Arithmetic of Hermitian Forms

Goro Shimura

Received: May 27, 2008

Communicated by Don Blasius

Abstract. We investigate the following two problems on a hermitian form Φ over an algebraic number field: (1) classification of Φ over the ring of algebraic integers; (2) hermitian Diophantine equations. The same types of problems for quadratic forms were treated in the author's previous articles. Here we discuss the hermitian case. Problem (2) concerns an equation $\xi\Phi \cdot {}^t\xi^\rho = \Psi$, where Φ and Ψ represent hermitian forms. We connect the number of such ξ modulo a group of units with the class number and mass of the unitary group of a form Θ such that $\Phi \approx \Psi \oplus \Theta$.

2000 Mathematics Subject Classification: 11E39 (primary), 11E41, 11D09 (secondary)

Introduction

To explain Problems (1) and (2) of the abstract, we take a quadratic extension K of an algebraic number field F, a vector space V over K of dimension n, and a nondegenerate hermitian form $\varphi : V \times V \to K$ with respect to the nontrivial automorphism ρ of K over F. We denote by $d_0(\varphi)$ the coset of $F^\times/N_{K/F}(K^\times)$ represented by $(-1)^{n(n-1)/2}\det(\varphi)$. It is classically known that n, $d_0(\varphi)$, and the indices of φ at certain archimedean primes of F, satisfying a natural consistency condition, determine the isomorphism class of (V, φ), and vice versa. This classification does not answer, however, the question of classification over the ring of integers. To be precise, let $\mathfrak{r}$ denote the ring of algebraic integers in K and $\mathfrak{g} = F \cap \mathfrak{r}$; let $\mathfrak{d}$ be the different of K relative to F. We put

$$\mathfrak{H}_n = \{\Phi \in GL_n(K) \,|\, \Phi = {}^t\Phi^\rho\}. \tag{0.1}$$

We call a matrix $\Phi = (\varphi_{ij}) \in \mathfrak{H}_n$ *semi-integral* if $\varphi_{ij} \in \mathfrak{d}^{-1}$ and $\varphi_{ii} \in \mathfrak{g}$ for every i and j, which means that $\sum_{i,j} \varphi_{ij} x_i x_j^\rho \in \mathfrak{g}$ for every $(x_i)_{i=1}^n \in \mathfrak{r}^n$. Further we call a semi-integral Φ *reduced* if the following condition is satisfied:

(R) *If* $\Phi = P\Psi \cdot {}^tP^\rho$ *with a semi-integral* Ψ *and* $P = (p_{ij}) \in GL_n(K)$, $p_{ij} \in \mathfrak{r}$, *then* $\det(P) \in \mathfrak{r}^\times$.

These definitions are natural, but cover only a special class of (V, φ), as an $\mathfrak{r}$-lattice in V may not be isomorphic to $\mathfrak{r}^n$. In order to classify all $\mathfrak{g}$-valued hermitian forms, we have to define the genus of a form relative to an isomorphism class of lattices, and study its connection with the isomorphism class of (V, φ). These are nontrivial, and will be treated in §§2.4 and 2.5. We are then able to classify all the genera of $\mathfrak{g}$-valued hermitian forms in terms of matrices (Theorems 2.10 and 2.11). The results can be presented in simpler forms if K is a real or an imaginary quadratic field of odd class number, in which case the above definitions cover all hermitian spaces. Let d be the discriminant of such a K; then $K = \mathbf{Q}(\sqrt{d}\,)$. For a semi-integral Φ with entries in K, put $s(\Phi) = p - q$ when $d < 0$ and Φ as a complex hermitian matrix has p positive and q negative eigenvalues; we do not define $s(\Phi)$ if $d > 0$. Let $\mathfrak{H}_n^0$ be the set of all reduced semi-integral elements of $\mathfrak{H}_n$. Then we can prove (Theorem 2.14):

(A) *Let three integers* n, σ, *and* e *be given as follows:* $0 < n \in 2\mathbf{Z}$, $\sigma \in 2\mathbf{Z}$, $|\sigma| \le n$; $\sigma = 0$ *if* $d > 0$; e *is positive and squarefree. Let* r *be the number of prime factors of* e. *Suppose that* $\sigma - 2r \in 4\mathbf{Z}$ *and no prime factor of* e *splits in* K. *Then there exists an element* Φ *of* $\mathfrak{H}_n^0$ *such that*

$$\begin{aligned} &\det(\sqrt{d}\,\Phi) = (-1)^{\sigma/2}e \quad \textit{and} \quad s(\Phi) = \sigma \qquad \textit{if } d < 0,\\ &\det(\sqrt{d}\,\Phi) = \tau e \qquad \textit{with} \qquad \tau = 1 \ \textit{ or } -1 \qquad \textit{if } d > 0. \end{aligned}$$

Moreover, every element of $\mathfrak{H}_n^0$ *is of this type. Its genus is determined by* (σ, e) *if* $d < 0$, *and by* e *if* $d > 0$. *If* $d > 0$ *and* $-1 \in N_{K/\mathbf{Q}}(K^\times)$, *then both* e *and* $-e$ *can occur as* $\det(\sqrt{d}\,\Phi)$ *for* Φ *in the same genus. If* $d > 0$ *and* $-1 \notin N_{K/\mathbf{Q}}(K^\times)$, *then* τ *is uniquely determined by the condition that a prime number* p *divides* e *if and only if* $\tau e \notin N_{K/\mathbf{Q}}(K_p^\times)$, *where* $K_p = K \otimes_\mathbf{Q} \mathbf{Q}_p$.

This concerns the case of even n. We have similar but somewhat different results for odd n (Theorem 2.15). In fact we discussed in [S5] and [S6] semi-integral and reduced quadratic forms and obtained results of the same type. If K is imaginary, the hermitian case is almost parallel to the case of quadratic forms over $\mathbf{Q}$, but the theory for real K is more subtle, as can be seen from the above statement.

Let us now turn to the second problem. Before explaining the principal results, let us first discuss natural problems which are more basic and which must be settled before investigating the main question. Given (V, φ) as before, let $U^\varphi(V)$ and $SU^\varphi(V)$ denote the unitary group and the special unitary group of φ, defined as subgroups of $GL(V, K)$. Take an $\mathfrak{r}$-lattice L in V and put

(0.2) $$\Gamma(L) = \{\alpha \in U^\varphi(V) \mid L\alpha = L\}, \qquad \Gamma^1(L) = \Gamma(L) \cap SU^\varphi(V).$$

Then we ask, for a fixed $q \in F^{\times}$, whether the set $\{h \in V \,|\, \varphi[h] = q\}$ modulo $\Gamma^1(L)$ is a finite set. A similar question can be asked by replacing F, K, (V, φ) and L by their localizations at a nonarchimedean prime and by defining an obvious analogue of $\Gamma^1(L)$. We will prove that the answer is affirmative in both global and local cases, provided $n > 1$ (Theorems 3.3 and 4.2). The same is true for the problem about the solutions ξ of the equation $\xi\Phi \cdot {}^t\xi^{\rho} = \Psi$, where Ψ is of size m, and ξ belongs to an $\mathfrak{r}$-lattice in the space of $(m \times n)$-matrices with entries in K, where m is a positive integer $< n$ (Theorems 5.2 and 5.3). We already proved in [S3] the analogues of these facts for quadratic forms and orthogonal groups.

In order to go beyond the mere finiteness, we consider the adelizations $U^{\varphi}(V)_{\mathbf{A}}$ and $SU^{\varphi}(V)_{\mathbf{A}}$, and define their open subgroups C and C^1 by

$$(0.3) \qquad C = \{\gamma \in U^{\varphi}(V)_{\mathbf{A}} \,|\, L\gamma = L\}, \quad C^1 = C \cap SU^{\varphi}(V)_{\mathbf{A}},$$

where L is a fixed $\mathfrak{r}$-lattice in V. Given two solutions ξ_0 and ξ_1 of the equation $\xi\Phi \cdot {}^t\xi^{\rho} = \Psi$, we say that they belong to the same *genus* (with respect to C) if $\xi_0\gamma_v = \xi_1$ for every nonarchimedean prime v with an element $(\gamma_v)_v \in C$. Naturally they are said to belong to the same *class* if $\xi_0\gamma = \xi_1$ with $\gamma \in \Gamma(L)$. Now to explain our principal ideas in the simplest case, put $G = U^{\varphi}(V)$ and $H = \{\alpha \in G \,|\, \xi_0\alpha = \xi_0\}$; also assume for the moment that $G_{\mathbf{A}} = GC$. Then there is a bijection of $H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)$ onto the set of classes in the genus of ξ_0, and so

$$\text{(B)} \qquad \#\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)\} = \text{the number of classes in the genus of } \xi_0.$$

Here and henceforth $\#\{X\}$ denotes the number of elements in a set X. If $G_{\mathbf{A}} \neq GC$, the right-hand side becomes a finite sum of the class numbers of several genera (Theorem 5.4). Since the left-hand side is *the class number* of the unitary group H with respect to $H_{\mathbf{A}} \cap C$, equality (B) connects it to the solutions ξ of $\xi\Phi \cdot {}^t\xi^{\rho} = \Psi$.

If $m = 1$, the results can be stated in a more transparent way. Returning to the hermitian form $\varphi : V \times V \to K$, put $\varphi[h] = \varphi(h, h)$ for $h \in V$. Then the equation $\xi\Phi \cdot {}^t\xi^{\rho} = \Psi$ can be written $\varphi[h] = q$ with $h \in V$ and $q \in F^{\times}$; thus h and q replace ξ and Ψ. Given a fractional ideal $\mathfrak{b}$ in K, put

$$(0.4) \qquad L[q, \mathfrak{b}] = \{h \in V \,|\, \varphi[h] = q, \, \varphi(h, L) = \mathfrak{b}\}.$$

We call L *integral* if $\varphi[x] \in \mathfrak{g}$ for every $x \in L$ and call L *maximal* if it is maximal among the integral $\mathfrak{r}$-lattices. The point of considering $L[q, \mathfrak{b}]$ is that $L[q, \mathfrak{b}]$, *if nonempty, consists of a single genus with respect to* C in the above sense. This is clearly a result of local nature; unfortunately, its proof given in Section 3 is not short. In this case $H = U^{\varphi}(W)$, where W is the orthogonal complement of Kh in V. Now we can prove (Theorem 4.4, Corollary 5.8):

(C) *For every* $y \in G_{\mathbf{A}}$, *there is a bijection of* $H\backslash(H_{\mathbf{A}} \cap GyC)/(H_{\mathbf{A}} \cap C)$ *onto* $(Ly^{-1})[q,\, \mathfrak{b}]/\varDelta_y$, *where* $\varDelta_y = G \cap yCy^{-1}$.

(D) *Take* $\{y_i\}_{i\in I} \subset G_{\mathbf{A}}$ *so that* $G_{\mathbf{A}} = \bigsqcup_{i\in I} Gy_iC$ *and put* $L_i = Ly_i^{-1}$. *Then*

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

(E) *If the archimedean factor of* $G_{\mathbf{A}}$ *is compact, then*

$$\sum_{i\in I} \#\bigl\{L_i[q,\, \mathfrak{b}]\bigr\}/\#\bigl\{\varGamma_i\bigr\} = \mathfrak{m}(H,\, H_{\mathbf{A}} \cap C),$$

where the right-hand side is the mass of H *with respect to the open subgroup* $H_{\mathbf{A}} \cap C$ *of* $H_{\mathbf{A}}$ *in the sense of* [S2].

These assertions are true with $SU^{\varphi}(V)$, $SU^{\varphi}(W)$ and C^1 in place of G, H, and C, if $\dim(V) > 2$ and we impose a certain condition on $(q,\, \mathfrak{b})$. Notice that (E) gives the mass of H by means of the number of solutions h of $\varphi[h] = q$ under the condition $\varphi(h,\, L) = \mathfrak{b}$, while (D) gives the class number of H.

In our recent book [S3, Chapter III] we developed a theory of a Diophantine equation $\varphi[h] = q$ for a quadratic form φ defined on a vector space over an algebraic number field. The principal result is that to each "primitive solution" h of this equation for a fixed q, considered modulo the group of units $\varGamma$, one can associate a "class" of lattices with respect to the orthogonal group H of the restriction of φ to a subspace of codimension 1. Consequently the class number of H equals the number of such h modulo $\varGamma$. This includes as a special case the result of Gauss that the number of primitive representations of q as the sum of three squares equals an elementary factor times the class number of primitive binary quadratic forms of discriminant $-q$. Also, formulas of type (B) and (E) were proved in [S3] and [S6] for quadratic forms. The reader is referred to [S7] for some more historical and technical comments on this subject. Now (B), (C), (D), and (E) are hermitian analogues of these results. In order to develop the theory for hermitian forms, we are naturally guided by the formulation in the case of quadratic forms, but we need new ideas and technique, and it is wrong to say that we can do things "in the same way." This is especially so when we consider the problem with respect to the special unitary group instead of the unitary group. Thus there are two theories with respect to these two types of groups, and one, that for the special unitary group, is more complex than the other, and in a sense more interesting.

1. Generalities on hermitian forms and unitary groups

1.1. For an associative ring A with an identity element we denote by $A^{\times}$ the group of all invertible elements of A, and for positive integers m and n we denote by A_n^m the A-module of all $(m \times n)$-matrices with entries in A. We put $M_n(A) = A_n^n$ when we view it as a ring, and denote by 1_n its identity element.

We take a basic field F and a couple (K, ρ) consisting of an F-algebra K and a nontrivial F-linear automorphism ρ of K belonging to the following two types:

(I) K is a separable quadratic extension of F and ρ generates $\mathrm{Gal}(K/F)$;
(II) $K = F \times F$ and $(x, y)^\rho = (y, x)$ for $(x, y) \in F \times F$.

In our later discussion, K of type (II) will appear as a localization of a global K of type (I). For a matrix $\alpha = (a_{ij})$ with entries in K we denote by ${}^t\alpha$ the transpose of α, and put $\alpha^\rho = (a_{ij}^\rho)$ and $\alpha^* = {}^t\alpha^\rho$; we put also $\alpha^{-\rho} = (\alpha^\rho)^{-1}$ when α is invertible. For a subring S of K we write $\alpha \prec S$ if all the entries of α are contained in S. Given a left K-module V, we denote by $\mathrm{End}(V, K)$ the ring of all K-linear endomorphisms of V and put $GL(V, K) = \mathrm{End}(V, K)^\times$. We let $\mathrm{End}(V, K)$ act on V on the right; namely we denote by $w\alpha$ the image of $w \in V$ under $\alpha \in \mathrm{End}(V, K)$.

Let V be a left K-module isomorphic to K_n^1; we put then $n = \dim(V)$. By a hermitian space we mean a structure (V, φ), where φ is a hermitian form on V, that is, an F-bilinear map $\varphi : V \times V \to K$ such that

$$\varphi(x, y)^\rho = \varphi(y, x), \tag{1.1}$$

$$\varphi(ax, by) = ab^\rho\varphi(x, y) \quad \textit{for every} \quad a, b \in K. \tag{1.2}$$

Whenever we speak of a hermitian space (V, φ), we assume that φ is nondegenerate, and put $\varphi[x] = \varphi(x, x)$ for $x \in V$. We define groups $U^\varphi(V)$ and $SU^\varphi(V)$ by

$$U^\varphi = U^\varphi(V) = \{\alpha \in GL(V, K) \mid \varphi[x\alpha] = \varphi[x] \text{ for every } x \in V\}, \tag{1.3a}$$

$$SU^\varphi = SU^\varphi(V) = \{\alpha \in U^\varphi(V) \mid \det(\alpha) = 1\}. \tag{1.3b}$$

For every free K-submodule X of V on which φ is nondegenerate, we put

$$X^\perp = \{y \in V \mid \varphi(y, X) = 0\}, \tag{1.4}$$

and define $U^\varphi(X)$ and $SU^\varphi(X)$ by (1.3a, b) with X in place of V; namely we use φ for its restriction to X. We always identify $U^\varphi(X)$ with the subgroup of $U^\varphi(V)$ consisting of the elements α such that $y\alpha = y$ for every $y \in X^\perp$. Similarly we view $SU^\varphi(X)$ as a subgroup of $SU^\varphi(V)$.

Let h be an element of V such that $\varphi[h] \neq 0$. Then

$$\{x \in V \mid \varphi[x] = \varphi[h]\} = \begin{cases} h \cdot U^\varphi & \text{if } \dim(V) = 1, \\ h \cdot SU^\varphi & \text{if } \dim(V) > 1. \end{cases} \tag{1.5}$$

This follows easily from the generalized Witt theorem; see [S2, Lemma 1.3], for example. The case $K = F \times F$ is not included in that theorem, but the structure of (V, φ) for such a K is determined by $\dim(V)$ as shown in [S2, §2.13], and so the fact corresponding to the Witt theorem is trivially true; see also §1.8 below.

1.2. Let φ_0 be the matrix that represents φ with respect to a K-basis of V; then we denote by $d_0(V, \varphi)$ the element of $F^\times/N_{K/F}(K^\times)$ represented by $(-1)^{n/2}\det(\varphi_0)$ or $(-1)^{(n-1)/2}\det(\varphi_0)$ according as n is even or odd. This does not depend on the choice of a K-basis of V. We denote $d_0(V, \varphi)$ simply by $d_0(V)$ or $d_0(\varphi)$ when there is no fear of confusion.

Given $s \in F^\times$, we denote by $\{K, s\}$ the quaternion algebra B over F in which K is embedded and which is given by

$$B = K + K\omega, \quad \omega^2 = s, \quad \omega a = a^\rho \omega \text{ for every } a \in K. \tag{1.6}$$

Since B is determined by K and $sN_{K/F}(K^\times)$, for a coset $\varepsilon \in F^\times/N_{K/F}(K^\times)$ we denote by $\{K, \varepsilon\}$ the algebra $\{K, s\}$ with any $s \in \varepsilon$. In particular, we can associate with (V, φ) a quaternion algebra $\{K, d_0(\varphi)\}$.

LEMMA 1.3. *Given (V, φ) as in §1.1, suppose $\dim(V) = 2$ and put $B = \{K, d_0(\varphi)\}$. Then there is a ring-injection j of B into $\mathrm{End}(V, K)$ and an element ℓ of V such that $\varphi[\ell] \neq 0$, $\ell j(B) = V$, $\ell j(a) = a\ell$ for every $a \in K$, and $\varphi[\ell j(\xi)] = \varphi[\ell]\xi\xi^\iota$ for every $\xi \in B$, where ι is the main involution of B. Moreover, $\mathrm{Tr}_{K/F}\big(\varphi(\ell\alpha, \ell\beta)\big) = \varphi[\ell]\mathrm{Tr}_{B/F}(\alpha\beta^\iota)$ for every $\alpha, \beta \in B$, and*

$$U^\varphi(V) = \big\{z^{-1}\alpha \,\big|\, z \in K^\times,\ \alpha \in B^\times,\ zz^\rho = \alpha\alpha^\iota\big\}, \tag{1.7a}$$

$$SU^\varphi(V) = \big\{\alpha \in B^\times \,\big|\, \alpha\alpha^\iota = 1\big\}, \tag{1.7b}$$

where we identify α with $j(\alpha)$ for $\alpha \in B$.

Proof. Identify V with K_2^1 so that $\varphi(x, y) = x\varphi_0 y^*$ for $x, y \in K_2^1$ with $\varphi_0 = \mathrm{diag}[c, -cs]$, where $c, s \in F^\times$. Then $d_0(\varphi) = sN_{K/F}(K^\times)$, and so B is given by (1.6). Define $j : B \to M_2(K)$ by $j(a+b\omega) = \begin{bmatrix} a & b \\ sb^\rho & a^\rho \end{bmatrix}$ and put $\ell = (1, 0)$. Then it is an easy exercise to verify all the statements; cf. [S2, Lemmas 4.3, 4.4, and (4.3.2)]. Notice that $j(B) = \big\{\alpha \in M_2(K) \,\big|\, \alpha^\iota\varphi_0 = \varphi_0\alpha^*\big\}$.

1.4. When K is a field, by a *weak Witt decomposition of* V we mean a direct sum decomposition of V with $2r$ elements e_i, f_i, and a subspace Z of V such that

$$V = \textstyle\sum_{i=1}^r (Ke_i + Kf_i) + Z, \qquad Z = \big(\sum_{i=1}^r (Ke_i + Kf_i)\big)^\perp, \tag{1.8a}$$

$$\varphi(e_i, e_j) = \varphi(f_i, f_j) = 0, \quad \varphi(e_i, f_j) = \delta_{ij} \quad \textit{for every } i \textit{ and } j. \tag{1.8b}$$

Clearly $\sum_{i=1}^r (Ke_i + Kf_i)$ is a subspace of dimension $2r$. We call this a *Witt decomposition* if $\varphi[x] \neq 0$ for every $x \in Z$, $\neq 0$, in which case we call Z a *core subspace* of (V, φ) and $\dim(Z)$ the *core dimension* of (V, φ). If ζ is the restriction of φ to Z, then clearly $d_0(\varphi) = d_0(\zeta)$.

1.5. In this paper a *global field* means an algebraic number field of finite degree, and a *local field* the completion of a global field at a nonarchimedean prime. For a global field F we denote by $\mathfrak{g}$ the ring of algebraic integers in F;

for a local F we denote by $\mathfrak{g}$ the ring of local integers in F in the standard sense. An archimedean completion of a global field will not be called a local field. In both local and global cases, by a $\mathfrak{g}$-*lattice* in a finite-dimensional vector space V over F, we mean a finitely generated $\mathfrak{g}$-submodule of V that spans V over F.

