Arithmetic of special unitary groups and their symplectic representations

Dedicated to Professor Shôkichi Iyanaga on his 60th birthday

By Kenichi IYANAGA

PREFACE*

The main purpose of this paper is to establish a relation between the arithmetic of Hermitian vector spaces and that of alternating vector spaces and to give an application to the theory of automorphic functions, using the theory of "symplectic representations" developed by I. Satake (cf. [20] etc.).

Let k be an algebraic number field of finite degree and K a quadratic extension of k. Let (V, H) be a non-degenerate Hermitian vector space defined over K/k, and let L be a lattice in V. The first problem is to obtain a system of invariants for the class of L with respect to the "SU-equivalence relation" (see 3.2, Chapter I). Using the results obtained by G. Shimura [24], and by R. Jacobowitz [13], we get a solution for a "modular lattice" L, under some conditions (Theorem 6.9, Chapter I).

Incidentally, these considerations enable us to obtain some results about the rational boundary components of the symmetric bounded domains of type (I) (Theorems 1.9 and 1.12, Chapter III).

In Chapter II, we look at a functor $\mathscr{R}_{K/k}\circ\Lambda^r$ which sends the Hermitian vector space (V, H) to an alternating vector space (V', A') defined over k; there exists a lattice L' in V' which corresponds naturally to L. Moreover, the functor gives rise to the "symplectic representation" ρ which maps $G_k=SU(V, H)$ into $G_k'=Sp(V', A')$. The elementary divisors of the lattice L' can be described in terms of the invariants of L, under certain conditions (Theorem 2.8, Chapter II).

Again under some conditions, the algebraic groups G and G' determine symmetric bounded domains D and D', and G_L and $G'_{L'}$ operate properly discontinuously on D and D' respectively (where, $G_L=\{g\in G_k | gL=L\}$ etc.); the representation ρ induces a "holomorphic imbedding" of D into D' such that we have

* This paper has been submitted as dissertation for Ph. D. in the University of Chicago, in Sept. 1967.

$\rho(G_L)\subset G'_{L'}$. This situation gives rise to a problem: under what condition is it possible to "extend" an automorphic form on D with respect to G_L to one on D' with respect to $G'_{L'}$?

A partial answer to this problem is given in Theorem 2.10 and its Corollary in Chapter III, which deals with the automorphic functions. To explain the result, let F be the field of automorphic functions with respect to G_L and let F' be the subfield of F consisting of those functions which can be extended to automorphic functions on D' with respect to $G'_{L'}$. And now for the sake of simplicity, let us assume that k is the field or rational numbers and K is an imaginary quadratic number field. Then, under some conditions, the field F becomes a finite Abelian extension of the field F' and the Galois group of the extension F/F' is isomorphic to a subgroup of the first Galois cohomology $H^1(\mathscr{G}, (\zeta_n))$, where $n=\dim V$, $(\zeta_n)=$the group of n-th roots of unity generated by ζ_n, and $\mathscr{G}$ is the Galois group of the extension K'/K, where K' is a Kummer extension of $K(\zeta_n)$ determined by a certain arithmetic group.

A similar problem was discussed by I. Sakata in [21] (for the case where G is a certain orthogonal group and ρ is a spin representation). We also wish to refer the reader to [9], [14].

I was able to prepare this paper under the guidance of Professor I. Satake to whom I am most grateful. I should also like to express my gratitude to Professors W. L. Baily, Jr., H. Hijikata, S. Iyanaga, S. MacLane and O.F.G. Schilling.

TABLE OF CONTENTS

NOTATION

Z: rational integers.

Q: rational numbers.

R: real numbers.

C: complex numbers.

k: the quotient field of a Dedekind domain $\mathcal{O}_k$, whose characteristic is not 2.

K: a semi-simple algebra over k such that $[K:k]\leqslant 2$.

$\mathcal{O}_K$: the $\mathcal{O}_k$-integral elements of K.

K^*: the invertible elements of K.

U_K: the group of units of $\mathcal{O}_K$.

We have three possibilities for our K:

(1) K is equal to k. (This does not mean that we are going into the theory of quadratic forms. It is only to get a unified description of the theory of $\mathcal{O}_K$-lattices that we include this case.)

(2) K is a separable quadratic extension of k.

(3) K is the direct sum of two copies of k. (So K is a commutative ring with unity $1=e_1+e_2$, where $e_1=(1,0)$ and $e_2=(0,1)$. We can identify an element a of the field k with the element (a,a) of K.)

For the cases (2) and (3), we denote by σ the non-trivial involution of K which fixes the elements of k. For any element a in K, we put $N(a)=a^\sigma\cdot a$, and $\mathrm{Tr}(a)=a^\sigma+a$.

By V, W etc., we denote free K-modules of finite rank. By $E(V)$, we mean the ring of all K-endomorphisms of V, and by $GL(V)$, the group of all invertible elements in $E(V)$. As usual, $SL(V)$ is the subgroup of $GL(V)$ formed by the elements with determinant equal to one. Sometimes, to emphasize K, we write $E(V)_K$, $GL(V)_K$ etc., in stead of $E(V)$, $GL(V)$ etc.

For any set S, we denote by $|S|$ the order of S.

Finally, for positive integers n and m, we denote by (n, m) the G.C.D. of n and m.

CHAPTER I

PRELIMINARIES ON THE ARITHMETIC OF HERMITIAN VECTOR SPACES

1. $\mathcal{O}_K$-lattices

1.1. An $\mathcal{O}_K$-module L is an *$\mathcal{O}_K$-lattice in V* if it is a finitely generated $\mathcal{O}_K$-submodule of the free K-module V and $KL=V$. We define $\mathrm{rk}(L)=\mathrm{rank}(V)$. A lattice in the K-module K is a *fractional ideal* in K. It is well known that a lattice L in V can be written as

$$L=\mathcal{A}_1 v_1 \oplus \cdots \oplus \mathcal{A}_n v_n\,, \qquad \text{(direct sum)}$$

for suitable elements v_i's in V and fractional ideal $\mathcal{A}_i$'s in K, and that the ideal class of $\prod_{i=1}^{n}\mathcal{A}_i$ is uniquely determined by L. Moreover, we can choose the system of elements $\{v_1, \cdots, v_n\}$ so that we have $\mathcal{A}_1=\cdots=\mathcal{A}_{n-1}=\mathcal{O}_K$ [8, § 22, Chapter III].

An element v of a lattice L is *primitive* if it satisfies

$$\{a\in K \mid av\in L\}=\mathcal{O}_K\,.$$

1.2. PROPOSITION.[1] *If* $\mathrm{rk}(L)\geqslant 2$, *then L is generated by its primitive elements.*

PROOF. It is enough to consider the case where K is a field. We may also assume that $\mathrm{rk}(L)=2$ and that $L=\mathcal{O}_K v_1\oplus\mathcal{A}v_2$, where $\mathcal{A}$ is a fractional ideal generated by 1 and a. It is known that there exists an element c in $\mathcal{O}_K$ such that $c\cdot\mathcal{O}_K+\mathcal{A}^{-1}=\mathcal{O}_K$.

Put $w_1=v_1$, $w_2=v_1+av_2$, and $w_3=cv_1+v_2$. Then w_i's are primitive and they generate L.

1.3. If G is a subgroup of $GL(V)$, we put

$$G_L=\{g\in G \mid gL=L\}\,.$$

1.4. LEMMA.[1] *If* $\mathrm{rk}(L)\geqslant 2$, *then $SL(V)_L$ acts transitively on the set of primitive elements of L.*

[1] These statements are well known. Here, for the sake of completeness, we sketch an outline of proofs, which are due to I. Satake. Also see [19].

PROOF. Let v and v' be primitive elements of L. Then we have

$$L=\mathcal{O}_K v_1 \oplus \cdots \oplus \mathcal{O}_K v_{n-1} \oplus \mathscr{A} v_n = \mathcal{O}_K v_1' \oplus \cdots \oplus \mathcal{O}_K v_{n-1}' \oplus \mathscr{A} v_n' ,$$

where $v_1=v, v_1'=v'$ and $\mathscr{A}$ is a fractional ideal. Hence we have an element g in $GL(V)_L$ sending v to v'. As $\det(g)$ belongs to U_K, we can define an element g' of $GL(V)_L$ by putting

$$g'(v_n')=\det(g)^{-1}\cdot v_n', \quad g'(v_i')=v_i' \quad \text{for all} \quad i\neq n .$$

Then $g'g$ is an element of $SL(V)_L$ sending v to v'.

1.5. LEMMA.[1] *Let L and L' be lattices in V and G a subgroup of $GL(V)$. Suppose that for any fractional ideal $\mathscr{A}'$ in K, G_L acts transitively on the set of primitive elements of $\mathscr{A}'L'$, and that $G_{L'}$ stabilizes L. Then there exists a fractional ideal $\mathscr{A}$ in K such that $L'=\mathscr{A}L$.*

PROOF. We may assume that $\mathrm{rk}(L)\geqslant 2$. Put

$$\begin{aligned} \mathscr{A} &= \{a\in K \mid aL\subset L'\} \\ &= \bigcap_e \mathscr{A}_e, \text{ where } e \text{ runs over all the primitive elements} \end{aligned}$$

in L and $\mathscr{A}_e=\{a\in K \mid ae\in L'\}$. (Proposition 1.2.)

Suppose v is any primitive element in the lattice $\mathscr{A}_e^{-1}L'$. Since e is primitive in $\mathscr{A}_e^{-1}L'$, we have an element g of $G_{L'}$ sending e to v. But

$$G_{L'}\subset GL(V)_L .$$

Therefore $v\in L$, which implies that $\mathscr{A}_e^{-1}L'\subset L$. (Proposition 1.2.) Hence, $L'\subset(\bigcap \mathscr{A}_e)L = \mathscr{A}L\subset L'$, which completes the proof.

1.6. Let L and L' be two lattices in V. We define $d(L, L')$ to be the fractional ideal generated by $\det(g)$ where g runs over the elements of $E(V)$ sending L into L'.

2. Arithmetic subgroups of linear groups

2.1. A subgroup Γ of a group $G\subset GL(V)$ is *arithmetic* (*with respect to L*) if there exists a lattice L in V such that Γ and G_L are commensurable.

2.2. PROPOSITION.[1] *$SL(V)_L$ is a maximal arithmetic subgroup of $SL(V)$.*

PROOF. Suppose Γ is an arithmetic subgroup of $SL(V)$ containing $SL(V)_L$.

Then there exists a lattice M such that $SL(V)_M \supset \Gamma$. Hence Lemma 1.5 implies that $M = \mathcal{A}L$. Hence $SL(V)_M = SL(V)_L$, which completes the proof.

2.3. PROPOSITION. *Let K be an algebraic number field of finite degree. Suppose L and M are lattices in the vector spaces V and W respectively. Let G be an algebraic subgroup of $GL(V)_C$ defined over K such that G_L is a maximal arithmetic subgroup of G_K. Suppose that we are given a rational homomorphism ρ of G into $GL(W)_C$, defined over K, which satisfies:*

(1) $\rho(G_L) \subset GL(W)_M$,

(2) $\operatorname{Ker} \rho \subset G_L$.

Then we have $\rho(G_L) = \rho(G)_M$.

PROOF.[2] By a result of A. Borel-Harish-Chandra, $\rho(G_L)$ is arithmetic subgroup of $\rho(G)_K$ (cf. [3], [5]). Hence we get

$$[\rho(G)_M : \rho(G_L)] < \infty .$$

Then the condition (2) implies that

$$[\rho^{-1}(\rho(G)_M) : G_L] < \infty .$$

Hence $\rho^{-1}(\rho(G)_M)$ is arithmetic, so by the maximality of G_L, is equal to G_L. This completes the proof.

2.4. COROLLARY. *Suppose ρ: $SL(V)_C \to GL(W)_C$ is a rational homomorphism defined over K such that*

(1) $\rho(SL(V)_L) \subset GL(W)_M$,

(2) $\operatorname{Ker} \rho$ *is finite.*

Then we have $\rho(SL(V)_L) = \rho(SL(V))_M$.

PROOF. This follows Proposition 2.3 immediately, since in this case, $\operatorname{Ker} \rho$ is contained in the center of $SL(V)$ which consists of all $a \cdot 1_n$ with $a^n = 1$ and $a \in K$; clearly we have $a \cdot 1_n \in SL(V)_L$.

3. Lattices in a Hermitian vector space

3.1. From now on, whenever we consider a Hermitian vector space, we assume that $[K : k] = 2$.

A k-bilinear form H of $V \times V$ into K is *Hermitian form over K/k* if

(1) $H(ax, by) = a^\sigma \cdot H(x, y) \cdot b$,

[2] This proof is due to H. Hijikata.

(2) $H(x, y)=H(y, x)^{\sigma}$, for $x, y \in V$ and $a, b \in K$.
H is *non-degenerate* if for any torsion free element x of V we have $H(x, V)=K$. From now on we always assume that H is non-degenerate. The pair (V, H) is *Hermitian vector space over K/k.*

(V, H) and (V', H') are *isomorphic* if there exists a K-isomorphism g of V onto V' such that

$$H(x, y)=H'(g(x), g(y)), \quad \text{for} \quad x, y \in V.$$

The group of automorphism of the Hermitian vector space (V, H) is denoted by $U(V, H)$. We put $SU(V, H)=U(V, H) \cap SL(V)$.

