J. Math. Soc. Japan
Vol. 15, No. 1, 1963

Arithmetic of alternating forms and quaternion hermitian forms

By Goro SHIMURA

(Received June 21, 1962)

Hecke's Dirichlet series obtained from modular forms can be regarded as zeta-functions attached to the general linear group $GL(2, \boldsymbol{Q})$ over the rational number field $\boldsymbol{Q}$. In general, we may expect to obtain zeta-functions of this kind for a fairly wide class of algebraic groups defined over $\boldsymbol{Q}$. In order to realize this, it is necessary to develop, in the first place, the theory of elementary divisors for any algebraic group G in question. This is actually done in the case where G is the multiplicative group of a semi-simple algebra. Further, the case of the orthogonal group is investigated in detail by M. Eichler [3]. In both cases, there are fundamental theorems, due to Eichler [4, 5] and M. Kneser [6], which may be called the approximation theorem in the group G, from which one can easily derive an important conclusion about the class-number for G. This approximation theorem plays an essential role also in the theory of Hecke-rings attached to quaternion algebras [8, 9]. In fact, by means of the theorem, we can prove the isomorphism between the Hecke-ring defined by the idele-group of a quaternion algebra D and the Hecke-ring defined by the unit-groups of maximal orders in D (cf. [9, § 2]).

The purpose of the present paper is to give an extension of the theory of elementary divisors for the group of similitudes of a hermitian form over a quaternion algebra, and to prove an approximation theorem for this group. Let F be the quotient field of a Dedekind domain $\mathfrak{g}$ and A a quaternion (not necessarily division) algebra over F. Let V be a left A-module which is isomorphic to the product of n copies of A. We consider an A-valued non-degenerate hermitian form $f(x, y)$ on V with respect to the canonical involution of A (cf. § 2.2). Let G be the group consisting of all A-automorphisms σ of V such that $f(x\sigma, y\sigma) = N(\sigma)f(x, y)$ for $x \in V$, $y \in V$ with $N(\sigma) \in F$. Take a maximal oder $\mathfrak{o}$ in A. Let L be a $\mathfrak{g}$-lattice in V such that $\mathfrak{o}L \subset L$. We denote by $N(L)$ the two-sided $\mathfrak{o}$-ideal generated by $f(x, y)$ for $x \in L$, $y \in L$, and call it the norm of L. We say that L is maximal if L is a maximal one among the lattices with the same norm. As in [3], our theory is mostly concerned with maximal lattices in V. If A is the total matric algebra of degree 2 over F, then G is isomorphic to the group of similitudes of an alternating

form over F with $2n$ variables. We treat this case in § 1 and § 2.5, and prove fundamental propositions concerning the existence of canonical bases for maximal lattices and their elementary divisors. We give in § 3 similar propositions in case where A is a division quaternion algebra over a $\mathfrak{p}$-adic field. These propositions correspond to the results of the same kind obtained in the case of orthogonal groups [Eicher, **3**] and of quaternion anti-hermitian forms [Tsukamoto, **10**]. In § 4, we consider the global theory, namely the case where F is an algebraic number field. Our principal aim is to prove approximation-theorems for G (Theorems 1 and 2 of § 4.6) in case where A is indefinite. As an application of the theorems, we can show that the classes of maximal lattices in each genus are in one-to-one correspondence with the ideal-classes modulo $\mathfrak{t}$ in F for a suitable product $\mathfrak{t}$ of infinite prime spots of F (Theorem 3). If we denote by G^0 the unitary group of f, i.e. the subgroup of G composed of the elements σ such that $N(\sigma)=1$, then each genus with respect to G^0 consists of only one class (§ 4.9). Finally we give a result on global set of elementary divisors of maximal lattices (Theorem 4). As explained in the beginning, our theory can be considered as preliminaries for the theory of the Hecke-ring of G. In fact, by means of our propositions and theorems, we can develop such a theory, which is a generalization of the theory in [**9**, § 2]. As for this, we have only given Proposition 4.11. A further investigation of the Hecke-ring of G will be made in a subsequent paper.

NOTATION. We denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ and $\boldsymbol{K}$, respectively, the ring of rational integers, the rational number field, the real number field, the complex number field, and the division ring of real quaternions. For a ring S with an identity element, $M_m(S)$ denotes the ring of matrices of degree m with entries in S; the identity matrix of degree m is denoted by 1_m; and the transpose of a matrix X is denoted by ${}^tX$. We mean by δ_{ij} the usual Kronecker's delta, namely $\delta_{ij}=0$ or 1 according as $i\neq j$ or $i=j$.

§ 1. Arithmetic of alternating forms.

1.1. Alternating form and symplectic group. Let F be an arbitrary field and W a vector space over F of finite dimension. We denote by $E(W)$ the ring of all F-linear mappings of W into itself, and by $GL(W)$ the group of regular elements of $E(W)$. We write the operation of an element of $E(W)$ on the right; so we have $(ax)\sigma=a(x\sigma)$ for $a\in F$, $x\in W$, $\sigma\in E(W)$. Let $g(x,y)$ be a non-degenerate alternating form on W. We denote by $G(W,g)$ the subgroup of $GL(W)$ consisting of the elements σ of $GL(W)$ for which there exists a number $N(\sigma)$ of F such that $g(x\sigma,y\sigma)=N(\sigma)g(x,y)$ for every $x,y\in W$, and denote by $G^0(W,g)$ the symplectic group associated to g, namely, the subgroup of $G(W,g)$ consisting of the elements σ such that $N(\sigma)=1$.

1.2. Lattices in a vector space. Let $\mathfrak{g}$ be a Dedekind domain and F the quotient field of $\mathfrak{g}$. Let W be a vector space over F. By a $\mathfrak{g}$-*lattice* in W, we understand a finitely generated $\mathfrak{g}$-submodule L of W such that $FL=W$. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{g}$. We denote by $F_\mathfrak{p}$ and $\mathfrak{g}_\mathfrak{p}$ the $\mathfrak{p}$-completions of F and $\mathfrak{g}$, respectively. Put $W_\mathfrak{p}=W\underset{F}{\otimes}F_\mathfrak{p}$. For every $\mathfrak{g}$-lattice L in W, put $L_\mathfrak{p}=\mathfrak{g}_\mathfrak{p}L$; then $L_\mathfrak{p}$ is a $\mathfrak{g}_\mathfrak{p}$-lattice in $W_\mathfrak{p}$. The following lemma is well-known.

LEMMA 1.1. *Let L be a $\mathfrak{g}$-lattice in W. Take, for each prime ideal $\mathfrak{p}$ of $\mathfrak{g}$, a $\mathfrak{g}_\mathfrak{p}$-lattice $M^\mathfrak{p}$ in $W_\mathfrak{p}$. Then there exists a $\mathfrak{g}$-lattice M in W such that $M_\mathfrak{p}=M^\mathfrak{p}$ for every $\mathfrak{p}$, if and only if $M^\mathfrak{p}=L_\mathfrak{p}$ for all except a finite number of $\mathfrak{p}$. If such a lattice M exists, we have $M=\bigcap_\mathfrak{p}(M_\mathfrak{p}\cap W)$.*

LEMMA 1.2. *Let $L_\mathfrak{p}$ be a $\mathfrak{g}_\mathfrak{p}$-lattice in $W_\mathfrak{p}$; let σ and τ be elements of $GL(W_\mathfrak{p})$. Suppose that $L_\mathfrak{p}(\sigma-\tau)\subset\mathfrak{p}L_\mathfrak{p}\sigma$. Then we have $L_\mathfrak{p}\sigma=L_\mathfrak{p}\tau$.*

PROOF. Let $x_1,\cdots,x_m$ be generators of $L_\mathfrak{p}$ over $\mathfrak{g}_\mathfrak{p}$. Put $M=L_\mathfrak{p}\sigma$, $K=L_\mathfrak{p}\tau$. Then we have $x_i\sigma-x_i\tau\in\mathfrak{p}M\subset M$ for every i. As M and K are respectively generated by the $x_i\sigma$ and the $x_i\tau$, we get $K\subset M$. Further we have $M\subset K+\mathfrak{p}M$. From this we obtain inductively $M\subset K+\mathfrak{p}^eM$ for every positive integer e. This implies $M\subset K$, so that $M=K$.

1.3. Canonical base of a lattice with respect to an alternating form. We first prove a generalization of a well-known theorem of Frobenius.

PROPOSITION 1.3. *Let $\mathfrak{g}$ be a Dedekind domain and F the quotient field of $\mathfrak{g}$. Let W be a vector space of dimension $2n$ over F and $g(x,y)$ a non-degenerate alternating form on W. Let M be a $\mathfrak{g}$-lattice in W. Then there exist a base $\{y_1,\cdots,y_n,z_1,\cdots,z_n\}$ of W over F and (fractional) $\mathfrak{g}$-ideals $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$ such that*

$$g(y_i,y_j)=g(z_i,z_j)=0\,,\qquad g(y_i,z_j)=\delta_{ij}\,,$$

$$M=\mathfrak{g}y_1+\mathfrak{g}y_2+\cdots+\mathfrak{g}y_n+\mathfrak{a}_1z_1+\mathfrak{a}_2z_2+\cdots+\mathfrak{a}_nz_n\,,$$

$$\mathfrak{a}_1\supset\mathfrak{a}_2\supset\cdots\supset\mathfrak{a}_n\,.$$

The ideals $\mathfrak{a}_i$ are uniquely determined by M and g.

PROOF. We prove this by induction on n. For every $x\in M$, put $\mathfrak{a}_x=g(x,M)$. Obviously, $\mathfrak{a}_x$ is a $\mathfrak{g}$-ideal. As M is a $\mathfrak{g}$-lattice, there exists a maximal one among the $\mathfrak{a}_x$, say $\mathfrak{a}_1$; and take an element y_1 of M so that $\mathfrak{a}_1=g(y_1,M)$. As we have $\mathfrak{g}=g(y_1,\mathfrak{a}_1^{-1}M)$, there exists an element z_1 of $\mathfrak{a}_1^{-1}M$ such that $g(y_1,z_1)=1$. Put $\mathfrak{b}=g(M,z_1)$. As $\mathfrak{b}\ni g(y_1,z_1)=1$, we have $\mathfrak{b}\supset\mathfrak{g}$, so that $\mathfrak{a}_1\mathfrak{b}=\mathfrak{a}_1g(M,z_1)\supset\mathfrak{a}_1$. Assume that $\mathfrak{b}\neq\mathfrak{g}$. Then $\mathfrak{a}_1g(M,z_1)\neq\mathfrak{a}_1$, and hence there exist an element u of M and an element α of $\mathfrak{a}_1$ such that $g(u,\alpha z_1)\notin\mathfrak{a}_1$. Put $\beta=-g(u,\alpha z_1)$, $\gamma=g(y_1,u)$. We have then $g(y_1+\alpha z_1,u-\gamma z_1)=\beta$. Since $\gamma\in\mathfrak{a}_1$ and $\mathfrak{a}_1z_1\subset M$, the element $u-\gamma z_1$ is contained in M. We note that $g(y_1+\alpha z_1,\mathfrak{a}_1z_1)=\mathfrak{a}_1$. Therefore, we have

$$g(y_1+\alpha z_1,M)\supset\mathfrak{a}_1+\mathfrak{g}\beta\supset\mathfrak{a}_1\,,\qquad\mathfrak{a}_1+\mathfrak{g}\beta\neq\mathfrak{a}_1\,.$$

This contradicts the maximality of $\mathfrak{a}_1$. Hence we must have $g(M, z_1) = \mathfrak{g}$. Now define a submodule M' of M by $M' = \{v \in M \mid g(y_1, v) = g(z_1, v) = 0\}$. For every $w \in M$, put $\xi = g(y_1, w)$, $\eta = g(z_1, w)$, $w_0 = w + \eta y_1 - \xi z_1$. Then $\xi \in \mathfrak{a}_1$, $\eta \in \mathfrak{g}$, and we have $g(y_1, w_0) = g(z_1, w_0) = 0$, so that $w_0 \in M'$. This shows that $M = \mathfrak{g}y_1 + \mathfrak{a}_1 z_1 + M'$. Applying our induction to M', we get an expression $M' = \mathfrak{g}y_2 + \cdots + \mathfrak{g}y_n + \mathfrak{a}_2 z_2 + \cdots + \mathfrak{a}_n z_n$ with the properties $\mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n$, $g(y_i, y_j) = g(z_i, z_j) = 0$, $g(y_i, z_j) = \delta_{ij}$ for $2 \leqq i \leqq n$, $2 \leqq j \leqq n$. Therefore, the first assertion is proved if we show $\mathfrak{a}_1 \supset \mathfrak{a}_2$. Let u and v be elements of M'. We have $g(y_1 + u, M) \supset g(y_1 + u, \mathfrak{a}_1 z_1 + \mathfrak{g}v) \supset \mathfrak{a}_1 + \mathfrak{g}g(u, v) \supset \mathfrak{a}_1$. By the maximality of $\mathfrak{a}_1$, we must have $g(u, v) \in \mathfrak{a}_1$, namely $g(M', M') \subset \mathfrak{a}_1$. This implies $\mathfrak{a}_1 \supset \mathfrak{a}_2$ and completes the proof of the first assertion. The invariance of the ideals $\mathfrak{a}_i$ is easily shown by "localization". Namely, for every prime ideal $\mathfrak{p}$ of $\mathfrak{g}$, consider $W_\mathfrak{p} = W \underset{F}{\otimes} F_\mathfrak{p}$ and a $\mathfrak{g}_\mathfrak{p}$-lattice $M_\mathfrak{p} = \mathfrak{g}_\mathfrak{p} M$ in $W_\mathfrak{p}$. Then the invariance is an immediate consequence of the theory of elementary divisors over a principal ideal domain (cf. [2, § 5.1, Theorem 1]). We can also prove the invariance more directly with no use of localization.

We call the ideals $\mathfrak{a}_i$ of Proposition 1.3 *the invariant factors of* M (with respect to g), and call $\{y_1, \cdots, y_n, z_1, \cdots, z_n\}$ a *canonical base of* M (with respect to g).

1.4. Maximal lattices. Let F, $\mathfrak{g}$, W, g be the same as in Proposition 1.3. For every $\mathfrak{g}$-lattice M in W, we see that the first member $\mathfrak{a}_1$ of the invariant factors of M is the $\mathfrak{g}$-ideal generated by $g(x, y)$ for $x, y \in M$. We put $N_g(M) = \mathfrak{a}_1$ and call $N_g(M)$ the *norm* of M with respect to g. For simplicity, we fix g and write $N(M) = N_g(M)$. We say that M is *maximal* (with respect to g) if M is a maximal one among the $\mathfrak{g}$-lattices in W with the same norm (with respect to g). It is clear that $N(M\sigma) = N(M)N(\sigma)$ for every $\sigma \in G(W, g)$. If M is maximal, $M\sigma$ is maximal for every $\sigma \in G(W, g)$. By Proposition 1.3, we see easily that M is maximal if and only if the invariant factors of M are all equal to $N(M)$. Furthermore, if M is a $\mathfrak{g}$-lattice in W and $\mathfrak{a}$ is a $\mathfrak{g}$-ideal such that $\mathfrak{a} \supset N(M)$, we can find a maximal lattice L in W such that $L \supset M$, $N(L) = \mathfrak{a}$.

PROPOSITION 1.4. *Let M_1 and M_2 be maximal lattices in W. Then we have $M_1\sigma = M_2$ for an element σ of $G(W, g)$, if and only if $N(M_1)^{-1}N(M_2)$ is a principal ideal.*

PROOF. If $M_1\sigma = M_2$ for an element $\sigma \in G(W, g)$, we have $N(M_2) = N(M_1\sigma) = N(M_1)N(\sigma)$; this proves the 'only if' part. Conversely, put $\mathfrak{a}_i = N(M_i)$ and $\mathfrak{a}_1^{-1}\mathfrak{a}_2 = \mathfrak{g}\alpha$ with $\alpha \in F$. Let $\{y_1, \cdots, y_n, z_1, \cdots, z_n\}$ and $\{u_1, \cdots, u_n, v_1, \cdots, v_n\}$ be respectively canonical bases of M_1 and M_2. Define an element σ of $E(W)$ by $y_i\sigma = u_i$, $z_i\sigma = \alpha v_i$ for $1 \leqq i \leqq n$. Then we see easily $\sigma \in G(W, g)$, $N(\sigma) = \alpha$, $M_1\sigma = M_2$. This proves the 'if' part.

We say that maximal lattices M_1 and M_2 in W are *equivalent* if $M_1=M_2\sigma$ for an element σ of $G(W,g)$, and call a maximal set of mutually equivalent maximal lattices a *class* of maximal lattices. By Proposition 1.4, we observe that *the mapping $M\to N(M)$ gives a one-to-one correspondence between the classes of maximal lattices in W and the ideal-classes of F.*

1.5. Invariant factors of elements of $G(W,g)$. Notation being as in §§ 1.3-4, suppose that $\mathfrak{g}$ is a principal ideal domain.

PROPOSITION 1.5. *Let L and M be maximal lattices in W. Let α be an element of F such that $N(M)=\alpha N(L)$. Put $N(L)=\mathfrak{a}$. Then there exist a canonical base $\{y_1,\cdots,y_n,z_1,\cdots,z_n\}$ of L and elements $a_1,\cdots,a_n,b_1,\cdots,b_n$ of F such that*

$$L=\mathfrak{g}y_1+\cdots+\mathfrak{g}y_n+\mathfrak{a}z_1+\cdots+\mathfrak{a}z_n,$$

$$M=\mathfrak{g}a_1y_1+\cdots+\mathfrak{g}a_ny_n+\mathfrak{a}b_1z_1+\cdots+\mathfrak{a}b_nz_n,$$

$$\alpha=a_1b_1=\cdots=a_nb_n,$$

$$\mathfrak{g}a_1\supset\cdots\supset\mathfrak{g}a_n\supset\mathfrak{g}b_n\supset\cdots\supset\mathfrak{g}b_1.$$

PROOF. We proceed by induction on n. Put $\mathfrak{c}=\{c\in F\mid cM\subset L\}$. It is easy to see that $\mathfrak{c}$ is a $\mathfrak{g}$-ideal. As $\mathfrak{g}$ is a principal ideal domain, we have $\mathfrak{c}=\mathfrak{g}c_0$ for an element c_0 of F. Put $M'=c_0M$. Then M' is a maximal lattice, and $N(M')=c_0^2\alpha\mathfrak{a}$, $\mathfrak{g}=\{c\in F\mid cM'\subset L\}$. If we prove our proposition for M' and $c_0^2\alpha$, we get easily the assertion for M and α. Therefore, we may assume that $M=M'$, namely, $\mathfrak{g}=\{c\in F\mid cM\subset L\}$. The last relation implies that $L\supset M$ and M contains an element $y_1\neq 0$ such that $L/\mathfrak{g}y_1$ is a free $\mathfrak{g}$-module. Put $M_1=M+\alpha L$. Then M_1 is a $\mathfrak{g}$-lattice in W. As $L\supset M$ and $N(M)=\alpha N(L)$, we must have $\alpha\in\mathfrak{g}$; hence we see easily $N(M_1)=\alpha N(L)=N(M)$. As M is maximal, we must have $M=M_1$, so that $M\supset\alpha L$. Now taking a canonical base of L, and expressing y_1 in a linear form of the base, we find that $g(y_1,L)=\mathfrak{a}$. By the proof of Proposition 1.3, we can find an element z_1 of $\mathfrak{a}^{-1}L$ such that $g(y_1,z_1)=1$; and if we put $U=\{x\in W\mid g(y_1,x)=g(z_1,x)=0\}$, $L_0=L\cap U$, we get $L=\mathfrak{g}y_1+\mathfrak{a}z_1+L_0$. We see easily that L_0 is a maximal lattice in U and $N(L_0)=\mathfrak{a}$. As $\alpha L\subset M$, we have $\alpha\mathfrak{a}z_1\subset M$. For every $x\in M$, we have $g(y_1,x)\in N(M)=\alpha\mathfrak{a}$, $g(z_1,x)\in\mathfrak{a}^{-1}N(L)=\mathfrak{g}$. Hence if we put $g(y_1,x)=\xi\alpha$, $g(z_1,x)=\eta$, then $\xi\in\mathfrak{a}$, $\eta\in\mathfrak{g}$. Put $x_0=x+\eta y_1-\xi\alpha z_1$. We have then $x_0\in M$ and $g(y_1,x_0)=g(z_1,x_0)=0$, so that $x_0\in U\cap M$. This proves that $M=\mathfrak{g}y_1+\mathfrak{a}\alpha z_1+M_0$, if we put $M_0=U\cap M$. As M is maximal, M_0 must be a maximal lattice in U such that $N(M_0)=\mathfrak{a}\alpha$. Applying our induction assumption to L_0 and M_0, we find a canonical base $\{y_2,\cdots,y_n,z_2,\cdots,z_n\}$ of L_0 and elements $a_2,\cdots,a_n,b_2,\cdots,b_n$ of F such that

$$L_0 = \mathfrak{g}y_2 + \cdots + \mathfrak{g}y_n + \mathfrak{a}z_2 + \cdots + \mathfrak{a}z_n ,$$
$$M_0 = \mathfrak{g}a_2 y_2 + \cdots + \mathfrak{g}a_n y_n + \mathfrak{a}b_2 z_2 + \cdots + \mathfrak{a}b_n z_n ,$$
$$\alpha = a_2 b_2 = \cdots = a_n b_n ,$$
$$\mathfrak{g}a_2 \supset \cdots \supset \mathfrak{g}a_n \supset \mathfrak{g}b_n \supset \cdots \supset \mathfrak{g}b_2 .$$

As $L_0 \supset M_0$, we have $\mathfrak{g} \supset \mathfrak{g}a_2$, so that $\mathfrak{g}b_2 \supset \mathfrak{g}\alpha$. Putting $a_1 = 1$ and $b_1 = \alpha$, we obtain our assertion for L and M.