Let (K, ρ) be as in §1.1 with a local or global F. We then denote by $\mathfrak{r}$ the ring of all elements of K integral over $\mathfrak{g}$, and by $\mathfrak{d}$ the different of K relative to F. We have $\mathfrak{r} = \mathfrak{d} = \mathfrak{g} \times \mathfrak{g}$ if $K = F \times F$. By a $\mathfrak{g}$-*ideal* we mean a fractional ideal in F, and similarly by an $\mathfrak{r}$-*ideal* we mean a fractional ideal in K if K is a field. If $K = F \times F$, an $\mathfrak{r}$-*ideal* means a subset of K of the form $\mathfrak{a} \times \mathfrak{b}$ with $\mathfrak{g}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$. In both local and global cases, by an $\mathfrak{r}$-*lattice* in a K-module V as in §1.1 we mean a $\mathfrak{g}$-lattice in V stable under multiplication by the elements of $\mathfrak{r}$. Given two $\mathfrak{r}$-lattices L and M in V, we denote by $[L/M]$ the $\mathfrak{r}$-ideal generated by $\det(\alpha)$ for all $\alpha \in GL(V)$ such that $L\alpha \subset M$. Thus $[L/L\alpha] = \det(\alpha)\mathfrak{r}$. In particular, if $\alpha \in U^{\varphi}$ and K is a field in the local case, then $[L/L\alpha] = \mathfrak{r}$. If $K = F \times F$, however, $[L/L\alpha] = \mathfrak{a} \times \mathfrak{a}^{-1}$ with a $\mathfrak{g}$-ideal $\mathfrak{a}$ for $\alpha \in U^{\varphi}$.

Lemma 1.6. *Two hermitian spaces (V, φ) and (V', φ') in the local case are isomorphic if and only if $\dim(V) = \dim(V')$ and $d_0(\varphi) = d_0(\varphi')$.*

This is well known. For the proof, see [S2, Proposition 5.3], for example.

1.7. Let (V, φ) be defined with a local or global F. For a $\mathfrak{g}$-lattice L in V we denote by $\mu(L)$ the $\mathfrak{g}$-ideal generated by $\varphi[x]$ for all $x \in L$. We call a $\mathfrak{g}$-lattice L in V *integral* if $\mu(L) \subset \mathfrak{g}$; we call an $\mathfrak{r}$-lattice L *maximal* if L is maximal among the integral $\mathfrak{r}$-lattices. (This is what we called $\mathfrak{g}$-maximal in [S2].) For basic properties of maximal lattices in V the reader is referred to [S1] or Sections 4 and 5 of [S2]. For example, we note ([S2, (4.7.1)])

$$\varphi(L, L) \subset \mathfrak{d}^{-1} \text{ if } L \text{ is integral.} \tag{1.9}$$

If $n > 1$ and L is maximal, then $\mu(L) = \mathfrak{g}$. This fact in the global case follows from the local case, which can be seen from [S2, Lemmas 5.4 and 5.6].

Given an $\mathfrak{r}$-lattice L in V, $q \in F^{\times}$, and an $\mathfrak{r}$-ideal $\mathfrak{b}$, we put

$$\widehat{L} = \{x \in V \,|\, \varphi(x, L) \subset \mathfrak{d}^{-1}\}, \tag{1.10a}$$

$$L[q] = \{x \in L \,|\, \varphi[x] = q\}, \tag{1.10b}$$

$$L[q, \mathfrak{b}] = \{x \in V \,|\, \varphi[x] = q,\ \varphi(x, L) = \mathfrak{b}\}. \tag{1.10c}$$

By (1.9), we have $L \subset \widehat{L}$ if L is integral. The set $L[q, \mathfrak{b}]$ is not necessarily contained in $L[q]$. If M is another $\mathfrak{r}$-lattice in V, then we easily see that $[L/M]^{\rho} = [\widehat{M}/\widehat{L}]$. If $L_1 = L\alpha$ with $\alpha \in U^{\varphi}$, then $\widehat{L}_1 = \widehat{L}\alpha$, and so $[\widehat{L}_1/L_1] = [\widehat{L}/L]$.

The notation being as in (1.8a, b), take a maximal $\mathfrak{r}$-lattice M in Z and put

$$L = \textstyle\sum_{i=1}^{r}(\mathfrak{r}e_i + \mathfrak{d}^{-1}f_i) + M. \tag{1.11}$$

Then L is maximal; see [S2, Lemma 4.9 (2)]. We can easily verify that

$$\widehat{L} = \textstyle\sum_{i=1}^{r}(\mathfrak{r}e_i + \mathfrak{d}^{-1}f_i) + \widehat{M}, \quad \widehat{M} = \{x \in Z \,|\, \varphi(x,\, M) \subset \mathfrak{d}^{-1}\}. \tag{1.12}$$

1.8. Let us now consider the case $K = F \times F$; then we define the core dimension of $(V,\, \varphi)$ to be 0. We can write an element of $V = K_n^1$ in the form $(x,\, y)$ with $x,\, y \in F_n^1$. Taking a suitable coordinate system, we can assume that

$$\varphi\big((x,\, y),\, (z,\, w)\big) = (x \cdot {}^t w,\, y \cdot {}^t z) \qquad (x,\, y,\, z,\, w \in F_n^1). \tag{1.13}$$

This is shown in [S2, §2.13]. We have then $\varphi\big[(x,\, y)\big] = x \cdot {}^t y$ and

$$U^\varphi = \{(\xi,\, \widetilde{\xi}) \,|\, \xi \in GL_n(F)\}, \quad SU^\varphi = \{(\xi,\, \widetilde{\xi}) \,|\, \xi \in SL_n(F)\}, \tag{1.14}$$

where $\widetilde{\xi} = {}^t\xi^{-1}$; also $\mathfrak{g}_n^1 \times \mathfrak{g}_n^1$ is a maximal lattice. It should be noted that if $h \in V$ and $\varphi[h] \neq 0$, then Kh is isomorphic to K.

LEMMA 1.9. *Let L be a maximal lattice in V and t the core dimension of $(V,\, \varphi)$; suppose K is a local field; put*

$$E = \{e \in \mathfrak{r}^\times \,|\, ee^\rho = 1\}, \quad E_0 = \{e^\rho/e \,|\, e \in \mathfrak{r}^\times\}, \quad E_L = \det\big(C(L)\big),$$

where $C(L) = \{\alpha \in U^\varphi(V) \,|\, L\alpha = L\}$. Then the following assertions hold:

(i) $[E : E_0] = 1$ *or 2 according as K is unramified or ramified over F.*

(ii) $E_L = E_0$ *if* $t = 0$; $E_L = E$ *if* $t > 0$.

This is included in [S1, Lemma 4.16 and Proposition 4.18] and [S2, Lemma 5.11].

Suppose K is a local field ramified over F; let L and M be maximal lattices in V. Then there exists an element $\alpha \in U^\varphi$ such that $M = L\alpha$ as shown in (i) of the following lemma. We then denote by $e(L/M)$ the element of E/E_0 represented by $\det(\alpha)$. This is well defined in view of (ii) above.

LEMMA 1.10. *Let L and M be maximal lattices in V in the local case, and let t be the core dimension of $(V,\, \varphi)$. Then the following assertions hold:*

(i) *There exists an element α of U^φ such that $M = L\alpha$.*

(ii) *We can take such an α from SU^φ if $t > 0$ or K is a field unramified over F.*

(iii) *Suppose K is ramified over F and $t = 0$; then $M = L\alpha$ with $\alpha \in SU^\varphi$ if and only if $e(L/M) = 1$.*

(iv) *Suppose $K = F \times F$; then $M = L\alpha$ with $\alpha \in SU^\varphi$ if and only if $[L/M] = \mathfrak{r}$.*

Proof. The first assertion is included in [S1, Propositions 3.3 and 4.13] and also in [S2, Lemmas 4.12 and 5.9]. Next, suppose K is a field; given M, take

$\alpha \in U^\varphi$ so that $L\alpha = M$ and put $c = \det(\alpha)$. Then $c \in E$. If K is unramified over F or $t > 0$, then Lemma 1.9 guarantees an element β of U^φ such that $L\beta = L$ and $\det(\beta) = c^{-1}$. Then $\beta\alpha \in SU^\varphi$ and $L\beta\alpha = M$. This proves (ii). Assertion (iii) can be proved in a similar way. Assertion (iv) is included in [S1, Proposition 3.3].

1.11. Let us now consider the case with $n = 2$ and a local F. Using the symbols B, j, and ℓ of Lemma 1.3, we first observe that

$$B \cong M_2(F) \iff t = 0 \iff 1 \in d_0(\varphi). \tag{1.15}$$

Let $\mathfrak{O}$ be a maximal order in B containing $\mathfrak{r}$. We can find an element $\gamma \in B^\times$ such that $\varphi[\ell]^{-1} = \gamma\gamma^\iota$. Put $M = \ell j(\mathfrak{O}\gamma)$ and $\widehat{\mathfrak{O}} = \bigl\{\alpha \in B \bigm| \mathrm{Tr}_{B/F}(\alpha\mathfrak{O}) \subset \mathfrak{g}\bigr\}$. Identifying B with $j(B)$, for $\alpha \in B$ we see that

$$\begin{aligned}\ell\alpha\gamma \in \widehat{M} \iff \varphi(\ell\alpha\gamma,\, M) \subset \mathfrak{d}^{-1} \iff \mathrm{Tr}_{K/F}\bigl(\mathfrak{r}\varphi(\ell\alpha\gamma,\, M)\bigr) \subset \mathfrak{g}\\ \iff \mathrm{Tr}_{B/F}(\alpha\mathfrak{O}) \subset \mathfrak{g} \iff \alpha \in \widehat{\mathfrak{O}}.\end{aligned}$$

Thus $\widehat{M} = \ell j(\widehat{\mathfrak{O}}\gamma)$. If B is not a division algebra, then $\widehat{\mathfrak{O}} = \mathfrak{O}$, so that $\widehat{M} = M$, which means that M is maximal. Suppose B is a division algebra; then $\mathfrak{O} = \bigl\{\alpha \in B \bigm| \alpha\alpha^\iota \in \mathfrak{g}\bigr\}$ as noted in [S3, Theorem 5.13], and so $M = \bigl\{x \in V \bigm| \varphi[x] \in \mathfrak{g}\bigr\}$, which is a unique maximal lattice in V by [S2, Lemma 5.4]. Since $\widehat{\mathfrak{O}} = \mathfrak{P}^{-1}$ with the maximal ideal $\mathfrak{P}$ of $\mathfrak{O}$, we have $\widehat{M} = \ell j(\mathfrak{P}^{-1}\gamma)$. Thus $[\widehat{M}/M] = \mathfrak{p}\mathfrak{r}$ with the maximal ideal $\mathfrak{p}$ of $\mathfrak{g}$.

2. Classification of hermitian forms over a global field

2.1. Throughout this section we assume that F is a global field and K is a quadratic extension of F. We denote by $\mathbf{a}$ and $\mathbf{h}$ the sets of archimedean primes and nonarchimedean primes of F respectively, and put $\mathbf{v} = \mathbf{a} \cup \mathbf{h}$. Given an algebraic group G defined over F, we define G_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, the adelization of the multiplicative group $F^\times$ is denoted by $F_\mathbf{A}^\times$, which is the idele group of F. For $x \in G_\mathbf{A}$ and $v \in \mathbf{v}$ we denote by x_v the v-component of x.

Given $(V,\, \varphi)$ over F, for each $v \in \mathbf{v}$ we can define the v-localization $(V,\, \varphi)_v = (V_v,\, \varphi_v)$ with $\varphi_v : V_v \times V_v \to K_v$ in a natural way. For $v \in \mathbf{h}$ let t_v be the core dimension of $(V,\, \varphi)_v$. Since $x \mapsto \varphi_v[x]$ for $x \in V_v$ can be viewed as an F_v-valued quadratic form, we have $2t_v \le 4$ by a well known principle, and so $t_v \le 2$. Let $\mathbf{r}_0$ denote the set of all real archimedean primes of F that do not split in K. If $v \in \mathbf{a}$ and $v \notin \mathbf{r}_0$, then there is only one isomorphism class of $(V,\, \varphi)_v$ for each n. For each fixed $v \in \mathbf{r}_0$ we have a pair of nonnegative integers $(p_v,\, q_v)$ such that φ_v is represented by $\mathrm{diag}[1_{p_v},\, -1_{q_v}]$ when F_v and K_v are identified with $\mathbf{R}$ and $\mathbf{C}$. We put then $s_v(\varphi) = p_v - q_v$, and call $s_v(\varphi)$ the *index* of φ at v. Clearly $|s_v(\varphi)|$ is the core dimension of φ_v, $s_v(\varphi) - n \in 2\mathbf{Z}$, and $|s_v(\varphi)| \le n$; also, n and $s_v(\varphi)$ determine (p_v, q_v), and vice versa.

For an $\mathfrak{r}$-lattice L in V and $v \in \mathbf{h}$ we denote by L_v the $\mathfrak{r}_v$-linear span of L in V_v. Also, for $\xi \in GL(V, K)_{\mathbf{A}}$ we denote by $L\xi$ the lattice in V such that $(L\xi)_v = L_v\xi_v$ for every $v \in \mathbf{h}$. By the $U^\varphi(V)$-genus (resp. $SU^\varphi(V)$-*genus*) of L we understand the set of all lattices of the form $L\xi$ with $\xi \in U^\varphi(V)_{\mathbf{A}}$ (resp. $\xi \in SU^\varphi(V)_{\mathbf{A}}$). Also, by the $U^\varphi(V)$-class (resp. $SU^\varphi(V)$-*class*) of L we understand the set of all lattices of the form $L\alpha$ with $\alpha \in U^\varphi(V)$ (resp. $\alpha \in SU^\varphi(V)$).

The classification of (V, φ) over a number field was done by Landherr in [L]. We formulate the results in the form that suits our later purposes, and give a proof for the reader's convenience. To be precise, we are going to show that the isomorphism classes of hermitian spaces correspond bijectively to the sets of data consisting of the following objects:

(2.1a) $0 < n \in \mathbf{Z}$; $\varepsilon \in F^\times$; *an integer* σ_v, *given for each* $v \in \mathbf{r}_0$, *such that* $|\sigma_v| \le n$ *and* $\sigma_v - n \in 2\mathbf{Z}$.

We look for (V, φ) such that $\dim(V) = n$, $d_0(\varphi)$ is represented by ε, and $s_v(\varphi) = \sigma_v$ for every $v \in \mathbf{r}_0$. Clearly the following condition is necessary:

(2.1b) $(-1)^{\sigma_v/2}\varepsilon > 0$ *for every* $v \in \mathbf{r}_0$ *if* $n \in 2\mathbf{Z}$ *and* $(-1)^{(\sigma_v-1)/2}\varepsilon > 0$ *for every* $v \in \mathbf{r}_0$ *if* $n - 1 \in 2\mathbf{Z}$.

THEOREM 2.2. (i) *The isomorphism class of* (V, φ) *is determined by* n, $\{\sigma_v\}$, *and* $d_0(\varphi)$.

(ii) *Given* n, ε, *and* $\{\sigma_v\}$ *satisfying* (2.1a, b), *there exists a hermitian space* (V, φ) *such that* $\dim(V) = n$, $\varepsilon \in d_0(\varphi)$, *and* $s_v(\varphi) = \sigma_v$ *for every* $v \in \mathbf{r}_0$.

Proof. Clearly n and $\{\sigma_v\}$ determine $(V, \varphi)_v$ for every $v \in \mathbf{a}$, and n and $d_0(\varphi)$ determine $(V, \varphi)_v$ for every $v \in \mathbf{h}$ by Lemma 1.6. Therefore we obtain (i) in view of the Hasse principle. We prove (ii) by induction on n. The case $n = 1$ is trivial, and so we assume $n > 1$. We first prove the case in which $\sigma_v \ge 0$ for every $v \in \mathbf{r}_0$. Let $\tau_v = \sigma_v - 1$. Then the set $\bigl(n - 1, (-1)^{n-1}\varepsilon, \{\tau_v\}\bigr)$ satisfies (2.1a, b), and therefore by induction we can find a hermitian space (W, ψ) such that $\dim(W) = n - 1$, $\tau_v = s_v(\psi)$ for every $v \in \mathbf{r}_0$, and $(-1)^{n-1}\varepsilon \in d_0(\psi)$. Put $V = K \oplus W$ and define φ on V by $\varphi[a \oplus y] = aa^\rho + \psi[y]$ for $a \in K$ and $y \in W$. Then clearly $\varepsilon \in d_0(\varphi)$ and $s_v(\varphi) = \sigma_v$ for every $v \in \mathbf{r}_0$.

Now, given $\{\sigma_v\}$ with possibly negative σ_v, take $c \in F^\times$ so that $c < 0$ or $c > 0$ at $v \in \mathbf{r}_0$ according as $\sigma_v < 0$ or $\sigma_v \ge 0$. Then the set $\bigl(n, c^n\varepsilon, \{|\sigma_v|\}\bigr)$ satisfies (2.1a, b). Therefore we can find a hermitian space (V_1, φ_1) such that $\dim(V_1) = n$, $c^n\varepsilon \in d_0(\varphi_1)$, and $s_v(\varphi_1) = |\sigma_v|$ for every $v \in \mathbf{r}_0$. Put $\varphi = c\varphi_1$. Then $\varepsilon \in d_0(\varphi)$ and $s_v(\varphi) = \sigma_v$ for every $v \in \mathbf{r}_0$. This completes the proof.

Theorem 2.3. *Given* (V, φ), *put* $B = \{K, d_0(\varphi)\}$ *using the notation of* §*1.2. Let* $\mathfrak{e}$ *be the product of the prime ideals of* F *ramified in* B; *also let* L *be a maximal lattice in* V. *Then the following assertions hold.*

(i) $[\widehat{L}/L] = \mathfrak{er}$ *if* n *is even.*

(ii) *When* n *is odd, put* $d_0(\varphi)\mathfrak{g} = \mathfrak{a}N_{K/F}(\mathfrak{b})$ *with an* $\mathfrak{r}$*-ideal* $\mathfrak{b}$ *and a squarefree integral* $\mathfrak{g}$*-ideal* $\mathfrak{a}$ *whose prime factors remain prime in* K. *Then* $[\widehat{L}/L] = \mathfrak{a}\mathfrak{d}$, *where* $\mathfrak{d}$ *is the different of* K *relative to* F.

Proof. For $v \in \mathbf{h}$ let t_v be the core dimension of $(V, \varphi)_v$. Suppose $n \in 2\mathbf{Z}$; then $t_v = 0$ if and only if $d_0(\varphi)$ is represented by an element of $N_{K/F}(K_v^\times)$, that is, if and only if v does not divide $\mathfrak{e}$. If n is odd, the isomorphism class of $(V, \varphi)_v$ depends on $\mathfrak{a}_v$ and $\mathfrak{d}_v$. Thus our assertions can be reduced to the question about $[\widehat{L}_v/L_v]$ for $v \in \mathbf{h}$. In fact, suppressing the subscript v, we have, in the local case,

(2.2) $[\widehat{L}/L] = \mathfrak{r}$ *if* $t = 0$; $[\widehat{L}/L] = \mathfrak{pr}$ *if* $t = 2$; $[\widehat{L}/L] = \mathfrak{d}$ *if* $t = 1$ *and* $d_0(\varphi) \cap \mathfrak{g}^\times \neq \emptyset$; $[\widehat{L}/L] = \mathfrak{pd}$ *if* $t = 1$ *and* $d_0(\varphi) \cap \mathfrak{g}^\times = \emptyset$.

Here $\mathfrak{p}$ is the maximal ideal of $\mathfrak{g}$. In view of Lemma 1.10 (i), it is sufficient to prove this for a special choice of L. If $K = F \times F$, then we can put $L = \mathfrak{g}_n^1 \times \mathfrak{g}_n^1$ as noted in §1.8, and so $\widehat{L} = L$. Thus we assume that K is a field. By (1.12), $L = \widehat{L}$ if $t = 0$. Let $M = \{x \in Z \mid \varphi[x] \in \mathfrak{g}\}$. By (1.12), $[\widehat{L}/L] = [\widehat{M}/M]$. We have seen that $[\widehat{M}/M] = \mathfrak{pr}$ in §1.11 if $t = 2$. If $t = 1$, then $M = \mathfrak{r}\ell$ with an element ℓ such that $\varphi[\ell]\mathfrak{g}$ is $\mathfrak{g}$ or $\mathfrak{pg}$. Thus $\widehat{M} = \mathfrak{d}^{-1}\varphi[\ell]^{-1}\ell$, and so $[\widehat{L}/L] = [\widehat{M}/M] = \varphi[\ell]\mathfrak{d}$, which completes the proof of (2.2). Combining the results on $[\widehat{L}_v/L_v]$ for all $v \in \mathbf{h}$, we obtain our theorem.

2.4. To illustrate Theorem 2.3 in terms of matrices, we have to define the genus and class of a hermitian matrix. We put

$$\mathfrak{G} = GL_n(K), \qquad \mathfrak{H}_n = \{\Phi \in \mathfrak{G} \mid \Phi^* = \Phi\}, \qquad L_0 = \mathfrak{r}_n^1, \tag{2.3}$$

$$E = \mathfrak{G}_\mathbf{a} \prod_{v \in \mathbf{h}} GL_n(\mathfrak{r}_v), \qquad E_\xi = \xi^{-1}E\xi \quad (\xi \in \mathfrak{G}_\mathbf{A}), \tag{2.4}$$

$$\Delta_\xi = E_\xi \cap \mathfrak{G}, \qquad \Delta_\xi^1 = E_\xi \cap SL_n(K). \tag{2.5}$$

Every $\mathfrak{r}$-lattice L in K_n^1 can be given as $L = L_0\xi$ with $\xi \in \mathfrak{G}_\mathbf{A}$, and $E_\xi = \{y \in \mathfrak{G}_\mathbf{A} \mid Ly = L\}$. We denote by $\mathfrak{H}_n(\xi)$ the set of all $\Phi \in \mathfrak{H}_n$ such that $x\Phi x^* \in \mathfrak{g}$ for every $x \in L_0\xi$. We call such a Φ *reduced* (relative to ξ) if the following condition is satisfied:

$$\Phi \in \mathfrak{H}_n(\zeta^{-1}\xi) \text{ with } \zeta \in \mathfrak{G}_\mathbf{h} \cap \prod_{v \in \mathbf{h}} M_n(\mathfrak{r}_v) \Longrightarrow \zeta \in E. \tag{2.6}$$

We denote by $\mathfrak{H}_n^0(\xi)$ the set of all reduced elements of $\mathfrak{H}_n(\xi)$.