3.2. Suppose we are given Hermitian vector spaces (V, H) and (V', H') and lattices L and L' in V and V' respectively.

L and L' are *unitary equivalent* if there exists a K-isomorphism g of V onto V' inducing isomorphism of (V, H) and (V', H') and $gL=L'$. And in this case we write $L \sim L'$. If L and L' are lattices in the same Hermitian vector space V and there exists an element g of $SU(V, H)$ sending L onto L', then we say that L and L' are *SU-equivalent* and write $L \approx L'$.

3.3. Suppose we are given a Hermitian vector space (V, H) and a lattice L in V. We put

$$\begin{aligned} C(K/k) &= \{\det(g) \mid g \in U(V, H)\} \\ &= \{a \in K \mid N(a)=1\}, \\ C_L(K/k) &= \{\det(g) \mid g \in U(V, H)_L\}. \end{aligned}$$

If L' is also a lattice in V, and we have $L \sim L'$ and $C(K/k)=C_L(K/k)$, then it is clear that we have $L \approx L'$.

On the other hand, if we have
(1) $C(K/k) \subset U_K$,
(2) $L=\mathcal{O}v \perp L_1$, (orthogonal sum),
then, clearly, $C(K/k)=C_L(K/k)$.

3.4. From now on we assume that V is supplied with a non-degenerate Hermitian form H. For a lattice L in V, we define

$$\mu(L)=\text{the fractional ideal in } K \text{ generated by } H(x)=H(x, x),\ x \in L,$$

$$\mu_0(L)=\text{the fractional ideal in } K \text{ generated by } H(x, y),\, x, y\in L.$$

They are σ invariant ideals. We call $\mu(L)$ the *norm* of L. L is *maximal* if it is maximal among the lattices with the same norm.

The *different* ∂ *of* K/k is defined by

$$\partial^{-1}=\{a\in K \mid \mathrm{Tr}(a\mathcal{O}_K)\subset\mathcal{O}_K\} .$$

As in [26], we look at

$$H(x+ay)=H(x)+H(ay)+\mathrm{Tr}(aH(x, y)) ,$$

and get

$$\mu(L)\subset\mu_0(L)\subset\mu(L)\partial^{-1} .$$

We call L to be *normal* if we have $\mu(L)=\mu_0(L)$.

3.5. We define *the dual of* L to be

$$L^\sharp=\{x\in V \mid H(L, x)\subset\mathcal{O}_K\} .$$

If

$$L=\mathscr{A}_1v_1\oplus\cdots\oplus\mathscr{A}_nv_n ,$$

then

$$L^\sharp=\mathscr{A}_1^{-\sigma}u_1\oplus\cdots\oplus\mathscr{A}_n^{-\sigma}u_n , \quad \text{where} \quad H(v_i, u_j)=\delta_{ij} .$$

And we have

$$d(L^\sharp, L)=\prod_{i=1}^{n} N(\mathscr{A}_i)\cdot(\det(H(v_i, v_j)))\subset\mu_0(L)^n .$$

Also it is clear that

$$L\subset\mu_0(L)\cdot L^\sharp .$$

(cf. [16 § 82, Chapter VIII]).

4. Modular lattices

4.1. Let L be a lattice in V. The following conditions are equivalent.

(1) $L=\mu_0(L)\cdot L^\sharp$,

(2) $d(L^\sharp, L)=\mu_0(L)^n$, $(n=\mathrm{rk}(L))$.

L is ($\mu_0(L)$-) *modular* if it satisfies either one of the above conditions. (Cf. [16, ibid.]). And in this case, $\mu_0(L)$ is called the *modulus* of L.

4.2. Suppose that $\mathcal{O}_K$ is a principal ideal ring (i.e. any ideal in $\mathcal{O}_K$ is principal). Then a lattice with $\mathcal{O}_K$-basis $\{v_1, \cdots, v_n\}$ is modular if and only if the matrix $(H(v_i, v_j))$ has elementary divisor of the form $((a), \cdots, (a))$. And again an $\mathcal{O}_K$-lattice L is modular if and only if we have $H(x, L)=\mu_0(L)$ for any primitive element x in L. (Cf. [16, ibid.]).

4.3. Suppose now that $\mathcal{O}_K$ is a discrete valuation ring. Then a lattice L can be decomposed into orthogonal sum of sublattices L_i's such that L_i's are modular and $\mathrm{rk}\,(L_i)\leqslant 2$ for all i. If, moreover, L is modular and $\mathrm{rk}\,(L_i)=1$ for some i, then L is normal. On the other hand if L is normal then we can assume that $\mathrm{rk}(L_1)=1$.

Hence if L is normal and K is a quadratic extension of k, then by 1.3 we have $C(K/k)=C_L(K/k)$. (Cf. [13], [24]).

4.4. REMARK. If L is modular and $\mu(L)=\delta\cdot\mu_0(L)$, then L is maximal. But not all the maximal lattices are modular. For example, if $k=Q_2=$ 2-adic number field, $K=Q_2(\sqrt{-3})$, and V is spanned by v_1, v_2;

$$(H(v_i, v_j))=\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix},$$

then V has maximal lattices but it has no modular lattices.

5. Local theory of modular lattices

5.1. In this section, we let k be a $\mathfrak{p}$-adic number field and $[K:k]=2$. So, K/k is either unramified or ramified or split. (i.e. $K=k\times k$).

The following Proposition follows immediately from [13], [24].

5.2. PROPOSITION. *Let L and L' be modular lattices in V. Then*
(1) $L\sim L'$ *if and only if* $\mu(L)=\mu(L')$ *and* $\mu_0(L)=\mu_0(L')$.
(2) *Suppose K/k does not split and L and L' are normal. Then $L\sim L'$ implies $L\approx L'$. Especially if K/k is unramified then $L\approx L'$ if and only if $\mu_0(L)=\mu_0(L')$.*
(3) *Suppose K/k splits. Then $L\approx L'$ if and only if $d(L, L')=\mathcal{O}_K$.*

PROOF. For the sake of completeness, we sketch a proof.

Firstly, assume that K/k splits. Then, as the different of K/k is equal to $\mathcal{O}_K$, 3.4 and 4.3 imply that any lattice has an orthogonal basis. From this it is easy to see that there exists a similitude g sending the modular lattice L onto L' so that

$d(L, L') = d(L, gL) = (\det(g))$. (3) follows from this easily. Also in this case we can see easily that $L \sim L'$ if and only if $\mu_0(L) = \mu_0(L')$. Hence we can assume that K/k does not split.

Now by a general result by Jacobowitz [13], L and L' are unitary equivalent if and only if $\mu(L) = (L')$, $\mu_0(L) = \mu_0(L')$ and

$$\det(H(v_i, v_j)) \equiv \det(H(v_i', v_j')) \mod. N(U_K),$$

where $\{v_1, \cdots, v_n\}$ and $\{v_1', \cdots, v_n'\}$ are the basis for L and L' respectively. But now we have (by 4.2)

$$\det(H(v_i, v_j)) = a^n u \equiv \det(H(v_i', v_j'))(= a^n u') \mod. N(K^*),$$

where $u, u' \in U_K$.

(1) follows from this, because now we have $N(K^*) \cap U_K = N(U_K)$.

(2) follows immediately from 3.3 and 4.3.

5.3. PROPOSITION. *Suppose that K/k is ramified and $\mathfrak{p}$ does not divide 2. If we are given modular lattices L and L' in V which are not normal, then*

(1) Ind (H) = Witt index of $H = \dim V/2$, $\mu_0(L) = \mathfrak{P}^s$, *for an odd s.* $(\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^2)$.

(2) *$L \sim L'$ if and only if $\mu_0(L) = L_0(L')$.*

(3) *If g belongs to $U(V, H)$ then* $\det(g)$ *is a unit and congruent to* ± 1 mod. $\mathfrak{P}$.

(4) *Suppose $L \sim L'$ and g is any element of $U(V, H)$ sending L onto L'. Then* $\det(g) \equiv 1$ mod. $\mathfrak{P}$ *if and only if $L \approx L'$.*

PROOF. (1) and (2) are shown in [13].

To show (3), take an element g of $U(V, H)$. $N(\det(g)) = 1$ therefore $\det(g)$ is a unit. As usual we write

$$\det(g) = u_0 + u_1 \Pi + u_2 \Pi^2 + \cdots,$$

where Π is a generator of $\mathfrak{P}$ such that $\Pi^2 \in k$, and $u_i \in \mathcal{O}_K$; representatives of $\mathcal{O}_K/\mathfrak{P}$. Then

$$N(\det(g)) = u_0^2 + \cdots = 1,$$

therefore

$$\det(g) \equiv u_0 \equiv \pm 1 \mod. \mathfrak{P}.$$

To show (4), we take a basis of L such that the matrix of the form H is

$$\pi^* \begin{pmatrix} 0 & \Pi 1_m \\ -\Pi 1_m & 0 \end{pmatrix} \text{ where } \pi = \Pi^2, \quad 2\mathrm{m} = \dim V.$$

Then it is known that the group $U(V, H)_L$ is generated by the matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & {}^tA^{-\sigma} \end{pmatrix}, \begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

where $A \in GL(m, \mathcal{O}_K)$, $B \in M(m, \mathcal{O}_K)$ such that ${}^tB^\sigma = B$. (Cf. [24], [26, Satz C]). Hence, if g belongs to $U(V, H)_L$ then $\det(g)$ is congruent to 1 mod. $\mathfrak{P}$.

Now suppose that $L \approx L'$ and let g be as in (4). There exists an element h of $SU(V, H)$ sending L onto L', so that $h^{-1}g$ belongs to $U(V, H)_L$. Hence $\det g \equiv 1$ mod. $\mathfrak{P}$.

To show the converse, let $\{v_1, \cdots, v_m; v_1', \cdots, v_m'\}$ be the basis of L mentioned above. Suppose g is as in (4) and let $\det(g)$ be congruent to 1 mod. $\mathfrak{P}$. Then it is easy to see that there exists an element u of U_K which is also congruent to 1 mod. $\mathfrak{P}$, and $u^2 = \det(g)$. We define an element h of $U(V, H)_L$ by

$$h(v_1) = u^{-1}v_1\,, \qquad h(v_1') = u^{-1}v_1'\,, \qquad h(v_i) = v_i\,, \qquad h(v_i') = v_i' \;\; (i \geqslant 2)\,.$$

By our choice of u, we have $N(u) = 1$, which implies that h belongs to $U(V, H)_L$. Thus we get the element $g \cdot h$ of $SU(V, H)$ sending L onto L'.

6. Global theory of modular lattices

6.1. In this section, we let k be an algebraic number field of finite degree and K be a quadratic extension of k. V is a finite dimensional vector space over K supplied with a non-degenerate Hermitian form H.

For any valuation v of k, we put $K_v = K \otimes K_v$, $V_v = V \otimes k_v$. V_v is supplied with a non-degenerate Hermitian form H_v which is the natural extension of the form H to V. If in particular, v is determined by a prime ideal $\mathfrak{p}$ (resp. an infinite place $\mathfrak{p}_{\infty,\lambda}$, $1 \leqslant \lambda \leqslant d$) of k, we write $K_v = K_\mathfrak{p}$ (resp. $K_v = K_\lambda$)

For an $\mathcal{O}_K$-lattice L in V, we put $L_\mathfrak{p} = L \otimes \mathcal{O}_\mathfrak{p}$. We have $\mu(L_\mathfrak{p}) = \mu(L)_\mathfrak{p}$, $\mu_0(L_\mathfrak{p}) = \mu_0(L)_\mathfrak{p}$, $(L_\mathfrak{p})^\sharp = (L^\sharp)_\mathfrak{p}$, and for any other $\mathcal{O}_K$-lattice L' in V, we have $d(L_\mathfrak{p}, L_\mathfrak{p}') = d(L, L')_\mathfrak{p}$.

Hence L is $\mathscr{A}$-modualar if and only if $L_\mathfrak{p}$ is $\mathscr{A}_\mathfrak{p}$-moduar for all the prime ideals $\mathfrak{p}$ in k.

Finally we put

$$L_A = \prod_{\mathfrak{p}} L_\mathfrak{p} \times \prod_{\lambda=1}^{d} V_\lambda\,.$$

6.2. Let $\tilde{G}$ be a linear algebraic group defined over k, whose k-rational points coincide with $U(V, H)$. Then we can consider the adèlized group $\tilde{G}_A$, where A denotes the adèle ring of k.

We say that the lattices L and L' belong to the same *genus* (with respect to $\tilde{G}$) if there exists an element g of $\tilde{G}_A$ sending L_A onto L_A'. In other words, L and L' belong to the same genus if and only if $L_{\mathfrak{p}} \sim L_{\mathfrak{p}}'$ for all the prime ideals $\mathfrak{p}$ in k.

