$ for simplicity, and define subgroups $T$ and $J$ of $G^+(V)$ by

$$T = \{\, \alpha \in G^+(V) \,|\, \tau(\alpha) \in C \,\}, \tag{1.10}$$

$$J = \{\, \gamma \in T \,|\, \nu(\gamma) \in \mathfrak{g}^\times \,\}. \tag{1.11}$$

In [S3], Proposition 8.8, Theorems 8.6, and 8.9 we discussed the structure of $A(L)$, $A^+(L)$, $\nu(J)$, and the connection of $\tau(J)$ with $C$ under the condition that $\delta(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$ if $n$ is odd. Let us now prove the results in the cases in which the condition is not satisfied.

Theorem 1.8. *Suppose $F$ is local, $1 < n - 1 \in 2\mathbf{Z}$, and $\delta(\varphi)$ contains a prime element. Then the following assertions hold.*

(i) *If $t = 1$, then there exist an order $\mathfrak{O}$ in $M_2(F)$ of discriminant $\mathfrak{p}$ (see §5.1 for the definition) and an isomorphism $\theta$ of $A^+(V)$ onto $M_s\big(M_2(F)\big)$ that maps $A^+(L)$ onto $M_s(\mathfrak{O})$, where $s = 2^{r-1}$.*

(ii) *If $t = 3$, then there exist a division quaternion algebra $B$ over $F$ and an isomorphism $\xi : B^\circ \to Z$ such that $\varphi[x\xi] = dxx^\iota$ for every $x \in B^\circ$ with a prime element $d$ of $F^\times$ independent of $x$, where $B^\circ$ is defined by (1.2). Moreover there exists an isomorphism $\theta$ of $A^+(V)$ onto $M_s(B)$ that maps $A^+(L)$ onto $M_s(\mathfrak{O})$, where $s = 2^r$ and $\mathfrak{O}$ is the unique maximal order in $B$.*

(iii) *In both cases $t = 1$ and $t = 3$ we have $\nu(J) = \mathfrak{g}^\times$, $C = \tau(T)$, $[C : \tau(J)] = 2$, and $T = F^\times(J \cup J\eta)$ with an element $\eta$ such that $\eta \notin F^\times J$, $\eta^2 \in F^\times$, $J\eta = \eta J$, and $\nu(\eta)\mathfrak{g} = \mathfrak{p}$.*

This will be proved after the proof of Lemma 5.4.

Theorem 1.9. *In the setting of Theorem 1.3 with even or odd $n > 2$, let $t$ be the core dimension of $(V, \varphi)$ and let $\sigma : SO^\varphi(V) \to F^\times/F^{\times 2}$ be the spinor norm map of* [S3, (3.7)]. Then $\sigma(C) = \mathfrak{g}^\times F^{\times 2}$ in the following three cases: (i) $t = 0$; (ii) $t = 1$ *and* $\delta(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$; (iii) $t = 2$ *and* $\widetilde{L} = L$. *We have $\sigma(C) = F^\times$ in all the remaining cases.*

*Proof.* That $\sigma(C) = \mathfrak{g}^\times F^{\times 2}$ in the three cases specified above is shown by Proposition 8.8 (iii) and Theorem 8.9 (i) of [S3]. Therefore we assume that those cases do not apply. If $\delta(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$ or $n$ is even, then Theorem 8.9 (ii) of [S3] shows that $\sigma(C) = F^\times$. If $n$ is odd and $\delta(\varphi) \cap \mathfrak{g}^\times = \emptyset$, then from (iii) of Theorem 1.8 we obtain $\sigma(C) = \nu(T) = F^\times$, which completes the proof.

## 2. Global quadratic Diophantine equations

2.1. Let us now turn to the global case. The main theorems of [S3, Sections 11 through 13] were given under a condition stated in [S3, (9.2)]: *if $n$ is odd, then $\delta(\varphi)$, at every nonarchimedean prime, contains a local unit.* By virtue of Theorem 1.3 we can now remove this condition from [S3, Theorem 11.6] and some others, which we will indicate in Remark 2.4 (3), (5), (6), and (7).

Throughout this section we assume that $F$ is an algebraic number field. Given a quadratic space $(V, \varphi)$ over $F$, we can define, for each $v \in \mathbf{v}$, the $v$-localization $(V_v, \varphi_v)$ of $(V, \varphi)$ as a quadratic space over $F_v$ by putting $V_v = V \otimes_F F_v$ and extending $\varphi$ to an $F_v$-valued quadratic form $\varphi_v$ on $V_v$ in a natural way.

In [S3, Section 13], we treated the equation $\varphi[h] = q$ not only for a scalar $q$, but also for a symmetric matrix $q$ of size $n-1$. We now consider a more general case by taking a new approach. Given ${}^t q = q \in GL_m(F)$ and ${}^t\varphi = \varphi \in GL_n(F)$, we consider the solutions $h \in F_n^m$ of the equation $h\varphi \cdot {}^t h = q$. Here and throughout this and the next sections we assume that $n > 2$ and $n > m > 0$. More intrinsically, take $(V, \varphi)$ as before and take also $(X, q)$ with a nondegenerate quadratic form $q$ on a vector space $X$ over $F$ of dimension $m$. We put

$$\mathscr{V} = \mathrm{Hom}(X, V), \tag{2.1}$$

and consider $h \in \mathscr{V}$ such that $\varphi[xh] = q[x]$ for every $x \in X$. Since $q$ is nondegenerate, $h$ must be injective. To simplify our notation, for every $k \in \mathscr{V}$ we denote by $\varphi[k]$ the quadratic form on $X$ defined by $\varphi[k][x] = \varphi[xk]$ for every $x \in X$. Then our problem concerns the solutions $h \in \mathscr{V}$ of the equation $\varphi[h] = q$ for a fixed $q$. If $m = 1$ and $X = F$, then $q \in F^\times$, and an element $h$ of $V$ defines an element of $\mathscr{V}$ that sends $c$ to $ch$ for $c \in F$, and $\mathscr{V}$ consists of all such maps. Thus we can put $\mathscr{V} = V$ if $m = 1$ and the problem about $\varphi[h] = q$ with $q \in F^\times$ is the one-dimensional special case. For $m \geq 1$, if $h \in \mathscr{V}$ and $\det(\varphi[h]) \neq 0$, then

$$\bigl\{k \in \mathscr{V} \bigm| \varphi[k] = \varphi[h]\bigr\} = h \cdot SO^\varphi(V). \tag{2.2}$$

This is a generalization of (1.1) and follows easily from the Witt theorem; see [S3, Lemma 1.5 (i)].

For a fixed $h \in \mathscr{V}$ such that $\det\bigl(\varphi[h]\bigr) \neq 0$, put $W = (Xh)^\perp$, $G = SO^\varphi(V)$, and $H = SO^\varphi(W)$. We identify $H$ with the subgroup of $G$ consisting of the elements that are the identity map on $Xh$; thus

$$H = \bigl\{\alpha \in G \bigm| h\alpha = h\bigr\}. \tag{2.3}$$

For $\xi \in G_{\mathbf{A}}$ the symbol $h\xi$ is meaningful as an element of $\mathscr{V}_{\mathbf{A}}$, and so for a subset $\varXi$ of $G_{\mathbf{A}}$ the symbol $h\varXi$ is meaningful as a subset of $\mathscr{V}_{\mathbf{A}}$.

Theorem 2.2. *Let $D = D_0 G_{\mathbf{a}}$ with an open compact subgroup $D_0$ of $G_{\mathbf{h}}$. Then the following assertions hold.*

(i) *For $y \in G_{\mathbf{A}}$ we have $H_{\mathbf{A}} \cap GyD \neq \emptyset$ if and only if $\mathscr{V} \cap hDy^{-1} \neq \emptyset$.*

(ii) *Fixing $y \in G_{\mathbf{A}}$, for every $\varepsilon \in H_{\mathbf{A}} \cap GyD$ take $\alpha \in G$ so that $\varepsilon \in \alpha yD$. Then the map $\varepsilon \mapsto h\alpha$ gives a bijection of $H\backslash(H_{\mathbf{A}} \cap GyD)/(H_{\mathbf{A}} \cap D)$ onto $(\mathscr{V} \cap hDy^{-1})/\varGamma^y$, where $\varGamma^y = G \cap yDy^{-1}$.*

(iii) *Take $Y \subset G_{\mathbf{A}}$ so that $G_{\mathbf{A}} = \bigsqcup_{y \in Y} GyD$. Then*

$$\#\bigl\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)\bigr\} = \sum_{y \in Y} \#\bigl\{(\mathscr{V} \cap hDy^{-1})/\varGamma^y\bigr\}. \tag{2.4}$$

(iv) *In particular, suppose $m = 1$ and $n > 2$. With a fixed maximal lattice $L$ in $V$ put $C = \bigl\{\xi \in G_{\mathbf{A}} \bigm| L\xi = L\bigr\}$, $q = \varphi[h]$, and $\mathfrak{b} = \varphi(h, L)$. Then*

$$V \cap hCy^{-1} = (Ly^{-1})[q, \mathfrak{b}] \quad \textit{for every} \quad y \in G_{\mathbf{A}}. \tag{2.5}$$

*Note:* Since $H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)$ is a finite set, from (ii) we see that $(\mathscr{V} \cap hDy^{-1})/\varGamma^y$ is a finite set.

*Proof.* Let $y$, $\varepsilon$, and $\alpha$ be as in (ii); then clearly $h\alpha \in \mathscr{V} \cap hDy^{-1}$. If $\eta\varepsilon\zeta \in \beta yD$ with $\eta \in H$, $\zeta \in H_{\mathbf{A}} \cap D$, and $\beta \in G$, then $\beta^{-1}\eta\alpha \in G \cap yDy^{-1} = \Gamma^y$, and hence $h\alpha = h\eta\alpha \in h\beta\Gamma^y$. Thus our map is well defined. Next let $k \in \mathscr{V} \cap hDy^{-1}$. Then $k = h\delta y^{-1}$ with $\delta \in D$, and moreover, by (2.2), $k = h\xi$ with $\xi \in G$. Then $h = h\xi y\delta^{-1}$, so that $\xi y\delta^{-1} \in H_{\mathbf{A}}$ by (2.3). Thus $\xi y\delta^{-1} \in H_{\mathbf{A}} \cap GyD$. This shows that $k$ is the image of an element of $H_{\mathbf{A}} \cap GyD$. To prove that the map is injective, suppose $\varepsilon \in \alpha yD \cap H_{\mathbf{A}}$ and $\delta \in \beta yD \cap H_{\mathbf{A}}$ 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 $\sigma \in yDy^{-1}$, we have $\beta yD = \beta\sigma yD = \omega\alpha yD$, and hence $\delta \in \beta yD \cap H_{\mathbf{A}} = \omega\alpha yD \cap H_{\mathbf{A}} = \omega(\alpha yD \cap H_{\mathbf{A}}) = \omega(\varepsilon D \cap H_{\mathbf{A}}) = \omega\varepsilon(D \cap H_{\mathbf{A}}) \subset H\varepsilon(D \cap H_{\mathbf{A}})$. This proves the injectivity, and completes the proof of (ii). At the same time we obtain (i).

Now $H_{\mathbf{A}} = \bigsqcup_{y \in Y}(H_{\mathbf{A}} \cap GyD)$, and so (iii) follows immediately from (ii). As for (iv), clearly $V \cap hC \subset L[q, \mathfrak{b}]$. Conversely, every element of $L[q, \mathfrak{b}]$ belongs to $hC$ by virtue of Theorem 1.3. Thus

$$V \cap hC = L[q, \mathfrak{b}]. \tag{2.6}$$

Let $k \in V \cap hCy^{-1}$ with $y \in G_{\mathbf{A}}$; put $M = Ly^{-1}$. Then $\varphi[k] = q$, $\varphi\bigl(k, M\bigr) = \varphi(h, L) = \mathfrak{b}$, and $kyCy^{-1} = hCy^{-1}$. Taking $k$, $M$, and $yCy^{-1}$ in place of $h$, $L$ and $C$ in (2.6), we obtain $V \cap hCy^{-1} = V \cap kyCy^{-1} = M[q, \mathfrak{b}] = (Ly^{-1})[q, \mathfrak{b}]$. This proves (2.5) 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 1.3, $\ell y \in hC$, 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 hence (2.5) holds for every $y \in G_{\mathbf{A}}$. This completes the proof.

If $k$ and $\ell$ are two elements of $\mathscr{V} \cap hDy^{-1}$, then $k = \ell x_v$ with $x_v \in y_v D_v y_v^{-1}$ for every $v \in \mathbf{h}$. Therefore we are tempted to say that $k$ *and* $\ell$ *belong to the same genus.* Then each orbit of $(\mathscr{V} \cap hDy^{-1})/\Gamma^y$ may be called a *class.* Thus (ii) of Theorem 2.2 connects such classes of elements of $\mathscr{V}$ with the classes of $H$ with respect to $H_{\mathbf{A}} \cap D$.

Combining (2.4) with (2.5), we obtain, in the setting of (iv),

$$\#\bigl\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)\bigr\} = \sum_{y \in Y} \#\bigl\{(Ly^{-1})[q, \mathfrak{b}]/\Gamma^y\bigr\}. \tag{2.7}$$

This was stated in [S3, (11.7)] under the condition mentioned at the beginning of this section, which we can now remove.

The above theorem concerns $SO^{\varphi}\bigl((Xh)^{\perp}\bigr)$. Let us now show that we can formulate a result with respect to $SO^q(X)$ instead, when $m = n - 1$. The notation being as above, put $Y = Xh$ and $J = SO^{\varphi}(Y)$. We identify $J$ with $\bigl\{\alpha \in G \,\big|\, \alpha = \text{id. on } W\bigr\}$. For every $\delta \in J$ there is a unique element $\delta'$ of $SO^q(X)$ such that $\delta' h = h\delta$, and $\delta \mapsto \delta'$ gives an isomorphism of $J$ onto $SO^q(X)$. In this section we employ the symbol $\delta'$ always in this sense. We note a simple fact:

(2.8) *If* $m = n - 1$ *and* $h\xi = h\eta$ *for* $\xi, \eta \in G_{\mathbf{A}}$, *then* $\xi = \eta$.

Indeed, for each $v \in \mathbf{v}$ we have $h\xi_v\eta_v^{-1} = h$, and so $\xi_v\eta_v^{-1}$ is the identity map on $X_v h$. Since $m = n-1$, it must be the identity map on the whole $V_v$. Thus $\xi_v\eta_v^{-1} = 1$ for every $v \in \mathbf{v}$, which proves (2.8).

Theorem 2.3. *Let $D = D_0 G_\mathbf{a}$ as in Theorem 2.2 and let $E = E_0 J_\mathbf{a}$ with an open compact subgroup $E_0$ of $J_\mathbf{h}$. Suppose $m = n-1$ and $J_\mathbf{A} \cap D \subset E$. Then for every $z \in J_\mathbf{A}$ and $y \in G_\mathbf{A}$ there exists a bijection*

$$J\backslash(JzE \cap GyD)/(J_\mathbf{A} \cap D) \longrightarrow \Delta'\backslash(\mathscr{V} \cap hzEDy^{-1})/\Gamma, \tag{2.9}$$

*where $\Gamma = yDy^{-1} \cap G$ and $\Delta' = \{\delta' \mid \delta \in \Delta\}$, $\Delta = zEz^{-1} \cap J$.*

*Proof.* Given $\sigma \in JzE \cap GyD$, take $\alpha \in G$ and $\beta \in J$ so that $\sigma \in \beta zE \cap \alpha yD$, and put $k = h\beta^{-1}\alpha$. Then $k \in \mathscr{V} \cap hzEDy^{-1}$. If $\sigma \in \beta_1 zE \cap \alpha_1 yD$ with $\alpha_1 \in G$ and $\beta_1 \in J$, then $\beta_1^{-1}\beta \in \Delta$ and $\alpha_1^{-1}\alpha \in \Gamma$, and so $\sigma \to h\beta^{-1}\alpha$ is a well-defined map as in (2.9). To show that it is surjective, take $k \in \mathscr{V} \cap hzEDy^{-1}$; then $\varphi[k] = q$, and so $k = h\alpha$ with $\alpha \in G$ by (2.2). We have also $k = hz\varepsilon\zeta y^{-1}$ with $\varepsilon \in E$ and $\zeta \in D$. By (2.8), $z\varepsilon\zeta y^{-1} = \alpha$, and so $z\varepsilon = \alpha y\zeta^{-1} \in zE \cap \alpha yD$. This shows that $k$ is the image of $z\varepsilon$, which proves the surjectivity. To prove the injectivity, let $\sigma \in \beta zE \cap \alpha yD$ and $\sigma_1 \in \beta_1 zE \cap \alpha_1 yD$ with $\alpha, \alpha_1 \in G$ and $\beta, \beta_1 \in E$. Suppose $h\beta_1^{-1}\alpha_1 = \delta' h\beta^{-1}\alpha\gamma$ with $\delta \in \Delta$ and $\gamma \in \Gamma$. Then $\beta_1^{-1}\alpha_1 = \delta\beta^{-1}\alpha\gamma$ by (2.8). Put $\lambda = \alpha\gamma\alpha_1^{-1}$. Then $\lambda = \beta\delta^{-1}\beta_1^{-1} \in J$. Since $\gamma \in yDy^{-1}$, we have $\sigma \in \alpha yD = \alpha\gamma yD = \lambda\alpha_1 yD = \lambda\sigma_1 D \subset J\sigma_1 D$. Also, since $\sigma, \sigma_1 \in J_\mathbf{A}$, we have $\sigma \in J\sigma_1(J_\mathbf{A} \cap D)$. This proves the injectivity, and completes the proof.