We say that two elements Φ and Ψ of $\mathfrak{H}_n(\xi)$ belong to the same *genus* (relative to ξ) if there exists an element ε of E_ξ such that $\varepsilon\Phi\varepsilon^* = \Psi$; they are said to belong to the same *U-class* (resp. *SU-class*) if $\alpha\Phi\alpha^* = \Psi$ for some $\alpha \in \Delta_\xi$ (resp. $\alpha \in \Delta_\xi^1$). These depend on the choice of $L = L_0\xi$.

Given $\Phi \in \mathfrak{H}_n$, put $V = K_n^1$ and $\varphi[x] = x\Phi x^*$ for $x \in V$. Then we obtain a hermitian space (V, φ), which we denote by $[\Phi]$, and we write $U(\Phi)$ and $SU(\Phi)$ for $U^\varphi(V)$ and $SU^\varphi(V)$ as subgroups of $\mathfrak{G}$. Put $L = L_0\xi$ with $\xi \in \mathfrak{G}_\mathbf{A}$. Clearly L is integral if $\Phi \in \mathfrak{H}_n(\xi)$, in which case L is maximal if and only if $\Phi \in \mathfrak{H}_n^0(\xi)$. Thus an element of $\mathfrak{H}_n^0(\xi)$ determines a hermitian space and a maximal lattice.

2.5. To parametrize all genera of $\Phi \in \mathfrak{H}_n^0(\xi)$, we need a few more symbols:

$$\mathfrak{t} = K_\mathbf{A}^\times \cap \left(K_\mathbf{a}^\times \prod_{v\in\mathbf{h}} \mathfrak{t}_v\right), \qquad \mathfrak{t}_v = \{y \in K_v^\times \mid yy^\rho \in \mathfrak{g}_v^\times\}, \tag{2.7}$$

$$T = \{x \in \mathfrak{G}_\mathbf{A} \mid \det(x) \in \mathfrak{t}\}. \tag{2.8}$$

Notice that $\mathfrak{t}_v = \mathfrak{r}_v^\times \cdot \{y \in K_v^\times \mid yy^\rho = 1\}$ for every $v \in \mathbf{h}$, and $\mathfrak{t}_v = \mathfrak{r}_v^\times$ if v does not split in K. Let $\mathfrak{I}_K$ denote the ideal group of K and $\mathfrak{I}_{K/F}^0$ the subgroup of $\mathfrak{I}_K$ generated by the ideals $\mathfrak{a}$ such that $N_{K/F}(\mathfrak{a}) = \mathfrak{g}$ and the principal ideals. Now there is a sequence of isomorphisms:

$$\mathfrak{G}_\mathbf{A}/T\mathfrak{G} \;\cong\; K_\mathbf{A}^\times/K^\times\mathfrak{t} \;\cong\; \mathfrak{I}_K/\mathfrak{I}_{K/F}^0. \tag{2.9}$$

The last isomorphism can be obtained by the map $y \mapsto y\mathfrak{r}$ for $y \in K_\mathbf{A}^\times$. As for the first isomorphism, we first note, for every $\xi \in \mathfrak{G}_\mathbf{A}$ and $\Phi \in \mathfrak{H}_n$,

$$T\mathfrak{G}\xi = E\xi U(\Phi)_\mathbf{A}\mathfrak{G} = \{x \in \mathfrak{G}_\mathbf{A} \mid \det(\xi^{-1}x) \in K^\times\mathfrak{t}\}. \tag{2.10}$$

Clearly the last set contains the second set. Conversely, suppose $x \in \mathfrak{G}_\mathbf{A}$ and $\det(\xi^{-1}x) = by$ with $b \in K^\times$ and $y \in \mathfrak{t}$. We can find $z, w \in K_\mathbf{A}^\times$ such that $z_v \in \mathfrak{r}_v^\times$ and $w_v w_v^\rho = 1$ for every $v \in \mathbf{h}$ and $y = zw$. We can find $\varepsilon \in E$, $\alpha \in \mathfrak{G}$, and $\gamma \in U(\Phi)_\mathbf{A}$ such that $\det(\varepsilon) = z$, $\det(\alpha) = b$, and $\det(\gamma) = w$. Then $\det(x^{-1}\varepsilon\xi\gamma\alpha) = 1$. By strong approximation in $SL_n(K)$ we see that $x^{-1}\varepsilon\xi\gamma\alpha \in x^{-1}ExSL_n(K)$, and so $x^{-1}\varepsilon\xi\gamma\alpha = x^{-1}\varepsilon' x\beta$ with $\varepsilon' \in E$ and $\beta \in SL_n(K)$. Then $x = (\varepsilon')^{-1}\varepsilon\xi\gamma\alpha\beta^{-1} \in E\xi U(\Phi)_\mathbf{A}\mathfrak{G}$, which proves the last equality of (2.10). That $T\mathfrak{G}$ equals the last set of (2.10) for $\xi = 1$ can be proved in the same way. Thus $T\mathfrak{G}$ is the inverse image of $K^\times\mathfrak{t}$ under the map $x \mapsto \det(x)$, and so $T\mathfrak{G}$ is a normal subgroup of $\mathfrak{G}_\mathbf{A}$. Then we obtain the first isomorphism of (2.9) and also the first equality of (2.10) for every $\xi \in \mathfrak{G}_\mathbf{A}$.

PROPOSITION 2.6. (i) *For $\Phi, \Psi \in \mathfrak{H}_n^0(\xi)$, $\xi \in \mathfrak{G}_\mathbf{A}$, the spaces $[\Phi]$ and $[\Psi]$ are isomorphic if and only if they belong to the same genus.*

(ii) *Let X be a complete set of representatives for $\mathfrak{G}_\mathbf{A}/T\mathfrak{G}$, and for each $\xi \in \mathfrak{G}_\mathbf{A}$ let Y_ξ be a complete set of representatives for the genera of the elements of $\mathfrak{H}_n^0(\xi)$. Then the hermitian spaces $[\Phi]$ obtained from $\Phi \in Y_\xi$ for all $\xi \in X$ exhaust all isomorphism classes of n-dimensional hermitian spaces without overlapping.*

Proof. Let Φ and Ψ be elements of $\mathfrak{H}_n^0(\xi)$ belonging to the same genus. Then there exists an element $\varepsilon \in E_\xi$ such that $\varepsilon\Phi\varepsilon^* = \Psi$, and the Hasse principle guarantees an element α of $\mathfrak{G}$ such that $\Psi = \alpha\Phi\alpha^*$. Thus $[\Psi]$ is isomorphic to $[\Phi]$. Conversely, suppose $[\Phi]$ and $[\Psi]$ are isomorphic for $\Phi, \Psi \in \mathfrak{H}_n^0(\xi)$. Then $\Phi = \beta\Psi\beta^*$ for some $\beta \in \mathfrak{G}$. 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 $\gamma \in U(\Psi)_{\mathbf{A}}$ by Lemma 1.10. Put $\zeta = \beta\gamma^{-1}$. Then $\zeta \in E_\xi$, and $\zeta\Psi\zeta^* = \Phi$. Therefore Ψ belongs to the genus of Φ. This proves (i). Clearly every n-dimensional hermitian space is isomorphic to $[\Psi]$ for some $\Psi \in \mathfrak{H}_n$. Take a maximal lattice L in $K_n^1 = V$ and put $L = L_0\eta$ with $\eta \in \mathfrak{G}_{\mathbf{A}}$. We have then $\eta \in T\mathfrak{G}\xi$ with some $\xi \in X$. By (2.10) we can put $\xi = \varepsilon\eta\gamma\alpha^{-1}$ with $\varepsilon \in E$, $\gamma \in U(\Psi)_{\mathbf{A}}$, and $\alpha \in \mathfrak{G}$. Put $\Phi = \alpha\Psi\alpha^*$. Then α gives an isomorphism of $[\Phi]$ onto $[\Psi]$. Now $L_0\eta\gamma$ is a maximal lattice in $[\Psi]$ and $L_0\xi\alpha = L_0\eta\gamma$, and so $L_0\xi$ is a maximal lattice in $[\Phi]$. Thus $\Phi \in \mathfrak{H}_n^0(\xi)$. By (i), Φ can be replaced by a member of Y_ξ. This shows that every (V, φ) can be obtained as described in (ii). Now suppose $[\Phi_1]$ and $[\Phi_2]$ are isomorphic for $\Phi_i \in Y_{\xi_i}$ with $\xi_1, \xi_2 \in X$. Then $\Phi_1 = \alpha\Phi_2\alpha^*$ with $\alpha \in \mathfrak{G}$. Since $L_0\xi_i$ is maximal, we have $L_0\xi_1\alpha = L_0\xi_2\zeta$ with $\zeta \in U(\Phi_2)_{\mathbf{A}}$. Then $\xi_1\alpha\zeta^{-1}\xi_2^{-1} \in E$, and so $\det(\xi_1\xi_2^{-1}) \in K^\times\mathfrak{t}$. We are taking the ξ_i from X, and therefore $\xi_1 = \xi_2$ by (2.10). By (i), Φ_2 belongs to the genus of Φ_1, and so $\Phi_2 = \Phi_1$. This completes the proof.

2.7. The connection of a class of hermitian matrices with a class of lattices is not so simple in general. Given $\Phi \in \mathfrak{H}_n^0(\xi)$ with a fixed ξ, in order to exhaust all classes in the $U(\Phi)$-genus of $L_0\xi$, we have to consider the genera of elements in $\mathfrak{H}_n^0(\xi\zeta)$ for all $\zeta \in T\mathfrak{G}/E_\xi\mathfrak{G}$. Thus $\mathfrak{H}_n^0(\xi)$ is sufficient if and only if $K^\times\mathfrak{t} = K^\times \det(E)$. We will not go into details, as we do not need the result in our later treatment.

The case of SU-class is simpler. Fix $\xi \in \mathfrak{G}$ and put $L = L_0\xi$. For $\Phi \in \mathfrak{H}_n(\xi)$ we define the *SU-genus* (relative to ξ) of Φ to be the set of all $\Psi \in \mathfrak{H}_n^0(\xi)$ such that $\Psi = \varepsilon\Phi\varepsilon^*$ with $\varepsilon \in E_\xi$ such that $\det(\varepsilon) = 1$. Clearly $\det(\Psi) = \det(\Phi)$. Given such Ψ and ε, the Hasse principle guarantees an element $\alpha \in \mathfrak{G}$ such that $\Psi = \alpha\Phi\alpha^*$. Then $\det(\alpha)\det(\alpha)^\rho = 1$. Changing α for $\alpha\gamma$ with a suitable $\gamma \in U(\Phi)$, we may assume that $\det(\alpha) = 1$. Since $L\alpha = L\varepsilon^{-1}\alpha$ and $\varepsilon^{-1}\alpha \in SU(\Phi)_{\mathbf{A}}$, we see that $L\alpha$ belongs to the $SU(\Phi)$-genus of L. We then associate the $SU(\Phi)$-class of $L\alpha$ to Ψ. We can easily verify that the set of all SU-classes in the SU-genus of Φ contained in $\mathfrak{H}_n(\xi)$ are in one-to-one correspondence with the set of $SU(\Phi)$-classes in the $SU(\Phi)$-genus of L.

2.8. Define (V, φ) by $V = K_n^1$ and $\varphi[x] = x\Phi x^*$ as above with any $\Phi \in \mathfrak{H}_n$. Put $L = L_0\xi$ with $\xi \in \mathfrak{G}_{\mathbf{A}}$. We easily see that $\widehat{L} = \mathfrak{d}^{-1}L_0(\Phi\xi^*)^{-1}$, and so

$$[\widehat{L}/L] = \det(\Phi\xi\xi^\rho)\mathfrak{d}^n \quad \text{if} \quad L = L_0\xi. \tag{2.11}$$

We need a few more symbols. First, we put $\mathfrak{d}_0 = \mathfrak{d}^2 \cap F$. For $v \in \mathbf{r}_0$ and (V, φ)

isomorphic to $[\Phi]$ with $\Phi \in \mathfrak{H}_n$ we put $s_v(\Phi) = s_v(\varphi)$ and $d_0(\Phi) = d_0(\varphi)$.

LEMMA 2.9. *Let B be a quaternion algebra over F and K a quadratic extension of F contained in B; let $\mathfrak{r}$ be the maximal order of K and $\mathfrak{O}$ a maximal order in B containing $\mathfrak{r}$; further let $\mathfrak{e}$ be the product of the prime ideals in F ramified in B and $\mathfrak{d}$ the different of K relative to F. Then there exists a $\mathfrak{g}$-ideal $\mathfrak{a}$ such that $\mathfrak{O}$ is isomorphic as a left $\mathfrak{r}$-module to $\mathfrak{r} \oplus \mathfrak{a}$ and $N_{K/F}(\mathfrak{d}\mathfrak{a}) = s\mathfrak{e}$ with an element s such that B is isomorphic to $\{K, s\}$. Moreover, the coset $\mathfrak{a}\mathfrak{I}^0_{K/F}$ is independent of the choice of $\mathfrak{O}$, and $\mathfrak{O}$ is isomorphic as a right $\mathfrak{r}$-module to $\mathfrak{r} \oplus \mathfrak{a}^\iota$, where ι is the main involution of B.*

Proof. Take $\varepsilon \in F^\times$ so that $B = \{K, \varepsilon\}$, and consider $(V, \varphi) = [\Phi]$ over K with $V = K^1_2$ and φ such that $\varepsilon \in d_0(\varphi)$. Using the symbols y, j of Lemma 1.3, identify $j(\alpha)$ with α for $\alpha \in B$, and put $M = y\mathfrak{O}\gamma$ with $\gamma \in B^\times_{\mathbf{h}}$ such that $\varphi[y]^{-1} = \gamma_v\gamma_v^\iota$ for every $v \in \mathbf{h}$. Applying the local result of §1.11 to M_v, we see that M is maximal and $[\widehat{M}/M] = \mathfrak{e}\mathfrak{r}$. Put $M = \mathfrak{r}^1_2\xi$ with some $\xi \in GL_2(K)_{\mathbf{A}}$ and $\mathfrak{a} = \det(\xi)\mathfrak{r}$. Then by a well-known principle M is $\mathfrak{r}$-isomorphic to $\mathfrak{r} \oplus \mathfrak{a}$. By (2.11) we have $\det(\Phi)N_{K/F}(\mathfrak{d}\mathfrak{a}) = \mathfrak{e}$. Then we obtain the first assertion of our lemma by taking $s = -\det(\Phi)^{-1}$. Let $\mathfrak{O}'$ be another maximal order in B containing $\mathfrak{r}$. By the Chevalley-Hasse-Noether theorem (see [E, Satz 7]) there exists an $\mathfrak{r}$-ideal $\mathfrak{b}$ such that $\mathfrak{b}\mathfrak{O}' = \mathfrak{O}\mathfrak{b}$. Take $c \in K^\times_{\mathbf{A}}$ so that $\mathfrak{b} = c\mathfrak{r}$. Then for each $v \in \mathbf{h}$ we can find $\eta_v \in GL_2(K_v)$ such that $yc_v^{-1}xc_v = yx\eta_v$ for every $x \in B_v$. Then $y\mathfrak{O}'_v = y\mathfrak{O}_v\eta_v$, and so $y\mathfrak{O}' = M\gamma^{-1}\eta$ with $\eta = (\eta_v)_{v\in\mathbf{h}}$. Using the map j in the proof of lemma 1.3, we find that $\eta_v = \mathrm{diag}[1, c_v^\rho/c_v]$, and so $\det(\gamma^{-1}\eta)\mathfrak{r} = \varphi[y]\mathfrak{b}^{-1}\mathfrak{b}^\rho \in \mathfrak{I}^0_{K/F}$. Thus $\det(\xi\gamma^{-1}\eta)\mathfrak{r} \in \mathfrak{a}\mathfrak{I}^0_{K/F}$, which proves the second assertion. We can put $\mathfrak{O} = \mathfrak{r}z + \mathfrak{a}w$ with elements z and w. Applying ι to this, we obtain the last assertion.

We call the coset $\mathfrak{a}\mathfrak{I}^0_{K/F}$ in the above lemma *the characteristic coset of K relative to B*. Using this notion, we now reformulate Theorems 2.2 and 2.3 in terms of the matrices Φ in $\mathfrak{H}^0_n(\xi)$.

THEOREM 2.10 (The case of even n). *Let the symbols n, $\{\sigma_v\}_{v\in\mathbf{r}_0}$, ε, and ξ be given as follows: $0 < n \in 2\mathbf{Z}$, $\sigma_v \in 2\mathbf{Z}$, $|\sigma_v| \le n$; $\varepsilon \in F^\times$, $\xi \in \mathfrak{G}_{\mathbf{A}}$. Let $B = \{K, \varepsilon\}$; let $\mathfrak{e}$ be the product of the prime ideals in F ramified in B, and $\mathfrak{k}$ the characteristic coset of K relative to B. Suppose that $(-1)^{\sigma_v/2}\varepsilon > 0$ at each $v \in \mathbf{r}_0$ and*

$$\det(\xi)\mathfrak{d}^{(n-2)/2} \in \mathfrak{k}. \tag{2.12}$$

Then there exists an element Φ of $\mathfrak{H}^0_n(\xi)$ such that

$$\varepsilon \in d_0(\Phi), \quad \det(\Phi\xi\xi^\rho)\mathfrak{d}_0^{n/2} = \mathfrak{e}, \quad s_v(\Phi) = \sigma_v \text{ for every } v \in \mathbf{r}_0. \tag{2.13}$$

Moreover, every element of $\mathfrak{H}^0_n(\xi)$ is of this type, and the coset $T\mathfrak{G}\xi$ and the genus of Φ are determined by $(\varepsilon N_{K/F}(K^\times), \{\sigma_v\}_{v\in\mathbf{r}_0})$.

Proof. Let the symbols n, $\{\sigma_v\}_{v\in\mathbf{r}_0}$, ε, and ξ be given as in our theorem. Then Theorem 2.2 combined with Proposition 2.6 guarantees an element Ψ of $\mathfrak{H}_n^0(\eta)$ with some $\eta \in \mathfrak{G}_{\mathbf{A}}$ such that $\varepsilon \in d_0(\Psi)$ and $\sigma_v = s_v(\Psi)$ for every $v \in \mathbf{r}_0$. Put $\mathfrak{y} = \det(\eta)\mathfrak{r}$. By Theorem 2.3 (i), (2.11), and Lemma 2.9 we see that $\mathfrak{y}\mathfrak{d}^{(n-2)/2} \in \mathfrak{k}$. Combining this with our condition (2.12), we see that $\mathfrak{y} \in \det(\xi)\mathfrak{I}_{K/F}^0$, and so $\det(\eta^{-1}\xi) \in K^\times\mathfrak{t}$, which implies $\eta \in T\mathfrak{G}\xi$; see (2.9). By Proposition 2.6 (ii), $[\Psi]$ is isomorphic to $[\Phi]$ with some $\Phi \in \mathfrak{H}_n^0(\xi)$. Replacing $(\Psi,\, \eta)$ by $(\Phi,\, \xi)$, we obtain (2.13). This proves the first part of our theorem. Conversely, given $\Phi \in \mathfrak{H}_n^0(\xi)$, put $L = L_0\xi$. Let $\mathfrak{e}$ be the product of the prime ideals in F ramified in $\{K,\, d_0(\varphi)\}$. By Theorem 2.2 (i) and (2.11), $\det(\Phi\xi\xi^\rho)\mathfrak{d}_0^{n/2} = \mathfrak{e}$, which together with Lemma 2.9 implies condition (2.12). This proves the second part. The last part follows from Proposition 2.6.

Theorem 2.11 (The case of odd n). *Let the symbols n, $\{\sigma_v\}_{v\in\mathbf{r}}$, ε, and ξ be given as follows: $0 < n-1 \in 2\mathbf{Z}$, $\sigma_v - 1 \in 2\mathbf{Z}$, $|\sigma_v| \le n$; $\varepsilon \in F^\times$ and $\xi \in \mathfrak{G}_{\mathbf{A}}$. Let $\varepsilon\mathfrak{g} = \mathfrak{a}N_{K/F}(\mathfrak{b})$ with an $\mathfrak{r}$-ideal $\mathfrak{b}$ and a squarefree integral $\mathfrak{g}$-ideal $\mathfrak{a}$ whose prime factors remain prime in K. Suppose $(-1)^{(\sigma_v-1)/2}\varepsilon > 0$ at each $v \in \mathbf{r}_0$ and*

$$\det(\xi)\mathfrak{d}^{(n-1)/2}\mathfrak{b} \in \mathfrak{I}_{K/F}^0. \tag{2.14}$$

Then there exists an element Φ of $\mathfrak{H}_n^0(\xi)$ such that

$$\varepsilon \in d_0(\Phi), \quad \det(\Phi\xi\xi^\rho)\mathfrak{d}_0^{(n-1)/2} = \mathfrak{a}, \quad s_v(\Phi) = \sigma_v \text{ for every } v \in \mathbf{r}_0. \tag{2.15}$$

Moreover, every element of $\mathfrak{H}_n^0(\xi)$ is of this type, and the coset $T\mathfrak{G}\xi$ and the genus of Φ are determined by $(\varepsilon N_{K/F}(K^\times),\, \{\sigma_v\}_{v\in\mathbf{r}_0})$.

This can be proved in exactly the same fashion as for Theorem 2.10.