PROPOSITION 1.6. *Let L be a maximal lattice in W. Let $\{u_1, \cdots, u_n, v_1, \cdots, v_n\}$ be a canonical base of L. Denote by Γ^0 the subgroup of $G^0(W, g)$ consisting of elements γ of $G^0(W, g)$ such that $L\gamma = L$, and by Δ the set of elements σ of $G(W, g)$ such that $u_i\sigma = a_i u_i$, $v_i\sigma = b_i v_i$ for $1 \leqq i \leqq n$ with elements a_i, b_i of F and $\mathfrak{g}a_1 \supset \cdots \supset \mathfrak{g}a_n \supset \mathfrak{g}b_n \supset \cdots \supset \mathfrak{g}b_1$. Then we have $G(W, g) = \Gamma^0 \cdot \Delta \cdot \Gamma^0$.*

PROOF. Let σ be an element of $G(W, g)$. Put $M = L\sigma$, $\alpha = N(\sigma)$, and apply Proposition 1.5 to this $\{L, M, \alpha\}$. Then we get a canonical base $\{y_i, z_i\}$ of L and elements a_i, b_i of F with the properties of that proposition. Define two elements γ and τ of $E(W)$ by $u_i\gamma = y_i$, $v_i\gamma = z_i$, $u_i\tau = a_i u_i$, $v_i\tau = b_i v_i$. We see easily that $\gamma \in \Gamma^0$ and $\tau \in \Delta$, $N(\tau) = \alpha$. Further we have $L\tau\gamma = L\sigma$. Hence if we put $\varepsilon\tau\gamma = \sigma$, we have $L\varepsilon = L$, $\varepsilon \in G(W, g)$, $N(\varepsilon) = 1$, so that $\varepsilon \in \Gamma^0$. It follows that $\sigma = \varepsilon\tau\gamma \in \Gamma^0 \cdot \Delta \cdot \Gamma^0$. Our proposition is thereby proved.

§ 2. Hermitian forms over a quaternion algebra.

2.1. Quaternion algebras. By a *quaternion algebra* over a field F, we understand a central simple algebra A over F such that $[A : F] = 4$. Every quaternion algebra A over F has an involution $a \to a'$, which is uniquely determined by the property that $(X-a)(X-a')$ is the principal polynomial of a over F. We call it the *canonical involution* of A and always denote it by $a \to a'$. For every $a \in A$, we put

$$N(a) = aa' , \qquad \mathrm{Tr}(a) = a + a' .$$

If A is not a division algebra, A is isomorphic to $M_2(F)$; and for every $a \in M_2(F)$, $N(a)$ is just the determinant of a and $\mathrm{Tr}(a)$ is the trace of a. Hereafter we assume that the characteristic of F is different from 2. Then, for an element a of A, we have $a = a'$ if and only if $a \in F$.

If F is the quotient field of a Dedekind domain $\mathfrak{g}$, we can develop ideal-theory in A. Here we recall only the definition of different and norm of ideals. Let $\mathfrak{o}$ be a maximal order in A. The different $\mathfrak{D} = \mathfrak{D}(\mathfrak{o}/\mathfrak{g})$ of $\mathfrak{o}$ with respect to $\mathfrak{g}$ is the integral two-sided $\mathfrak{o}$-ideal defined by

$$\mathfrak{D}^{-1} = \{x \in A \mid \mathrm{Tr}(x\mathfrak{o}) \subset \mathfrak{g}\} .$$

Let $\mathfrak{a}$ be a right (resp. left) $\mathfrak{o}$-ideal. We denote by $N(\mathfrak{a})$ the $\mathfrak{g}$-ideal generated

by the elements $N(a)$ for $a \in \mathfrak{a}$. If we put $\mathfrak{a}' = \{x' \mid x \in \mathfrak{a}\}$, then $\mathfrak{a}'\mathfrak{a} = N(\mathfrak{a})\mathfrak{o}$ (resp. $\mathfrak{a}\mathfrak{a}' = N(\mathfrak{a})\mathfrak{o}$).

2.2. *Q*-hermitian forms. Let A be a quaternion algebra over a field F. By an *A-space of dimension n*, we understand a left A-module V isomorphic to the product of n copies of A; and we put $n = \dim_A V$. We call a set of elements $\{x_1, \cdots, x_n\}$ of V a *base of V over A* if $V = Ax_1 + \cdots + Ax_n$.

Let V be an A-space of dimension n. We understand by a *Q-hermitian form* on V an F-bilinear mapping f of $V \times V$ into A satisfying

$$f(ax, y) = af(x, y), \qquad f(x, y)' = f(y, x)$$

for $a \in A$, $x \in V$, $y \in V$. We call f *non-degenerate* if $f(x, V) = \{0\}$ implies $x = 0$.

PROPOSITION 2.1. *Let A be a quaternion algebra over a field F and V be an A-space of dimension n. For every Q-hermitian form $f(x, y)$ on V, there exists a base $\{x_1, \cdots, x_n\}$ of V over A such that $f(x_i, x_j) = \alpha_i \delta_{ij}$ for $1 \leqq i \leqq n$, $1 \leqq j \leqq n$ with $\alpha_i \in F$. Moreover, suppose that f is non-degenerate and A satisfies the following condition:*

(D) *For every $\alpha \in F$, there exists an element a of A such that $N(a) = \alpha$.*

Then there exists a base $\{y_1, \cdots, y_n\}$ of V over A such that $f(y_i, y_j) = \delta_{ij}$.

This is well-known and in fact easily proved. If $A = M_2(F)$, the condition (D) is clearly satisfied.

Let V be an A-space. We denote by $E(V, A)$ the ring of all F-linear mappings σ of V into itself satisfying $(ax)\sigma = a(x\sigma)$ for every $a \in A$, $x \in V$, and by $GL(V, A)$ the group of regular elements of $E(V, A)$. Let f be a non-degenerate Q-hermitian form on V. We denote by $G(V, f)$ the subgroup of $GL(V, A)$ consisting of the elements σ for which there exists a number $N(\sigma)$ of F such that $f(x\sigma, y\sigma) = N(\sigma) f(x, y)$ for every $x \in V$, $y \in V$; and put $G^0(V, f) = \{\sigma \in G(V, f) \mid N(\sigma) = 1\}$. $G^0(V, f)$ is clearly a normal subgroup of $G(V, f)$. If ξ is a non-zero element of F, we have $f(\xi x, \xi y) = \xi^2 f(x, y)$; so we often consider ξ as an element of $G(V, f)$. If $\dim_A V = 1$, $E(V, A)$ is isomorphic to A, and $G(V, f)$ is isomorphic to the group of regular elements of A; for every $\sigma \in G(V, f)$, $N(\sigma)$ coincides with $N(\sigma)$ of σ considered as an element of A.

Fix a base $\{x_1, \cdots, x_n\}$ of V over A. Every element σ of $E(V, A)$ is represented by a matrix (s_{ij}) of $M_n(A)$ with respect to $\{x_i\}$:

$$x_i\sigma = \sum_{j=1}^{n} s_{ij} x_j \qquad (1 \leqq i \leqq n). \tag{1}$$

For every element $S = (s_{ij})$ of $M_n(A)$, we put $S' = (t_{ij})$ with $t_{ij} = s_{ji}'$. Then $S \to S'$ is an involution of $M_n(A)$. Let $f(x, y)$ be a Q-hermitian form on V. Define an element $H = (h_{ij})$ of $M_n(A)$ by $h_{ij} = f(x_i, x_j)$. Then we have $H' = H$. An element σ of $GL(V, A)$ belongs to $G(V, f)$ if and only if we have $SHS' = \alpha H$ with $\alpha \in F$ for the matrix S corresponding to σ; and then we have $N(\sigma) = \alpha$.

2.3. Elementary theory of maximal lattices. Let $\mathfrak{g}$ be a Dedekind domain and F the quotient field of $\mathfrak{g}$. Let A be a quaternion algebra over F and V an A-space of dimension n. Take a non-degenerate Q-hermitian form f on V. Let L be a $\mathfrak{g}$-lattice in V. Put $\mathfrak{o}=\{a\in A \mid aL\subset L\}$. Then $\mathfrak{o}$ is an order in A. We call $\mathfrak{o}$ *the order of* L and say that L is *normal* if $\mathfrak{o}$ is a maximal order in A. Assume that L is normal. We denote by $N_f(L)$ the two-sided $\mathfrak{o}$-ideal generated by the elements $f(x,y)$ for $x\in L$, $y\in L$, and call $N_f(L)$ the norm of L with respect to f. We denote $N_f(L)$ simply by $N(L)$ when we fix f and there is no fear of confusion.

Now, for every prime ideal $\mathfrak{p}$ of $\mathfrak{g}$, consider the $\mathfrak{p}$-completion $F_\mathfrak{p}$ and $\mathfrak{g}_\mathfrak{p}$ of F and $\mathfrak{g}$. Put $A_\mathfrak{p}=A\underset{F}{\otimes}F_\mathfrak{p}$, $V_\mathfrak{p}=V\underset{F}{\otimes}F_\mathfrak{p}$. Then $V_\mathfrak{p}$ can be considered as an $A_\mathfrak{p}$-space of dimension n in a natural manner. Further f is uniquely extended to a non-degenerate Q-hermitian form on $V_\mathfrak{p}$, which we denote again by f. The following proposition is an easy consequence of our definition.

PROPOSITION 2.2. *Let L be a $\mathfrak{g}$-lattice in V. If $\mathfrak{o}$ is the order of L, then $\mathfrak{o}_\mathfrak{p}$ $(=\mathfrak{g}_\mathfrak{p}\mathfrak{o})$ is the order of $L_\mathfrak{p}$ $(=\mathfrak{g}_\mathfrak{p}L)$. L is normal if and only if $L_\mathfrak{p}$ is normal for every prime ideal $\mathfrak{p}$ of $\mathfrak{g}$. If L is normal, we have $N(L)_\mathfrak{p}=N(L_\mathfrak{p})$.*

Let L be a normal lattice in V and $\mathfrak{o}$ the order of L. We call L *maximal* (with respect to f) if L is a maximal one among the normal lattices with the same order $\mathfrak{o}$ and the same norm $N(L)$.

PROPOSITION 2.3. *Let L be a $\mathfrak{g}$-lattice in V and σ an element of $G(V,f)$. Then $L\sigma$ is a $\mathfrak{g}$-lattice in V with the same order as L. If L is normal, so is $L\sigma$; and we have $N(L\sigma)=N(L)N(\sigma)$. Moreover, if L is maximal, so is $L\sigma$.*

This is also an easy consequence of definition. Further, by Lemma 1.1 and Proposition 2.2, we obtain

PROPOSITION 2.4. *A normal $\mathfrak{g}$-lattice in V is maximal if and only if $L_\mathfrak{p}$ is maximal for every prime ideal $\mathfrak{p}$ of $\mathfrak{g}$.*

Hereafter, we call a normal maximal $\mathfrak{g}$-lattice in V simply a *maximal lattice* in V.

PROPOSITION 2.5. *Let L be a normal $\mathfrak{g}$-lattice in V with the order $\mathfrak{o}$. Let $\mathfrak{a}$ be a right $\mathfrak{o}$-ideal and $\mathfrak{o}_1$ the left order of $\mathfrak{a}$. Then $\mathfrak{a}L$ is a normal $\mathfrak{g}$-lattice in V with the order $\mathfrak{o}_1$, and $N(\mathfrak{a}L)=\mathfrak{a}N(L)\mathfrak{a}^{-1}\cdot N(\mathfrak{a})$. Moreover, if L is maximal, so is $\mathfrak{a}L$.*

PROOF. The first assertion is clear. Let $x=\sum_i a_ix_i$ and $y=\sum_j b_jy_j$ be elements of $\mathfrak{a}L$ where $a_i, b_j\in\mathfrak{a}$ and $x_i, y_j\in L$. Then we have $f(x,y)=\sum_{i,j}a_if(x_i,y_j)b_j'$ $\in\mathfrak{a}N(L)\mathfrak{a}'$. As $\mathfrak{a}\mathfrak{a}'=\mathfrak{o}_1N(\mathfrak{a})$, we get $\mathfrak{a}N(L)\mathfrak{a}'=\mathfrak{a}N(L)\mathfrak{a}^{-1}\cdot N(\mathfrak{a})$. Therefore we obtain $N(\mathfrak{a}L)\subset\mathfrak{a}N(L)\mathfrak{a}^{-1}\cdot N(\mathfrak{a})$. Substituting $\mathfrak{a}^{-1}$ and $\mathfrak{a}L$ for $\mathfrak{a}$ and L, we get the inverse inclusion, so that the equality $N(\mathfrak{a}L)=\mathfrak{a}N(L)\mathfrak{a}^{-1}N(\mathfrak{a})$ holds. The last assertion follows easily from this relation.

PROPOSITION 2.6. *Let $\{x_1,\cdots,x_n\}$ be a base of V over A such that $f(x_i,x_j)$*

$=\alpha_i\delta_{ij}$ *with* $\alpha_i \in F$. *Let* $\mathfrak{o}$ *be a maximal order in* A *and* $\mathfrak{b}_1, \cdots, \mathfrak{b}_n$ *be left* $\mathfrak{o}$*-ideals such that* $\alpha_1 N(\mathfrak{b}_1) = \cdots = \alpha_n N(\mathfrak{b}_n)$. *Then* $L = \mathfrak{b}_1 x_1 + \cdots + \mathfrak{b}_n x_n$ *is a maximal lattice with the order* $\mathfrak{o}$ *and* $N(L) = \alpha_1 N(\mathfrak{b}_1)\mathfrak{o}$.

PROOF. It is clear that L is a $\mathfrak{g}$-lattice in V with the order $\mathfrak{o}$, and $N(L) = \alpha_i N(\mathfrak{b}_i)\mathfrak{o}$. Let M be a $\mathfrak{g}$-lattice with the order $\mathfrak{o}$ such that $M \supset L$ and $N(M) = N(L)$. Let $y = \sum_{i=1}^{n} b_i x_i$ be an element of M with $b_i \in A$. We have $b_i \alpha_i \mathfrak{b}_i' = f(y, \mathfrak{b}_i x_i) \subset N(M) = N(L) = \alpha_i \mathfrak{b}_i \mathfrak{b}_i'$, so that $b_i \in \mathfrak{b}_i$. This implies $y \in L$ and hence $M = L$. Therefore L is maximal.

PROPOSITION 2.7. *Let* L *and* M *be maximal lattices in* V *with the same order. Let* $\mathfrak{a}$ *be a* $\mathfrak{g}$*-ideal. If* $L \supset M$ *and* $N(M) \supset \mathfrak{a}N(L)$, *then* $M \supset \mathfrak{a}L$.

PROOF. As $\mathfrak{a}N(L) \subset N(M) \subset N(L)$, $\mathfrak{a}$ is an integral ideal. Put $K = M + \mathfrak{a}L$. Then K is a $\mathfrak{g}$-lattice in V with the same order as L. We have $f(K, K) \subset f(M, M) + \mathfrak{a}f(M, L) + \mathfrak{a}f(L, M) + \mathfrak{a}^2 f(L, L) \subset N(M)$, so that $N(K) = N(M)$. By the maximality of M, we must have $K = M$, and hence $\mathfrak{a}L \subset M$.

PROPOSITION 2.8. *Let* M *be a normal* $\mathfrak{g}$*-lattice in* V. *Then there exists a maximal lattice* L, *with the same order as* M, *such that* $N(L) = N(M)$ *and* $L \supset M$.

PROOF. Let $\mathfrak{o}$ be the order of M. Take a base $\{x_1, \cdots, x_n\}$ of V over A such that $x_i \in M$ for every i. Put $K = \{y \mid f(y, x_i) \in N(M) \text{ for every } i\}$. It is easy to see that K is a $\mathfrak{g}$-lattice in V with order $\mathfrak{o}$. Now, let L be a $\mathfrak{g}$-lattice in V with order $\mathfrak{o}$ such that $L \supset M$ and $N(L) = N(M)$. If $y \in L$, we have $f(y, x_i) \in N(L) = N(M)$, so that $y \in K$. Hence L is contained in K. As K is a $\mathfrak{g}$-lattice, the ascending chain condition holds for the $\mathfrak{g}$-lattices contained in K. Therefore, we can find a maximal one among the lattices containing M, with order $\mathfrak{o}$ and with norm $N(M)$. This proves our proposition.

2.4. The relation between alternating form and Q-hermitian form. We now consider the case $A = M_2(F)$ for an arbitrary field F. Let e_{ij} $(i = 1, 2;\ j = 1, 2)$ be the matrix units of A. We note that $e_{11}' = e_{22}$, $e_{12}' = -e_{12}$, $e_{21}' = -e_{21}$. Let V be an A-space of dimension n and f a Q-hermitian form on V. Put $W_i = e_{ii}V$ for $i = 1, 2$. Then W_i is a vector space over F of dimension n for $i = 1, 2$; and V is the direct sum of W_1 and W_2. If $x, y \in W_1$, we have $f(x, y) = f(e_{11}x, e_{11}y) = e_{11}f(x, y)e_{22} \in Fe_{12}$. Hence we can define an F-bilinear mapping g of $W_1 \times W_1$ into F by

$$f(x, y) = g(x, y)e_{12}. \tag{2}$$

As $e_{12}' = -e_{12}$, we have $g(y, x)e_{12} = f(y, x) = f(x, y)' = -g(x, y)e_{12}$, so that g is an alternating form on W_1. If $\sigma \in E(V, A)$, we have $W_1\sigma \subset W_1$; so the restriction of σ to W_1 gives rise to an element of $E(W_1)$, which we denote by σ_1.

PROPOSITION 2.9. *Notation being as above, the mapping* $\sigma \to \sigma_1$ *gives an isomorphism of* $E(V, A)$ *and* $GL(V, A)$ *onto* $E(W_1)$ *and* $GL(W_1)$, *respectively. Moreover, suppose that* f *is non-degenerate. Then* g *is non-degenerate; and* $\sigma \to \sigma_1$

gives an isomorphism of $G(V,f)$ *and* $G^0(V,f)$ *onto* $G(W_1,g)$ *and* $G^0(W_1,g)$, *respectively; and further we have* $N(\sigma)=N(\sigma_1)$ *for* $\sigma\in G(V,f)$.

This can be proved in an almost straightforward way. By Proposition 2.1, there exists a base $\{x_1,\cdots,x_n\}$ of V over A such that $f(x_i,x_j)=\delta_{ij}$. Using matricial representation with respect to this base, the mapping $\sigma\to\sigma_1$ is given explicitly as follows. First note that $\{e_{11}x_i, e_{12}x_i\ (1\leqq i\leqq n)\}$ is a base of W_1 over F. Let σ be an element of $E(V,A)$ and $S=(s_{ij})$ the element of $M_n(A)$ determined by (1) of § 2.2. Put $e_{11}x_i=y_i$, $e_{12}x_i=z_i$ and $s_{ij}=\begin{pmatrix} a_{ij} & b_{ij} \\ c_{ij} & d_{ij}\end{pmatrix}$ with a_{ij}, b_{ij}, c_{ij}, d_{ij} in F. Then we have $y_i\sigma=\sum_{j=1}^{n}a_{ij}y_j+\sum_{j=1}^{n}b_{ij}z_j$, $z_i\sigma=\sum_{j=1}^{n}c_{ij}y_j+\sum_{j=1}^{n}d_{ij}z_j$. Now define an isomorphism ι of $M_n(A)$ onto $M_{2n}(F)$ by $\iota(s_{ij})=\begin{pmatrix} (a_{ij}) & (b_{ij}) \\ (c_{ij}) & (d_{ij})\end{pmatrix}$. Then σ_1 is represented by $\iota(S)$ with respect to the base $\{y_i,z_i\}$. As $f(x_i,x_j)=\delta_{ij}$, we get $g(y_i,y_j)=g(z_i,z_j)=0$, $g(y_i,z_j)=-\delta_{ij}$. Put $J=\begin{pmatrix} 0 & 1_n \\ -1_n & 0\end{pmatrix}$. Then we have $\iota(S')=\begin{pmatrix} {}^t(d_{ij}) & -{}^t(b_{ij}) \\ -{}^t(c_{ij}) & {}^t(a_{ij})\end{pmatrix}=J\cdot{}^t\iota(S)J^{-1}$. Therefore, if $SS'=\alpha 1_n$ with $\alpha\in F$, we have $\iota(S)J\cdot{}^t\iota(S)=\alpha J$. This will give a 'non-intrinsic' proof of Proposition 2.8.