Remark 2.4. (1) We can take $E = J_\mathbf{A} \cap D$ in the above theorem. Then (2.9) takes a simpler form

$$J\backslash(JzE \cap GyD)/E \longrightarrow \Delta'\backslash(\mathscr{V} \cap hzDy^{-1})/\Gamma, \tag{2.10}$$

(2) Let $G_\mathbf{A} = \bigsqcup_{y \in Y} GyD$ as in Theorem 2.2 and let $J_\mathbf{A} = \bigsqcup_{z \in Z} JzE$ with a finite subset $Z$ of $J_\mathbf{A}$. Then $J_\mathbf{A} = \bigsqcup_{z,y}(JzE \cap GyD)$. For each $(z, y)$ such that $JzE \cap GyD \neq \emptyset$ pick $\xi \in JzE \cap GyD$ and denote by $\Xi$ the set of all such $\xi$. Then $J_\mathbf{A} = \bigsqcup_{\xi \in \Xi}(J\xi E \cap G\xi D)$, and we obtain

$$\#\{J\backslash J_\mathbf{A}/(J_\mathbf{A} \cap D)\} = \sum_{\xi \in \Xi} \#\{\Delta'_\xi\backslash(\mathscr{V} \cap h\xi ED\xi^{-1})/\Gamma^\xi\}, \tag{2.11}$$

where $\Gamma^\xi = \xi D\xi^{-1} \cap G$ and $\Delta'_\xi = \{\delta' \mid \delta \in J \cap \xi E\xi^{-1}\}$.

(3) For $\ell \in V$ let us denote by $\varphi(h, \ell)$ the element of $\mathrm{Hom}(X, F)$ defined by $x\varphi(h, \ell) = \varphi(xh, \ell)$ for $x \in X$; then for a subset $S$ of $V$ let us put $\varphi(h, S) = \{\varphi(h, s) \mid s \in S\}$. Now, fixing a maximal lattice $L$ in $V$, put $\Lambda = \widetilde{L}$, $\mathfrak{B} = \varphi(h, \Lambda)$, and $E = \{\varepsilon \in J_\mathbf{A} \mid \varepsilon'\mathfrak{B} = \mathfrak{B}\}$. Since $\mathfrak{B}$ is a $\mathfrak{g}$-lattice in $\mathrm{Hom}(X, F)$, we see that $E$ is a subgroup of $J_\mathbf{A}$ of the type considered in Theorem 2.3. Then we can prove

$$\mathscr{V} \cap hzEDy^{-1} = \{k \in \mathscr{V} \mid \varphi[k] = q,\ \varphi(k, \Lambda y^{-1}) = z'\mathfrak{B}\}. \tag{2.12}$$

This is similar to (2.5), and proved in the proof of [S3, Theorem 13.10]. It should be noted that condition (9.2) imposed in that theorem and also (8.1) in [S3 Theorem 13.8] are unnecessary for the reason explained at the beginning of this section.

(4) Suppose $m = n - 1$ in the setting of Theorem 2.2; then $H = \{1\}$. Therefore $H_{\mathbf{A}} \cap GyD \neq \emptyset$ only when $GyD = GD$. Then (2.4) gives $\#\{(\mathscr{V} \cap hD)/(G \cap D)\} = 1$, but this is an immediate consequence of (2.2).

(5) Let us note some more statements in [S3] from which condition (9.2) of [S3] can be removed. First of all, that is the case with Theorem 9.26 of [S3]. In fact, we can state an improved version of that theorem as follows. Using the notation employed in the theorem, let $\mathfrak{I}'_\varphi$ be the subgroup of $\mathfrak{I}$ generated by $\mathfrak{I}_0$ and the prime ideals for which $\sigma(C_v) = F_v^\times$. (Such prime ideals are determined by Theorem 1.9.) *Then* $\#\{SO^\varphi \backslash SO^\varphi_{\mathbf{A}}/C\} = [\mathfrak{I} : \mathfrak{I}'_\varphi]$ *for* $C$ *of* [S3, (9.15)], which equals $C$ of Theorem 2.2 (iv). The last group index is 1 if $F = \mathbf{Q}$, and so the genus of maximal lattices consists of a single class. Consequently we can state a clear-cut result as follows. Let $\mathfrak{S}_n$ denote the set of symmetric matrices of $GL_n(\mathbf{Q})$ that represent $\mathbf{Z}$-valued quadratic forms on $\mathbf{Z}^n$, and $\mathfrak{S}_n^0$ the subset of $\mathfrak{S}_n$ consisting of the reduced elements of $\mathfrak{S}_n$ in the sense of [S5], that is, the set of $\Phi \in \mathfrak{S}_n$ which cannot be represented nontrivially over $\mathbf{Z}$ by another element of $\mathfrak{S}_n$. For $\Phi \in \mathfrak{S}_n$ put $\sigma(\Phi) = p - q$ where $\Phi$ as a real matrix has $p$ positive and $q$ negative eigenvalues. Now the number of genera of $\Phi \in \mathfrak{S}_n^0$ with given $\sigma(\Phi)$ and $\det(2\Phi)$ was determined in [S5, Theorem 6.6]. If $n \geq 3$ and $\sigma(\Phi) \neq n$, then the number of genera of $\Phi$ given there equals the number of classes, as each genus of maximal lattices consists of a single class as explained above.

(6) Next, (9.2) is unnecessary in Theorem 12.1 of [S3]. What we need, in addition to Theorem 1.3, is the following fact: *If* $v \in \mathbf{h}$, $\varphi[h]\mathfrak{g}_v = \varphi(h, L_v)^2$, *then* $L_v \cap W_v$ *is maximal and* $C \cap H_v = \{\alpha \in H_v \mid (L_v \cap W_v)\alpha = L_v \cap W_v\}$. Here the notation is the same as in the proof of Theorem 12.1. The statement is valid irrespective of the nature of $L_v$ and $t_v$. Indeed, replacing $h$ by an element of $F^\times h$, we may assume that $\varphi[h]\mathfrak{g}_v = \varphi(h, L_v) = \mathfrak{g}_v$. Then, by Lemma 10.2 (i) of [S3], we have $L_v = \mathfrak{g}_v h \oplus (L_v \cap W_v)$, from which we immediately obtain the expected facts on $L_v \cap W_v$. Consequently, $\mathfrak{g}_v^\times \subset \sigma(C \cap H_v)$ by Theorem 1.9, as $n-1 > 2$, and the original proof of Theorem 12.1 is valid without (9.2).

(7) In [S4] we proved a result of type (2.7) in terms of $G^+(V)$, but imposed the condition that *if* $n$ *is odd, then* $\det(\varphi)\mathfrak{g}$ *is a square in the ideal group of* $F$; see Theorem 1.6 (iv) of [S4]. We can remove this condition by virtue of Theorem 1.3.

## 3. New mass formulas

3.1. We first recall the symbols $\mathfrak{m}(G, D)$ and $\nu(\Gamma)$ introduced in [S1] and [S2]. Here $G = SO^\varphi(V)$ and $D$ is an open subgroup of $G_{\mathbf{A}}$ containing $G_{\mathbf{a}}$ and such that $D \cap G_{\mathbf{h}}$ is compact. Fixing such a $D$, we put $\Gamma^a = G \cap aDa^{-1}$ for every $a \in G_{\mathbf{A}}$. Let $C_{\mathbf{a}}$ be a maximal compact subgroup of $G_{\mathbf{a}}$ and let $\mathscr{Z} = G_{\mathbf{a}}/C_{\mathbf{a}}$.

Then $\mathscr{Z}$ is a symmetric space on which $G$ acts through its projection into $G_{\mathbf{a}}$. Taking a complete set of representatives $\mathscr{B}$ for $G\backslash G_{\mathbf{A}}/D$, we put

$$\mathfrak{m}(G,\,D) = \mathfrak{m}(D) = \sum_{a\in\mathscr{B}} \nu(\Gamma^a). \tag{3.1}$$

Here $\nu(\Gamma)$ is a quantity defined by

$$\nu(\Gamma) = \begin{cases} [\Gamma : 1]^{-1} & \text{if } G_{\mathbf{a}} \text{ is compact}, \\ \mathrm{vol}(\Gamma\backslash\mathscr{Z})/\#(\Gamma\cap\{\pm 1\}) & \text{otherwise}. \end{cases} \tag{3.2}$$

We fix a Haar measure on $G_{\mathbf{a}}$, which determines a unique $G_{\mathbf{a}}$-invariant measure on $\mathscr{Z}$ by a well known principle. (In fact, $\mathfrak{m}(D)$ and $\nu(\Gamma)$ are the measure of $D\cap G_{\mathbf{a}}$ and that of $\Gamma\backslash G_{\mathbf{a}}$; see [S6, Theorem 9].) We easily see that $\mathfrak{m}(D)$ does not depend on the choice of $\mathscr{B}$. We call $\mathfrak{m}(G,\,D)$ *the mass of $G$ relative to $D$*. If $D'$ is a subgroup of $G_{\mathbf{A}}$ of the same type as $D$ and $D'\subset D$, then, as proven in [S1, Lemma 24.2 (1)],

$$\mathfrak{m}(G,\,D') = [D : D']\mathfrak{m}(G,\,D). \tag{3.3}$$

Next, in the setting of §2.1 we consider a subset $S$ of $\mathscr{V}$ of the form $S = \bigsqcup_{\zeta\in Z} h\zeta\Gamma$, where $h$ is as in (2.2), $Z$ is a finite subset of $G$, and $\Gamma = G\cap D$ with $D$ as above. Then we put

$$\mathfrak{m}(S) = \sum_{\zeta\in Z} \nu(\Delta_\zeta)/\nu(\Gamma), \quad \Delta_\zeta = H\cap\zeta\Gamma\zeta^{-1}, \tag{3.4}$$

and call $\mathfrak{m}(S)$ the *mass* of $S$. Here, to define $\nu(\Delta_\zeta)$, we need to fix a measure on $H_{\mathbf{a}}$. Thus $\mathfrak{m}(S)$ depends on the choice of measures on $G_{\mathbf{a}}$ and $H_{\mathbf{a}}$, but $\mathfrak{m}(S)$ is independent of the choice of $Z$ and $\Gamma$. (Let $\mathfrak{Y} = \{x\in\mathscr{V}_{\mathbf{a}} \mid \varphi[x] = q\}$. Since $\mathfrak{Y}$ can be identified with $H_{\mathbf{a}}\backslash G_{\mathbf{a}}$, once a measure on $G_{\mathbf{a}}$ is fixed, a measure on $\mathfrak{Y}$ determines a measure on $H_{\mathbf{a}}$, and vice versa. The replacement of $h$ by an element of $hG$ changes the group $H$, but that does not change $\mathfrak{m}(S)$ if we start with a fixed measure on $\mathfrak{Y}$. Notice also that an identification of $\mathscr{V}_{\mathbf{a}}$ with a Euclidean space determines a $G_{\mathbf{a}}$-invariant measure on $\mathfrak{Y}$.) Since the left-hand side of (2.4) is finite, we see that $(\mathscr{V}\cap hDy^{-1})/\Gamma^y$ is a finite set for every $y\in G_{\mathbf{A}}$. Thus we can define $\mathfrak{m}(\mathscr{V}\cap hDy^{-1})$ for every $y\in G_{\mathbf{A}}$.

If $G_{\mathbf{a}}$ is compact, we naturally take the measures of $G_{\mathbf{a}}$ and $H_{\mathbf{a}}$ to be 1. Then $\mathfrak{m}(S)$ can be defined in a unique way. We easily see that $S = \bigsqcup_{\zeta\in Z}\bigsqcup_{\gamma\in\Delta'_\zeta\backslash\Gamma} h\zeta\gamma$, where $\Delta'_\zeta = \zeta^{-1}\Delta_\zeta\zeta$, and so $\#S = \sum_{\zeta\in Z}[\Gamma : \Delta'_\zeta] = \mathfrak{m}(S)$ if $G_{\mathbf{a}}$ is compact. Thus we obtain

$$\mathfrak{m}(S) = \#(S) \quad \text{if } G_{\mathbf{a}} \text{ is compact}. \tag{3.5}$$

Theorem 3.2. *The notation being the same as in Theorem 2.2, we have*

$$\mathfrak{m}(H,\,H_{\mathbf{A}}\cap D) = \sum_{y\in Y} \nu(\Gamma^y)\mathfrak{m}(\mathscr{V}\cap hDy^{-1}). \tag{3.6}$$

*In particular if $m = 1$ and the notation is as in* (iv) *of Theorem 2.2, then*

$$\mathfrak{m}(H,\, H_{\mathbf{A}} \cap C) = \sum_{y \in Y} \nu(\Gamma^y)\mathfrak{m}\bigl((Ly^{-1})[q,\, \mathfrak{b}]\bigr). \tag{3.7}$$

*Proof.* Let $E_y = H\backslash(H_{\mathbf{A}} \cap GyD)/(H_{\mathbf{A}} \cap D)$. For each $\varepsilon \in E_y$ take $\zeta_\varepsilon \in G$ so that $\varepsilon \in \zeta_\varepsilon y D$. By Theorem 2.2 (ii) we have $\mathscr{V} \cap hDy^{-1} = \bigsqcup_{\varepsilon \in E_y} h\zeta_\varepsilon \Gamma^y$ and $H \cap \varepsilon(H_{\mathbf{A}} \cap D)\varepsilon^{-1} = H \cap H_{\mathbf{A}} \cap \varepsilon D \varepsilon^{-1} = H \cap \zeta_\varepsilon y D y^{-1}\zeta_\varepsilon^{-1} = H \cap \zeta_\varepsilon \Gamma^y \zeta_\varepsilon^{-1}$, so that

$$\nu(\Gamma^y)\mathfrak{m}(\mathscr{V} \cap hDy^{-1}) = \sum_{\varepsilon \in E_y} \nu(H \cap \zeta_\varepsilon \Gamma^y \zeta_\varepsilon^{-1}) = \sum_{\varepsilon \in E_y} \nu(H \cap \varepsilon(H_{\mathbf{A}} \cap D)\varepsilon^{-1}).$$

Since $\bigsqcup_{y \in Y} E_y$ gives $H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)$, we obtain

$$\mathfrak{m}(H,\, H_{\mathbf{A}} \cap D) = \sum_{y \in Y} \sum_{\varepsilon \in E_y} \nu(H \cap \varepsilon(H_{\mathbf{A}} \cap D)\varepsilon^{-1}) = \sum_{y \in Y} \nu(\Gamma^y)\mathfrak{m}(\mathscr{V} \cap hDy^{-1}).$$

This proves (3.6), which combined with (2.5) gives (3.7).

Formula (3.7) was given in [S3, (13.17b)] under the condition mentioned at the beginning of Section 2. That condition can be removed by the above theorem.

It should be noted that (3.6) and (3.7) are different from any of the mass formulas of Siegel. Indeed, the left-hand side of (3.6) concerns an orthogonal group in dimension $n - m$, and the right-hand side concerns the space $\mathscr{V}$, whereas both sides of Siegel's formulas are defined with respect to matrices of the same size. See also [S3, p. 137] for a comment on the connection with the work of Eisenstein and Minkowski on the sums of five squares.

## 4. Classification and genera of quadratic forms in terms of matrices

4.1. Traditionally the genus and class of a quadratic form over $\mathbf{Q}$ were defined in terms of matrices, but it is easy to see that they are equivalent to those defined in terms of lattices. In the general case, however, there is a standard definition in terms of lattices, but the definition in terms of matrices is nontrivial. Also, we treated in [S5] the classification of quadratic forms over a number field, but gave explicit results in terms of matrices only when $\mathbf{Q}$ is the base field. Let us now discuss how we can handle such problems over an arbitrary number field, as the generalization is far from obvious and requires some new concepts. Before proceeding, we recall two basic facts: Given $(V,\, \varphi)$ over a global $F$ and a lattice $L$ in $V$, the $O^\varphi(V)$-genus of $L$ is the same as the $SO^\varphi(V)$-genus of $L$; all the maximal lattices in $V$ form a single $O^\varphi(V)$-genus; see [S3, Lemmas 6.8 and 6.9].

We take a global field $F$, and denote by $F_n^1$ the vector space of all $n$-dimensional row vectors with components in $F$, and by $\mathfrak{g}_n^1$ the set of elements of $F_n^1$ with components in $\mathfrak{g}$. Define subgroups $E$ and $E_\xi$ of $GL_n(F)_{\mathbf{A}}$ by

$$E = GL_n(F)_{\mathbf{a}} \prod_{v \in \mathbf{h}} GL_n(\mathfrak{g}_v), \qquad E_\xi = \xi^{-1}E\xi \quad (\xi \in GL_n(F)_{\mathbf{A}}). \tag{4.1}$$

Put $L_0 = \mathfrak{g}_n^1$. An arbitrary $\mathfrak{g}$-lattice $L$ in $F_n^1$ can be given as $L = L_0\xi$ with $\xi \in GL_n(F)_{\mathbf{A}}$; then $E_\xi = \{y \in GL_n(F)_{\mathbf{A}} \mid Ly = L\}$. It is well known that the map $x \mapsto \det(x)\mathfrak{g}$ gives a bijection of $E\backslash GL_n(F)_{\mathbf{A}}/GL_n(F)$ onto the ideal class group of $F$; see [S1, Lemma 8.14], for example. Thus the ideal class of $\det(\xi)\mathfrak{g}$ is determined by the $GL_n(F)$-class of $L_0\xi$, and vice versa. Consequently, $L$ is isomorphic as a $\mathfrak{g}$-module to the direct sum of $\mathfrak{g}_{n-1}^1$ and $\det(\xi)\mathfrak{g}$.