Lemma 2.12. *Suppose F has class number 1. Then the class number of K is odd if and only if $\mathfrak{I}_K = \mathfrak{I}_{K/F}^0$, in which case $-1 \in N_{K/\mathbf{Q}}(K^\times)$ if and only if $-1 \in N_{K/\mathbf{Q}}(\mathfrak{r}^\times)$.*

Proof. Suppose the class number of K is odd. Then every $\mathfrak{r}$-ideal $\mathfrak{a}$ is of the form $\mathfrak{a} = c\mathfrak{b}^2$ with an $\mathfrak{r}$-ideal $\mathfrak{b}$ and $c \in K^\times$. Thus $\mathfrak{a} = c\mathfrak{b}\mathfrak{b}^\rho\mathfrak{b}(\mathfrak{b}^\rho)^{-1} \in \mathfrak{I}_{K/F}^0$ as $\mathfrak{b}\mathfrak{b}^\rho$ is principal, and so $\mathfrak{I}_K = \mathfrak{I}_{K/F}^0$. Suppose the class number of K is even. Then there exists an $\mathfrak{r}$-ideal $\mathfrak{x}$ whose ideal class is not a square. Suppose $\mathfrak{x} \in \mathfrak{I}_{K/F}^0$. Then $\mathfrak{x} = z\mathfrak{y}^{-1}\mathfrak{y}^\rho$ with $z \in K^\times$ and an $\mathfrak{r}$-ideal $\mathfrak{y}$. Thus $\mathfrak{x} = z\mathfrak{y}\mathfrak{y}^\rho\mathfrak{y}^{-2}$, a contradiction, as $\mathfrak{y}\mathfrak{y}^\rho$ is principal. This proves the first part. To prove the second part, suppose $-1 = \alpha\alpha^\rho$ with $\alpha \in K^\times$; put $\alpha\mathfrak{r} = \mathfrak{b}\mathfrak{c}^{-1}$ with integral $\mathfrak{r}$-deals $\mathfrak{b}$ and $\mathfrak{c}$ that are relatively prime. Then $\mathfrak{b}\mathfrak{b}^\rho = \mathfrak{c}\mathfrak{c}^\rho$ and we easily see that $\mathfrak{b} = \mathfrak{c}^\rho$, and so $\mathfrak{c}^2 = \alpha^{-1}\mathfrak{c}\mathfrak{c}^\rho$, which is principal. If the class number of K is odd, then $\mathfrak{c} = c\mathfrak{r}$ with $c \in \mathfrak{r}$. Thus $\alpha c = \varepsilon c^\rho$ with $\varepsilon \in \mathfrak{r}^\times$. Then $\varepsilon\varepsilon^\rho = \alpha\alpha^\rho = -1$. This completes the proof.

The last statement of the above lemma is false if the class number of K is even. For example, let $K = \mathbf{Q}(\sqrt{34}\,)$. Then the class number is 2 and $-1 = \alpha\alpha^\rho$ with $\alpha = (3 + \sqrt{34}\,)/5$, but $-1 \notin N_{K/\mathbf{Q}}(\mathfrak{r}^\times)$.

2.13. Let us now take K to be a real or an imaginary quadratic field whose class number is odd. We denote by d the discriminant of K. Thus $F = \mathbf{Q}$ and $K = \mathbf{Q}(\sqrt{d}\,)$. By Lemma 2.12 we have $\mathfrak{I}_K = \mathfrak{I}^0_{K/F}$, and so $\mathfrak{G}_\mathbf{A} = T\mathfrak{G}$ by (2.9). Therefore by Proposition 2.6, every hermitian space over K is isomorphic to $[\Phi]$ with $\Phi \in \mathfrak{H}^0_n(1_n)$, and $\mathfrak{r}^1_n$ is a maximal lattice in it. For simplicity we put $\mathfrak{H}^1_n = \mathfrak{H}_n(1_n)$ and $\mathfrak{H}^0_n = \mathfrak{H}^0_n(1_n)$. Then $\mathfrak{H}^1_n$ consists of all $\Phi = (c_{ij}) \in \mathfrak{H}_n$ such that $\sqrt{d}\,c_{ij} \in \mathfrak{r}$ and $c_{ii} \in \mathbf{Z}$ for every i and j; $\mathfrak{H}^0_n$ consists of all $\Phi \in \mathfrak{H}^1_n$ satisfying the following condition:

(2.16) *If* $\Phi = P\Psi P^*$, $\Psi \in \mathfrak{H}^1_n$, *and* $P \in GL_n(K) \cap M_n(\mathfrak{r})$, *then* $\det(P) \in \mathfrak{r}^\times$.

For $\Phi \in \mathfrak{H}_n$ we put $s(\Phi) = p - q$ if K is imaginary and Φ as a complex hermitian matrix has p positive and q negative eigenvalues; we put $s(\Phi) = 0$ if $d > 0$ and $n \in 2\mathbf{Z}$; we do not define $s(\Phi)$ if $d > 0$ and $n \notin 2\mathbf{Z}$, and so the symbol $s(\Phi)$ in that case must be ignored. Clearly two elements Φ_1 and Φ_2 of $\mathfrak{H}^1_n$ belong to the same genus if $s(\Phi_1) = s(\Phi_2)$ and $\Phi_1 = P_v\Phi_2P_v^*$ with some $P_v \in GL_n(\mathfrak{r}_v)$ for every $v \in \mathbf{h}$. Now, for $L = \mathfrak{r}^1_n$ we have $[\widehat{L}/L] = \det(\sqrt{d}\,\Phi)\mathfrak{r}$ by (2.11). For $d > 0$ we fix an embedding of K into $\mathbf{R}$, and take $\sqrt{d} > 0$.

THEOREM 2.14 (The case of even n). *Let $K = \mathbf{Q}(\sqrt{d}\,)$ as in §2.13, and let three integers n, σ, and e be given as follows: $0 < n \in 2\mathbf{Z}$, $\sigma \in 2\mathbf{Z}$, $|\sigma| \le n$; $\sigma = 0$ if $d > 0$; e is positive and squarefree. Let r be the number of prime factors of e. Suppose that $\sigma - 2r \in 4\mathbf{Z}$ and no prime factor of e splits in K. Then there exists an element Φ of $\mathfrak{H}^0_n$ such that*

$$\det(\sqrt{d}\,\Phi) = (-1)^{\sigma/2}e \quad \textit{and} \quad s(\Phi) = \sigma \quad \textit{if } d < 0, \tag{2.17a}$$

$$\det(\sqrt{d}\,\Phi) = \tau e \quad \textit{with} \quad \tau = 1 \textit{ or } -1 \quad \textit{if } d > 0. \tag{2.17b}$$

Moreover, every element of $\mathfrak{H}^0_n$ is of this type. Its genus is determined by (σ, e) if $d < 0$, and by e if $d > 0$. If $d > 0$ and $-1 \in N_{K/\mathbf{Q}}(K^\times)$, then both e and $-e$ can occur as $\det(\sqrt{d}\,\Phi)$ for Φ in the same genus. If $d > 0$ and $-1 \notin N_{K/\mathbf{Q}}(K^\times)$, then τ is uniquely determined by the condition that a prime number p divides e if and only if $\tau e \notin N_{K/\mathbf{Q}}(K_p^\times)$.

Proof. Given (n, σ, e) as in our theorem, we can find a quaternion algebra B over $\mathbf{Q}$ which is ramified at p if and only if $p|e$. Then B is definite if and only if r is odd. Since $\sigma - 2r \in 4\mathbf{Z}$, we see that $d < 0$ if r is odd. Our assumption on the prime factors of e allows us to put $B = \{K, \varepsilon\}$ with $\varepsilon \in \mathbf{Q}^\times$. Then $(-1)^{\sigma/2}\varepsilon > 0$ if $d < 0$. By Theorem 2.10, we obtain $\Phi \in \mathfrak{H}^0_n$ satisfying (2.13) with $\xi = 1_n$, as (2.12) can be ignored. Then $\mathfrak{e} = e\mathbf{Z}$ and $\det(\sqrt{d}\,\Phi) = \tau e$ with $\tau = \pm 1$. Since $s(\Phi) = \sigma$, we see that $\tau = (-1)^{\sigma/2}$ if $d < 0$. The same theorem says that every element of $\mathfrak{H}_n^0$ is of this type, and its genus is determined by $\varepsilon N_{K/F}(K^\times)$ and σ. We easily see that $(e,\,\sigma)$ determines $(\varepsilon N_{K/F}(K^\times),\,\sigma)$, and vice versa. If $-1 \in N_{K/\mathbf{Q}}(K^\times)$, then by Lemma 2.12, $\mathfrak{r}^\times$ contains an element ζ such that $\zeta\zeta^\rho = -1$. Then $\det(P\Phi P^*) = -\det(\Phi)$ for $P = \mathrm{diag}[\zeta,\,1_{n-1}]$. Thus both e and $-e$ can happen. Suppose $d > 0$ and $-1 \notin N_{K/\mathbf{Q}}(K^\times)$. Then $\{K,\,e\}$ is not isomorphic to $\{K,\,-e\}$. Since $-d \in N_{K/\mathbf{Q}}(K^\times)$, $d_0(\varphi)$ is represented by $\det(\sqrt{d}\Phi)$. If $\det(\sqrt{d}\Phi) = \tau e$, then $B = \{K,\,\tau e\}$. Thus τ is uniquely determined by the condition that a prime number p divides e if and only if $\tau e \notin N_{K/\mathbf{Q}}(K_p^\times)$.

Theorem 2.15 (The case of odd n). *Let $K = \mathbf{Q}(\sqrt{d}\,)$ as in §2.13 and let four integers n, σ, τ, and e be given as follows: $0 < n-1 \in 2\mathbf{Z}$; σ is necessary only if $d < 0$, $\sigma - 1 \in 2\mathbf{Z}$, and $|\sigma| \le n$; τ is necessary only if $d > 0$, and $\tau = 1$ or -1; e is positive and squarefree, and every prime factor of e remains prime in K. Then there exists an element Φ of $\mathfrak{H}_n^0$ such that*

$$\det(\sqrt{d}\,\Phi) = (-1)^{(\sigma-1)/2} e\sqrt{d} \quad \text{and} \quad s(\Phi) = \sigma \quad \text{if } d < 0, \tag{2.18a}$$

$$\det(\sqrt{d}\,\Phi) = \tau e\sqrt{d} \quad \text{if } d > 0. \tag{2.18b}$$

Moreover, every element of $\mathfrak{H}_n^0$ is of this type, and its genus is determined by $(\sigma,\,e)$ if $d < 0$ and by $(\tau,\,e)$ if $d > 0$. For $d > 0$ the sets $(1,\,e)$ and $(-1,\,e)$ determine the same genus if and only if $-1 \in N_{K/\mathbf{Q}}(K^\times)$.

Proof. Given $(n,\,\sigma,\,\tau,\,e)$ as in our theorem, take $\varepsilon = (-1)^{(\sigma-1)/2}e$ if $d < 0$ and $\varepsilon = (-1)^{(n-1)/2}\tau e$ if $d > 0$. Then Theorem 2.11 with $\xi = 1_n$ and $\mathfrak{a} = e\mathbf{Z}$ guarantees an element Φ of $\mathfrak{H}_n^0$ satisfying (2.15). We can easily verify that (2.18a, b) hold. That every $\Phi \in \mathfrak{H}_n^0$ is of this type also follows from Theorem 2.11, as $d_0(\Phi)$ can be represented by e or $-e$ with a positive integer e as in our theorem. Since the last assertion is obvious, our proof is complete.

Corollary 2.16. *Let $K = \mathbf{Q}(\sqrt{d}\,)$ and $\mathfrak{H}_n^1$ be as in §2.13; let $0 < n \in \mathbf{Z}$ and $\sigma \in \mathbf{Z}$.*

(i) *If $d < 0$, there exists an element Φ of $\mathfrak{H}_n^1$ such that $\det(\sqrt{d}\,\Phi) = 1$ and $s(\Phi) = \sigma$ exactly when $n \in 2\mathbf{Z}$ and $\sigma \in 4\mathbf{Z}$.*

(ii) *Suppose $d > 0$; then there exists an element Φ of $\mathfrak{H}_n^1$ such that $\det(\sqrt{d}\,\Phi) = 1$ if and only if $n \in 2\mathbf{Z}$. Moreover, there exists an element Φ' of $\mathfrak{H}_n^1$ such that $\det(\sqrt{d}\,\Phi') = -1$ if and only if $n \in 2\mathbf{Z}$ and $-1 \in N_{K/\mathbf{Q}}(K^\times)$.*

Proof. From Theorem 2.15 we see that $\det(\sqrt{d}\,\Phi) = \pm 1$ for $\Phi \in \mathfrak{H}_n^1$ cannot happen if n is odd. Take $e = 1$ in Theorem 2.14. Then $r = 0$, and we obtain our results immediately from that theorem. Notice that if $d > 0$ and $-1 \notin N_{K/\mathbf{Q}}(K^\times)$, then $\{K,\,-1\}$ is a division algebra, and so $-1 \notin N_{K/\mathbf{Q}}(K_p^\times)$ for some prime number p.

The above corollary is a natural analogue of a well-known fact on unimodular quadratic form over $\mathbf{Q}$.

2.17. EXAMPLES. (2) Take $n = 2$, $d = 21$, and $e_1 = 11 \cdot 13$; then the class number of K is 1 and $-1 \notin N_{K/\mathbf{Q}}(K^\times)$. For $\Phi_1 = \begin{bmatrix} 7 & 2/\sqrt{21} \\ -2/\sqrt{21} & -1 \end{bmatrix}$ we have $\det(\sqrt{21}\,\Phi_1) = -e_1$ and $\Phi_1 \in \mathfrak{H}_2^0$. But we cannot have $\det(\sqrt{21}\,\Phi) = e_1$ for $\Phi \in \mathfrak{H}_2^0$.

Next take $e_2 = 3 \cdot 7 \cdot 11 \cdot 13$. Then $\det(\sqrt{21}\,\Phi)$ for $\Phi \in \mathfrak{H}_2^0$ can be $-e_2$ but cannot be e_2. Also, $\{K,\, 11 \cdot 13\}$ is ramified at $p = 3, 7,$ but $\{K,\, -11 \cdot 13\}$ is not. From this we can derive that $\mathrm{diag}[11,\, -13]$ is reduced, but $\mathrm{diag}[11,\, 13]$ is not.

3. HERMITIAN DIOPHANTINE EQUATIONS OVER A LOCAL FIELD

3.1. Throughout this section we fix (V, φ) in the local case, and put $n = \dim(V)$. We denote by $\mathfrak{p}$ the maximal ideal of $\mathfrak{g}$, and by t the core dimension of (V, φ). Then $t \le 2$ as observed in §2.1. For an $\mathfrak{r}$-lattice L in V we put

$$C(L) = \{\alpha \in U^\varphi(V) \,|\, L\alpha = L\}, \qquad C^1(L) = C(L) \cap SU^\varphi(V). \tag{3.1}$$

Define $L[q,\, \mathfrak{b}]$ and $L[q]$ by (1.10b, c). Clearly $L[q,\, \mathfrak{b}]$ and $L[q]$ are stable under right multiplication by the elements of $C(L)$, and so the four orbit sets $L[q,\, \mathfrak{b}]/C(L)$, $L[q]/C(L)$, $L[q,\, \mathfrak{b}]/C^1(L)$, and $L[q]/C^1(L)$ are meaningful. Now our principal results of this section are the following two theorems.

THEOREM 3.2. *Suppose that F is local and $n > 1$. Let L be a maximal $\mathfrak{r}$-lattice in V. Then for every $q \in F^\times$ and every $\mathfrak{r}$-ideal $\mathfrak{b}$ the following assertions hold:*

(i) $\#\{L[q,\, \mathfrak{b}]/C(L)\} \le 1$.

(ii) $\#\{L[q,\, \mathfrak{b}]/C^1(L)\} < \infty$.

(iii) $\#\{L[q,\, \mathfrak{b}]/C^1(L)\} \le 1$ *if we exclude the following two cases:* (a) $n = 2$ *and* $t = 0$; (b) $t = 1$, $q\mathfrak{r} = \mathfrak{b}\mathfrak{b}^\rho$, *and* $\mathfrak{d} \ne \mathfrak{r}$.

(iv) *If* $n = 2$ *and* $t = 0$, *then*

$$\#\{L[q,\, \mathfrak{d}^{-1}]/C^1(L)\} = \begin{cases} 1 & \text{if } \; q \in \mathfrak{g}^\times, \\ N(q\mathfrak{g})\big[1 - \{K/F\}N(\mathfrak{p})^{-1}\big] & \text{if } \; q \in \mathfrak{p}, \end{cases} \tag{3.2}$$

where $N(\mathfrak{a}) = \#(\mathfrak{g}/\mathfrak{a})$, *and* $\{K/F\} = 1,\, -1$, *or* 0, *according as* $K = F \times F$, K *is an unramified quadratic extension of* F, *or* K *is ramified over* F.

(v) $L[q,\, \mathfrak{d}^{-1}] \ne \emptyset$ *exactly in the following cases:* (a) $t = 0$ *and* $q \in \mathfrak{g}$; (b) $t = 1$, $\mathfrak{d} = \mathfrak{r}$, $d_0(\varphi) = N_{K/F}(K^\times)$, *and* $q \in \mathfrak{g}$; (c) $t = 1$, $d_0(\varphi) \not\subset \mathfrak{g}^\times N_{K/F}(K^\times)$, *and* $q \in \mathfrak{p}^{-1}$; (d) $t = 1$, $\mathfrak{d} \ne \mathfrak{r}$, *and* $q \in \mathfrak{p}\mathfrak{d}^{-2} \cup \big(\mathfrak{d}^{-2} \cap d_0(\varphi)\big)$; (e) $n = t = 2$ *and* $\mathfrak{g} \subset q\mathfrak{g} \subset \mathfrak{p}^{-1}$ *if* $\mathfrak{d} = \mathfrak{r}$; $q\mathfrak{g} = \mathfrak{p}^{-1}$ *if* $\mathfrak{d} \ne \mathfrak{r}$; (f) $n > 2 = t$ *and* $q \in \mathfrak{p}^{-1}$.

The proof will be given in §3.6 through §3.12.

The quantity $\#\{L[q,\, \mathfrak{b}]/C^1(L)\}$ in Case (b) of (iii) is not so simple. We will discuss that case in Lemma 3.13 (ii).

For every $\alpha \in U^\varphi$ we have $C(L\alpha) = \alpha^{-1}C(L)\alpha$, $C^1(L\alpha) = \alpha^{-1}C^1(L)\alpha$, and $(L\alpha)[q,\, \mathfrak{b}] = L[q,\, \mathfrak{b}]\alpha$. Therefore, in view of Lemma 1.10 (i), it is sufficient to prove Theorem 3.2 for a special choice of L. Also, since $c \cdot L[q,\, \mathfrak{b}] = L[cc^\rho q,\, c\mathfrak{b}]$ for every $c \in K^\times$, it is sufficient to prove our theorem when $\mathfrak{b} = \mathfrak{d}^{-1}$ or $\mathfrak{b} = \mathfrak{r}$.

Theorem 3.3. *If $n > 1$, we have $\#\big\{\Lambda[q]/C^1(\Lambda)\big\} < \infty$ for every $q \in F^\times$ and every $\mathfrak{r}$-lattice Λ in V.*

Proof. Let L be a maximal lattice in V. Given Λ, we can find $c \in F^\times$ such that $c\Lambda \subset L$. Then $c\Lambda[q] \subset L[c^2q]$. For any two open compact subgroups D and E of SU^φ we have $[D : D \cap E] < \infty$. Therefore it is sufficient to prove that $\#\big\{L[q]/C^1(L)\big\} < \infty$. Given $h \in L[q]$, put $\mathfrak{b} = \varphi(h,\, L)$. Then $q\mathfrak{r} \subset \mathfrak{b} \subset \mathfrak{d}^{-1}$, and hence $L[q] \subset \bigcup_{\mathfrak{b}} L[q,\, \mathfrak{b}]$, where $\mathfrak{b}$ runs over the $\mathfrak{r}$-ideals $\mathfrak{b}$ such that $q\mathfrak{r} \subset \mathfrak{b} \subset \mathfrak{d}^{-1}$. Therefore the desired fact follows from Theorem 3.2 (ii).

Lemma 3.4. *Let L be a maximal lattice in V. Suppose $\dim(V) > 1$ and $q \in \mathfrak{g}^\times$; then $\#\big\{L[q,\, \mathfrak{r}]/C(L)\big\} \le 1$. Moreover, $\#\big\{L[q,\, \mathfrak{r}]/C^1(L)\big\} \le 1$ if K is a field unramified over F, or the core dimension of $(Kh)^\perp$ is not 0 for some $h \in L[q,\, \mathfrak{r}]$.*

Proof. Let $h,\, k \in L[q,\, \mathfrak{r}]$. We see that $L + \mathfrak{r}h$ is integral, and so $h \in L$, as L is maximal. Given $x \in L$, put $y = x - \varphi[h]^{-1}\varphi(x,\, h)h$. Then $y \in L \cap (Kh)^\perp$. From this we can derive that $L = \mathfrak{r}h \oplus M$ with $M = L \cap (Kh)^\perp$. Similarly $L = \mathfrak{r}k \oplus M'$ with $M' = L \cap (Kk)^\perp$. Since L is maximal, M and M' must be maximal. By (1.5) we can find an element α of $SU^\varphi(V)$ such that $k = h\alpha$. Then $M\alpha$ is a maximal lattice in $(Kk)^\perp$. By Lemma 1.10 (i) we can find an element β of $U^\varphi\big((Kk)^\perp\big)$ such that $M\alpha\beta = M'$; by Lemma 1.10 (ii) such a β can be taken from $SU^\varphi\big((Kk)^\perp\big)$ if K is a field unramified over F, or the core dimension of $(Kk)^\perp$ is not 0. Extend β to V by putting $k\beta = k$. Then $\alpha\beta \in C(L)$ and $h\alpha\beta = k$. We have $\alpha\beta \in C^1(L)$ under the said conditions on K or on Kk. This proves our lemma. Notice that the core dimension of $(Kh)^\perp$ depends only on $hU(\varphi)$.

3.5. We call an element x of $\mathfrak{r}_n^1$ *primitive* if $x\mathfrak{r}_1^n = \mathfrak{r}$. Replacing $\mathfrak{r}$ by $\mathfrak{g}$, we can similarly define the primitive elements of $\mathfrak{g}_n^1$. Given an integral $\mathfrak{r}$-lattice L in V, identify V and L with K_n^1 and $\mathfrak{r}_n^1$ with respect to an $\mathfrak{r}$-basis $\{z_i\}_{i=1}^n$ of L; also let $\varphi_0 = \big(\varphi(z_i,\, z_j)\big)_{i,j=1}^n$. By (1.9) we have $\delta\varphi_0 \prec \mathfrak{r}$ for any element δ of $\mathfrak{r}$ such that $\delta\mathfrak{r} = \mathfrak{d}$. Moreover, $\varphi(x,\, L) = \mathfrak{d}^{-1}$ for $x \in L = \mathfrak{r}_n^1$ if and only if $\delta x\varphi_0$ is primitive.