2.5. Paraphrase of the result of § 1. The notation $A=M_2(F)$, V, f, W_i, g being as in § 2.4, suppose that F is the quotient field of a Dedekind domain $\mathfrak{g}$. For every $\mathfrak{g}$-ideal $\mathfrak{c}$, put $\mathfrak{o}(\mathfrak{c})=\mathfrak{g}e_{11}+\mathfrak{c}e_{12}+\mathfrak{c}^{-1}e_{21}+\mathfrak{g}e_{22}=\begin{pmatrix} \mathfrak{g} & \mathfrak{c} \\ \mathfrak{c}^{-1} & \mathfrak{g}\end{pmatrix}$. Then, $\mathfrak{o}(\mathfrak{c})$ is a maximal order in A; and for every maximal order $\mathfrak{o}$ in A, there exist an element a of A and a $\mathfrak{g}$-ideal $\mathfrak{c}$ such that $a\mathfrak{o}a^{-1}=\mathfrak{o}(\mathfrak{c})$. Fix a $\mathfrak{g}$-ideal $\mathfrak{c}$ and put $\mathfrak{o}=\mathfrak{o}(\mathfrak{c})$. Let L be a $\mathfrak{g}$-lattice in V with the order $\mathfrak{o}$. Put $e_{ii}L=M_i$. Then we have $M_i=L\cap W_i$, $L=M_1+M_2$; and M_i is a $\mathfrak{g}$-lattice in W_i. Further we have $M_1=\mathfrak{c}e_{12}M_2$, $M_2=\mathfrak{c}^{-1}e_{21}M_1$. Now, by Proposition 1.3, there exist $\mathfrak{g}$-ideals $\mathfrak{a}_1,\cdots,\mathfrak{a}_n$ and a base $\{y_i,z_i\}$ of W_1 over F with the properties of that proposition for $M=M_1$. Then we have

$$M_2=\mathfrak{c}^{-1}e_{21}y_1+\cdots+\mathfrak{c}^{-1}e_{21}y_n+\mathfrak{c}^{-1}\mathfrak{a}_1e_{21}z_1+\cdots+\mathfrak{c}^{-1}\mathfrak{a}_ne_{21}z_n\,.$$

Put $x_i=y_i-e_{21}z_i$, $\mathfrak{b}_i=\mathfrak{g}e_{11}+\mathfrak{c}\mathfrak{a}_ie_{12}+\mathfrak{c}^{-1}e_{21}+\mathfrak{a}_ie_{22}=\begin{pmatrix} \mathfrak{g} & \mathfrak{a}_i \\ \mathfrak{c}^{-1} & \mathfrak{c}^{-1}\mathfrak{a}_i\end{pmatrix}$ for $1\leqq i\leqq n$. Then the $\mathfrak{b}_i$ are left $\mathfrak{o}$-ideals; and we see easily $L=\mathfrak{b}_1x_1+\cdots+\mathfrak{b}_nx_n$, $\mathfrak{b}_1\supset\cdots\supset\mathfrak{b}_n$, $f(x_i,x_j)=\delta_{ij}$. Further we have $N(L)=N(\mathfrak{b}_1)\mathfrak{o}$, $N(\mathfrak{b}_1)=\mathfrak{c}^{-1}\mathfrak{a}_1=\mathfrak{c}^{-1}N_{\mathfrak{g}}(M_1)$. Therefore, if L is maximal, we must have $\mathfrak{b}_1=\cdots=\mathfrak{b}_n$, and hence $\mathfrak{a}_1=\cdots=\mathfrak{a}_n$, so that M_1 is maximal with respect to g. Thus we obtain

PROPOSITION 2.10. *Let* F *be the quotient field of a Dedekind domain* $\mathfrak{g}$, *and* $A=M_2(F)$. *Let* V *be an* A*-space of dimension* n *and* f *be a non-degenerate* Q*-hermitian form on* V. *Let* L *be a normal lattice in* V *and* $\mathfrak{o}$ *the order of* L. *Then there exist left* $\mathfrak{o}$*-ideals* $\mathfrak{b}_1,\cdots,\mathfrak{b}_n$ *and a base* $\{x_1,\cdots,x_n\}$ *of* V *over* A *such*

that

$$L=\mathfrak{b}_1x_1+\cdots+\mathfrak{b}_nx_n,\qquad \mathfrak{b}_1\supset\cdots\supset\mathfrak{b}_n,$$
$$f(x_i,x_j)=\delta_{ij};$$

and we have $N(L)=N(\mathfrak{b}_1)\mathfrak{o}$. *Moreover, if* L *is maximal,* $\mathfrak{b}_1=\cdots=\mathfrak{b}_n$.

PROPOSITION 2.11. *Notation being as in Proposition* 2.10, *let* L_1 *and* L_2 *be maximal lattices in* V *with the same order* $\mathfrak{o}$. *If* $L_1\sigma=L_2$ *for an element* σ *of* $G(V,f)$, *then* $\alpha N(L_1)=N(L_2)$ *for an element* α *of* F. *Conversely, if* $\alpha N(L_1)=N(L_2)$ *with* $\alpha\in F$, *we can find an element* σ *of* $G(V,f)$ *such that* $L_1\sigma=L_2$, $N(\sigma)=\alpha$.

PROOF. The first assertion is obvious. Now suppose that $N(L_2)=\alpha N(L_1)$ with $\alpha\in F$. We may assume that $\mathfrak{o}=\mathfrak{o}(\mathfrak{c})$ for a $\mathfrak{g}$-ideal $\mathfrak{c}$. Put $M_i^1=e_{ii}L_1$, $M_i^2=e_{ii}L_2$ for $i=1,2$. By the above consideration, M_1^1 and M_1^2 are maximal lattices in W_1, and $N_g(M_1^1)\alpha=N_g(M_1^2)$. By Proposition 1.4 and its proof, there exists an element σ_1 of $G(W_1,g)$ such that $M_1^1\sigma_1=M_1^2$, $N(\sigma_1)=\alpha$. Let σ be an element of $G(V,f)$ corresponding to σ_1 by the mapping of Proposition 2.9. We get then $N(\sigma)=\alpha$, and $L_1\sigma=L_2$, since $L_1=\mathfrak{o}M_1^1$, $L_2=\mathfrak{o}M_1^2$. This completes our proof. We can also derive our proposition more directly from Proposition 2.10.

PROPOSITION 2.12. *Notation being as in Proposition* 2.10, *suppose that* $\mathfrak{g}$ *is a principal ideal domain. Put* $\mathfrak{o}=M_2(\mathfrak{g})$. *Let* L *and* M *be maximal lattices in* V *with the order* $\mathfrak{o}$. *Let* η *and* α *be elements of* F *such that* $N(L)=\eta\mathfrak{o}$ *and* $N(M)=\alpha N(L)$. *Then there exist a base* $\{x_1,\cdots,x_n\}$ *of* V *over* A *and elements* $a_1,\cdots,a_n$, $b_1,\cdots,b_n$ *of* F *such that*

$$f(x_i,x_j)=\eta\delta_{ij},$$
$$L=\mathfrak{o}x_1+\cdots+\mathfrak{o}x_n,$$
$$M=\mathfrak{o}e_1x_1+\cdots+\mathfrak{o}e_nx_n,\qquad e_i=\begin{pmatrix}a_i&0\\0&b_i\end{pmatrix}\qquad(0\leqq i\leqq n),$$
$$\mathfrak{g}a_1\supset\cdots\supset\mathfrak{g}a_n\supset\mathfrak{g}b_n\supset\cdots\supset\mathfrak{g}b_1,$$
$$\alpha=a_1b_1=\cdots=a_nb_n.$$

PROOF. Put $L_1=e_{11}L$, $M_1=e_{11}M$. Then L_1 and M_1 are maximal lattices in W_1 with respect to g, and $N(L_1)=\mathfrak{g}\eta$, $N(M_1)=\mathfrak{g}\alpha\eta$. Applying Proposition 1.5 to this $\{L_1,M_1,\alpha\}$, we obtain $\{y_i,z_i\}$ and $\{a_i,b_i\}$ with the properties of that proposition for L_1 and M_1. Put $x_i=y_i-e_{21}\eta z_i$. Then we can easily verify that $f(x_i,x_j)=\eta\delta_{ij}$, $L=\mathfrak{o}x_1+\cdots+\mathfrak{o}x_n$, $M=\mathfrak{o}e_1x_1+\cdots+\mathfrak{o}e_nx_n$ with $e_i=\begin{pmatrix}a_i&0\\0&b_i\end{pmatrix}$. This proves our proposition.

Notation being as in Proposition 2.12, we call $\{\mathfrak{g}a_1,\cdots,\mathfrak{g}a_n,\mathfrak{g}b_1,\cdots,\mathfrak{g}b_n\}$ *the set of elementary divisors of* M *relative to* L and denote it by $\{L:M\}$. We get an assertion for $\{V,f\}$ which is a paraphrase of Proposition 1.6. Instead of stating it, we give the following proposition.

PROPOSITION 2.13. *Notation and assumption being as in Proposition* 2.12,

let L, M, K be maximal lattices in V with the order $\mathfrak{o}$. Then there exists an element σ of $G^0(V,f)$ such that $L\sigma=L$ and $M\sigma=K$, if and only if $\{L:M\}=\{L:K\}$.

PROOF. The 'only if' part is clear. Put $N(L)=\mathfrak{o}\eta$, $N(M)=\mathfrak{o}\alpha\eta$, $N(K)=\mathfrak{o}\beta\eta$ with $\alpha,\beta,\eta\in F$. By Proposition 2.12, we get a base $\{x_i\}$ of V over A and a set of elements $\{a_i,b_i\}$ of F for M with the properties of that proposition, and a base $\{u_i\}$ of V over A and a set of elements $\{c_i,d_i\}$ of F with the corresponding properties for K. If $\{L:M\}=\{L:K\}$, we have $\mathfrak{g}a_i=\mathfrak{g}c_i$, $\mathfrak{g}b_i=\mathfrak{g}d_i$, so that $\mathfrak{g}\alpha=\mathfrak{g}\beta$. Hence we may put $\alpha=\beta$. We have then $a_ib_i=c_id_i$. Let ε_i, for each i, be a unit of $\mathfrak{g}$ such that $\varepsilon_ia_i=c_i$; then we have $\varepsilon_i^{-1}b_i=d_i$. Define an element σ of $E(V,A)$ by $x_i\sigma=\begin{pmatrix}\varepsilon_i & 0\\ 0 & \varepsilon_i^{-1}\end{pmatrix}u_i$. Then we see easily $\sigma\in G^0(V,f)$, $L\sigma=L$, $M\sigma=K$. This proves the 'if' part.

REMARK. Notation being as in Proposition 2.13, suppose that $L\supset M$, $L\supset K$. Then the following three conditions are equivalent to each other.

i) $\{L:M\}=\{L:K\}$.

ii) L/M and L/K are isomorphic as $\mathfrak{g}$-modules.

iii) L/M and L/K are isomorphic as $\mathfrak{o}$-modules.

§ 3. Local theory of Q-hermitian forms.

3.1. Quaternion algebras over local fields. By a $\mathfrak{p}$-*adic number field*, we understand a finite extension of the p-adic number field, for any prime number p. In this § 3, $F_\mathfrak{p}$, $\mathfrak{g}_\mathfrak{p}$, $\mathfrak{p}$ denote respectively a $\mathfrak{p}$-adic number field, the ring of $\mathfrak{p}$-integers in $F_\mathfrak{p}$, the maximal ideal of $\mathfrak{g}_\mathfrak{p}$. It is well-known that there exist, up to isomorphism, only two quaternion algebras over $F_\mathfrak{p}$, the matric algebra $M_2(F_\mathfrak{p})$ and a division algebra. The latter is written as $(B,S,\pi)=B+Bu$ in the usual notation of cyclic algebra, where B is the unique unramified quadratic extension of $F_\mathfrak{p}$, S is the Frobenius automorphism of B over $F_\mathfrak{p}$, π is a prime element of $F_\mathfrak{p}$, and $u\beta u^{-1}=\beta^S$ for $\beta\in B$, $u^2=\pi$. We denote this division quaternion algebra over $F_\mathfrak{p}$ by $D_\mathfrak{p}$.

For every maximal order $\mathfrak{o}_\mathfrak{p}$ in $M_2(F_\mathfrak{p})$, there exists an element w such that $w\mathfrak{o}_\mathfrak{p}w^{-1}=M_2(\mathfrak{g}_\mathfrak{p})$. Every one-sided $\mathfrak{o}_\mathfrak{p}$-ideal is principal. Every two-sided $\mathfrak{o}_\mathfrak{p}$-ideal $\mathfrak{a}_\mathfrak{p}$ is written in the form $\mathfrak{a}_\mathfrak{p}=\mathfrak{p}^\nu\mathfrak{o}_\mathfrak{p}$ with $\nu\in\boldsymbol{Z}$, and conversely. Further $\mathfrak{D}(\mathfrak{o}_\mathfrak{p}/\mathfrak{g}_\mathfrak{p})=\mathfrak{o}_\mathfrak{p}$. As for $D_\mathfrak{p}$, it has only one maximal order $\mathfrak{o}_\mathfrak{p}=\{x\in D_\mathfrak{p}\mid N(x)\in\mathfrak{g}_\mathfrak{p}\}$; and every one-sided $\mathfrak{o}_\mathfrak{p}$-ideal is principal and equal to a power of the maximal ideal $\mathfrak{P}$, so that it is a two-sided $\mathfrak{o}_\mathfrak{p}$-ideal. We have $\mathfrak{P}^2=\mathfrak{p}\mathfrak{o}_\mathfrak{p}$, $\mathfrak{P}=\mathfrak{D}(\mathfrak{o}_\mathfrak{p}/\mathfrak{g}_\mathfrak{p})$.

PROPOSITION 3.1. *Let $A_\mathfrak{p}$ be a quaternion algebra over $F_\mathfrak{p}$ and $\mathfrak{o}_\mathfrak{p}$ a maximal order in $A_\mathfrak{p}$. For every two-sided $\mathfrak{o}_\mathfrak{p}$-ideal $\mathfrak{a}_\mathfrak{p}$, we have* $\mathrm{Tr}(\mathfrak{a}_\mathfrak{p})=\mathfrak{a}_\mathfrak{p}\cap F_\mathfrak{p}$.

PROOF. This is clear if $A_\mathfrak{p}=M_2(F_\mathfrak{p})$. Therefore suppose that $A_\mathfrak{p}=D_\mathfrak{p}$. Then every $\mathfrak{o}_\mathfrak{p}$-ideal $\mathfrak{a}_\mathfrak{p}$ is written in the form $\mathfrak{a}_\mathfrak{p}=\mathfrak{P}^e\cdot(\mathfrak{a}_\mathfrak{p}\cap F_\mathfrak{p})$ with $e=0$ or

-1. We have $\mathrm{Tr}(\mathfrak{a}_\mathfrak{p})=\mathrm{Tr}(\mathfrak{P}^e)\cdot(\mathfrak{a}_\mathfrak{p}\cap F_\mathfrak{p})$ and $\mathrm{Tr}(\mathfrak{o}_\mathfrak{p})\subset\mathrm{Tr}(\mathfrak{P}^e)\subset\mathrm{Tr}(\mathfrak{P}^{-1})\subset\mathfrak{g}_\mathfrak{p}$. Therefore, it is sufficient to prove $\mathrm{Tr}(\mathfrak{o}_\mathfrak{p})=\mathfrak{g}_\mathfrak{p}$. As $\mathrm{Tr}(\mathfrak{o}_\mathfrak{p})$ is an integral $\mathfrak{g}_\mathfrak{p}$-ideal, there exists an integer $\nu\geqq 0$ such that $\mathrm{Tr}(\mathfrak{o}_\mathfrak{p})=\mathfrak{p}^\nu\mathfrak{g}_\mathfrak{p}$. We get then $\mathrm{Tr}(\mathfrak{p}^{-\nu}\mathfrak{o}_\mathfrak{p})\subset\mathfrak{g}_\mathfrak{p}$, so that $\mathfrak{p}^{-\nu}\mathfrak{o}_\mathfrak{p}\subset\mathfrak{D}(\mathfrak{o}_\mathfrak{p}/\mathfrak{g}_\mathfrak{p})^{-1}=\mathfrak{P}^{-1}$, which implies $\nu=0$, since $\mathfrak{P}^2=\mathfrak{p}\mathfrak{o}_\mathfrak{p}$. This completes our proof.

PROPOSITION 3.2. *$A_\mathfrak{p}$ and $\mathfrak{o}_\mathfrak{p}$ being as in Proposition* 3.1, *let β be a non-zero element of $\mathfrak{g}_\mathfrak{p}$ and a an element of $\mathfrak{o}_\mathfrak{p}$ such that $\beta^{-1}N(a)\equiv 1 \bmod \mathfrak{p}^\lambda$ where λ is a positive integer. Then there exists an element b of $\mathfrak{o}_\mathfrak{p}$ such that $N(b)=\beta$, $b\equiv a \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$.*

PROOF. We first consider the case $A_\mathfrak{p}=M_2(F_\mathfrak{p})$. We may then put $\mathfrak{o}_\mathfrak{p}=M_2(\mathfrak{g}_\mathfrak{p})$. Let π be a prime element of F. We can find elements x, y of $\mathfrak{o}_\mathfrak{p}$ such that $N(x)=N(y)=1$, $xay=\begin{pmatrix}\pi^\mu\varepsilon & 0\\ 0 & \pi^\nu\eta\end{pmatrix}$ where $0\leqq\mu\leqq\nu$, and ε,η are units of $\mathfrak{g}_\mathfrak{p}$. As $\beta^{-1}N(a)\equiv 1 \bmod \mathfrak{p}^\lambda$, we have $\beta=\pi^{\mu+\nu}\delta$ with a unit δ of $\mathfrak{g}_\mathfrak{p}$, and $\delta\equiv\varepsilon\eta \bmod \mathfrak{p}^\lambda$. Put $b=x^{-1}\begin{pmatrix}\pi^\mu\varepsilon & 0\\ 0 & \pi^\nu\varepsilon^{-1}\delta\end{pmatrix}y^{-1}$. As $\varepsilon^{-1}\delta\equiv\eta \bmod \mathfrak{p}^\lambda$, and as x^{-1}, $y^{-1}\in\mathfrak{o}_\mathfrak{p}$, we have $b\equiv a \bmod \mathfrak{p}^\lambda$, and clearly $N(b)=\pi^{\mu+\nu}\delta=\beta$. This proves our assertion for $A_\mathfrak{p}=M_2(F_\mathfrak{p})$. Now put $A_\mathfrak{p}=D_\mathfrak{p}$. Let Π be a prime element in $\mathfrak{o}_\mathfrak{p}$; put $N(\Pi)=\pi$; then π is a prime element in $\mathfrak{g}_\mathfrak{p}$. Put $a=\Pi^\nu e$ with a unit e of $\mathfrak{o}_\mathfrak{p}$. As $\beta^{-1}N(a)\equiv 1 \bmod \mathfrak{p}^\lambda$, we have $\beta=\pi^\nu\varepsilon$ with a unit ε of $\mathfrak{g}_\mathfrak{p}$, and $N(e)\equiv\varepsilon \bmod \mathfrak{p}^\lambda$. Now we construct inductively a sequence $\{e_0, e_1, \cdots, e_n, \cdots\}$ of units of $\mathfrak{o}_\mathfrak{p}$ such that $e_0=e$, $N(e_n)\equiv\varepsilon \bmod \mathfrak{p}^{\lambda+n}$, $e_{n+1}\equiv e_n \bmod \mathfrak{p}^{\lambda+n}\mathfrak{o}_\mathfrak{p}$. Assume that e_n is already defined. Put $\varepsilon-N(e_n)=\pi^{\lambda+n}\cdot\gamma$ with $\gamma\in\mathfrak{g}_\mathfrak{p}$. By Proposition 3.1, we have $\mathrm{Tr}(e_n'\mathfrak{o}_\mathfrak{p})=\mathrm{Tr}(\mathfrak{o}_\mathfrak{p})=\mathfrak{g}_\mathfrak{p}$, so that there exists an element d of $\mathfrak{o}_\mathfrak{p}$ such that $\mathrm{Tr}(e_n'd)=\gamma$. Put $e_{n+1}=e_n+\pi^{\lambda+n}d$. Then we have $N(e_{n+1})=N(e_n)+\pi^{\lambda+n}\mathrm{Tr}(e_n'd)+\pi^{2(\lambda+n)}N(d)\equiv\varepsilon \bmod \mathfrak{p}^{\lambda+n+1}$. We get thus a sequence $\{e_n\}$ with the required property. As $e_{n+1}\equiv e_n \bmod \mathfrak{p}^{\lambda+n}\mathfrak{o}_\mathfrak{p}$, this converges to a unit h of $\mathfrak{o}_\mathfrak{p}$, for which we have $N(h)=\varepsilon$, $h\equiv e \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$. Put $b=\Pi^\nu h$. Then we have $N(b)=\beta$, $b\equiv a \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$. This completes our proof.

PROPOSITION 3.3. *$A_\mathfrak{p}$ and $\mathfrak{o}_\mathfrak{p}$ being as in Proposition* 3.1, *let ξ be an element of $\mathfrak{g}_\mathfrak{p}$. Then there exists an element x of $\mathfrak{o}_\mathfrak{p}$ such that $N(x)=\xi$. In particular, $A_\mathfrak{p}$ satisfies the condition* (D) *of Proposition* 2.1.

PROOF. If $A_\mathfrak{p}=M_2(F_\mathfrak{p})$, we may put $\mathfrak{o}_\mathfrak{p}=M_2(\mathfrak{g}_\mathfrak{p})$, so that our assertion is obvious. If $A_\mathfrak{p}=D_\mathfrak{p}$, it is well-known that any quadratic extension of $F_\mathfrak{p}$ is isomorphic to a subfield of $D_\mathfrak{p}$, over $F_\mathfrak{p}$. Hence, for every $\xi\in F_\mathfrak{p}$, there exists an element x of $D_\mathfrak{p}$ such that $N(x)=\xi$. If $\xi\in\mathfrak{g}_\mathfrak{p}$, we have $x\in\mathfrak{o}_\mathfrak{p}$ automatically. This completes our proof.

