Tôhoku Math. J.
41 (1989), 1–30

CLASS NUMBERS OF DEFINITE UNIMODULAR HERMITIAN FORMS OVER THE RINGS OF IMAGINARY QUADRATIC FIELDS

Dedicated to Professor Ichiro Satake on his sixtieth birthday

KI-ICHIRO HASHIMOTO AND HARUTAKA KOSEKI

(Received December 10, 1986)

CONTENTS

Introduction.

0.1. Hermitian forms, or lattices in Hermitian metric spaces, have been studied by many authors in various context. Over global fields or rings, one defines in a given Hermitian space the genera and the classes of lattices, which are of central interests in the arithmetic of Hermitian forms. Especially to determine the number of classes in a given genus is one of the fundamental problems. If the form is indefinite, this problem was solved by Shimura [19], and the class number is then equal to the class number of the base field, up to certain elementary factors. On the other hand, if the form is definite at all Archimedean places, very little is known about the class numbers, except some special results that we mention below. In fact, it is quite difficult to compute the class numbers of definite Hermitian forms of higher ranks. Even in cases of low ranks, one has to specify a number of parameters (the base field, isometry class of Hermitian space, and genus), as well as the group (i.e., unitary, or special unitary group, etc.) with respect to which the class number is defined. This is perhaps another reason that there are only a few results for the class numbers, compared with those for quadratic forms (cf. (0.3)).

In a series of papers which follow, we shall determine the class numbers of positive Hermitian forms of low ranks, over the rings of integers of the imaginary quadratic fields. In this first paper, we deal with general results which provide an effective procedure to compute the class number of definite Hermitian forms of a given genus: We present, among others, (1) a general formula (Theorem 3.2) for the class number of a given genus, which is a reformulation of a result of the first author (cf. [6]). Up to the local factors, it is a sum of the masses of (idelic) arithmetic subgroups of the centralizers of certain torsion elements in the unitary group. We shall also give (2) explicit formulas for these masses with respect to the principal genera, and as an application we give (3) a lower and an upper estimate for the class number, in terms of the mass. These are the first main results of this paper. Using these results, we shall derive in our forthcoming paper [10], explicit formulas for the class numbers of an arbitrary genus consisting of *unimodular* Hermitian lattices of rank *two*, and the principal genus of rank *three*. As for the second point noted above, we shall give (4) a relation between the class numbers with respect to the unitary group and the special unitary group (Theorem 2.9), which holds under some conditions.

0.2. Now we mention briefly the explicit results which have been known. The first general result on the class numbers of definite Hermitian forms is that of Hayashida [12]. There he gave an explicit formula for the class numbers of the positive unimodular Hermitian matrices of rank two, with coefficients in the ring $\mathcal{O}$ of integers of an arbitrary imaginary quadratic field. As we shall see in § 2, this result can be interpreted as giving the class numbers of certain genera of unimodular Hermitian lattices. We shall give in [10] a simplified proof for it, as well as its generalization. The next general result is that of Otremba [18], where he computed explicitly the mass (or average) for the representation numbers of definite Hermitian matrices over $\mathcal{O}$, using a result of Braun [4]. Especially he gave an explicit formula for the mass of a given genus, from which one can derive a list of genera having class number one (cf. Proposition 5.13). This result is very important, because the mass of a genus is regarded as giving the main term for the class number formula, when the discriminant of K and $\mathscr{L}$ increase (see Theorem 5.11). While Otremba computed the mass by means of Gauss sums, we shall reproduce the same result in the special case of the principal genus, by a more direct and elementary method, which is easily generalized to the cases where the basic field is an abelian extension over $\boldsymbol{Q}$. We should refer also to a work of Iyanaga [13], who determined the class numbers of unimodular Hermitian forms over the ring $\boldsymbol{Z}[i]$ of Gaussian integers of rank $n=1, 2, \cdots, 7$. However the method he used (i.e., Kneser's method of adjacent lattices) does not seem to be extended easily to the general base field.

0.3. The method we shall use to compute the class numbers is an arithmetic version of the trace formula (cf. Hashimoto [6]). This has been proved to be useful for the class number calculations by many authors such as Eichler, Pizer, Ponomarev, Asai and Hashimoto-Ibukiyama, in the cases where the groups are obtained from quaternion algebras (cf. [5], [8]), or orthogonal groups (cf. [2]). Although the general procedure in our calculation does not differ from those in the above works, there are some features which are proper to the unitary groups. For example, the fact that the base field has a parameter causes an essential difference. This is one of the reasons why we think it convenient to collect here basic facts in the form useful for our purpose, although some of them could be found in the literature.

0.4. This paper is organized as follows:

In § 1, we recall the definitions and basic facts on the unitary groups and genera of a given Hermitian space. In § 2, we study the relation between the class numbers with respect to the unitary group and the special unitary group. A general formula for the class numbers will be given in § 3. In § 4, we study the structure or the parametrization of conjugacy classes in the unitary group over a field of characteristic zero. Then we specialize to the case of local and global fields, and describe the image under the natural mapping of the conjugacy classes over global fields, in the conjugacy classes of the idele groups. This part follows from Asai [1], who omitted the details in the case of unitary groups. In § 5, we calculate the mass of the principal genus of positive Hermitian forms by a method different from Otremba [18]. Applying the mass formula, we also give new remarks on the lower and upper bounds for the class numbers. In § 6 we recall briefly results of Landherr [15], Jacobowitz [14], on the Hermitian spaces and genera of unimodular lattices.

NOTATION. As usual, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ denote the field of rational, real, and complex numbers, respectively, and $\boldsymbol{Z}$ denotes the ring of rational integers. For an algebraic object B over $\boldsymbol{Q}$ or $\boldsymbol{Z}$, we denote by B_p the p-adic completion of B. Thus $\boldsymbol{Q}_p$ (resp. $\boldsymbol{Z}_p$) is as usual the field (resp. ring) of p-adic numbers (resp. integers). Also we denote by $B_{\mathbb{A}}$ the idelization of B. If G is a group, and H is a subgroup of G, we denote the set of H-conjugacy classes in G by $G /\!/ H$, and its element containing g by $[g]_H$. When $H = \mathbb{G}$ is a $\boldsymbol{Q}$-group, we put simply $[g]_{\boldsymbol{Q}} := [g]_G$, $[g]_p := [g]_{G_p}$, where $G = \mathbb{G}_{\boldsymbol{Q}}$, G_p are the group of $\boldsymbol{Q}$-rational, $\boldsymbol{Q}_p$-rational points of $\mathbb{G}$, respectively. Also, we denote by $\mathbb{G}(g)$ the centralizer of g in $\mathbb{G}$. The cardinality of a finite set S is written as $\sharp(S)$. Throughout this paper, K denotes an imaginary quadratic field. For $c \in \boldsymbol{Q}^\times$ and a place v of $\boldsymbol{Q}$, we denote by $(c, K/\boldsymbol{Q})_v$ the local norm residue symbol of c, i.e., $(c, K/\boldsymbol{Q})_v = 1$ or -1 according as c is a norm of an element of $K_v^\times$ or not. Notice that we have $(c, K/\boldsymbol{Q})_v = (c, m)_v$ ($:=$ the Hilbert symbol) if $K = \boldsymbol{Q}(\sqrt{m})$. Also we denote by $\chi(*) = (K/*) = (d(K)/*)$ the Dirichlet character attached to K, where $d(K)$ is the discriminant of K.

1. Hermitian forms and unitary groups. Let K be an imaginary quadratic field and let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers of K. For any place v of $\boldsymbol{Q}$, we put $K_v := K \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_v$. Also we put $\mathcal{O}_p := \mathcal{O} \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p$ at any finite place p of $\boldsymbol{Q}$, and $\boldsymbol{Z}_\infty := \boldsymbol{R}$, $\mathcal{O}_\infty := \boldsymbol{C}$ at the infinite place ∞. Denote by ρ the non-trivial automorphism of $K/\boldsymbol{Q}$. Let (V, H) be a non-degenerate ρ-Hermitian space over K. Namely V is a (left) vector space over K, and $H\colon V \times V \to K$ is a $\boldsymbol{Q}$-bilinear form which satisfies the following conditions:

(i) $H(ax, y) = a \cdot H(x, y)$ for any $a \in K$, $x, y \in V$.

(ii) $H(y, x) = H(x, y)^\rho$ for any $x, y \in V$;

and (V, H) being nondegenerate means that

(iii) if $H(x, y) = 0$ for any $y \in V$, then $x = 0$.

Now we put $\mathbb{G} := \mathbb{U}(V, H)$. Namely $\mathbb{G}$ is the unitary group of (V, H), which is a reductive group defined over $\boldsymbol{Q}$ whose set $G = \mathbb{G}_{\boldsymbol{Q}}$ of $\boldsymbol{Q}$-rational points is given by

$$G := \{g \in GL_K(V);\ H(xg, yg) = H(x, y) \text{ for any } x, y \in V\}\,.$$

For any place v of $\boldsymbol{Q}$, we denote by $(V, H)_v$ or (V_v, H) the completion of (V, H) at v, i.e., $V_v := V \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_v$ and H is the unique continuous extension of $H\colon V \times V \to K$ to $V_v \times V_v \to K_v$. It is a non-degenerate ρ-Hermitian space over K_v.

Let L be an $\mathcal{O}$-lattice in V. Namely, L is a finitely generated $\mathcal{O}$-module in V which contains a basis of V over K so that $K \cdot L = V$. We put $L_v := \mathcal{O}_v \cdot L$ at any place v of $\boldsymbol{Q}$ and see that L_v is an $\mathcal{O}_v$-lattice in V_v. Let U_v be the open subgroup of $G_v := \mathbb{U}(V_v, H)$ defined by

$$U_v := \{g \in G_v;\ L_v \cdot g = L_v\}\,,$$

and put

$$\boldsymbol{U} = \boldsymbol{U}(L) := \prod_v U_v\,. \tag{1.1}$$

This is an open subgroup of $G_{\mathbb{A}}$, the idele group of $\mathbb{G}$. As a subgroup of $GL(K_{\mathbb{A}})$, the group $G_{\mathbb{A}}$ acts naturally on the set of $\mathcal{O}$-lattices in V:

$$L \cdot g := \bigcap_v (L_v \cdot g_v \cap V)\,.$$

The group $\boldsymbol{U}(L)$ is the stabilizer of L in $G_{\mathbb{A}}$. The G-genus $\mathscr{L} = \mathscr{L}(L)$ is by definition the $G_{\mathbb{A}}$-orbit of L. Namely, it consists of the $\mathcal{O}$-lattices L' in V such that for any v there exists $g_v \in G_v$ with $L'_v = L_v \cdot g_v$. Obviously, $\mathscr{L}(L)$ is stable under G. Each G-orbit in $\mathscr{L}(L)$ is called a G-class in $\mathscr{L}(L)$. It follows that the set of G-classes is in one-to-one correspondence with the double coset space $\boldsymbol{U}(L)\backslash G_{\mathbb{A}}/G$. The cardinality of this set is called the *class number* of $\mathscr{L}(L)$ with respect to $\mathbb{G}$ and denoted by $\boldsymbol{h}(\mathscr{L}(L))$. Thus we have, for the G-genus $\mathscr{L} = \mathscr{L}(L)$.

$$\boldsymbol{h}(\mathscr{L}) = \sharp[\boldsymbol{U}(L)\backslash G_{\mathbb{A}}/G]\,. \tag{1.2}$$

Now let $\mathbb{G}^{(1)} := \mathbb{SU}(V, H) = \mathbb{U}(V, H) \cap \mathbb{SL}(V)$ be the special unitary group of (V, H). Then, in exactly the same way as for $\mathbb{G}$, we can define the genus $\mathscr{L}^{(1)} = \mathscr{L}^{(1)}(L)$ as the $G_{\mathbb{A}}^{(1)}$-orbit of L, and see that the class number $\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})$ of $\mathscr{L}^{(1)}$ (with respect to $\mathbb{G}^{(1)}$) is equal to

$$\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)}) = \sharp[\boldsymbol{U}^{(1)}(L)\backslash G_{\mathbb{A}}^{(1)}/G^{(1)}]\,. \tag{1.3}$$

Now the reduction theory of Borel and Harish-Chandra [3] shows that the homogeneous space $G_{\mathbb{A}}^{(1)}/G^{(1)}$ has finite volume with respect to an invariant measure of $G_{\mathbb{A}}^{(1)}$, from which follows that the class numbers $\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})$ and $\boldsymbol{h}(\mathscr{L})$ are *finite* for any genus of $\mathcal{O}$-lattices. Moreover, if $(V, H)_\infty$ is *indefinite*, then by Shimura [19] we know, as an application of the strong approximation theorem, that $\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})$ is always equal to *one*, and that $\boldsymbol{h}(\mathscr{L})$ is equal to the class number $h(K)$ of K multiplied by certain elementary factors. If, on the other hand, $(V, H)_\infty$ is definite, it is in general quite difficult to determine the class number for a given genus.

2. Class number relation between $\mathbb{U}(n)$ and $\mathbb{SU}(n)$.

2.1. In this section, we consider general questions concerning (possible) relations between genera and class numbers in a given Hermitian space (V, H) with respect to $\mathbb{G}=\mathbb{U}(V, H)$ and $\mathbb{G}^{(1)}=\mathbb{SU}(V, H)$, which are suggested by our main results in binary and ternary cases. Namely, for a given $\mathbb{G}$-genus $\mathscr{L}$ of $\mathcal{O}$-lattices, we ask:

(2.1) How can one describe the decomposition of $\mathscr{L}$ into the disjoint union of $\mathbb{G}^{(1)}$-genera?