To define the generalization of $\mathbf{Z}$-valued quadratic forms, we denote by $S_n$ the set of all symmetric elements of $GL_n(F)$, fix an element $\xi$ of $GL_n(F)_{\mathbf{A}}$, and denote by $S_n(\xi)$ the set of all $T \in S_n$ such that $xT \cdot {}^t x \in \mathfrak{g}$ for every $x \in L_0\xi$. We call such a $T$ *reduced* (relative to $\xi$) if the following condition is satisfied:

$$T \in S_n(\zeta^{-1}\xi) \text{ with } \zeta \in GL_n(F)_{\mathbf{h}} \cap \textstyle\prod_{v \in \mathbf{h}} M_n(\mathfrak{g}_v) \implies \zeta \in E. \tag{4.2}$$

We denote by $S_n^0(\xi)$ the set of all reduced elements of $S_n(\xi)$. These depend essentially on $E\xi GL_n(F)$, as will be seen in Proposition 4.3 (i) below.

4.2. To define the genus and class of an element of $S_n$, put

$$\Delta_\xi = E_\xi \cap GL_n(F), \qquad \Delta_\xi^1 = E_\xi \cap SL_n(F). \tag{4.3}$$

We say that two elements $\Phi$ and $\Psi$ of $S_n(\xi)$ belong to the same *genus* (relative to $\xi$) if there exists an element $\varepsilon$ of $E_\xi$ such that $\varepsilon\Phi \cdot {}^t\varepsilon = \Psi$; they are said to belong to the same *O-class* (resp. *SO-class*) if $\alpha\Phi \cdot {}^t\alpha = \Psi$ for some $\alpha \in \Delta_\xi$ (resp. $\alpha \in \Delta_\xi^1$). These depend on the choice of $L = L_0\xi$, or rather, on the choice of the ideal class of $\det(\xi)\mathfrak{g}$. There is no reason to think that $\xi = 1$ is the most natural choice.

Given $\Phi \in S_n$, put $V = F_n^1$ and $\varphi[x] = x\Phi \cdot {}^t x$ for $x \in V$. Then we obtain a quadratic space $(V, \varphi)$, which we denote by $[\Phi]$; we put then $O(\Phi) = O^\varphi(V)$ and $SO(\Phi) = SO^\varphi(V)$. Now put $L = L_0\xi$ with $\xi \in GL_n(F)_{\mathbf{A}}$. Clearly $L$ is integral if $\Phi \in S_n(\xi)$, in which case $L$ is maximal if and only if $\Phi \in S_n^0(\xi)$.

Proposition 4.3. (i) *If $\eta \in E\xi\alpha$ with $\xi, \eta \in GL_n(F)_{\mathbf{A}}$ and $\alpha \in GL_n(F)$, then $S_n(\xi) = \alpha S_n(\eta) \cdot {}^t\alpha$ and $S_n^0(\xi) = \alpha S_n^0(\eta) \cdot {}^t\alpha$.*

(ii) *For $\Phi, \Psi \in S_n^0(\xi)$, $\xi \in GL_n(F)_{\mathbf{A}}$, the spaces $[\Phi]$ and $[\Psi]$ are isomorphic if and only if they belong to the same genus.*

(iii) *Let $X$ be a complete set of representatives for $E\backslash GL_n(F)_{\mathbf{A}}/GL_n(F)$ and for each $\xi \in GL_n(F)_{\mathbf{A}}$ let $Y_\xi$ be a complete set of representatives for the genera of the elements of $S_n^0(\xi)$. Then the spaces $[\Phi]$ obtained from $\Phi \in Y_\xi$ for all $\xi \in X$ exhaust all isomorphism classes of $n$-dimensional quadratic spaces over $F$ without overlapping.*

*Proof.* Assertion (i) can be verified in a straightforward way. Let $\Phi$ and $\Psi$ be elements of $S_n^0(\xi)$ belonging to the same genus. Then there exists an element $\varepsilon \in E_\xi$ such that $\varepsilon\Phi \cdot {}^t\varepsilon = \Psi$, and the Hasse principle guarantees an element $\alpha$ of $GL_n(F)$ such that $\Psi = \alpha\Phi \cdot {}^t\alpha$. Thus $[\Psi]$ is isomorphic to $[\Phi]$. Conversely, suppose $[\Phi]$ and $[\Psi]$ are isomorphic for $\Phi, \Psi \in S_n^0(\xi)$. Then $\Phi = \beta\Psi \cdot {}^t\beta$ for some $\beta \in GL_n(F)$. Now $L_0\xi$ is maximal in both $[\Phi]$ and $[\Psi]$, and $L_0\xi\beta$ is maximal in $[\Psi]$. Thus $L_0\xi\beta = L_0\xi\gamma$ with $\gamma \in O(\Psi)_{\mathbf{A}}$. Put $\zeta = \beta\gamma^{-1}$. Then $\zeta \in E_\xi$, and $\zeta\Psi \cdot {}^t\zeta = \Phi$. Therefore $\Psi$ belongs to the genus of $\Phi$. This proves (ii). As for (iii), clearly every $n$-dimensional quadratic space is isomorphic to $[\Psi]$ for some $\Psi \in S_n$. Putting $V = F_n^1$, pick a maximal lattice $L$ in $V$ and put $L = L_0\eta$ with $\eta \in GL_n(F)_{\mathbf{A}}$. Then $\eta \in E\xi GL_n(F)$ for some $\xi \in X$, and by (i) we can replace $\eta$ by $\xi$. Take a member $\Phi$ of $Y_\xi$ belonging to the genus of $\Psi$. Then by (ii), $[\Psi]$ is isomorphic to $[\Phi]$. Thus every $n$-dimensional quadratic space is isomorphic to $[\Phi]$ for some $\Phi \in Y_\xi$ with $\xi \in X$. To prove that there is no overlapping, take $\Phi_i \in Y_{\xi_i}$ with $\xi_i \in X$, $i = 1, 2$, and suppose that $[\Phi_1]$ is isomorphic to $[\Phi_2]$. Then $\Phi_1 = \alpha\Phi_2 \cdot {}^t\alpha$ with $\alpha \in GL_n(F)$. Now $L_0\xi_1$ is maximal in $[\Phi_1]$, and so $L_0\xi_1\alpha$ is maximal in $[\Phi_2]$. Therefore $L_0\xi_1\alpha = L_0\xi_2\gamma$ with $\gamma \in O(\Phi_2)_{\mathbf{A}}$. Then $\xi_1\alpha\gamma^{-1}\xi_2^{-1} \in E$, and so $\det(\xi_1\xi_2^{-1}) \in F^\times \det(E)$, which implies that $\xi_1 = \xi_2$, as $\xi_i \in X$. Thus both $\Phi_1$ and $\Phi_2$ belong to $Y_{\xi_1}$. By (ii) they must belong to the same genus. This completes the proof.

4.4. Take $\Phi \in S_n^0(\xi)$ and suppose another member $\Psi$ of$S_n^0(\xi)$ belongs to the genus of $\Phi$. Put $L = L_0\xi$. Then $\Psi = \varepsilon\Phi \cdot {}^t\varepsilon = \alpha\Phi \cdot {}^t\alpha$ with $\varepsilon \in E_\xi$ and $\alpha \in GL_n(F)$, as observed in the above proof. Clearly $\varepsilon^{-1}\alpha \in O(\Phi)_{\mathbf{A}}$. Since $L\alpha = L\varepsilon^{-1}\alpha$, we see that $L\alpha$ belongs to the genus of $L$. We associate the $O(\Phi)$-class of $L\alpha$ to the $O$-class of $\Psi$. We easily see that the class of $L\alpha$ is determined by the class of $\Psi$. Moreover, it gives a bijection of the set of $O$-classes in the genus of $\Phi$ onto the set of $O(\Phi)$-classes in the genus of $L_0\xi$. Indeed, let $M = L\sigma$ with $\sigma \in SO(\Phi)_{\mathbf{A}}$. Then $\det(\sigma)\mathfrak{g} = \mathfrak{g}$, and so $\sigma = \tau\beta$ with $\tau \in E_\xi$ and $\beta \in GL_n(F)$. Put $\Psi = \tau^{-1}\Phi \cdot {}^t\tau^{-1}$. Then $\Psi = \beta\Phi \cdot {}^t\beta$ and $M = L\beta$, which corresponds to $\Psi$. This proves the surjectivity. The injectivity can be easily verified too.

For $\Phi \in S_n^0(\xi)$ we define the *SO-genus* of $\Phi$ to be the set of all $\Psi$ in the genus of $\Phi$ such that $\det(\Psi) = \det(\Phi)$. For $\Psi = \varepsilon\Phi \cdot {}^t\varepsilon = \alpha\Phi \cdot {}^t\alpha$ as above, suppose $\det(\Psi) = \det(\Phi)$; then $\det(\alpha)^2 = 1$. Since $-1 \in \det\big(O(\Phi)\big)$, changing $\alpha$ for $\alpha\gamma$ with a suitable $\gamma \in O(\Phi)$, we may assume that $\det(\alpha) = 1$. We then associate the $SO(\Phi)$-class of $L\alpha$ to $\Psi$ We can easily verify that the set of all $SO$-classes in the $SO$-genus of $\Phi$ contained in $S_n^0(\xi)$ are in one-to-one correspondence with the set of $SO(\Phi)$-classes in the genus of $L$.

In general, if $\Psi = \varepsilon\Phi\cdot{}^t\varepsilon = \alpha\Phi\cdot{}^t\alpha$ as above, then $\det(\alpha)^2 = \det(\varepsilon)^2 \in \det(E_\xi)$, and so $\det(\alpha) \in \mathfrak{g}^\times$. Therefore, if $F = \mathbf{Q}$, then $\det(\Psi) = \det(\Phi)$, and the $SO$-genus of $\Phi$ coincides with the genus of $\Phi$.

4.5. Define $(V, \varphi)$ by $V = F_n^1$ and $\varphi[x] = x\Phi \cdot {}^t x$ as above with any $\Phi \in S_n$. Put $L = L_0\xi$ with $\xi \in GL_n(F)_{\mathbf{A}}$. We easily see that $\widetilde{L} = L_0(2\Phi \cdot {}^t\xi)^{-1}$, and so

$$[\widetilde{L}/L] = \det(2\Phi\xi^2)\mathfrak{g} \quad \text{if} \quad L = L_0\xi. \tag{4.4}$$

In order to state our main results, we need a basic fact on an algebraic extension $K$ of $F$. Let $\mathfrak{r}$ be the maximal order of $K$, and $\mathfrak{d}$ the different of $K$ relative to $F$; let $\mathfrak{d}_0 = N_{K/F}(\mathfrak{d})$, $m = [K : F]$, and $d(K/F) = \det\big[(\mathrm{Tr}_{K/F}(e_ie_j))_{i,j=1}^m\big]$ with an $F$-basis $\{e_i\}_{i=1}^m$ of $K$. Strictly speaking, $d(K/F)$ should be viewed as a coset in $F^\times/F^{\times 2}$ represented by that determinant, but we denote any number in that coset by $d(K/F)$. By the *characteristic ideal class* for the extension $K/F$ we understand the ideal class $\mathfrak{k}$ in $F$ determined by the property that $\mathfrak{r}$ is isomorphic as a $\mathfrak{g}$-module to $\mathfrak{g}^1_{m-1} \oplus \mathfrak{x}$ with an ideal $\mathfrak{x}$ belonging to $\mathfrak{k}$. Then we have

(4.5) *The characteristic ideal class for $K/F$ contains an ideal $\mathfrak{x}$ such that $\mathfrak{d}_0 = d(K/F)\mathfrak{x}^2$.*

To prove this, take $V = K$, $\varphi(x, y) = \mathrm{Tr}_{K/F}(xy)$ for $x, y \in K$, and $L = \mathfrak{r}$ in (4.4). Then $\widetilde{L} = (2\mathfrak{d})^{-1}$, and (4.4) shows that $\mathfrak{d}_0 = d(K/F)\mathfrak{x}^2$ with $\mathfrak{x} = \det(\xi)\mathfrak{g}$, which proves (4.5). This fact was noted, in substance, by Artin in 1949; that $\mathfrak{d}$ defines a square ideal class in $K$ is due to Hecke. We can easily generalize (4.5) to the case of a maximal order $\mathfrak{o}$ in a simple algebra over $F$. The ideal class which is an obvious analogue of $\mathfrak{k}$ is independent of the choice of $\mathfrak{o}$.

We also need a few more symbols. We denote by $\mathbf{r}$ the set of all real primes in $\mathbf{a}$. For $T \in S_n$ and $v \in \mathbf{r}$ we put $s_v(T) = p_v - q_v$ if $T$ as a real symmetric matrix in $GL_n(F_v) = GL_v(\mathbf{R})$ has $p_v$ positive and $q_v$ negative eigenvalues. Given a quadratic space $(V, \varphi)$, we denote by $Q(\varphi)$ the characteristic quaternion algebra of $(V, \varphi)$ in the sense of [S5, §3.1]; if $\varphi$ is obtained from $\Phi \in S_n$ as above, we put $\delta(\Phi) = \delta(\varphi)$ and $Q(\Phi) = Q(\varphi)$. In [S5, Theorem 4.4] we showed that the isomorphism class of $(V, \varphi)$ is determined by $\{n, \delta(\varphi), Q(\varphi), \{s_v(\varphi)\}_{v\in\mathbf{r}}\}$. We will now state this fact in terms of the matrices $\Phi$ in $S^0_n(\xi)$.

THEOREM 4.6 (The case of even $n$). *Let the symbols $n$, $\{\sigma_v\}_{v\in\mathbf{r}}$, $\delta$, $K_0$, $\mathfrak{e}_0$, $\mathfrak{e}_1$, and $\xi$ be given as follows: $4 \le n \in 2\mathbf{Z}$, $\sigma_v \in 2\mathbf{Z}$, $|\sigma_v| \le n$; $\delta \in F^\times$, $K_0 = F(\sqrt{\delta}\,)$; $\mathfrak{e}_0$ and $\mathfrak{e}_1$ are squarefree integral ideals in $F$; $\xi \in GL_n(F)_\mathbf{A}$. Let $r$ be the number of prime factors of $\mathfrak{e}_0\mathfrak{e}_1$, and $\mathfrak{d}$ the different of $K_0$ relative to $F$; put $\mathfrak{d}_0 = \mathfrak{d}^2 \cap F$. Suppose that $\mathfrak{e}_0$ divides $\mathfrak{d}_0$, $\mathfrak{e}_1$ is prime to $\mathfrak{d}_0$, $(-1)^{\sigma_v/2}\delta > 0$ at each $v \in \mathbf{r}$, $\det(\xi)\mathfrak{e}_1^{-1}$ belongs to the characteristic ideal class for $K_0/F$, and*

$$r + \#\bigl\{v \in \mathbf{r} \bigm| \sigma_v \equiv 4 \text{ or } 6 \pmod 8\bigr\} \in 2\mathbf{Z}. \tag{4.6}$$

*Then there exists an element $\Phi$ of $S^0_n(\xi)$ such that*

$$\delta \in \delta(\Phi), \quad \det(2\Phi\xi^2)\mathfrak{g} = \mathfrak{d}_0\mathfrak{e}_1^2, \quad s_v(\Phi) = \sigma_v \text{ for every } v \in \mathbf{r}, \tag{4.7}$$

*and $Q(\Phi)$ is ramified at $v \in \mathbf{h}$ if and only if $v|\mathfrak{e}_0\mathfrak{e}_1$. Moreover, every element of $S^0_n(\xi)$ is of this type, and its genus is determined by $(\{\sigma_v\}_{v\in\mathbf{r}}, \delta, \mathfrak{e}_0, \mathfrak{e}_1)$. These statements are true even for $n = 2$ under the following additional condition on $\mathfrak{e}_1$ : if $\mathfrak{e}_1 \ne \mathfrak{g}$, then $K_0 \ne F$ and every prime factor of $\mathfrak{e}_1$ remains prime in $K_0$.*

*Proof.* Given the symbols as in our theorem, let $B$ be the quaternion algebra over $F$ ramified exactly at the prime factos of $\mathfrak{e}_0\mathfrak{e}_1$ and at those $v \in \mathbf{r}$ for which $\sigma_v \equiv 4$ or $6 \pmod 8$. Such a $B$ exists because of (4.6). By the main theorem of classification [S5, Theorem 4.4] there exists a quadratic space $(V, \varphi)$ over $F$ such that $B = Q(\varphi)$, $\delta \in \delta(\varphi)$, and $\sigma_v = s_v(\varphi)$ for every $v \in \mathbf{r}$. By Proposition 4.3 (ii) we can take $(V, \varphi) = [\Psi]$ with $\Psi \in S^0_n(\eta)$, $\eta \in GL_n(F)_\mathbf{A}$. Put $L = L_0\eta$. By [S5, Theorem 6.2 (ii)] we have $[\widetilde{L}/L] = \mathfrak{d}_0\mathfrak{e}_1^2$, which combined with (4.4) shows that $\det(2\Psi\eta^2)\mathfrak{g} = \mathfrak{d}_0\mathfrak{e}_1^2$. By our assumption on $\xi$ and (4.5) we have $\mathfrak{d}_0\mathfrak{e}_1^2 = c^2\delta\det(\xi)^2\mathfrak{g}$ with $c \in F^\times$. Thus $\det(2\Psi\eta^2)\mathfrak{g} = c^2\delta\det(\xi)^2\mathfrak{g}$. Since $(-1)^{n/2}\delta = b^2\det(2\Psi)$ with $b \in F^\times$, we see that $\det(\eta)\mathfrak{g} = bc\det(\xi)\mathfrak{g}$, which implies that $\eta \in E\xi\alpha$ with $\alpha \in GL_n(F)$. Then by Proposition 4.3 (i) we can replace $\eta$ by the given $\xi$, and we obtain the first part of our theorem.