6.3. PROPOSITION. *The number of genera among the $\mathscr{A}$-modular lattices is finite. Denoting by $g(\mathscr{A}, V)$ such a number, we have $g(\mathscr{A}, V) \leqslant 1$ if either* dim V *is odd or K/k is unramified.*

PROOF. By 3.4, 5.2 and 5.3, we have

$$L_{\mathfrak{p}} \sim L_{\mathfrak{p}}' \quad \text{if} \quad \mu_0(L_{\mathfrak{p}}) = \mu_0(L_{\mathfrak{p}}') \,,$$

except for the primes $\mathfrak{p}$ which ramify and divide 2. Suppose $\mathfrak{q}$ is one of such exceptional primes. Then, again by 5.2 we have

$$L_{\mathfrak{q}} \sim L_{\mathfrak{q}}' \quad \text{if} \quad \mu_0(L_{\mathfrak{q}}) = \mu_0(L_{\mathfrak{q}}') \quad \text{and} \quad \mu(L_{\mathfrak{q}}) = \mu(L_{\mathfrak{q}}').$$

But 3.4 implies that there are only finite number of posibilities for $\mu(L_{\mathfrak{q}})$'s if $\mu_0(L_{\mathfrak{q}})$ is fixed. Thus $g(\mathscr{A}, V)$ is finite. The last statement is clear from the above argument.

6.4. Let $\tilde{G}$ be as in 6.2. For a lattice L in V, we put

$$\tilde{G}_{A \cdot L} = \prod_{\mathfrak{p}} (G_{k_{\mathfrak{p}}})_{L_{\mathfrak{p}}} \times \prod_{\lambda=1}^{d} G_{K_\lambda} \,.$$

Clearly, there exists a bijective correspondence between the double coset space $\tilde{G}_k \backslash \tilde{G}_A / \tilde{G}_{A, L}$ and the set of unitary equivalence class of lattices belonging to the same genus as L. By a well-known result by A. Borel-Harish-Chandra [5], the number of classes is finite. We denote such a number by $c((L), V)$, where (L) means the genus of L.

6.5. Let us denote by $h(\mathscr{A}, V)$ the number of unitary equivalence classes among the $\mathscr{A}$-modular lattices in V. By 6.3 and 6.4, $h(\mathscr{A}, V)$ is finite. In particular, if $g(\mathscr{A}, V) = 1$, then we can write $h(\mathscr{A}, V) = c(\mathscr{A}, V)$.

6.6. The Hermitian from H is *definite* if $K_\lambda = C$ and Ind$(H_\lambda) = 0$, for all the infinite places $\mathfrak{p}_{\infty, \lambda}$ of k. Otherwise, H is *indefinite*.

6.7. It has been shown by Shimura [24] that if our non-degenrate Hermitian form is indefinite and dim $V>1$, then for a lattice L in V,

$$c((L), V)=[\underline{C} : \underline{C}'] \quad \text{or} \quad [\underline{C} : \underline{C}']\cdot[\tilde{C}(L) : \tilde{U}(L)]$$

according as dim$V$ is odd or even, where $\underline{C}$ is the group of ideal classes in K and $\underline{C}'$ is the subgroup of $\underline{C}$ consisting of the classes containig ideals which are σ-invariant; and

$$\tilde{C}(L)=\prod_{\mathfrak{q}} C(K_{\mathfrak{q}}/k_{\mathfrak{q}})/C_{L_{\mathfrak{q}}}(K_{\mathfrak{q}}/k_{\mathfrak{q}}) ,$$

where $\mathfrak{q}$ runs over the ramifying prime ideals in k;

$$\tilde{U}(L)=\{(a_{\mathfrak{q}})\in\tilde{C}(L) \mid a_{\mathfrak{q}}=u\cdot C_{L_{\mathfrak{q}}}(K_{\mathfrak{q}}/k_{\mathfrak{q}}) , \quad \text{for} \quad u\in U_K, N(u)=1\} .$$

(The groups $\tilde{C}(L)$ and $\tilde{U}(L)$ depend only on the genus of L.)

Moreover, under the above conditions, two lattices L and L' are SU-equivalent if and only if $L_{\mathfrak{p}}\approx L_{\mathfrak{p}}'$ for every prime ideal $\mathfrak{p}$ in k.

6.8. Suppose dim$V$ is even and $\mathfrak{p}$ is a prime ideal in k which ramifies in K and does not divide 2. We put $\mathfrak{p}\mathcal{O}_K=\mathfrak{P}^2$. Assume that $H_{\mathfrak{p}}$ is of maximal index. Then for any odd s, we have exactly two SU-equivalence classes among the modular lattices with the same modulus $\mathfrak{P}^s$(5.3). Let $\mathrm{L}_s{}^1(\mathfrak{p})$ and $L_s{}^2(\mathfrak{p})$ be their representatives.

Now suppose that we are given a modular lattice L in V such that L is normal for every prime ideal $\mathfrak{q}$ which ramifies and divides 2. For such a lattice we define

$$i_{\mathfrak{p}}(L)=\begin{cases} \;\;0 & \text{if } L_{\mathfrak{p}} \text{ is normal,} \\ \;\;1 & \text{if } L_{\mathfrak{p}} \text{ is not normal and } L_{\mathfrak{p}}\approx L_s{}^1(\mathfrak{p}), \\ -1 & \text{if } L_{\mathfrak{p}} \text{ is not normal and } L_{\mathfrak{p}}\approx L_s{}^2(\mathfrak{p}), \end{cases}$$

where $\mathfrak{p}$ runs over all the prime ideals in k, and $\mu_0(L_{\mathfrak{p}})=\mathfrak{P}^s$, for the latter two cases. (If $\mathfrak{p}$ does not ramify, then $L_{\mathfrak{p}}$ is normal; so the above definition makes sense.)

6.9. THEOREM. *Let (V, H) be a non-degenerate Hermitian vector space with* dim $V>1$. *Suppose H is indefinite. Let L and L' be modular lattices in V. Then*
(1) *If* dim V *is odd then $L\approx L'$ if and only if $\mu_0(L)=\mu_0(L')$ and $d(L, L')=\mathcal{O}_K$.*
(2) *If* dim V *is even then there are $|\tilde{C}(L)|$ SU-equivalence classes among the modular lattices L' such that $\mu(L)=\mu(L')$, $\mu_0(L)=\mu_0(L')$ and $d(L, L')=\mathcal{O}_K$.*

In particular, if $L_{\mathfrak{q}}$ and $L_{\mathfrak{q}}'$ are normal for every prime ideal $\mathfrak{q}$ in k which *divides 2, then we have* $L\approx L'$ *if and only if* $\mu_0(L)=\mu_0(L')$, $d(L, L')=\mathcal{O}_K$ *and* $i_{\mathfrak{p}}(L)=i_{\mathfrak{p}}(L')$ *for all the prime ideals* $\mathfrak{p}$ *in* k.

PROOF. If $\dim V$ is odd then by 4.3 any modular lattice in V is normal. Hence (1) follows from 5.2 and 6.7. (2) follows easily from the definitions.

CHAPTER II

MODULAR LATTICES AND SYMPLECTIC REPRESENTATIONS OF SPECIAL UNITARY GROUPS

1. Functors $\otimes$, Λ^r

1.1. Let V_i be free K-modules of finite rank supplied with non-degenerate Hermitian forms H_i (i=1, 2). We define a non-degenerate Hermitian form $H_1\otimes H_2$ on $V_1\otimes V_2$ by putting

$$H_1\otimes H_2(v_1\otimes v_2, u_1\otimes u_2)=H_1(v_1, u_1)\cdot H_2(v_2, u_2) \quad \text{for} \quad v_i, u_i\in V_i\ .$$

Now take a lattice $L_i=\sum_j \oplus\mathscr{A}_{ij}v_{ij}$ in V_i. Then we get a lattice: $L_1\otimes L_2=\sum\oplus\mathscr{A}_{1i}\cdot\mathscr{A}_{2j}v_{1i}\otimes v_{2j}$ in $V_1\otimes V_2$.

And it is easy to see that: $(L_1\otimes L_2)^\#=L_1^\#\otimes L_2^\#$, $\mu_0(L_1\otimes L_2)=\mu_0(L_1)\mu_0(L_2)$, and $d(L_1\otimes L_2, L_1'\otimes L_2')=d(L_1, L_1')^{n_2}\, d(L_2, L_2')^{n_1}$, ($n_i=\dim V_i$).

In particular, if L_i is $\mathscr{A}_i$-modular, then $L_1\otimes L_2$ is an $\mathscr{A}_1\cdot\mathscr{A}_2$-modular lattice.

If $L_i\sim L_i'$ (resp. $L_i\approx L_i'$) then $L_1\otimes L_2\sim L_1'\otimes L_2'$ (resp. $L_1\otimes L_2\approx L_1'\otimes L_2'$).

Also if k is an algebraic number field of finite degree and K is a quadratic extension of k, then we have $L_{\mathfrak{p}}\otimes L_{\mathfrak{p}}'=(L\otimes L')_{\mathfrak{p}}$ for any prime ideal $\mathfrak{p}$ in k.

1.2. Let V be a free K-module of finite rank supplied with a non-degenerate Hermitian form H. We define a non-degenerate Hermitian form $\Lambda^r H$ on the exterior product space $\Lambda^r V$ by putting

$$\Lambda^r H(v_1\wedge\cdots\wedge v_r, u_1\wedge\cdots\wedge u_r)=\det(H(v_i, u_j))\ , \quad \text{for} \quad v_i, u_j\in V\ .$$

($r\leqslant n$. $\Lambda^1=\text{id.}$)

1.3. Let $g\in GL(V)$, $n=\dim V$, $1\leqslant r\leqslant$n. Then using

$$\binom{n-1}{r-1}\cdot n=\binom{n}{r}\cdot r\ ,$$

we get

$$\det(\Lambda^r g) = (\det(g))^{\binom{n-1}{r-1}} ,$$

Also if $1 \leqslant r < n$, and $|K| > 3$, then using the simplicity of $PSL(n, K)$, we get

$$\operatorname{Ker} \Lambda^r \cap SL(V) = \{a \cdot 1_n \mid a \in K^*, a^{(n,r)} = 1\} .$$

1.4. If we take a lattice $L = \sum \oplus \mathscr{A}_i v_i$ in V, we get a lattice

$$\Lambda^r L = \sum_{1 < i_1 < \cdots < i_r < n} \oplus \left(\prod_{\nu=1}^{r} \mathscr{A}_{i_\nu} \right) v_{i_1} \wedge \cdots \wedge v_{i_r} ,$$

in $\Lambda^r V$.

We have

$$\Lambda^r(L^\sharp) = (\Lambda^r L)^\sharp , \ d(\Lambda^r L, \Lambda^r L') = d(L, L')^{\binom{n-1}{r-1}} , \qquad (n = \dim V) .$$

This implies that if L is $\mathscr{A}$-modular then $\Lambda^r L$ is $\mathscr{A}^r$-modular in $\Lambda^r V$. (In fact, if L is modular then, $d(\Lambda^r L, \Lambda^r L^\sharp) = \mu_0(L)^{n\binom{n-1}{r-1}} \subset \mu_0(\Lambda^r L)^{\binom{n}{r}} \subset \mu_0(L)^{r\binom{n}{r}} = \mu_0(L)^{n\binom{n-1}{r-1}}$.

Also we have in general,

$$\Lambda^r \sum_{i=1}^{m} \oplus L_i \cong \sum_{s_1 + \ldots + s_m = r} \oplus (\Lambda^{s_1} L_1 \otimes \cdots \otimes \Lambda^{s_m} L_m) ,$$

where we put $\Lambda^0 L_i = \mathscr{O}_K$.

2. The functor $\mathscr{R}$

2.1. In this section, we let (V, H) to be a non-degenerate Hermitian vector space over K/k. We put $K = k + k$w, for a fixed element w such that $w^\sigma = -w$.

We denote by $\mathscr{R}$ or $\mathscr{R}_{K/k}$ the functor of restriction of the ground ring from K to k. Let f be the canonical k-linear isomorphism of $V = V_K$ onto $V' = \mathscr{R} V = (\mathscr{R}_{K/k} V)_K$. $\mathscr{R}$ defines canonically an isomorphism f^* of $E(V)$ into $E(V')$, and we have $\det(f^*(g)) = N(\det(g))$ for an element g of $E(V)$.

If L is an $\mathscr{O}_K$-lattice in V then $f(L)$ is an $\mathscr{O}_K$-lattice in V', which we also call $\mathscr{R}(L)$.

2.2. Now we have a natural way to assign an alternating vector space (V', A') to (V, H). Namely, we put $V' = \mathscr{R} V$, and

$$A'(f(x), f(y)) = (H(x, y) - H(y, x))/2w, \quad \text{for} \quad x, y \in V .$$

(The definition of A' depends on the choice of w, but is unique up to a multiplication by a scalar in k.)

We put $\mathscr{R}(V, H)=(V', A')$. We now have $f^*(U(V, H))\subset Sp(V', A')$.

More explicitly, suppose $\{v_1, \cdots, v_n\}$ is a basis of V over K. Then $\{v_1, \cdots, v_n, wv_1, \cdots, wv_n\}=\{v_1', \cdots, v_{2n}'\}$ is a basis of V' over k and

$$(A'(v_i', v_j'))=\begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}\cdot f^*(H(v_k, v_l)) .$$

Hence the alternating form A' is non-degenerate.

2.3. Let us recall some of the basic facts concerning a lattice L' in a non-degenerate alternating vector space V'. (Cf. [23]).