(2.2) Let $\mathscr{L}^{(1)}$ be one of the $\mathbb{G}^{(1)}$-genera in $\mathscr{L}$. Then in which way the class numbers $\boldsymbol{h}(\mathscr{L})$ and $\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})$ are related? Can one show that the latter is independent of the choice of $\mathscr{L}^{(1)}$?

There is another question concerning the class number of a genus $\mathscr{L}$ and that of the equivalence classes in the integral Hermitian matrices. For simplicity, let us assume that $\mathscr{L}$ is the principal genus. Then we may ask:

(2.3) Describe, if any, a relation between the class numbers of $\mathscr{L}$, $\mathscr{L}^{(1)}$ and those of the integral unimodular Hermitian matrices.

We note that complete answers to these questions were given by Shimura [19], in the case (V, H) is indefinite. Following his method, we can give answers to them also in the case (V, H) is definite. Suppose we are given an $\mathcal{O}$-lattice L hence the genus $\mathscr{L}=\mathscr{L}(L)$. For each member M of $\mathscr{L}$ we define a fractional ideal $[L:M]$ in K by

$$[L:M]:=\{\det(g);\, g\in \mathrm{End}_K(V),\, L\cdot g\subset M\}\mathcal{O}\,. \tag{2.4}$$

Then it is easily seen that $[L:M]$ has the following properties (cf. [19]):

(i) $[L:M][M:N]=[L:N]$

(ii) If $L\supset M$ and $L/M\simeq \mathcal{O}/\mathfrak{a}$ as $\mathcal{O}$-modules, then $[L:M]=\mathfrak{a}$.

(iii) $[L:L\cdot g]=(\det(g))\mathcal{O}$ for any $g\in GL_K(V)$.

(iv) $[L:M]\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p=[L_p:M_p]$ for any p,

where $[L_p:M_p]$ is the ideal in K_p defined similarly as in (2.4). Denote by $\mathbb{P}$ the group of fractional ideals $\mathfrak{a}$ in K such that $N_{K/\boldsymbol{Q}}(\mathfrak{a})=(1)$. Then we have $\mathbb{P}\simeq K_{\mathbb{A}}^{(1)}/\mathcal{O}_{\mathbb{A}}^{(1)}$. Here, for a subgroup J of $K_{\mathbb{A}}^\times$ we put $J^{(1)}:=J\cap \mathrm{Ker}(N_{K/\boldsymbol{Q}}\colon K_{\mathbb{A}}^\times\to \boldsymbol{Q}_{\mathbb{A}}^\times)$. For $\mathfrak{a}\in\mathbb{P}$, we put

$$\mathscr{L}_{\mathfrak{a}}:=\{M\in\mathscr{L};\, [L:M]=\mathfrak{a}\}\,. \tag{2.5}$$

Then the following lemma is immediately checked.

LEMMA 2.1. *We have* $\mathscr{L}=\bigcup_{\mathfrak{a}\in\mathbb{P}}\mathscr{L}_{\mathfrak{a}}$ (disjoint), *hence the mapping* $\mathscr{L}\to\mathbb{P}$, *sending*

$M \in \mathscr{L}_{\mathfrak{a}}$ to $\mathfrak{a}$, gives a fibration of $\mathscr{L}$ over $\mathbb{P}$. Moreover, each fibre $\mathscr{L}_{\mathfrak{a}}$ is stable under the natural action of $G_{\mathbb{A}}^{(1)}$.

It follows that, if we let $G_{\mathbb{A}}$ act on $\mathbb{P}$ through the multiplication of the determinant of its elements, the above fibration is $G_{\mathbb{A}}$-equivariant. Now define subgroups G^{u}, $G_{\mathbb{A}}^{u}$ of G, $G_{\mathbb{A}}$, respectively, by

$$(2.6) \qquad G_{\mathbb{A}}^{u} := \{g \in G_{\mathbb{A}};\ \det(g) \in \mathcal{O}_{\mathbb{A}}^{(1)}\}\,,$$
$$G^{u} := G_{\mathbb{A}}^{(1)} \cap G = \{g \in G;\ \det(g) \in W(K)(:=\mathcal{O}^{(1)})\}\,.$$

Then we see, more precisely, that each $\mathscr{L}_{\mathfrak{a}}$ is $G_{\mathbb{A}}^{u}$-stable and that the stabilizer of each point in $\mathbb{P}$ is $G_{\mathbb{A}}^{u}$, since we have

$$G_{\mathbb{A}}/G_{\mathbb{A}}^{u} \underset{\det}{\overset{\simeq}{\to}} K_{\mathbb{A}}^{(1)}/K^{(1)} \simeq \mathbb{P}\,.$$

LEMMA 2.2. *We have*

$$\boldsymbol{h}(\mathscr{L}) = \sum_{[\mathfrak{a}] \in \mathbb{P}/K^{(1)}} \sharp[\mathscr{L}_{\mathfrak{a}}/G^{u}]\,,$$

where the summation is taken over the ideal classes $[\mathfrak{a}]$ *(in the principal genus) represented by* $\mathfrak{a} \in \mathbb{P}$.

PROOF. First note that $\mathbb{P}/K^{(1)} \simeq \{$ideal classes in the principal genus$\}$, which follows from Hilbert's theorem 90. Then the assertion is a consequence of the fact that $G_{\mathbb{A}}^{u}$ (resp. G) acts on each $\mathscr{L}_{\mathfrak{a}}$ (resp. ideal class $[\mathfrak{a}]$) transitively, and that the stabilizer of $\mathfrak{a}$ is G^{u}. q.e.d.

Since G^{u} and $G^{(1)}$ are normal subgroups of G, we have the following from the above argument:

COROLLARY 2.3. *Suppose* $[\mathfrak{a}] = [\mathfrak{b}]$ *for* $\mathfrak{a}, \mathfrak{b} \in \mathbb{P}$. *Then we have*

$$\sharp[\mathscr{L}_{\mathfrak{a}}/G^{u}] = \sharp[\mathscr{L}_{\mathfrak{b}}/G^{u}]\,, \qquad \sharp[\mathscr{L}_{\mathfrak{a}}/G^{(1)}] = \sharp[\mathscr{L}_{\mathfrak{b}}/G^{(1)}]\,.$$

Next we decompose $\mathscr{L}_{\mathfrak{a}}$ into the union of $G_{\mathbb{A}}^{(1)}$-orbits. For this purpose we put $e = e(\mathscr{L}) := [\mathcal{O}_{\mathbb{A}}^{(1)}: \det(U(L))]$. Note that e is determined by $\mathscr{L}$ and is independent of the choice of L.

LEMMA 2.4. (i) *Each $\mathscr{L}_{\mathfrak{a}}$ is a disjoint union of exactly e $G_{\mathbb{A}}^{(1)}$-genera.*

(ii) *We always have $e \leq 2$; and $e=1$ if L_p $(p=2)$ contains a normal modular component at the prime $p=2$ which is always the case for $n=$ odd or $(K/2) \neq 0$.*

(iii) *If $n=2$, and L is unimodular, then* $e=2 \Leftrightarrow d(K) \equiv 12 \pmod{16}$ *and L is subnormal.*

(See §6 *for the definition of normal, or subnormal unimodular lattices).*

PROOF. The first assertion is a direct consequence of the fact that $\mathscr{L}_{\mathfrak{a}}$ consists of a single $G^u_{\mathbb{A}}$-orbit, and that, if we write $M \in \mathscr{L}_{\mathfrak{a}}$ as $M = L \cdot g$ ($g \in G_{\mathbb{A}}$), the stabilizer of M in $G_{\mathbb{A}}$ is $\boldsymbol{U}(M) = g^{-1}\boldsymbol{U}(L)g$. The assertions (ii), (iii) are easy consequences of the results in [10, §3], and we omit the details. q.e.d.

Now we assume, throughout the following, that (V, H) is positive definite. Denote by $\Gamma(M)$ the unit group of an $\mathcal{O}$-lattice. The following result refines Proposition 1.8 of Iyanaga [13].

PROPOSITION 2.5. *For each* $\mathfrak{a} \in \mathbb{P}$, *let* $M_1, \cdots, M_\kappa$ *be a complete representatives of the* G^u*-orbits in* $\mathscr{L}_{\mathfrak{a}}$. *Then we have*

$$\sharp[\mathscr{L}_{\mathfrak{a}}/G^{(1)}] = \sharp(W(K)) \cdot \sum_{j=1}^{\kappa} \frac{1}{\sharp[\det(\Gamma(M_j))]}\,.$$

PROOF. Let $M^{(i)}$ $(1 \leq i \leq \lambda)$ be a complete representatives of the $G^{(1)}$-orbits in $\mathscr{L}_{\mathfrak{a}}$, so that $\mathscr{L}_{\mathfrak{a}} = \bigcup_i G^{(1)} \cdot M^{(i)}$. If we let G^u act on the set of these $G^{(1)}$-orbits, we see that it factors through the quotient $G^u/G^{(1)} \simeq W(K)$, which is a cyclic group with a generator, say, ζ. Now if $M_j = M^{(1)}, \cdots, M^{(m)}$ are the members of a $W(K)$-orbit under this action, we clearly have $\det(\Gamma(M_j)) = \langle \zeta^m \rangle$, hence $m = \sharp(W(K))/\sharp[\det(\Gamma(M_j)]$. Summing these equalities over j, we get the result. q.e.d.

COROLLARY 2.6. *Suppone* n = *odd, and either* $K \neq \boldsymbol{Q}(\sqrt{-3})$ *or* $(n, 3) = 1$. *Then*:
(i) *Each* $\mathscr{L}_{\mathfrak{a}}$ *consists of a single* $G^{(1)}$*-genus.*
(ii) $\boldsymbol{h}^{(1)}(\mathscr{L}_{\mathfrak{a}}) = \sharp[\mathscr{L}_{\mathfrak{a}}/G^u]$,
(iii) $\boldsymbol{h}(\mathscr{L}) = \sum_{[\mathfrak{a}] \in \mathbb{P}/K^{(1)}} \boldsymbol{h}^{(1)}(\mathscr{L}_{\mathfrak{a}})$.

PROOF. (i) follows from our assumption n = odd and Lemma 2.4. Moreover, the additional assumption implies $(n, \sharp(W(K))) = 1$, so that $\zeta \longmapsto \zeta^n$ is an automorphism of $W(K)$. It follows that the determinant of the scalar matrix $\zeta \cdot 1_n$ $(\in \Gamma(M))$ generates $W(K)$, hence $\det(\Gamma(M)) = W(K)$ for any $M \in \mathscr{L}$. (ii) and (iii) follows from this and Proposition 2.5. q.e.d.

COROLLARY 2.7. *Notation being as above, we have*

$$\sum_{[\mathfrak{a}] \in \mathbb{P}/K^{(1)}} \sharp[\mathscr{L}_{\mathfrak{a}}/G^{(1)}] \geq \boldsymbol{h}(\mathscr{L})\,,$$

where the equality holds if and only if $\det(\Gamma(M)) = W(K)$ *for all* $M \in \mathscr{L}$.

PROOF. By Proposition 2.5, we have

$$\sharp[\mathscr{L}_{\mathfrak{a}}/G^{(1)}] = \sum_{j=1}^{\kappa} \frac{\sharp(W(K))}{\sharp[\det(\Gamma(M_j))]} \geq \kappa = \sharp[\mathscr{L}_{\mathfrak{a}}/G^u]\,.$$

If we put $\mathscr{L}_{[\mathfrak{a}]} := \bigcup_{\mathfrak{b} \in [\mathfrak{a}]} \mathscr{L}_{\mathfrak{b}}$ (disjoint), we immediately have

$$\sharp[\mathscr{L}_{\mathfrak{a}}/G^u] = \sharp[\mathscr{L}_{[\mathfrak{a}]}/G]\,, \tag{2.7}$$

from which the assertion follows. q.e.d.

From the above arguments, we can give an answer to the questions (2.1), (2.2).

PROPOSITION 2.8. (i) *If* $(n, h(K)/2^{t-1})=1$, *then the class numbers* $\sharp[\mathscr{L}_{\mathfrak{a}}/G^{(1)}]$ *and* $\sharp[\mathscr{L}_{\mathfrak{a}}/G^{u}]$ *are independent of the ideal* $\mathfrak{a}\in\mathbb{P}$ $(t:=\sharp\{p; p\,|\,d(K)\})$.

(ii) *If, moreover,* $e(\mathscr{L})=1$ (see Lemma 2.4), *then the class number* $\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})$ *is independent of the choice* $\mathscr{L}^{(1)}$ *of a* $\mathbb{G}^{(1)}$*-genus in* $\mathscr{L}$.

PROOF. (i): Since $\det(\alpha\cdot 1_n)=\alpha^n$ $(\alpha\in K_{\mathbb{A}}^{(1)})$, we find, for each $\mathfrak{a}\in\mathbb{P}$, an ideal $\mathfrak{b}\in\mathbb{P}$ and $c\in K^{(1)}$ such that $\mathfrak{a}=\mathfrak{b}^n(c)$. Then we have $\sharp[\mathscr{L}_{\mathfrak{a}}/G^{(1)}]=\sharp[\mathscr{L}_{\mathfrak{b}^n}/G^{(1)}]$ by Corollary 2.3. Writing $\mathfrak{b}=\alpha\cdot\mathcal{O}$ we then see that $\mathscr{L}_{\mathfrak{b}^n}=\mathscr{L}\cdot\alpha$. Since α is in the center of $G_{\mathbb{A}}$, we see that $M_1\cdot\alpha$ and $M_2\cdot\alpha$ are in the same $G^{(1)}$-orbit if and only if so are M_1, M_2 $(\in\mathscr{L})$. This proves (i). (ii) is a direct consequence of (i) and $\mathscr{L}_{\mathfrak{a}}=\mathscr{L}^{(1)}$, which follows from the assumption. q.e.d.