To prove Theorem 3.2, we fix a maximal lattice L in V, and hereafter write simply C and C^1 for $C(L)$ and $C^1(L)$; we always assume $n > 1$.

3.6. In this subsection we consider the case $K = F \times F$, using the notation of §1.8. We can put $L = \mathfrak{g}_n^1 \times \mathfrak{g}_n^1$.

Let $h = (a, b) \in L[q, \mathfrak{r}]$ with $a, b \in F_n^1$. Then $\varphi(h, L) = (a\mathfrak{g}_1^n, b\mathfrak{g}_1^n)$, and so both a and b are primitive. Let $\{e_i\}_{i=1}^n$ be the standard basis of F_n^1. Take $\alpha \in SL_n(\mathfrak{g})$ so that $a\alpha = e_1$ and put $c = b \cdot {}^t\alpha^{-1} = (c_i)_{i=1}^n$. Then $c_1 = q$. Suppose $q \in \mathfrak{g}^\times$; then define $\beta \in SL_n(\mathfrak{g})$ by $\beta = \begin{bmatrix} 1 & x \\ 0 & 1_{n-1} \end{bmatrix}$ with $x = (q^{-1}c_2, \ldots, q^{-1}c_n)$ and put $\gamma = \alpha \cdot {}^t\beta$. Then $a\gamma = e_1$ and $b \cdot {}^t\gamma^{-1} = c\beta^{-1} = qe_1$. Thus $L[q, \mathfrak{r}]/C^1$ is represented by (e_1, qe_1) if $q \in \mathfrak{g}^\times$.

Next suppose $q \in \mathfrak{p}$; then $(c_2, \ldots, c_n)$ is primitive, and so we can find $\beta \in GL_{n-1}(\mathfrak{g})$ such that $(c_2, \ldots, c_n)\beta = (1, 0, \ldots, 0)$. Put $\gamma = \alpha \cdot \mathrm{diag}[1, {}^t\beta^{-1}]$. Then $a\gamma = e_1$ and $b \cdot {}^t\gamma^{-1} = (q, 1, 0, \ldots, 0)$. This shows that $\#\{L[q, \mathfrak{r}]/C\} = 1$. If $n > 2$, we can take $\beta \in SL_{n-1}(\mathfrak{g})$, and hence $\#\{L[q, \mathfrak{r}]/C^1\} = 1$.

Finally suppose $n = 2$ and $q \in \mathfrak{p}$; then we have shown that $L[q, \mathfrak{r}]/C^1$ can be represented by the elements of the form $\bigl(e_1, (q, s)\bigr)$ with $s \in \mathfrak{g}^\times$. Suppose $\bigl(e_1, (q, s)\bigr)\alpha = \bigl(e_1, (q, t)\bigr)$ with $\alpha = (\gamma, {}^t\gamma^{-1}) \in C^1$, $\gamma \in SL_2(\mathfrak{g})$, and $s, t \in \mathfrak{g}^\times$. Clearly $\gamma = \begin{bmatrix} 1 & 0 \\ v & 1 \end{bmatrix}$ with $v \in \mathfrak{g}$, and so $t = s - qv$. Since the procedure is reversible, we see that $\#\{L[q, \mathfrak{r}]/C^1\} = \#(\mathfrak{g}/q\mathfrak{g})^\times$, which gives (3.2) for $K = F \times F$. This completes the proof of Theorem 3.2 in the case $K = F \times F$.

Hereafter from §3.7 through §3.12 we assume that K is a field.

3.7. Let us consider the case $n = t = 2$. Let the symbols be as in Lemma 1.3 and §1.11; we identify B with $j(B)$. In view of Lemma 1.6 we can take $\varphi[\ell] = c = 1$ in the proof of Lemma 1.3, and so we can take $\gamma = 1$ in §1.11. Thus $M = \ell\mathfrak{O}$. Since φ is anisotropic, $SU^\varphi(V) = C^1(M) = \bigl\{\alpha \in \mathfrak{O}^\times \bigm| \alpha\alpha^\iota = 1\bigr\}$. From (1.5) we see that $\#\bigl\{M[q, \mathfrak{d}^{-1}]/C^1\bigr\} = 1$ if $M[q, \mathfrak{d}^{-1}] \neq \emptyset$. Since $\mathrm{Tr}_{K/F}\bigl(\varphi(\ell\alpha, \ell\beta)\bigr) = \mathrm{Tr}_{B/F}(\alpha\beta^\iota)$ for $\alpha, \beta \in B$, we have $\varphi(\ell\alpha, M) = \mathfrak{d}^{-1}$ only if $\mathrm{Tr}_{B/F}(\alpha\mathfrak{O}) = \mathfrak{g}$, which is so if and only if $\alpha\mathfrak{O} = \mathfrak{O}$ or $\alpha\mathfrak{O} = \mathfrak{P}^{-1}$. Take such an α and assume that K is unramified over F. Then $\ell\alpha \in M[\alpha\alpha^\iota, \mathfrak{r}]$. Thus $M[q, \mathfrak{d}^{-1}] \neq \emptyset$ if and only if $q\mathfrak{g}$ is $\mathfrak{g}$ or $\mathfrak{p}^{-1}$. Next suppose that K is ramified over F. Clearly $M[q, \mathfrak{d}^{-1}] \neq \emptyset$ for some q, and $q\mathfrak{g}$ is $\mathfrak{g}$ or $\mathfrak{p}^{-1}$ for the same reason as above. Suppose $q \in \mathfrak{g}^\times$. Then we can find an element $\xi \in \mathfrak{O}^\times$ such that $\xi\xi^\iota = q$. Then $\varphi[x\xi] = q\varphi[x]$ for every $x \in V$, $M\xi = M$, and $M[1, \mathfrak{b}]\xi = M[q, \mathfrak{b}]$. Let $d_0(\varphi) = sN_{K/F}(K^\times)$ as in the proof of Lemma 1.3. We may assume that $s \in \mathfrak{g}^\times$, $s \notin N_{K/F}(\mathfrak{r}^\times)$, and $\varphi_0 = \mathrm{diag}[1, -s]$. Observe that $\mathfrak{O}$ consists of the elements $a + b\omega$ with $a, b \in K$ such that $a + a^\rho \in \mathfrak{g}$ and $aa^\rho - sbb^\rho \in \mathfrak{g}$. Now let $\ell\alpha \in M[1, \mathfrak{d}^{-1}]$ with $\alpha \in B$. Then $\alpha\alpha^\iota = 1$, and so $\ell \in M[1, \mathfrak{d}^{-1}]$. Thus $\mathfrak{d}^{-1} = \varphi(\ell, M) = \varphi(\ell, \ell\mathfrak{O})$. For $a + b\omega \in \mathfrak{O}$ as above, we have $\varphi(\ell, \ell(a + b\omega)) = a^\rho$, and so $\mathfrak{O}$ contains an element $a + b\omega$ such that $a\mathfrak{r} = \mathfrak{d}^{-1}$. Put $N_{K/F}(\mathfrak{d}) = \mathfrak{p}^\kappa$ with $0 < \kappa \in \mathbf{Z}$. Then $aa^\rho\mathfrak{g} = \mathfrak{p}^{-\kappa}$, and $bb^\rho\mathfrak{g} = \mathfrak{p}^{-\kappa}$ as $aa^\rho - sbb^\rho \in \mathfrak{g}$. Putting $a^{-1}b = c$, we obtain $scc^\rho - 1 \in \mathfrak{p}^\kappa$, a contradiction, as $s \notin N_{K/F}(\mathfrak{r}^\times)$. Thus $M[q, \mathfrak{d}^{-1}] \neq \emptyset$ only if $q\mathfrak{g} = \mathfrak{p}^{-1}$. This proves Theorem 3.2 when $n = t = 2$.

3.8. Take an element $u \in \mathfrak{r}$ so that $\mathfrak{r} = \mathfrak{g}[u]$ and put $\delta = u - u^\rho$. Then $\mathfrak{d} = \delta\mathfrak{r}$ and $\delta^\rho = -\delta$. We will often use these u and δ in our later treatment.

Take a decomposition of V as in (1.8a, b), and assume that it is a Witt decomposition; thus $t = \dim(Z)$. Put $g_i = \delta^{-1} f_i$ and

$$L = \sum_{i=1}^{r} (\mathfrak{r}e_i + \mathfrak{r}g_i) + M, \qquad M = \bigl\{ y \in Z \,\big|\, \varphi[y] \in \mathfrak{g} \bigr\}. \tag{3.3}$$

Then L is a maximal lattice in V as noted in §1.7. With an $\mathfrak{r}$-basis $\{m_i\}_{i=1}^t$ of M, consider matrix representation with respect to $\{e_1, \dots, e_r, m_1, \dots, m_t, g_1, \dots, g_r\}$. Then φ is represented by

$$\varphi_0 = \begin{bmatrix} 0 & 0 & -\delta^{-1}1_r \\ 0 & \zeta & 0 \\ \delta^{-1}1_r & 0 & 0 \end{bmatrix}, \tag{3.4}$$

where $\zeta = \bigl(\varphi(m_i, m_j)\bigr)_{i,j=1}^t$. Now write an element of $GL(V)$ as a matrix with 9 matrix blocks corresponding to the blocks of (3.4), and let P be the group consisting of the elements of U^φ whose lower left 3 blocks under the diagonal blocks are all 0; also let $P^1 = P \cap SU^\varphi$. Then

$$U^\varphi = PC(L) \quad \text{and} \quad SU^\varphi = P^1C^1(L); \tag{3.5}$$

see [S2, Proposition 5.16]. If $r = 1$, P consists of the matrices of the form

$$\begin{bmatrix} a & b & a^{-\rho}(s + u^\rho b\zeta b^*) \\ 0 & e & -\delta a^{-\rho} e\zeta b^* \\ 0 & 0 & a^{-\rho} \end{bmatrix}, \tag{3.6}$$

where $a \in K^\times$, $b \in K_t^1$, $e \in U^\zeta(Z)$, and $s \in F$.

3.9. The case $t = 0$. Represent the elements of V by row vectors in $K_r^1 \times K_r^1$ with respect to the basis $\{e_1, \dots, e_r, g_1, \dots, g_r\}$, and $GL(V)$ by $GL_{2r}(K)$, acting on the right. Then for $h = (y, z) \in K_r^1 \times K_r^1$ we have $\varphi[h] = \delta^{-1}(zy^* - yz^*)$ and $\varphi(h, L) = \delta^{-1} \sum_{i=1}^r (\mathfrak{r}y_i + \mathfrak{r}z_i)$. Now φ is represented by $\delta^{-1}\eta$, where

$$\eta = \begin{bmatrix} 0 & -1_r \\ 1_r & 0 \end{bmatrix}.$$

Therefore $\mathrm{diag}[\alpha, \widetilde{\alpha}] \in U^\varphi$ for every $\alpha \in GL_r(K)$, where $\widetilde{\alpha} = (\alpha^*)^{-1}$. Suppose $\varphi(h, L) = \mathfrak{d}^{-1}$ for $h = (y, z)$; then $\sum_{i=1}^r (\mathfrak{r}y_i + \mathfrak{r}z_i) = \mathfrak{r}$ and $\varphi[h] \in \mathfrak{g}$. Putting $k = (e_1, qug_1)$ with $q \in F$ (not necessarily $\neq 0$), let us prove

$$\varphi[h] = q \ \textit{and} \ \varphi(h, L) = \mathfrak{d}^{-1} \implies h \in kC(L); \ h \in kC^1(L) \ \textit{if} \ r > 1. \tag{3.7}$$

Since $\eta \in C^1$, changing h for $h\eta$ if necessary, we may assume that $\sum_{i=1}^r \mathfrak{r}y_i = \mathfrak{r}$. We can find an element $\alpha \in GL_r(\mathfrak{r})$ such that $y\alpha = e_1$; we can even take α from $SL_r(\mathfrak{r})$ if $r > 1$. Put $w = z\widetilde{\alpha}$. Then $(y, z)\mathrm{diag}[\alpha, \widetilde{\alpha}] = (e_1, w)$, and so $w_1 - w_1^\rho = q\delta$. Thus we can put $w_1 = p + qu$ with $p \in \mathfrak{g}$. Define an element $s = s^* \in M_r(\mathfrak{r})$ so that $s_{11} = p$ and $s_{1j} = w_j$ for $j > 1$, and put

$\beta = \begin{bmatrix} 1_r & s \\ 0 & 1_r \end{bmatrix}$. Then $\beta \in C^1$ and $k\beta = (e_1, w)$. If $r > 1$, then we see that $h \in kC^1$, and so $L[q, \mathfrak{d}^{-1}] = kC^1$. This proves (3.7) and also Theorem 3.2 (i), (iii), (v) when $t = 0$.

Suppose $r = 1$; then $y \in \mathfrak{r}^\times$. Since C^1 is a normal subgroup of C, the above argument shows that $h \in \bigcup_t (t, t^{-\rho}qu)C^1$, where t runs over $\mathfrak{r}^\times$. Define B as in Lemma 1.3. From (1.7b), (1.15), and the last equality in the proof of Lemma 1.3 we obtain $B = M_2(F)$, $SU^\varphi = SL_2(F)$, and $C^1 = SL_2(\mathfrak{g})$. Let $t \in \mathfrak{r}^\times \cap \mathfrak{g}[qu]$. Then $t = a + cqu$ with $a, c \in \mathfrak{g}$, and we can find an element $\gamma \in SL_2(\mathfrak{g})$ of the form $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. We have $(1, qu)\gamma = (t, t^{-\rho}v)$ with $v \in \mathfrak{r}$. Then $v - v^\rho = q\delta$, so that $v = qu - s$ with $s \in \mathfrak{g}$. Since $tt^\rho \in \mathfrak{g}^\times$, we can put $s = tt^\rho s'$ with $s' \in \mathfrak{g}$. Put $\sigma = \begin{bmatrix} 1 & s' \\ 0 & 1 \end{bmatrix}$. Then $\sigma \in C^1$ and $(t, t^{-\rho}v)\sigma = (t, t^{-\rho}qu)$, which shows that $(t, t^{-\rho}qu) \in (1, qu)C^1$ if $t \in \mathfrak{g}[qu]$. Since the converse is obvious, we thus obtain $L[q, \mathfrak{d}^{-1}] = \bigsqcup_{t\in\tau}(t, t^{-\rho}qu)C^1$, where $\tau = \mathfrak{r}^\times/\mathfrak{g}[qu]^\times$. This proves (3.2) and completes the proof of Theorem 3.2 when $t = 0$.

3.10. The notation being as in (3.3), put $H_j = \sum_{i=1}^{j}(Ke_i + Kg_i)$. Let us now show that given $h \in V$, there exists an element α of C^1 such that $h\alpha \in H_1 + Z$. This is obvious if $h \in Z$ or $r = 1$. So assume that $h \notin Z$ and $r > 1$. Put $h = w + k$ with $k \in Z$ and $w = \sum_{i=1}^{r}(y_i e_i + z_i g_i) \in H_r$, $y_i, z_i \in K$. Then we can put $\sum_{i=1}^{r}(y_i\mathfrak{r} + z_i\mathfrak{r}) = d\mathfrak{r}$ with $d \in K^\times$. Taking $d^{-1}w$ as h of (3.7), we can find an element $\gamma \in C^1(L \cap H_r)$ such that $d^{-1}w\gamma \in H_1$. Extend γ to an element of $C^1(L)$ by defining $x\gamma = x$ for every $x \in Z$. Then we obtain the desired fact. This means that if $n > t > 0$, then it is sufficient to prove Theorem 3.2 when $r = 1$.

3.11. Case $t > 0$, $r = 1$. Writing simply e and g for e_1 and g_1, we have $V = Ke + Z + Kg$ and $L = \mathfrak{r}e + M + \mathfrak{r}g$ with a maximal lattice M in Z. Let $h = ye + x + zg$ with $y, z \in K$ and $x \in Z$. Then $\varphi[h] = \delta^{-1}(zy^\rho - yz^\rho) + \zeta[x]$, where ζ is the restriction of φ to Z, and $\varphi(h, L) = \delta^{-1}(\mathfrak{r}y + \mathfrak{r}z) + \zeta(x, M)$. Suppose $h \in L[q, \mathfrak{d}^{-1}]$. Then $\mathfrak{r}y + \mathfrak{r}z + \mathfrak{d}\zeta(x, M) = \mathfrak{r}$, and hence $y, z \in \mathfrak{r}$, $x \in \widehat{M}$, and $\varphi[h] - \zeta[x] \in \mathfrak{g}$. We identify an element of Z with a row vector of K_t^1 with respect to an $\mathfrak{r}$-basis of M. Then an element $ae + b + cg$ of V with $a, c \in K$ and $b \in Z$ can be identified with a row vector $[a \quad b \quad c]$ of K_{t+2}^1. If $t = 2$ and M corresponds to $\mathfrak{O}$ as in §1.11, then $\widehat{M}$ corresponds to $\mathfrak{P}^{-1}$, and so $\zeta[x] \in \mathfrak{p}^{-1}$; consequently $\varphi[h] \in \mathfrak{p}^{-1}$. Since $e + qug \in L[q, \mathfrak{d}^{-1}]$ if $q \in \mathfrak{g}$, we see that $L[q, \mathfrak{d}^{-1}] \neq \emptyset$ for every $q \in \mathfrak{g}$.

(a) First suppose $t = 2$ and $q \in \mathfrak{p}$. Suppose also that $\mathfrak{r}y + \mathfrak{r}z \neq \mathfrak{r}$. Then $yz^\rho \in \mathfrak{p}\mathfrak{r}$, and so $\delta^{-1}(zy^\rho - yz^\rho) \in \mathfrak{p}$. Thus $\zeta[x] \in \mathfrak{p}$, and hence $\zeta(x, M) \neq \mathfrak{d}^{-1}$. (In §3.7 we showed that $\zeta(x, M) = \mathfrak{d}^{-1}$ only if $\mathfrak{g} \subset \varphi[x]\mathfrak{g} \subset \mathfrak{p}^{-1}$.) Therefore

$\delta\varphi(h,\, L) \neq \mathfrak{r}$, a contradiction. This shows that $(y,\, z)$ must be primitive. By (3.7) there is an element α of $C(\mathfrak{r}e + \mathfrak{r}g)$ such that $(ye + zg)\alpha = e + aug$ with $a \in \mathfrak{g}$. Extend α to an element γ of $SU^{\varphi}(V)$ by defining $w\gamma = w\sigma$ for $w \in Z$ with $\sigma \in U^{\varphi}(Z)$ such that $\det(\sigma) = \det(\alpha)^{-1}$. Since $M\sigma = M$, we see that $\gamma \in C^1$, and $h\gamma = [1 \quad k \quad au]$ with $k \in M$ such that $\zeta[k] = q - a$. Given another $h' \in L[q,\, \mathfrak{d}^{-1}]$, we can similarly find an element γ' of C^1 such that $h'\gamma' = [1 \quad k' \quad a'u]$ with $a' \in \mathfrak{g}$ and $k' \in M$ such that $\zeta[k'] = q - a'$. Put $b = k' - k$ and

$$\tau = \begin{bmatrix} 1 & b & s + u^{\rho} b\zeta b^* \\ 0 & 1 & -\delta\zeta b^* \\ 0 & 0 & 1 \end{bmatrix} \tag{3.8}$$

with some $s \in \mathfrak{g}$. This is a special case of (3.6) and belongs to $SU^{\varphi}(V)$. Since $b \prec \mathfrak{r}$ and $\delta\zeta \prec \mathfrak{r}$, we see that $\tau \in C^1$. We choose s so that $h\gamma\tau = [1 \quad k' \quad a'u]$, which is so if and only if $a'u = s + u^{\rho} b\zeta b^* - \delta k\zeta b^* + au$. This can be achieved by taking $s = \mathrm{Tr}_{K/F}\big(u\zeta(k,\, k')\big) - (u + u^{\rho})\zeta[k']$. Then $h'\gamma' = h\gamma\tau$, and so $h' \in hC^1$ as expected.

(b) Next suppose $t = 2$ and $q \notin \mathfrak{p}$. Then $q \in \mathfrak{g}^{\times}$ or $q\mathfrak{g} = \mathfrak{p}^{-1}$. If $\mathfrak{d} \neq \mathfrak{r}$ and $q \in \mathfrak{g}$, then $\zeta[x] \in \mathfrak{g}$, and so $\delta\zeta(x,\, M) \neq \mathfrak{r}$ as shown in §3.7. Consequently $\mathfrak{r}y + \mathfrak{r}z = \mathfrak{r}$ in such a case, and the argument of case (a) is applicable. Therefore we may assume that $q\mathfrak{g} = \mathfrak{p}^{-1}$ if $\mathfrak{d} \neq \mathfrak{r}$. Then as observed in §3.7, we can find an element v of $M[q,\, \mathfrak{d}^{-1}]$. The same can be said for both cases $q \in \mathfrak{g}^{\times}$ and $q\mathfrak{g} = \mathfrak{p}^{-1}$ if $\mathfrak{d} = \mathfrak{r}$. We identify v with the row vector $[0 \quad v \quad 0]$, which can be viewed as an element of $L[q,\, \mathfrak{d}^{-1}]$, and so $L[q,\, \mathfrak{d}^{-1}] \neq \emptyset$ in such cases. Combining (1.5) and (3.5), we have $h \in vP^1C^1$, and hence $h = v\pi\alpha$ with $\pi \in P^1$ and $\alpha \in C^1$. Write π in the form (3.6) and focus our attention on the element e of $U^{\zeta}(Z)$ there. Since $U^{\zeta}(Z) = C(M)$, we see that $ve \in M[q,\, \mathfrak{d}^{-1}]$, and hence $ve = v\varepsilon$ with $\varepsilon \in C^1(M) = SU^{\zeta}(Z)$ as shown in §3.7. Let $\beta = \mathrm{diag}[1,\, \varepsilon,\, 1]$ and $\pi_1 = \pi\beta^{-1}$. Then $\beta \in C^1, \pi_1 \in P^1$, and $v\pi_1 = h\alpha^{-1}\beta^{-1} \in L[q,\, \mathfrak{d}^{-1}]$. Our choice of ε shows that $v\pi_1 = [0 \quad v \quad p]$ with $p \in \mathfrak{r}$. Since $v \in M[q,\, \mathfrak{d}^{-1}]$, $\delta v\zeta$ is primitive (see §3.5), and so we can find an element b of $\mathfrak{r}_2^1$ such that $\delta v\zeta b^* = -p$. Define τ by (3.8) with this b and $s = 0$. Then $\tau \in C^1$ and $v\tau = v\pi_1 = h\alpha^{-1}\beta^{-1}$. This shows that $h \in vC^1$. Thus we obtain Theorem 3.2 when $n > t = 2$.