(1) There exists a basis $\{v_1', \cdots, v_{2n}'\}$ of V' and a uniquely determined system of fractional ideals $\mathscr{A}_1\supset \cdots \supset \mathscr{A}_n$ of k such that

$$L'=\sum_{i=1}^{n} \mathcal{O}_k v_i'\oplus\sum_{i=1}^{n}\mathscr{A}_i v_{n+i}' ,$$

$$A'(v_i', v_j')=A'(v_{n+i}', v_{n+j}')=0 \quad \text{for} \quad 1\leqslant i, j\leqslant n ,$$

$$A'(v_i', v_{n+j}')=\delta_{ij} .$$

We put $e(L')=\{\mathscr{A}_1, \cdots, \mathscr{A}_n\}$ and call it *the elementary divisors of* L'. Also we put $n(L')=\mathscr{A}_1$ and call it *the norm of* L'.

(2) L' is called $(n(L')-)$ *maximal* if it is maximal among the lattices with the same norm.

L' is maximal if and only if $e(\mathrm{L}')=\{\mathscr{A}, \cdots, \mathscr{A}\}$.

(3) Let L' and M' be two lattices in V'. There exists an element g of $Sp(V', A')$ sending L' onto M' if and only if $e(L')=e(M')$.

(4) For a prime ideal $\mathfrak{p}$ of k, we consider the non-degenerate alternating vector space $(V_{\mathfrak{p}}', A_{\mathfrak{p}}')$. Then $L_{\mathfrak{p}}'$ is a lattice in $V_{\mathfrak{p}}'$ and $e(L_{\mathfrak{p}}')=\{\mathscr{A}_{1\mathfrak{p}}, \cdots, \mathscr{A}_{n\mathfrak{p}}\}$.

In particular, L' is maximal if and only if $L_{\mathfrak{p}}'$ is for all the prime ideals $\mathfrak{p}$.

We have

$$\mathscr{R}_{K_{\mathfrak{p}}/k_{\mathfrak{p}}}(V_{\mathfrak{p}})=\mathscr{R}_{K/k}(V)_{\mathfrak{p}} , \qquad \mathscr{R}_{K_{\mathfrak{p}}/k_{\mathfrak{p}}}(L_{\mathfrak{p}})=\mathscr{R}_{K/k}(L)_{\mathfrak{p}} .$$

2.4. LEMMA. *Suppose $\mathcal{O}_K$ and $\mathcal{O}_k$ are principal ideal rings and that $\mathcal{O}_K=\mathcal{O}_k+\mathcal{O}_k\cdot w$, $(w^\sigma=-w)$. Let L be an $a\cdot\mathcal{O}_K$-modular lattice in (V, H), where a is an element of k^*. Then $\mathscr{R}(L)$ is a maximal lattice in $\mathscr{R}(V, H)$, and $n(\mathscr{R}(L))=a\cdot\mathcal{O}_k$.*

PROOF. By 4.2, Chapter I, L has a basis $\{v_1, \cdots, v_n\}$ such that $(H(v_i, v_j))$ has elementary divisor of the form $(\underbrace{(a), \cdots, (a)}_{n})$. Hence by 2.2 of this Chapter, we get the desired results.

2.5. LEMMA. *Let k be an algebraic number field of finite degree and K a quadratic extension of k. Suppose that we are given a prime ideal $\mathfrak{p}$ of k which does not divide 2. Then there exists an element w such that $\mathcal{O}_{K\mathfrak{p}}=\mathcal{O}_{\mathfrak{p}}+\mathcal{O}_{\mathfrak{p}}w$, and $w^\sigma=-w$, ($\mathcal{O}_{\mathfrak{p}}=\mathcal{O}_{k\mathfrak{p}}$=the ring of $\mathfrak{p}$-adic integers).*

PROOF. If $\mathfrak{p}$ is unramified, then there exists a unit w such that $w^\sigma=-w$. K is spanned by 1 and w. But as $1/2$ is a unit, $a+bw\in\mathcal{O}_{K\mathfrak{p}}$ $(a, b\in k_{\mathfrak{p}})$ implies that a and b belong to $\mathcal{O}_{\mathfrak{p}}$ and vice-versa.

If $\mathfrak{p}$ splits, then we can put $w=(1, -1)$.

If $\mathfrak{p}$ ramifies, then we have $\mathfrak{p}=(\pi)$, $\mathfrak{p}\mathcal{O}_K=\mathfrak{P}^2$, $\mathfrak{P}=(\Pi)$, $\Pi^2=\pi$. We can put $w=\Pi$.

2.6. LEMMA. *The situation being the same as above, assume that $\mathfrak{p}$ is a prime ideal of k which ramifies in K and does not divide 2. Let $\mathfrak{p}\mathcal{O}_K=\mathfrak{P}^2$, and suppose $L_{\mathfrak{p}}$ is a $\mathfrak{P}^s$-modular lattice in $(V_{\mathfrak{p}}, H_{\mathfrak{p}})$ where $s=2t+1$. Then* dim $V=2m$, *$\mathscr{R}(L_{\mathfrak{p}})$ is not maximal in $\mathscr{R}(V_{\mathfrak{p}}, H_{\mathfrak{p}})$ and its elementary divisors are*

$$\{\underbrace{\mathfrak{p}^t, \cdots, \mathfrak{p}^t}_{m}, \underbrace{\mathfrak{p}^{t+1}, \cdots, \mathfrak{p}^{t+1}}_{m}\} .$$

PROOF. Let $\mathscr{R}(V_{\mathfrak{p}}, H_{\mathfrak{p}})=(V_{\mathfrak{p}}', A_{\mathfrak{p}}')$. In virtue of the theory of classification of the modular lattices, we may assume that $s=1$, $m=1$. (It was shown in 5.3, Chapter I that $\dim V$ becomes even.) Now by Lemmas 2.5 and 2.2, there exists a basis $\{v_1', \cdots, v_4'\}$ of $V_{\mathfrak{p}}'$ such that

$$(\det(\mathrm{A}'(v_i', v_j')))=(N\mathfrak{P}^2)=\mathfrak{p}^2 .$$

On the other hand, it is clear that the elementary divisors of $\mathscr{R}(L_{\mathfrak{p}})$ are of the form $\{\mathfrak{p}^{r_1}, \mathfrak{p}^{r_2}\}$ where $0\leqslant r_1\leqslant r_2$. We have $2(r_1+r_2)=2$, hence $r_1=0$, $r_2=1$. This proves the Lemma.

2.7. The situation being the same as in 2.5, suppose that $\mathscr{A}$ is a fractional ideal of K which is σ-invariant. Then we can write $\mathscr{A}=\mathscr{A}_1\cdot\mathscr{A}_2$, where $\mathscr{A}_1=\mathfrak{P}_1\cdots\mathfrak{P}_t$, $\mathfrak{P}_i$ running over all prime ideals in K which ramify in K/k, and the $\mathfrak{P}_i$-exponent of $\mathscr{A}$ is odd. Hence $\mathscr{A}_2$ is the extension of an ideal in k, with which it shall be identified.

Combining 2.3, 2.4, 2.5 and 2.6 we get immediately the following:

2.8. THEOREM. *Let k be an algebraic number field of finite degree and K a quadratic extension of k. Let (V, H) be a non-degenerate Hermitian vector space over K/k, and L an $\mathscr{A}$-modular lattice in V. Assume that for any prime ideal $\mathfrak{q}$ of k dividing 2 we have $\mathcal{O}_{K\mathfrak{q}}=\mathcal{O}_{\mathfrak{q}}+\mathcal{O}_{\mathfrak{q}}w_{\mathfrak{q}}$, for an element $w_{\mathfrak{q}}$ such that $w_{\mathfrak{q}}^{\sigma}=-w_{\mathfrak{q}}$ and $L_{\mathfrak{q}}$ is normal. Then we have*

(1) *If $\mathscr{A}$ is an ideal of k, then $\mathscr{R}(L)$ is $\mathscr{A}$-maximal in $\mathscr{R}(V, H)$.*

(2) *If $\mathscr{A}$ is not an ideal of k, and $\mathscr{A}=\mathscr{A}_1\cdot\mathscr{A}_2$, $(\mathscr{A}_1\neq(1))$, then,* dim $V=2m$, *$\mathscr{R}(L)$ is not maximal in $\mathscr{R}(V, H)$, and*

$$e(\mathscr{R}(L))=\{\underbrace{\mathscr{A}\cdot\mathscr{A}_1^{-1}, \cdots, \mathscr{A}\cdot\mathscr{A}_1^{-1}}_{m}, \underbrace{\mathscr{A}\cdot\mathscr{A}_1, \cdots, \mathscr{A}\cdot\mathscr{A}_1}_{m}\} .$$

2.9. REMARK. If $k=Q$, and $K=Q(\sqrt{-1})$, then we get the above statements (1) and (2) for a modular lattice L without any further requirements (as in the Theorem) concerning the ramifying prime 2.

CHAPTER III

APPLICATIONS

1. $G_L\backslash G_k/G_W$ and rational boundary components of the domains of type (I)

1.1. Let k be an algebraic number field of finite degree and K a quadratic extension of k. Let (V, H) be a non-degenerate Hermitian vector space over K/k, and L an $\mathcal{O}_K$-lattice in V.

Let $\underline{W}_s$ be the set of all totally isotropic subspaces of V with dimension s. Let $G_k=SU(V, H)$, and for an element W of $\underline{W}_s$ we put

$$G_W=\{g\in G_k \mid gW=W\} .$$

For elements W and W' of $\underline{W}_s$, we set $W\sim W'$ if and only if there exists an element g in $U(V, H)_L$ sending W onto W'; $W\approx W'$ if and only if there exists an element g in G_L sending W onto W'.

Then it is easy to see that there exists a bijection between the double coset space $G_L\backslash G_k/G_W$ and the set $\underline{W}_s/\approx$, $(W\in \underline{W}_s)$.

1.2. For any subset S of V, we set

$$S^{\perp}=\{x\in V \mid H(x, s)=0 \quad \text{for all} \quad s\in S\} .$$

If $W \in \underline{W}_s$, then the vector space $W^{\perp}/W$ has a structure of a non-degenerate Hermitian vector space which is isomorphic to a subspace of V, and the isomorphic class of $W^{\perp}/W$ is uniquely determined by s (Witt's Theorem).

For convenience, we shall fix once for all a subspace V_s of V which is isomorphic to $W^{\perp}/W$, $(W \in \underline{W}_s)$.

The module $W^{\perp} \cap L/W \cap L$ is a lattice in vector space $W^{\perp}/W$, so by the above we get a lattice $L_s(W)$ in V_s. If $W \sim W'$ then $L_s(W) \sim L_s(W')$.

1.3. In the following in this section, we assume that K/k satisfies

(A) $h(K)$ =the class number of $K=1$,

(B) $[\mathcal{O}_k : \mathrm{Tr}(\mathcal{O}_K)] \leqslant 2$.

The condition (B) is satisfied if, for example, $k=Q$. Also, if K/k is unramified, then we have $\mathcal{O}_k = \mathrm{Tr}\,(\mathcal{O}_K)$.

The condition (A) implies that $h(k)$ =the class number of $k=1$ or 2, and in the latter case K is the absolute class field of k (cf. [25, § 12.4]).

1.4. LEMMA. *Let L be an (a)-modular lattice in V, and W an element of $\underline{W}_s$. Then there exists a basis $\{w_1, \cdots, w_s\}$ of W and elements $\{w_1', \cdots, w_s'\}$ in V such that*

$$L = \sum_{i=1}^{s} \oplus (\mathcal{O}_K w_i + \mathcal{O}_K w_i') \oplus L' ,$$

$$H(w_i', w_j') = 0 , \qquad H(w_i, w_j') = \delta_{ij} \cdot a ,$$

$$L' = L \cap \{w_1, \cdots, w_s, w_1', \cdots, w_s'\}^{\perp} ,$$

L' is an (a)-modular lattice.

If in particular, L' is normal and $a \in k^*$, then we may assume that $H(w_j') = 0$, for all j's.

PROOF. We take a basis $\{u_1, \cdots, u_s\}$ of W where u_1 is a primitive element in L. Put $w_1 = u_1$. Then in view of 4.2, Chapter I, we have an element w_1' in L such that $H(w_1, w_1') = a$. Then it is easy to see that we have

$$L = (\mathcal{O}_K w_1 + \mathcal{O}_K w_1') \oplus L_1' , \qquad L_1' = L \cap \{w_1, w_1'\}^{\perp} .$$

Now, we have for $i \geqslant 2$, $u_i = \lambda_i w_1 + \mu_i w_1' + u_i'$ $(\lambda_i, \mu_i \in K$, and $u_i' \in \{w_1, w_1'\}^{\perp})$, and $H(w_1, u_i) = a \cdot \mu_i = 0$. Hence $u_i = \lambda_i w_1 + u_i'$ and we get a new basis $\{w_1, u_2', \cdots, u_s'\}$ of W. Now we can use the induction on s to get the desired decomposition.

(Again in virtue of 4.2, Chapter I, it is clear that L' is an (a)-modular lattice.)

Now suppose that L' is normal and $a \in k^*$. We look at the following:

$$(1) \qquad H(-\nu w_j + w_j' + x) = H(w_j') - H(x) - a \cdot \mathrm{Tr}\,(\nu)\,, \qquad (x \in L')\,.$$

We have $H(w_j') = a \cdot t$ for $t \in \mathcal{O}_k$. If $t \in \mathrm{Tr}\,(\mathcal{O}_K)$, then the statement is obvious, so we assume otherwise (hence, in particular, $[\mathcal{O}_k : \mathrm{Tr}\,(\mathcal{O}_K)] = 2$). It is enough to show that there exists an element x in L' such that $H(x) = a \cdot t'$, for $t' \notin \mathrm{Tr}\,(\mathcal{O}_K)$. (Because in that case, $t + t' \in \mathrm{Tr}\,(\mathcal{O}_K)$, so there exists an element ν in $\mathcal{O}_K$ such that the right side of the equation (1) becomes equal to 0; then we replace w_j' by $-\nu w_j + w_j' + x$).