Next, given $\Phi \in S_n^0(\xi)$, put $L = L_0\xi$. Let $\mathfrak{e}$ be the product of all the prime ideals in $F$ ramified in $Q(\Phi)$ and let $K_0 = F(\sqrt{\delta}\,)$ with $\delta \in \delta(\Phi)$. By [S5, (4.2b)], $Q(\Phi)$ is ramified at $v \in \mathbf{r}$ if and only if $s_v(\Phi) \equiv 4$ or $6 \pmod 8$. Put $\mathfrak{e} = \mathfrak{e}_0\mathfrak{e}_1$, where $\mathfrak{e}_0$ is the product of the prime factors of $\mathfrak{e}$ ramified in $K_0$. Then in [S5, Theorem 6.2 (ii)] we showed that $[\widetilde{L}/L] = \mathfrak{d}_0\mathfrak{e}_1^2$, where $\mathfrak{d}_0$ is defined for this $K_0$ as in our theorem. Combining this with (4.4) we obtain $\det(2\Phi\xi^2)\mathfrak{g} = \mathfrak{d}_0\mathfrak{e}_1^2$. We have $\mathfrak{d}_0 = \delta\mathfrak{x}^2$ with an ideal $\mathfrak{x}$ as in (4.5), and so $\det(\xi)\mathfrak{g} = \mathfrak{x}\mathfrak{e}_1$, if we take $\delta$ to be $(-1)^{n/2}\det(2\Phi)$. This proves the second part of our theorem. The last part concerning the case $n = 2$ follows from [S5, Theorem 4.4, (4.4b)].

Theorem 4.7 (The case of odd $n$). *Let the symbols $n$, $\{\sigma_v\}_{v\in\mathbf{r}}$, $\delta$, $K_0$, $\mathfrak{e}$, and $\xi$ be given as follows: $0 < n - 1 \in 2\mathbf{Z}$, $\sigma_v - 1 \in 2\mathbf{Z}$, $|\sigma_v| \le n$; $\delta \in F^\times$, $K_0 = F(\sqrt{\delta}\,)$; $\mathfrak{e}$ is a squarefree integral ideal in $F$; $\xi \in GL_n(F)_\mathbf{A}$. Let $r$ be the number of prime factors of $\mathfrak{e}$; let $\delta\mathfrak{g} = \mathfrak{a}\mathfrak{b}^2$ with a squarefree integral ideal $\mathfrak{a}$ and a fractional ideal $\mathfrak{b}$ in $F$; put $\mathfrak{e} = \mathfrak{e}_0\mathfrak{e}_1$ with $\mathfrak{e}_1 = \mathfrak{a} + \mathfrak{e}$. Suppose $(-1)^{(\sigma_v-1)/2}\delta > 0$ at each $v \in \mathbf{r}$, $\det(\xi)\mathfrak{b}$ belongs to the ideal class of $\mathfrak{e}_0$, and*

$$r + \#\bigl\{v \in \mathbf{r}\,\big|\,\sigma_v \equiv \pm 3 \pmod 8\bigr\} \in 2\mathbf{Z}. \tag{4.8}$$

*Then there exists an element $\Phi$ of $S_n^0(\xi)$ such that*

$$\delta \in \delta(\Phi), \quad \det(2\Phi\xi^2)\mathfrak{g} = 2\mathfrak{a}\mathfrak{e}_0^2, \quad s_v(\Phi) = \sigma_v \text{ for every } v \in \mathbf{r}, \tag{4.9}$$

*and $Q(\Phi)$ is ramified at $v \in \mathbf{h}$ if and only if $v|\mathfrak{e}$. Moreover, every element of $S_n^0(\xi)$ is of this type, and its genus is determined by $(\{\sigma_v\}_{v\in\mathbf{r}}, \delta, \mathfrak{e})$.*

*Proof.* In [S5, Theorem 6.2 (iii)] we showed that $[\widetilde{L}/L] = 2\mathfrak{a}^{-1}\mathfrak{e}^2 \cap 2\mathfrak{a}$ for a maximal lattice $L$ if $\delta(\varphi)\mathfrak{g} = \mathfrak{a}\mathfrak{b}^2$ as above. We easily see that $2\mathfrak{a}^{-1}\mathfrak{e}^2 \cap 2\mathfrak{a} = 2\mathfrak{a}\mathfrak{e}_0^2$. Therefore the proof can be given in exactly the same fashion as for Theorem 4.6.

Remark. (1) Let $\mathfrak{x}$ be the ideal belonging to the characteristic ideal class for $K_0/F$ such that $\mathfrak{d}_0 = \delta\mathfrak{x}^2$. Suppose $\Phi$ has the last two properties of (4.7) and $\det(\xi)\mathfrak{e}_1^{-1}$ belongs to the class of $\mathfrak{x}$. Then $b^2\det(2\Phi)\mathfrak{g} = \delta\mathfrak{g}$ with $b \in F^\times$, and so $(-1)^{n/2}\det(2\Phi) = b^{-2}\delta c$ with $c \in \mathfrak{g}^\times$. Since $s_v(\Phi) = \sigma_v$ for every $v \in \mathbf{r}$, we see that $c > 0$ at every $v \in \mathbf{r}$. Suppose an element of $\mathfrak{g}^\times$ positive at every $v \in \mathbf{r}$ is always a square. Then we obtain $\delta \in \delta(\Phi)$. Thus the first property of $\Phi$ in (4.7) follows from the assumption on $\det(\xi)\mathfrak{g}$ and the last two properties of (4.7) under that condition on $\mathfrak{g}^\times$. The same comment applies to (4.9).

(2) The last two statements of (1) apply to the case $F = \mathbf{Q}$. Therefore the above two theorems for $F = \mathbf{Q}$ are the same as [S5, Theorems 6.4 and 6.5]. The new features in the general case are that we need $\xi \in GL_n(F)_\mathbf{A}$ and we have to impose a condition on the ideal class of $\det(\xi)\mathfrak{g}$. In other words, the

coset $E\xi GL_n(F)$ is determined by $\{\sigma_v\}_{v\in\mathbf{r}}$, $\delta$, and the characteristic quaternion algebra.

(3) A $\mathfrak{g}$-valued *symmetric* form is represented by an element of $S_n$ with entries in $\mathfrak{g}$. This is different from the notion of a $\mathfrak{g}$-valued *quadratic* form, and so the classification of $\mathfrak{g}$-valued symmetric forms is different from that of $\mathfrak{g}$-valued quadratic forms. We refer the reader to [S7] for the classification of $\mathfrak{g}$-valued symmetric forms and its connection with the classification of quadratic forms.

## 5. Ternary forms

5.1. Before proceeding further, let us recall several basic facts on quaternion algebras. Let $B$ be a quaternion algebra over a global field $F$, and $\mathfrak{O}$ an order in $B$ containing $\mathfrak{g}$. For $\xi \in B_{\mathbf{A}}^\times$ the principle of §1.2 about the lattice $Lx$ enables us to define $\mathfrak{O}\xi$ as a $\mathfrak{g}$-lattice in $B$. We call a $\mathfrak{g}$-lattice in $B$ of this form a *proper left $\mathfrak{O}$-ideal.* Thus the $B^\times$-genus of $\mathfrak{O}$ consists of all proper left $\mathfrak{O}$-ideals, and the genus is stable under right multiplication by the elements of $B^\times$, and so a $B^\times$-class of proper left $\mathfrak{O}$-ideals is meaningful. Define a subgroup $U$ of $B_{\mathbf{A}}^\times$ by $U = B_{\mathbf{a}}^\times \prod_{v\in\mathbf{h}} \mathfrak{O}_v^\times$. Then $\#(U\backslash B_{\mathbf{A}}^\times/B^\times)$ gives the number of $B^\times$-classes in this genus, which we call *the class number of* $\mathfrak{O}$. Next, for $x \in B_{\mathbf{A}}^\times$ we denote by $x\mathfrak{O}x^{-1}$ the order $\mathfrak{O}'$ in $B$ such that $\mathfrak{O}'_v = x_v\mathfrak{O}_v x_v^{-1}$ for every $v \in \mathbf{h}$. By *the type number of* $\mathfrak{O}$ we mean $\#S$ for a minimal set $S$ of such orders $\mathfrak{O}'$ with the property that every order of type $x\mathfrak{O}x^{-1}$ can be transformed to a member of $S$ by an inner automorphism of $B$.

Given an order $\mathfrak{O}$ in $B$ over a local or global $F$, put $\widetilde{\mathfrak{O}} = \{x \in B \,|\, \mathrm{Tr}_{B/F}(x\mathfrak{O}) \subset \mathfrak{g}\}$. It can be shown that $[\widetilde{\mathfrak{O}}/\mathfrak{O}]$ is a square of an integral ideal $\mathfrak{t}$. We call $\mathfrak{t}$ *the discriminant of* $\mathfrak{O}$. In the local case, if $B$ is a division algebra, then $\mathfrak{O}$ is maximal if and only if the disriminant is the prime ideal of $\mathfrak{g}$. In the global case, if $\mathfrak{O}$ is maximal, then the discriminant of $\mathfrak{O}$ is the product of all the prime ideals where $B$ is ramified. Thus we call it the *discriminant of* $B$. If $F = \mathbf{Q}$, then writing the discriminant of $\mathfrak{O}$ or of $B$ in the form $t\mathbf{Z}$ with a positive integer $t$, we call $t$ *the discriminant of* $\mathfrak{O}$ *or of* $B$. Let us quote here a result due to Eichler [E2, Satz 3]:

(5.1) *If $F$ is local, $B$ is isomorphic to $M_2(F)$, and the discriminant of an order $\mathfrak{O}$ in $B$ is the prime ideal $\mathfrak{p}$ of $\mathfrak{g}$, then there is an isomorphism of $B$ onto $M_2(F)$ that maps $\mathfrak{O}$ onto*

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathfrak{g}) \,\middle|\, c \in \mathfrak{p} \right\}. \tag{5.1a}$$

If $\mathfrak{O}$ is the order of (5.1a), then we can easily verify that

$$\widetilde{\mathfrak{O}} = \mathfrak{O}\eta^{-1} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \,\middle|\, a,\, c,\, d \in \mathfrak{g},\, b \in \mathfrak{p}^{-1} \right\}, \quad \eta = \begin{bmatrix} 0 & -1 \\ \pi & 0 \end{bmatrix}, \tag{5.1b}$$

where $\pi$ is a prime element of $F$.

Let $\mathfrak{O}$ be an order in $B$ in the global case, and let $\mathfrak{e}$ be the discriminant of $B$; suppose the discriminant of $\mathfrak{O}$ is squarefree. Then the discriminant of

$\mathfrak{O}$ is of the form $\mathfrak{a}_0\mathfrak{e}$ with a squarefree integral ideal $\mathfrak{a}_0$ prime to $\mathfrak{e}$. For each $v|\mathfrak{a}_0$ the order $\mathfrak{O}_v$ can be transformed to an order of type (5.1a). We will be considering such an order $\mathfrak{O}$ in the following treatment.

5.2. Let us now consider $(V, \varphi)$ with $n = 3$ over a local or global $F$. As shown in [S3, §7.3], we can find a quaternion algebra $B$ over $F$ with which we can put $V = B^\circ\xi$, $A(V) = B + B\xi$, $A^+(V) = B$, $\varphi[x\xi] = dxx^\iota$ and $2\varphi(x\xi, y\xi) = d\mathrm{Tr}_{B/F}(xy^\iota)$ for $x, y \in B^\circ$, where $B^\circ$ is as in (1.2) and $\xi$ is an element such that $\xi^2 = -d \in \delta(\varphi)$; $F + F\xi$ is the center of $A(V)$; $G^+(V) = B^\times$; $\nu(\alpha) = N_{B/F}(\alpha)$ and $x\xi\tau(\alpha) = \alpha^{-1}x\alpha\xi$ for $x \in B^\circ$ and $\alpha \in B^\times$.

Given $h \in V$ such that $\varphi[h] \neq 0$, take $k \in B^\circ$ so that $h = k\xi$. Put $W = (Fh)^\perp$ and $K = F + Fk$. It can easily be seen that $K = \{\alpha \in B \,|\, \alpha k = k\alpha\}$, and $K$ is either a quadratic extension of $F$, or isomorphic to $F \times F$. In either case we can find an element $\omega$ of $B$ such that

$$B = K + \omega K, \quad \omega^2 \in F^\times, \quad \omega k = -k\omega. \tag{5.2}$$

Then $B^\circ = Fk + \omega K$ and $\mathrm{Tr}_{B/F}(k\omega K) = 0$, and so $W = \omega K\xi = F\omega\xi + F\omega k\xi$, and $\varphi[\omega x\xi] = -d\omega^2 xx^\rho$ for $x \in K$, where $\rho$ is the nontrivial automorphism of $K$ over $F$. Since $-dk^2 = \varphi[h]$, we have $K = F \times F$ if $-d\varphi[h]$ is a square in $F$; otherwise $K = F(\kappa^{1/2})$ with $\kappa = -d\varphi[h]$. We easily see that

$$A^+(W) = K, \qquad G^+(W) = K^\times. \tag{5.3}$$

The group $SO^\varphi(W)$ can be identified with $\{b \in K^\times \,|\, bb^\rho = 1\}$, and the map $\tau : K^\times \to SO^\varphi(W)$ is given by $\tau(a) = a/a^\rho$ for $a \in K^\times$. To be precise, $\omega x\xi\tau(a) = \omega(a/a^\rho)x\xi$ for $x \in K$.

Clearly the isomorphism class of $(V, \varphi)$ is determined by $B$ and $dF^{\times 2}$, and vice versa. If $F$ is a totally real number field and $\varphi$ is positive definite at every $v \in \mathbf{a}$, then $B$ is totally definite and $d$ is totally positive.

Assuming $F$ to be global, put $d\mathfrak{g} = \mathfrak{a}\mathfrak{x}^2$ with a squarefree integral ideal $\mathfrak{a}$ and a fractional ideal $\mathfrak{x}$; let $\mathfrak{e}$ be the product of all the prime ideals of $F$ ramified in $B$. In general the pair $(\mathfrak{e}, \mathfrak{a})$ does not necessarily determine $(V, \varphi)$, but it does if $F = \mathbf{Q}$ and $\varphi$ is positive definite.

LEMMA 5.3. *Suppose $F$ is global; let $(V, \varphi)$, $B$, $\mathfrak{a}$, and $\mathfrak{e}$ be as above. Put $\mathfrak{e}_1 = \mathfrak{a} + \mathfrak{e}$, $\mathfrak{e} = \mathfrak{e}_0\mathfrak{e}_1$, and $\mathfrak{a} = \mathfrak{a}_0\mathfrak{e}_1$. Let $L$ be an integral lattice in $V$. Then the following assertions hold:*

(i) *$L$ is maximal if and only if $[\widetilde{L}/L] = 2\mathfrak{a}\mathfrak{e}_0^2$.*

(ii) *If $L$ is maximal, then there is a unique order of $B$ $\big(= A^+(V)\big)$ of discriminant $\mathfrak{a}_0\mathfrak{e}$ containing $A^+(L)$.*

*Proof.* Let $\Lambda$ be a maximal lattice containing $L$. Since $[\widetilde{L}/L] = [\widetilde{\Lambda}/\Lambda][\Lambda/L]^2$, the "if"-part of (i) follows from the "only if"-part. Clearly the problem can be reduced to the local case. In the local case, we may assume that $d\mathfrak{g}$ equals $\mathfrak{g}$ or the prime ideal $\mathfrak{p}$ of $\mathfrak{g}$. Let $t$ and $M$ be as in §1.4. Then $[\widetilde{L}/L] = [\widetilde{M}/M]$. If $t = 1$, we can easily find $[\widetilde{M}/M]$. Suppose $t = 3$; if $d\mathfrak{g} = \mathfrak{p}$, then the explicit forms of $M$ and $\widetilde{M}$ given in §1.5, (B) show that $[\widetilde{M}/M] = 2\mathfrak{p}$. If $d\mathfrak{g} = \mathfrak{g}$. we have $[\widetilde{M}/M] = 2\mathfrak{p}^2$ as shown in [S3, (7.9)]. This proves (i).

Next, since all the maximal lattices form a genus, it is sufficient to prove (ii) for a special choice of $L$. We take an order $\mathfrak{O}$ in $B$ of discriminant $\mathfrak{a}\mathfrak{e}_0$, and take the $\mathfrak{g}$-lattice $\mathfrak{M}$ in $B$ such that $\mathfrak{M}_v = \widetilde{\mathfrak{O}}_v$ if $v|\mathfrak{a}$ and $\mathfrak{M}_v = \mathfrak{O}_v$ if $v \nmid \mathfrak{a}$. We then put

$$L = \mathfrak{x}^{-1}(\mathfrak{M} \cap B^\circ)\xi, \tag{5.4}$$

Our task is to show that $L$ is maximal and to prove (ii) for this $L$. The problems can be reduced to the local case. For simplicity we fix $v \in \mathbf{h}$ and denote $F_v$ and $\mathfrak{g}_v$ by $F$ and $\mathfrak{g}$, suppressing the subscript $v$. We can take $\mathfrak{x} = \mathfrak{g}$, and $d\mathfrak{g}$ to be $\mathfrak{g}$ or $\mathfrak{p}$. If $B = M_2(F)$ and $d\mathfrak{g} = \mathfrak{g}$, then $\mathfrak{O} = \widetilde{\mathfrak{O}} = M_2(\mathfrak{g})$. If $B = M_2(F)$ and $d\mathfrak{g} = \mathfrak{p}$, then $\mathfrak{O}$ and $\widetilde{\mathfrak{O}}$ can be given by (5.1a, b). Thus, for either type of $d\mathfrak{g}$ we have

$$L = \left\{ \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \,\middle|\, a,\, c \in \mathfrak{g},\, b \in d^{-1}\mathfrak{g} \right\} \cdot \xi, \tag{5.5a}$$

$$\widetilde{L} = \left\{ \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \,\middle|\, a \in (2d)^{-1}\mathfrak{g},\, c \in \mathfrak{g},\, b \in d^{-1}\mathfrak{g} \right\} \cdot \xi, \tag{5.5b}$$

so that $[\widetilde{L}/L] = 2d\mathfrak{g}$, which together with (i) shows that $L$ is maximal. If $v|\mathfrak{e}$, then there is a unique maximal lattice in $V$ given in the form $\{x \in V \mid \varphi[x] \in \mathfrak{g}\}$. It can easily be seen that this coincides with (5.4). Now, in the local case we easily see that $A^+(L) = \mathfrak{O}$ except when $B$ is a division algebra and $d\mathfrak{g} = \mathfrak{g}$, in which case $B$ has a unique order of prime discriminant. This completes the proof.