(c) Finally suppose $t = 1$; let M and ζ be as in (3.3) and (3.4). Then $\zeta = \varphi[m]$ and $M = \mathfrak{r}m$ with an element m. Clearly $\zeta \in \mathfrak{g}^{\times}$ or $\zeta\mathfrak{g} = \mathfrak{p}$; the latter case occurs only when $\mathfrak{d} = \mathfrak{r}$. We first treat the case where $\zeta \in \mathfrak{g}^{\times}$; the other case will be treated in §3.12. Thus $h = ye + zg + sm$ with $y,\, z,\, s \in K$ such that $y\mathfrak{r} + z\mathfrak{r} + s\mathfrak{d} = \mathfrak{r}$ and $\delta^{-1}(zy^{\rho} - yz^{\rho}) + \zeta ss^{\rho} = q$. Suppose $\mathfrak{d} = \mathfrak{r}$ and $y\mathfrak{r} + z\mathfrak{r} \neq \mathfrak{r}$. Then $s \in \mathfrak{r}^{\times}$ and we see that $q = \varphi[h] \in \mathfrak{g}^{\times}$. Then $\#\big\{L[q,\, \mathfrak{d}^{-1}]/C^1(L)\big\} \leq 1$ by Lemma 3.4.

(c1) Let us now prove the case in which $q \in \mathfrak{g}$ and $y\mathfrak{r} + z\mathfrak{r} = \mathfrak{r}$ for both ramified and unramified K. Putting $p = \delta^{-1}(zy^\rho - yz^\rho)$ and applying (3.7) to $ye + zg$, we find $\gamma \in C(L)$ such that $M\gamma = M$ and $(y,\, z)\gamma = (1,\, pu)$ with $p \in \mathfrak{g}$. Replacing γ by $\gamma\alpha$ with $\alpha \in C$ such that $m\alpha = \det(\gamma)^{-1}m$ and α is the identity map on $Ke + Kg$, we may assume that $\gamma \in C^1$. We have $h\gamma = [1 \quad x \quad pu]$ with $x \in \mathfrak{r}$. We consider

$$\sigma = \begin{bmatrix} 1 & -x & u^\rho \zeta x x^\rho \\ 0 & 1 & \delta\zeta x^\rho \\ 0 & 0 & 1 \end{bmatrix}, \tag{3.9}$$

which is similar to (3.8) and belongs to C^1. We have then $h\gamma\sigma = [1 \quad 0 \quad s]$ with $s \in \mathfrak{g}$. Taking $(1,\, s)$ as $(y,\, z)$ above, we find $\gamma' \in C^1$ such that $h\gamma\sigma\gamma' = [1 \quad 0 \quad qu]$. Thus $h \in kC^1$ with $k = e + qug$; also Theorem 3.2 (v), (b) is valid.

(c2) Suppose K is ramified over F. If $q \in \mathfrak{g}$, then $s \in \mathfrak{r}$, so that $y\mathfrak{r} + z\mathfrak{r} = \mathfrak{r}$. and (c1) covers this case. Thus we assume that $q \notin \mathfrak{g}$. Then $s \notin \mathfrak{r}$ and $q\mathfrak{g} = ss^\rho\mathfrak{g}$. Put $\mathfrak{d} = \mathfrak{q}^\kappa$ with the maximal ideal $\mathfrak{q}$ of $\mathfrak{r}$ and $0 < \kappa \in \mathbf{Z}$. Since $s\mathfrak{d} \subset \mathfrak{r}$, we can put $s^{-1}\mathfrak{r} = \mathfrak{q}^a$ with $0 < a \le \kappa$; then $q\mathfrak{g} = \mathfrak{p}^{-a}$. Thus a is determined by q. Suppose $a < \kappa$; then $s\mathfrak{d} \ne \mathfrak{r}$, so that $y\mathfrak{r} + z\mathfrak{r} = \mathfrak{r}$. By the same technique as in (c1), we can find $\gamma \in C^1$ such that $h\gamma = [1 \quad x \quad pu]$ with $p \in \mathfrak{g}$ and $x \in K$. Then $x\mathfrak{q}^a = \mathfrak{r}$. Let $k = [1 \quad x_1 \quad p_1 u] \in L[q,\, \mathfrak{d}^{-1}]$ with $p_1 \in \mathfrak{g}$ and x_1 such that $x_1\mathfrak{q}^a = \mathfrak{r}$. Our task is to show that $k \in hC$. For simplicity put $N(w) = ww^\rho$ for $w \in K^\times$. We have $\zeta N(x) + p = q = \zeta N(x_1) + p_1$, and so $N(x^{-1}x_1) - 1 \in \mathfrak{p}^a$. Thus $N(x^{-1}x_1) \in N(\mathfrak{r}^\times) \cap (1 + \mathfrak{p}^a) = N(1 + \mathfrak{q}^a)$ by [S2, Lemma 17.6 (2)]. We can therefore put $N(x^{-1}x_1) = N(d)$ with $d \in 1 + \mathfrak{q}^a$. Put $\alpha = \mathrm{diag}[1_r,\, dx_1^{-1}x,\, 1_r]$. Then $\alpha \in C^1$ and $k\alpha = [1 \quad dx \quad p_1 u]$. Put $b = dx - x$ and consider τ of (3.8) with this b and any $s \in \mathfrak{g}$. Then $\tau \in C^1$ and $h\gamma\tau = [1 \quad dx \quad c]$ with $c \in \mathfrak{g}$ such that $c - c^\rho = \delta p_1$. Choosing s suitably, we obtain $c = p_1 u$. Then $k \in hC^1$.

(c3) It remains to treat the case $a = \kappa$. Then $s\mathfrak{d} = \mathfrak{r}$ and $q\mathfrak{r} = \mathfrak{d}^{-2}$. Put $h_0 = \delta h$ and $q_0 = -\delta^2 q$. Then $h_0 \in L[q_0,\, \mathfrak{r}]$. Since $q_0 \in \mathfrak{g}^\times$, by Lemma 3.4 we see that $\#\{L[q,\, \mathfrak{d}^{-1}]/C\} = \#\{L[q_0,\, \mathfrak{r}]/C\} \le 1$.

(c4) As for (d) of Theorem 3.2 (v), we have seen that $L[q,\, \mathfrak{d}^{-1}] \ne \emptyset$ only if $q \in \mathfrak{d}^{-2}$; also $e + qug \in L[q,\, \mathfrak{d}^{-1}]$ if $q \in \mathfrak{g}$. Thus it remains to consider the case where $\mathfrak{d} \ne \mathfrak{r}$ and $q \notin \mathfrak{g}$. Suppose $q\mathfrak{g} = \mathfrak{p}^{-a}$ with $0 < a < \kappa$. We can find $c \in \mathfrak{g}^\times$ such that $c - 1 \in \mathfrak{p}^a$ and $c \notin N(\mathfrak{r}^\times)$. Then q or $c^{-1}q$ represents $d_0(\varphi)$. If $q \in d_0(\varphi)$, then $q = \zeta ss^\rho$ with $s \in K$, and $e + sm \in L[q,\, \mathfrak{d}^{-1}]$. If $q \in cd_0(\varphi)$, put $q = c\zeta ss^\rho$ with $s \in K$ and $p = \zeta ss^\rho(c - 1)$. Then $p \in \mathfrak{g}$ and $e + pu\mathfrak{g} + sm \in L[q,\, \mathfrak{d}^{-1}]$. Thus $L[q,\, \mathfrak{d}^{-1}] \ne \emptyset$ if $q \in \mathfrak{p}\mathfrak{d}^{-2}$. The case $q\mathfrak{r} = \mathfrak{d}^{-2}$ will be settled in Lemma 3.13.

3.12. Let us now treat the case where $t = 1$ and $\zeta\mathfrak{g} = \mathfrak{p}$. Then $\mathfrak{d} = \mathfrak{r}$ and $\delta \in \mathfrak{r}^\times$. To avoid possible confusion, we use the letter π instead of ζ; thus $\varphi[m] = \pi$. Let $h = ae + bf + cm \in L[q,\, \mathfrak{r}]$. Then $\mathfrak{r}a + \mathfrak{r}b + \mathfrak{r}\pi c = \mathfrak{r}$ and $ab^\rho + a^\rho b + \pi cc^\rho = q$. Clearly $q \in \mathfrak{p}^{-1}$; also $c \in \mathfrak{r}$ if and only if $q \in \mathfrak{g}$. Given

$q \in \mathfrak{g}$, we can find $b \in \mathfrak{r}$ such that $b + b^\rho = q$. Then $e + bf \in L[q, \mathfrak{r}]$. Given $q \in \mathfrak{p}^{-1}, \notin \mathfrak{g}$, we can find $d \in \mathfrak{r}^\times$ such that $dd^\rho = \pi q$. Then $\pi^{-1}dm \in L[q, \mathfrak{r}]$. Thus $L[q, \mathfrak{r}] \neq \emptyset$ if and only if $q \in \mathfrak{p}^{-1}$.

(1) Let us first assume that $q \in \mathfrak{g}$; then $c \in \mathfrak{r}$ and $\mathfrak{r}a + \mathfrak{r}b = \mathfrak{r}$. By (3.7) there exists an element β of $C(\mathfrak{r}e + \mathfrak{r}f)$ such that $k\beta = e + sf$ with $s \in \mathfrak{r}$. Extend β to an element α of $C^1(L)$ by defining $m\alpha = \det(\beta)^{-1}m$. Then $h\alpha = e + sf + c_1 m$ with $c_1 \in \mathfrak{r}$. Now represent the elements of $U^\varphi(V)$ by matrices with respect to $\{e, m, f\}$. Then (3.5) holds with the subgroup P of U^φ consisting of the upper triangular matrices. Observe that P contains every matrix of the form

$$\begin{bmatrix} 1 & -x & y \\ 0 & 1 & \pi x^\rho \\ 0 & 0 & 1 \end{bmatrix} \tag{3.10}$$

with $x, y \in K$ such that $y + y^\rho = -\pi x x^\rho$. Since $\mathrm{Tr}_{K/F}(\mathfrak{r}) = \mathfrak{g}$, for any $x \in \mathfrak{r}$ we can take such a y from $\mathfrak{r}$. Let γ be the matrix of (3.10) with $x = c_1$ and $y \in \mathfrak{r}$. Then $\gamma \in C^1(L)$ and $h\alpha\gamma = e + zf$ with $z \in \mathfrak{r}$ such that $z + z^\rho = q$. Take $z_1 \in \mathfrak{r}$ so that $z_1 + z_1^\rho = q$. Denote by ε the matrix of (3.10) with $x = 0$ and $y = z_1 - z$. Then $\varepsilon \in C^1(L)$ and $(e + zf)\varepsilon = e + z_1 f$. This gives the desired result when $q \in \mathfrak{g}$.

(2) Next we consider the case $c \notin \mathfrak{r}$; put $d = \pi c$. Then $d \in \mathfrak{r}^\times$ and $q = ab^\rho + a^\rho b + \pi^{-1}dd^\rho$. Thus $\pi q \in \mathfrak{g}^\times$, and so we can find an element $d_0 \in \mathfrak{r}^\times$ such that $d_0 d_0^\rho = \pi q$. Put $k = \pi^{-1}d_0 m$. Then $k \in L[q, \mathfrak{r}]$. By (1.5), we have $h = k\alpha$ with $\alpha \in SU^\varphi$, and by (3.5) we can put $\alpha = \beta\gamma$ with $\beta \in P^1$ and $\gamma \in C^1$. Replacing β by $\beta\xi$ with a suitable diagonal matrix ξ belonging to C^1, we may assume that the center entry of β is 1. (Here we need Lemma 1.9 (i).) Let $[0 \;\; 1 \;\; j]$ be the second row of β. Then $[0 \;\; \pi^{-1}d_0 \;\; \pi^{-1}d_0 j] = k\beta = h\gamma^{-1} \in L[q, \mathfrak{r}]$, and so $\pi^{-1}d_0 j \in \mathfrak{r}$. Put $x = \pi^{-1}j^\rho$; then $x \in \mathfrak{r}$. Let ε be the matrix of (3.10) with this x and y such that $y + y^\rho = -\pi x x^\rho$. Then $\varepsilon \in C^1$ and $k\varepsilon = k\beta = h\gamma^{-1}$, which gives the desired fact.

It only remains to discuss $L[q, \mathfrak{d}^{-1}]/C^1$ when $\mathfrak{d} \neq \mathfrak{r}$ and $q\mathfrak{r} = \mathfrak{d}^{-2}$. (In (c3) we treated $L[q, \mathfrak{d}^{-1}]/C$.) The problem is settled by (ii) of the following Lemma.

Lemma 3.13. *If K is a field ramified over F, then the following assertions hold:*

(i) *Let $W = (Kh)^\perp$ with $h \in L[q, \mathfrak{b}]$ and let $E_1 = \det\bigl(C \cap U^\varphi(W)\bigr)$, where we view $U^\varphi(W)$ as the subgroup of $U^\varphi(V)$ consisting of the elements ξ such that $h\xi = h$. Then $\#\bigl\{L[q, \mathfrak{b}]/C^1\bigr\} = [E_L : E_1] < \infty$, where E_L is as in Lemma 1.9.*

(ii) *If $1 < n - 1 \in 2\mathbf{Z}$ and $q\mathfrak{r} = \mathfrak{d}^{-2}$, then $\#\bigl\{L[q, \mathfrak{d}^{-1}]/C^1\bigr\} = 2$ or 0 according as q represents $d_0(\varphi)$ or not.*

Proof. Clearly $C \cap U^\varphi(W)$ is an open subgroup of $U^\varphi(W)$. Now $\det : U^\varphi(W) \to E$ is a continuous surjective map, and so it is an open map by virtue of a well know principle; see [S3, Lemma 8.0]. Thus E_1 is an open subgroup of E, and so $[E : E_1] < \infty$, as E is compact. Therefore $[E_L : E_1] < \infty$. Next, take a finite subset $B \subset C$ so that $\{\det(\beta)\}_{\beta \in B}$ gives E_L/E_1. Let $k \in L[q, \mathfrak{b}]$. By Theorem 3.2 (i), $k = h\alpha$ with $\alpha \in C$. Then $\det(\alpha\beta^{-1}) \in E_1$ for some $\beta \in B$, so that $\det(\alpha\beta^{-1}) = \det(\gamma)$ with $\gamma \in C \cap U^{\varphi}(W)$. Put $\xi = \alpha^{-1}\gamma\beta$. Then $\xi \in C^1$ and $h\beta = h\gamma\beta = k\xi$, that is, $k \in h\beta C^1$. Thus $L[q, \mathfrak{b}] = \bigcup_{\beta \in B} h\beta C^1$. We easily see that the last union is disjoint, and so we obtain (i). To prove (ii), let the notation be as in (3.3) and (3.4); let $M = \mathfrak{r}m$, $\varphi[m] = \zeta \in \mathfrak{g}^{\times}$, and $\mathfrak{d} = \mathfrak{q}^{\kappa}$ as in (c2) above. Then ζ represents $d_0(\varphi)$. Suppose $q\mathfrak{r} = \mathfrak{d}^{-2}$ and $h \in L[q, \mathfrak{d}^{-1}]$; put $h = \sum_{i=1}^{r}(y_i e_i + z_i g_i) + sm$ with $y_i, z_i, s \in K$. Then $y_i, z_i \in \mathfrak{r}$, and $q - \zeta s s^{\rho} \in \mathfrak{g}$, so that $s\mathfrak{r} = \mathfrak{d}^{-1}$ and $(\zeta s s^{\rho})^{-1} q \in 1 + \mathfrak{p}^{\kappa} \in N_{K/F}(\mathfrak{r}^{\times})$; thus q represents $d_0(\varphi)$. This shows that $L[q, \mathfrak{d}^{-1}] \neq \emptyset$ only for such a q. Taking such a q, we can put $q = \zeta x x^{\rho}$ with $x \in K^{\times}$. Let $k = xm$ and $W = (Kk)^{\perp}$. Then $k \in L[q, \mathfrak{d}^{-1}]$, $W = \sum_{i=1}^{r}(Ke_i + Kg_i)$, and $C \cap U^{\varphi}(W) = C(\Lambda)$ with $\Lambda = \sum_{i=1}^{r}(\mathfrak{r}e_i + \mathfrak{r}g_i)$; thus $E_1 = E_{\Lambda}$. By Lemma 1.9, $E_L = E$, $E_{\Lambda} = E_0$, and $[E : E_0] = 2$, which together with (i) shows that $\#\{L[q, \mathfrak{d}^{-1}]/C^1\} = 2$. This completes the proof.

LEMMA 3.14. *Let $W = (Kh)^{\perp}$ with $h \in L[q, \mathfrak{b}]$ and let $\Lambda = L \cap W$. Suppose that $0 < n - 1 \in 2\mathbf{Z}$. Then there is a unique maximal lattice in W containing Λ at least in the following two cases:* (1) $q(\mathfrak{b}\mathfrak{b}^{\rho})^{-1} = \mathfrak{r}$; (2) $q(\mathfrak{b}\mathfrak{b}^{\rho})^{-1} = \mathfrak{p}\mathfrak{r}$ *and $\{K, qd_0(\varphi)\}$ is a division algebra. Moreover, Λ is maximal and $C(\Lambda) = C(L) \cap U^{\varphi}(W)$ in Case (1); Λ is maximal and $[C(\Lambda) : C(L) \cap U^{\varphi}(W)] = N(\mathfrak{p}) + 1$ in Case (2) if K is unramified over F and $d_0(\varphi) = N_{K/F}(K^{\times})$. These assertions are true with C^1 instead of C.*

Proof. Changing h for ch with some $c \in K^{\times}$, we may assume that $\mathfrak{b} = \mathfrak{r}$. This does not change the ideal $q(\mathfrak{b}\mathfrak{b}^{\rho})^{-1}$ nor $\{K, qd_0(\varphi)\}$. Thus $q \in \mathfrak{g}^{\times}$ in Case (1) and $q\mathfrak{g} = \mathfrak{p}$ in Case (2). Suppose $q \in \mathfrak{g}^{\times}$. Then $L = \mathfrak{r}h \oplus \Lambda$ as shown in the proof of Lemma 3.4, and Λ is maximal as noted there; clearly $C(\Lambda) = C(L) \cap U^{\varphi}(W)$ and $C^1(\Lambda) = C^1(L) \cap U^{\varphi}(W)$. Next suppose $q\mathfrak{g} = \mathfrak{p}$ and $\{K, qd_0(\varphi)\}$ is a division algebra. Let u, δ, and $\{e_i, g_i\}$ be as in §3.8. Since $n \notin 2\mathbf{Z}$, we have $L = \mathfrak{r}m + \sum_{i=1}^{r}(\mathfrak{r}e_i + \mathfrak{r}g_i)$ with an element m such that $\varphi[m] = \zeta$. Theorem 3.2 (i) allows us to replace h by any element in $L[q, \mathfrak{r}]$. Thus we can put $h = e_1 + qug_1$. Put now $k = e_1 + qu^{\rho}g_1$, $Y = Kk + Km$, and $N = \mathfrak{r}k + \mathfrak{r}m$. Then $\varphi[k] = -q$, $W = Y \oplus \sum_{i=2}^{r}(Ke_i + Kg_i)$, $\Lambda = N + \sum_{i=2}^{r}(\mathfrak{r}e_i + \mathfrak{r}g_i)$, and $d_0(Y) = qd_0(\varphi)$. Since $\{K, qd_0(\varphi)\}$ is a division algebra, (Y, φ) is anisotropic, and so has a unique maximal lattice M as noted in §3.7. Put $\Lambda' = M + \sum_{i=2}^{r}(\mathfrak{r}e_i + \mathfrak{r}g_i)$. Then clearly Λ' is the unique maximal lattice in W containing Λ.

To prove the remaining part, we assume that $q\mathfrak{g} = \mathfrak{p}$, $\mathfrak{d} = \mathfrak{r}$, and $d_0(\varphi) = N_{K/F}(K^{\times})$. Since $N \subset M$ and $[\widehat{M} : M] = N(\mathfrak{p})^2 = [\widehat{N} : N]$, we obtain $M = N$, and so Λ is maximal. We easily see that $C(L) \cap U^{\varphi}(W) \subset C(\Lambda)$. Let $\gamma \in C(\Lambda)$.