But by our assumption, the $\mathcal{O}_k$-ideal generated by $H(x)$ for $x \in L'$ is $a \cdot \mathcal{O}_k$, and $a \cdot \mathcal{O}_k \supsetneqq a \cdot \mathrm{Tr}\,(\mathcal{O}_K)$. This implies the existence of the desired element x.

1.5. REMARK. In the above, if $h(k) = 1$, then the normality of L' implies that $a \in k^*$.

1.6. In Lemma 1.4, we have $L' \sim L_s(W)$. Now, let L be an (a)-modular lattice in V for $a \in k^*$, and assume that either dim V is odd or K/k is unramified (so that L' is always normal !). Then, for elements W and W' of $\underline{W}_s$, we have $W \sim W'$ if and only if $L_s(W) \sim L_s(W')$.

On the other hand, suppose in general that $W \sim W'$ with respect to a modular lattice L, with an element g of $U(V, H)_L$ sending W onto W'. If moreover, there exists an element u in U_K such that $\det(g) = u^{1-\sigma}$, then $W \approx W'$.

In fact, taking the decomposition of L with respect to W as in 1.4, we define an element g' of $U(V, H)$ by

$$g'(w_1) = u^{-1} w_1\,, \qquad g'(w_1') = u^{\sigma} w_1'\,, \qquad g' \mid \{w_1, w_1'\}^{\perp} = \mathrm{id}\,.$$

Then $g \cdot g'$ belongs to G_L sending W onto W'.

1.7. Generally, for a finite Galois extension $\tilde{K}$ of k, we let $G(\tilde{K}/k)$ be the Galois group of $\tilde{K}/k$. Then it is known that the group $H^1(G(\tilde{K}/k), U_{\tilde{K}})$ is isomorphic to the factor group of the group of ambigous principal ideals of $\tilde{K}$ modulo the group of principal ideals of k [12], [25, § 13.2]. We denote by $h(\tilde{K}/k)$ the order of the above cohomology group.

In particular, if $\tilde{K}/k$ is a cyclic extension of degree m, then

$$(1) \qquad h(\tilde{K}/k) = (h(k) \prod_{\mathfrak{p}} e(\mathfrak{q}))/a_0\,,$$

$$(2) \qquad = m[U_k : N(U_{\tilde{K}})]/2^{r'}\,,$$

where in (1), $\mathfrak{q}$ runs over the ramifying prime ideals of k, $e(\mathfrak{q})$ is the ramification exponent of $\mathfrak{q}$, and a_0 is the number of ideal classes in $\tilde{K}$ repesented by ambigous ideals; while in (2), r' is the number of real conjugates of k which are contained in complex conjugates of $\tilde{K}$.

As a consequence, we get the following Lemma.

1.8. LEMMA. *Suppose K is a quadratic extension of k, and $h(K)=1$. Then we have*

$$h(K/k)=\begin{cases} 2, & \textit{if} \quad h(k)=2, \\ 2^m, & \textit{if} \quad h(k)=1, \ \textit{and } m \textit{ is the number of the} \\ & \quad \textit{ramifying prime ideals of } k. \qquad (m>0) \end{cases}$$

If moreover, k is totally real and K is totally imaginary, then $h(K/k)=2$.

PROOF. The first half of the statement follows at once from the formula (1) of 1.7, in view of 1.3. (Also, if $h(k)=1$, then the absolute class field of k is k itself. Hence $m>0$.)

So, let k be totally real of degree d over Q, K totally imaginary. Then, by the formula (2) of 1.7, we have

$$h(K/k)=[U_k : N(U_K)]/2^{d-1} .$$

Let $\{e, \cdots, e_{d-1}\}$ be a system of fundamental units of k. Then

$$U_k=\{\pm 1\cdot e_1^{x_1} \cdots e_{d-1}^{x_{d-1}}\} \cong \{\pm 1\} \times Z^{d-1} .$$

As $N(U_K)\supset U_k^2, [U_k : N(U_K)]$ divides 2^d, therefore $h(K/k)=2^{1-d+d'}$, $(d\geqslant d')$. $h(K/k)$ being an integer, this completes the proof.

1.9. THEOREM. *Let k be an algebraic number field of finite degree and K a quadratic extension of k satisfying the conditions (A) and (B) of 1.3. Let (V, H) be a non-degenerate Hermitian vector space over K/k, $G_k=SU(V, H)$, L an (a)-modular lattice in V with $a\in k^*$, and $W\in \underline{W}_s$. Then,*

(1) *If K/k is unramifield or* dim V *is odd* (>1), *then*

$$h((a), V_s)\leqslant|G_L\backslash G_k/G_W|\leqslant h(K/k)h((a), V_s) .$$

(2) *If* dim $V=2s+1$, *and* $U_k\cap N(K)=N(U_K)$, *then,*

$$|G_L\backslash G_k/G_W|=1 .$$

PROOF. (The first inequality of (1)):— Take a decomposition of L with respect to W:

$$L=\sum_{i=1}^{s}(\mathcal{O}_K w_i+\mathcal{O}_K w_i')\oplus L' ,$$

as in 1.4. Let M' be any (a)-modular lattice in V_s $(=KL')$, and put

$$M=\sum_{i=1}^{s}(\mathcal{O}_K w_i+\mathcal{O}_K w_i')\oplus M' .$$

M is an (a)-modular lattice in V. But now, our assumptions imply that $h((a), V)=1$. So, $L\sim M$; which in virtue of 1.1, and 1.6, implies the desired inequality.

(The second inequality of (1)):— We decompose the set $\underline{W}_s$ into $\sim$-classes and choose one representative W_ι from each class. Let W be any element of $\underline{W}_s$ such that $W\sim W_\iota$, with an element g of $U(V, H)_L$ sending W onto W_ι. Consider the correspondence: $W\rightarrow((L_s(W)), (\det(g)))$, where $(L_s(W))$ is the unitary equivalence class of $L_s(W)$, and $(\det(g))$ is the cohomology class of $\det(g)$ $(\in U_K, N(\det(g))=1)$. (This correspondence may depend on the choice of g; here, we fix such an element g for each W, such that $\det(g)$ is determined by the $\approx$-class of W.) Then, in virtue of 1.6, this correspondence gives a one to one mapping of $\underline{W}_s/\approx$ into a finite set whose order is equal to $h(K/k)h((a), V_s)$.

(2):— Let $W\in\underline{W}_s$ and take the decomposition of L with respect to W:

$$L=\sum_{i=1}^{s}(\mathcal{O}_K w_i+\mathcal{O}_K w_i')\oplus L' , \qquad L'=\mathcal{O}_K v .$$

L' is (a)-modular lattice of rank 1. But our assumptions imply that any two (a)-modular lattices of rank 1 are unitary equivalent, therefore, in virture of 1.6 again, any two elements W and W' of $\underline{W}_s$ are $\sim$-equivalent, say via the element g of $U(V, H)_L$. We define an element g' of $U(V, H)_L$ by

$$g'(v)=u^{-1}v , \qquad g' \mid \{v\}^{\perp}=\mathrm{id} . \qquad (u=\det(g)) .$$

Then $g\cdot g'$ belongs to G_L sending W onto W'.

1.10. REMARK. (1) In the above, if V_s is indefinite then $h((a), V_s)=1$, and if V_s is definite, then $h((a), V_s)=c((a), V_s)$. (cf. 6.3, 6.5 and 6.7 of Chapter I).
(2) If $k=Q$, K=imaginary quadratic number field, then

$$U_k\cap N(K)=\{1\}=N(U_K).$$

1.11. Let k be totally real and K totally imaginary. If $\mathscr{K}$ is a maximal compact subgroup of the Lie group $\mathscr{R}_{k/Q}(G))_R$, then the coset space $D=(\mathscr{R}_{k/Q}(G))_R/\mathscr{K}$ has the structure of a bounded symmetric domain of type (I) [1], [7], [18]. For a boundary component F of $\bar{D}$, the group $N(F)=\{g\in(\mathscr{R}_{k/Q}(G))_R \mid g(F)=F\}$ is a maximal parabolic subgroup of $(\mathscr{R}_{k/Q}(G))_R$, and conversely, for any such subgroup P there exists a boundary component F such that $N(F)=P$ [1]. We call F *rational* if $N(F)_C$ is defined over Q. There exists a bijection of the set of rational boundary components onto the set of proper maximal parabolic k-subgroup of G_k [1], [6].

A proper maximal parabolic k-subgroup of G is the stabilizer of a totally isotropic subspace of V which is uniquely determined by the subgroup.

Given a lattice L in V, there exists a bijection of the set of G_L-equivalence classes of rational boundary components of $\bar{D}$ onto the set $\bigcup_{1\leq s\leq i}(\underline{W}_s/\approx)$, $(i=\text{Ind}\,(H))$.

We put $b_s(L)=|\underline{W}_s/\approx|$, and $b(L)=\sum_{s=1}^{i} b_s(L)$.

As a consequence of Theorem 1.9, we obtain the following:

1.12. Situations being the same as in 1.11, we further more assume that $h(K)=1$. Let $i=\text{Ind}\,(H)$ (>1), L an (a)-modular lattice in V with $a\in k^*$. Then,
(1) If dim $V=3$, and $U_k\cap N(K)=N(U_K)$, and K/k satisfies (B), then

$$b(L)=1\ .$$

(2) In general, if K/k satisfies (B), and if either K/k is unramified or dim V is odd (>1), then

$$1\leqslant b(L)/(i-1+c((a),\ V_i))\leqslant 2\ .$$

2. A symplectic representation of special unitary groups and automorphic functions

2.1. Let k be an algebraic number field of finite degree, and G a connected, absolutely simple algebraic group defined over k, Γ an arithmetic subgroup of G_k. Γ may be identified with a discrete subgroup of the Lie group $(\mathscr{R}_{k/Q}(G))_R$. Suppose that we are given a maximal compact subgroup $\mathscr{K}$ of $(\mathscr{R}_{k/Q}(Q))_R$ such that $D=(\mathscr{R}_{k/Q}(G))_R/\mathscr{K}$ has the structure of a symmetric bounded domain. Let $D^*=D\cup$ {rational boundary components of $\bar{D}$} supplied with a suitable topology, and put $\mathscr{V}^*=\Gamma\diagdown D^*$. $\mathscr{V}^*$ has the structure of a projective variety [1].

Now let G' be another algebraic group defined over k satisfying the above requirements for G. Let Γ', $\mathscr{K}'$ etc. be the corresponding notions for G'.

Suppose that we are given a rational representation ρ of G into G' defined over k such that $\rho(\Gamma)\subset\Gamma'$, $(\mathscr{R}_{k/Q}\rho)(\mathscr{K})\subset\mathscr{K}'$, and $\mathscr{R}_{k/Q}\rho$ induces a holomorphic imbedding ρ of D into D' [18]. It has been shown by I. Satake that this ρ induces a rational mapping of $\mathscr{V}^*$ into $\mathscr{V}'^*$. (See [19].) Hence the field $C(\rho(\mathscr{V}^*))$ of rational functions on $\rho(\mathscr{V}^*)$ can be identified with a subfield of $C(\mathscr{V}^*)$.

If $\dim G>3$, then the field $C(\mathscr{V}^*)$ can be identified with the field of automorphic functions on D with respect to Γ, and under the above identification, $C(\rho(\mathscr{V}^*))$ is the subfield of $C(\mathscr{V}^*)$ consisting of those functions which can be extended to automorphic functions on D' with respect to Γ'.

Let us put

$$Z(\rho(D))=\{g'\in(\mathscr{R}_{k/Q}(G'))_R \mid g'(\rho(z))=\rho(z), \quad \text{for all} \quad z\in D\}\ ,$$

$$N(\rho(D))=\{g'\in(\mathscr{R}_{k/Q}(G'))_R \mid g'(\rho(D))=\rho(D)\}\ .$$

It has been shown by I. Satake [21], that

$$[C(\mathscr{V}^*):C(\rho(\mathscr{V}^*))]=[\Gamma'\cap N(\rho(D))/\Gamma'\cap Z(\rho(D)) : \rho(\Gamma)/\rho(\Gamma)\cap Z(\rho(D))]\ ,$$

and it is finite. We denote such a number by d_ρ.

Now

$$\rho(\Gamma)/\rho(\Gamma)\cap Z(\rho(D))=\rho(\Gamma)\cdot(\Gamma'\cap Z(\rho(D)))/\Gamma'\cap Z(\rho(D))\ .$$

Hence,

$$d_\rho=[\Gamma'\cap N(\rho(D)) : \rho(\Gamma)\cdot(\Gamma'\cap Z(\rho(D))]\ .$$

Moreover, if $\rho(\Gamma)\cdot(\Gamma'\cap Z(\rho(D))$ is a normal subgroup of $\Gamma'\cap N(\rho(D))$ then $C(\mathscr{V}^*)$ is a Galois extension of $C(\rho(\mathscr{V}^*))$ of degree d_ρ, with Galois group isomorphic to $\Gamma'\cap N(\rho(D))/\rho(\Gamma)\cdot(\Gamma'\cap Z(\rho(D)))$.