Lemma 5.4. *In the setting of Lemma 5.3 let $L$ be a maximal lattice in $V$ and let $\mathfrak{O}$ be the order in $B$ of discriminat $\mathfrak{a}_0\mathfrak{e}$ established in Lemma 5.3 (ii). Put*

$$C = \{x \in SO^\varphi(V)_\mathbf{A} \mid Lx = L\}, \tag{5.6}$$

$$T = \{y \in B_\mathbf{A}^\times \mid y\mathfrak{O} = \mathfrak{O}y\}, \quad T_v = B_v^\times \cap T. \tag{5.7}$$

*Then $C = \tau(T)$; moreover, for $v \in \mathbf{h}$ we have $T_v = B_v^\times$ if $v|\mathfrak{e}$, $T_v = F_v^\times \mathfrak{O}_v^\times$ if $v \nmid \mathfrak{a}_0\mathfrak{e}$, and $T_v = F_v^\times(\mathfrak{O}_v^\times \cup \mathfrak{O}_v^\times \eta_v)$ if $v|\mathfrak{a}_0$, where $\eta_v$ is $\eta$ of (5.1b). Furthermore,*

$$\{\gamma \in SO^\varphi(V) \mid L\gamma = L\} = \tau\bigl(\{\alpha \in B^\times \mid \alpha\mathfrak{O} = \mathfrak{O}\alpha\}\bigr). \tag{5.8}$$

*Proof.* The statements about $T_v$ are well known if $\mathfrak{O}_v$ is maximal, that is, if $v \nmid \mathfrak{a}_0$. If $v|\mathfrak{a}_0$, then $\mathfrak{O}_v$ is of type (5.1a), and the desired fact follows from [E2, Satz 5]. To prove $\tau(T) = C$, we first recall the equality $SO^\varphi(V) = \tau\bigl(G^+(V)\bigr)$, which holds over any field. Thus it is sufficient to show that $\tau(T_v) = C_v$ for every $v \in \mathbf{h}$, where $C_v = C \cap SO^\varphi(V)_v$. This is trivial if $v|\mathfrak{e}$, as $C_v = SO^\varphi(V)_v$ and $T_v = B_v^\times$ then. For $v \in \mathbf{h}$ put $D_v = \{\alpha \in B_v^\times \mid \alpha^{-1}L_v\alpha = L_v\}$. Then $\tau(D_v) = C_v$. We have seen in the proof of Lemma 5.3 that $A^+(L_v) = \mathfrak{O}_v$ if $v \nmid \mathfrak{e}$. Therefore if $\alpha \in D_v$ for such a $v$, then $\alpha^{-1}\mathfrak{O}_v\alpha = \mathfrak{O}_v$, and so $\alpha \in T_v$. Conversely, if $\alpha \in T_v$, then $\alpha\mathfrak{O}_v = \mathfrak{O}_v\alpha$ and we easily see that $\alpha\widetilde{\mathfrak{O}}_v = \widetilde{\mathfrak{O}}_v\alpha$.

We may assume that $L$ is of the form (5.4). Since $\mathfrak{M}_v$ is $\mathfrak{O}_v$ or $\widetilde{\mathfrak{O}}_v$, we have $\alpha^{-1}L_v\alpha = L_v$, and so $\alpha \in D_v$. Thus $T_v = D_v$. Since $\tau(D_v) = C_v$, we obtain $\tau(T) = C$. Since $\mathrm{Ker}(\tau) = F_{\mathbf{A}}^\times \subset T$, if $\tau(\alpha) \in C$ with $\alpha \in B^\times$, then $\alpha \in T \cap B^\times$, from which we obtain (5.8).

*Proof of Theorem 1.8.* Since $\tau\bigl(G^+(V)\bigr) = SO^\varphi(V)$, the equality $\tau(T) = C$ stated in (iii) is clear from the definition of $T$. To prove the remaining statements, we first consider the case $n = 3$. Then $C$ of §1.7 and Theorem 1.8 is $C_v$ of Lemma 5.4 with a divisor $v$ of $\mathfrak{a}$, and $A^+(L) = \mathfrak{O}_v$ as noted at the end of the proof of Lemma 5.3. Moreover, by Lemma 5.4, we have $F_v^\times \subset T_v$ and $\tau(T_v) = C_v$, and so $T_v$ coincides with $T$ of our theorem. Thus $T = B_v^\times$ if $v|\mathfrak{e}$ and $T = F_v^\times(\mathfrak{O}_v^\times \cup \mathfrak{O}_v^\times\eta_v)$ if $v|\mathfrak{a}_0$. The last expression for $T$ is valid even for $v|\mathfrak{e}$, if we take $\eta_v$ to be an element of $B_v$ such that $\eta_v^2$ is a prime element of $F_v$. Clearly $J = \mathfrak{O}_v^\times$ and $\nu(J) = \mathfrak{g}_v^\times$; also, all the other statements of our theorem can easily be verified.

Next suppose $n > 3$; using the symbols of (1.4a, b, c), put $W = Z$ and $N = M$ if $t = 3$; put $W = Z + Fe_r + Ff_r$ and $N = M + \mathfrak{g}e_r + \mathfrak{g}f_r$ if $t = 1$. Then $V = W + \sum_{i=1}^u (Fe_i + Ff_i)$ and $L = N + \sum_{i=1}^u (\mathfrak{g}e_i + \mathfrak{g}f_i)$, where $u = r$ if $t = 3$ and $u = r - 1$ if $t = 1$. Observe that $N$ contains an element $g$ such that $\varphi[g] \in \mathfrak{g}^\times$. Therefore, as shown in [S3, §8.2], there exists an isomorphism $\theta$ of $A^+(V)$ onto $M_2\bigl(A^+(W)\bigr)$ such that $\theta\bigl(A^+(L)\bigr) = M_s\bigl(A^+(N)\bigr)$, where $s = 2^u$. Thus (i) and (ii) of our theorem follow from what we proved in the case $n = 3$; namely, $A^+(L)$ can be identified with $M_s(\mathfrak{O})$ with an order $\mathfrak{O}$ as stated. As for (iii) in the general case, clearly $\nu(J) = \mathfrak{g}^\times$. We already found an element $\eta$ of $G^+(W)$ such that $N\tau(\eta) = N$, $\eta^2 \in F^\times$, and $\nu(\eta)\mathfrak{g} = \mathfrak{p}$; also $\eta J = J\eta$ as can easily be seen. Put $T_0 = F^\times(J \cup J\eta)$. Then $T_0$ is a subgroup of $G^+(V)$, $\tau(T_0) \subset C$, and $\nu(T_0) = F^\times$. Let $\alpha \in T$. Take $\beta \in T_0$ so that $\nu(\alpha) = \nu(\beta)$. Then $\nu(\beta^{-1}\alpha) = 1$, and so $\beta^{-1}\alpha \in J$. Thus $\alpha \in \beta J \subset T_0$, and we obtain $T = T_0$ and $C = \tau(T_0) = \tau(J) \cup \tau(J\eta)$. If $\tau(\eta) \in \tau(J)$, then $\eta \in F^\times J$, which is impossible, as $\nu(\eta)\mathfrak{g} = \mathfrak{p}$. Thus $\tau(\eta) \notin \tau(J)$, and so $[C : \tau(J)] = 2$. This completes the proof.

5.5. We now return to $(V, \varphi)$ over a global $F$ of an odd dimension $n > 1$, and fix a maximal lattice $L$ in $V$. For each $v \in \mathbf{h}$ we take an element $\varepsilon_v \in \delta(\varphi_v)$ that is either a unit or a prime element of $F_v$. Then $\varepsilon_v\mathfrak{g}_v^{\times 2}$ is determined by $\varphi_v$, where $\mathfrak{g}_v^{\times 2} = \bigl\{a^2 \bigm| a \in \mathfrak{g}_v^\times\bigr\}$. Given $h \in V$ such that $\varphi[h] \neq 0$, take an element $\beta_v \in F_v$ such that $\varphi(h, L_v) = \beta_v\mathfrak{g}_v$, and put $r_v(h) = \varepsilon_v^{-1}\varphi[h]\beta_v^{-2}$. Then $r_v(h)$ determines a coset of $F_v^\times/\mathfrak{g}_v^{\times 2}$, which depends only on $\varphi_v$, $L$, and $F_v^\times hC(L_v)$. Strictly speaking, $r_v(h)$ should be defined as a coset, but for simplicity we view it as an element of $F_v^\times$, and write $r_v(h) \in X$ or $r_v(h) \in X$ for any subset $X$ of $F_v$ stable under multiplication by the elements of $\mathfrak{g}_v^{\times 2}$. For example, we can take as $X$ the set

$$\mathfrak{E}_v = \bigl\{u^2 + 4w \bigm| u,\, w \in \mathfrak{g}_v\bigr\}. \tag{5.9}$$

Then the condition $r_v(h) \in \mathfrak{E}_v$ is meaningful. Obviously $\mathfrak{E}_v = \mathfrak{g}_v$ if $v \nmid 2$. We can also define $r_v(h)$ for $h \in V_v$.

The following lemma concerns the local case, that is, $v$ is fixed, and so we write $r(h)$ and $\mathfrak{E}$ for $r_v(h)$ and $\mathfrak{E}_v$.

LEMMA 5.6. *Let $(V, \varphi)$, $B$, $\xi$, $d$, and $B^\circ$ be as in §5.2 with a local field $F$ and $B = M_2(F)$; suppose $d$ is a prime element of $F$; let $\mathfrak{O}$ be the order of (5.1a) and $L$ be as in (5.5a); put $C = \{\alpha \in SO^\varphi(V) \mid L\alpha = L\}$. Fixing $h = k\xi$ as in §5.2, put $K = F[k]$, $\mathfrak{f} = K \cap \mathfrak{O}$, $\mathfrak{y} = \widetilde{\mathfrak{O}} \cap K$, $W = (Fh)^\perp$, and*

$$J = \{\alpha \in SO^\varphi(W) \mid (L \cap W)\alpha = L \cap W\}. \tag{5.10}$$

*Then the following assertions hold:*

(i) *$\mathfrak{f}$ is the order of $K$ whose discriminant is $r(h)\mathfrak{p}^2$.*

(ii) *There exists an element $\omega$ of $B^\times$ such that (5.2) is satisfied, $\tau(\omega) \in C$, $W = \omega K\xi$; $L \cap W = \omega\mathfrak{f}\xi$ if $r(h) \notin \mathfrak{p}^{-1}$, and $L \cap W = \omega\mathfrak{y}\xi$ if $r(h) \in \mathfrak{p}^{-1}$.*

(iii) *If $r(h) \notin \mathfrak{p}^{-1}$, then $K \cong F \times F$, $\mathfrak{f}$ is the maximal order of $K$, $L \cap W$ is a maximal lattice in $W$, and $J = SO^\varphi(W) \cap C = \tau(\mathfrak{f}^\times)$.*

(iv) *If $r(h) \in \mathfrak{E}$, then $\mathfrak{y}$ is the order in $K$ whose discriminant is $r(h)\mathfrak{g}$, $\mathfrak{f}$ is not maximal, $J = \tau(\{a \in K^\times \mid a/a^\rho \in \mathfrak{y}^\times\})$, and $SO^\varphi(W) \cap C = \tau(\mathfrak{f}^\times)$.*

(v) *If $r(h) \in \mathfrak{p}^{-1}$ and $r(h) \notin \mathfrak{E}$, then $K$ is ramified over $F$, $\mathfrak{f}$ is the maximal order of $K$, $J = \tau(\{a \in K^\times \mid a/a^\rho \in \mathfrak{f}^\times\})$, and $SO^\varphi(W) \cap C = \{x \in K \mid xx^\rho = 1\}$, which has $\tau(\mathfrak{f}^\times)$ as a subgroup of index 2.*

(vi) *Cases* (iii), (iv), *and* (v) *cover all possibilities for $h$, and mutually exclusive.*

*Proof.* To prove our assertions, we can replace $h$ by any element of $F^\times hC$. Indeed, if we replace $h$ by $ch\tau(\alpha)$ with $c \in F^\times$ and $\alpha$ in the set $T_v$ of (5.7), then $K$, $\mathfrak{f}$, and other symbols are replaced by their images under the inner asutomorphism $x \mapsto \alpha^{-1}x\alpha$ of $A(V)$. Thus we may assume that $2\varphi(h, L) = \mathfrak{g}$. We can take $\begin{bmatrix} 0 & -d^{-1} \\ 0 & 0 \end{bmatrix}\xi$, $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\xi$, and $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\xi$ as the elements $e_1$, $f_1$, and $g$ of §1.6. Therefore the result there guaratees an element $\gamma \in C$ such that $h\gamma = j\xi$ with $j$ of the following two types: (1) $j = \mathrm{diag}[c, -c]$, $2c\mathfrak{p} = \mathfrak{g}$; (2) $j = \begin{bmatrix} c & b \\ 1 & -c \end{bmatrix}$ with $b \in \mathfrak{p}^{-1}$ and $c \in 2^{-1}\mathfrak{g}$. Thus we may assume that $k = j$ with such a $j$. Take $\omega = \begin{bmatrix} 0 & d^{-1} \\ -1 & 0 \end{bmatrix}$ for type (1) and $\omega = \begin{bmatrix} -1 & 2c \\ 0 & 1 \end{bmatrix}$ for type (2). Then $\tau(\omega) \in C$ and $\omega^{-1}k\omega = -k$; also $W = \omega K\xi$ and $L \cap W = (\widetilde{\mathfrak{O}} \cap \omega K)\xi$. We now treat our problems according to the type of $j$.

Type (1). Put $\ell = \mathrm{diag}[2c, 0]$. Then $K = F + F\ell$, as $\ell = j + c$. Clearly $K$ consists of the diagonal matrices, and $\mathfrak{f}$ is its maximal order. Since $2c\mathfrak{p} = \mathfrak{g}$, we have $\mathfrak{f} = \mathfrak{g}[d\ell]$. Now, $\widetilde{\mathfrak{O}} \cap \omega K = \omega(\mathfrak{O} \cap K) = \omega\mathfrak{f}$, so that $L \cap W = \omega\mathfrak{f}\xi$, which is a maximal lattice in $W$. It can easily be seen that $J = SO^\varphi(W) \cap C = \tau(\mathfrak{f}^\times)$. Also, $r(h)\mathfrak{g} = 4c^2\mathfrak{g} = \mathfrak{p}^{-2}$, so that $r(h) \notin \mathfrak{p}^{-1}$, and $r(h)\mathfrak{p}^2 = \mathfrak{g}$, which is the discriminant of $\mathfrak{f}$. Since $r(h) \in \mathfrak{p}^{-1}$ for type (2) as can easily be seen, we have type (1) if and only if $r(h) \notin \mathfrak{p}^{-1}$.

Type (2). For $j$ of type (2), we have $r(h) \in \mathfrak{p}^{-1}$. We easily see that $r(h) \in \mathfrak{E}$ if $b \in \mathfrak{g}$. Conversely suppose $r(h) \in \mathfrak{E}$; then we have $-4\varphi[h] = d(u^2 + 4w)$

with $u$, $w \in \mathfrak{g}$. Put $h' = j'\xi$ with $j' = \begin{bmatrix} u/2 & w \\ 1 & -u/2 \end{bmatrix}$. Then $\varphi[h'] = \varphi[h]$ and $2\varphi(h', L) = \mathfrak{g} = 2\varphi(h, L)$, so that $h' \in hC$ by Theorem 1.3. Thus if $r(h) \in \mathfrak{E}$, then we can put $h = j\xi$ with $j$ of the above form such that $b \in \mathfrak{g}$. Without assuming $b \in \mathfrak{g}$, put $\ell = \begin{bmatrix} 2c & b \\ 1 & 0 \end{bmatrix}$. Then $\ell = c + j$ and $K = F + F\ell$. For $y, z \in F$ we have $y + z\ell = \begin{bmatrix} y + 2cz & bz \\ z & y \end{bmatrix}$. This belongs to $\mathfrak{O}$ if and only if $y \in \mathfrak{g}$ and $z \in \mathfrak{p}$. Thus $\mathfrak{f} = \mathfrak{g}[d\ell]$. This has discriminant $4(b + c^2)\mathfrak{p}^2$, which equals $r(h)\mathfrak{p}^2$. Since $\omega^2 = 1$ and $\omega \in \mathfrak{O}^\times$, we have $L \cap W = \omega(\widetilde{\mathfrak{O}} \cap K)\xi$. We see that $y + z\ell \in \widetilde{\mathfrak{O}}$ if and only if $y \in \mathfrak{g}$ and $z \in \mathfrak{g}$. Thus $\mathfrak{y} = \mathfrak{g} + \mathfrak{g}\ell$ and $L \cap W = \omega\mathfrak{y}\xi$. For $x \in K$ and $a \in K^\times = G^+(W)$, we have $\omega x\xi\tau(a) = \omega ex\xi$, where $e = a/a^\rho$. Thus $(L \cap W)\tau(a) = L \cap W$ if and only if $(a/a^\rho)\mathfrak{y} = \mathfrak{y}$. Also $\tau(a) \in C$ if and only if $\tau(a) = \tau(s)$ with $s \in \mathfrak{O}^\times \cup \mathfrak{O}^\times\eta^{-1}$, as can be seen from Lemma 5.4. If $s \in \mathfrak{O}^\times$, then $a \in F^\times\mathfrak{O}^\times \cap K^\times = F^\times\mathfrak{f}^\times$, so that $\tau(a) \in \tau(\mathfrak{f}^\times)$. If $s \in \mathfrak{O}^\times\eta^{-1}$, then $s \in \mathfrak{O}^\times\eta^{-1} \cap K \subset \mathfrak{y}$.