Then $L\gamma$ is a maximal lattice in V containing Λ, so that $\sum_{i=2}^{r}(\mathfrak{r}e_i+\mathfrak{r}g_i) \subset L\gamma$. By [S2, Lemma 4.9 (i)] we have $L\gamma = J+\sum_{i=2}^{r}(\mathfrak{r}e_i+\mathfrak{r}g_i)$ with a maximal lattice J in $Km+Ke_1+Kg_1$. Since $m \in J$, from (1.9) we see that $\varphi(m,\, J) = \mathfrak{r}$, and so $J = \mathfrak{r}m + H$ with a maximal lattice H in $Ke_1 + Kg_1$ as shown in the proof of Lemma 3.4. Now $h = h\gamma \in L\gamma$ and $k \in \Lambda = \Lambda\gamma$; thus $h,\, k \in J$. Put $H_0 = \mathfrak{r}e_1+\mathfrak{r}g_1$. By Lemma 1.10 (ii), $H = H_0\alpha$ with $\alpha \in SU^{\varphi}(Ke_1+Kg_1)$. By (3.5) we can take α in the form (3.6). Identify $GL(Ke_1 + Kg_1)$ with $GL_2(K)$ with respect to the basis $\{e_1,\, g_1\}$. Replacing α by an element of $C(H_0)\alpha$, we can put $\alpha = \begin{bmatrix} a^{-1} & b \\ 0 & a \end{bmatrix}$ with $a \in F^{\times}$ and $b \in F$. Put $z = a^{-1}e_1 + bg_1$ and $w = ag_1$; then $H = \mathfrak{r}z + \mathfrak{r}w$. Since $\delta e_1 = uk - u^{\rho}h \in H$ and $q\delta g_1 = h - k \in H$, we see that $\mathfrak{p} \subset a\mathfrak{g} \subset \mathfrak{g}$, and so we may assume that $a = 1$ or $a = q$. Now $\varphi(z,\, e_1) \in \mathfrak{r}$, and so $b \in \mathfrak{g}$. Thus if $a = 1$, then $H = H_0$. Suppose $a = q$; put $\alpha_b = \begin{bmatrix} a^{-1} & b \\ 0 & a \end{bmatrix}$. Then $H_0\alpha_b = H_0\alpha_{b'}$ if and only if $b - b' \in \mathfrak{p}$. Thus there exist exactly $N(\mathfrak{p}) + 1$ maximal lattices in $Ke_1 + Kg_1$ containing h and k, and so there exist at most $N(\mathfrak{p}) + 1$ lattices of the form $L\gamma$ with $\gamma \in C(\Lambda)$. This shows that

$$\big[C(\Lambda) : C(L) \cap U^{\varphi}(W)\big] \le N(\mathfrak{p}) + 1. \tag{3.11}$$

To show that this is actually an equality, define the symbols $\ell,\, j,\, \omega$, and $\mathfrak{O}$ as in Lemma 1.3, (1.6), and §3.7, with Y as the space V there. In the proof of Lemma 1.3 take $\varphi_0 = \mathrm{diag}[\zeta,\, -q]$ and $s = \zeta^{-1}q$. Then the identification of V with K_2^1 in the proof of Lemma 1.3 (which is unrelated to the above identification of $GL(Ke_1 + Kg_1)$ with K_2^2) identifies m with $(1,\,0)$ and k with $(0,\,1)$, so that m here equals ℓ of Lemma 1.3; also, $M = \ell j(\mathfrak{O}) = mj(\mathfrak{O})$. Let β be an element of $\mathfrak{O}$ such that $\beta\beta^{\iota} = 1$; define $\xi \in SU^{\varphi}(V)$ by $\xi = j(\beta)$ on Y and $x\xi = x$ for every $x \in Kh+\sum_{i=2}^{r}(Ke_i+Kg_i)$. Then $\xi \in C^1(\Lambda)$. Put $\beta = c+d\omega$ with $c,\, d \in \mathfrak{r}$. Then $\ell\xi = c\ell + dk$ and $k\xi = sd^{\rho}\ell + c^{\rho}k$. Since $\delta e_1 = uk - u^{\rho}h$ and $q\delta g_1 = h - k$, we have $q\delta g_1\xi = (1 - c^{\rho})e_1 - sd^{\rho}\ell + q(u - c^{\rho}u^{\rho})g_1$. Thus $\xi \in C^1(L)$ if and only if $c - 1 \in \mathfrak{p}\mathfrak{r}$, which is so if and only if $\beta - 1 \in \mathfrak{P}$. Since $\beta\beta^{\iota} = 1$, this shows that there exist at least $N(\mathfrak{p}) + 1$ different $L\gamma$ with $\gamma \in C^1(\Lambda)$, and so

$$N(\mathfrak{p}) + 1 \le \big[C^1(\Lambda) : C^1(L) \cap U^{\varphi}(W)\big].$$

This combined with (3.11) proves that

$$\big[C^1(\Lambda) : C^1(L) \cap U^{\varphi}(W)\big] = \big[C(\Lambda) : C(L) \cap U^{\varphi}(W)\big] = N(\mathfrak{p}) + 1,$$

which completes the proof.

We insert here the classification of the structures $(V,\, s\varphi)$ with $s \in F^{\times}$. If $K = F \times F$, the matter is settled in §1.8.

Proposition 3.15. (i) *If F is a local field and* $\dim(V)$ *is even, then* $(V,\,\varphi)$ *is isomorphic to* $(V,\,s\varphi)$ *for every* $s \in F^\times$.

(ii) *Suppose F is an arbitrary field and* $\dim(V)$ *is odd; let* $s \in F^\times$; *then* $(V,\,\varphi)$ *is isomorphic to* $(V,\,s\varphi)$ *if and only if* $s \in N_{K/F}(K^\times)$.

Proof. The first assertion is included in Lemma 1.6. The second assertion can be proved easily in the same manner as for [S3, Theorem 7.13] in the even-dimensional case.

4. Hermitian Diophantine equations over a global field

4.1. Throughout this section we assume that F is an algebraic number field and K is a quadratic extension of F; we fix a hermitian space $(V,\,\varphi)$ and use the notation of §2.1. For an $\mathfrak{r}$-lattice L in V we put

$$\Gamma(L) = \{\alpha \in U^\varphi(V) \mid L\alpha = L\}, \qquad \Gamma^1(L) = \Gamma(L) \cap SU^\varphi(V). \tag{4.1}$$

Given $h \in V$ such that $\varphi[h] \neq 0$, put $W = (Kh)^\perp$. We view $U^\varphi(W)$ as a subgroup of $U^\varphi(V)$, and $SU^\varphi(W)$ as a subgroup of $SU^\varphi(V)$ as explained in §1.1. For $\sigma \in U^\varphi(V)_\mathbf{A}$, the symbol $h\sigma$ is meaningful as an element of $V_\mathbf{A}$.

Theorem 4.2. *If* $\dim(V) > 1$, *then* $\#\{\Lambda[q]/\Gamma^1(\Lambda)\} < \infty$ *for every* $q \in F^\times$ *and every* $\mathfrak{r}$*-lattice* Λ *in* V.

Proof. Assuming $\dim(V) > 1$ and $\Lambda[q] \neq \emptyset$, take $h \in \Lambda[q]$ and define W as above; put $G = SU^\varphi(V)$, $H = SU^\varphi(W)$, $D = \{x \in G_\mathbf{A} \mid \Lambda x = \Lambda\}$, and $D_v = G_v \cap D$ for $v \in \mathbf{h}$. Then $\Gamma^1(\Lambda) = G \cap D$ and $D_v = C^1(\Lambda_v)$. By Theorem 3.3 and (1.5) we have $\Lambda_v[q] = \bigcup_{\alpha \in X_v} h\alpha D_v$ with a finite subset X_v of G_v. By Theorem 3.2 (iii) and (iv) we can take $X_v = \{1\}$ if Λ_v is maximal, v is not ramified in K, and $q \in \mathfrak{g}_v^\times$. Thus $X_v = \{1\}$ for almost all $v \in \mathbf{h}$. Put $X = \prod_{v\in\mathbf{h}} X_v$. This is a finite subset of $G_\mathbf{h}$. For each $\xi \in X$ we can find a finite subset E_ξ of $H_\mathbf{h}$ such that $H_\mathbf{A} = \bigcup_{\varepsilon\in E_\xi} H\varepsilon(H_\mathbf{A} \cap \xi D\xi^{-1})$. Then $H_\mathbf{A}\xi D = \bigcup_{\varepsilon\in E_\xi} H\varepsilon\xi D$. For each $(\varepsilon,\,\xi)$ such that $G \cap \varepsilon\xi D \neq \emptyset$ pick $\beta_{\varepsilon,\xi} \in G \cap \varepsilon\xi D$. Now let $k \in \Lambda[q]$. Then $k = h\xi\zeta$ for some $\xi \in X$ and $\zeta \in D$. On the other hand $k = h\alpha$ with $\alpha \in G$ by (1.5). Then $\alpha\zeta^{-1}\xi^{-1} \in H_\mathbf{A}$, so that $\alpha \in H_\mathbf{A}\xi D$. Thus $\alpha \in H\varepsilon\xi D$ for some $\varepsilon \in E_\xi$. Then $\alpha \in H\beta_{\varepsilon,\xi}D \cap G = H\beta_{\varepsilon,\xi}\Gamma^1(\Lambda)$, and hence $k = h\alpha \in hb_{\varepsilon,\xi}\Gamma^1(\Lambda)$. Since the $b_{\varepsilon,\xi}$ form a finite set, we obtain our theorem.

4.3. We now fix a maximal lattice L in V, and put

$$C = \{\gamma \in U^\varphi(V)_\mathbf{A} \mid L\gamma = L\}, \quad C^1 = C \cap SU^\varphi(V)_\mathbf{A}. \tag{4.2}$$

We are going to state our main theorem with respect to a pair $(G,\,H)$ belonging to the following two types of objects:

Type U: $G = U^\varphi(V)$ and $H = U^\varphi(W)$;

Type SU: $G = SU^\varphi(V)$ and $H = SU^\varphi(W)$.

Here $W = (Kh)^{\perp}$ with a fixed $h \in V$. For a subset S of $U^{\varphi}(V)_{\mathbf{A}}$ the symbol hS is meaningful as a subset of $V_{\mathbf{A}}$. Therefore $V \cap hS$ is a well-defined subset of V.

Theorem 4.4. *Suppose* $\dim(V) > 1$. *For a fixed* $h \in V$ *such that* $\varphi[h] \neq 0$ *put* $W = (Kh)^{\perp}$, *and take* (G, H) *of Type U or SU as above. Let* $D = D_0G_{\mathbf{a}}$ *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* $V \cap hDy^{-1} \neq \emptyset$.

(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* $(V \cap hDy^{-1})/\Delta_y$, *where* $\Delta_y = G \cap yDy^{-1}$.

(iii) *Take* $\{y_i\}_{i\in I} \subset G_{\mathbf{A}}$ *so that* $G_{\mathbf{A}} = \bigsqcup_{i\in I} Gy_iD$, *and put* $\Gamma_i = G \cap y_iDy_i^{-1}$. *Then*

$$\#\bigl\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)\bigr\} = \sum_{i\in I} \#\bigl\{(V \cap hDy_i^{-1})/\Gamma_i\bigr\}. \tag{4.3}$$

(iv) *Let* $q = \varphi[h]$ *and* $\mathfrak{b} = \varphi(h, L)$. *Then for every* $y \in U^{\varphi}(V)_{\mathbf{A}}$, *we have*

$$V \cap hCy^{-1} = \bigl(Ly^{-1}\bigr)[q, \mathfrak{b}]. \tag{4.4}$$

(v) *Suppose moreover that* $\dim(V) > 2$ *and the following condition is satisfied:*

(4.5) *If* n *is odd, then* $q_v\mathfrak{r}_v \neq \mathfrak{b}_v\mathfrak{b}_v^{\rho}$ *for every* $v \in \mathbf{h}$ *ramified in* K.

Then for every $y \in SU^{\varphi}(V)_{\mathbf{A}}$ *we have*

$$V \cap hC^1y^{-1} = \bigl(Ly^{-1}\bigr)[q, \mathfrak{b}]. \tag{4.6}$$

Proof. Let y, ε, and α be as in (ii); then clearly $h\alpha \in V \cap hDy^{-1}$. If $\eta\varepsilon\zeta \in \beta yD$ with $\eta \in H$, $\zeta \in H_{\mathbf{A}} \cap D$, and $\beta \in G$, then $\beta^{-1}\eta\alpha \in G \cap yDy^{-1} = \Delta_y$, and hence $h\alpha = h\eta\alpha \in h\beta\Delta_y$. Thus our map is well defined. Next let $k \in V \cap hDy^{-1}$. Then $k = h\delta y^{-1}$ with $\delta \in D$, and moreover, by (1.5), $k = h\xi$ with $\xi \in G$. Then $h = h\xi y\delta^{-1}$, so that $\xi y\delta^{-1} \in H_{\mathbf{A}}$. Thus $\xi y\delta^{-1} \in H_{\mathbf{A}} \cap GyD$. 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 $\sigma \in \Delta_y$. 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).

Since $H_{\mathbf{A}} = \bigsqcup_{i\in I}(H_{\mathbf{A}} \cap Gy_iD)$, we can derive (iii) immediately from (ii).

As for (v), clearly $V \cap hC^1 \subset L[q, \mathfrak{b}]$. Conversely, if $x \in L[q, \mathfrak{b}]$, then $x \in hC^1$ by Theorem 3.2 (iii). Thus

$$V \cap hC^1 = L[q, \mathfrak{b}]. \tag{4.7}$$

If $k \in V \cap hC^1y^{-1}$, then $hC^1y^{-1} = kyC^1y^{-1}$. Now $\varphi\bigl(k, Ly^{-1}\bigr) = \varphi(h, L) = \mathfrak{b}$. Taking k, yC^1y^{-1}, and Ly^{-1} in place of h, C^1, and L in (4.7), we obtain $V \cap kyC^1y^{-1} = \bigl(Ly^{-1}\bigr)[q, \mathfrak{b}]$. This proves (4.6) when $V \cap hC^1y^{-1} \neq \emptyset$. To prove the remaining case, suppose $\ell \in \bigl(Ly^{-1}\bigr)[q, \mathfrak{b}]$; then $\varphi\bigl(\ell_v y_v, L_v\bigr) = \mathfrak{b}_v = \varphi(h, L)_v$ for every $v \in \mathbf{h}$, and so, by Theorem 3.2 (iii), $\ell y \in hC^1$. Taking ℓ, yC^1y^{-1}, and Ly^{-1} in place of h, C^1, and L in (4.7), we obtain $\emptyset \neq \bigl(Ly^{-1}\bigr)[q, \mathfrak{b}] = V \cap \ell yC^1y^{-1} = V \cap hC^1y^{-1}$. This shows that $\bigl(Ly^{-1}\bigr)[q, \mathfrak{b}] = \emptyset$ if $V \cap hC^1y^{-1} = \emptyset$, and hence (4.6) holds for every $y \in G_{\mathbf{A}}$. This proves (v). Assertion (iv) can be proved in the same way.

In view of (i) we can restrict the indices i on the right-hand side of (4.3) to those for which $H_{\mathbf{A}} \cap Gy_iD \neq \emptyset$. If I' denotes the set of all such i's, then $H_{\mathbf{A}} = \bigsqcup_{j \in I'} (H_{\mathbf{A}} \cap Gy_jD)$.

Combining (4.3) and (4.4), we obtain, for (G, H) of type U, an equality

$$\#\bigl\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap C)\bigr\} = \sum_{i \in I} \#\bigl\{(Ly_i^{-1})[q, \mathfrak{b}]/\Gamma_i\bigr\}, \tag{4.8}$$

where $\{y_i\}$ is such that $G_{\mathbf{A}} = \bigsqcup_{i \in I} Gy_iC$ and $\Gamma_i = G \cap y_iCy_i^{-1}$. We can state a similar formula for (G, H) of type SU when $n > 2$ and (4.5) is satisfied. Formula (4.8) connects the class number of H with respect to $H_{\mathbf{A}} \cap C$ to the solutions h of the equation $\varphi[h] = q$ under the condition $\varphi(h, Ly_i^{-1}) = \mathfrak{b}$.

5. Nonscalar hermitian Diophantine equations

5.1. So far we discussed the equation $\varphi[h] = q$ with a scalar q. We can formulate a similar problem with nonscalar q, which can be stated in terms of matrices as follows. We take F to be local or global. Given $q^* = q \in GL_m(K)$ and $\varphi^* = \varphi \in GL_n(K)$, we consider the solutions $h \in K_n^m$ of the equation $h\varphi h^* = q$. Here and throughout this section we assume $n > m > 0$. More intrinsically, take (V, φ) as before and take also (X, q) with a nondegenerate hermitian form q on a free K-module X of dimension m. We consider $h \in \mathrm{Hom}(X, V)$ 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 $k \in \mathrm{Hom}(X, V)$ we denote by $\varphi[k]$ the hermitian form on X defined by $\varphi[k][x] = \varphi[xk]$ for every $x \in X$. Then our problem concerns the solutions $h \in \mathrm{Hom}(X, V)$ of the equation $\varphi[h] = q$ for a fixed q. If $m = 1$ and $X = K$, then $q \in F^\times$, and an element h of V defines an element of $\mathrm{Hom}(K, V)$ that sends c to ch for $c \in K$, and every element of $\mathrm{Hom}(K, V)$ is of this type. Thus the problem about $\varphi[h] = q$ with $q \in F^\times$ is the one-dimensional special case. Let h be an element of $\mathrm{Hom}(X, V)$ such that $\mathrm{rank}(\varphi[h]) = m$. Then

$$\bigl\{x \in \mathrm{Hom}(X, V) \bigm| \varphi[x] = \varphi[h]\bigr\} = h \cdot SU^{\varphi}. \tag{5.1}$$

This is similar to (1.5), and follows easily from the Witt theorem in the unitary case. Though we take V to be coordinate-free, it is practical to take X to be

K^1_m, and so take q to be a hermitian element of $GL_m(K)$, and $q[x] = xqx^*$ for $x \in K^1_m$. For $h \in \mathrm{Hom}(X, V)$ and $1 \le i \le m$ we define "the i-th row" of h to be the element h_i of V determined by $ah = \sum_{i=1}^m a_ih_i$ for $a = (a_i)_{i=1}^m \in K^1_m = X$.

We first prove a local finiteness result that generalizes Theorem 3.3.

Theorem 5.2. *Suppose F is a local field; let Λ be an $\mathfrak{r}$-lattice in $\mathrm{Hom}(X, V)$ and let $D = \{\gamma \in SU^\varphi(V) \mid \Lambda\gamma = \Lambda\}$. Then, given $h \in \mathrm{Hom}(X, V) \cap \Lambda$ such that $\varphi[h]$ is nondegenerate, there exists a finite subset A of $SU^\varphi(V)$ such that*

$$\{ x \in \Lambda \mid \varphi[x] = \varphi[h] \} = \textstyle\bigsqcup_{\alpha \in A} h\alpha D. \tag{5.2}$$

Moreover, suppose $K = F \times F$ or K is a field unramified over F; suppose also that $\varphi[h] \in GL_m(\mathfrak{r})$ and $\Lambda = \{\lambda \in \mathrm{Hom}(X, V) \mid \mathfrak{r}^1_m\lambda \subset L\}$ with a maximal lattice L in V. Then we can take $A = \{1\}$.

Proof. The first part is Theorem 3.3 if $m = 1$, and so we assume $m > 1$ and prove (5.2) by induction on m. Put $q = \varphi[h]$. Changing (h, q, Λ) for $(ch, cqc^*, c\Lambda)$ with a suitable $c \in GL_m(K)$, we may assume that $q = \mathrm{diag}[a, \eta]$ with $a \in F^\times$ and $\eta^* = \eta \in GL_{m-1}(K)$. Also we may assume that $\Lambda = \{\kappa \in \mathrm{Hom}(X, V) \mid M\kappa \subset L\}$ with $M = \mathfrak{r}^1_m$ and an $\mathfrak{r}$-lattice L in V. Then $D = \{\alpha \in SU^\varphi(V) \mid L\alpha = L\}$. If $x \in \Lambda$ and $\varphi[x] = q$, then $x_1, h_1 \in L$ and $\varphi[x_1] = \varphi[h_1] = a$, and hence by Theorem 3.3 there exists a finite subset B of L such that such an x_1 belongs to $\bigcup_{b\in B} bD$ and $\varphi[b] = a$ for every $b \in B$. Suppose $x_1 = b\gamma$ with $b \in B$ and $\gamma \in D$. Put $W_b = (Kb)^\perp$, $y = x\gamma^{-1}$ and $z = [y_i]_{i=2}^m$. Then $y_1 = b$ and $\varphi[y] = \varphi[h]$, so that $\varphi[z] = \eta$, and $y_i \in W_b$ for $i > 1$. We can view z as an element of $\mathrm{Hom}(K^1_{m-1}, W_b)$. Then $\mathfrak{r}^1_{m-1}z \subset L \cap W_b$. Put $E = \{\varepsilon \in SU^\varphi(W_b) \mid (L \cap W_b)\varepsilon = L \cap W_b\}$. By induction there exists a finite subset U_b of $\mathrm{Hom}(K^1_{m-1}, W_b)$ such that

$$\{z \in \mathrm{Hom}(K^1_{m-1}, W_b) \mid \mathfrak{r}^1_{m-1}z \subset L \cap W_b,\ \varphi[z] = \eta \} = \textstyle\bigsqcup_{u\in U_b} uE.$$

We can find a finite subset S of E such that $E = \bigsqcup_{\sigma\in S} \sigma(D \cap E)$. Then $y = \begin{bmatrix} b \\ z \end{bmatrix} = \begin{bmatrix} b \\ u\sigma\tau \end{bmatrix}$ with $u \in U_b$, $\sigma \in S$, and $\tau \in D \cap E$. Thus $x = \begin{bmatrix} b \\ u\sigma \end{bmatrix}\tau\gamma$, and $\tau\gamma \in D$. This shows that $x \in \bigsqcup_{k\in P} kD$ with a finite subset P of the left-hand side of (5.2), as the elements (b, u, σ) form a finite set. By (5.1), for each $k \in P$ there exists an element α of $SU^\varphi(V)$ such that $k = h\alpha$. This proves the first assertion.