Summing up, we now have the following:

THEOREM 2.9. *Notation being as above, suppose that* (i) $(n, h(K)/2^{t-1})=1$, (ii) $e(\mathscr{L})=1$ *and* (iii) $\det(\Gamma(M))=W(K)$ *for any* $M\in\mathscr{L}$. *Then for any* $\mathfrak{a}\in\mathbb{P}$, $\mathscr{L}_{\mathfrak{a}}$ *consists of a single* $\mathbb{G}^{(1)}$*-genus, and we have*

$$\boldsymbol{h}(\mathscr{L})=(h(K)/2^{t-1})\cdot\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})\qquad \textit{for any}\quad \mathscr{L}^{(1)}=\mathscr{L}_{\mathfrak{a}}\,.$$

2.2. Next we consider the question (2.3).
For simplicity, we assume that L is a free $\mathcal{O}$-lattice. Then we have:

LEMMA 2.10. *For a member* M *of* $\mathscr{L}=\mathscr{L}(L)$, *the following conditions are equivalent*:

(i) M *is a free* $\mathcal{O}$*-lattice.*

(ii) $[L:M]=(a)$ *for an* $a\in K^{(1)}$.

(iii) $M\in\mathscr{L}_{[1]}$.

Indeed, this is an immediate consequence of the well known facts that the class number of $SL_n(K)$ is one and that, for any ideals $\mathfrak{a}$, $\mathfrak{b}$, one has $\mathfrak{a}\oplus\mathfrak{b}\simeq\mathcal{O}\oplus\mathfrak{a}\mathfrak{b}$ (as $\mathcal{O}$-modules).

Now to each member M of $\mathscr{L}_{[1]}$, we associate an equivalence class of the Hermitian matrix

$$H_M:=(H(e_i, e_j))\,,$$

where $\{e_1,\cdots,e_n\}$ is a basis of M over $\mathcal{O}$. Recall that two Hermitian matrices H_1, H_2 are called (integrally) equivalent, if there exists $A\in GL_n(\mathcal{O})$ such that $H_2=AH_1{}^t\bar{A}$. Then the equivalence class of H_M is independent of the choice of the basis. Denote by $\mathscr{H}(\mathscr{L})$ the image of this correspondence $M\longmapsto H_M$ when M ranges over $\mathscr{L}_{[1]}$. From the above remark, we have a canonical bijection

$$\mathscr{L}_{[1]}/G \simeq \mathscr{H}(\mathscr{L})/GL_n(\mathcal{O}) . \tag{2.8}$$

We note also that, in the above correspondence, we have

$$\Gamma(M) \simeq \Gamma(H_M) := \{A \in GL_n(\mathcal{O});\ AH_M{}^t\bar{A} = H_M\} . \tag{2.9}$$

DEFINITION 2.11. (i) Two Hermitian matrices H_1, H_2 are called *properly equivalent*, if there exists $A \in SL_n(\mathcal{O})$ such that $H_2 = AH_1{}^t\bar{A}$.

(ii) Let Ξ be a subgroup of $W(K)$. Then $M \in \mathscr{L}_{\mathcal{O}}$ or H_M is said to be *properly of type* Ξ, or Ξ*-proper*, for short, if $\det(\Gamma(H_M)) = \Xi$.

For $M \in \mathscr{L}_{\mathcal{O}}$, denote by $O^u(M)$ (resp. $O^1(M)$) the G^u-orbit (resp. $G^{(1)}$-orbit) of M in $\mathscr{L}$.

The proof for the following two lemmas are immediate:

LEMMA 2.12. *Suppose that* $M \in \mathscr{L}_{\mathcal{O}}$ *is* Ξ*-proper. Then*

(i) $O^u(M)$ *consists of* $[W(K): \Xi]$ $G^{(1)}$*-orbits.*

(ii) *Each member* M_i *of* $O^u(M)$ *is again* Ξ*-proper.*

LEMMA 2.13. *Suppose that* $H = {}^t\bar{H}$ *is* Ξ*-proper. Then*:

(i) *The equivalence class of* H *consists of* $[W(K): \Xi]$ *proper equivalence classes.*

(ii) *Each member* H_i *of the class of* H *is again* Ξ*-proper.*

Combining these results, we get:

THEOREM 2.14. *There exists a canonical bijection*

$$\mathscr{L}_{\mathcal{O}}/G^{(1)} \simeq \mathscr{H}(\mathscr{L})/SL_n(\mathcal{O})$$

which satisfies the following conditions:

(i) *It preserves the unit group, that is,* $\Gamma(M) \simeq \Gamma(H_M)$. *In particular,* M *is* Ξ*-proper if and only if* H_M *is* Ξ*-proper.*

(ii) *The following diagram is commutative*:

$$\begin{array}{ccc}
\mathscr{L}_{\mathcal{O}}/G^{(1)} & \simeq & \mathscr{H}(\mathscr{L})/SL_n(\mathcal{O}) \\
\downarrow & & \downarrow \\
\mathscr{L}_{\mathcal{O}}/G^u \simeq \mathscr{L}_{[1]}/G & \overset{(2.8)}{\simeq} & \mathscr{H}(\mathscr{L})/GL_n(\mathcal{O}) .
\end{array}$$

We remark that, if $\mathscr{L}$ is a genus of unimodular $\mathcal{O}$-lattices, then $\mathscr{H}(\mathscr{L})$ consists of the integral Hermitian matrices in $M_n(\mathcal{O})$ of determinant one, with the condition that the greatest common divisor of their diagonal elements are odd or even, according as $\mathscr{L}$ is normal or subnormal.

3. General class number formula. Here we give a closed expression for the class numbers $\boldsymbol{h}(\mathscr{L})$ and $\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})$ of the genera $\mathscr{L}$, $\mathscr{L}^{(1)}$ in a given Hermitian space (V, H), which we assume, throughout this paper, to be positive definite. This is a special case of the trace formula for the Brandt matrices given in [6].

For the sake of simplicity, we treat the class number $\boldsymbol{h}(\mathscr{L})$ with respect to the unitary group $\mathbb{G}$, and note that the result for $\boldsymbol{h}^{(1)}(\mathscr{L}^{(1)})$ is obtained simply by changing notation. Thus, suppose we are given in (V, H) a genus $\mathscr{L}=\mathscr{L}(L)$ of $\mathcal{O}$-lattices, and let $\boldsymbol{h}=\boldsymbol{h}(\mathscr{L})$ be its class number. Then one can express $G_{\mathbb{A}}$ as a disjoint union of the double cosets:

$$G_{\mathbb{A}}=\bigcup_{i=1}^{\boldsymbol{h}} \boldsymbol{U}\xi_i G \qquad (\boldsymbol{U}=\boldsymbol{U}(L)), \tag{3.1}$$

so that the $\mathcal{O}$-lattices $L_i:=L\cdot\xi_i$ $(1\le i\le \boldsymbol{h})$ form a complete set of representatives of the classes in $\mathscr{L}$. We put for each i

$$\Gamma_i:=G\cap\xi_i^{-1}\boldsymbol{U}\xi_i=\{\gamma\in G;\, L_i\cdot\gamma=L_i\}\,. \tag{3.2}$$

Since $(V, H)_\infty$ is definite, $\boldsymbol{U}$ is a compact subgroup of $G_{\mathbb{A}}$; and each Γ_i, being a discrete subgroup of $\boldsymbol{U}$, is a finite subgroup of G (see Lemma 5.10). Therefore each element of Γ_i has a finite order, and hence its characteristic polynomial is a product of cyclotomic polynomials over K. Let F be the (finite) set of all possible characteristic polynomials of the torsion elements of G. For each $f\in F$, denote by $G(f)$ (resp. $\Gamma_i(f)$) the set of elements of G (resp. Γ_i) having f as their characteristic polynomial. Then one has an obvious expression for the class number $\boldsymbol{h}$:

$$\boldsymbol{h}=\sum_{i=1}^{\boldsymbol{h}}\frac{\sharp[\Gamma_i]}{\sharp[\Gamma_i]}=\sum_{f\in F}\sum_{i=1}^{\boldsymbol{h}}\frac{\sharp[\Gamma_i(f)]}{\sharp[\Gamma_i]}\,.$$

Note that $G(f)$ is stable under the G-conjugation. In general, however, it consists of an infinite number of G-conjugacy classes (see §4). We say that a G-conjugacy class $[g]_{\boldsymbol{Q}}$ is *locally integral*, if $\Gamma_i\cap[g]_{\boldsymbol{Q}}\neq\varnothing$ for some i $(1\le i\le\boldsymbol{h})$. This is easily seen to be equivalent to $\boldsymbol{U}\cap[g]_{G_{\mathbb{A}}}\neq\varnothing$, where $[g]_{G_{\mathbb{A}}}$ is the $G_{\mathbb{A}}$-conjugacy class of g. From Lemma 5.10 below and the above expression, we see that the number of locally integral G-conjugacy classes of finite orders is *finite*.

Next we put, for each $[g]_{\boldsymbol{Q}}=[g]_G$

$$\boldsymbol{h}([g]_{\boldsymbol{Q}};\mathscr{L})=\sum_{i=1}^{\boldsymbol{h}}\frac{\sharp[\Gamma_i\cap[g]_{\boldsymbol{Q}}]}{\sharp[\Gamma_i]}\,. \tag{3.3}$$

Note that this is an invariant of the G-conjugacy class $[g]_{\boldsymbol{Q}}$ and does not depend on the choice of the representatives $\{\xi_i\}$ in (3.1). Let $\mathbb{G}(g)$ be the centralizer of g in $\mathbb{G}$. It is known that $\mathbb{G}(g)$ is again a reductive group over $\boldsymbol{Q}$, if g is a semisimple element of G. Let $\boldsymbol{V}$ be an idelic arithmetic subgroup of $G(g)_{\mathbb{A}}$ which can be decomposed as in (1.1) for $\boldsymbol{U}$. Then in the same way as for $G_{\mathbb{A}}$, we have a decomposition

$$G(g)_{\mathbb{A}}=\bigcup_{j=1}^{\boldsymbol{h}'} G(g)\eta_j\boldsymbol{V} \qquad (\text{disjoint}),$$

and obtain a system of (global) arithmetic subgroups

$$\Lambda_j := \eta_j V \eta_j^{-1} \cap G(g) \qquad (1 \leq j \leq \boldsymbol{h}') .$$

Now we put

$$\mathbb{M}(V) := \sum_{j=1}^{\boldsymbol{h}'} \frac{1}{\#[\Lambda_j]} , \tag{3.4}$$

and call it *the mass* of V in $\mathbb{G}(g)$.

PROPOSITION 3.1 (Hashimoto [6]). *We have*

$$\boldsymbol{h}([g]_{\boldsymbol{Q}}; \mathscr{L}) = \sum_{\mathscr{L}(V)} \mathbb{M}(V) \prod_p c_p(g, U_p, V_p) , \tag{3.5}$$

where $\mathscr{L}(V)$ ranges over a (finite) set of genera of the idelic arithmetic subgroups of $\mathbb{G}(g)$, and

$$c_p(g, U_p, V_p) := \#[G_p(g) \backslash M_p(g, U_p, V_p)/U_p] ,$$

$$M_p(g, U_p, V_p) = \left\{ x \in G_p(g);\ \begin{matrix} x^{-1}gx \in U_p, \text{ and } G(g)_p \cap xU_px^{-1} \\ \text{is conjugate in } G(g)_p \text{ to } V_p \end{matrix} \right\} .$$

We note that $c_p(g, U_p, V_p)$ is the number of U_p-conjugacy classes in $[g]_p \cap U_p$ such that $G_p(g) \cap xU_px^{-1}$ is conjugate in $G_p(g)$ to V_p. If we choose and fix one V in $G(g)_{\mathbb{A}}$ and put

$$M_p(g, U_p) := \{x \in G_p;\ x^{-1}gx \in U_p\} ,$$

$$\mathrm{Ind}_p(x; g) := [V_p : G_p(g) \cap xU_px^{-1}]$$

$$(= \text{the generalized index for commensurable groups}) ,$$

then we have another expression for $\boldsymbol{h}([g]_{\boldsymbol{Q}}; \mathscr{L})$:

$$\boldsymbol{h}([g]_{\boldsymbol{Q}}; \mathscr{L}) = \mathbb{M}(V) \cdot \prod_p \left\{ \sum_\delta \mathrm{Ind}_p(\delta; g) \right\} , \tag{3.6}$$

where the summation is taken over a complete set of representatives of $G_p(g) \backslash M_p(g, U_p)/U_p$. Substituting this into the above formula we get:

THEOREM 3.2. *The class number of the $\mathbb{G}$-genus $\mathscr{L}$ is given by the following expression*:

$$\boldsymbol{h}(\mathscr{L}) = \sum_{f \in F} \sum_{[g]_{\boldsymbol{Q}}} \boldsymbol{h}([g]_{\boldsymbol{Q}}; \mathscr{L}) , \tag{3.7}$$

where the second summation is taken over the locally integral G-conjugacy classes $[g]_{\boldsymbol{Q}} = [g]_G$ in $G(f)$, and $\boldsymbol{h}([g]_{\boldsymbol{Q}}; \mathscr{L})$ is given by (3.5) *or* (3.6).