Suppose now $r(h) \in \mathfrak{E}$; then we may assume that $b \in \mathfrak{g}$. Since $\ell^2 = 2c\ell + b$, we see that $\mathfrak{y}$ is an order, and so $J$ is as in (iv). If $s \in \mathfrak{O}^\times\eta^{-1}$, then $dss^\iota \in \mathfrak{g}^\times$, which is impossible as $\mathfrak{y}$ is an order. Thus $SO^\varphi(W) \cap C = \tau(\mathfrak{f}^\times)$. Since $\mathfrak{f} = \mathfrak{g}[d\ell] \neq \mathfrak{g}[\ell] = \mathfrak{y}$, $\mathfrak{f}$ is not maximal and the discriminant of $\mathfrak{y}$ is $r(h)\mathfrak{g}$. This proves (iv).

Next suppose $r(h) \notin \mathfrak{E}$; then $b \notin \mathfrak{g}$ and $b\mathfrak{p} = \mathfrak{g}$. We easily see that $\ell\mathfrak{f} = \mathfrak{y}$, and so $e\mathfrak{y} = \mathfrak{y}$ if and only if $e \in \mathfrak{f}^\times$. Thus $J$ is as in (v). Put $\pi = b^{-1}$ and $\sigma = \pi\ell$. Then $K = F[\sigma]$. Since $\sigma^2 = 2c\pi\sigma + \pi$, $K$ is ramified over $F$ and its maximal order is $\mathfrak{g}[\sigma]$, which coincides with $\mathfrak{f}$. Now $SO^\varphi(W) = \{x \in K^\times \mid xx^\rho = 1\}$, which has $\tau(\mathfrak{f}^\times)$ as a subgroup of index 2 by a general principle [S3, Lemma 5.6 (iii)]. Since $\ell \in \mathfrak{O}^\times\eta^{-1}$, we have $\tau(\ell) \in SO^\varphi(W) \cap C$. If $\tau(\ell) \in \tau(\mathfrak{f}^\times)$, then $\ell \in F^\times\mathfrak{f}^\times$, which is impossible. Thus $\tau(\mathfrak{f}^\times) \subsetneqq SO^\varphi(W) \cap C \subset SO^\varphi(W)$, which proves (v). Finally (vi) is clear from the above discussion. This completes the proof, as (i) and (ii) have been proved.

If we apply (2.7) to the present setting, then $H = \{b \in K^\times \mid bb^\rho = 1\}$ with $K = F + Fk$ as noted in §5.2. Thus $H$ is commutative and the left-hand side of (2.7) becomes $[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)]$. We can determine this index explicitly as follows.

THEOREM 5.7. *In the setting of §5.2 with a global $F$, let $L$ be a maximal lattice in $V$, and $\mathfrak{e}$ the product of all the prime ideals in $F$ ramified in $B$; put $d\mathfrak{g} = \mathfrak{a}\mathfrak{x}^2$ with a squarefree integral ideal $\mathfrak{a}$ and a fractional ideal $\mathfrak{x}$. Let $\mathfrak{O}$ be the order in $B$ of discriminant $\mathfrak{a} \cap \mathfrak{e}$ containing $A^+(L)$. (See Lemma 5.3 (ii).) Given $h = k\xi \in V$ with $k \in B^\circ$ such that $\varphi[h] \neq 0$, put $K = F + Fk$; denote by $\mathfrak{r}$ the maximal order of $K$ and by $\mathfrak{d}$ the different of $K$ relative to $F$. Let $\mathfrak{a}^*$ be the product of the prime factors $v$ of $\mathfrak{a}$ such that $v \nmid \mathfrak{e}$, $r_v(h) \in \mathfrak{p}_v^{-1}$, and $r_v(h) \notin \mathfrak{E}_v$, where $\mathfrak{p}_v$ is the local prime ideal at $v$. 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 $v|\mathfrak{a}^*\mathfrak{e}$ and $\mathfrak{c}_v^2 N_{K/F}(\mathfrak{d})_v = \mathfrak{a}_v\varphi[h]\varphi(h, L)_v^{-2}$ if $v \nmid \mathfrak{e}$. Moreover,* *put $H = SO^\varphi(W)$ and identify $H$ with $\{\alpha \in K^\times \mid \alpha\alpha^\iota = 1\}$; define $C$ by (5.6). Suppose $K$ is a field; then*

$$\begin{aligned}(5.11)\qquad \bigl[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)\bigr] &= (c_K/c_F)\cdot 2^{1-\mu-\nu}\bigl[\mathfrak{g}^\times : N_{K/F}(\mathfrak{r}^\times)\bigr]\\ &\quad \cdot [U:U']^{-1}N(\mathfrak{c})\prod_{\mathfrak{p}|\mathfrak{c}}\bigl\{1-[K/F,\,\mathfrak{p}]N(\mathfrak{p})^{-1}\bigr\}.\end{aligned}$$

*Here $c_K$ resp. $c_F$ is the class number of $K$ resp. $F$; $\mu$ is the number of prime ideals dividing $\mathfrak{a}^*\mathfrak{e}$ and ramified in $K$; $\nu$ is the number of $v \in \mathbf{a}$ ramified in $K$;*

$$U = \bigl\{x \in \mathfrak{r}^\times \bigm| xx^\rho = 1\bigr\} \quad \textit{and} \quad U' = \bigl\{\, x \in U \bigm| x - 1 \in \mathfrak{c}_v\mathfrak{d}_v \text{ for every } v\nmid\mathfrak{a}^*\mathfrak{e}\,\bigr\};$$

*$\mathfrak{p}$ 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.* If $d \in \mathfrak{g}^\times$, this is [S3, Theorem 12.3]. Our proof here is a modified version of the proof there. For $v|\mathfrak{e}$ we have $\mathfrak{r}_v \subset \mathfrak{O}_v$, so that $\mathfrak{f}_v = \mathfrak{r}_v$ and $\mathfrak{c}_v = \mathfrak{g}_v$. Next suppose $v\nmid\mathfrak{e}$; then we can put $B_v = M_2(F_v)$, and so [S3, Lemma 11.11] is applicable if $v\nmid\mathfrak{a}$; by (i) of that lemma, $\mathfrak{c}_v^2 N_{K/F}(\mathfrak{d})_v = \varphi[h]\varphi(h,\,L)_v^{-2}$. If $v|\mathfrak{a}$, then we use (i) of Lemma 5.6. If $v|\mathfrak{a}^*$, then $\mathfrak{c}_v = \mathfrak{g}_v$ by (v) of Lamma 5.6. Thus we obtain our assertion concerning $\mathfrak{c}$.

To prove (5.11), suppose $K$ is a field. Then we have

$$[H_{\mathbf{A}} : HE] = (c_K/c_F)\cdot 2^{1-\kappa}[\mathfrak{g}^\times : N_{K/F}(\mathfrak{r}^\times)],$$

where $E = H_{\mathbf{a}}\prod_{v\in\mathbf{h}} E_v$ with $E_v = \mathfrak{r}_v^\times \cap H_v$ and $\kappa$ is the number of $v \in \mathbf{v}$ ramified in $K$. Indeed, $[H_{\mathbf{A}} : HE]$ equals the number of classes in the genus of $\mathfrak{g}$-maximal lattices in $W$, and in [S3, (9.16)] we noted that it is the right-hand side of the above equality. 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 $v\nmid\mathfrak{a}^*\mathfrak{e}$, then, by [S3, Lemma 11.11 (iv)] and Lemma 5.6 (iii), (iv), we have $D_v = \tau(\mathfrak{f}_v^\times)$. If $v|\mathfrak{a}^*$, then $D_v = E_v$ by Lemma 5.6 (v). Thus $U \cap D = \bigl\{x \in U \bigm| x \in \tau(\mathfrak{f}_v^\times) \text{ for every } v\nmid\mathfrak{a}^*\mathfrak{e}\bigr\}$. Applying [S3, Lemma 11.10 (iii)] to $\tau(\mathfrak{f}_v^\times)$, we obtain $U \cap D = U'$. Now we have $U = E \cap H$,

$$[HE : HD] = [E : E\cap HD] = [E : UD] = [E : D]/[UD : D] = [E : D]/[U : U\cap D],$$

$$[E : D] = \textstyle\prod_{v\nmid\mathfrak{a}^*\mathfrak{e}}[E_v : D_v] = \prod_{v\nmid\mathfrak{a}^*\mathfrak{e}}\bigl[E_v : \tau(\mathfrak{r}_v^\times)\bigr]\bigl[\tau(\mathfrak{r}_v^\times) : \tau(\mathfrak{f}_v^\times)\bigr].$$

By [S3, Lemma 5.6 (iii)], $\bigl[E_v : \tau(\mathfrak{r}_v^\times)\bigr] = 2$ if $v$ is ramified in $K$, and $= 1$ otherwise. The index $\bigl[\tau(\mathfrak{r}_v^\times) : \tau(\mathfrak{f}_v^\times)\bigr]$ is given by [S3, Lemma 11.10 (i), (iv)]. Thus we obtain

$$[E : D] = 2^b N(\mathfrak{c})\textstyle\prod_{\mathfrak{p}|\mathfrak{c}}\bigl\{1 - [K/F,\,\mathfrak{p}]N(\mathfrak{p})^{-1}\bigr\},$$

where $b$ is the number of the primes $v\nmid\mathfrak{a}^*\mathfrak{e}$ ramified in $K$. Now $[H_{\mathbf{A}} : HD] = [H_{\mathbf{A}} : HE][HE : HD]$. Combining all these, we obtain (5.11).

COROLLARY 5.8. *The notation and assumption being as in Theorem 5.7, let $c(\mathfrak{f})$ denote the class number of $\mathfrak{f}$ in the sense of* [S3, §12.5] *and let $U_\mathfrak{f} = U \cap \mathfrak{f}^\times$. Then $U' \subset U_\mathfrak{f}$ and*

$$(5.12)\quad \big[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)\big] = \big(c(\mathfrak{f})/c_F\big) \cdot 2^{1-\mu-\nu}\big[\mathfrak{g}^\times : N_{K/F}(\mathfrak{f}^\times)\big][U_{\mathfrak{f}} : U']^{-1}.$$

*Proof.* By [S3, Lemma 11.10 (ii) ] we have $U_{\mathfrak{f}} = \{\, x \in U \,|\, x^\rho - x \in \mathfrak{c}\mathfrak{d} \,\}$. Since $\mathfrak{c}$ is prime to $\mathfrak{a}^*\mathfrak{e}$, for $x \in U$ we have $x^\rho - x \in \mathfrak{c}\mathfrak{d}$ if and only if $x^\rho - x \in \mathfrak{c}_v\mathfrak{d}_v$ for every $v \nmid \mathfrak{a}^*\mathfrak{e}$. We have also $x^\rho - x = (1-x)(1+x^\rho)$, and hence $U' \subset U_{\mathfrak{f}}$. Now we recall a well known formula (see [S3, (12.3)])

$$(5.13)\qquad c(\mathfrak{f}) = c_K \cdot [\mathfrak{r}^\times : \mathfrak{f}^\times]^{-1} N(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \big\{1 - [K/F,\, \mathfrak{p}]N(\mathfrak{p})^{-1}\big\}.$$

As shown in [S3, p. 117, line 7], we have

$$(5.14)\qquad [\mathfrak{r}^\times : \mathfrak{f}^\times] = [U : U_{\mathfrak{f}}]\big[N_{K/F}(\mathfrak{r}^\times) : N_{K/F}(\mathfrak{f}^\times)\big].$$

Combining (5.11), (5.13), and (5.14) together, we obtain (5.12).

Theorem 5.9. *In the setting of Lemma 5.4 and Theorem 5.7, the class number of the genus of maximal lattices in the ternary space $(V, \varphi)$ equals the type number of $\mathfrak{O}$.*

*Proof.* We easily see that the type number of $\mathfrak{O}$ equals $\#\{B^\times \backslash B_{\mathbf{A}}^\times / T\}$ with $T$ of (5.7). By Lemma 5.4, $\tau(T) = C$ and clearly $F_{\mathbf{A}}^\times \subset T$, and so $\tau$ gives a bijection of $B^\times \backslash B_{\mathbf{A}}^\times / T$ onto $SO^\varphi(V) \backslash SO^\varphi(V)_{\mathbf{A}} / C$. This proves our theorem.

This theorem should not be confused with the results in [Pe] (Satz 9 and its corollary), which concern the classes with respect to the group of similitudes.

Theorem 5.10. *In the setting of Theorem 5.7, suppose the genus of maximal lattices consists of a single class (which is the case if $\mathfrak{O}$ has type number 1). Put $\Gamma(L) = \{\gamma \in SO^\varphi(V) \,|\, L\gamma = L\}$. Then*

$$(5.15\text{a})\quad \#\big\{L[q,\, \mathfrak{b}]/\Gamma(L)\big\} = \big(c(\mathfrak{f})/c_F\big) \cdot 2^{1-\mu-\nu}\big[\mathfrak{g}^\times : N_{K/F}(\mathfrak{f}^\times)\big][U_{\mathfrak{f}} : U']^{-1}.$$

*Moreover, if $B$ is totally definite, then*

$$(5.15\text{b})\qquad \#L[q,\, \mathfrak{b}]/\#\Gamma(L) = \big(c(\mathfrak{f})/c_F\big) \cdot 2^{1-\mu-\nu}\big[\mathfrak{g}^\times : N_{K/F}(\mathfrak{f}^\times)\big]\#(U_{\mathfrak{f}})^{-1}.$$

*Proof.* The left-hand side of (2.7) in the present case is $\big[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)\big]$, as $H$ is commutative; the right-hand side consists of a single term. Thus (2.7) combined with (5.12) gives (5.15a). Since $H \cap C = U \cap D = U'$, we have $\mathfrak{m}(H,\, H_{\mathbf{A}} \cap C) = \big[H_{\mathbf{A}} : H(H_{\mathbf{A}} \cap C)\big]\#(U')^{-1}$, which together with (3.7) and (5.15a) proves (5.15b).

Lemma 5.11. *Let $B$ be a quaternion algebra over a global field $F$, and $\mathfrak{e}$ the product of all the prime ideals in $F$ ramified in $B$; let $\mathfrak{a}_0$ be a squarefree integral ideal prime to $\mathfrak{e}$. Further let $K$ be a quadratic extension of $F$ contained in $B$ and $\mathfrak{f}$ an order in $K$ containing $\mathfrak{g}$ that has conductor $\mathfrak{c}$. Then there exists an order $\mathfrak{O}$ in $B$ of discriminant $\mathfrak{a}_0\mathfrak{e}$ such that $\mathfrak{O} \cap K = \mathfrak{f}$ if and only if $\mathfrak{c} + \mathfrak{e} = \mathfrak{g}$ and every prime factor of $\mathfrak{a}_0$ not dividing $\mathfrak{c}$ does not remain prime in $K$.*

This is due to Eichler [E2, Satz 6].

Lemma 5.12. *Let $B$, $\mathfrak{e}$, $\mathfrak{a}_0$, $K$, $\mathfrak{f}$ and $\mathfrak{c}$ be as in Lemma 5.11; let $\mathfrak{O}$ be an order in $B$ of discriminant $\mathfrak{a}_0\mathfrak{e}$. Suppose that $\mathfrak{O}$ has type number 1, $\mathfrak{c}+\mathfrak{e}=\mathfrak{g}$ and every prime factor of $\mathfrak{a}_0$ not dividing $\mathfrak{c}$ does not remain prime in $K$. Then there exists an element $\alpha$ of $B^\times$ such that $\alpha^{-1}\mathfrak{O}\alpha\cap K=\mathfrak{f}$.*

*Proof.* Since $\mathfrak{O}$ has type number 1, every order in $B$ of discriminant $\mathfrak{a}_0\mathfrak{e}$ is of the form $\alpha^{-1}\mathfrak{O}\alpha$ with $\alpha\in B^\times$. Therefore our assertion follows from Lemma 5.11.

## 6. Positive definite ternary forms over $\mathbf{Q}$

6.1. Every positive definite ternary quadratic space $(V,\,\varphi)$ over $\mathbf{Q}$ is obtained by taking $B$ to be a definite quaternion algebra over $\mathbf{Q}$ and $d$ to be a squarefree positive integer in the setting of §5.2. If we represent $\varphi$ with respect to a $\mathbf{Z}$-basis of an integral $\mathbf{Z}$-lattice $L$ in $V$, then we obtain a $\mathbf{Z}$-valued ternary form. If $L$ is maximal, then the form is *reduced* in the sense that it cannot be represented nontrivially by another $\mathbf{Z}$-valued ternary form, and vice versa. This definition of a reduced form is different from Eisenstein's terminology for ternary forms.