3.2. Canonical bases of maximal lattices. Let $A_\mathfrak{p}$ be a quaternion algebra over $F_\mathfrak{p}$, and $V_\mathfrak{p}$ be an $A_\mathfrak{p}$-space of dimension n. Take a non-degenerate Q-hermitian form f on $V_\mathfrak{p}$. By Proposition 3.3 and Proposition 2.1, we see that, for every regular element $H=(h_{ij})$ of $M_n(A_\mathfrak{p})$ such that $H'=H$, there exists

a base $\{x_1, \cdots, x_n\}$ of $V_\mathfrak{p}$ over $A_\mathfrak{p}$ for which $f(x_i, x_j) = h_{ij}$. In particular we get

PROPOSITION 3.4. *$V_\mathfrak{p}$ has a base $\{x_1, \cdots, x_m, y_1, \cdots, y_m, z\}$ over $A_\mathfrak{p}$ such that*

$$f(x_i, x_j) = f(y_i, y_j) = f(x_i, z) = f(y_i, z) = 0,$$
$$f(x_i, y_j) = a\delta_{ij}, \qquad f(z, z) = \beta \qquad (1 \leqq i \leqq m,\ 1 \leqq j \leqq m),$$

where a is a regular element of $A_\mathfrak{p}$, β is a non-zero element of $F_\mathfrak{p}$, the last member z (and hence β) occurring only in the case where n is odd.

We call a base $\{x_1, \cdots, x_m, y_1, \cdots, y_m, z\}$ of $V_\mathfrak{p}$ over $A_\mathfrak{p}$ with the property of the above proposition a *canonical base* of $V_\mathfrak{p}$. Proposition 3.4 implies that, if $n > 1$, $V_\mathfrak{p}$ contains an element x such that $f(x, x) = 0$, $A_\mathfrak{p}x \cong A_\mathfrak{p}$.

Now we want to study the arithmetic of maximal lattices in $V_\mathfrak{p}$. If $A_\mathfrak{p} = M_2(F_\mathfrak{p})$, we can apply the theory of § 2.5 and § 1 to the present case, since $\mathfrak{g}_\mathfrak{p}$ is a principal ideal domain ; and this is sufficient for our later use. Therefore, we have only to consider the case $A_\mathfrak{p} = D_\mathfrak{p}$. From now on, until the end of this § 3.2, $V_\mathfrak{p}$ is a $D_\mathfrak{p}$-space of dimension n, and $\mathfrak{o}_\mathfrak{p}$ denotes the unique maximal order in $D_\mathfrak{p}$.

PROPOSITION 3.5. *Let L be a maximal lattice in $V_\mathfrak{p}$. Let a be an element of $D_\mathfrak{p}$ such that $N(L) = \mathfrak{o}_\mathfrak{p}a$, and β be an element of $F_\mathfrak{p}$ such that $N(L) \cap F_\mathfrak{p} = \mathfrak{g}_\mathfrak{p}\beta$. Then there exists a canonical base $\{x_1, \cdots, x_m, y_1, \cdots, y_m, z\}$ of $V_\mathfrak{p}$ such that*

$$L = \mathfrak{o}_\mathfrak{p}x_1 + \mathfrak{o}_\mathfrak{p}y_1 + \cdots + \mathfrak{o}_\mathfrak{p}x_m + \mathfrak{o}_\mathfrak{p}y_m + \mathfrak{o}_\mathfrak{p}z, \tag{3}$$

$$f(x_i, y_j) = a\delta_{ij}, \qquad f(z, z) = \beta, \tag{4}$$

where the term $\mathfrak{o}_\mathfrak{p}z$ and β occur only when n is odd. Conversely, let a be a regular element of $D_\mathfrak{p}$ and β an element of $F_\mathfrak{p}$ such that $(\mathfrak{o}_\mathfrak{p}a) \cap F_\mathfrak{p} = \mathfrak{g}_\mathfrak{p}\beta$. Let $\{x_i, y_i, z\}$ be a canonical base of $V_\mathfrak{p}$ satisfying (4). *Then the lattice L defined by* (3) *is normal, maximal and $N(L) = \mathfrak{o}_\mathfrak{p}a$ or $\mathfrak{o}_\mathfrak{p}\beta$ according as $n > 1$ or $n = 1$.*

PROPOSITION 3.6. *Let L be a $\mathfrak{g}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$. Let $\mathfrak{b}$ be an $\mathfrak{o}_\mathfrak{p}$-ideal such that $N(L) \subset \mathfrak{b}$. Then there exists a maximal lattice M such that $M \supset L$, $N(M) = \mathfrak{b}$ or $N(M) = \mathfrak{o}_\mathfrak{p} \cdot (\mathfrak{b} \cap F_\mathfrak{p})$ according as $n > 1$ or $n = 1$.*

We first show that, if Proposition 3.5 is true for n, then Proposition 3.6 is true for n. Let the notation be as in Proposition 3.6. By Proposition 2.8, we may assume that L is maximal. Put $N(L) = \mathfrak{o}_\mathfrak{p}a$, $N(L) \cap F_\mathfrak{p} = \mathfrak{g}_\mathfrak{p}\beta$ with $a \in D_\mathfrak{p}$, $\beta \in F_\mathfrak{p}$. If $n = 1$, we put $a = \beta$. By Proposition 3.5, there exists a canonical base $\{x_i, y_i, z\}$ of $V_\mathfrak{p}$ satisfying (3) and (4). Put $\mathfrak{b} = \mathfrak{o}_\mathfrak{p}b$, $\mathfrak{b} \cap F_\mathfrak{p} = \mathfrak{g}_\mathfrak{p}\gamma$, $a = cb$, $\beta = \varepsilon\gamma$. Then $c \in \mathfrak{o}_\mathfrak{p}$, $\varepsilon \in \mathfrak{g}_\mathfrak{p}$. By Proposition 3.3, we can find an element e of $\mathfrak{o}_\mathfrak{p}$ such that $N(e) = \varepsilon$. Put $M = \sum_{i=1}^{m} \mathfrak{o}_\mathfrak{p}c^{-1}x_i + \sum_{i=1}^{m} \mathfrak{o}_\mathfrak{p}y_i + \mathfrak{o}_\mathfrak{p}e^{-1}z$. As $f(c^{-1}x_i, y_j) = b\delta_{ij}$ and $f(e^{-1}z, e^{-1}z) = \gamma$, we see, from Proposition 3.5, that M is a maximal lattice and $N(M) = \mathfrak{b}$ or $\mathfrak{o}_\mathfrak{p} \cdot (\mathfrak{b} \cap F_\mathfrak{p})$ according as $n > 1$ or $n = 1$. By our construction of M, we have $M \supset L$. This proves Proposition 3.6.

Now we want to prove the converse part of Proposition 3.5. Define L as

in Proposition 3.5. It is clear that L has $\mathfrak{o}_\mathfrak{p}$ as its order and $N(L)=\mathfrak{o}_\mathfrak{p}a$ or $\mathfrak{o}_\mathfrak{p}\beta$ according as $n>1$ or $n=1$. Let M be a lattice with order $\mathfrak{o}_\mathfrak{p}$ such that $M\supset L$, $N(M)=N(L)$. Let $u=\sum_{i=1}^{m}(c_ix_i+d_iy_i)+ez$, with $c_i, d_i, e\in D_\mathfrak{p}$, be an element of M, the term ez occurring only when n is odd. As the x_i and y_i are contained in M, we have

$$d_ia'=f(u, x_i)\in N(M)=\mathfrak{o}_\mathfrak{p}a\,,\qquad ac_i=f(u, y_i)\in N(M)=\mathfrak{o}_\mathfrak{p}a\,.$$

This implies $d_i\in\mathfrak{o}_\mathfrak{p}$, $c_i\in\mathfrak{o}_\mathfrak{p}$. It follows that $ez=u-\sum_{i=1}^{m}(c_ix_i+d_iy_i)\in M$. Hence we have $N(e)\beta=f(ez, ez)\in N(M)\cap F_\mathfrak{p}=\mathfrak{g}_\mathfrak{p}\beta$, so that $N(e)\in\mathfrak{g}_\mathfrak{p}$, and hence $e\in\mathfrak{o}_\mathfrak{p}$. Therefore u must be contained in L; so we have $M=L$; this proves the maximality of L.

Let us prove the direct part of Proposition 3.5 by induction on n. If $n=1$, take a base x of $V_\mathfrak{p}$ over $D_\mathfrak{p}$. Then L is written in the form $L=\mathfrak{a}x$ with an $\mathfrak{o}_\mathfrak{p}$-ideal $\mathfrak{a}$. We have $N(L)=\mathfrak{o}_\mathfrak{p}N(\mathfrak{a})f(x, x)$, so that $N(\mathfrak{a})f(x, x)=\mathfrak{g}_\mathfrak{p}\beta$. By Proposition 3.3, there exists an element b of $D_\mathfrak{p}$ such that $N(b)=\beta f(x, x)^{-1}$. Put $z=bx$. Then $f(z, z)=\beta$, $N(b)\mathfrak{g}_\mathfrak{p}=N(\mathfrak{a})$ and hence $\mathfrak{o}_\mathfrak{p}b=\mathfrak{a}$. We have therefore $L=\mathfrak{o}_\mathfrak{p}z$. This proves the case $n=1$. Now suppose that $n>1$. By the remark after Proposition 3.4, $V_\mathfrak{p}$ contains an element $x\neq 0$ such that $f(x, x)=0$. Put $\mathfrak{c}=\{c\in D_\mathfrak{p}\mid cx\in L\}$. Obviously, $\mathfrak{c}$ is an $\mathfrak{o}_\mathfrak{p}$-ideal, so it is written in the form $\mathfrak{c}=\mathfrak{o}_\mathfrak{p}c_0$. Put $c_0x=x_1$. Then we see that

$$\mathfrak{o}_\mathfrak{p}=\{c\in D_\mathfrak{p}\mid cx_1\in L\} \tag{5}$$

and $f(x_1, x_1)=0$. Put $\mathfrak{b}=f(x_1, L)$. It is clear that $\mathfrak{b}$ is an $\mathfrak{o}_\mathfrak{p}$-ideal. If $b\in N(L)\mathfrak{b}^{-1}$ and $u\in L$, we have $f(bx_1, u)=bf(x_1, u)\in\mathfrak{b}N(L)\mathfrak{b}^{-1}=N(L)$. Therefore, if b, $c\in N(L)\mathfrak{b}^{-1}$ and u, $v\in L$, we have

$$f(bx_1+u, cx_1+v)=f(bx_1, v)+f(u, cx_1)+f(u, v)\in N(L)\,. \tag{6}$$

Put $M=N(L)\mathfrak{b}^{-1}x_1+L$. The relation (6) shows that $N(M)=N(L)$. As L is maximal, we must have $L=M$, so that $N(L)\mathfrak{b}^{-1}x_1\subset L$. By (5), we have $N(L)\mathfrak{b}^{-1}\subset\mathfrak{o}_\mathfrak{p}$, so that $N(L)\subset\mathfrak{b}$. As $\mathfrak{b}=f(x_1, L)\subset N(L)$, we must have $\mathfrak{b}=N(L)=\mathfrak{o}_\mathfrak{p}a$. Hence there exists an element y of L such that $f(x_1, y)=a$. By Proposition 3.1, we have $\mathrm{Tr}(\mathfrak{o}_\mathfrak{p}a)=N(L)\cap F_\mathfrak{p}\ni -f(y, y)$. Therefore we can find an element t of $\mathfrak{o}_\mathfrak{p}$ such that $\mathrm{Tr}(ta)=-f(y, y)$. Put $y_1=tx_1+y$. Then $y_1\in L$, and we have $f(x_1, y)=a$, $f(y_1, y_1)=0$. Put

$$U=\{u\in V_\mathfrak{p}\mid f(x_1, u)=f(y_1, u)=0\}\,,$$
$$K=U\cap L\,.$$

For every $w\in V$, if we put $a^{-1}f(x_1, w)=d$ and $f(w, y_1)a^{-1}=c$, we see easily $w-cx_1-d'y_1\in U$. This implies $V_\mathfrak{p}=D_\mathfrak{p}x_1+D_\mathfrak{p}y_1+U$. If $w\in L$, then $f(x_1, w)$ and $f(w, y_1)$ are contained in $N(L)=\mathfrak{o}_\mathfrak{p}a$, so that c and d are contained in $\mathfrak{o}_\mathfrak{p}$.

We have therefore, $L=\mathfrak{o}_\mathfrak{p}x_1+\mathfrak{o}_\mathfrak{p}y_1+K$. Obviously, K is a lattice in U with the order $\mathfrak{o}_\mathfrak{p}$, and $N(K)\subset N(L)$. As L is maximal, K must be maximal; so we can apply our induction to K. By the assumption of induction, Proposition 3.6 is true for $n-2$. Therefore, if $n>3$, we must have $N(K)=N(L)=\mathfrak{o}_\mathfrak{p}a$, while if $n=3$, $N(K)=\mathfrak{o}_\mathfrak{p}\beta$. This completes our proof.

We call the base $\{x_i, y_i, z\}$ in the above proposition a *canonical base* of L.

PROPOSITION 3.7. *Let L and M be maximal lattices in $V_\mathfrak{p}$. If $L\sigma=M$ for an element σ of $G(V_\mathfrak{p},f)$, then $N(L)^{-1}N(M)$ is an even power of the maximal ideal of $\mathfrak{o}_\mathfrak{p}$, namely $N(L)^{-1}N(M)=\mathfrak{o}_\mathfrak{p}\alpha$ for an element α of $F_\mathfrak{p}$. Conversely, if $\alpha N(L)=N(M)$ with $\alpha\in F$, there exists an element σ of $G(V_\mathfrak{p},f)$ such that $L\sigma=M$, $N(\sigma)=\alpha$.*

PROOF. If $L\sigma=M$ for some $\sigma\in G(V_\mathfrak{p},f)$, we have $N(L)N(\sigma)=N(M)$, so that $N(L)^{-1}N(M)=N(\sigma)\mathfrak{o}_\mathfrak{p}$. This proves the first assertion. Conversely, suppose that $\alpha N(L)=N(M)$ with $\alpha\in F_\mathfrak{p}$. Put $N(L)=\mathfrak{o}_\mathfrak{p}a$, $N(L)\cap F_\mathfrak{p}=\mathfrak{g}_\mathfrak{p}\beta$ with $a\in D_\mathfrak{p}$, $\beta\in F_\mathfrak{p}$. Then we have $N(M)=\mathfrak{o}_\mathfrak{p}\alpha a$, $N(M)\cap F_\mathfrak{p}=\mathfrak{g}_\mathfrak{p}\alpha\beta$. By Proposition 3.5, there exists a canonical base $\{x_i, y_i, z\}$ of L such that $f(x_i, y_j)=a\delta_{ij}$, $f(z,z)=\beta$, and a canonical base $\{u_i, v_i, w\}$ of M such that $f(u_i, v_j)=\alpha a\delta_{ij}$, $f(w,w)=\alpha\beta$. Define an element σ of $E(V_\mathfrak{p}, D_\mathfrak{p})$ by $x_i\sigma=u_i$, $y_i\sigma=v_i$, $z\sigma=w$. Then we see easily that $\sigma\in G(V_\mathfrak{p},f)$, $L\sigma=M$ and $N(\sigma)=\alpha$. This completes our proof.

PROPOSITION 3.8. *Let L be a maximal lattice in $V_\mathfrak{p}$. If $n>1$, there exists a base $\{u_1,\cdots,u_n\}$ of $V_\mathfrak{p}$ over $D_\mathfrak{p}$ such that $L=\mathfrak{o}_\mathfrak{p}u_1+\cdots+\mathfrak{o}_\mathfrak{p}u_n$, $f(u_i,u_i)=0$ for $1\leqq i\leqq n$.*

PROOF. Take a canonical base $\{x_i, y_i, z\}$ of L. If n is even, our assertion is a consequence of the relation $f(x_i,x_i)=f(y_i,y_i)=0$. Suppose that n is odd. The elements a and β being as in Proposition 3.5, we get, by Proposition 3.1, $\beta\in F_\mathfrak{p}\cap\mathfrak{o}_\mathfrak{p}a=\mathrm{Tr}(\mathfrak{o}_\mathfrak{p}a)$. Hence there exists an element b of $\mathfrak{o}_\mathfrak{p}$ such that $\mathrm{Tr}(ba)=\beta$. Put $w=z+bx_1-y_1$. Then we have $f(w,w)=0$ and $L=\mathfrak{o}_\mathfrak{p}x_1+\mathfrak{o}_\mathfrak{p}y_1+\cdots+\mathfrak{o}_\mathfrak{p}x_m+\mathfrak{o}_\mathfrak{p}y_m+\mathfrak{o}_\mathfrak{p}w$. This proves our proposition.

PROPOSITION 3.9. *Let L and M be maximal lattices in $V_\mathfrak{p}$. Put $N(L)=h\mathfrak{o}_\mathfrak{p}$, $N(L)\cap F_\mathfrak{p}=\eta\mathfrak{g}_\mathfrak{p}$ with $h\in D_\mathfrak{p}$, $\eta\in F_\mathfrak{p}$, and suppose that $N(M)=\alpha N(L)$ for an element α of $F_\mathfrak{p}$. Then there exist a canonical base $\{x_i, y_i, z\}$ of $V_\mathfrak{p}$ and elements a_i, b_i, c of $D_\mathfrak{p}$ such that*

$$L=\mathfrak{o}_\mathfrak{p}x_1+\mathfrak{o}_\mathfrak{p}y_1+\cdots+\mathfrak{o}_\mathfrak{p}x_m+\mathfrak{o}_\mathfrak{p}y_m+\mathfrak{o}_\mathfrak{p}z\,,$$

$$M=\mathfrak{o}_\mathfrak{p}a_1x_1+\mathfrak{o}_\mathfrak{p}b_1y_1+\cdots+\mathfrak{o}_\mathfrak{p}a_mx_m+\mathfrak{o}_\mathfrak{p}b_my_m+\mathfrak{o}_\mathfrak{p}cz\,,$$

$$f(x_i,y_j)=h\delta_{ij}\,,\qquad f(z,z)=\eta\,,$$

$$a_1hb_1'=\cdots=a_mhb_m'=\alpha h\,,\qquad cc'=\alpha\,,$$

$$\mathfrak{o}_\mathfrak{p}a_1\supset\cdots\supset\mathfrak{o}_\mathfrak{p}a_m\supset\mathfrak{o}_\mathfrak{p}c\supset\mathfrak{o}_\mathfrak{p}b_m\supset\cdots\supset\mathfrak{o}_\mathfrak{p}b_1\,,$$

where z and c occur only when n is odd.

PROOF. We proceed by induction on n. If $n=1$, this is obvious. Suppose that $n>1$. Put $\mathfrak{e}=\{e\in D_\mathfrak{p} \mid eM\subset L\}$. As $\mathfrak{e}$ is an $\mathfrak{o}_\mathfrak{p}$-ideal, we have $\mathfrak{e}=\mathfrak{o}_\mathfrak{p}e_0$ for an element $e_0\in\mathfrak{o}_\mathfrak{p}$. Put $e_0M=M_1$; then $N(M_1)=N(e_0)N(L)$. If we prove our proposition for M_1, we get easily the assertion for M. In fact, suppose that we get a canonical base $\{x_i, y_i, z\}$ of $V_\mathfrak{p}$ and elements r_i, s_i, t of $D_\mathfrak{p}$ such that $L=\sum_{i=1}^{m}(\mathfrak{o}_\mathfrak{p}x_i+\mathfrak{o}_\mathfrak{p}y_i)+\mathfrak{o}_\mathfrak{p}z$, $M_1=\sum_{i=1}^{m}(\mathfrak{o}_\mathfrak{p}r_ix_i+\mathfrak{o}_\mathfrak{p}s_iy_i)+\mathfrak{o}_\mathfrak{p}tz$, $f(x_i,y_i)=h$, $f(z,z)=\eta$, $r_ihs_i'=N(e_0)\alpha h$, $tt'=N(e_0)\alpha$, $\mathfrak{o}_\mathfrak{p}r_1\supset\cdots\supset\mathfrak{o}_\mathfrak{p}r_m\supset\mathfrak{o}_\mathfrak{p}t\supset\mathfrak{o}_\mathfrak{p}s_m\supset\cdots\supset\mathfrak{o}_\mathfrak{p}s_1$. Put $a_i=e_0^{-1}r_i$, $b_i=h^{-1}e_0^{-1}hs_i$, $c=e_0^{-1}t$. Then we can easily verify that $\{x_i, y_i, z\}$ and $\{a_i, b_i, c\}$ have the properties of our proposition for M and L. Therefore we may assume that $M=M_1$, namely $\mathfrak{o}_\mathfrak{p}=\{e\in D_\mathfrak{p} \mid eM\subset L\}$. Let Π be a prime element of $\mathfrak{o}_\mathfrak{p}$. By Proposition 3.8, M contains an element x_1 such that $f(x_1,x_1)=0$, $\Pi^{-1}x_1\notin L$. Namely, the relation (5) holds for this $\{x_1, L\}$. Hence, applying the proof of Proposition 3.5 to the present case, we get an element y_1 of L such that $f(x_1,y_1)=h$, $f(y_1,y_1)=0$. By Proposition 2.7, we have $\alpha L\subset M$, so that $\alpha y_1\in M$. Put $U=\{u\in V_\mathfrak{p} \mid f(x_1,u)=f(y_1,u)=0\}$, $L_0=U\cap L$, $M_0=U\cap M$. Then, as in the proof of Proposition 3.5, we obtain

$$V_\mathfrak{p}=D_\mathfrak{p}x_1+D_\mathfrak{p}y_1+U, \qquad L=\mathfrak{o}_\mathfrak{p}x_1+\mathfrak{o}_\mathfrak{p}y_1+L_0;$$

and L_0 is a maximal lattice in U such that $N(L_0)=h\mathfrak{o}_\mathfrak{p}$ or $\eta\mathfrak{o}_\mathfrak{p}$ according as $n>1$ or $n=1$. Let $w=dx_1+ey_1+w_0$, with $d\in\mathfrak{o}_\mathfrak{p}$, $e\in\mathfrak{o}_\mathfrak{p}$, $w_0\in L_0$, be an element of M. Then we have $e=f(w,x_1)\in N(M)=\mathfrak{o}_\mathfrak{p}\alpha h$, so that $e\in\mathfrak{o}_\mathfrak{p}\alpha$, $ey_1\in\mathfrak{o}_\mathfrak{p}\alpha y_1\subset M$, and hence $w_0=w-dx_1-ey_1\in M\cap U=M_0$. This implies $M=\mathfrak{o}_\mathfrak{p}x_1+\mathfrak{o}_\mathfrak{p}\alpha y_1+M_0$. We observe that M_0 is a maximal lattice in U such that $N(M_0)=\alpha N(L_0)$. Therefore we can apply our induction to L_0 and M_0. Then we obtain a canonical base $\{x_2,\cdots,x_m,y_2,\cdots,y_m,z\}$ of U and elements $a_2,\cdots,a_m,b_2,\cdots,b_m,c$ of $D_\mathfrak{p}$ such that $L_0=\sum_{i=2}^{m}(\mathfrak{o}_\mathfrak{p}x_i+\mathfrak{o}_\mathfrak{p}y_i)+\mathfrak{o}_\mathfrak{p}z$, $M_0=\sum_{i=2}^{m}(\mathfrak{o}_\mathfrak{p}a_ix_i+\mathfrak{o}_\mathfrak{p}b_iy_i)+\mathfrak{o}_\mathfrak{p}cz$, $f(x_i,y_i)=h$ for $2\leqq i\leqq m$, $f(z,z)=\eta$, $a_2hb_2'=\cdots=a_mhb_m'=\alpha h$, $cc'=\alpha$, $\mathfrak{o}_\mathfrak{p}a_2\supset\cdots\supset\mathfrak{o}_\mathfrak{p}a_m\supset\mathfrak{o}_\mathfrak{p}c\supset\mathfrak{o}_\mathfrak{p}b_m\supset\cdots\supset\mathfrak{o}_\mathfrak{p}b_2$. As $L_0\supset M_0$, we have $\mathfrak{o}_\mathfrak{p}\ni a_2$, so that $\mathfrak{o}_\mathfrak{p}b_2\supset\mathfrak{o}_\mathfrak{p}\alpha$. Putting $a_1=1$ and $b_1=\alpha$, we obtain our assertion for L and M. This completes the proof.