In the subsequent paper [10], we shall be interested in the evaluation of the right hand side of (3.7) to obtain explicit formulas in the cases where $n=\dim_K(V)=2$ or 3.

4. Conjugacy classes in the unitary groups.

4.1. Let F be a field of characteristic zero and E be either a quadratic extension of F or the sum of two copies of F. We denote by ρ the non-trivial automorphism of E/F. Let (V, H) be a non-degenerate ρ-Hermitian space over E, and put $G_F := \mathbb{U}(V, H)_F$. We investigate the semi-simple conjugacy classes of $\mathbb{G}$. Put $n=\mathrm{rank}_E(V)$. Let $f=f(X)$ be a monic polynomial in X of degree n with coefficients in E such that $f(0)\in E^\times$. Denote by $G(f)$ the set of all semi-simple elements of G_F with the characteristic polynomials f. If $p=p(X)\in E[X]$ is monic and $p(0)\in E^\times$, we define its *dual* $p^*\in E[X]$ by

$$p^*(X):=(p(0)^\rho)^{-1}p^\rho(X^{-1})X^l,$$

where $l=\deg(p)$ and $p\longmapsto p^\rho$ is the natural action of ρ on $E[X]$. It is easy to see that $f=f^*$ if $G(f)\neq\varnothing$. Hereafter, we assume that $f=f^*$. Then we can write

$$f(X)=\prod_{i=1}^{r} m_i(X)^{e_i}, \tag{4.1}$$

where each m_i is a $*$-invariant monic polynomial in $E[X]$ of positive degree which cannot be expressed as a product of such polynomials. Note that when E is a field, m_i is either irreducible over E, or is of the form $n_i n_i^*$ with $n_i\in E[X]$ monic and irreducible over E, and with $n_i\neq n_i^*$. We then put $m(X):=\prod_{i=1}^r m_i$, $\boldsymbol{A}:=E[X]/(m(X))$, $\boldsymbol{A}_i:=E[X]/(m_i(X))$, hence we have $\boldsymbol{A}=\bigoplus_i \boldsymbol{A}_i$. Note that $\boldsymbol{A}$ and $\boldsymbol{A}_i$ are semi-simple algebras over E. Since $m=m^*$, $m_i=m_i^*$, there exists a unique involution σ of $\boldsymbol{A}$ such that

$$E^\sigma=E, \qquad \sigma|_E=\rho, \quad \text{and} \quad XX^\sigma=1 \tag{4.2}$$

(we abbreviate "$X \bmod (m(X))$" as X), and that each $\boldsymbol{A}_i$ is stable under σ. The restriction of σ to $\boldsymbol{A}_i$ will be denoted by the same letter σ. We define the subalgebra $\boldsymbol{B}$ of $\boldsymbol{A}$ by $\boldsymbol{B}:=\{a\in\boldsymbol{A};\, a^\sigma=a\}$, and put $\boldsymbol{B}_i:=\boldsymbol{B}\cap\boldsymbol{A}_i$. Note that each $\boldsymbol{B}_i$ is a field containing F.

Let (W, I) be a σ-Hermitian space over $\boldsymbol{A}$. By the scalar restriction, we may regard W as an E-module. Let $\mathrm{Tr}_{\boldsymbol{A}/E}=\sum_i \mathrm{Tr}_{\boldsymbol{A}_i/E}$ be the reduced trace of $\boldsymbol{A}/E$. We define on W a ρ-Hermitian form $\mathrm{Tr}_{\boldsymbol{A}/E}(I)$ over E by putting

$$\mathrm{Tr}_{\boldsymbol{A}/E}(I)(x, y):=\mathrm{Tr}_{\boldsymbol{A}/E}(I(x, y)) \qquad (x, y\in W).$$

For a given σ-Hermitian form I_i over an $\boldsymbol{A}_i$-module W_i, we define on W_i a ρ-Hermitian form $\mathrm{Tr}_{\boldsymbol{A}_i/E}(I(x, y))$ over E in the same way.

Now suppose that $G(f)\neq\varnothing$ for a polynomial f satisfying (4.1), and fix an element g of $G(f)$. Then $m(X)$ is the minimal polynomial of g. We introduce an $\boldsymbol{A}$-module structure on V via $x\cdot X=x\cdot g$ $(x\in V)$, and denote it by $\tilde{V}^{(g)}$. Let (x, y) be an element of $V\times V$. Since (V, H) is non-degenerate, there exists a unique element $\tilde{H}^g(x, y)$ of $\boldsymbol{A}$ such that the equality

(4.3) $$H(x\cdot a, y)=\mathrm{Tr}_{A/E}(a\cdot \tilde{H}^g(x, y))$$

holds for any $a\in A$. It is easy to see that the map $(x, y)\longmapsto \tilde{H}^g(x, y)$ is a non-degenerate σ-Hermitian form on $\tilde{V}^{(g)}$. The principle of Milnor [16] and Springer-Steinberg [21] in the unitary group case is described in the following way:

LEMMA 4.1. (i) *The set $G(f)$ is not empty if and only if there exists a non-degenerate σ-Hermitian space $(\tilde{V}, \tilde{H})$ over A such that $(\tilde{V}, \mathrm{Tr}_{A/E}(\tilde{H}))$ is isomorphic to (V, H).*

(ii) *Suppose that $G(f)\neq\varnothing$. Then the map $g\longmapsto(\tilde{V}^{(g)}, \tilde{H}^g)$ induces a canonical bijection*

$$G(f)/\!\!/G\simeq\left\{\begin{matrix}\text{The isometric classes of } \sigma\text{-Hermitian spaces}\\ (\tilde{V}, \tilde{H}) \text{ over } A \text{ such that } (\tilde{V}, \mathrm{Tr}_{A/E}(\tilde{H}))\simeq(V, H)\end{matrix}\right\}.$$

Moreover, the right hand side is canonically identified with the set

$$\left\{([\tilde{V}_1, \tilde{H}_1], \cdots, [\tilde{V}_r, \tilde{H}_r]);\ \bigoplus_i(\tilde{V}_i, \mathrm{Tr}_{A_i/E}(\tilde{H}_i))\simeq(V, H)\right\},$$

by the map $[\tilde{V}, \tilde{H}]\longmapsto([\tilde{V}\cdot A_1, \tilde{H}\,|\,\tilde{V}\cdot A_1], \cdots, [\tilde{V}\cdot A_r, \tilde{H}\,|\,\tilde{V}\cdot A_r])$. Here $[\tilde{V}, \tilde{H}]$ (resp. $[\tilde{V}_i, \tilde{H}_i]$) denotes the isometry class of σ-Hermitian spaces over A (resp. A_i) containing $(\tilde{V}, \tilde{H})$ (resp. $(\tilde{V}_i, \tilde{H}_i)$).

In the two special cases described in the following lemma, the isometry class of $(\tilde{V}, \tilde{H})$ or $(\tilde{V}_i, \tilde{H}_i)$ is uniquely determined by (V, H), (V_i, H_i):

LEMMA 4.2. *Let the notation be as in Lemma* 4.1.

(i) *Suppose that $E=F\oplus F$. Then any non-degenerate σ-Hermitian space $(\tilde{V}, \tilde{H})$ over A belongs to a unique isometry class. Moreover, we have $(\tilde{V}, \mathrm{Tr}_{A/E}(\tilde{H}))\simeq(V, H)$ if and only if $\mathrm{rank}_E(\tilde{V})=\mathrm{rank}_E(V)$. Therefore $G(f)/\!\!/G$ consists of a single conjugacy class.*

(ii) *Suppose that E is a field, and that $m_i=n_in_i^*$. Put $A_i=A_{i1}\oplus A_{i2}$, A_{ij} being a field and $A_{i1}^\sigma=A_{i2}$. Then any non-degenerate σ-Hermitian space $(\tilde{V}_i, \tilde{H}_i)$ over A_i with a given rank belongs to a unique isometry class. The class of $(\tilde{V}_i, \mathrm{Tr}_{A_i/E}(\tilde{H}_i))$ is characterized by the fact that the restriction of $\mathrm{Tr}_{A_i/E}(\tilde{H}_i)$ to $\tilde{V}_i\cdot A_{ij}$ $(j=1, 2)$ are totally isotropic.*

These facts are proved quite easily, so we omit the proof. In the situation of Lemma 4.1, we can determine the discriminant $d(\tilde{V}_i, \mathrm{Tr}_{A_i/E}(\tilde{H}_i))\in F^\times/N_{E/F}(E^\times)$ from the discriminant $d(\tilde{V}_i, \tilde{H}_i)\in \boldsymbol{B}_i^\times/N_{A_i/B_i}(A_i^\times)$ of $(\tilde{V}_i, \tilde{H}_i)$. Put $l_i=\mathrm{rank}_E(A_i)$, and for each E-basis $a_1, \cdots, a_{l_i}$ of A_i, put

(4.4) $$\Delta_{A_i/E}[a_1, \cdots, a_{l_i}]:=\det((\mathrm{Tr}_{A_i/E}(a_ja_k^\sigma))_{j,k=1}^{l_i}).$$

Then we have the following:

LEMMA 4.3. (i) *$\Delta_{A_i/E}[a_1, \cdots, a_{l_i}]$ belongs to $F^\times\cap N_{A_i/B_i}(\boldsymbol{B}_i^\times)$, and its class modulo*

$N_{E/F}(E^\times)$ *does not depend on the choice of the basis* (a_i).

(ii) *The above two discriminants are related by*

$$d(\tilde{V}_i, \operatorname{Tr}_{A_i/E}(\tilde{H}_i)) \equiv \Delta[a_1, \cdots, a_{l_i}]^{e_i} \cdot N_{B_i/F}(d(\tilde{V}_i, \tilde{H}_i)) \pmod{N_{E/F}(E^\times)}. \tag{4.5}$$

PROOF. The first assertion is easy to see. We prove (ii). First suppose that E and A_i are fields. For simplicity, we put $l_i = l$ and $e_i = e$. Let $x_1, \cdots, x_e$ be an orthogonal basis of $\tilde{V}_i$ over A_i. Then $\{x_i a_j\}_{1 \le i \le e, 1 \le j \le l}$ form a E-basis of $\tilde{V}_i$. Now we regard A_i as a subfield of the algebraic closure $\bar{F}$ of F, and denote by $a \longmapsto a^{(s)}$ $(1 \le s \le l)$ the distinct embeddings of A_i into $\bar{F}$ which stabilize each element of E. The involution σ is carried over to that of $A_i^{(s)}$, which we denote again by σ. Then the matrix

$$(\operatorname{Tr}_{A_i/E}(\tilde{H}_i)(x_j a_p, x_k a_q)) = (\operatorname{Tr}_{A_i/E}(a_p a_q^\sigma \cdot \tilde{H}_i(x_j, x_k))) \in M_{e,l}(E)$$

is written as

$$\begin{bmatrix} T J_1 {}^t T^\sigma & & 0 \\ & \ddots & \\ 0 & & T J_e {}^t T^\sigma \end{bmatrix}$$

with

$$T := \begin{bmatrix} a_1^{(1)} \cdots a_1^{(l)} \\ \cdots\cdots\cdots \\ a_l^{(1)} \cdots a_l^{(l)} \end{bmatrix}, \qquad J_s := \begin{bmatrix} \tilde{H}_i(x_s, x_s)^{(1)} & & 0 \\ & \ddots & \\ 0 & & \tilde{H}_i(x_s, x_s)^{(l)} \end{bmatrix}$$

$(1 \le s \le e)$. Since $T {}^t T^\sigma = (\operatorname{Tr}_{A_i/E}(a_j a_k^\sigma))$, we get (4.5). When E or A_i is not a field, the assertion is proved by reduction to the above case. q.e.d.

4.2. Now we assume that K is an imaginary quadratic field and ρ is the nontrivial automorphism of K. Let (V, H) be a positive definite ρ-Hermitian space over K. We denote by $\mathbb{G}$ the unitary group $\mathbb{U}(V, H)$ of (V, H). In order to describe the conjugacy classes of G and G_v, we need the classification theorem of Hermitian spaces in local and global versions over various extensions of $\boldsymbol{Q}$ or $\boldsymbol{Q}_v$, which was proved by Landherr [15]. We first review those results of [15] which we need in this paper.