Define $\mathfrak{a}$ and $\mathfrak{e}$ as in §5.2. Then $\mathfrak{a}=d\mathbf{Z}$ and $\mathfrak{e}=e\mathbf{Z}$ with a squarefree positive integer $e$. We have $\mathfrak{e}\cap\mathfrak{a}=d_0e\mathbf{Z}$ with a positive divisor $d_0$ of $d$ prime to $e$. Thus $\mathfrak{O}$ of Theorem 5.7 is an order of discriminant $d_0e$. The pair $(e,\,d)$ determines the isomorphism class of $(V,\,\varphi)$ and hence the genus of a reduced $\mathbf{Z}$-valued ternary form. If $\Phi$ is a matrix which represents a ternary form belonging to that genus, then $\det(2\Phi)=2d_0^2e^2/d$; this follows from Lemma 5.3 (i). As to the general theory of reduced forms and $\det(2\Phi)$ for an arbitrary $n$, the reader is referred to [S5]. Taking a maximal lattice $L$ in $V$, put $C=\bigl\{SO^\varphi(V)_\mathbf{A}\bigm| L\alpha=L\bigr\}$. Then we have

Lemma 6.2. $$\mathfrak{m}\bigl(SO^\varphi(V),\,C\bigr)=\frac{1}{12}\prod_{p|e}\frac{p-1}{2}\prod_{p|d_0}\frac{p+1}{2}.$$

*Proof.* Define a quadratic form $\beta$ on $B^\circ$ by $\beta[x]=xx^\iota$ for $x\in B^\circ$; put $G=SO^\beta(B^\circ)$. Then $x\mapsto x\xi$ for $x\in B^\circ$ gives an isomorphism of $(B^\circ,\,d\beta)$ onto $(V,\,\varphi)$, and also an isomorphism of $G$ onto $SO^\varphi(V)$. Moreover, for $\alpha\in B^\times$ we have $\alpha^{-1}x\alpha\xi=\alpha^{-1}x\xi\alpha$. Thus the symbol $\tau(\alpha)$ is consistent. We can identify $C$ with the subgroup $\bigl\{\gamma\in G_\mathbf{A}\bigm|(\mathfrak{M}\cap B^\circ)\gamma=(\mathfrak{M}\cap B^\circ)\bigr\}$ of $G_\mathbf{A}$, where $\mathfrak{M}$ is as in (5.4). Let $\mathfrak{O}_0$ be a maximal order in $B$ containing $\mathfrak{O}$; put $M=\mathfrak{O}_0\cap B^\circ$ and $D=\bigl\{\gamma\in G_\mathbf{A}\bigm| M\gamma=M\bigr\}$. Then $M$ is a maximal lattice with respect to $\beta$, and from [S2, Theorem 5.8] we obtain

$$\mathfrak{m}(G,\,D)=\frac{1}{12}\prod_{p|e}\frac{p-1}{2}. \tag{6.1}$$

By (3.3) we have $[C:C\cap D]\mathfrak{m}(G,\,C)=\mathfrak{m}(G,\,C\cap D)=[D:C\cap D]\mathfrak{m}(G,\,D)$. Clearly $D_p=C_p$ if $p\nmid d_0$. Suppose $p|d_0$; then we can put $B_p=M_2(\mathbf{Q}_p)$, $(\mathfrak{O}_0)_p=M_2(\mathbf{Z}_p)$, $D_p=\tau\bigl(GL_2(\mathbf{Z}_p)\bigr)$, and $\mathfrak{O}_p$ is of the type (5.1a). From Lemma 5.4 we obtain $[C_p:C_p\cap D_p]=2$ and $[D_p:C_p\cap D_p]=p+1$.

Thus $\mathfrak{m}(G, C) = \mathfrak{m}(G, D)\prod_{p|d_0}\{(p+1)/2\}$. Combining this with (6.1), we obtain our lemma.

6.3. Now Eichler gave a formula for the class number of $\mathfrak{O}$ and also a formula for the type number of $\mathfrak{O}$ in [E2, (64)]. However, his formula for the type number is not completely correct, and correct formulas were given by Peters in [Pe] and by Pizer in [Pi]. There is a table for the type number of $\mathfrak{O}$ for $d_0e \le 30$ in [Pe, p. 360]; a larger table for $d_0e \le 210$ is given at the end of [Pi]; in these papers, $e$ and $d_0$ are denoted by $q_1$ and $q_2$. From these tables we see that the type number of $\mathfrak{O}$ for $d_0e \le 210$ is 1 exactly when $(e, d_0)$ is one of the following 20 pairs:

$$(2,\,1),\,(2,\,3),\,(2,\,5),\,(2,\,7),\,(2,\,11),\,(2,\,23),\,(2,\,15),\,(3,\,1),\,(3,\,2),\,(3,\,5),$$
$$(3,\,11),(5,\,1),\,(5,\,2),\,(7,\,1),\,(7,\,3),\,(13,\,1),\,(30,\,1),\,(42,\,1),\,(70,\,1),\,(78,\,1).$$

Now $d$ is $d_0$ times a factor of $e$. Therefore if $e$ has exactly $t$ prime factors, then there are $2^t$ choices for $(e, d)$ with the same $(e, d_0)$. Consequently there are exactly 64 choices for $(e, d)$ obtained from the above 20 pairs of $(e, d_0)$, and each $(e, d)$ determines $(V, \varphi)$; $\det(2\Phi) = 2d_0^2e^2/d$ as noted in §6.1. By Theorem 5.9, $\#\{SO^\varphi(V)\backslash SO^\varphi(V)_\mathbf{A}/C\} = 1$ in all these cases. We have actually

Theorem 6.4. *The spaces $(V, \varphi)$ obtained from these 64 pairs $(e, d)$ exhaust all positive definite ternary quadratic spaces over $\mathbf{Q}$ for which the genus of maximal lattices has class number 1. In other words, there are exactly 64 genera of positive definite, $\mathbf{Z}$-valued, and reduced ternary forms consisting of a single class.*

*Proof.* Our task is to show that the class number is not 1 for $d_0e > 210$. If the inverse of the right-hand side of the equality of Lemma 6.2 is not an integer, then the class number cannot be 1. For $d_0e > 210$, the inverse is an integer exactly when $(e, d_0)$ is one of the following six: $(2\cdot 7\cdot 17,\,1)$, $(2\cdot 5\cdot 13,\,3)$, $(2\cdot 3\cdot 17,\,5)$, $(2\cdot 3\cdot 13,\,7)$, $(2\cdot 3\cdot 5,\,23)$, $(2\cdot 3\cdot 5,\,11)$. The verification is easy, as the mass $\le 1$ for relatively few cases of $(e, d_0)$. Among those six, the mass is $1/2$ for the last one; in the other five cases the mass is 1. Now, by the formula in [Pe, p. 361] the type number of $\mathfrak{O}$ (which is the class number in question by virtue of Theorem 5.9) is given by $2^{-\kappa}\sum_t Sp\{P^*(t)\}$, where $\kappa$ is the number of prime factors of $d_0e$, $t$ runs over all positive divisors of $d_0e$, and $Sp\{P^*(t)\}$ is given on the same page. From the formulas there we can easily verify that $Sp\{P^*(1)\} = 2^\kappa$ and $Sp\{P^*(d_0e)\} > 0$ in the first five cases, and hence the type number is greater than 1. As for the last case $(2\cdot 3\cdot 5,\,11)$, computing $Sp\{P^*(t)\}$ for all $t|d_0e$, we find that the type number is 2. Thus we obtain our theorem.

Remark. In the setting of §6.1, if $\det(2\Phi)/2$ is squarefree, then $\Phi$ must be reduced and $\det(2\Phi)/2 = d = d_0e$ with squarefree $d_0$ and $e$. If the genus of $\Phi$ has class number 1, then in view of the above theorem such a $\Phi$ is obtained from one of the pairs listed in §6.3 by taking $d = d_0e$. Thus there are exactly 20 genera of $\mathbf{Z}$-valued positive definite ternary forms with class number 1 such that $\det(2\Phi)/2$ is squarefree. This result was obtained by Watson [W], and we derived it from a stronger result, Theorem 6.4.

6.5. We are going to specialize Theorem 5.7 and (5.15b) to these cases, and give explicit formulas for $\#L[q, \mathbf{Z}]$. For simplicity, we consider only the cases in which $e$ is a prime, and $d_0$ is 1 or a prime; thus we consider only 15 pairs $(e, d_0)$, and consequently 30 pairs $(e, d)$ with $d = d_0$ or $d = d_0e$. In this setting we have

$$\#\{\Gamma(L)\} = 48/[(d_0+1)(e-1)]. \tag{6.2}$$

This is because $\#\{\Gamma(L)\}$ equals the inverse of the quantity of Lemma 6.2, as the class number is 1.

To study the nature of $q$ for which $L[q, \mathbf{Z}] \neq \emptyset$, we consider the localization of $B$ at $e$. Let $\mathfrak{r}$ denote the maximal order in the unramified quadratic extension of $\mathbf{Q}_e$. We can put $B_e^\circ = \mathbf{Q}_e\sigma + \mathbf{Q}_e\eta$, $\mathfrak{O}_e = \mathfrak{r} + \mathfrak{r}\eta$, and $\widetilde{\mathfrak{O}}_e = \mathfrak{r} + \mathfrak{r}\eta^{-1}$ with $\sigma$ and $\eta$ as in (B) of §1.5; we can take $\eta^2 = e$, though this is often unnecessary. We have $L = (\mathfrak{M} \cap B^\circ)\xi$, and so

$$L_e = (\mathbf{Z}_e\sigma + \mathfrak{r}\eta)\xi \quad \text{and} \quad \widetilde{L}_e = (2^{-1}\mathbf{Z}_e\sigma + \mathfrak{r}\eta^{-1})\xi \quad \text{if} \quad e \nmid d, \tag{6.3a}$$

$$L_e = (\mathbf{Z}_e\sigma + \mathfrak{r}\eta^{-1})\xi \quad \text{and} \quad \widetilde{L}_e = ((2e)^{-1}\mathbf{Z}_e\sigma + \mathfrak{r}\eta^{-1})\xi \quad \text{if} \quad e | d. \tag{6.3b}$$

Here is an easy fact: given an element $\eta_0$ of $B_e^\times$ such that $\eta_0^2$ is a prime element, we can find an element $\alpha$ of $B_e^\times$ such that (6.3a, b) are true with $(\alpha^{-1}\sigma\alpha, \alpha^{-1}\mathfrak{r}\alpha, \eta_0)$ in place of $(\sigma, \mathfrak{r}, \eta)$. Indeed, since $\eta_0^2/\eta^2 \in \mathbf{Z}_e^\times$, we have $\eta_0^2/\eta^2 = aa^\iota$ with $a \in \mathfrak{r}^\times$. Then $\eta_0^2 = (a\eta)^2$, and hence there exists an element $\alpha$ of $B_e^\times$ such that $\alpha^{-1}a\eta\alpha = \eta_0$. Since $\alpha^{-1}L_e\alpha = L_e$ and $\alpha^{-1}\widetilde{L}_e\alpha = \widetilde{L}_e$, we obtain the desired result.

THEOREM 6.6. *Given $0 < q \in \mathbf{Q}$ in the setting of §6.5, put $K_0 = \mathbf{Q}(\sqrt{-dq}\,)$ and denote by $\delta$ the discriminant of $K_0$. Then the following assertions hold:*

(i) *$L[q, \mathbf{Z}] \neq \emptyset$ only if $q$ is as follows:*

$$d_0eq = r^2m \quad \textit{when} \quad e \neq 2 \quad \textit{or} \quad e|d, \tag{6.4a}$$

$$d_0q = r^2m \quad \textit{when} \quad e = 2 \quad \textit{and} \quad e \nmid d. \tag{6.4b}$$

*Here $m$ is a squarefree positive integer such that $e$ does not split in $K_0$, and also that $m - 3 \in 8\mathbf{Z}$ if $e = 2$ and $2|d$; $r$ is a positive integer prime to $e$.*

(ii) *Moreover, put $a^* = d_0$ in the following two cases:* (A) $d_0 \geq 2$, $d_0|m$, *and* $d_0 \nmid r$; (B) $d_0 = 2$, $r - 2 \in 2\mathbf{Z}$, *and 2 is ramified in $K_0$; put $a^* = 1$ if neither* (A) *nor* (B) *applies. Let $\mathfrak{C}$ be the set of all positive integers $c$ prime to $a^*e$ such that $d_0|c$ if $d_0$ is a prime that remains prime in $K_0$. (Thus $\mathfrak{C}$ depends on $d$, $e$, and $q$.) Then $r/2 \in \mathfrak{C}$ if $4|\delta$ and $e \neq 2$; $r \in \mathfrak{C}$ otherwise.*

(iii) *Conversely, given $r$ and $m$ satisfying all these conditions, determine $q$ by (6.4a, b). Then $L[q, \mathbf{Z}] \neq \emptyset$.*

Notice that $K_0 = \mathbf{Q}(\sqrt{-m}\,)$ if $e|d$ or $e = 2$, and $K_0 = \mathbf{Q}(\sqrt{-em}\,)$ otherwise. Also, $\mathfrak{C} = \emptyset$ if $a^*$ is a prime that remains prime in $K_0$.

*Proof.* Suppose $h = k\xi \in L[q, \mathbf{Z}]$ with $k \in B^\circ$; put $K = F[k]$ as in §5.2 and $\mathfrak{f} = K \cap \mathfrak{O}$; let $c$ be the conductor of $\mathfrak{f}$. Then $K \cong K_0$ and $h \in 2\widetilde{L}$. Then from (6.3a, b) we see that $eq \in \mathbf{Z}_e$ if $e \neq 2$ or $e|d$, and $q \in \mathbf{Z}_e$ otherwise. The set $\widetilde{L}_p$ for $p \neq e$ can be given by (5.5b), and so $dq \in \mathbf{Z}_p$. Thus $d_0eq \in \mathbf{Z}$ if $e \neq 2$ or $e|d$; $d_0q \in \mathbf{Z}$ otherwise. Take $0 < r \in \mathbf{Z}$ and a squarefree positive integer $m$ as in (6.4a, b). Define $\mathfrak{a}^*$ as in Theorem 5.7 and put $\mathfrak{a}^* = a^*\mathbf{Z}$ with $0 < a^* \in \mathbf{Z}$. Clearly $a^* = 1$ if $d_0 = 1$. Suppose $d_0$ is a prime number. To make our exposition easier, denote this prime by $s$; then $s \neq e$ and $r_s(h) = -d^{-1}q$. We can easily verify that $a^* = s$ exactly in Cases (A) and (B) stated in (ii) above. By Theorem 5.7 and Lemma 5.11, we see that $c \in \mathfrak{C}$. Notice that $s$ is ramified in $K_0$ if $a^* = s$.

(1) We first consider the case $e|d$. Then $d = d_0e$ and $dq = d_0eq$ and so $K \cong \mathbf{Q}(\sqrt{-m}\,)$. Suppose $e|r$; put $\ell = e^{-1}k$. Then $d^2\ell\ell^\iota = de^{-2}q = (r/e)^2m \in \mathbf{Z}$, and hence $d\ell \in \mathfrak{O}_e \cap B^\circ$. Thus $\ell \in e^{-1}\mathfrak{O}_e \cap B^\circ = e^{-1}\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r}$, and so $\ell\xi \in 2\widetilde{L}_e$ by (6.3b). Therefore $h = e\ell\xi \in 2e\widetilde{L}_e$, which implies that $\varphi(h, L)_e \subset e\mathbf{Z}_e$, a contradiction. Thus $e{\nmid}r$.

(2) Next suppose $e \nmid d$; then $d = d_0$. Assuming $e|r$, put $\ell = e^{-1}k$. Then $d^2\ell\ell^\iota = de^{-2}q \in e^{-1}\mathbf{Z}_e$, and hence $\ell \in \widetilde{\mathfrak{O}}_e \cap B^\circ = \mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r}$. Thus $\ell\xi \in 2\widetilde{L}_e$ by (6.3a), which leads to a contradiction for the same reason as in Case (1). Therefore $e{\nmid}r$ in this case too. This reasoning is valid even when $e = 2$.

(3) Since $K_0$ must be embeddable in $B$, the prime $e$ cannot split in $K_0$. Suppose $e = 2$, $e|d$, and $e|m$. Since $kk^\iota = d^{-2}r^2m$, we have $k \in \eta^{-1}\mathfrak{O}_e^\times \cap B^\circ$, so that $k = a\sigma + \eta^{-1}b$ with $a \in \mathbf{Z}_e$ and $b \in \mathfrak{r}$. Since $\eta k \in \mathfrak{O}_e^\times$, we have $b \in \mathfrak{r}^\times$. By (6.3b), $2\varphi(h, L)_e = 2\mathrm{Tr}_{B/F}\big(k(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\big) = 4a\mathbf{Z}_e + \mathrm{Tr}_{K/\mathbf{Q}}(b\mathfrak{r}) = \mathbf{Z}_e$, a contradiction. Therefore $m$ must be odd if $e = 2$ and $e|d$. In this case, $k \in 2^{-1}\mathfrak{O}_e^\times \cap B^\circ$, so that $2k = x\sigma + \eta y$ with $x \in \mathbf{Z}_e^\times$ and $y \in \mathfrak{r}$. Thus $2\mathbf{Z}_e = 2\varphi(h, L)_e = 2\mathrm{Tr}_{B/F}\big(k(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\big) = 2\mathbf{Z}_e + \mathrm{Tr}_{K/\mathbf{Q}}(y\mathfrak{r})$, so that $y \in 2\mathfrak{r}$. Now $r^2m = dq = d^2kk^\iota = -d_0^2(x^2\sigma^2 + 2yy^\iota)$. We can take $\mathfrak{r} \subset \mathbf{Q}_2(\sqrt{5}\,)$ and $\sigma = \sqrt{5}$. Therefore we see that $m - 3 \in 8\mathbf{Z}$. Thus we obtain the condition on $m$ as stated in our theorem.

(4) By Theorem 5.7, $c$ is prime to $a^*e$ and $c^2\delta\mathbf{Z}_p = d_0q\mathbf{Z}_p = r^2m\mathbf{Z}_p$ for every $p \neq e$. We have seen that $r$ is prime to $e$. First suppose $4|\delta$ and $e \neq 2$. Then we see that $\delta\mathbf{Z}_p = 4m\mathbf{Z}_p$ for $p \neq e$, and so $4c^2\mathbf{Z}_p = r^2\mathbf{Z}_p$ for $p \neq e$. Since both $2c$ and $r$ are prime to $e$, we obtain $2c = r$. Similarly we easily find that $c = r$ if $4{\nmid}\delta$ or $e = 2$. Thus we obtain (ii). This completes the proof of the "if"-part.