PROPOSITION 3.10. *Let L be a maximal lattice in $V_\mathfrak{p}$. Put $N(L)=h\mathfrak{o}_\mathfrak{p}$, $N(L)\cap F_\mathfrak{p}=\eta\mathfrak{g}_\mathfrak{p}$ with $h\in D_\mathfrak{p}$, $\eta\in F_\mathfrak{p}$. Let $\{u_i, v_i, w\}$ be a canonical base of L such that $f(u_i,v_j)=h\delta_{ij}$, $f(w,w)=\eta$. Denote by Γ^0 the subgroup of $G^0(V_\mathfrak{p},f)$ consisting of the elements $\gamma\in G^0(V_\mathfrak{p},f)$ such that $L\gamma=L$, and by Δ the set of elements σ of $G(V_\mathfrak{p},f)$ such that $u_i\sigma=a_iu_i$, $v_i\sigma=b_iv_i$, $w\sigma=cw$ with elements a_i, b_i, c of $D_\mathfrak{p}$ satisfying the relation*

$$\mathfrak{o}_\mathfrak{p}a_1\supset\cdots\supset\mathfrak{o}_\mathfrak{p}a_m\supset\mathfrak{o}_\mathfrak{p}c\supset\mathfrak{o}_\mathfrak{p}b_m\supset\cdots\supset\mathfrak{o}_\mathfrak{p}b_1.$$

Then we have $G(V_\mathfrak{p},f)=\Gamma^0\cdot\Delta\cdot\Gamma^0$.

PROOF. Let τ be an element of $G(V_\mathfrak{p},f)$. Put $M=L\tau$, $\alpha=N(\tau)$, and apply Proposition 3.9 to this $\{L, M, \alpha\}$. Then we get a canonical base $\{x_i, y_i, z\}$ of

L and elements a_i, b_i, c of $D_\mathfrak{p}$ with the properties of that proposition. Define two elements γ and σ of $E(V_\mathfrak{p}, A_\mathfrak{p})$ by $u_i\gamma = x_i$, $v_i\gamma = y_i$, $w\gamma = z$, $u_i\sigma = a_iu_i$, $v_i\sigma = b_iv_i$, $w\sigma = cw$. We see easily that $\gamma \in \Gamma^0$ and $\sigma \in \Delta$, $N(\sigma) = \alpha$. Further we have $L\sigma\gamma = L\tau$. Hence if we put $\varepsilon\sigma\gamma = \tau$, we have $L\varepsilon = L$, $\varepsilon \in G(V_\mathfrak{p}, f)$, $N(\varepsilon) = 1$, so that $\varepsilon \in \Gamma^0$. It follows that $\tau = \varepsilon\sigma\gamma \in \Gamma^0 \cdot \Delta \cdot \Gamma^0$. Our proposition is thereby proved.

Notation being as in Proposition 3.9, we call $\{\mathfrak{o}_\mathfrak{p}a_1, \cdots, \mathfrak{o}_\mathfrak{p}a_m, \mathfrak{o}_\mathfrak{p}c, \mathfrak{o}_\mathfrak{p}b_1, \cdots, \mathfrak{o}_\mathfrak{p}b_m\}$ *the set of elementary divisors of* M *relative to* L and denote it by $\{L : M\}$.

PROPOSITION 3.11. *Let L, M, K be maximal lattices in $V_\mathfrak{p}$ such that $N(M) = \alpha N(L)$, $N(K) = \beta N(L)$ with $\alpha, \beta \in F_\mathfrak{p}$. Then, there exists an element σ of $G^0(V_\mathfrak{p}, f)$ such that $L\sigma = L$ and $M\sigma = K$, if and only if $\{L : M\} = \{L : K\}$.*

By virtue of Proposition 3.9, this can be proved by the same argument as in the proof of Proposition 2.13. When $L \supset M$ and $L \supset K$, the equality $\{L : M\} = \{L : K\}$ holds if and only if L/M and L/K are isomorphic as $\mathfrak{o}_\mathfrak{p}$-modules.

3.3. Local approximation theorem. Let $A_\mathfrak{p}$ be a quaternion algebra over $F_\mathfrak{p}$, which may be or may not be a division algebra. Let $\mathfrak{o}_\mathfrak{p}$ be a maximal order in $A_\mathfrak{p}$.

PROPOSITION 3.12. *Let $V_\mathfrak{p}$ be an $A_\mathfrak{p}$-space of dimension n and f be a non-degenerate Q-hermitian form on $V_\mathfrak{p}$. Let L be a maximal lattice in $V_\mathfrak{p}$ such that $N(L) = \mathfrak{o}_\mathfrak{p}$. Then there exists a base $\{x_1, \cdots, x_n\}$ of $V_\mathfrak{p}$ over $A_\mathfrak{p}$ such that $f(x_i, x_j) = \delta_{ij}$ and $L = \mathfrak{o}_\mathfrak{p}x_1 + \cdots + \mathfrak{o}_\mathfrak{p}x_n$.*

PROOF. By Proposition 2.1 and Proposition 3.3, $V_\mathfrak{p}$ has a base $\{y_1, \cdots, y_n\}$ over $A_\mathfrak{p}$ such that $f(y_i, y_j) = \delta_{ij}$. Put $M = \mathfrak{o}_\mathfrak{p}y_1 + \cdots + \mathfrak{o}_\mathfrak{p}y_n$. By Proposition 2.6, M is a maximal lattice in $V_\mathfrak{p}$ and $N(M) = \mathfrak{o}_\mathfrak{p}$. By Proposition 2.11 (if $A_\mathfrak{p} = M_2(F_\mathfrak{p})$) and by Proposition 3.7 (if $A_\mathfrak{p} = D_\mathfrak{p}$), there exists an element σ of $G^0(V_\mathfrak{p}, f)$ such that $L = M\sigma$. Putting $x_i = y_i\sigma$ for $1 \leqq i \leqq n$, we get the desired result.

PROPOSITION 3.13. *Let $V_\mathfrak{p}$ and $U_\mathfrak{p}$ be $A_\mathfrak{p}$-spaces of the same dimension; let f and h be non-degenerate Q-hermitian forms on $V_\mathfrak{p}$ and on $U_\mathfrak{p}$, respectively. Let L and M be maximal lattices in $V_\mathfrak{p}$ and in $U_\mathfrak{p}$, respectively, such that $N_f(L) = N_h(M) = \mathfrak{o}_\mathfrak{p}$. Let τ be an $A_\mathfrak{p}$-linear mapping of $V_\mathfrak{p}$ into $U_\mathfrak{p}$ such that $L\tau \subset M$, $f(x, y) \equiv h(x\tau, y\tau) \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$ for every x, $y \in L$, where λ is an integer $\geqq 0$. Then there exists an $A_\mathfrak{p}$-isomorphism σ of $V_\mathfrak{p}$ onto $U_\mathfrak{p}$ such that $L\sigma = M$, $f(x, y) = h(x\sigma, y\sigma)$ for every x, $y \in V_\mathfrak{p}$ and $L(\sigma - \tau) \subset \mathfrak{p}^\lambda M$.*

PROOF. Our proposition is clear if $\lambda = 0$; so we assume $\lambda \geqq 1$. Let n be the common dimension of $V_\mathfrak{p}$ and $U_\mathfrak{p}$. We proceed by induction on n. By Proposition 3.12, there exists a base $\{u_1, \cdots, u_n\}$ of $U_\mathfrak{p}$ over $A_\mathfrak{p}$ such that $M = \mathfrak{o}_\mathfrak{p}u_1 + \cdots + \mathfrak{o}_\mathfrak{p}u_n$, $h(u_i, u_j) = \delta_{ij}$; and L contains an element v such that $f(v, v) = 1$. Put $v\tau = \sum_{i=1}^{n} a_iu_i$ with $a_i \in \mathfrak{o}_\mathfrak{p}$. Then $1 = f(v, v) \equiv h(v\tau, v\tau) = \sum_{i=1}^{n} N(a_i) \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$.

Therefore $N(a_i)$ is a unit of $\mathfrak{g}_\mathfrak{p}$ for some i, say 1. Put $\beta=1-\sum_{i=2}^{n}N(a_i)$. Then $N(a_1)\equiv\beta \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$, and hence β is a unit of $\mathfrak{g}_\mathfrak{p}$. By Proposition 3.2, there exists an element b of $\mathfrak{o}_\mathfrak{p}$ such that $b\equiv a_1 \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$ and $N(b)=\beta$. Put $w=bu_1+\sum_{i=2}^{n}a_iu_i$. Then $h(w,w)=1$, $w\equiv v\tau \bmod \mathfrak{p}^\lambda M$, and $w\in M$. Put

$$V^0=\{x\in V_\mathfrak{p}\mid f(x,v)=0\}\,,\qquad U^0=\{x\in U_\mathfrak{p}\mid h(x,w)=0\}\,,$$
$$L^0=L\cap V^0\,,\qquad M^0=M\cap U^0\,.$$

As $f(v,v)=h(w,w)=1$, we obtain

$$V_\mathfrak{p}=A_\mathfrak{p}v+V^0\,,\qquad U_\mathfrak{p}=A_\mathfrak{p}w+V^0\,,$$
$$L=\mathfrak{o}_\mathfrak{p}v+L^0\,,\qquad M=\mathfrak{o}_\mathfrak{p}w+M^0\,.$$

It can be easily seen that L and M are respectively maximal lattices in V^0 and U^0; and $N_f(L^0)=N_h(M^0)=\mathfrak{o}_\mathfrak{p}$. Now define an $A_\mathfrak{p}$-linear mapping ρ of V^0 into U^0 by $x\tau=tw+x\rho$ for $x\in V^0$, where $t\in A_\mathfrak{p}$. We see easily $L^0\rho\subset M^0$. If $x\in L^0$ and $x\tau=tw+x\rho$, we have $0=f(v,x)\equiv h(v\tau,x\tau)\equiv h(w,tw+x\rho)=t \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$. This shows $x\tau\equiv x\rho \bmod \mathfrak{p}^\lambda M$ for $x\in L^0$. If further $y\in L^0$, we have $f(x,y)\equiv h(x\tau,y\tau)\equiv h(x\rho,y\rho) \bmod \mathfrak{p}^\lambda\mathfrak{o}_\mathfrak{p}$. Therefore we can apply induction to L^0, M^0, ρ. Namely there exists an $A_\mathfrak{p}$-isomorphism σ^0 of V^0 onto U^0 such that $L^0\sigma^0=M^0$, $f(x,y)=h(x\sigma^0,y\sigma^0)$ for every x, $y\in V^0$, and $L^0(\sigma^0-\rho)\subset\mathfrak{p}^\lambda M^0$. Now define an $A_\mathfrak{p}$-isomorphism σ of $V_\mathfrak{p}$ onto $U_\mathfrak{p}$ by $v\sigma=w$ and $x\sigma=x\sigma^0$ for every $x\in V^0$. Then we have clearly $L\sigma=M$, $f(x,y)=h(x\sigma,y\sigma)$ for every x, $y\in V_\mathfrak{p}$. Furthermore, $v\sigma=w\equiv v\tau \bmod \mathfrak{p}^\lambda M$; and if $x\in L^0$, $x\sigma=x\sigma^0\equiv x\rho\equiv x\tau \bmod \mathfrak{p}^\lambda M$. Therefore $L(\sigma-\tau)\subset\mathfrak{p}^\lambda M$. This completes our proof.

§ 4. Global theory of Q-hermitian forms.

In this section, we always mean by F an algebraic number field of finite degree, and by $\mathfrak{g}$ the ring of integers in F. For every prime ideal $\mathfrak{p}$ of F, $F_\mathfrak{p}$ and $\mathfrak{g}_\mathfrak{p}$ denote respectively the $\mathfrak{p}$-completions of F and $\mathfrak{g}$. We denote by $\mathfrak{p}_{\infty\kappa}$ for $1\leqq\kappa\leqq v$ the infinite prime spots of F and by F_κ the completion of F with respect to $\mathfrak{p}_{\infty\kappa}$.

4.1. Quaternion algebras over an algebraic number field. Let A be a quaternion algebra over F. For each prime ideal $\mathfrak{p}$ of F, and for each infinite prime spot $\mathfrak{p}_{\infty\kappa}$ of F, we put

$$A_\mathfrak{p}=A\otimes_F F_\mathfrak{p}\,,\qquad A_\kappa=A\otimes_F F_\kappa\,.$$

A finite or infinite prime spot of F is called *ramified* in A/F if the corresponding completion $A_\mathfrak{p}$ or A_κ is a division algebra. Let $\mathfrak{o}$ be a maximal order in A. Let $\mathfrak{D}=\mathfrak{D}(\mathfrak{o}/\mathfrak{g})$ be the different of $\mathfrak{o}$ with respect to $\mathfrak{g}$. Then we have

$\mathfrak{D}=\prod_{i=1}^{s}\mathfrak{Q}_i$, $\mathfrak{Q}_i^2=\mathfrak{q}_i$, where the $\mathfrak{q}_i$ are all the prime ideals of F which are ramified in A/F, and $\mathfrak{Q}_i$ is a prime $\mathfrak{o}$-ideal. Every two-sided $\mathfrak{o}$-ideal $\mathfrak{a}$ is written in the form $\mathfrak{a}=\prod\mathfrak{Q}_i^{e_i}\cdot\mathfrak{a}_0$, where $e_i=0$ or 1, and $\mathfrak{a}_0$ is a $\mathfrak{g}$-ideal.

PROPOSITION 4.1. *Let $\mathfrak{p}_{\infty_1},\cdots,\mathfrak{p}_{\infty_u}$ be the infinite prime spots of F ramified in A/F, and ξ be a non-zero element of F. Then there exists an element x of A such that $N(x)=\xi$, if and only if $\xi\equiv 1 \bmod \mathfrak{p}_{\infty_1}\cdots\mathfrak{p}_{\infty_u}$.*

PROOF. Consider $N(x)=xx'$ as a quadratic form on A over F. By Hasse's theorem, the equation $xx'=\xi$ has a solution if and only if it is solvable in every local fields. Our proposition is therefore an immediate consequence of Proposition 3.3.

We call A *definite* (or *totally definite*) if all the infinite prime spots of F are ramified in A/F, and call A *indefinite* otherwise. If A is definite, then F must be totally real and $A_\kappa=\boldsymbol{K}$ for every infinite prime spot $\mathfrak{p}_{\infty_\kappa}$ of F. Now the following two fundamental lemmas are due to Eichler; they are originally given in a more general case (cf. [**5**, Satz 5]).

LEMMA 4.2. *Suppose that A is indefinite. Let $\mathfrak{o}$ be a maximal order in A and let $\mathfrak{p}_{\infty_1},\cdots,\mathfrak{p}_{\infty_u}$ be the infinite prime spots ramified in A/F. Let $\mathfrak{b}$ and $\mathfrak{c}$ be left $\mathfrak{o}$-ideals. Then there exists an element x of A such that $\mathfrak{b}=\mathfrak{c}x$, if and only if $N(\mathfrak{b})$ and $N(\mathfrak{c})$ belong to the same ideal-class modulo $\mathfrak{p}_{\infty_1}\cdots\mathfrak{p}_{\infty_u}$ of F.*

LEMMA 4.3. *Notation and assumption being as in Lemma 4.2, let $\mathfrak{a}$ be an integral two-sided $\mathfrak{o}$-ideal. Let β be an element of $\mathfrak{g}$ and b an element of $\mathfrak{o}$ such that $\beta\equiv 1 \bmod \mathfrak{p}_{\infty_1}\cdots\mathfrak{p}_{\infty_u}$, $N(b)\equiv\beta \bmod^*(\mathfrak{a}\cap F)$. Then there exists an element b_0 of $\mathfrak{o}$ such that $b\equiv b_0 \bmod \mathfrak{a}$, $N(b_0)=\beta$.*

Here mod * means the multiplicative congruence. Lemma 4.2 is easily derived from Lemma 4.3 (cf. [**5**, p. 239]). Our later discussion will prove this fact as a particular case.

4.2. Hasse principle for Q-hermitian forms. In view of Proposition 3.3, there exists, among the quaternion algebras over local fields $F_\mathfrak{p}$ and F_κ, only one which does not satisfy the condition (D) of Proposition 2.1; it is the division ring $\boldsymbol{K}$ of real quaternions. Let V be a $\boldsymbol{K}$-space of dimension n and f a non-degenerate Q-hermitian form on V. Then there exists a base $\{x_1,\cdots,x_n\}$ of V over $\boldsymbol{K}$ such that $f(x_i,x_j)=\varepsilon_i\delta_{ij}$ for $1\leqq i\leqq n$, $1\leqq j\leqq n$ and $\varepsilon_i=1$ for $1\leqq i\leqq\nu$, $\varepsilon_i=-1$ for $\nu<i\leqq n$. The integer ν is uniquely determined by f. We put $\nu=\nu(f)$.

Let A be a quaternion algebra over F and let $\mathfrak{p}_{\infty_1},\cdots,\mathfrak{p}_{\infty_u}$ be all the infinite prime spots of F ramified in A/F. Consider an A-space V and a non-degenerate Q-hermitian form f on V. Put $V_\kappa=V\otimes_F F_\kappa$ for $1\leqq\kappa\leqq u$. Then V_κ can be considered as an A_κ-space in a natural manner; and f is uniquely extended to a non-degenerate Q-hermitian form f_κ on V_κ. As A_κ is isomorphic

to $\boldsymbol{K}$, we can define $\nu(f_\kappa)$. We put $\nu_\kappa(f)=\nu(f_\kappa)$. Now, by Ramanathan [7], the structure of $\{V,f\}$ is completely determined by the $\nu_\kappa(f)$. We state this result in the following form.

LEMMA 4.4. *Let f and g be non-degenerate Q-hermitian forms on an A-space V. There exists an element σ of $GL(V,A)$ such that $f(x\sigma,y\sigma)=g(x,y)$ for every x, y of V, if and only if $\nu_\kappa(f)=\nu_\kappa(g)$ for every infinite prime spot $\mathfrak{p}_{\infty\kappa}$ of F ramified in A/F.*

This can be proved easily by means of Proposition 4.1 and the approximation theorem in the number field F.