Let $\boldsymbol{N}$ be a totally real number field of finite degree over $\boldsymbol{Q}$, and let $\boldsymbol{M}$ be a totally imaginary quadratic extension of $\boldsymbol{N}$. For any place w of N, we put $\boldsymbol{M}_w = \boldsymbol{M} \otimes_{\boldsymbol{N}} N_w$. We denote the non-trivial automorphism of $\boldsymbol{M}/\boldsymbol{N}$ and that of $\boldsymbol{M}_w/\boldsymbol{N}_w$ by σ. Then we have:

LEMMA 4.4 (Landherr [15]). (i) *If w is a finite place of N, the isometry class of a non-degenerate σ-Hermitian space (W, I) over $\boldsymbol{M}_w$ is determined by the rank n, and the discriminant $d(W_w, I) \in \boldsymbol{N}_w^\times / N_{\boldsymbol{M}_w/\boldsymbol{N}_w}(\boldsymbol{M}_w^\times)$.*

(ii) *If w is an infinite place of $\boldsymbol{N}$, the isometry class of a non-degenerate σ-Hermitian space (W, I) over $\boldsymbol{M}_w$ $(\simeq \boldsymbol{C})$ is determined by the rank and the signature (p_w, q_w).*

LEMMA 4.5 (Landherr [15]). *The isometry class of a non-degenerate σ-Hermitian space (W, I) is determined by the rank, the discriminant $d(W, I) \in \boldsymbol{N}^{\times}/N_{\boldsymbol{M}/\boldsymbol{N}}(\boldsymbol{M}^{\times})$ and the signatures $\{(p_w, q_w)\}_w$, where w runs through all infinite places of $\boldsymbol{N}$. They can take arbitrary values subject to the following conditions for every infinite place w:*

$$p_w + q_w = n\,, \quad \textit{and} \quad (d(V), \boldsymbol{M}/\boldsymbol{N})_w = (-1)^{q_w}\,.$$

Here $(c, \boldsymbol{M}/\boldsymbol{N})_w$ is the local norm residue symbol of c at w. Note that the above lemmas, together with *the Hasse principle* for the norm map in a cyclic extension, imply *the Hasse principle* for the isometry of the Hermitian spaces. Namely, two non-degenerate σ-Hermitian spaces (W, I) and (W', I') over $\boldsymbol{M}$ are isometric if and only if so are $(W, I)_w$ and (W', I') at any place w of $\boldsymbol{N}$.

Let $f=f(X)$ be a monic polynomial in $\mathcal{O}[X]$ of degree n whose roots in $\bar{\boldsymbol{Q}}$ are all roots of unity. We also assume f to satisfy $f=f^*$. Decompose f into the form (4.1) in $K[X]$, and let $\boldsymbol{A}$, $\boldsymbol{A}_i$, σ, $\boldsymbol{B}$, and $\boldsymbol{B}_i$ be as before. Then each $\boldsymbol{A}_i$ is a field, which can be regarded as a subfield of $\bar{\boldsymbol{Q}}$. It is easy to see that $\boldsymbol{B}_i$ is totally real and $\boldsymbol{A}_i$ is a totally imaginary quadratic extension of $\boldsymbol{B}_i$. By Lemma 4.1, each element of $G(f)/\!/G$ corresponds canonically to an r-ple $([\tilde{V}_1, \tilde{H}_1], \cdots, [\tilde{V}_r, \tilde{H}_r])$ satisfying the condition that $\bigoplus_i (\tilde{V}_i, \mathrm{Tr}_{\boldsymbol{A}_i/E}(\tilde{H}_i)) \simeq (V, H)$. From this condition we see that, for each i, $\mathrm{rank}_{\boldsymbol{A}_i}(\tilde{V}_i) = e_i$ (fixed by (4.1)) and $(\tilde{V}_i, \tilde{H}_i)_w$ is positive definite at any infinite place w of $\boldsymbol{B}_i$. Then applying Lemma 4.5, we see that the isometry class of $(\tilde{V}_i, \tilde{H}_i)$ is determined by $d(\tilde{V}_i) \in \boldsymbol{B}_i^{\times}/N_{\boldsymbol{A}_i/\boldsymbol{B}_i}(\boldsymbol{B}_i^{\times})$. By Lemma 4.3, the above condition is expressed as

$$\prod_i (\Delta_{\boldsymbol{A}_i/K})^{e_i} N_{\boldsymbol{B}_i/\boldsymbol{Q}}(d(\tilde{V}_i)) \equiv d(V) \pmod{N_{K/\boldsymbol{Q}}(K^{\times})} \tag{4.6}$$

where $\Delta_{\boldsymbol{A}_i/K}$ stands for $\Delta_{\boldsymbol{A}_i/K}[a_1, \cdots, a_{l_i}]$ defined by (4.4).

Now we localize everything above. Let p be a finite place of $\boldsymbol{Q}$. For each i, let $\{P_{i,1}, \cdots, P_{i,t(i,p)}\}$ be the set of all places of $\boldsymbol{B}_i$ lying above p. Then the decomposition (4.1) applied to $m_i \in K_p[X]$ becomes

$$m_i(X) = \prod_{j=1}^{t(i,p)} m_{i,j}(X)\,.$$

Now put

$$\boldsymbol{A}_{i,p} := \boldsymbol{A}_i \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_p\,, \qquad \boldsymbol{B}_{i,p} := \boldsymbol{B}_i \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_p\,, \qquad \boldsymbol{A}_{i,P_{i,j}} := \boldsymbol{A}_i \otimes_{\boldsymbol{B}_i} \boldsymbol{B}_{i,P_{i,j}}\,,$$

$$\boldsymbol{A}_{i,p,j} := K_p[X]/(m_{i,j}(X))\,, \quad \text{and} \quad \boldsymbol{B}_{i,p,j} := \boldsymbol{B}_{i,p} \cap \boldsymbol{A}_{i,p,j}\,.$$

Then we may assume that $\boldsymbol{A}_{i,P_{i,j}} = \boldsymbol{A}_{i,p,j}$ and $\boldsymbol{B}_{i,P_{i,j}} = \boldsymbol{B}_{i,p,j}$. By Lemma 4.1, each element of $G_p(f)/\!/G_p$ corresponds canonically to a system $([\tilde{V}(P_{i,j}), \tilde{H}(P_{i,j})])$ $(1 \le i \le r,\ 1 \le j \le t(i,p))$, where each $[\tilde{V}(P_{i,j}), \tilde{H}(P_{i,j})]$ is an isometry class of σ-Hermitian space over $\boldsymbol{A}_{i,p,j}$. They satisfy the condition

$$(V, H) \simeq \bigoplus_{i,j} (\tilde{V}(P_{i,j}), \mathrm{Tr}_{\boldsymbol{A}_{i,p,j}/K_p}(\tilde{H}(P_{i,j})))\,.$$

By Lemma 4.5, this is equivalent to

$$\prod_{i,j}(\Delta_{A_{i,p,j}/K_p})^{e_i}\cdot N_{B_{i,p,j}/Q_p}(d(\tilde{V}(P_{i,j})))\equiv d(V) \tag{4.7}$$

$(\bmod N_{K_p/Q_p}(K_p^\times))$, where $\Delta_{A_{i,p,j}/K_p}$ is defined by (4.4). In the local case, we have the following:

PROPOSITION 4.6. *Let f be a monic polynomial of degree n $(=\dim_K(V))$ which is a product of cyclotomic polynomials over K. Let v be a place of Q.*

(i) *When $v=\infty$, $G_\infty(f)\,/\!/\,G_\infty$ consists of a single conjugacy class.*

(ii) *Let $v=p$ be a finite place, and let the notation be as above. For any $g\in G_p(f)$, define an A_p-module $\tilde{V}_p^{(g)}$ as in Lemma 4.1. Let $d(\tilde{V}_p^{(g)}\cdot A_{i,p,j})$ be the discriminant of the ρ-Hermitian subspace $\tilde{V}_p^{(g)}\cdot A_{i,p,j}$ in $(V,H)_p$. Then the mapping $g\longmapsto(d(\tilde{V}_p^{(g)}\cdot A_{i,p,j}))_{i,j}$ induces a canonical bijection*

$$G_p(f)\,/\!/\,G_p\simeq\left\{(d_{i,p,j})_{i,j};\quad\begin{array}{c}d_{i,p,j}\in Q_p^\times/N_{K_p/Q_p}(K_p^\times),\\ \prod_{i,j}d_{i,p,j}=d(V_p),\ \text{and}\\ (d_{i,p,j},K/Q)_p=(-1,K/Q)_p^{e_i[B_{i,p,j}:Q_p]}\end{array}\right\}$$

where, on the right hand side, we delete the last condition if $A_{i,p,j}$ is a field.

PROOF. The first assertion is easy to see. We prove (ii). The above $d(\tilde{V}_p^{(g)}\cdot A_{i,p,j})$ is nothing but the factor corresponding to (i,j), on the left hand side of (4.7). The surjectivity of the mapping follows immediately from this remark. On the other hand, the translation theorem in local class field theory shows that $d(\tilde{V}(P_{i,j}),\tilde{H}(P_{i,j}))$ is uniquely determined by $d(\tilde{V}_p^{(g)}\cdot A_{i,p,j})$. Then the injectivity follows. q.e.d.

In the global case, we have the following:

PROPOSITION 4.7. *Let $f,g\in G(f)$ and $\tilde{V}^{(g)}$ be as above. Then the mapping $g\longmapsto(d(\tilde{V}_p^{(g)}\cdot A_{i,p,j}))_{p<\infty,1\le i\le r,1\le j\le t(i,p)}$ induces a canonical bijection*

$$G(f)\,/\!/\,G\simeq\left\{(d_{i,p,j})_{p,i,j};\quad\begin{array}{c}d_{i,p,j}\in Q_p^\times/N_{K_p/Q_p}(K_p^\times),\\ \prod_{i,j}d_{i,p,j}=d(V_p)\ \text{for any}\ p<\infty\\ (d_{i,p,j},K/Q)_p=(-1,K/Q)_p^{e_i[B_{i,p,j}:Q_p]}\ (\text{if}\ A_{i,p,j}\neq\text{field})\\ (d_{i,p,j},K/Q)_p=+1\ \text{for almost all}\ p,\\ \prod_{p,j}(d_{i,p,j},K/Q)_p=+1\ \text{for any}\ i\end{array}\right\}$$

where $d(\tilde{V}_p^{(g)}\cdot A_{i,p,j})$ is as in Proposition 4.6.

We can prove this proposition by using (4.6) and an argument similar to that in the proof of Proposition 4.6. From the above two propositions, we get the following result which was proved by Asai [1]:

PROPOSITION 4.8 (The Hasse principle for conjugacy classes). *The notation being as above, the natural map*

$$G(f)/\!/G \to \prod_{p<\infty} G_p(f)/\!/G_p$$

is injective.

5. Mass formulas. In this section we use the notation of § 1, § 3 and § 4.

5.1. We shall calculate the mass $\mathbb{M}(V)$ which appears in (3.4). As is well known, this is equivalent to evaluating the volume $\mathrm{vol}(G(g)_{\mathbb{A}}/G(g))$ with respect to the invariant measure normalized by $\mathrm{vol}(V)=1$.

Let $f=f(X)\in\mathcal{O}[X]$ be as in Theorem 3.2, and let $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{A}_i$, $\boldsymbol{B}_i$ $(1\le i\le r)$ be as in § 2.1. Let g be an element of $G(f)$. Then we get a non-degenerate σ-Hermitian space $(\tilde{V}^{(g)}, \tilde{H}^g)$ over $\boldsymbol{A}$ (see (4.3)). For each i, we put

$$(5.1)\qquad \begin{aligned} &\tilde{\mathbb{G}}(g;i):=\mathbb{U}(\tilde{V}_i^{(g)}, \tilde{H}_i)\\ &(\tilde{V}_i^{(g)}, \tilde{H}_i^g):=(\tilde{V}^{(g)}\cdot\boldsymbol{A}_i, \tilde{H}^g\,|\,\tilde{V}^{(g)}\cdot\boldsymbol{A}_i)\,. \end{aligned}$$

Each $\tilde{G}(g;i)$ is a reductive group defined over the totally real field $\boldsymbol{B}_i$. We can identify $\mathbb{G}(g)$ with $\prod_i \mathrm{Res}_{\boldsymbol{B}_i/\boldsymbol{Q}}(\tilde{\mathbb{G}}(g;i))$, where $\mathrm{Res}_{\boldsymbol{B}_i/\boldsymbol{Q}}$ denotes the restriction of the base field from $\boldsymbol{B}_i$ to $\boldsymbol{Q}$. Therefore we have

$$(5.2)\qquad \mathbb{G}(g)_{\mathbb{A}}/\mathbb{G}(g)_{\boldsymbol{Q}}\simeq\prod_i \tilde{\mathbb{G}}(g;i)_{\mathbb{A}}/\tilde{\mathbb{G}}(g;i)_{\boldsymbol{B}_i}\,.$$

Thus the calculation of $\mathbb{M}(V)$ is reduced to that of $\mathrm{vol}(\tilde{\mathbb{G}}(g;i)_{\mathbb{A}}/\tilde{\mathbb{G}}(g;i)_{\boldsymbol{B}_i})$ for each i.