2.2. The situation being the same as in 1.11, we put $G_k=SU(V,H)$ and $D=(\mathscr{R}_{k/Q}(G))_R/\mathscr{K}$. Let us put $(V',A')=\mathscr{R}_{K/k}\circ\Lambda^r(V,H)$, $G_k'=Sp(V',A')$ ($1\leqslant r<\dim V$, and if we have $\mathrm{Ind}\,(H_\lambda)>1$ for any one of infinite places $\mathfrak{p}_{\infty,\lambda}$ of k, we put $r=1$).

The functor $\mathscr{R}_{K/k}\circ\Lambda^r$ determines in a natural way, a rational homomorphism ρ of G into G', and ρ induces a holomorphic imbedding of the domain D into the domain $D'=(\mathscr{R}_{k/Q}(G'))_R/\mathscr{K}'$, for a suitable maximal compact subgroup $\mathscr{K}'$ of $(\mathscr{R}_{k/Q}(G'))_R$ such that $(\mathscr{R}_{k/Q}\rho)(\mathscr{K})\subset\mathscr{K}'$. As in 2.1, we again use ρ to denote this holomorphic imbedding. (See [18], [20].)

We have a commutative diagram:

$$\begin{tikzcd}
G_k \arrow[rr, "\tilde{\rho}=\Lambda^r"] \arrow[dr, "\rho"'] & & \tilde{G}_k=U(\tilde{V},\tilde{H})=U(\Lambda^r V,\Lambda^r H) \arrow[dl, "\rho'=\mathscr{R}_{K/k}"] \\
& G_k' &
\end{tikzcd}$$

For a lattice L in V, we put $\tilde{L}=\Lambda^r L$, $L'=\mathscr{R}_{K/k}(\tilde{L})$. Hence $\tilde{\rho}(G_L)\subset\tilde{G}_{\tilde{L}}$, $\rho(G_L)\subset G_{L'}$.

Let k^{σ_i} (resp. K^{σ_i}) be the conjugates of k (resp. K) over Q $(1\leqslant i\leqslant d)$. $\mathscr{R}_{k/Q}(G)\cong G^{\sigma_1}\times\cdots\times G^{\sigma_d}$, etc. ρ etc. induce homomorphisms sending $G^{\sigma_1}\times\cdots\times G^{\sigma_d}$ into $G'^{\sigma_1}\times\cdots\times G'^{\sigma_d}$ etc which will again be denoted by ρ etc. ρ induces a homomorphism of i-th component G^{σ_i} into G'^{σ_i} which we denote by ρ_i. We define $\tilde{\rho}_i$, and ρ_i' similarly.

Let us also put $Z^{(i)}=Z(\rho(D))\cap G_R'^{\sigma_i}$, $N^{(i)}=N(\rho(D))\cap G_R'^{\sigma_i}$, and $\tilde{Z}^{(i)}=\rho_i'^{-1}(Z^{(i)})$, $\tilde{N}^{(i)}=\rho_i'^{-1}(N^{(i)})$ for $i=1,\cdots,d$.

Now we arrange the order of σ_i's so that $G_R^{\sigma_1},\cdots,G_R^{\sigma_c}$ are non-compact and the rest are compact $(1\leqslant c\leqslant d)$.

2.3. PROPOSITION. *Suppose* $\dim V>2$ *and that we have the following condition:*
(C) $Z_{k^{\sigma_i}}^{(i)}$ *is Zariski dense in* $Z^{(i)}$, *for* $1\leqslant i\leqslant c$.
Then,

$$(1)\quad Z^{(i)}=\{\rho_i'(a1_N)\mid a\in C,\ |a|=1\}\ ,\quad N=\dim\tilde{V}=\binom{n}{r},\quad 1\leqslant i\leqslant c\ ,\quad (n=\dim V)\ ,$$

$$(2)\qquad Z^{(j)}=N^{(j)}=\mathscr{K}_j'(=\mathscr{K}'\cap G_R'^{\sigma_j})\ ,\qquad c<j\leqslant d\ .$$

PROOF. (2) is obvious. To show (1), it is enough to show that $Z_{k^{\sigma_i}}^{(i)}$ is contained in $\{\rho_i'(a1_N)\mid a\in C,|a|=1\}$.

Suppose $g_i'\in Z_{k^{\sigma_i}}^{(i)}$. There exists an element g' of $Z(\rho(D))_Q$ whose i-th component is equal to g_i'. Consider the set $S=\{\rho(\gamma)^{-1}g'\rho(\gamma)\mid\gamma\in G_L\}$. S is a discrete set contained in $\mathscr{K}'$, hence finite. G_L operates on S by inner automorphism, so that there exists a subgroup Γ_1 of finite index in G_L which stabilizes every element of the set S. By the density theorm of A. Borel [2], it follows that g' commutes with every element of the image $\rho(G)$. In particular, g_i' commutes with every element of the image $\rho_i(G_R^{\sigma_i})$.[3]

Hence it is enough to show that the linear closure T of $\rho_i(G_R^{\sigma_i})$ contains the linear transformation $\rho_i'(w^{\sigma_i}\cdot 1_N)$, where $K=k(w)$, $w^2=u\in k$. (Because in that case Λ^r being an absolutely irreducible representation, we can use Schur's lemma to prove the desired result.)

Let us look at a specific case where $r=1$, $\dim V^{\sigma_i}=3$. Let $\{v_1,v_2,v_3\}$ be an orthogonal basis for V^{σ_i}, and we take $\{v_j, w^{\sigma_i}v_j\}_{j=1,2,3}$ for a basis of $\tilde{V}^{\sigma_i}$ over k^{σ_i}. There exists a pair of real numbers x and y such that

[3] The essential point in the above argument is due to M. Kuga.

$$N_{K^{\sigma_i}/k^{\sigma_i}}(x+yw^{\sigma_i})=1\,, \qquad x\neq 1\,, \qquad y\neq 0\,.$$

We put $\theta=x+yw^{\sigma_i}$. Then $g=\operatorname{diag}(\theta, \theta^{\sigma}, 1)\in G_K^{\sigma_i}$, and

$$\rho_i'(g)=\left(\begin{array}{ccc|ccc} x & & & u^{\sigma_i}y & & \\ & x & & & -u^{\sigma_i}y & \\ & & 1 & & & 0 \\ \hline y & & & x & & \\ & -y & & & x & \\ & & 0 & & & 1 \end{array}\right).$$

As $\operatorname{diag}(\theta^{\sigma}, \theta, 1)$ is also contained in $G_R^{\sigma_i}$, we have the element $t(1, -1, 0)$ in T, where, by definition,

$$t(a, b, c)=\begin{pmatrix} 0 & u^{\sigma_i}X \\ X & 0 \end{pmatrix}, \qquad X=\operatorname{diag}(a, b, c) \qquad (a, b, c\in R)\,.$$

Similarly, we get $t(1, 0, -1)$ and $t(0, 1, -1)$ in T. Our purpose is to find the element $t(1, 1, 1)$ in T. But now the element $\operatorname{diag}(\theta^2, \theta^{\sigma}, \theta^{\sigma})$ is contained in $G_R^{\sigma_i}$ which implies that $t(2xy, -y, -y)$ is contained in T. Hence,

$$y(t(2x, -1, -1)+t(0, 1, -1)-t(2, 0, -2))=2(x-1)y\cdot t(1, 0, 0)\in T\,.$$

This implies the existence of $t(1, 1, 1)$ as desired.

The general case can be easily reduced to the above special case.

2.4. REMARK. Let us give an example for which the condition (C) holds. Let $k=Q$, $K=Q\sqrt{-1})$. Assume that V has a fixed basis $\{v_1, \cdots, v_n\}$ (n>2) with respect to which the form H has the matrix equal to $\operatorname{diag}(1_a, -1_b)$. For the representation we take $\rho=\rho'\mid G$. For the basis of V', we take

$$\{v_1, \cdots, v_n, -iv_1, \cdots, -iv_a, iv_{a+1}, \cdots, iv_n\}\,.$$

And we put

$$\mathscr{K}=\left\{\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}\middle| X\in U(a),\ Y\in U(b),\ \det(X)=\det(Y)^{-1}\right\},$$

$$\mathscr{K}'=\left\{\begin{pmatrix} X & Y \\ -Y & X \end{pmatrix}\in Sp(n, R)\right\}.$$

In this case, the condition (C) holds. (To see this, we take an explicit realization of D and D' as bounded domains using the Harish-Chandra imbedding. And by an easy calculation, we can show directly that

$$Z(\rho(D))=\{\rho'(a1_n)\mid a\in C,\ |a|=1\}$$

which of course implies (C).)

2.5. REMARK. If dim $V=2$, then the situation is different. For example, in the above if $a=b=1$, the

$$Z(\rho(D))=\left\{\begin{pmatrix} X & Y \\ -Y & X \end{pmatrix} \middle| X=\begin{pmatrix} x & z \\ z & x \end{pmatrix},\ Y=\begin{pmatrix} y & t \\ -t & -y \end{pmatrix},\ \begin{matrix} x, y, z, t \in R \\ x^2+y^2+z^2+t^2=1 \\ xz+yt=0 \end{matrix}\right\},$$

and it is not contained in the image $\rho'(U(2))$.

2.6. Generally, for a bounded domain D, we set $A(D)=$the group of all holomorphic automorphisms of D. Especially, if $D=SU(a,b)/\mathscr{K}$, where

$$\mathscr{K}=SU(a,b)\cap U(a+b)\ ,$$

then $A(D)$ is connected except when $a=b>1$. If a$=b>1$, then the connected component of the identity $A(D)^\circ$ forms a subgroup of index 2 in $A(D)$, and D is realized as a bounded domain in the complex vector space formed by complex $a\times a$ matrices; the transformation

$$M(a,c)\ni X \longrightarrow {}^tX\in M(a,C)\ ,$$

gives rise to an element of $A(D)$ which is not contained in $A(D)^\circ$ ([1], [7], [15]).

2.7. Coming back to the situation in 2.2, let us put $N^\circ=N(\rho(D))\cap A(D)^\circ$. Then $N^\circ\subset Z(\rho(D))\cdot\rho((\mathscr{R}_{k/Q}(G))_R)$. Therefore, if dim $V>2, 1\leqslant i\leqslant c$, and (C) holds, then there exists a subgroup $\tilde{N}_i{}^\circ$ of $\tilde{G}_R^{\sigma_i}$ such that $\rho_i'(\tilde{N}_i{}^\circ)=N_i{}^\circ=N^\circ\cap G_R'^{\sigma_i}$.

In view of 2.6, we have $[N(\rho(D)):N^\circ]\leqslant 2^{d'}$, where d' is the number of infinite valuations $\mathfrak{p}_{\infty,\lambda}$ for which Ind $(H_\lambda)=$ dim $V/2>1$.

We put $N_{L'}^\circ=N^\circ\cap G'_{L'}$, $Z_{L'}=Z(\rho(D))\cap G'_{L'}$, $\tilde{N}_{\tilde{L}}^\circ=\rho'^{-1}(N_{L'}^\circ)$, $\tilde{Z}_{\tilde{L}}=\rho'^{-1}(Z_{L'})$.

2.8. LEMMA. *The situation being the same as above, we have*

(1) $\tilde{\rho}(G_L)=\tilde{\rho}(G)_{\tilde{L}}$.

(2) *If* dim $V>2$, $1\leqslant i\leqslant c$, *and* (C) *holds, then*

$$\tilde{Z}_i\cap\tilde{\rho}_i(G_R^{\sigma_i})=\{\tilde{\rho}_i(a1_n)\mid a^n=1\}\ ,\qquad (n=\dim V)\ .$$

PROOF. (2) follows from Proposition 2.3.

To show (1), we firstly notice that

$$(\tilde{\rho}(G_L)=)\Lambda^r(SU(V, H)_L)=\Lambda^r(SU(V, H))\cap\Lambda^r(SL(V)_L) .$$

Obviously, the left side is contained in the right side. To see the converse, let us suppose that $\Lambda^r(g)=\Lambda^r(\gamma)$, $g\in SU(V, H)$, $\gamma\in SL(V)_L$. Then in virtue of 1.3, Chapter II, $\gamma=ag$, $a^{(n,r)}=1$. Therefore $\gamma\in SU(V, H)_L$.

Now we use 2.4, Chapter I to get

$$\begin{aligned}\Lambda^r(SU(V, H)_L)&=\Lambda^r(SU(V, H))\cap\Lambda^r(SL(V)_L)\\&=\Lambda^r(SU(V, H))\cap\Lambda^r(SL(V))\cap SL(\Lambda^r V)_{\Lambda^r L}\\&=\Lambda^r(SU(V, H))\cap SL(\Lambda^r V)_{\Lambda^r L}\\&\supset\Lambda^r(SU(V, H))\cap SU(\Lambda^r V, \Lambda^r H)_{\Lambda^r L}\\&\supset\Lambda^r(SU(V, H)_L) .\end{aligned}$$

This proves the Lemma.