4.3. Adele-group of $G(V,f)$. Let A be a quaternion algebra over F and V an A-space of dimension n. For each prime ideal $\mathfrak{p}$ of F and for each infinite prime spot $\mathfrak{p}_{\infty\kappa}$ of F, we put

$$V_\mathfrak{p}=V\underset{F}{\otimes}F_\mathfrak{p}\,,\qquad V_\kappa=V\underset{F}{\otimes}F_\kappa\,.$$

Then $V_\mathfrak{p}$ (resp. V_κ) can be considered as an $A_\mathfrak{p}$-space (resp. A_κ-space) in a natural manner. Let f be a non-degenerate Q-hermitian form on V. We extend f to non-degenerate Q-hermitian forms on $V_\mathfrak{p}$ and on V_κ, and denote them again by f. Put now $G=G(V,f)$, $G_\mathfrak{p}=G(V_\mathfrak{p},f)$, $G_\kappa=G(V_\kappa,f)$. Then $G_\mathfrak{p}$, G_κ are locally compact topological groups with usual topology. Let L be a $\mathfrak{g}$-lattice in V. For each $\mathfrak{p}$, denote by $\mathfrak{U}_\mathfrak{p}$ the set of elements τ of $G_\mathfrak{p}$ such that $L_\mathfrak{p}\tau=L_\mathfrak{p}$. Then $\mathfrak{U}_\mathfrak{p}$ is a compact subgroup of $G_\mathfrak{p}$. Put

$$\mathfrak{U}_L=\prod_\mathfrak{p}\mathfrak{U}_\mathfrak{p}\times\prod_\kappa G_\kappa\,.$$

By the product topology, $\mathfrak{U}_L$ is a locally compact group. Now we define the *adele-group* $\mathfrak{G}$ of $G(V,f)$ as the set of elements $(\sigma_\mathfrak{p},\sigma_\kappa)$ of $\prod_\mathfrak{p}G_\mathfrak{p}\times\prod_\kappa G_\kappa$ such that $\sigma_\mathfrak{p}\in\mathfrak{U}_\mathfrak{p}$ for all except a finite number of $\mathfrak{p}$. Define a topology of $\mathfrak{G}$ so that $\mathfrak{U}_L$ is an open subgroup of $\mathfrak{G}$. Then $\mathfrak{G}$ becomes a locally compact group. The topological group $\mathfrak{G}$ is determined independently of the choice of L. By the injection $\sigma\to(\cdots,\sigma,\sigma,\cdots)$, G can be considered as a discrete subgroup of $\mathfrak{G}$. By a general theorem of Borel [1], $\mathfrak{G}$ is the union of a finite number of double cosets $\mathfrak{U}_L\xi G$ with $\xi\in\mathfrak{G}$ (cf. also Weil [11, 12]).

4.4. Classes and Genera of maximal lattices. Notation being as in § 4.3, let $\mathfrak{o}$ be a maximal order in A, and $\mathfrak{o}_\mathfrak{p}=\mathfrak{g}_\mathfrak{p}\mathfrak{o}$. We denote by $\mathfrak{L}(\mathfrak{o})$ the set of all maximal lattices in V with the order $\mathfrak{o}$. Let L and M be two members of $\mathfrak{L}(\mathfrak{o})$. We say that L and M belong to the same *genus*, if there exists, for each prime ideal $\mathfrak{p}$ of F, an element $\sigma_\mathfrak{p}$ of $G(V_\mathfrak{p},f)$ such that $L_\mathfrak{p}\sigma_\mathfrak{p}=M_\mathfrak{p}$. Further we say that L and M belong to the same *class*, if there exists an element σ of $G(V,f)$ such that $L\sigma=M$.

PROPOSITION 4.5. *If $n>1$, for every two-sided $\mathfrak{o}$-ideal $\mathfrak{a}$, there exists a member L of $\mathfrak{L}(\mathfrak{o})$ such that $N(L)=\mathfrak{a}$.*

PROOF. Take an arbitrary maximal lattice M in V with the order $\mathfrak{o}$. There exist only a finite number of $\mathfrak{p}$ such that $N(M_\mathfrak{p}) \neq \mathfrak{a}_\mathfrak{p}$. For each one of such $\mathfrak{p}$, take a maximal lattice $L^\mathfrak{p}$ in $V_\mathfrak{p}$ with the order $\mathfrak{o}_\mathfrak{p}$, such that $N(L^\mathfrak{p}) = \mathfrak{a}_\mathfrak{p}$. This is possible by Propositions 2.6 and 3.5. Put $L^\mathfrak{p} = M_\mathfrak{p}$ for every $\mathfrak{p}$ such that $N(M_\mathfrak{p}) = \mathfrak{a}_\mathfrak{p}$. Then, by Lemma 1, there exists a $\mathfrak{g}$-lattice L in V such that $L_\mathfrak{p} = L^\mathfrak{p}$ for any $\mathfrak{p}$. It is clear that L is a member of $\mathfrak{L}(\mathfrak{o})$ and $N(L) = \mathfrak{a}$.

PROPOSITION 4.6. *Let $\mathfrak{o}$ be a maximal order in A. If $n = 1$, $\mathfrak{L}(\mathfrak{o})$ consists of only one genus, $\mathfrak{L}(\mathfrak{o})$ itself. If $n > 1$, there are exactly 2^s genera in $\mathfrak{L}(\mathfrak{o})$, where s is the number of prime ideals ramified in A/F.*

PROOF. The $\mathfrak{Q}_i$ being as in § 4.1, we have $N(L) = \mathfrak{Q}_1^{e_1} \cdots \mathfrak{Q}_s^{e_s} \cdot \mathfrak{a}$ for every $L \in \mathfrak{L}(\mathfrak{o})$, where $e_i = 0$ or 1, and $\mathfrak{a}$ is a $\mathfrak{g}$-ideal. By Proposition 2.11 and Proposition 3.7, the genus of L is determined only by $\{e_1, \cdots, e_s\}$. This together with Proposition 4.5 proves our proposition.

We denote, for any set of integers $\{e_1, \cdots, e_s\}$ such that $e_i = 0$ or 1, by $\mathfrak{L}(\mathfrak{o}; \{e_i\})$ the genus of L such that $N(L) = \coprod_{i=1}^{s} \mathfrak{Q}_i^{e_i} \cdot \mathfrak{a}$ with an ideal $\mathfrak{a}$ of F. We call especially $\mathfrak{L}(\mathfrak{o}; \{0, \cdots, 0\})$ *the principal genus with the order* $\mathfrak{o}$ and denote it by $\mathfrak{L}_0(\mathfrak{o})$.

Fix a member L of $\mathfrak{L}(\mathfrak{o})$ and define $\mathfrak{U}_L$ as in § 4.3. For every element $\xi = (\xi_\mathfrak{p}, \xi_\kappa)$ of the adele-group $\mathfrak{G}$, put $L\xi = \bigcap_\mathfrak{p} (L_\mathfrak{p}\xi_\mathfrak{p} \cap V)$. By Lemma 1.1, $L\xi$ is a $\mathfrak{g}$-lattice in V; and $(L\xi)_\mathfrak{p} = L_\mathfrak{p}\xi_\mathfrak{p}$. By Propositions 2.2, 2.3, 2.4, we see that $L\xi$ is a member of $\mathfrak{L}(\mathfrak{o})$. Further, by our definition, $L\xi$ belongs to the same genus as L. Conversely, if M is a maximal lattice belonging to the same genus as L, we can find an element ξ of $\mathfrak{G}$ such that $L\xi = M$. If $\xi \in G$, the notation $L\xi$ is just the same as the transform of L by ξ; so there is no fear of confusion. We have $L\xi = L\eta$ if and only if $\mathfrak{U}_L\xi = \mathfrak{U}_L\eta$. Therefore, the mapping $\xi \to L\xi$ gives a one-to-one mapping of $\mathfrak{U}_L\backslash\mathfrak{G}$ onto the genus of L. Moreover, we note that this gives a one-to-one correspondence between $\mathfrak{U}_L\backslash\mathfrak{G}/G$ and the classes in the genus. By the fact remarked at the end of § 4.3, this implies that each genus consists of a finite number of classes. Further, by Proposition 2.5, we observe that the number of classes in $\mathfrak{L}(\mathfrak{o}; \{e_i\})$ depends only on $\{e_i\}$ and is independent of the choice of $\mathfrak{o}$.

4.5. An existence theorem in the case $n = 2$. Let A be a quaternion algebra over F. We denote by $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ all the prime ideals of F which are ramified in A/F, and by $\mathfrak{p}_{\infty 1}, \cdots, \mathfrak{p}_{\infty u}$ all the infinite prime spots of F which are ramified in A. We put

$$\mathfrak{d} = \coprod_{h=1}^{s} \mathfrak{q}_h, \qquad \mathfrak{u} = \coprod_{\kappa=1}^{u} \mathfrak{p}_{\infty\kappa}.$$

Let V be an A-space of dimension n and f a non-degenerate Q-hermitian form on V. Fix a maximal order $\mathfrak{o}$ in A; and for each $\mathfrak{q}_h$, let $\mathfrak{Q}_h$ be the prime

$\mathfrak{o}$-ideal such that $\mathfrak{Q}_h^2=\mathfrak{q}_h$. We put $\mathfrak{g}_\mathfrak{p}\mathfrak{p}=\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of F, and $\mathfrak{o}_{\mathfrak{q}_h}\mathfrak{Q}_h=\mathfrak{Q}_h$ for every h, when there is no fear of confusion.

LEMMA 4.7. *Let $\mathfrak{p}$ be a prime ideal of F which is unramified in A/F. Let $\mathfrak{o}_\mathfrak{p}$ be a maximal order in $A_\mathfrak{p}$. Let a be a regular element of $A_\mathfrak{p}$ and δ be an element of $\mathfrak{g}_\mathfrak{p}$. Then there exists an element d of $\mathfrak{o}_\mathfrak{p}\cap a\mathfrak{o}_\mathfrak{p}a^{-1}$ such that $N(d)=\delta$.*

PROOF. We may assume that $A_\mathfrak{p}=M_2(F_\mathfrak{p})$ and $\mathfrak{o}_\mathfrak{p}=M_2(\mathfrak{g}_\mathfrak{p})$. Then we can find units ε, η of $\mathfrak{o}_\mathfrak{p}$ such that $\varepsilon a\eta=\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$ with $\alpha, \beta\in F_\mathfrak{p}$. Put $d=\varepsilon^{-1}\begin{pmatrix}1 & 0\\ 0 & \delta\end{pmatrix}\varepsilon$. Then we have $N(d)=\delta$ and $d\in\mathfrak{o}_\mathfrak{p}$. Further we get

$$a^{-1}da=a^{-1}\varepsilon^{-1}\begin{pmatrix}1 & 0\\ 0 & \delta\end{pmatrix}\varepsilon a=\eta\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}^{-1}\begin{pmatrix}1 & 0\\ 0 & \delta\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\eta^{-1}=\eta\begin{pmatrix}1 & 0\\ 0 & \delta\end{pmatrix}\eta^{-1}\in\mathfrak{o}_\mathfrak{p},$$

so that $d\in a\mathfrak{o}_\mathfrak{p}a^{-1}$, which completes the proof.

PROPOSITION 4.8. *Suppose that A is indefinite and $n=2$. Let L be a $\mathfrak{g}$-lattice in V written in the form $L=\mathfrak{o}x+\mathfrak{c}^{-1}y$, where $\mathfrak{c}$ is an integral right $\mathfrak{o}$-ideal, $f(x,x)=1$, $f(x,y)=0$, $f(y,y)=\gamma$, $N(\mathfrak{c})=\gamma\mathfrak{g}$ with an element γ of $\mathfrak{g}$. Suppose that γ is prime to $\mathfrak{d}$. Let $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ be distinct prime ideals which are prime to $\mathfrak{d}$, and let α be a non-zero element of $\mathfrak{g}$ such that $\alpha\equiv 1 \bmod \mathfrak{p}_{\varkappa\kappa}$ whenever $\gamma\equiv 1 \bmod \mathfrak{p}_{\infty\kappa}$ for $1\leqq\kappa\leqq u$. Put $\mathfrak{g}_{\mathfrak{p}_i}\alpha=\mathfrak{p}_i^{\mu_i}$ for $1\leqq i\leqq r$ and $\mathfrak{g}_{\mathfrak{q}_h}\alpha=\mathfrak{q}_h^{\lambda_h}$ for $1\leqq h\leqq s$. Let ξ_i, η_i, for $1\leqq i\leqq r$, and ν_h, for $1\leqq h\leqq s$, be integers such that*

$$0\leqq\xi_i\leqq\eta_i\leqq\mu_i-\eta_i\leqq\mu_i-\xi_i\leqq\mu_i\,,\qquad 0\leqq\nu_h\leqq\lambda_h\,.$$

Then there exists an element σ of $G(V,f)$ such that $L\sigma\subset L$, $N(\sigma)=\alpha$,

$$\{L_{\mathfrak{p}_i}:L_{\mathfrak{p}_i}\sigma\}=\{\mathfrak{p}_i^{\xi_i},\mathfrak{p}_i^{\eta_i},\mathfrak{p}_i^{\mu_i-\xi_i},\mathfrak{p}_i^{\mu_i-\eta_i}\}\qquad \text{for}\quad 1\leqq i\leqq r,$$

$$\{L_{\mathfrak{q}_h}:L_{\mathfrak{q}_h}\sigma\}=\{\mathfrak{Q}_h^{\nu_h},\mathfrak{Q}_h^{2\lambda_h-\nu_h}\}\qquad \text{for}\quad 1\leqq h\leqq s\,.$$

PROOF. For simplicity, we denote the indices $\mathfrak{p}_i$ and $\mathfrak{q}_h$ respectively by i and h; for example, L_i means $L_{\mathfrak{p}_i}$ and $\mathfrak{g}_h$ means $\mathfrak{g}_{\mathfrak{q}_h}$. By Proposition 2.6, L is maximal and $N(L)=\mathfrak{o}$. Now, for each $\mathfrak{p}_i$, we identify $\mathfrak{o}_i$ with $M_2(\mathfrak{g}_i)$, and fix an element π_i of $\mathfrak{g}$ such that $\mathfrak{p}_i=\mathfrak{g}_i\pi_i$. Put $\mathfrak{g}_i\gamma=\mathfrak{p}_i^{e_i}$. Without any loss of generality, we may assume that $\mathfrak{c}_i^{-1}$ is written in the form $\mathfrak{c}_i^{-1}=\begin{pmatrix}\mathfrak{p}_i^{-c_i} & \mathfrak{p}_i^{-d_i}\\ \mathfrak{p}_i^{-c_i} & \mathfrak{p}_i^{-d_i}\end{pmatrix}$, where c_i and d_i are integers such that $c_i\geqq d_i\geqq 0$ and $c_i+d_i=e_i$. Consider the ideal-class modulo $\mathfrak{u}$ containing the inverse of the ideal

$$\prod_{i=1}^{r}\mathfrak{p}_i^{2\mu_i+2+c_i-d_i+\eta_i-\xi_i}\prod_{h=1}^{s}\mathfrak{q}_h^{\nu_h}\,.$$

We can find an integral ideal $\mathfrak{a}$ in that class which is prime to $\gamma\alpha\prod_{i=1}^{r}\mathfrak{p}_i\cdot\mathfrak{d}$. We get then

$$\mathfrak{a}\cdot\prod_{i=1}^{r}\mathfrak{p}_i^{2\mu_i+2+c_i-d_i+\eta_i-\xi_i}\prod_{h=1}^{s}\mathfrak{q}_h^{\nu_h}=(\beta)\,,\qquad \beta\equiv 1 \bmod \mathfrak{u}$$

for an element β of $\mathfrak{g}$. By Lemma 4.3, there exists an element a_1 of $\mathfrak{o}$ such that $N(a_1)=\beta$ and

(11) $$a_1 \equiv \begin{pmatrix} \pi_i^{\mu_i+1} & 0 \\ 0 & \beta\pi_i^{-\mu_{i'}-1} \end{pmatrix} \mod \beta\mathfrak{p}_i^{\mu_i+e_i+1}\mathfrak{o}_i \qquad (1 \leqq i \leqq r).$$

Let ε be a unit of F such that $\alpha(1-\varepsilon^2) \equiv 1 \bmod \mathfrak{u}$. Such an ε really exists, because $\mathfrak{u}$ is not the product of all the infinite prime spots of F. Then, by our assumption on α, we have

$$\alpha - \varepsilon^{2m} N(a_1)\gamma \equiv 1 \mod \mathfrak{u}$$

for a suitably large integer m. Fix such an m. By Lemma 4.3, there exists an element b_1 of $\mathfrak{o}$ such that $N(b_1) = \alpha - \varepsilon^{2m}N(a_1)\gamma$. By our choice of β, we observe that $\mathfrak{g}_i N(b_1) = \mathfrak{p}_i^{\mu_i}$ for $1 \leqq i \leqq r$. Put $a = \varepsilon^m a_1$. For every prime ideal $\mathfrak{r}$ of F, let $\tilde{\mathfrak{o}}_\mathfrak{r}$ denote the right order of $(\mathfrak{c}^{-1}a^{-1})_\mathfrak{r}$. Let $\{\mathfrak{r}\}$ be the set of prime ideals $\mathfrak{r}$ such that $(\mathfrak{r}, \mathfrak{d} \cdot \prod_{i=1}^{r} \mathfrak{p}_i) = 1$, $\tilde{\mathfrak{o}}_\mathfrak{r} \neq \mathfrak{o}_\mathfrak{r}$. Obviously $\{\mathfrak{r}\}$ is a finite set. For each $\mathfrak{r}$, take an element $b_\mathfrak{r}$ of $\tilde{\mathfrak{o}}_\mathfrak{r} \cap \mathfrak{o}_\mathfrak{r}$ such that $N(b_\mathfrak{r}) = N(b_1)$. This is possible by virtue of Lemma 4.7. Now by Lemma 4.3, we can find an element b of $\mathfrak{o}$ such that $N(b) = N(b_1)$, $b \equiv b_\mathfrak{r} \bmod (\tilde{\mathfrak{o}}_\mathfrak{r} \cap \mathfrak{o}_\mathfrak{r})$ for $\mathfrak{r} \in \{\mathfrak{r}\}$, and

(12) $$b \equiv \begin{pmatrix} 0 & \pi_i^{\xi_i} \\ -N(b_1)\pi_i^{-\xi_i} & 0 \end{pmatrix} \mod \beta\mathfrak{p}_i^{\mu_i+e_i+1}\mathfrak{o}_i \qquad (1 \leqq i \leqq r).$$

Then we have $N(b) + \gamma N(a) = \alpha$, and by (11) and (12),

$$a^{-1}ba = a_1^{-1}ba_1 = \beta^{-1}a_1'ba_1 \equiv \begin{pmatrix} 0 & \beta\pi_i^{\xi_i-2\mu_i-2} \\ -N(b)\beta^{-1}\pi_i^{-\xi_i+2\mu_i+2} & 0 \end{pmatrix} \mod \mathfrak{p}_i^{\mu_i+e_i+1}\mathfrak{o}_i,$$

so that

(13) $$a^{-1}b'a \equiv \begin{pmatrix} 0 & \theta\pi_i^{\eta_i+c_i-d_i} \\ \psi\pi_i^{\mu_i-\eta_i-c_i+d_i} & 0 \end{pmatrix} \mod \mathfrak{p}_i^{\mu_i+e_i+1}\mathfrak{o}_i$$

with units θ and ψ of $\mathfrak{g}_i$. It follows that

(14) $$\mathfrak{c}_i^{-1}(a^{-1}b'a) = \begin{pmatrix} \mathfrak{p}_i^{\mu_i-\eta_i-c_i} & \mathfrak{p}_i^{\eta_i-d_i} \\ \mathfrak{p}_i^{\mu_i-\eta_i-c_i} & \mathfrak{p}_i^{\eta_i-d_i} \end{pmatrix}.$$

Hence we have $\mathfrak{c}_i^{-1}(a^{-1}b'a) \subset \mathfrak{c}_i^{-1}$. By our choice of $b_\mathfrak{r}$, we have $b' \in \tilde{\mathfrak{o}}_\mathfrak{r}$ for every $\mathfrak{r}$ such that $(\mathfrak{r}, \mathfrak{d} \cdot \prod_{i=1}^{r} \mathfrak{p}_i) = 1$, and hence $\mathfrak{c}_\mathfrak{r}^{-1}(a^{-1}b'a) \subset \mathfrak{c}_\mathfrak{r}^{-1}$ for any such $\mathfrak{r}$. Further it is obvious that $\mathfrak{c}_h^{-1}(a^{-1}b'a) \subset \mathfrak{c}_h^{-1}$. Therefore, we have

(15) $$\mathfrak{c}^{-1}(a^{-1}b'a) \subset \mathfrak{c}^{-1}.$$

As $a \in \mathfrak{o} \subset \mathfrak{c}^{-1}$ and $N(\mathfrak{c}) = \gamma\mathfrak{g}$, we have

(15′) $$\mathfrak{c}^{-1}\gamma a' \subset \mathfrak{o}.$$

Moreover, by (11) we have

(16) $$\mathfrak{c}_i^{-1}\gamma a' \subset \mathfrak{p}_i^{\mu_i+1}\mathfrak{o}_i.$$

Now define an element σ of $E(V, A)$ by

(17) $$x\sigma = bx + ay, \qquad y\sigma = -\gamma a'x + a^{-1}b'ay.$$

By the relation $N(b) + \gamma N(a) = \alpha$, we can easily verify that $\sigma \in G(V, f)$ and