We start with the following situation: Let $\boldsymbol{N}$ be a totally real number field and $\boldsymbol{M}$ be a totally imaginary quadratic extension of $\boldsymbol{N}$ with a non-trivial automorphism σ over $\boldsymbol{N}$. Let $R=R_{\boldsymbol{M}}$ and $S=S_{\boldsymbol{N}}$ be the ring of integers of $\boldsymbol{M}$, $\boldsymbol{N}$ respectively. Like $\boldsymbol{Z}_v$ and $\mathcal{O}_v$, we define the completions R_w and S_w at each place w of $\boldsymbol{N}$. Let m be a positive integer and I a σ-Hermitian matrix in $M_m(R)$, which we assume to be positive definite at all infinite places of $\boldsymbol{N}$. We put $I(x,y)=x\cdot I\cdot {}^t y^{\sigma}$ for $x, y\in\boldsymbol{M}^m$. Let $\mathbb{M}_m(I)$ be the mass of the genus containing the standard lattice R^m in the σ-Hermitian space $(\boldsymbol{M}^m, I)$ with respect to $\mathbb{U}(\boldsymbol{M}^m, I)$. Namely, we have

$$\mathbb{M}_m(I):=\mathrm{vol}(\mathbb{U}(\boldsymbol{M}^m, I)_{\mathbb{A}}/\mathbb{U}(\boldsymbol{M}^m, I)_{\boldsymbol{N}};\, du_{\mathbb{A}})\,,$$

where $du_{\mathbb{A}}:=\prod_w du_w$ is the normalized Haar measure of $\mathbb{U}(\boldsymbol{M}^m, I)_{\mathbb{A}}$ such that

$$(5.3)\qquad \int_{\mathbb{U}(\boldsymbol{M}^m, I)_{\mathbb{A}}\cap GL_m(R_{\mathbb{A}})} du_{\mathbb{A}}=1\,.$$

When $\boldsymbol{N}=\boldsymbol{Q}$ and $\boldsymbol{M}=K$ is an imaginary quadratic field, Braun [4] gave a formula for $\mathbb{M}_m(I)$, which is analogous to Siegel's formula (cf. [20]). Modifying Braun's argument, or using the fact that the Tamagawa number of the unitary group $\mathbb{U}(\boldsymbol{M}^m, I)$ is two (cf. Ono [17]), one easily gets the following:

PROPOSITION 5.1. *Notation being as above, the mass* $\mathbb{M}_m(I)$ *is expressed as*

$$\mathbb{M}_m(I)=2\cdot d(N)^{m^2/2}\cdot N_{N/\boldsymbol{Q}}(d(\boldsymbol{M}/N))^{m(m+1)/4}\cdot N_{N/\boldsymbol{Q}}(\det(I))^m\prod_w \alpha_w(I)\,. \tag{5.4}$$

Here $d(N)$ *and* $d(\boldsymbol{M}/N)$ *denote the discriminant of* N *and the relative discriminant of* $\boldsymbol{M}/N$, *respectively; and for each place* w *of* N, $\alpha_w(I)$ ($=$ *the local density of* I *at* w) *is defined as follows: If* $w=P$ (*finite*),

$$\alpha_P(I):=\lim_{k\to\infty} A_{P^k}(I)/N(P)^{km^2}\,,$$

$$A_{P^k}(I):=\#\{X\in M_m(R/P^k);\ XI\,{}^tX^\sigma=I\}\,.$$

If w *is an infinite place,*

$$\alpha_w(I):=\prod_{j=1}^m (2\pi)^j/(j-1)!\,.$$

Otremba [18] computed $\alpha_P(I)$ in the case $\boldsymbol{M}/N=K/\boldsymbol{Q}$, by the technique using Gauss' sums. Here we compute the number $A_{P^k}(I)$ directly in the case $I=1_m$, from which the results of Otremba are reproduced easily. Although this method can be applied only to a restricted class of Hermitian matrices I, it would be of some interest, since it is immediately generalized to more general cases of $\boldsymbol{M}/N$, which we need for our purpose.

Now we return to our case $\boldsymbol{M}/N=K/\boldsymbol{Q}$. For each finite place p we abbreviate $\mathbb{U}_m(\mathcal{O}/p^k, 1_m)$ to $\mathbb{U}_m(\mathcal{O}/p^k)$, and consider the natural projection:

$$\phi_k:\ \mathbb{U}_m(\mathcal{O}/p^k)\to\mathbb{U}_m(\mathcal{O}/p^{k-1})\,.$$

Then the first two assertions in each of the following lemmas are proved immediately, since in these cases every non-degenerate ρ-Hermitian matrix in $M_m(\mathcal{O}/p)$ which is equivalent to 1_m can be lifted to a ρ-Hermitian matrix in $M_m(\mathcal{O}_p)$, equivalent to 1_m.

LEMMA 5.2. *Suppose* $(K/p)=+1$. *Then we have*:
(i) ϕ_k *is surjective for all* $k\geq 2$.
(ii) $\mathrm{Ker}(\phi_k)\simeq\{1+p^{k-1}X;\ X\in M_m(\boldsymbol{Z}_p/p^k)\}\simeq M_m(\boldsymbol{Z}/p)$.
(iii) $A_{p^k}(1_m)=p^{(k-1)m^2}\,\#(GL_m(\boldsymbol{Z}/p))$.
(iv) $\alpha_p(1_m)=\prod_{j=1}^m(1-(K/p)^jp^{-j})$.

LEMMA 5.3. *Suppose* $(K/p)=-1$. *Then we have*:
(i) ϕ_k *is surjective for all* $k\geq 2$.
(ii) $\mathrm{Ker}(\phi_k)\simeq\{X\in M_m(\mathcal{O}/p);\ X+{}^tX^\rho=0\}$ $(k\geq 2)$.
(iii) $A_{p^k}(1_m)=p^{(k-1)m^2}\,\#(\mathbb{U}_m(\mathcal{O}/p))$.
(iv) $\alpha_p(1_m)=\prod_{j=1}^m(1-(K/p)^jp^{-j})$.

LEMMA 5.4. *Suppose* $(K/p)=0$, *and* $p\neq 2$. *Then we have*:

(i) ϕ_k *is surjective for all* $k \geq 2$.

(ii) $\mathrm{Ker}(\phi_k) \simeq \{X \in M_m(\boldsymbol{Z}/p);\ X + {}^tX = 0\}$ $(k \geq 2)$.

(iii) $A_{p^k}(1_m) = p^{(k-1)m^2 + m(m+1)/2}\, \sharp(\mathbb{O}_m(\boldsymbol{Z}/p))$.

(iv) $\alpha_p(1_m) = 2\prod_{j=1}^m (1 - (K/p)^j p^{-j}) \times \begin{cases} [1 + (-1/p)^{m/2} p^{-m/2}]^{-1} & \cdots\ m\text{: even} \\ 1 & \cdots\ m\text{: odd}. \end{cases}$

Here we understand that $(K/p)^j = +1$ *if* j *is even, and* $(K/p)^j = 0$ *if* j *is odd.*

LEMMA 5.5. *Suppose that* $(K/p) = 0$ *and* $p = 2$. *Write* $p = P^2$ *in* K, *and consider the following diagram consisting of natural projections*:

$$\begin{tikzcd} \mathbb{U}_m(\mathcal{O}/p^k) \arrow[rr, "\phi_k"] \arrow[dr, "\phi_k^{(1)}"'] & & \mathbb{U}_m(\mathcal{O}/p^{k-1}) \\ & \mathbb{U}_m(\mathcal{O}/P^{2k-1}) \arrow[ur, "\phi_k^{(2)}"'] & \end{tikzcd}$$

We have:

(i) ϕ_k *is surjective for all* $k \geq 2$.

(ii) $\sharp(\mathrm{Coker}\,\phi_2^{(2)}) = 2^{m-1}$, $\sharp(\mathrm{Coker}\,\phi_k^{(2)}) = 2^m$ $(k \geq 3)$ $\cdots$ $4 \,\|\, d(K)$,
$\sharp(\mathrm{Coker}\,\phi_3^{(2)}) = 2^{m-1}$, $\sharp(\mathrm{Coker}\,\phi_k^{(2)}) = 2^m$ $(k \geq 2, k \neq 3)$ $\cdots$ $8 \,\|\, d(K)$.

(iii) $\sharp(\mathrm{Ker}\,\phi_k^{(1)}) = \sharp(\mathrm{Ker}\,\phi_k^{(2)}) = 2^{m(m+1)/2}$ *for all* $k \geq 2$.

(iv) $A_{p^k}(1_m) = p^{(k-1)m^2 + 1 + m(m+1)/2}\, \sharp(\mathbb{O}_m(\boldsymbol{Z}/p))$ $(k \geq 3)$,
$A_{p^2}(1_m) = p^{m^2 + m(m+1)/2}\, \sharp(\mathbb{O}_m(\boldsymbol{Z}/p)) \times \begin{cases} p & \cdots\ 4 \,\|\, d(K) \\ 1 & \cdots\ 8 \,\|\, d(K). \end{cases}$

(v) $\alpha_p(1_m) = 2\prod_{j=1}^m (1 - (K/p)^j p^{-j}) \times \begin{cases} [1 + p^{-m}]^{-1} & \cdots\ m\text{: even} \\ 1 & \cdots\ m\text{: odd}. \end{cases}$

Here $d(K)$ *is the descriminant of* K, *and we apply the same convention in* (v) *as in Lemma* 5.4.

The proofs of these lemmas will be given in the next paragraph. Now, substituting these results for $\alpha_v(1_m)$ to (5.4) and applying the well-known formula for the values of Dirichlet's L-function at integral points, we get the following:

THEOREM 5.6 (cf. Otremba [18]). *When* $\boldsymbol{M} = K$ *and* $\boldsymbol{N} = \boldsymbol{Q}$, *the mass* $\boldsymbol{M}_m(1_m)$ *is expressed as follows*:

$$\mathbb{M}_m(1_m) = 2^{1-t} \prod_{j=1}^m \frac{|B_{j,\chi^j}|}{2j} \prod_{\substack{p \mid d(K) \\ p \neq 2}} (p^{m/2} + (-1/p)^{m/2}) \times \begin{cases} 2^m - 1 & \cdots\ 4 \,\|\, d(K) \\ 2^{m/2}(2^m - 1) & \cdots\ 8 \,\|\, d(K) \\ 1 & \cdots\ (2, d(K)) = 1 \end{cases} \qquad (m\text{: even}), \tag{5.5}$$

$$\mathbb{M}_m(1_m) = 2^{1-t} \prod_{j=1}^m \frac{|B_{j,\chi^j}|}{2j} \qquad (m\text{: odd}).$$

Here $\chi(*):=(K/*)$ *is the Dirichlet character attached to* K, *and* B_{j,χ^j} *is the* j-*th generalized Bernoulli number attached to the primitive character* χ^j (*see the convention above*).

Our method can be applied without any difficulty, to more general cases of M/N. In particular, we have the following generalization of Theorem 5.6 which we need later in [10] (cf. Hashimoto [7]).

THEOREM 5.7. *Suppose that* M *is abelian over* Q, *and* m *is odd. Let* $X(M/Q)$ *be the set of primitive Dirichlet characters attached to* M/Q *in class field theory. Then the mass of the genus of* R_M^m *in the Hermitian space* $(M^m, 1_m)$ *is given as follows*:

$$\mathbb{M}_m(1_m)=2^{1-T}\prod_{j=1}^{m}\prod_{\substack{\psi\in X(M/Q)\\ \psi(-1)=(-1)^j}}\frac{|B_{j,\psi}|}{2j}, \tag{5.6}$$

where T *is the number of distinct prime divisors of* $d(M/N)$.

Since the proof of this theorem is exactly the same as that of Theorem 5.6, we omit it.

Next we mention the relationship between the masses with respect to the unitary and the special unitary groups. To avoid unnecessary complications, we consider the simplest case of principal genera. Let $\mathbb{G}=\mathbb{U}(V, H)$ be as usual, and let $\mathbb{G}^{(1)}=\mathbb{SU}(V, H)$ be the special unitary group, where $(V, H)=(K^m, 1_m)$ is the standard Hermitian space. Let $\mathscr{L}$, $\mathscr{L}^{(1)}$ be the principal genus of $\mathbb{G}$, $\mathbb{G}^{(1)}$, respectively. Then we have the following:

PROPOSITION 5.8. *For the masses* $\mathbb{M}_m(\mathbb{G};\mathscr{L})$ *and* $\mathbb{M}_m(\mathbb{G}^{(1)};\mathscr{L}^{(1)})$ *of the principal genus with respect to* $\mathbb{G}$ *and* $\mathbb{G}^{(1)}$, *we have*

$$\mathbb{M}_m(\mathbb{G};\mathscr{L})=\mathbb{M}_1(\mathbb{G};\mathscr{L})\cdot\mathbb{M}_m(\mathbb{G}^{(1)};\mathscr{L}^{(1)}), \qquad \mathbb{M}_1(\mathbb{G};\mathscr{L})=|B_{1,\chi}|/2^{t-1}.$$

PROOF. We normalize the measure $dt_{\mathbb{A}}=\prod_v dt_v$ of $G_{\mathbb{A}}$ by the condition $\mathrm{vol}(U_v; dt_v)=1$ for all v. Since the $\mathcal{O}_p$-lattice L_p has an orthogonal basis, we see that the image of the determinant of $U_p=\mathbb{U}(L_p)$ is the set $\mathcal{O}_p^{(1)}$ of norm one elements in $\mathcal{O}_p$ for all L in the principal genus. Therefore we can define the measure $ds_{\mathbb{A}}=\prod_v ds_v$ in such a way that $\mathrm{vol}(U_v^{(1)}; ds_v)=1$ for all v, and that the quotient $dt_{\mathbb{A}}/ds_{\mathbb{A}}$ induces on $G_{\mathbb{A}}/G_{\mathbb{A}}^{(1)}\simeq K_{\mathbb{A}}^{(1)}$ the same measure as that we defined for $G_{\mathbb{A}}$ with $m=1$. Applying Theorem 5.6 to $m=1$, we get the assertion. q.e.d.

5.2. Now we prove Lemmas 5.2, 5.3, 5.4 and 5.5. In the first three of these lemmas, the assertions (i), (ii) are easy consequences of the remark preceding Lemma 5.2. Then (iii), (iv) follows from the following formulae for the orders of the classical groups over finite fields.

LEMMA 5.9. *Let* $\mathbb{F}_p=Z/p$, *and let* $\mathbb{F}_q$ $(q=p^2)$ *be the quadratic extension of* $\mathbb{F}_p$. *Then we have*:

(i) $\sharp(GL_m(\mathbb{F}_p))=\prod_{j=1}^m(p^m-p^{j-1})$.

(ii) $\#(\mathbb{U}_m(\mathbb{F}_q/\mathbb{F}_p))=p^{m(m-1)/2}\prod_{j=1}^{m}(p^j-(-1)^j)$.