Next suppose that the conditions on K, q, Λ, and φ as in the second assertion are satisfied. Take an $\mathfrak{r}$-basis of L and identify V, L, and φ with K^1_n, $\mathfrak{r}^1_n$, and a hermitian matrix with respect to that basis. Given $\ell \in L = \mathfrak{r}^1_n$, put $z = q^{-1}h\varphi\ell^*$ and $y = \ell - z^*h$. Since $\varphi \prec \mathfrak{r}$ and $q \in GL_m(\mathfrak{r})$, we see that $y \in L$, and for every $w \in X$ we have $wh\varphi y^* = 0$, so that $y \in (Xh)^\perp$. Put $M = \mathfrak{r}^1_m$ and $Y = (Xh)^\perp$. Then $V = Xh \oplus Y$ and $L = Mh \oplus (L \cap Y)$. Suppose $\varphi[k] = q$ with $k \in \Lambda$. Then similarly $L = Mk \oplus (L \cap Z)$ with $Z = (Xk)^\perp$. Since L

is maximal, Mh resp. Mk is maximal in Xh resp. Xk, and $L \cap Y$ resp. $L \cap Z$ is maximal in Y resp. Z. By (5.1) there exists an element $\gamma \in SU^\varphi(V)$ such that $h\gamma = k$. Then $Mh\gamma = Mk$, $Y\gamma = Z$, and $(L \cap Y)\gamma$ is $\mathfrak{r}$-maximal in Z, so that by Lemma 3.4 (i), $(L \cap Y)\gamma\varepsilon = L \cap Z$ with some $\varepsilon \in U^\varphi(Z)$. Define $\alpha \in GL(V)$ by $\alpha = \gamma$ on Xh and $\alpha = \gamma\varepsilon$ on Y. Then $\alpha \in U^\varphi(V)$, $L\alpha = L$, and $h\alpha = k$. Since $\det(\alpha) \in \mathfrak{r}^\times$, we can find an element ξ of $U^\varphi(Z)$ such that $(L \cap Z)\xi = L \cap Z$ and $\det(\xi) = \det(\alpha)^{-1}$. This is clear if $K = F \times F$; see §3.6. If K is a field unramified over F, then the fact is included in Lemma 1.9. Extend ξ to an element of $U^\varphi(V)$ by putting $xk\xi = xk$ for $x \in X$. Then $\alpha\xi \in SU^\varphi(V)$, $h\alpha\xi = k$, and $L\alpha\xi = L$. Clearly $\Lambda\alpha\xi = \Lambda$, and hence we obtain (5.2) with $A = \{1\}$. This completes the proof.

Next we prove a generalization of Theorem 4.2, which is a global version of the above theorem.

Theorem 5.3. *Suppose that F is an algebraic number field; let Λ be an $\mathfrak{r}$-lattice in $\mathrm{Hom}(X, V)$, $\Gamma = \{\, \gamma \in SU^\varphi(V) \mid \Lambda\gamma = \Lambda \,\}$, and $T_q = \{\, x \in \Lambda \mid \varphi[x] = q \,\}$ with $q^* = q \in GL_m(K)$. Then T_q/Γ is a finite set.*

Proof. We assume the existence of $h \in T_q$. Put $W = (Xh)^\perp$, $G = SU^\varphi(V)$, $H = SU^\varphi(W)$, $M = \mathfrak{r}_m^1$, $D = \{\gamma \in G_{\mathbf{A}} \mid \Lambda\gamma = \Lambda\}$, and $D_v = D \cap G_v$ for $v \in \mathbf{h}$. We identify H with $\{\alpha \in G \mid h\alpha = h\}$. Fix a maximal lattice L in V. By Theorem 5.2, for each $v \in \mathbf{h}$ there exists a finite subset E_v of G_v such that

$$\{x \in \Lambda_v \mid \varphi[x] = q\,\} = \textstyle\bigsqcup_{\varepsilon \in E_v} h\varepsilon D_v.$$

Now for almost all $v \in \mathbf{h}$ we have $\Lambda_v = \{\gamma \in \mathrm{Hom}(X_v, V_v) \mid M_v\gamma \subset L_v\}$, L_v is maximal, v is unramified in K, and $q \in GL_m(\mathfrak{r}_v)$. Therefore, by Theorem 5.2, we can take $E_v = \{1\}$ for almost all $v \in \mathbf{h}$. Consequently we can find a finite subset E of $G_{\mathbf{h}}$ such that $T_q \subset \bigcup_{\eta \in E} h\eta D$. If $x \in T_q$, then $x \in hG$ by (5.1). Thus $x = h\alpha = h\eta\delta$ with $\alpha \in G$, $\eta \in E$, and $\delta \in D$. We have $\alpha\delta^{-1}\eta^{-1} \in H_{\mathbf{A}}$, and hence $\alpha \in H_{\mathbf{A}}\eta D$. For each $\eta \in E$ we can find a finite subset Z_η of $H_{\mathbf{h}}$ such that $H_{\mathbf{A}} = \bigsqcup_{\zeta \in Z_\eta} H\zeta(H_{\mathbf{A}} \cap \eta D\eta^{-1})$. Then $H_{\mathbf{A}}\eta D = \bigcup_{\zeta \in Z_\eta} H\zeta\eta D$, and hence $\alpha \in \bigcup_{\eta,\zeta}(G \cap H\zeta\eta D) = \bigcup_{\eta,\zeta} H(G \cap \zeta\eta D)$. For each (ζ, η) such that $G \cap \zeta\eta D \neq \emptyset$, pick any $\beta \in G \cap \zeta\eta D$. Then $G \cap \zeta\eta D = G \cap \beta D = \beta\Gamma$. Let B be the set of such β's chosen for each (ζ, η). Then $\alpha \in \bigcup_{\beta \in B} H\beta\Gamma$, and thus $h\alpha \in \bigcup_{\beta \in B} h\beta\Gamma$, which proves our theorem.

Theorem 5.4. *Suppose that F is an algebraic number field. With a fixed $h \in \mathrm{Hom}(X, V)$ such that $\mathrm{rank}\big(\varphi[h]\big) = m$, put $q = \varphi[h]$, $W = (Xh)^\perp$, $G = U^\varphi(V)$, $H = U^\varphi(W)$, and $\mathscr{V} = \mathrm{Hom}(X, V)$. Let D be an open subgroup of $G_{\mathbf{A}}$ containing $G_{\mathbf{a}}$ such that $D \cap G_{\mathbf{h}}$ is compact, and let $G_{\mathbf{A}} = \bigsqcup_{i \in I} Gy_iD$. Then assertions (i), (ii), and (iii) of Theorem 4.4 are valid if we take the symbols h, G, H, and D there to be those of the present setting, and replace V there by $\mathscr{V}$. In particular we have*

$$\#\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}}\cap D)\} = \sum_{i\in I}\#\{(\mathscr{V}\cap hDy_i^{-1})/\Gamma_i\}, \tag{5.3}$$

where $\Gamma_i = G\cap y_iDy_i^{-1}$. *The same is true with* $G = SU^{\varphi}(V)$ *and* $H = SU^{\varphi}(W)$.

Proof. We can repeat the proof of Theorem 4.4 with obvious modifications.

Theorem 5.5. *In the setting of Theorem 5.4 with* $G = SU^{\varphi}(V)$ *and* $H = SU^{\varphi}(W)$ *suppose that* $n-m>1$ *and neither* $G_{\mathbf{a}}$ *nor* $H_{\mathbf{a}}$ *is compact. Let* k *be an element of* $\mathrm{Hom}(X,\,V)$ *such that* $k = h\gamma_v$ *for every* $v\in\mathbf{h}$ *with some* $(\gamma_v)_{v\in\mathbf{h}}\in D\cap G_{\mathbf{h}}$. *Then there exists an element* $\alpha\in G\cap D$ *such that* $k = h\alpha$. *In particular, if* $m=1$ *and (4.5) is satisfied, then* $\#\{L[q,\,\mathfrak{b}]/\Gamma^1(L)\}\le 1$ *for every maximal lattice* L *in* V.

Proof. By our assumptions, strong approximation holds on G and H, and so we have $G_{\mathbf{A}} = GD$ and $H_{\mathbf{A}} = H(H_{\mathbf{A}}\cap D)$. Thus we can take $\{y_i\}_{i\in I} = \{1\}$. Therefore (5.3) implies that $\#\{(\mathscr{V}\cap hD)/(G\cap D)\} = 1$, which gives the first assertion. This combined with (4.6) proves the second assertion.

5.6. Before proceeding further, let us recall the notion of the mass of an algebraic group G with respect to an open subgroup D of $G_{\mathbf{A}}$ containing $G_{\mathbf{a}}$ and such that $G_{\mathbf{h}}\cap D$ is compact. For simplicity here we take G to be U^{φ} or SU^{φ} and assume that $U^{\varphi}_{\mathbf{a}}$ is compact. For $x\in G_{\mathbf{A}}$ put $\Delta_x = G\cap xDx^{-1}$ and $\nu(\Delta_x) = [\Delta_x : 1]^{-1}$. Then the *the mass of* G *with respect to* D is defined by

$$\mathfrak{m}(G,\,D) = \sum_{b\in\mathscr{B}}\nu(\Delta_b),\quad \mathscr{B} = G\backslash G_{\mathbf{A}}/D. \tag{5.4}$$

For this the reader is referred to [S2, (10.9.4), (24.1.1), (24.1.2)]. If D' is a subgroup of $G_{\mathbf{A}}$ of the same type as D, then from [S2, Lemma 24.2] we obtain

$$[D : D\cap D']\mathfrak{m}(G,\,D) = \mathfrak{m}(G,\,D\cap D') = [D' : D\cap D']\mathfrak{m}(G,\,D'). \tag{5.5}$$

Theorem 5.7. *In the setting of Theorem 5.4, suppose that* $G_{\mathbf{a}}$ *is compact. Then for every* $y\in G_{\mathbf{A}}$ *we have*

$$\nu(\Delta_y)\#\{\mathscr{V}\cap hDy^{-1}\} = \sum_{\varepsilon\in\mathscr{E}}\nu(\Delta_\varepsilon), \tag{5.6}$$

where $\mathscr{E} = H\backslash(H_{\mathbf{A}}\cap GyD)/(H_{\mathbf{A}}\cap D)$ *and* $\Delta_x = H\cap xDx^{-1}$. *Moreover, let* $G_{\mathbf{A}} = \bigsqcup_{i\in I} Gy_iD$ *and* $\Gamma_i = G\cap y_iDy_i^{-1}$; *then*

$$\sum_{i\in I}\nu(\Gamma_i)\#\{\mathscr{V}\cap hDy_i^{-1}\} = \mathfrak{m}(H,\,H_{\mathbf{A}}\cap D). \tag{5.7}$$

Proof. To prove (5.6), we may assume that $H_{\mathbf{A}}\cap GyD\neq\emptyset$. For $\varepsilon\in\mathscr{E}$ take $\alpha_\varepsilon\in G$ so that $\varepsilon\in\alpha_\varepsilon yD$. Then $H\cap\alpha_\varepsilon\Delta_y\alpha_\varepsilon^{-1} = H\cap\alpha_\varepsilon yDy^{-1}\alpha_\varepsilon^{-1} = H\cap\varepsilon D\varepsilon^{-1} = \Delta_\varepsilon$. Now $\mathscr{V}\cap hDy^{-1} = \bigsqcup_{\varepsilon\in\mathscr{E}} h\alpha_\varepsilon\Delta_y$ by the part of Theorem 5.4 corresponding to Theorem 4.4 (ii). For $\gamma,\,\gamma'\in\Gamma(\Lambda)$ we have $h\alpha_\varepsilon\gamma = h\alpha_\varepsilon\gamma'$ if and only if $\alpha_\varepsilon\gamma'\gamma^{-1}\alpha_\varepsilon^{-1}\in H$, that is, $\gamma'\gamma^{-1}\in\alpha_\varepsilon^{-1}H\alpha_\varepsilon\cap\Delta_y = \alpha_\varepsilon^{-1}\Delta_\varepsilon\alpha_\varepsilon$, so that

$$\#\{h\alpha_\varepsilon\Delta_y\} = [\Delta_y : \alpha_\varepsilon^{-1}\Delta_\varepsilon\alpha_\varepsilon] = \nu(\Delta_\varepsilon)/\nu(\Delta_y).$$

Therefore we obtain (5.6). Next, let $\mathscr{E}_i = H\backslash(H_{\mathbf{A}} \cap Gy_iD)/(H_{\mathbf{A}} \cap D)$. Then $H_{\mathbf{A}} = \bigsqcup_{i\in I}(H_{\mathbf{A}} \cap Gy_iD) = \bigsqcup_{i\in I}\bigsqcup_{\varepsilon\in\mathscr{E}_i} H\varepsilon(H_{\mathbf{A}} \cap D)$, and so $\mathfrak{m}(H,\, H_{\mathbf{A}} \cap D) = \sum_{i\in I}\sum_{\varepsilon\in\mathscr{E}_i}\nu(\Delta_\varepsilon)$, which combined with (5.6) proves (5.7).

COROLLARY 5.8. *Define C and C^1 by (4.2) with a maximal lattice L in V; take $(G,\, H)$ of type U as in Theorem 4.4; suppose that $G_{\mathbf{a}}$ is compact. Let $G_{\mathbf{A}} = \bigsqcup_{i\in I} Gy_iC$, $L_i = Ly_i^{-1}$, and $\Gamma_i = \Gamma(L_i)$. Then*

$$\sum_{i\in I}\nu(\Gamma_i)\#\{L_i[q,\,\mathfrak{b}]\} = \mathfrak{m}(H,\, H_{\mathbf{A}} \cap C), \tag{5.8}$$

where $q = \varphi[h]$ and $\mathfrak{b} = \varphi(h,\, L)$. This is valid for $(G,\, H)$ of type SU if we replace C and $\Gamma(\cdot\cdot)$ by C^1 and $\Gamma^1(\cdot\cdot)$, provided $n > 2$ and (4.5) is satisfied.

Proof. Take $m = 1$ and $D = C$ in Theorem 5.7. Combining (5.7) with (4.4), we obtain (5.8). The case of SU^φ follows similarly from (4.6).

5.9. Formulas (5.7) and (5.8) are similar to, but different from, the formula of Siegel about $\sum_i \nu(\Gamma_i)\#\{L_i[q]\}$. We already explained in [S3, §13.13] the main differences between our formulas in the orthogonal case given in that book and that of Siegel. In principle, our comments there apply to the present unitary case.

Now in [S2, Theorem 24.4] we gave an exact formula for $\mathfrak{m}(G,\, D)$ for $G = U^\varphi$ and a certain type of D, under the condition that if n is odd, then $d_0(\varphi)$ is represented by an element of $\mathfrak{g}^\times$. The group $H_{\mathbf{A}} \cap C$ in (5.8) does not necessarily belong to the types of D there, but we can compute $[D : H_{\mathbf{A}} \cap C]$ by means of Lemma 3.14 under some conditions on $(q,\, \mathfrak{b})$. Then we obtain $\mathfrak{m}(H,\, H_{\mathbf{A}} \cap C)$ from [S2, Theorem 24.4] by (5.5).

PROPOSITION 5.10. *In the setting of Theorem 5.4 suppose that $n - m$ is odd. Then the structure $(W,\, \det(q)\varphi)$ depends only on φ and the indices of q at the real archimedean primes of F ramified in K.*

Proof. Let ψ be the restriction of φ to W. Then we can easily verify that $d_0\bigl(\det(q)\psi\bigr) = \det(q)^{n-m}d_0(\psi) = (-1)^{n-1}d_0(\varphi)$ as $m - n$ is odd. This combined with Theorem 2.2 (i) proves our proposition.

This is an analogue of the fact concerning a quadratic form in even dimension with square discriminant given in [S4, Theorem 1.12].

We insert here some results about the relationship between various invariants associated with U^φ and those with SU^φ.

PROPOSITION 5.11. *Let D be an open subgroup of $U^\varphi_{\mathbf{A}}$ containing $U^\varphi_{\mathbf{a}}$ and such that $U^\varphi_{\mathbf{h}} \cap D$ is compact; put $P = \{x \in K^\times \mid xx^\rho = 1\}$ and $D^1 = D \cap SU^\varphi_{\mathbf{A}}$. Then $U^\varphi SU^\varphi_{\mathbf{A}}D$ is a normal subgroup of $U^\varphi_{\mathbf{A}}$ and*

$$\text{(5.9a)} \qquad [U^\varphi_{\mathbf{A}} : U^\varphi SU^\varphi_{\mathbf{A}} D] = [P_{\mathbf{A}} : P\det(D)],$$

$$\text{(5.9b)} \qquad \#(U^\varphi\backslash U^\varphi_{\mathbf{A}}/D) \le \sum_{x\in\Xi} \#(SU^\varphi\backslash SU^\varphi_{\mathbf{A}}/xD^1x^{-1}),$$

where $\Xi = U^\varphi_{\mathbf{A}}/U^\varphi SU^\varphi_{\mathbf{A}}D$. *Moreover, if* $U^\varphi_{\mathbf{a}}$ *is compact, then*

$$\text{(5.9c)} \qquad \mathfrak{m}(U^\varphi,\, D) \le [P_{\mathbf{A}} : P\det(D)]\cdot \mathfrak{m}(SU^\varphi,\, D^1).$$

Furthermore, if $P \cap \det(D) = \det(U^\varphi \cap yDy^{-1})$ *for every* $y \in U^\varphi_{\mathbf{A}}$, *then the equality holds in (5.9b), and*

$$\text{(5.9d)} \qquad \#\big(P\cap\det(D)\big)\mathfrak{m}(U^\varphi,\, D) = [P_{\mathbf{A}} : P\det(D)]\mathfrak{m}(SU^\varphi,\, D^1).$$

Proof. Since $P = \det(U^\varphi)$, we can easily show that

$$\text{(5.10)} \qquad U^\varphi SU^\varphi_{\mathbf{A}}Dx = \big\{y \in U^\varphi_{\mathbf{A}} \bigm| \det(y) \in P\det(Dx)\big\}$$

for every $x \in U^\varphi_{\mathbf{A}}$. This shows that $U^\varphi SU^\varphi_{\mathbf{A}}D$ is a normal subgroup of $U^\varphi_{\mathbf{A}}$ and $U^\varphi_{\mathbf{A}}/U^\varphi SU^\varphi_{\mathbf{A}}D$ is isomorphic to $P_{\mathbf{A}}/[P\det(D)]$, as $P_{\mathbf{A}} = \det(U^\varphi_{\mathbf{A}})$. Thus we obtain (5.9a); we also see that $U^\varphi SU^\varphi_{\mathbf{A}}\backslash U^\varphi_{\mathbf{A}}/D$ can be identified with $U^\varphi_{\mathbf{A}}/U^\varphi SU^\varphi_{\mathbf{A}}D$. Given $x \in U^\varphi_{\mathbf{A}}$, take $B_x \subset SU^\varphi_{\mathbf{A}}$ so that $SU^\varphi_{\mathbf{A}} = \bigsqcup_{b\in B_x} SU^\varphi bxD^1x^{-1}$. Then we have $U^\varphi SU^\varphi_{\mathbf{A}}xD = \bigcup_{b\in B_x} U^\varphi bxD$, and hence $U^\varphi_{\mathbf{A}} = \bigcup_{x\in\Xi}\bigcup_{b\in B_x} U^\varphi bxD$. From this we obtain (5.9b). To prove (5.9c), put $\Gamma_x = U^\varphi \cap xDx^{-1}$ and $\Gamma^1_x = SU^\varphi \cap xD^1x^{-1}$ for $x \in U^\varphi_{\mathbf{A}}$. Then $\mathfrak{m}(U^\varphi,\, D) \le \sum_{x\in\Xi}\sum_{b\in B_x}\nu(\Gamma_{bx}) \le \sum_{x\in\Xi}\sum_{b\in B_x}\nu(\Gamma^1_{bx}) = \sum_{x\in\Xi}\mathfrak{m}(SU^\varphi,\, xD^1x^{-1})$. Now formula (5.5) shows that $\mathfrak{m}(SU^\varphi,\, D^1)$ depends only on the measure of D^1. (If $U^\varphi_{\mathbf{a}}$ is not compact, we have to consider the measure of $D^1_{\mathbf{h}}$.) Since $\mathfrak{m}(SU^\varphi,\, xD^1x^{-1}) = \mathfrak{m}(SU^\varphi, D^1)$, we obtain (5.9c).

Suppose $P\cap\det(D) = \det(\Gamma_y)$ for every $y \in U^\varphi_{\mathbf{A}}$. Suppose also that $b'x = abxd$ for $a \in U^\varphi$, $d \in D$, and $b, b' \in B_x$. Then $\det(a) = \det(d^{-1}) \in P \cap \det(D) = \det(\Gamma_{bx})$, and so $\det(a) = \det(c)$ with $c \in \Gamma_{bx}$. Put $e = x^{-1}b^{-1}cbx$. Then $e \in D$, $\det(ed) = 1$, and $b'x = abxd = ac^{-1}bxed \in SU^\varphi bxD^1$. Thus $b' = b$. This shows that $U^\varphi SU^\varphi_{\mathbf{A}}xD = \bigsqcup_{b\in B_x} SU^\varphi bxD$, from which we obtain the equality in (5.9b). Also, $\nu(\Gamma^1_{bx})/\nu(\Gamma_{bx}) = [\Gamma_{bx} : \Gamma^1_{bx}] = \#\big(\det(\Gamma_{bx})\big) = \#\big(P\cap\det(D)\big)$, and so

$$\begin{aligned}\#\big(P\cap\det(D)\big)\mathfrak{m}(U^\varphi,\, D) &= \sum_{x\in\Xi}\sum_{b\in B_x}\nu(\Gamma^1_{bx})\\ &= \sum_{x\in\Xi}\mathfrak{m}(SU^\varphi,\, xD^1x^{-1}) = \#(\Xi)\cdot\mathfrak{m}(SU^\varphi,\, D^1),\end{aligned}$$

which is (5.9d).

Department of Mathematics, Princeton University, Princeton, NJ

References

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

[L] W. Landherr, Äquivalenz Hermitscher Formen über einem beliebigen algebraischen Zahlkörper, Abh. Math. Sem. Hamb., 11 (1936), 245-248.

[S1] G. Shimura, Arithmetic of unitary groups, Ann. of Math., 79 (1964), 369–409 (=Collected Papers, I, 473-513).

[S2] G. Shimura, Euler Products and Eisenstein series, CBMS Regional Conference Series in Mathematics, No. 93, American Mathematical Society, 1997.

[S3] G. Shimura, Arithmetic and analytic theories of quadratic forms and Clifford groups, Mathematical Surveys and Monographs, vol. 109, American Mathematical Society, 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, Amer. J. Math. 128 (2006), 1521–1552.

[S6] G. Shimura, Integer-valued quadratic forms and quadratic Diophantine equations, Documenta Mathematica 11, (2006), 333-367.

[S7] G. Shimura, Quadratic Diophantine equations, the class number, and the mass formula, Bull. Amer. Math. Soc. 43 (2006), 285-304.

Goro Shimura
Department of Mathematics
Princeton University
Princeton
NJ 08544–1000
USA
goro@Math.Princeton.EDU