$N(\sigma)=\alpha$. Further by (15), (15′), we have $L\sigma\subset L$. By Proposition 2.7, we have $\mathfrak{p}_i^{\mu_i}L_i=\alpha L_i\subset L_i\sigma$, so that

$$\mathfrak{p}_i^{\mu_i+1}L_i\subset\mathfrak{p}_iL_i\sigma\,. \tag{18}$$

Put $M_i=\mathfrak{o}_ibx+\mathfrak{c}_i^{-1}a^{-1}b'ay$. Then we have, by (11), (16), (17), (18) and by Lemma 1.2, $M_i=L_i\sigma$, so that $L_i/L_i\sigma=L_i/M_i\cong\mathfrak{o}_i/\mathfrak{o}_ib+\mathfrak{c}_i^{-1}/\mathfrak{c}_i^{-1}a^{-1}b'a$ (as $\mathfrak{o}_i$-modules). By (12) and (14), $L_i/L_i\sigma$ has the desired elementary divisors. Let us now consider $\mathfrak{q}_h$ for $1\leqq h\leqq s$. As $N(\sigma)=\alpha$ and $\mathfrak{o}_h\alpha=\mathfrak{Q}_h^{2\lambda_h}$, we have, by Proposition 2.7, $L_h\sigma\supset\mathfrak{Q}_h^{2\lambda_h}L_h$. As $N(a_1)=\beta$ and $\mathfrak{g}_h\beta=\mathfrak{q}_h^{\nu_h}$, we have $\mathfrak{o}_ha=\mathfrak{Q}_h^{\nu_h}$. If $\lambda_h=0$, we have $L_h\sigma=L_h$. Suppose that $\lambda_h>0$. If $\nu_h=\lambda_h$, we have $\mathfrak{o}_ha=\mathfrak{Q}_h^{\lambda_h}$ and hence $N(b)=\alpha-\gamma N(a)\in\mathfrak{Q}_h^{2\lambda_h}$. It follows that a, b, $-\gamma a'$, $a^{-1}b'a$ are contained in $\mathfrak{Q}_h^{\lambda_h}$. Hence we have $x\sigma$, $y\sigma\in\mathfrak{Q}_h^{\lambda_h}L_h$, so that $L_h\sigma\subset\mathfrak{Q}_h^{\lambda_h}L_h$. As $L_h\sigma$ is maximal and $N(L_h\sigma)=\mathfrak{Q}_h^{2\lambda_h}=N(\mathfrak{Q}_h^{\lambda_h}L_h)$, we must have $L_h\sigma=\mathfrak{Q}_h^{\lambda_h}L_h$. Then $L_h/L_h\sigma\cong\mathfrak{o}_h/\mathfrak{Q}_h^{\lambda_h}+\mathfrak{o}_h/\mathfrak{Q}_h^{\lambda_h}$. It remains to consider the case $\lambda_h>\nu_h\geqq 0$. As $N(b)+\gamma N(a)=\alpha$, $\mathfrak{o}_ha=\mathfrak{Q}_h^{\nu_h}$, $\mathfrak{o}_h\alpha=\mathfrak{Q}_h^{2\lambda_h}$, we must have $\mathfrak{o}_hb=\mathfrak{Q}_h^{\nu_h}$. It follows that $a'b^{-1}$ is a unit of $\mathfrak{o}_h$. We note that

$$y\sigma+\gamma(a'b^{-1})x\sigma=(a^{-1}b'a+\gamma a'b^{-1}a)y=a^{-1}b^{-1}(bb'+\gamma baa'b^{-1})ay$$
$$=a^{-1}b^{-1}(N(b)+\gamma N(a))ay=\alpha(a^{-1}b^{-1}a)y\,.$$

Therefore we have $L_h\sigma=\mathfrak{o}_hx\sigma+\mathfrak{o}_hy\sigma=\mathfrak{o}_hx\sigma+\mathfrak{o}_h\alpha(a^{-1}b^{-1}a)y$. On the other hand, as $b^{-1}a$ is a unit of $\mathfrak{o}_h$ and as $x=b^{-1}x\sigma-b^{-1}ay$, we have $L_h=\mathfrak{o}_hx+\mathfrak{o}_hy=\mathfrak{o}_hb^{-1}x\sigma+\mathfrak{o}_hy$. Hence $L_h/L_h\sigma\cong\mathfrak{o}_hb^{-1}/\mathfrak{o}_h+\mathfrak{o}_h/\mathfrak{o}_h(a^{-1}b^{-1}a)\alpha=\mathfrak{o}_h/\mathfrak{Q}_h^{\nu_h}+\mathfrak{o}_h/\mathfrak{Q}_h^{2\lambda_h-\nu_h}$ (as $\mathfrak{o}_h$-modules). This completes our proof.

4.6. Global approximation theorem. As in §4.2, we define $\nu_\kappa(f)$ for $1\leqq\kappa\leqq u$, and reorder the $\mathfrak{p}_{\infty\kappa}$ so that $\nu_\kappa(f)\neq n/2$ for $1\leqq\kappa\leqq t$ and $\nu_\kappa(f)=n/2$ for $t<\kappa\leqq u$. Put

$$\mathfrak{t}=\mathfrak{t}_f=\prod_{\kappa=1}^{t}\mathfrak{p}_{\infty\kappa}\,.$$

For every $\sigma\in G(V,f)$, we have $N(\sigma)\equiv 1 \bmod \mathfrak{t}$. If n is odd, we have $t=u$ and $\mathfrak{t}=\mathfrak{u}$.

Now we are ready to state and prove our main theorems.

THEOREM 1. *Suppose that A is indefinite. Let L be a maximal lattice belonging to the principal genus $\mathfrak{L}_0(\mathfrak{o})$. Let $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ be prime ideals of F; and let σ_i, for each i, be an element of $G(V_{\mathfrak{p}_i},f)$ such that $L_{\mathfrak{p}_i}\sigma_i\subset L_{\mathfrak{p}_i}$. Let α be an element of $\mathfrak{g}$. Suppose that*

$$\alpha^{-1}N(\sigma_i)\equiv 1 \mod \mathfrak{p}_i^{\lambda_i}\,,\qquad (1\leqq i\leqq r)\,,$$
$$\alpha\equiv 1 \mod \mathfrak{t}\,,$$

where the λ_i are positive integers. Then there exists an element σ of $G(V,f)$ such that $L\sigma\subset L$, $N(\sigma)=\alpha$, $L_{\mathfrak{p}_i}(\sigma-\sigma_i)\subset\mathfrak{p}_i^{\lambda_i}L_{\mathfrak{p}_i}$ $(1\leqq i\leqq r)$.

We prove Theorem 1 in several steps. For simplicity, we denote $L_{\mathfrak{p}_i}$, $\mathfrak{g}_{\mathfrak{p}_i}$, etc. by L_i, $\mathfrak{g}_i$, etc.

ASSERTION 1. If Theorem 1 is proved when $N(L)=\mathfrak{o}$ for every maximal order $\mathfrak{o}$, then it is true for any L belonging to the principal genus.

In fact, if L belongs to $\mathfrak{L}_0(\mathfrak{o})$, we can find a left $\mathfrak{o}$-ideal $\mathfrak{x}$ such that $N(L)=N(\mathfrak{x})\mathfrak{o}$. Then by Proposition 2.5, $\mathfrak{x}^{-1}L$ is a maximal lattice, and $N(\mathfrak{x}^{-1}L)=\mathfrak{o}_1$, where $\mathfrak{o}_1$ is the right order of $\mathfrak{x}$. We see easily that if Theorem 1 is true for $\mathfrak{x}^{-1}L$, then it is true for L.

ASSERTION 2. If Theorem 1 is true for L, then, for every $\tau\in G(V,f)$, Theorem 1 is true for $L\tau$.

This is clear.

ASSERTION 3. If Theorem 1 is proved for a certain $L^0\in\mathfrak{L}_0(\mathfrak{o})$ such that $N(L^0)=\mathfrak{o}$, then for any $L\in\mathfrak{L}_0(\mathfrak{o})$ such that $N(L)=\mathfrak{o}$, we have $L=L^0\tau$ for an element $\tau\in G^0(V,f)$.

Let β be a non-zero element of $\mathfrak{g}$ such that $\beta L\subset L^0$. Take an integral $\mathfrak{g}$-ideal $\mathfrak{a}$ such that $\beta L\supset\mathfrak{a}L^0$. Let $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ be the prime factors of $\mathfrak{a}$. By Proposition 2.11 and by Proposition 3.7, there exists, for each $\mathfrak{p}_i$, an element τ_i of $G^0(V_i,f)$ such that $L_i^0\tau_i=L_i$. Put $\sigma_i=\beta\tau_i$. Then we have $N(\sigma_i)=\beta^2$. Applying Theorem 1 to L^0 and these σ_i, we get an element σ of $G(V,f)$ such that $L^0\sigma\subset L^0$, $N(\sigma)=\beta^2$, $L_i^0(\sigma-\sigma_i)\subset\mathfrak{p}_i\mathfrak{a}L_i^0$ for $1\leqq i\leqq r$. As we have $\mathfrak{p}_i\mathfrak{a}L_i^0\subset\mathfrak{p}_i\beta L_i=\mathfrak{p}_iL_i^0\sigma_i$, we see, from Lemma 1.2, $L_i^0\sigma=L_i^0\sigma_i=\beta L_i$. If $\mathfrak{p}$ is a prime ideal which does not divide $\mathfrak{a}$, we have $L_{\mathfrak{p}}^0=\beta L_{\mathfrak{p}}$, since $L^0\supset\beta L\supset\mathfrak{a}L^0$. It follows that $N(L_{\mathfrak{p}}^0)=\beta^2N(L_{\mathfrak{p}})$, and hence β is a $\mathfrak{p}$-unit. As $L^0\sigma\subset L^0$ and $N(\sigma)=\beta^2$, we have $L_{\mathfrak{p}}^0\sigma=L_{\mathfrak{p}}^0=\beta L_{\mathfrak{p}}$. Therefore, we have $L_{\mathfrak{p}}^0\sigma=\beta L_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of F, so that $L^0\sigma=\beta L$. Putting $\tau=\beta^{-1}\sigma$, we get $L^0\tau=L$.

ASSERTION 4. In order to prove Theorem 1, we may exchange the Q-hermitian form f for θf for any non-zero element θ of F.

In fact, put $g(x,y)=\theta f(x,y)$ for $(x,y)\in V\times V$. Then g is a non-degenerate Q-hermitian form. We see easily $G(V,f)=G(V,g)$, $G^0(V,f)=G^0(V,g)$, and, for every $\sigma\in G(V,f)$, $N(\sigma)$ is common for f and g. Further, for every $\mathfrak{g}$-lattice L in V, we have $N_g(L)=\theta N_f(L)$. When L is normal, L is maximal with respect to f if and only if L is maximal with respect to g. The genera and the classes of normal maximal lattices do not change by exchanging f for g. Finally we note that $t_f=t_g$. Therefore we get Assertion 4.

Now we proceed by induction on n. If $n=1$, Theorem 1 is just a restatement of Lemma 4.3. Assume that $n>1$ and Theorem 1 is true for $\dim_A V<n$.

ASSERTION 5. If $N(L)=\mathfrak{o}$ and L contains an element x such that $f(x,x)=1$, then Theorem 1 is true for this L and for $\alpha=1$.

As $N(\sigma_i)\equiv 1 \bmod \mathfrak{p}_i^{\lambda_i}$ and $N(L)=\mathfrak{o}$, we have $f(u\sigma_i,v\sigma_i)\equiv f(u,v) \bmod \mathfrak{p}_i^{\lambda_i}\mathfrak{o}_i$ for

$u, v \in L$. By Proposition 3.13, there exists an element τ_i of $G(V_i, f)$ such that $N(\tau_i)=1$, $L_i\tau_i = L_i$, $L_i(\sigma_i - \tau_i) \subset \mathfrak{p}_i^{\lambda_i} L_i$. Put

$$W = \{v \in V \mid f(x, v) = 0\}, \qquad M = W \cap L.$$

Then we have $V = Ax + W$, $L = \mathfrak{o}x + M$; and M is a maximal lattice in W such that $N(M) = \mathfrak{o}$. Put $x\tau_i = a_i x + y_i$ with $a_i \in \mathfrak{o}_i$ and $y_i \in M_i$. As $f(x\tau_i, x\tau_i) = f(x, x) = 1$, we have $N(a_i) + f(y_i, y_i) = 1$. Now reorder the $\mathfrak{p}_i$ so that $N(a_i) \neq 0$ for $1 \leqq i \leqq h$, $N(a_i) = 0$ for $h < i \leqq r$, where h is an integer such that $0 \leqq h \leqq r$. Put $\mathfrak{g}_i N(a_i) = \mathfrak{p}_i^{\mu_i}$ for $1 \leqq i \leqq h$. We can find a regular element a of A such that $a \in \mathfrak{o}$, and

$$a \equiv a_i \mod \mathfrak{o}_i \mathfrak{p}_i^{\lambda_i + \mu_i} \qquad \text{for} \quad 1 \leqq i \leqq h,$$

$$a \equiv a_i \mod \mathfrak{o}_i \mathfrak{p}_i^{\lambda_i} \qquad \text{for} \quad h < i \leqq r.$$

We have then

$$N(a) \equiv N(a_i) \mod \mathfrak{p}_i^{\lambda_i + \mu_i} \qquad \text{for} \quad 1 \leqq i \leqq h,$$

$$N(a) \equiv 0 \mod \mathfrak{p}_i^{\lambda_i} \qquad \text{for} \quad h < i \leqq r,$$

and hence $\mathfrak{g}_i N(a) = \mathfrak{p}_i^{\mu_i}$ for $1 \leqq i \leqq h$. Put $\mathfrak{g}_i N(a) = \mathfrak{p}_i^{\mu_i}$ for $i > h$. We have then $\mu_i \geqq \lambda_i \geqq 1$ for $i > h$. Now, as $1 - N(a) \equiv 1 \mod \mathfrak{p}_i^{\mu_i}$, we can find, by Proposition 3.2, for each $i > h$, an element ε_i of $\mathfrak{o}_i$ such that $\varepsilon_i \equiv 1 \mod \mathfrak{o}_i \mathfrak{p}_i^{\mu_i}$, $N(\varepsilon_i) = 1 - N(a)$. Take an element y of M so that

$$y \equiv y_i \mod \mathfrak{p}_i^{\lambda_i + \mu_i} M_i \qquad \text{for} \quad 1 \leqq i \leqq h,$$

$$y \equiv \varepsilon_i y_i \mod \mathfrak{p}_i^{\lambda_i + \mu_i} M_i \qquad \text{for} \quad h < i \leqq r.$$

Then we can easily verify that $f(y, y) \equiv 1 - N(a) \mod \mathfrak{p}_i^{\lambda_i + \mu_i}$ for every i. Since $\mathfrak{u}$ is not the product of all infinite prime spots of F, the projection of the set $\{\beta \mid \beta = 1 + \xi, \xi \in \prod_{i=1}^{r} \mathfrak{p}_i^{\mu_i + \lambda_i}\}$ on $F_1 \times \cdots \times F_u$ is dense. Hence there exists an element β of $\mathfrak{g}$ such that $1 - \beta^2 \equiv 1 \mod \mathfrak{u}$, $\beta \equiv 1 \mod \prod_{i=1}^{r} \mathfrak{p}_i^{\mu_i + \lambda_i}$. For a suitably large integer k, $1 - \beta^{2k} f(y, y) \equiv 1 \mod \mathfrak{u}$. Put $w = \beta^k y$ for such an integer k. Then we have

$$w \equiv y \mod \prod_{i=1}^{r} \mathfrak{p}_i^{\lambda_i + \mu_i} M,$$

$$1 - f(w, w) \equiv 1 - f(y, y) \equiv N(a) \mod \prod_{i=1}^{r} \mathfrak{p}_i^{\lambda_i + \mu_i},$$

$$1 - f(w, w) \equiv 1 \mod \mathfrak{u}.$$

As $N(a)\mathfrak{g}_i = \mathfrak{p}_i^{\mu_i}$, we have $N(a)^{-1}(1 - f(w, w)) \equiv 1 \mod \prod_{i=1}^{r} \mathfrak{p}_i^{\lambda_i}$. Therefore, by Lemma 4.3, there exists an element b of $\mathfrak{o}$ such that

$$N(b) = 1 - f(w, w), \qquad b \equiv a \mod \prod_{i=1}^{r} \mathfrak{p}_i^{\lambda_i} \mathfrak{o}.$$

Put $u = bx + w$. Then $f(u, u) = N(b) + f(w, w) = 1$, and

$$u \equiv ax+y \equiv a_i x+y_i = x\tau_i \mod \mathfrak{p}_i^{\lambda_i} L_i \qquad (1 \leqq i \leqq r).$$

Hence, putting

$$U = \{z \in V \mid f(u,z)=0\}, \qquad K = U \cap L,$$

we have $V = Au+U$, $L = \mathfrak{o}u+K$; and K is a maximal lattice in U such that $N(K)=\mathfrak{o}$. By Lemma 4.4, (U,f) and (W,f) are isomorphic. Therefore we can find an element ρ of $G^0(V,f)$ such that $x\rho = u$, $W\rho = U$. We see easily that $M\rho$ is a maximal lattice in U and $N(M\rho)=\mathfrak{o}$. By our induction assumption and Assertion 3, there exists an element φ of $G^0(U,f)$ such that $M\rho\varphi = K$. Exchanging ρ for $\rho\varphi$ on W, we may assume that $M\rho = K$ for ρ itself. Then we have $L\rho = L$, and $x\tau_i\rho^{-1} \equiv x \mod \mathfrak{p}_i^{\lambda_i} L_i$. For every $z \in W_i$, denote by $z\psi_i$ the projection of $z\tau_i\rho^{-1}$ onto W_i defined by the decomposition $V_i = A_i x + W_i$. Then ψ_i can be considered as an element of $E(W_i, A_i)$. If $z \in M_i$, we have $f(z\tau_i\rho^{-1}, x) \equiv f(z\tau_i\rho^{-1}, x\tau_i\rho^{-1}) = f(z,x) = 0 \mod \mathfrak{p}_i^{\lambda_i}\mathfrak{o}_i$. It follows that $M_i(\tau_i\rho^{-1}-\psi_i) \subset \mathfrak{p}_i^{\lambda_i}\mathfrak{o}_i x$, and hence $f(z_1\psi_i, z_2\psi_i) \equiv f(z_1, z_2) \mod \mathfrak{p}_i^{\lambda_i}\mathfrak{o}_i$ for $z_1 \in M_i$, $z_2 \in M_i$. By Proposition 3.13, there exists an element θ_i of $G^0(W_i,f)$ such that $M_i\theta_i \subset M_i$ and $M_i(\psi_i-\theta_i) \subset \mathfrak{p}_i^{\lambda_i} M_i$. Applying our induction assumption to M and the θ_i, we find an element θ of $G^0(W,f)$ such that $M\theta \subset M$, $M_i(\theta-\theta_i) \subset \mathfrak{p}_i^{\lambda_i} M_i$ for $1 \leqq i \leqq r$. Define an element σ of $E(V,A)$ by $x\sigma = u$, $z\sigma = z\theta\rho$ for $z \in W$. Then we have $\sigma \in G(V,f)$ and $N(\sigma)=1$, $L\sigma \subset L$. Further, we have

$$x\sigma = u \equiv x\tau_i \equiv x\sigma_i \mod \mathfrak{p}_i^{\lambda_i} L_i \qquad (1 \leqq i \leqq r),$$

and if $z \in M_i$,

$$z\sigma = z\theta\rho \equiv z\theta_i\rho \equiv z\psi_i\rho \equiv z\tau_i \equiv z\sigma_i \mod \mathfrak{p}_i^{\lambda_i} L_i \qquad (1 \leqq i \leqq r).$$

Therefore $L_i(\sigma-\sigma_i) \subset \mathfrak{p}_i^{\lambda_i} L_i$. This completes the proof of Assertion 5.

PROPOSITION 4.9. *Let L be a maximal lattice belonging to $\mathfrak{L}_0(\mathfrak{o})$. Let α be an element of $\mathfrak{g}$ such that $\alpha \equiv 1 \bmod \mathfrak{t}$, and let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be prime ideals of F. Let σ_i, for $1 \leqq i \leqq r$, be an element of $G(V_{\mathfrak{p}_i}, f)$ such that $N(\sigma_i)\mathfrak{g}_{\mathfrak{p}_i} = \alpha\mathfrak{g}_{\mathfrak{p}_i}$, $L_{\mathfrak{p}_i}\sigma_i \subset L_{\mathfrak{p}_i}$. Then there exists an element σ of $G(V,f)$ such that $N(\sigma)=\alpha$, $L\sigma \subset L$, and $L_{\mathfrak{p}_i}/L_{\mathfrak{p}_i}\sigma$ is isomorphic to $L_{\mathfrak{p}_i}/L_{\mathfrak{p}_i}\sigma_i$ as $\mathfrak{o}_{\mathfrak{p}_i}$-modules for $1 \leqq i \leqq r$.*

ASSERTION 6. If Theorem 1 is true, then Proposition 4.9 is true.

In fact, as $N(\sigma_i)^{-1}\alpha$ is a $\mathfrak{p}_i$-unit for each i, there exists, by Proposition 3.3 and Proposition 3.12, an element τ_i of $G(V_i,f)$ such that $L_i\tau_i = L_i$, $N(\tau_i) = N(\sigma_i)^{-1}\alpha$. Then we have $L_i\tau_i\sigma_i \subset L_i$, $N(\tau_i\sigma_i) = \alpha$. By Theorem 1, there exists an element σ of $G(V,f)$ such that $L\sigma \subset L$, $N(\sigma)=\alpha$, $L_i(\sigma-\tau_i\sigma_i) \subset \mathfrak{p}_i^{\lambda_i+1} L_i = \mathfrak{p}_i \alpha L_i$ for every i. By Proposition 2.7, we have $\alpha L_i \subset L_i\tau_i\sigma_i$. Therefore, by Lemma 1.2, we have $L_i\sigma = L_i\tau_i\sigma_i = L_i\sigma_i$. This proves our assertion.

Now exchanging f for θf with a suitable θ of F, if necessary, we may assume that $\nu_\kappa(f) > n/2$ for $1 \leqq \kappa \leqq t$, $\nu_\kappa(f) = n/2$ for $\kappa < t \leqq u$. By Assertion 4, this does not influence the validity of our proof of Theorem 1.

ASSERTION 7. There exists a member L of $\mathfrak{L}_0(\mathfrak{o})$ satisfying the following

conditions: i) $N(L)=\mathfrak{o}$; ii) L contains an element x such that $f(x,x)=1$; iii) Proposition 4.9 is true for L.