(iii) *If* $p\neq 2$, *then*

$$\#(\mathbb{O}_m(\mathbb{F}_p))=2p^{m(m-1)/2}\prod_{j=1}^{[(m-1)/2]}(1-p^{-2j})$$
$$\times\begin{cases}1-(-1/p)^{m/2}p^{-m/2} & \cdots\ m\text{: even}\\ 1 & \cdots\ m\text{: odd}\,.\end{cases}$$

(iv) *If* $p=2$, *then*

$$\#(\mathbb{O}_m(\mathbb{F}_p))=p^{m(m-1)/2}\prod_{j=1}^{[(m-1)/2]}(1-p^{-2j})\,.$$

PROOF. (i), (ii) and (iii) are well-known (cf. Wall [23], see also Siegel [20, Hilfssatz 18], for (iii). So we prove (iv). Note first that our group $\mathbb{O}_m(\mathbb{F}_p)$ is not equal to the group of linear transformations in $X_1,\cdots,X_m$ which leave the quadratic form $X_1^2+\cdots+X_m^2=(X_1+\cdots+X_m)^2$ invariant. Put $e_0:={}^t(1,0,\cdots,0)$, $e^*={}^t(1,\cdots,1)\in\mathbb{F}_p^m$. We note that, for any vector $e\in\mathbb{F}_p^m$, we have the equality $(e,e)=(e,e^*)$ for the inner products. We claim that the orbit E_m of the vector e_0 under the natural action of $\mathbb{O}_m(\mathbb{F}_p)$ is given by the set

$$(*)\qquad E_m=\{e\in\mathbb{F}_p^m;\ (e,e)=1,\ e\neq e^*\}\,.$$

To prove this, take an arbitrary vector e_1 belonging to the right hand side of $(*)$. We look for the vectors $e_2,\cdots,e_m$ inductively, satisfying the conditions $(e_i,e_1)=(e_i,e_2)=\cdots=(e_i,e_{i-1})=0$. The existence of $e_1,\cdots,e_{m-1}$ is easily seen from the above remark. To find e_m is equivalent to solving the system of linear equations in e_m:

$$(**)\qquad (e_m,e^*)=1\,,\qquad (e_m,e_j)=0\qquad (1\leq j\leq m-1)\,.$$

Hence it is also equivalent to the linear independence of $e^*,e_1,\cdots,e_{m-1}$ over $\mathbb{F}_p$. Suppose they satisfy a linear equation

$$\sum_{j=1}^{m-1}\lambda_j e_j+\lambda_0 e^*=0\qquad (\lambda_j\in\mathbb{F}_p)\,.$$

Taking the inner product with e_j, one gets $\lambda_j=\lambda_0$ $(1\leq j\leq m-1)$. Again taking the inner product with e^*, one then has

$$0=\sum_{j=1}^{m-1}\lambda_j+\lambda_0(e^*,e^*)=(2m-1)\lambda_0\,,$$

which shows that $\lambda_j=0$ for all j, hence the existence of e_m. Then we see that the matrix $(e_1,\cdots,e_m)$ belongs to $\mathbb{O}_m(\mathbb{F}_p)$, and it transforms e_0 to e_1. This proves our claim.

Now it follows easily that

$$\#(E_m)=\#(\mathbb{O}_m(\mathbb{F}_p)/\mathbb{O}_{m-1}(\mathbb{F}_p))=2^{m-1}\quad\text{or}\quad 2^{m-1}-1$$

according as m is even or odd. Our assertion (iv) follows from this by induction.

q.e.d.

PROOF OF LEMMA 5.5. First note that $\mathbb{U}_m(\mathcal{O}/p^k)=\mathbb{U}_m(\mathcal{O}_p/p^k)$, $\mathbb{U}_m(\mathcal{O}/P^{2k-1})=\mathbb{U}_m(\mathcal{O}_p/P^{2k-1})$ for all k. Hence it suffices to prove the assertion with $\mathcal{O}_p$ instead of $\mathcal{O}$. We denote the prime elements of $\boldsymbol{Z}_p$, $\mathcal{O}_P$ by the same letters p, P, respectively. It satisfies

$$p^\rho=p\,,\qquad P^\rho\equiv P\pmod{p}\,. \tag{5.7}$$

(i): Fix an arbitrary element X_0 of $M_m(\mathcal{O}_p)$ satisfying $X_0{}^tX_0^\rho\equiv 1_m \pmod{P^{2k-1}}$. Put $C:=p^{1-k}(1_m-X_0{}^tX_0^\rho)$. Then C is a Hermitian matrix in $P\cdot M_m(\mathcal{O}_p)$. So, writing $C=(c_{ij})$, we have

$$c_{ii}=c_{ii}^\rho\in p\cdot\mathcal{O}_p\,,\qquad c_{ij}^\rho=c_{ji}\in P\cdot\mathcal{O}_p\qquad(i\neq j)\,. \tag{5.8}$$

It suffices to show that there exists $X_1\in M_m(\mathcal{O}_p)$ such that $X_0+p^{k-1}PX_1 \pmod{p^k}$ belongs to $\mathbb{U}_m(\mathcal{O}_p/p^k)$. Thanks to (5.7), we can rewrite this condition as

$$P\cdot(X_1{}^tX_1^\rho-X_0{}^tX_0^\rho)\equiv C\pmod{p}\,. \tag{5.9}$$

Here (5.8) shows the existence of $Y\in M_m(\mathcal{O}_p)$ such that $P\cdot(Y-{}^tY^\rho)\equiv C \pmod{p}$. Since X_0 is invertible, we may put $X_1=Y({}^tX_0^\rho)^{-1}$. Now it follows that this X_1 satisfies (5.9), which completes the proof of (i).

(ii): We give a description of the homogeneous space $\mathbb{U}_m(\mathcal{O}_p/p^{k-1})/\mathrm{Im}(\phi_k^{(2)})$ as follows. Let X_0 be an arbitrary element of $M_m(\mathcal{O}_p)$ such that $X_0 \pmod{p^{k-1}}$ belongs to $\mathbb{U}_m(\mathcal{O}_p/p^{k-1})$. Put $C=C(X_0):=p^{1-k}(1_m-X_0{}^tX_0^\rho)$, $C=(c_{ij})$. Then $C={}^tC^\rho\in M_m(\mathcal{O}_p)$. We define an element $e=e(X_0)$ of $\mathbb{F}_p^m$ by

$$e:=(c_{11},\cdots,c_{mm})\pmod{p}\,,$$

and a subset $E(k)$ of $\mathbb{F}_p^m$ by

$$E(k):=\{e\in\mathbb{F}_p^m;\ \exists\, X_0\in M_m(\mathcal{O}_p)\text{ with }X_0 \pmod{p^{k-1}}\in\mathbb{U}_m(\mathcal{O}_p/p^{k-1})\text{ and }e(X_0)=e\}\,.$$

For any $g\in\mathbb{U}_m(\mathcal{O}_p/p^{k-1})$ and any $e\in E(k)$, write

$$g\equiv X \pmod{p^{k-1}}\,,\qquad X\in M_m(\mathcal{O}_p)\,,$$

$$e=e(X_0)\,,\qquad X_0\in M_m(\mathcal{O}_p)\,,\qquad X_0 \pmod{p^{k-1}}\in\mathbb{U}_m(\mathcal{O}_p/p^{k-1})\,.$$

It is easy to see that $e(XX_0)$ does not depend on the choice of X or X_0, and we can define an action of $\mathbb{U}_m(\mathcal{O}_p/p^{k-1})$ on $E(k)$ by

$$g\cdot e(X_0)=e(XX_0)\,.$$

Here we can show, as in the proof of (i), that the stabilizer of $e=(0,\cdots,0)$ is nothing but $\mathrm{Im}(\phi_k^{(2)})$. Hence we have

$$\mathbb{U}_m(\mathcal{O}_p/p^{k-1})/\mathrm{Im}(\phi_k^{(2)})\simeq E(k)\,.$$

Moreover, it is not difficult to show

$$(5.10)\qquad E(k)=\begin{cases}\left\{(\varepsilon_1,\cdots,\varepsilon_m)\in\mathbb{F}_p^m;\ \sum_{i=1}^m \varepsilon_i=0\right\} & \cdots\ k=2\\ \mathbb{F}_p^m & \cdots\ k\geq 3\end{cases}\qquad (4\,\|\,d(K))\,,$$

$$(5.11)\qquad E(k)=\begin{cases}\left\{(\varepsilon_1,\cdots,\varepsilon_m)\in\mathbb{F}_p^m;\ \sum_{i=1}^m \varepsilon_i=0\right\} & \cdots\ k=3\\ \mathbb{F}_p^m & \cdots\ k\geq 2,\ k\neq 3\end{cases}\qquad (8\,\|\,d(K))\,.$$

The assertion (ii) is a consequence of these results.

(iii): Let g be an element of $\mathrm{Ker}(\phi_k^{(1)})$. Then we may write $g=1_m+p^{k-1}PX_1 \pmod{p^k}$ with $X_1\in M_m(\mathcal{O}_p)$, and g is seen to be determined by $X_1 \pmod P$. Here, a straightforward calculation shows that the unitarity of g is translated into the equality $X_1+{}^tX_1^\rho\equiv 0 \pmod P$. Now it is easy to see that

$$\sharp(\mathrm{Ker}(\phi_k^{(1)}))=\sharp\{X_1 \pmod P;\ X_1+{}^tX_1^\rho\equiv 0\}=2^{m(m+1)/2}\,.$$

Similarly we get $\sharp(\mathrm{Ker}(\phi_k^{(2)}))=2^{m(m+1)/2}$. q.e.d.

5.3. Here we give some remarks on the above results. Let again K be an imaginary quadratic field, and let (V, H) be a positive definite Hermitian space over K of rank m. Let L be an $\mathcal{O}$-lattice, and $\mathscr{L}=\mathscr{L}(L)$ be the genus containing L. Let $L_1,\cdots,L_h$ be a complete set of representatives of the classes in $\mathscr{L}$, and let $\Gamma_i:=\mathbb{U}(L_i)$ $(1\leq i\leq h)$ be the unit group of L_i. As remarked in §3, the positivity of (V, H) implies that Γ_i's are finite groups. The following lemma shows that the orders of these groups are bounded by a constant which depends only on the genus $\mathscr{L}$.

LEMMA 5.10. *Let $d(\mathscr{L})$ be the product of the local discriminant $d(L_p)$ of L_p*

$$d(\mathscr{L}):=\prod_p p^{m_p}\,,\qquad d(L_p)\boldsymbol{Z}_p=p^{m_p}\boldsymbol{Z}_p\,,$$

extended over the finite places p. Let p be any finite place not dividing $2d(\mathscr{L})$. Then we have:

(i) *If $(K/p)=+1$, then each Γ_i is isomorphic to a subgroup of $GL_m(\mathbb{F}_p)$.*

(ii) *If $(K/p)=-1$, then each Γ_i is isomorphic to a subgroup of $U_m(\mathbb{F}_q/\mathbb{F}_p)$, where $q=p^2$.*

(iii) *If $(K/p)=0$, then each Γ_i is isomorphic to a subgroup of an orthogonal group of degree m over $\mathbb{F}_p$.*

PROOF. We prove (ii). Let p be as above, and $(K/p)=-1$. Then it is easy to see that H induces a non-degenerate Hermitian form on L_p/pL_p, which is an m-dimensional vector space over $\mathbb{F}_q$. Since $\Gamma_i=\mathrm{Aut}(L_i, H)$, the elements of Γ_i induce naturally isometries on $L_{ip}/pL_{ip}\simeq L_p/pL_p$. We claim that the correspondence

$$\Gamma_i = \mathrm{Aut}(L_i, H) \to \mathrm{Aut}(L_{ip}/pL_{ip}, H) \simeq \mathrm{Aut}(L_p/pL_p, H)$$

is an injective homomorphism. Indeed, if $g \in \Gamma_i$ corresponds to the identity of $\mathrm{Aut}(L_p/pL_p, H)$, it follows that all the eigenvalues ζ of g must satisfy $\zeta \equiv 1 \pmod{p}$, which implies $g = 1_m$, because g is of finite order (hence ζ's are roots of unity), and we are assuming that $p > 2$. This proves the assertion (ii). The other assertions are proved quite similarly. q.e.d.

The above lemma has the following important application:

THEOREM 5.11. *Notation being as above, let C be the greatest common divisor of the orders of the finite groups $GL_m(\mathbb{F}_p)$, $\mathbb{U}_m(\mathbb{F}_q/\mathbb{F}_p)$ and $\mathbb{O}_m(\mathbb{F}_p)$, where p varies as in Lemma* 5.10. *Then C depends only on the genus $\mathscr{L}$, and we have the following estimates for the class number $\boldsymbol{h} = \boldsymbol{h}(\mathscr{L})$ of $\mathscr{L}$*:

$$\sharp(W(K)) \cdot \mathbb{M}(\mathbb{G}; \mathscr{L}) \leq \boldsymbol{h}(\mathscr{L}) \leq C \cdot \mathbb{M}(\mathbb{G}; \mathscr{L}), \tag{5.12}$$

where $\mathbb{M}(\mathbb{G}; \mathscr{L})$ is the mass of $\mathscr{L}$.

PROOF. This is an immediate consequence of the above lemma and the definition (3.4) of the mass $\mathbb{M}(\mathbb{G}; \mathscr{L}) = \mathbb{M}(U(L))$, together with the fact that $W(K) = \mathcal{O}^\times$ is a subgroup of every Γ_i. q.e.d.