2.9. Let k be an algebraic number field of finite degree. We put $K^{(n)}=K(\zeta_n)$, where $\zeta_n=e^{2\pi i/n}$.

As before, (1.7), if $\tilde{K}$ is a Galois extension of K, we put $G(\tilde{K}/K)=$Galois group of $\tilde{K}/K$.

We denote by (ζ_n) the group of n-th roots of unity.

2.10. THEOREM. *Let k be a totally real algebraic number field and K a totally imaginary quadratic extension of k. Let (V, H) be a non-degenerate indefinite Hermitian vector space over K/k, $G_k=SU(V, H)$. Situation being the same as in 2.2, we assume that* $\dim V=n>2$, *and (C) holds (2.3). Let L be a lattice in V, and $\mathscr{R}_{K/k}\circ\Lambda^r(L)=L'$. Then*

(1) *For any i such that $1\leqslant i\leqslant c$, there exists a Kummer extension K_i' of $K^{\sigma_i}(\zeta_n)$ which is uniquely determined by $N_{L'}^{\circ}$, and we have the following exact sequence:*

$$1\longrightarrow\rho(G)_L\cdot Z_{L'}\longrightarrow N_{L'}^{\circ}\longrightarrow\prod_{i=1}^{c}H^1(G(K_i'/K^{\sigma_i}),\ (\zeta_n)) .$$

(2) *If $k=Q$, and $(r, n)=1$, then we have the following exact sequence:*

$$1\longrightarrow\rho(G_L)\cdot Z_{L'}\longrightarrow N_{L'}^{\circ}\longrightarrow H^1(g,\ (\zeta_m)) ,$$

where $\mathscr{G}=G(K^{(\varepsilon\binom{n}{r})}/K)$, $\varepsilon=|U_K|(=2, 4$ *or* $6)$, $(\zeta_m)=(\zeta_n)\cap K^{(\varepsilon\binom{n}{r})}$.

If moreover, the discriminant of K is equal to -4 or $-p$ (p is an odd prime), and $(n, \varepsilon)=1$, then we have

$$N^{\circ}_{L'}=N(\rho(D))\cap G'_{L'}, \quad \textit{and} \quad H^1(\mathscr{G}, (\zeta_m))=\{1\} .$$

2.11. COROLLARY. *d_ρ is a divisor of $2^{d'}\prod_{i=1}^{c}|H^1(G(K_i'/K^{\sigma_i}), (\zeta_n))|$ (cf. 2.7). In particular, if $d'=0$ then $C(\mathscr{Y}^*)$ is a finite Abelian extension of $C(\rho(\mathscr{Y}^*))$ and Galois group of the extension is isomorphic to a subgroup of*

$$\prod_{i=1}^{c} H^1(G(K_i'/K^{\sigma_i}),\ (\zeta_n)) .$$

If moreover $k=Q$ and the discriminant of K is equal to -4 or $-p$, and $(r, n)=(n, \varepsilon)=1$, then $C(\mathscr{Y}^*)=C(\rho(\mathscr{Y}^*))$.

2.12. PROOF OF 2.10. In virtue of Proposition 2.3, we may assume that $c=d$, and also in view of 2.7, we may replace ρ by $\tilde{\rho}$, $Z_{L'}$ by $\tilde{Z}_{\tilde{L}}$, $N^{\circ}_{L'}$ by $\tilde{N}^{\circ}_{\tilde{L}}$ in the above sequences.

Suppose $\tilde{g}\in\tilde{N}^{\circ}_{\tilde{L}}$. Then by 2.3 and 2.7, $\tilde{g}=(\hat{g}_i)=(a_i\tilde{\rho}_i(g_i))$, for a scalar a_i and an element g_i of $G^{\sigma_i}_R$ $(i=1, \cdots, c)$. $\tilde{g}_i\in\tilde{G}^{\sigma_i}_{\tilde{L}^{\sigma_i}}$, so taking the determinant, we have $a_i^{\binom{n}{r}}\in U_{K^{\sigma_i}}$. Hence we may assume that $g_i\in G^{\sigma_i}_k$ in the above.

Especially if $k=Q$, then $\tilde{g}=a\tilde{\rho}(g)$ and $a^{\varepsilon\binom{n}{r}}=1$. So, if moreover $(r, n)=1$, i.e. $\tilde{\rho}$ is one to one, then g belongs to $K^{(\varepsilon\binom{n}{r})}$-rational points of the special unitary group G_R (with respect to the usual representation; $G_R\subset M(n, C)$).

Now, since $N^{\circ}_{\tilde{L}}$ is an arithmetic group, it has a finite number of generators $\{\tilde{g}^{(1)}, \cdots, \tilde{g}^{(t)}\}$. Put $\tilde{g}^{(j)}=(a_{ij}\cdot\tilde{\rho}_i(g_{ij}))$ for $i=1, \cdots, c$; $j=1, \cdots, t$. Suppose $\tilde{K}_i$ is a finite Galois extension of $K^{\sigma_i}(\zeta_n)$ such that $g_{ij}\in G^{\sigma_i}_{\tilde{K}_i}$ (with respect to the usual representation) for all $j=, \cdots, t$.

If $\tau\in G(\tilde{K}_i/K^{\sigma_i})$ then $a^{\tau}_{ij}\tilde{\rho}_i(g^{\tau}_{ij})=a_{ij}\tilde{\rho}_i(g_{ij})$, hence $g^{\tau-1}_{ij}\in(\zeta_n)$ and it gives rise to an element of $Z^1(G(\tilde{K}_i/K^{\sigma_i}), \tilde{K}_i^*)$. So by "Theorem 90" of Hilbert, $g^{\tau-1}_{ij}=c^{\tau-1}_{ij}\cdot 1_n$, for $c_{ij}\in\tilde{K}_i^*$. Here, we have $(c^{\tau-1}_{ij})_n=1$, so $c^n_{ij}\in K^{\sigma_i}$. We put $K_i'=K^{\sigma_i}(\zeta_n, c_{i1}, \cdots, c_{it})$, i$=1, \cdots, c$. Then $g_i\in G^{\sigma_i}_{K_i'}$, whenever $(a_i\tilde{\rho}_i(g_i))\in\tilde{N}^{\circ}_L$ for a suitable system of scalars $\{a_i\}$. This implies that K_i' is independent of the choice of the generators of $\tilde{N}^{\circ}_L$.

Let $(a_i\tilde{\rho}_i(g_i))\in\tilde{N}^{\circ}_L$, $(\tau_i)\in\prod_{i=1}^{c}G(K_i'/K^{\sigma_i})$. Then as above, $g_i^{\tau_i-1}\in(\zeta_n)$ and it gives rise to an element of $Z^1(G(K_i'/K^{\sigma_i}), (\zeta_n))$. In this way we get a map Ψ of $N^{\circ}_{\tilde{L}}$ into $\prod_{i=1}^{c}H^1(K_i'/K^{\sigma_i}), (\zeta^n))$, which is obviously well-defined.

Suppose $\tilde{g}=(a_i\tilde{\rho}_i(g_i))\in$ Ker (Ψ). Then $g_i\in SU(V^{\sigma_i}, H^{\sigma_i})$, so $a_i\in K^{\sigma_i}$. But as $a_i^{\binom{n}{r}}\in U_{K^{\sigma_i}}$, it follows that a_i itself is a unit of K^{σ_i}; which implies that $\tilde{g}\in\tilde{\rho}(G)_{\tilde{L}}$, Thus the exactness of the sequence is reduced to Lemma 2.8.

The exactness of the squence in (2) is proved similarly.

And if $(n, \varepsilon)=1$, then $d'=0$ because in that case n is odd.

The vanishing of the cohomology group in (2) requires more detailed consideration and will be proved in the Appendix.

APPENDIX

STRUCTURE OF THE GROUP $H^1(\mathscr{G}, (\zeta_n))$

1. Let us recall some of the notations which will be used here. If K is an algebraic number field of finite degree, we put $K^{(n)}=K(\zeta_n)$ where $\zeta_n=e^{2\pi i/n}$. And if K' is a Galois extension of K, we put $G(K'/K)=$Galois group of K'/K.

Also we denote by $d(K)$ the discriminant of K, and by U_K^1 the roots of unity contained in K.

If in particular, K is an imaginary quadratic number field, then we denote by ε the order of the group of untis U_K.

Finally, $(\zeta_n)=$the group of n-th roots of unity.

2. $Q^{(4)} \ni \sqrt{-1}$, $Q^{(8)} \ni \sqrt{2}$, $\sqrt{-2}$, $Q^{(p)} \ni \sqrt{\left(\frac{-1}{p}\right)p}$, for an odd prime p.

In fact $\left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\zeta_p{}^x\right)^2=\left(\frac{-1}{p}\right)p$. (Gaußian sum !)

3. If K is a quadratic number field then

$$Q^{(n)} \supset K \text{ if and only if } d(K) \text{ divides } n.$$

"Only if" part is obvious. (Look at the ramifying primes !)

"If" part follows directly from 2.

4. $U_{Q^{(n)}}^1=\begin{cases} (\zeta_n) & \text{if } n \text{ is even,} \\ (\zeta_{2n}) & \text{if } n \text{ is odd.} \end{cases}$

In fact, let $U_{Q^{(n)}}^1=(\zeta_{sn})$. Then $Q^{(n)}=Q^{(sn)}$, and $\varphi(n)=\varphi(sn)$. The statement follows from this easily.

5. Suppose K is a quadratic number field with the discriminant equal to -4 or $-p$ (p is an odd prime). The $U_{K^{(n)}}^1=U_K{}^1 \cdot U_{Q^{(n)}}^1$.

Moreover, if $d(K)=-p$, $p>3$, then $U_{K^{(n)}}^1=U_{Q^{(n)}}^1$.

In fact suppose there exists an element ζ_{sn} in $U_{K^{(n)}}^1$ which does not belong to

$U^1_{Q^{(n)}}$. Then we have $K^{(n)}=Q^{(sn)}$, and $[K^{(n)}:Q^{(n)}]=2$. By 3, we have $d(K)\nmid n$, $d(K)\mid sn$, and also $\varphi(sn)=2\cdot\varphi(n)$.

There are just four possibilities for such s and n:

(i) $s=2$, $(n,2)=2$,
(ii) $s=3$, $(n,3)=1$,
(iii) $s=4$, $(n,2)=1$,
(iv) $s=6$, $(n,6)=1$.

Now we use the assumption for the discriminant.

If $d(K)=-4$, then the only possible cases are (i) and (iii). And in the case (i), the exponent of 2 in n is equal to 1.

If $d(K)=-p$, then the only possible cases are $p=3$, and (ii) or (iv).

From these, we can get the statement easily.

6. REMARK. If we do not have the assumption for the discriminant, the above statement does not always hold. For example, take $K=Q(\sqrt{-5})$. Then $K^{(10)}=Q^{(20)}\ni\zeta_{20}$, and ζ_{20}, is not contained in $U^1_K\cdot U^1_{Q^{(10)}}$.

From now on we shall fix the field K to be an imaginary quadratic number field with the discriminant $d=-4$ or $-p$ (p is an odd prime). Also we put $\mathscr{G}^{(n)}=G(K^{(n)}/K)$.

7. Let A be a subgroup of $U^1_{K^{(n)}}$. Then there exists a subgroup A' of (ζ_n) and a subgroup A'' of $U_K{}^1$, such that

$$A=A'\times A'', H^1(\mathscr{G}^{(n)},A)=H^1(\mathscr{G}^{(n)},A')\times H^1(\mathscr{G}^{(n)},A''), \qquad \text{(direct)}.$$

Moreover, $H^1(\mathscr{G}^{(n)},A'')\cong\text{Hom}\,(\mathscr{G}^{(n)},A'')$.

In fact, firstly suppose that $U^1_{K^{(n)}}=U^1_{Q^{(n)}}$. Then in view of 4, $A=A'$ if n is even, and if n is odd, we can put $A'=A\cap(\zeta_n)$, $A''=A\cap\{\pm1\}$.

So, in virtue of 5, we may assume that $d=-4$ or -3, and $U^1_{K^{(n)}}\neq U^1_{Q^{(n)}}$.

If $d=-4$, we put

$$\begin{cases} A'=A\cap(\zeta_n),\ A''=A\cap U^1_K & \text{if } n \text{ is odd,}\\ A'=A\cap(\zeta_{n/2}),\ A''=A\cap U^1_K & \text{if } n \text{ is even, (hence}(n,4)=2) .\end{cases}$$

If $d=-3$, we put

$$\begin{cases} A'=A\cap(\zeta_n),\ A''=A\cap U^1_K & \text{if } n \text{ is odd, (hence } (n,6)=1),\\ A'=A\cap(\zeta_n),\ A''=A\cap(\zeta_3) & \text{if } n \text{ is even, (hence } (n,3)=1).\end{cases}$$

Thus we get $A=A'\times A''$. A', A'' are $\mathscr{G}^{(n)}$-invariant; $\mathscr{G}^{(n)}$ operates trivially on A''. This proves the statement.