To prove this, let $U=Ax+Ay$ be an A-space of dimension 2. We can find an element γ of $\mathfrak{g}$ such that $(\gamma,\mathfrak{d})=1$, $\gamma\equiv 1 \bmod \mathfrak{p}_{\infty\kappa}$ for $1\leqq\kappa\leqq t$, $\gamma\equiv -1 \bmod \mathfrak{p}_{\infty\kappa}$ for $t<\kappa\leqq u$. Define a Q-hermitian form f_0 on U by $f_0(x,x)=1$, $f_0(x,y)=0$, $f_0(y,y)=\gamma$. Now let W be an A-space of dimension $n-2$ and f_1 be a non-degenerate Q-hermitian form on W such that $\nu_\kappa(f_1)=\nu_\kappa(f)-2$ for $1\leqq\kappa\leqq t$ and $\nu_\kappa(f_1)=\nu_\kappa(f)-1$ for $t<\kappa\leqq u$. Then, by Lemma 4.4, (V,f) is isomorphic to the direct sum of (U,f_0) and (W,f_1). Therefore, we may assume that $V=U+W=Ax+Ay+W$, $W=\{z\in V \mid f(x,z)=f(y,z)=0\}$, $f=f_0$ on $U\times U$ and $f=f_1$ on $W\times W$. Further we see easily that $\mathfrak{k}(f_1)$ is a factor of $\mathfrak{k}(f)$. Let $\mathfrak{c}$ be an integral right $\mathfrak{o}$-ideal such that $N(\mathfrak{c})=\mathfrak{g}\gamma$, and let M be a maximal lattice in W such that $N(M)=\mathfrak{o}$. Put

$$K=\mathfrak{o}x+\mathfrak{c}^{-1}y, \qquad L=K+M.$$

Then, K is a maximal lattice in U, L is a maximal lattice in V; and $N(K)=N(L)=\mathfrak{o}$. Now let the notation be as in Proposition 4.9. The structure of the $\mathfrak{o}_i$-module $L_i/L_i\sigma_i$ is determined by Proposition 2.12 and Proposition 3.9. In view of those propositions, we can find an element τ_i of $G(U_i,f_0)$ and an element ρ_i of $G(W_i,f_1)$ such that $N(\tau_i)=\alpha$, $N(\rho_i)=\alpha$, and

$$L_i/L_i\sigma_i\cong K_i/K_i\tau_i\oplus M_i/M_i\rho_i \qquad (1\leqq i\leqq r),$$

where $\cong$ means $\mathfrak{o}_i$-isomorphism. As $\alpha\equiv 1 \bmod \mathfrak{k}(f)$, we have $\alpha\equiv 1 \bmod \mathfrak{k}(f_1)$. By Assertion 6 and by our assumption of induction, there exists an element ρ of $G(W,f_1)$ such that $N(\rho)=\alpha$, $M\rho\subset M$,

$$M_i/M_i\rho\cong M_i/M_i\rho_i \qquad (1\leqq i\leqq r).$$

By Proposition 4.8, there exists an element τ of $G(U,f_0)$ such that $N(\tau)=\alpha$, $K\tau\subset K$, $K_i/K_i\tau\cong K_i/K_i\tau_i$ $(1\leqq i\leqq r)$. Define an element σ of $E(V,A)$ by $z\sigma=z\tau$ for $z\in U$ and $w\sigma=w\rho$ for $w\in W$. Then it is clear that this σ has the required properties of Proposition 4.9. Our assertion is thereby proved.

ASSERTION 8. For every maximal order $\mathfrak{o}$ in A, there exists a member L of $\mathfrak{L}_0(\mathfrak{o})$ for which Theorem 1 is true and $N(L)=\mathfrak{o}$.

We take as L the one which satisfies the conditions i-iii) of Assertion 7. By Assertion 5, Theorem 1 is true for $\alpha=1$, for this L. Now let the notation be as in Theorem 1. Then $\mathfrak{g}_iN(\sigma_i)=\mathfrak{g}_i\alpha$. By Assertion 7, there exists an element τ of $G(V,f)$ such that $N(\tau)=\alpha$, $L\tau\subset L$ and $L_i/L_i\tau$ is isomorphic to $L_i/L_i\sigma_i$ as $\mathfrak{o}_i$-module for $1\leqq i\leqq r$. By Proposition 2.13 and Proposition 3.11, there exists, for each i, an element ε_i of $G^0(V_i,f)$ such that $L_i\varepsilon_i=L_i$, $L_i\tau\varepsilon_i=L_i\sigma_i$. Then we have $L_i\sigma_i\varepsilon_i^{-1}\tau^{-1}=L_i$ and $N(\sigma_i\varepsilon_i^{-1}\tau^{-1})\equiv 1 \bmod \mathfrak{p}_i^{\lambda_i}$. By Assertion 5, there exist elements ρ and η of $G^0(V,f)$ such that $L\rho=L$, $L\eta=L$, $L_i(\rho-\sigma_i\varepsilon_i^{-1}\tau^{-1})\subset\mathfrak{p}_i^{\lambda_i}L_i$, $L_i(\eta-\varepsilon_i)\subset\mathfrak{p}_i^{\lambda_i}L_i$. Put $\sigma=\rho\tau\eta$. We have then $N(\sigma)=\alpha$, $L\sigma\subset L$. If

$z \in L_i$, we have

$$z\sigma \equiv z\rho\tau\eta \equiv z\rho\tau\varepsilon_i \equiv z(\sigma_i\varepsilon_i^{-1}\tau^{-1})\tau\varepsilon_i \equiv z\sigma_i \mod \mathfrak{p}_i^{\lambda_i}L_i,$$

so that $L_i(\sigma-\sigma_i) \subset \mathfrak{p}_i^{\lambda_i}L_i$ for every i. This proves our assertion.

By Assertions 1, 2, 3 and 8, our Theorem 1 is completely proved.

We get a little weaker result than Theorem 1 for general maximal lattices, namely:

THEOREM 2. *Suppose that A is indefinite. Let M be a maximal lattice in V not necessarily belonging to the principal genus. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be distinct prime ideals of F and let α be an element of $\mathfrak{g}$. Let σ_i, for $1 \leqq i \leqq r$, be an element of $G(V_{\mathfrak{p}_i}, f)$. Suppose that $\alpha \equiv 1 \mod \mathfrak{t}$, $M_{\mathfrak{p}_i}\sigma_i \subset M_{\mathfrak{p}_i}$, $N(\sigma_i) = \alpha$ for $1 \leqq i \leqq r$. Then, for any set of positive integers $\{\lambda_1, \cdots, \lambda_r\}$, there exists an element σ of $G(V,f)$ such that $M\sigma \subset M$, $N(\sigma) = \alpha$, $M_{\mathfrak{p}_i}(\sigma-\sigma_i) \subset \mathfrak{p}_i^{\lambda_i}M_{\mathfrak{p}_i}$ for $1 \leqq i \leqq r$.*

PROOF. Let $\mathfrak{o}$ be the order of M. Take a member L of $\mathfrak{L}_0(\mathfrak{o})$. Let $\{\mathfrak{p}_{r+1}, \cdots, \mathfrak{p}_w\}$ be the set of prime ideals $\mathfrak{p}$ of F such that $M_{\mathfrak{p}} \neq L_{\mathfrak{p}}$ and $\mathfrak{p} \notin \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$. For each $\mathfrak{p}_{r+i}$, we can find, in view of Proposition 2.10 and Proposition 3.5, an element σ_{r+i} of $G(V_{r+i}, f)$ such that $M_{r+i}\sigma_{r+i} \subset M_{r+i}$, $N(\sigma_{r+i}) = \alpha$. Take an integral ideal $\mathfrak{a}$ of F such that $\mathfrak{a}L \subset M$, $\mathfrak{a}M \subset L$, $\mathfrak{a}L_k\sigma_k \subset L_k$ for $1 \leqq k \leqq w$. We may assume that the prime factors of $\mathfrak{a}$ belong to $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_r, \mathfrak{p}_{r+1}, \cdots, \mathfrak{p}_w\}$. For a suitably large positive integer h, $\mathfrak{a}^h$ is a principal ideal $\mathfrak{g}\beta$; we have then $\beta L \subset M$, $\beta M \subset L$, $\beta L_k\sigma_k \subset L_k$ for $1 \leqq k \leqq w$. By Theorem 1, there exists an element τ of $G(V,f)$ such that $L\tau \subset L$, $N(\tau) = \beta^2\alpha$, $L_k(\tau-\beta\sigma_k) \subset \beta^3\mathfrak{p}_k^{\lambda_k}L_k$ for $1 \leqq k \leqq w$. Put $\sigma = \beta^{-1}\tau$. Then $N(\sigma) = \alpha$ and $M_k(\sigma-\sigma_k) = \beta^{-1}M_k(\tau-\beta\sigma_k) \subset \beta^{-2}L_k(\tau-\beta\sigma_k) \subset \beta\mathfrak{p}_k^{\lambda_k}L_k \subset \mathfrak{p}_k^{\lambda_k}M_k$ for $1 \leqq k \leqq w$. As $M_k\sigma_k \subset M_k$, this implies $M_k\sigma \subset M_k$ for $1 \leqq k \leqq w$. If $\mathfrak{p} \notin \{\mathfrak{p}_1, \cdots, \mathfrak{p}_w\}$, we have $L_{\mathfrak{p}} = M_{\mathfrak{p}}$, and β is a $\mathfrak{p}$-unit. We have therefore $M_{\mathfrak{p}}\sigma = L_{\mathfrak{p}}\beta^{-1}\sigma = L_{\mathfrak{p}}\tau \subset L_{\mathfrak{p}} = M_{\mathfrak{p}}$. Hence $M_{\mathfrak{p}}\sigma \subset M_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$ of F. It follows that $M\sigma \subset M$. This completes the proof.

4.7. Class-number theorem. For every maximal lattice L in V, put $N^0(L) = N(L) \cap F$. Then $N^0(L)$ is a $\mathfrak{g}$-ideal. If L is a member of $\mathfrak{L}(\mathfrak{o}; \{e_i\})$, we have $N(L) = N^0(L) \cdot \prod_{i=1}^{s} \mathfrak{Q}_i^{-e_i}$.

THEOREM 3. *Suppose that A is indefinite. Then, for every maximal order $\mathfrak{o}$ in A and for every genus $\mathfrak{L}(\mathfrak{o}; \{e_i\})$ of maximal lattices in V, the mapping $L \to N^0(L)$ gives a one-to-one correspondence between the classes of maximal lattices in $\mathfrak{L}(\mathfrak{o}; \{e_i\})$ and the ideal-classes modulo $\mathfrak{t}$ in F.*

Therefore the number of classes in the genus $\mathfrak{L}(\mathfrak{o}; \{e_i\})$ is equal to the number of ideal-classes modulo $\mathfrak{t}$ in F.

PROOF. Let L and M be members of $\mathfrak{L}(\mathfrak{o}; \{e_i\})$. If we have $L\rho = M$ for an element $\rho \in G(V,f)$ we have $N(L)N(\rho) = N(M)$, so that $N^0(L)N(\rho) = N^0(M)$. As $N(\rho) \equiv 1 \mod \mathfrak{t}$, the ideals $N^0(L)$ and $N^0(M)$ belong to the same ideal-class modulo $\mathfrak{t}$ in F. Conversely, suppose that $\alpha N^0(L) = N^0(M)$ for an element $\alpha \in F$

and $\alpha \equiv 1 \bmod \mathfrak{k}$. Let β be an element of $\mathfrak{g}$ such that $\beta M \subset L$. Let $\mathfrak{a}$ be an integral ideal of F such that $\beta M \subset \mathfrak{a}L$. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be the prime factors of $\mathfrak{a}$. As we have $N(\beta M) = \beta^2 \alpha N(L)$, we find, for each $\mathfrak{p}_i$, by Proposition 2.11 and Proposition 3.7, an element σ_i of $G(V_i, f)$ such that $L_i\sigma_i = \beta M_i$, $N(\sigma_i) = \beta^2\alpha$. Since $\beta^2\alpha \equiv 1 \bmod \mathfrak{k}$, we can apply Theorem 2 to $\{L, \sigma_i, \beta^2\alpha\}$. Then we get an element σ of $G(V,f)$ such that $L\sigma \subset L$, $N(\sigma) = \beta^2\alpha$, $L_i(\sigma - \sigma_i) \subset \mathfrak{p}_i\mathfrak{a}L_i$. As $\mathfrak{p}_i\mathfrak{a}L_i \subset \mathfrak{p}_i\beta M_i = \mathfrak{p}_i L_i\sigma_i$, we have $L_i\sigma = L_i\sigma_i = \beta M_i$ by Lemma 1.2. If $\mathfrak{p}$ is a prime ideal which does not divide $\mathfrak{a}$, we have $L_\mathfrak{p} = \beta M_\mathfrak{p}$, because $L \supset \beta M \supset \mathfrak{a}L$. It follows that $N(L_\mathfrak{p}) = \beta^2\alpha N(L_\mathfrak{p})$, and hence $\beta^2\alpha$ is a $\mathfrak{p}$-unit. As $L\sigma \subset L$ and $N(\sigma) = \beta^2\alpha$, we must have $L_\mathfrak{p}\sigma = L_\mathfrak{p} = \beta M_\mathfrak{p}$. Therefore we have $L_\mathfrak{p}\sigma = \beta M_\mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of F, so that $L\sigma = \beta M$. Putting $\tau = \beta^{-1}\sigma$, we get $L\tau = M$. In view of Proposition 4.5, this proves our theorem.

4.8. Classes with respect to $G^0(V, f)$. If we take $G^0(V,f)$ instead of $G(V,f)$, we find that the class-number of each genus is equal to one. In fact, by Theorem 3 and its proof, we obtain easily

PROPOSITION 4.10. *Suppose that A is indefinite. Let L and M be maximal lattices in V with the same order. Then, there exists an element σ of $G^0(V,f)$ such that $L\sigma = M$, if and only if $N(L) = N(M)$.*

Notation being as in § 4.3, let $\mathfrak{G}^0$ be the subgroup of $\mathfrak{G}$ consisting of elements $(\sigma_\mathfrak{p}, \sigma_\kappa)$ such that $\sigma_\mathfrak{p} \in G^0(V_\mathfrak{p}, f)$ for every $\mathfrak{p}$ and $\sigma_\kappa \in G^0(V_\kappa, f)$ for every κ. Then $\mathfrak{G}^0$ can be regarded as the adele-group of $G^0(V,f)$. Put $G^0 = G^0(V,f)$ and $\mathfrak{U}_L^0 = \mathfrak{U}_L \cap \mathfrak{G}^0$. Then Proposition 4.10 implies the equality

$$\mathfrak{G}^0 = \mathfrak{U}_L^0 \cdot G^0$$

for every maximal lattice L in V.

4.9. Elementary divisors of lattices. Let L and M be members of the same genus $\mathfrak{L}(\mathfrak{o}; \{e_i\})$. For every prime ideal $\mathfrak{p}$ of F, we can define, as in § 2.5 and § 3.2, the set of elementary divisors $\{L_\mathfrak{p} : M_\mathfrak{p}\}$. We put $\{L : M\}_\mathfrak{p} = \{L_\mathfrak{p} : M_\mathfrak{p}\}$ and call it the $\mathfrak{p}$-part of the set of elementary divisors of M relative to L. *The* (global) *set of elementary divisors of M relative to L* is defined as the join of $\{L : M\}_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of F and denoted by $\{L : M\}$.

THEOREM 4. *Suppose that A is indefinite. Let L, M, K be maximal lattices in V belonging to the same genus. Then, we have $\{L : M\} = \{L : K\}$ if and only if there exists an element γ of $G^0(V,f)$ such that $L\gamma = L$ and $M\gamma = K$.*

PROOF. The 'if' part is clear. Suppose that $\{L : M\} = \{L : K\}$. Let Ψ be the set of prime ideals $\mathfrak{p}$ of F for which $L_\mathfrak{p} = M_\mathfrak{p} = K_\mathfrak{p}$ does not hold. By Lemma 1.1, Ψ is a finite set. By Proposition 2.13 and Proposition 3.11, there exists, for each $\mathfrak{p} \in \Psi$, an element $\gamma_\mathfrak{p}$ of $G^0(V_\mathfrak{p}, f)$ such that $L_\mathfrak{p}\gamma_\mathfrak{p} = L_\mathfrak{p}$ and

$M_\mathfrak{p}\gamma_\mathfrak{p}=K_\mathfrak{p}$. Take a positive integer c such that $\mathfrak{p}^cM_\mathfrak{p}\subset L_\mathfrak{p}$ and $\mathfrak{p}^cL_\mathfrak{p}\subset K_\mathfrak{p}$ for every $\mathfrak{p}\in\Psi$. By Theorem 2, there exists an element γ of $G(V,f)$ such that $N(\gamma)=1$, $L\gamma\subset L$, $L_\mathfrak{p}(\gamma-\gamma_\mathfrak{p})\subset\mathfrak{p}^{2c+1}L_\mathfrak{p}$ for every $\mathfrak{p}\in\Psi$. Then obviously $L\gamma=L$, and $M_\mathfrak{p}(\gamma-\gamma_\mathfrak{p})\subset\mathfrak{p}^{-c}L_\mathfrak{p}(\gamma-\gamma_\mathfrak{p})\subset\mathfrak{p}\cdot\mathfrak{p}^cL_\mathfrak{p}\subset\mathfrak{p}K_\mathfrak{p}=\mathfrak{p}M_\mathfrak{p}\gamma_\mathfrak{p}$. By Lemma 1.2, we have $M_\mathfrak{p}\gamma=M_\mathfrak{p}\gamma_\mathfrak{p}=K_\mathfrak{p}$ for every $\mathfrak{p}\in\Psi$. If $\mathfrak{p}\notin\Psi$, we have $M_\mathfrak{p}\gamma=L_\mathfrak{p}\gamma=L_\mathfrak{p}=K_\mathfrak{p}$. Hence $M_\mathfrak{p}\gamma=K_\mathfrak{p}$ holds for any prime ideal $\mathfrak{p}$ of F, so that $M\gamma=K$. This proves the 'only if' part.

PROPOSITION 4.11. *Suppose that A is indefinite. Let L and M be maximal lattices in V belonging to the same genus. Define the subgroups $\mathfrak{U}_L$ and $\mathfrak{U}_M$ of the adele-group $\mathfrak{G}$ as in* § 4.3. *Put $\Gamma_L=\mathfrak{U}_L\cap G$, $\Gamma_M=\mathfrak{U}_M\cap G$. Then we have, for every $\xi\in\mathfrak{G}$,*

$$\mathfrak{U}_L\xi\mathfrak{U}_M=\mathfrak{U}_L\xi\Gamma_M=\Gamma_L\xi\mathfrak{U}_M.$$

PROOF. It is clear that $\mathfrak{U}_L\xi\mathfrak{U}_M\supset\mathfrak{U}_L\xi\Gamma_M$. Let u be an element of $\mathfrak{U}_M$. As $Mu=M$, we see easily, on account of the definition of $\mathfrak{U}_M$, that $\{M:L\xi u\}=\{M:L\xi\}$. By Theorem 4, there exists an element γ of Γ_M such that $L\xi u=L\xi\gamma$. It follows that $\mathfrak{U}_L\xi u=\mathfrak{U}_L\xi\gamma\subset\mathfrak{U}_L\xi\Gamma_M$. This shows $\mathfrak{U}_L\xi\mathfrak{U}_M\subset\mathfrak{U}_L\xi\Gamma_M$, and hence $\mathfrak{U}_L\xi\mathfrak{U}_M=\mathfrak{U}_L\xi\Gamma_M$. Similarly we get $\mathfrak{U}_M\xi^{-1}\mathfrak{U}_L=\mathfrak{U}_M\xi^{-1}\Gamma_L$, so that $\mathfrak{U}_L\xi\mathfrak{U}_M=\Gamma_L\xi\mathfrak{U}_M$. This completes the proof.

The above theorem and proposition are generalization of [**9**, Proposition 1.4, Proposition 2.3]. These are necessary for our future investigation of the Hecke-ring of G.

Osaka University

References

[1] A. Borel, Some properties of adele groups attached to algebraic groups, Bull. Amer. Math. Soc., **67** (1961), 583-585.

[2] N. Bourbaki, Algèbre, Chap. 9, Formes sesquilinéaires et formes quadratiques, Hermann, Paris, 1959.

[3] M. Eichler, Quadratische Formen und orthogonale Gruppen, Berlin-Göttingen-Heidelberg (Springer), 1952.

[4] M. Eichler, Die Ähnlichkeitsklassen indefiniter Gitter, Math. Z., **55** (1952), 216-252.

[5] M. Eichler, Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen, J. Reine Angew. Math., **179** (1938), 227-251.

[6] M. Kneser, Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen, Arch. Math., **7** (1956), 323-332.

[7] K. G. Ramanathan, Quadratic forms over involutorial division algebras, J. Indian Math. Soc., **20** (1956), 227-257.

[8] G. Shimura, On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. Japan, **13** (1961), 275-331.

[9] G. Shimura, On Dirichlet series and abelian varieties attached to automorphic

forms, Ann. Math., **76** (1962), 237-294.

[10] T. Tsukamoto, On the local theory of quaternionic anti-hermitian forms, J. Math. Soc. Japan, **13** (1961), 387-400.

[11] A. Weil, Discontinuous subgroups of classical groups, lecture note, Univ. of Chicago, 1958.

[12] A. Weil, Adeles and algebraic groups, lecture note, Institute for Advanced Study, Princeton, 1961.