(5) Conversely, suppose $q$ is given with $r$ and $m$ as in our theorem; put $c = r/2$ or $c = r$ according as $r/2 \in \mathfrak{C}$ or $r \in \mathfrak{C}$. Let $\mathfrak{o}$ be the order in $K_0$ whose conductor is $c$. By Lemma 5.12, our conditions on $r$ and $m$ guarantees an injection $\theta$ of $K_0$ into $B$ such that $\theta(\mathfrak{o}) = \theta(K_0) \cap \mathfrak{O}$. Our task is to find an element $h$ such that $\varphi[h] = q$ and $\varphi(h, L) = \mathbf{Z}$. Put $\mu = \theta(\sqrt{-m}\,)$ if $K_0 = \mathbf{Q}(\sqrt{-m}\,)$.

(5a) First we consider the case $e|d$ and $|\delta| = m$. Then $d = d_0e$, $r = c$, and $K_0 = \mathbf{Q}(\sqrt{-m}\,)$. Put $h = k\xi$ with $k = d^{-1}r\mu$. Then $\varphi[h] = q$ and by Theorem 5.7, $dq\varphi(h, L)_p^{-2} = c^2\delta\mathbf{Z}_p = r^2m\mathbf{Z}_p$ for every $p \neq e$, so that $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq e$. Now $2\varphi(h, L)_e = d\mathrm{Tr}_{B/F}\big(k(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\big) = \mathrm{Tr}_{B/F}\big(\mu(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\big)$ by (6.3b). If $e|m$, then we can take $\mu$ as $\eta$, changing $\mathfrak{r}$ by an inner automorphism, as noted after (6.3b). (Since $|\delta| = m$, we have $e \neq 2$.) If $e \nmid m$, then we can take $\mathfrak{r} \subset \theta(K_0)_e$ and $\sigma = \mu$. In either case we easily see that $2\varphi(h, L)_e = 2\mathbf{Z}_e$. Thus $\varphi(h, L) = \mathbf{Z}$, and $L[q, \mathbf{Z}] \neq \emptyset$ as expected.

(5b) Next suppose $e|d$ and $|\delta| = 4m$; then $r = 2c$ if $e \neq 2$ and $r = c$ if $e = 2$. We have $K_0 = \mathbf{Q}(\sqrt{-m}\,)$ and we again take $h = k\xi$ with $k = d^{-1}r\mu$. Then $\varphi[h] = q$ and $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq e$ for the same reason as in (5a). If $e \neq 2$, the same argument as in (5a) shows that $\varphi(h, L)_e = \mathbf{Z}_e$, which leads to the desired result. Thus suppose $e = 2$. Then $m-3 \in 8\mathbf{Z}$ as stipulated in our theorem. We can take $\sigma = \sqrt{5}$ as we did in (3). Put $\mu = a\sigma + \eta b$ with $a \in \mathbf{Z}_e$ and $b \in \mathfrak{r}$. Then $a \in \mathbf{Z}_e^\times$ and $-m = a^2\sigma^2 + 2bb^\rho$. Since $m+\sigma^2 \in 8\mathbf{Z}_e$, we see that $b \in 2\mathfrak{r}$. Thus $2\varphi(h, L)_e = \mathrm{Tr}_{B/F}\big(\mu(\mathbf{Z}_e\sigma + \eta^{-1}\mathfrak{r})\big) = 2\mathbf{Z}_e + \mathrm{Tr}_{K/\mathbf{Q}}(b\mathfrak{r}) = 2\mathbf{Z}_e$, which gives the expected result.

(5c) Suppose $e \nmid d$ and $e = 2$. Then $d = d_0$ and $K_0 = \mathbf{Q}(\sqrt{-m}\,)$; we take $h = k\xi$ with $k = d^{-1}r\mu$. We find that $\varphi[h] = q$ and $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq 2$ in the same manner as in (5a). Now $2\varphi(h, L)_2 = \mathrm{Tr}_{B/F}\big(\mu(\mathbf{Z}_2\sigma + \eta\mathfrak{r})\big)$ by (6.3a). If $2|m$, then taking $\mu$ as $\eta$, we obtain $2\varphi(h, L)_2 = 2\mathbf{Z}_2$ as expected. Suppose $2 \nmid m$; then $\mu = a\sigma + \eta b$ with $a \in \mathbf{Z}_2^\times$ and $b \in \mathfrak{r}$, and so $\mathrm{Tr}_{B/F}\big(\mu(\mathbf{Z}_2\sigma + \eta\mathfrak{r})\big) = 2\mathbf{Z}_2$, which gives the desired result.

(5d) Finally suppose $e \nmid d$ and $e \neq 2$. Then $d = d_0$ and $K_0 = \mathbf{Q}(\sqrt{-em}\,)$; we take $h = k\xi$ with $k = \theta(d^{-1}e^{-1}r\sqrt{-em}\,)$; then $\varphi[h] = q$. For $p \neq e$, $\delta\mathbf{Z}_p$ equals $m\mathbf{Z}_p$ or $4m\mathbf{Z}_p$, and $r = c$ or $r = 2c$ accordingly. Then we easily see that $\varphi(h, L)_p = \mathbf{Z}_p$ for every $p \neq e$ in the same manner as in (5a). Now $2\varphi(h, L)_e = \mathrm{Tr}_{B/F}\big(e^{-1}\theta(\sqrt{-em}\,)(\mathbf{Z}_2\sigma + \eta\mathfrak{r})\big)$. If $e|m$, then we can put $\theta(\sqrt{-em}\,) = e(a\sigma + \eta b)$ with $a \in \mathbf{Z}_e^\times$ and $b \in \mathfrak{r}$, and obtain $\varphi(h, L)_e = \mathbf{Z}_e$. If $e \nmid m$. then taking $\eta = \theta(\sqrt{-em}\,)$, we obtain the desired result. This completes the proof.

THEOREM 6.7. *If $L[q, \mathbf{Z}] \neq \emptyset$ in the setting of Theorem 6.6, then*

$$\#L[q, \mathbf{Z}] = \frac{2^{1-\mu} \cdot 48 \cdot \mathbf{c}(K_0)}{(d_0+1)(e-1)w} \cdot c\prod_{p|c}\big\{1 - [K_0/\mathbf{Q}, p]p^{-1}\big\}.$$

*Here $\mu$ is the number of prime factors of $a^*e$ ramified in $K_0$; $\mathbf{c}(K_0)$ is the class number of $K_0$; $w$ is the number of roots of unity in $K$; $c = r/2$ if $4|\delta$ and $e \neq 2$; $c = r$ otherwise; $[K_0/\mathbf{Q}, p]$ is defined as in Theorem 5.7.*

*Proof.* Specialize (5.15b) to the present case. Then $[U : 1] = w$ and $\#\Gamma(L)$ is given by (6.2); $c(\mathfrak{f})$ can be connected to $\mathbf{c}(K_0)$ by (5.13) and (5.14). Thus we obtain our formula.

6.8. Before discussing examples, let us insert here a remark applicable to $(V, \varphi)$ over $\mathbf{Q}$ with an arbitrary $n$. If $F = \mathbf{Q}$ and $\mathfrak{g} = \mathbf{Z}$, it is natural to consider $L[q, \mathbf{Z}]$, but it is not always best to formulate the result with respect to a $\mathbf{Z}$-basis of $L$. To see this, first take the standard basis $\{e_i\}_{i=1}^n$ of $\mathbf{Z}^n = L$, and define a matrix $\Phi$ by $\Phi = [\varphi(e_i,\, e_j)]_{i,j=1}^n$; put $f_i = e_i\Phi^{-1}$. Then $2\widetilde{L} = \sum_{i=1}^n \mathbf{Z}f_i$. Let $h \in L[q,\, \mathbf{Z}]$. Then $h \in 2\widetilde{L}$, and so $h = \sum_{i=1}^n a_i f_i$ with $a_i \in \mathbf{Z}$. We easily see that $\varphi(h,\, L) = \mathbf{Z}$ if and only if $\sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z}$, and also that $\Phi^{-1} = [\varphi(f_i,\, f_j)]_{i,j=1}^n$. This means that

$$L[q,\, \mathbf{Z}] = \left\{ \sum_{i=1}^n a_i f_i \;\middle|\; a\Phi^{-1} \cdot {}^t a = q,\ \sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z} \right\}, \quad a = (a_i)_{i=1}^n. \tag{6.5}$$

Therefore if we follow the traditional definition of primitivity, we have to use the matrix $\Phi^{-1}$ instead of $\Phi$. Recall that $\Gamma(L) = \Gamma(\widetilde{L})$. Thus $\Gamma(L)$ can be represented, with respect to the basis $\{f_i\}_{i=1}^n$, by the group

$$\Gamma' = \left\{ \gamma \in SL_n(\mathbf{Z}) \;\middle|\; \gamma\Phi^{-1} \cdot {}^t\gamma = \Phi^{-1} \right\}. \tag{6.6}$$

Consequently, $L[q,\, \mathbf{Z}]/\Gamma(L)$ corrresponds to the vectors $a$ such that $a\Phi^{-1} \cdot {}^t a = q$ and $\sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z}$, considered modulo $\Gamma'$. We note here an easy fact:

$$|\det(2\Phi)| = [\widetilde{L} : L]. \tag{6.7}$$

6.9. Let us now illustrate Theorem 6.6 by considering five examples and formulating the results in terms of the matrix $\Phi^{-1}$ of §6.8. For $(e,\, d) = (2,\, 1)$ we obtain the result on sums of three squares, which Gauss treated; we do not include this in our examples, as it is easy and too special. Indeed, in this case we have $\Phi = \Phi^{-1}$, and so the result concerns the primitive solutions of $\sum_{i=1}^3 x_i^2 = q$. But in all other cases, $\Phi \neq \Phi^{-1}$, and the results have more interesting features. From Lemma 5.3 (i) and (6.7) we obtain $\det(2\Phi) = 2d_0^2e^2/d$. In each case we state only the condition for $L[q,\, \mathbf{Z}] \neq \emptyset$. We will dispense with the statement about $\#L[q,\, \mathbf{Z}]$, as it is merely a specialization of Theorem 6.7.

(1) We first take $e = d = 3$ in Theorem 6.6. Then

$$2\Phi = \mathrm{diag}\left[2,\ \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 3\Phi^{-1} = \mathrm{diag}\left[3,\ \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}\right]. \tag{6.8}$$

These forms of matrices can be obtained by analyzing $L$ of (5.4) in the present case. Alternatively, since $\det(2\Phi) = 6$ for $\Phi$ of (6.8), we can conclude that $\Phi$ is the matrix representing $\varphi$ by the principle explained in [S5]. Theorem 6.6 (or the form of $\Phi^{-1}$) in the present case shows that $L[q,\, \mathbf{Z}] \neq \emptyset$ only when $3q \in \mathbf{Z}$. Thus with $s = 3q \in \mathbf{Z}$, the principle of §6.8 says that $L[s/3,\, \mathbf{Z}]$ corresponds to the set of vectors $(x,\, y,\, z)$ such that

$$3x^2 + 4(y^2 + yz + z^2) = s \quad \text{and} \quad x\mathbf{Z} + y\mathbf{Z} + z\mathbf{Z} = \mathbf{Z}. \tag{6.9}$$

Theorem 6.6 specialized to this case means that given $0 < s \in \mathbf{Q}$, we can find $(x,\, y,\, z)$ satisfying (6.9) if and only if $s = r^2m$ with a squarefree positive integer $m$ such that $m + 1 \notin 3\mathbf{Z}$ and a positive integer $r$ prime to 3 such that $2|r$ if $m + 1 \notin 4\mathbf{Z}$; $K_0 = \mathbf{Q}(\sqrt{-m}\,)$.

(2) Next we take $e = 3$ and $d = 1$. Then

$$2\Phi = \mathrm{diag}\left[6,\ \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 3\Phi^{-1} = \mathrm{diag}\left[1,\ \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}\right]. \tag{6.10}$$

Therefore $L[s/3,\, \mathbf{Z}]$ corresponds to the set of vectors $(x,\, y,\, z)$ such that

$$x^2 + 4(y^2 + yz + z^2) = s \quad \text{and} \quad x\mathbf{Z} + y\mathbf{Z} + z\mathbf{Z} = \mathbf{Z}. \tag{6.11}$$

Such vectors exist if and only if $s = r^2m$ with a squarefree positive integer $m$ such that 3 does not split in $K_0 = \mathbf{Q}(\sqrt{-3m}\,)$ and a positive integer $r$ prime to 3 such that $2|r$ if 4 divides the discriminant of $K_0$.

In both cases (1) and (2) the group $\Gamma(L)$ has order 12. Represent $(x, y, z) \in \mathbf{Z}^3$ by $(x, \beta)$ with $\beta = y + z\zeta$, where $\zeta$ is a primitive cubic root of unity. Then $\Gamma'$ of (6.6) consists of the maps $(x, \beta) \mapsto (x, \varepsilon\beta)$ and $(x, \beta) \mapsto (-x, \varepsilon\overline{\beta})$, where $\varepsilon$ is a sixth root of unity. Therefore a set of representatives for $L[q, \mathbf{Z}]/\Gamma(L)$ can be found numerically. For instance, take $s = m = 79$ in (6.9); then we easily find that $\#\{L[q, \mathbf{Z}]/\Gamma(L)\} = 5$, which combined with (5.15a) confirms that $\mathbf{Q}(\sqrt{-79}\,)$ has class number 5.

(3) Our third example concerns the case $e = d = 2$. We have

$$2\Phi = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix}, \quad 2\Phi^{-1} = \begin{bmatrix} 3 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 3 \end{bmatrix}. \tag{6.12}$$

Then $L[s/2, \mathbf{Z}]$ corresponds to the set of vectors $x = (x_i)_{i=1}^3 \in \mathbf{Z}^3$ such that

$$x \cdot 2\Phi^{-1} \cdot {}^t x = s \quad \text{and} \quad \textstyle\sum_{i=1}^3 x_i\mathbf{Z} = \mathbf{Z}. \tag{6.13}$$

Such vectors $x$ exist if and only if $s = r^2m$ with an odd integer $r$ and a squarefree positive integer $m$ such that $m - 3 \in 8\mathbf{Z}$. In this case, $K_0 = \mathbf{Q}(\sqrt{-m}\,)$.

(4) Take $e = d = 7$. We have then

$$2\Phi = \mathrm{diag}\left[2, \begin{bmatrix} 4 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 7\Phi^{-1} = \mathrm{diag}\left[7, \begin{bmatrix} 4 & 2 \\ 2 & 8 \end{bmatrix}\right], \tag{6.14}$$

and $L[s/7, \mathbf{Z}]$ with $s \in \mathbf{Z}$ corresponds to the set of vectors $(x, y, z)$ such that

$$7x^2 + 4(y^2 + yz + 2z^2) = s \quad \text{and} \quad x\mathbf{Z} + y\mathbf{Z} + z\mathbf{Z} = \mathbf{Z}. \tag{6.15}$$

Such vectors exist if and only if $s = r^2m$ with a positive integer $r$ prime to 7 and a squarefree positive integer $m$ such that 7 does not split in $K_0 = \mathbf{Q}(\sqrt{-m}\,)$; $2|r$ if $m + 1 \notin 4\mathbf{Z}$.

(5) Let us finally take $e = 2$ and $d = 22$. We have then

$$2\Phi = \mathrm{diag}\left[4, \begin{bmatrix} 6 & -1 \\ -1 & 2 \end{bmatrix}\right], \quad 22\Phi^{-1} = \mathrm{diag}\left[11, \begin{bmatrix} 8 & 4 \\ 4 & 24 \end{bmatrix}\right], \tag{6.16}$$

and the result about $L[s/22, \mathbf{Z}]$ is what we stated in the introduction.

## References

[E1] M. Eichler, Quadratische Formen und orthogonale Gruppen, Springer, Berlin, 1952, 2nd ed. 1974.

[E2] M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, J. reine angew. Math. 195 (1956), 127–151.

[Pe] M. Peters, Ternäre und quaternäre quadratische Formen und Quaternionenalgebren, Acta Arithmetica 15 (1969), 329–365.

[Pi] A. Pizer, Type numbers of Eichler orders, J. reine angew. Math. 264 (1973), 76–102.

[S1] G. Shimura, Euler Products and Eisenstein series, CBMS Regional Conference Series in Mathematics, No. 93, Amer. Math. Soc. 1997.

[S2] G. Shimura, An exact mass formula for orthogonal groups, Duke Math. J. 97 (1999), 1–66 (=Collected Papers, IV, 509–574).

[S3] G. Shimura, Arithmetic and analytic theories of quadratic forms and Clifford groups, Mathematical Surveys and Monographs, vol. 109, Amer. Math. Soc. 2004.

[S4] G. Shimura, Quadratic Diophantine equations and orders in quaternion algebras, Amer. J. Math. 128 (2006), 481–518.

[S5] G. Shimura, Classification, construction, and similitudes of quadratic forms, to appear in Amer. J. Math. 128 (2006).

[S6] G. Shimura, Quadratic Diophantine equations, the class number, and the mass formula, Bulletin, Amer. Math. Soc. 43 (2006), 285–304.

[S7] G. Shimura, Classification of integer-valued symmetric forms, to appear in Amer. J. Math. 129 (2007).

[W] G. L. Watson, One-class genera of positive ternary quadratic forms, Mathematika 19 (1972), 96–104.

Goro Shimura
Department of Mathematics
Princeton University
Princeton, New Jersey 08544-1000
U.S.A.
goro@Math.Princeton.EDU