8. Suppose $(n_1, n_2)=1$, and A is a subgroup of $(\zeta_{n_1n_2})$ such that $(|A|, \varepsilon)=1$. Then

$$H^1(\mathscr{G}^{(n_1n_2)}, A)\cong H^1(\mathscr{G}^{(n_1)}, A_1)\times H^1(\mathscr{G}^{(n_2)}, A_2)\ ,$$

$$A_i=A\cap(\zeta_{n_i})\ , \qquad (i=1, 2).$$

Firstly, let us show that

$$\mathscr{G}^{(n_1n_2)}=\mathscr{G}_1\times\mathscr{G}_2,\quad \mathscr{G}_i=\{\tau\in\mathscr{G}^{(n_1n_2)}\mid \tau|K^{(n_j)}=1\}\cong\mathscr{G}^{(n_i)}\ , \qquad (i+j=3)\ .$$

In fact, if $Q^{(n_1)}$, $Q^{(n_2)}\not\supset K$, then using the condition on the discriminant (see 6), $Q^{(n_1n_2)}\not\supset K$. Therefore

$$[K^{(n_1n_2)} : K]=\varphi(n_1n_2)=[K^{(n_1n_2)} : K^{(n_1)}]\cdot[K^{(n_1)} : K]\ ,$$

therefore

$$[K^{(n_1n_2)} : K^{(n_1)}]=\varphi(n_2)\ ,$$

which implies that

$$G(K^{(n_1n_2)}/K^{(n_1)})\cong G(Q^{(n_2)}/Q)\ , \qquad G(K^{(n_1)}/K)\cong G(Q^{(n_1)}/Q)\ ,$$

$$G(K^{(n_1n_2)}/K)\cong G(Q^{(n_1)}/Q)\times G(Q^{(n_2)}/Q)\ .$$

If $Q^{(n_1)}\supset K$, then as $Q^{(n_1)}\cap Q^{(n_2)}=Q$, we have $Q^{(n_2)}\not\supset K$, $Q^{(n_1n_2)}\supset K$. Using an argument similar to the above, we get the desired decomposition of the Galois group.

Now we have

$$A_i^{\mathscr{G}_j}=\{a\in A_i\mid a^\tau=a, \tau\in\mathscr{G}_j\}=A\ ,$$

$$A_i^{\mathscr{G}_i}=\{1\}\ ,\ (i+j=3)\ .$$

Hence we have the following exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & H^1(\mathscr{G}_i, A_i^{\mathscr{G}_j}) \arrow[r, dash, "\mathrm{Inf}"] \arrow[d, equal] & H^1(\mathscr{G}, A_i) \arrow[r, dash, "\mathrm{Res}"] & H^1(\mathscr{G}_j, A_i) \\
 & H^1(\mathscr{G}_i, A_i) & & \\
1 \arrow[r] & H^1(\mathscr{G}_j, A_i^{\mathscr{G}_i}) \arrow[r, "\mathrm{Inf}"] \arrow[d, equal] & H^1(\mathscr{G}, A_i) \arrow[r, dash, "\mathrm{Res}"] & H^1(\mathscr{G}_i, A_i)\ , \\
 & \{1\} & &
\end{tikzcd}$$

$$(\mathscr{G}=\mathscr{G}^{(n_1n_2)})\ .$$

(Cf. [22, §6, Chapter VII].)

From these it follows that

$$H^1(\mathscr{G}, A_i)\cong H^1(\mathscr{G}_i, A_i)\ .$$

Hence we have

$$H^1(\mathscr{G}, A)\cong H^1(\mathscr{G}, A_1)\times H^1(\mathscr{G}, A_2)\cong H^1(\mathscr{G}^{(n_1)}, A_1)\times H^1(\mathscr{G}^{(n_2)}, A_2)\ .$$

9. The structure of the group $G(Q^{(p^e)}/Q)$ is well-know [10]. To describe them, let us put $(n)_m$=the congruence class of n mod. m, for $n, m\in Z$. $G(Q^{(m)}/Q)$ is isomorphic to the multiplicative group formed by

$$\{(n)_m \mid n\in Z,\ (n, m)=1\}\ .$$

(1) $\tilde{\mathscr{G}}=G(Q^{(p^e)}/Q)$, p is an odd prime:—

$$\tilde{\mathscr{G}}=\tilde{\mathscr{G}}_1\times\tilde{\mathscr{G}}_2\ ,$$

$$\tilde{\mathscr{G}}_1\cong C_{p-1}=\text{the cyclic group of order } p-1\ ,$$

$$\tilde{\mathscr{G}}_2\cong C_{p^{e-1}}\ .$$

Moreover, $\tilde{\mathscr{G}}_2$ is generated by $(p+1)_{p^e}$ and

$$\tilde{\mathscr{G}}_2=\{(m)_{p^e}\mid \mathrm{m}\equiv 1 \text{ mod. } p\}\ .$$

Also if $\tau\in\tilde{\mathscr{G}}_1$, $\tau\neq 1$, then we have

$$(\zeta_{p^e})^{(\tau)}=\{1\}\ .$$

(2) $\tilde{\mathscr{G}}=G(Q^{(2^e)}/Q)$, $e\geqslant 3$:—

$$\tilde{\mathscr{G}}=\tilde{\mathscr{G}}_1\times\tilde{\mathscr{G}}_2,\ \tilde{\mathscr{G}}_1=\{(-1)_{2^e}\},\ \tilde{\mathscr{G}}_2\cong C_{2^{e-2}}\ ,$$

and $\tilde{\mathscr{G}}_2$ is generated by $(5)_{2^e}$.

10. LEMMA. *Suppose $\mathscr{G}$ is a finite group of order c, and A is a $\mathscr{G}$-module, such that $c: A\ni a\longrightarrow c\cdot a=\underbrace{a+a+\cdots+a}_{c}\in A$ is a bijective endomorphism. Then for $q\geqslant 1$, we have $H^q(\mathscr{G}, A)=\{0\}$.*

PROOF. If $f\in Z^q(\mathscr{G}, A)$, we put $h(g_1,\cdots,g_{q-1})=c^{-1}\sum_{g\in\mathscr{G}} f(g_1,\cdots,g_{q-1}, g)$. Then $d((-1)^q h)=f$.

11. PROPOSITION. *Suppose A is a finite group of roots of unity such that $(|A|, \varepsilon)=1$, and on which $\mathscr{G}^{(n)}$ operates. Then for any n, we have $H^1(\mathscr{G}^{(n)}, A)=\{1\}$.*

PROOF. By 7, 8 and 10, we may assume that $n=q^e$ for odd prime q, and the that $A\subset(\zeta_n)$.

(i) Suppose $d(K)\nmid q^e$:—

By 3, $\mathscr{G}^{(n)}\cong G(Q^{(n)}/Q)$ canonically. So, $\mathscr{G}^{(n)}=\mathscr{G}_1\times\mathscr{G}_2$, $\mathscr{A}^{\mathscr{G}_1}=\{1\}$. And we have the following exact sequence:

$$\begin{tikzcd}
1 \arrow[r] & H^1(\mathscr{G}_2, A^{\mathscr{G}_1}) \arrow[r, "\mathrm{Inf}"] \arrow[d, equal] & H^1(\mathscr{G}^{(n)}, A) \arrow[r, "\mathrm{Res}"] & H^1(\mathscr{G}_1, A)\ . \\
 & \{1\} & &
\end{tikzcd}$$

And moreover $\mathscr{G}_1\cong C_{q-1}$. Hence, by Lemma 10, $H^1(\mathscr{G}^{(n)}, A)=\{1\}$.

(ii) Suppose $d(K)\mid q^e$:—

Under our assumption, we many assume that $q\neq 3$. Because if $q=3$, then $d(K)=-3$, therefore $\varepsilon=6$, which contradicts with our assumption $(n, \varepsilon)=1$. By 3, we now have

$$\mathscr{G}^{(n)}=\mathscr{G}_1\times\mathscr{G}_2\ , \qquad \mathscr{G}_1\cong C_{\frac{q-1}{2}}\ , \qquad \mathscr{G}_2\cong C_{q^{e-1}}\ .$$

As $q>3$, $\mathscr{G}_1$ is non-trivial. This makes it possible to repeat the same argument as above and we can get the desired result.

12. REMARK. The above proposition completes the proof for the Theorem 2.10 of the last chapter. But using the same method, we can get further information about the structure of $H^1(\mathscr{G}^{(q^e)}, A)$, where q is a prime and A is a subgroup of (ζ_{q^e}), of course different from $\{1\}$.

We put $d=d(K)(=-4$ or $-p)$, $|A|=q^f$ $(0<f\leqslant e)$. Then we get the following table:

	$d\nmid q^e$ $q\neq 2$	$d=-p,\ q=2$	$d\mid q^e$ $q\neq 2, 3$	$d=-4, q=2, e\geqslant 3$	$d=-3, q=3, e\geqslant 2$
$H^1(\mathscr{G}^{(q^e)}, A)$	$\{1\}$	C_2 $(e=2)$ $C_2\times C_2$ $(e\geqslant 3)$	$\{1\}$	$\{1\}$ $(e=f)$ C_4 $(e-f, f\geqslant 2)$ C_2 (otherwise)	$\{1\}$ $(e=f)$ C_3 $(e>f)$

An explanation may be in order the case where $d=-p$, $q=2$, and $e\geqslant 3$. In this case, we can identify $\mathscr{G}^{(2^e)}$ with $G(Q^{(2^e)}/Q)=\tilde{\mathscr{G}}_1\times\tilde{\mathscr{G}}_2$, where $\tilde{\mathscr{G}}_1$, $\tilde{\mathscr{G}}_2$ are generated by $(-1)_{2^e}$, $(5)_{2^e}$ respectively. And we get the exact sequence

$$1\longrightarrow H^1(\tilde{\mathscr{G}}_2, A^{\mathscr{G}_1})\xrightarrow{\mathrm{Inf}} H^1(\tilde{\mathscr{G}}^{(2^e)}, A)\xrightarrow{\mathrm{Res}} H^1(\tilde{\mathscr{G}}_1, A),$$

and

$$H^1(\tilde{\mathscr{G}}_2, A^{\mathscr{G}_1})\cong H^1(\tilde{\mathscr{G}}_1, A)\cong C_2\ .$$

$\{c_5=-1, c_{-1}=i\}$ and $\{c_5=1, c_{-1}=-i\}$ give rise to two 1-cocycles which become the generators of $H^1(\mathscr{G}^{(2^e)}, A)\cong C_2\times C_2$.

University of Tokyo

References

[1] W. L. Baily, Jr. and A. Borel, Compactification of arithmetic quotients of bounded symmetric domains, Ann. of Math. (3), **84** (1966), 442-528.

[2] A. Borel, Density and maximality of arithmetic subgroups, J. Reine Angew. Math., **224** (1966), 78-89.

[3] ———, "Linear algebraic groups," in Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R. I., 1966.

[4] ———, "Reduction theory for arithmetic groups," ibid.

[5] A. Borel and Harish-Chandra, Arithmetic subgroups of algebraic groups, Ann. of Math. (2), **75** (1962), 485-535.

[6] A. Borel and J. Tits, "Groupes réductifs," in Publ. I.H.E.S. **27** (1965), 55-150.

[7] E. Cartan, Sur les domaines bornés homogènes de l'espace de n variables, Abh. Math. Sem. Hamburg, **11** (1935), 116-162.

[8] C. W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience Publ., New York, London, 1962.

[9] W. F. Hammond, The modular groups of Hilbert and Siegel, Amer. J. Math. **88** (1966), 497-516.

[10] H. Hasse, Vorlesungen über Zahlentheorie, Springer, Berlin-Göttingen-Heidelberg, 1964.

[11] S. Helgason, Differential Geometry and Symmetric Spaces, Academic Press, New York, 1962.

[12] K. Iwasawa, Group of units of an algebraic number field, J. Math. Pures Appl. **35**, (1956), 184-192.

[13] R. Jacobowitz, Hermitian forms over local fields, Amer. J. Math., **84** (1962), 441-465.

[14] H. Klingen, Über einen Zusammenhang zwischen Siegelschen und Hermiteschen Modulfunktionen, Abh. Math. Sem. Hamburg, **27** (1964), 1-12.

[15] H. Matsumoto, Quelques remarques sur les groupes de Lie algébriques réels, J. Math. Soc. Japan, **16** (1964), 419-446.

[16] O. T. O'Meara, Introduction to Quadratic Forms, Academic Press, New York, 1963.

[17] I. Satake, Maximal compact subgroups of $\mathfrak{p}$-adic algebraic groups, (Japanese), Sugaku no. 1, **13** (1961), 36-39.

[18] ———, Holomorphic imbeddings of symmetric domains into a Siegel space, Amer. J. Math., **87** (1964), 425-461.

[19] ———, A note on holomorphic imbeddings and compactifications of symmetric domains, Amer. J. Math., to appear.

[20] ———, Symplectic representations of algebraic groups satisfying a certain analiticity condition, Acta Math., **117** (1967), 215-279.

[21] ———, Introduction to automorphic forms, mimeographed notes of the lectures at University of Chicago, 1967.

[22] J. P. Serre, Corps locaux, Actualités Sci. Ind., 1296, Hermann, Paris, 1962.

[23] G. Shimura, Arithmetic of alternating forms and quaternion hermitian forms, J. Math. Soc. Japan, **15** (1963), 33-65.

[24] ———, Arithmetic of unitary groups, Ann. of Math., (2), **79** (1964), 369-409.

[25] T. Takagi, Algebraic Number Theory, (Japanese), Iwanami Shoten, 1947.

[26] E. Witt, Eine Identität zwischen Modulformen zweiten Grades, Abh. Math. Sem. Hamburg, **14** (1941), 323-337.

(Received October 20, 1967)