By a more detailed argument using the method of Hashimoto [6], it would be possible to decide all possible subgroups of $GL_m(\mathbb{F}_p)$, $\mathbb{U}_m(\mathbb{F}_q/\mathbb{F}_p)$ and $\mathbb{O}_m(\mathbb{F}_p)$ which appear as the image of some Γ_i, provided the rank m is small enough and $\mathscr{L}$ is sufficiently simple. However, we shall not go into this problem here and content ourselves with the following observation:

PROPOSITION 5.12. *Let K be imaginary quadratic, and (V, H) be a positive Hermitian space. Take, in this space, a genus $\mathscr{L}$ of $\mathcal{O}$-lattices. Then the contribution $T_1 = T(f_1)$ from the identity element to the class number formula* (3.7) *is equal to $\mathbb{M}(G; \mathscr{L})$. In particular, if $(V, H) = (K^m, 1_m)$, $\mathscr{L}$ is the principal genus and $m = 3$, it is given by*

$$T_1 = \frac{h(K)B_{3,\chi}}{2^{t+3}3^2 \cdot \sharp(W(K))}. \tag{5.13}$$

This follows from Theorem 5.6 and a well-known formula:

$$-B_{1,\chi} = 2h(K)/\sharp(W(K)). \tag{5.14}$$

As a corollary to the above lemma, we have:

PROPOSITION 5.13 (cf. Otremba [18]). *Let $(V, H) = (K^m, 1_m)$ and $\mathscr{L}$ be the principal genus, and suppose that $m > 1$. Then $\boldsymbol{h}(\mathscr{L}) = 1$ exactly in the following cases*:

(i) $m = 2$: $d(K) = -3, -4, -7, -8$.

(ii) $m = 3$: $d(K) = -3, -4$.

(iii) $m=4$: $d(K)=-3, -4$.
(iv) $m=5$: $d(K)=-3$.

PROOF. For the standard lattice $\mathcal{O}^m \in \mathcal{L}$, we know that its unit group is the semi-direct product of $(W(K))^m$ and the symmetric group of degree m, hence its order is $(m!)\cdot(\# W(K))^m$. On the other hand, we see from the table of the generalized Bernoulli numbers given below, that $1/\mathbb{M}(\mathbb{G}; \mathcal{L})$ is equal to this number exactly in the cases listed above. Since $\boldsymbol{h}(\mathcal{L})=1$ if and only if these two numbers are equal, we have the assertion. q.e.d.

TABLE OF THE GENERALIZED BERNOULLI NUMBERS. In the following table, we give, for each imaginary quadratic field K with discriminant $|d(K)|<250$, the Bernoulli numbers $B_{1,\chi}$, $B_{3,\chi}$, and $B_{5,\chi}$, where χ is the Dirichlet character attached to K, that is, $\chi(*)=(d(K)/*)$.

(l)	$d(K)$	ramified primes	$B_{1,\chi}$	$B_{3,\chi}$	$B_{5,\chi}$
(1)	−3	3	−1/3	2/3	−10/3
(2)	−4	2	−1/2	3/2	−25/2
(3)	−7	7	−1	48/7	−160
(4)	−8	2	−1	9	−285
(5)	−11	11	−1	18	−12750/11
(6)	−15	3*5	−2	48	−4960
(7)	−19	19	−1	66	−13450
(8)	−20	2*5	−2	90	−17610
(9)	−23	23	−3	144	−34080
(10)	−24	2*3	−2	138	−39850
(11)	−31	31	−3	288	−129600
(12)	−35	5*7	−2	324	−211860
(13)	−39	3*13	−4	528	−365600
(14)	−40	2*5	−2	474	−395210
(15)	−43	43	−1	498	−530410
(16)	−47	47	−5	864	−849600
(17)	−51	3*17	−2	804	−1148500
(18)	−52	2*13	−2	906	−1286570
(19)	−55	5*11	−4	1200	−1709920
(20)	−56	2*7	−4	1188	−1811700
(21)	−59	59	−3	1206	−2221950
(22)	−67	67	−1	1506	−3902410
(23)	−68	2*17	−4	1908	−4337940
(24)	−71	71	−7	2448	−5440800
(25)	−79	79	−5	2976	−8724800
(26)	−83	83	−3	2790	−10315230
(27)	−84	2*3*7	−4	3156	−11186900
(28)	−87	3*29	−6	3888	−13515360
(29)	−88	2*11	−2	3354	−13725770
(30)	−91	7*13	−2	3300	−15487700

(l)	$d(K)$	ramified primes	$B_{1,\chi}$	$B_{3,\chi}$	$B_{5,\chi}$
(31)	−95	5*19	−8	5040	−20166240
(32)	−103	103	−5	5712	−28772000
(33)	−104	2*13	−6	5598	−29370750
(34)	−107	107	−3	5238	−32344830
(35)	−111	3*37	−8	7248	−40477600
(36)	−115	5*23	−2	5892	−44394260
(37)	−116	2*29	−6	7326	−48004350
(38)	−119	7*17	−10	8928	−55588800
(39)	−120	2*3*5	−4	7620	−55668020
(40)	−123	3*41	−2	7140	−60305620
(41)	−127	127	−5	9600	−73836800
(42)	−131	131	−5	8874	−80468850
(43)	−132	2*3*11	−4	9636	−85463540
(44)	−136	2*17	−4	10164	−97412500
(45)	−139	139	−3	9558	−104207550
(46)	−143	11*13	−10	13968	−126996000
(47)	−148	2*37	−2	12282	−142408970
(48)	−151	151	−7	15024	−161000800
(49)	−152	2*19	−6	14238	−161914110
(50)	−155	5*31	−4	13320	−171476520
(51)	−159	3*53	−10	17808	−203962400
(52)	−163	163	−1	13890	−213225610
(53)	−164	2*41	−8	17496	−228069000
(54)	−167	167	−11	20592	−255272160
(55)	−168	2*3*7	−4	17556	−252966740
(56)	−179	179	−5	19242	−327860850
(57)	−183	3*61	−8	24816	−383680480
(58)	−184	2*23	−4	21540	−379597300
(59)	−187	11*17	−2	19716	−395673620
(60)	−191	191	−13	29088	−467361600
(61)	−195	3*5*13	−4	22920	−479879720
(62)	−199	199	−9	30096	−557594400
(63)	−203	7*29	−4	25992	−577203240
(64)	−211	211	−3	26982	−681635550
(65)	−212	2*53	−6	32526	−723516510
(66)	−215	5*43	−14	39024	−795959520
(67)	−219	3*73	−4	30696	−809210600
(68)	−223	223	−7	39360	−930190720
(69)	−227	227	−5	34506	−954428850
(70)	−228	2*3*19	−4	37572	−999666740
(71)	−231	3*7*11	−12	45216	−1095201600
(72)	−232	2*29	−2	37770	−1076601770
(73)	−235	5*47	−2	34980	−1106475860
(74)	−239	239	−15	50976	−1281729600
(75)	−244	2*61	−6	43902	−1351919550
(76)	−247	13*19	−6	50544	−1473281760
(77)	−248	2*31	−8	48456	−1465634280

6. Unimodular lattices.

6.1. In this section, we use the notation of § 1; thus we assume that K is an imaginary quadratic field, and (V, H) is a positive definite Hermitian space over K of rank m. Here our purpose is to recall briefly some basic results on the local theory of Hermitian lattices, which were settled by Jacobowitz [14] and Shimura [19]. Especially the former's result on the Jordan splitting of the general lattices will play an essential role in our calculation of the class numbers. This fact also shows a limit of our calculation, thus explaining our restriction to the genera of unimodular lattices.

Let us recall some definitions. An $\mathcal{O}$-lattice L in (V, H) is said to be $\mathfrak{a}$-modular, for an ideal $\mathfrak{a}=\mathfrak{a}^\rho$ of K, if it satisfies $L=\mathfrak{a}\cdot L^*$, where $L^*:=\{x\in V;\ H(x, L)\subset\mathcal{O}\}$ is the dual lattice of L. In particular, an $\mathcal{O}$-modular lattice is called *unimodular*. Let p be a finite place of $\boldsymbol{Q}$. For an ideal $\mathfrak{a}=\mathfrak{a}^\rho$ of $\mathcal{O}_p$, we define $\mathfrak{a}$-modular lattices similarly. Let L_p be an $\mathcal{O}_p$-lattice in (V_p, H). Define the discriminant $d(L_p)$ to be an element of $\boldsymbol{Q}_p^\times/N_{K_p/\boldsymbol{Q}_p}(\mathcal{O}_p^\times)$ represented by $\det[H(x_i, x_j)]$, where $x_1, \cdots, x_m$ is an $\mathcal{O}_p$-basis of L_p. Notice that $d(L_p)$ does not depend on the choice of the basis. The following assertion is easily proved.

LEMMA 6.1. *For an $\mathcal{O}_p$-lattice L_p in (V_p, H), the following three conditions are equivalent*:

(i) *L_p is unimodular.*

(ii) *$d(L_p)$ is represented by an element of $\boldsymbol{Z}_p^\times$.*

(iii) *$H(x, L_p)=\mathcal{O}_p$ for any primitive vector $x\in L_p$ (i.e. $x\notin P\cdot L_p$).*

6.2. We denote by $s(L_p)$ the $\mathcal{O}_p$-ideal generated by $\{H(x, y);\ x, y\in L_p\}$, and by $n(L_p)$ the ideal generated by $\{H(x, x);\ x\in L_p\}$. When $(K/p)=+1$, we have $K_p=\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p$, $\mathcal{O}_p=\boldsymbol{Z}_p\oplus\boldsymbol{Z}_p$, and we may put

$$V_p=K_p^m=\boldsymbol{Q}_p^m\oplus\boldsymbol{Q}_p^m\,. \tag{6.1}$$

Then we may write

$$\begin{aligned} &H(x, y)=(x_1H_0{}^ty_2,\ x_2{}^tH_0{}^ty_1)\,, \qquad x=(x_1, x_2)\,,\quad y=(y_1, y_2) \\ &G_p=\{(g,\ {}^tH_0{}^tg^{-1}{}^tH_0^{-1})\,;\qquad g\in GL_m(\boldsymbol{Q}_p)\}\,, \end{aligned} \tag{6.2}$$

where H_0 is an element of $GL_m(\boldsymbol{Q}_p)$. Let L_p be a unimodular $\mathcal{O}_p$-lattice in (V_p, H). Then it is easy to see that

$$L_p=L_0\oplus L_0^*\,, \tag{6.3}$$

where L_0 is a $\boldsymbol{Z}_p$-lattice in $\boldsymbol{Q}_p^m$ and

$$L_0^*:=\{x\in\boldsymbol{Q}_p^m;\ yH_0{}^tx\in\boldsymbol{Z}_p \text{ for any } y\in L_0\}\,.$$

From (6.2) and (6.3), we see that all unimodular lattices in (V_p, H) are isometric, and the automorphism group $\mathbb{U}(L_p)$ of (L_p, H) is

$$\mathbb{U}(L_p)=\{(g, {}^tH_0{}^tg^{-1}{}^tH_0^{-1});\ g\in GL_{\mathbf{Z}_p}(L_0)\}\ . \tag{6.4}$$

Next let us assume $(K/p)\neq +1$. In this case, we have the following:

LEMMA 6.2 (Jacobowitz [14]). (i) *If $(K/p)=-1$, then (V_p, H) contains a unimodular lattice if and only if $(d(V_p), K/\mathbf{Q}_p)=+1$. In this case, any unimodular lattice has an orthogonal basis, hence any two such lattices are isometric.*

(ii) *If $(K/p)=0$, and $p\neq 2$, then there is a unique isometry class of unimodular lattices in each Hermitian space (V_p, H); and any member of this class has an orthogonal basis.*

(iii) *If $(K/p)=0$ and $p=2$, then (V_p, H) always contain a unimodular lattice. Two such lattices L_p, L'_p are isometric if and only if $n(L_p)=n(L'_p)$. Moreover, the set $\{n(L_p);\ L_p(\subset V_p)$: unimodular$\}$ is equal to either $\{\mathcal{O}_p, p\mathcal{O}_p\}$ or $\{\mathcal{O}_p\}$.*

We say that an $\mathcal{O}_p$-lattice L_p in (V_p, H) is *normal*, if $n(L_p)=s(L_p)$, and *subnormal* otherwise. If L_p is a modular lattice, it is normal if and only if it has an orthogonal basis (see [14, Proposition 4.4]). Thus every unimodular lattice is normal in the cases (i), (ii) of the above lemma. As for (iii), we can state exactly when a subnormal unimodular lattice exists in (V_p, H); but for our purpose we need only the following:

LEMMA 6.3. *Suppose $(K/p)=0$, $p=2$, and put $m=\mathrm{rank}(V_p)$.*

(i) *If m is odd, then every unimodular lattice in (V_p, H) is normal.*

(ii) *Suppose $m=2$. Then if either $8\,\|\,d(K)$, or $4\,\|\,d(K)$ with $(d(V_p), K/\mathbf{Q})_p=-1$, there exist subnormal unimodular lattices in (V_p, H). For any such L_p, we have*

$$(L_p, H)=\begin{pmatrix}0&1\\1&0\end{pmatrix}\cdots \text{ if } (-d(V), K/\mathbf{Q})_p=+1\ , \tag{6.5}$$

$$(L_p, H)=\begin{pmatrix}2&1\\1&2\end{pmatrix}\cdots \text{ if } (-d(V), K/\mathbf{Q})_p=-1\ . \tag{6.6}$$

Here, (6.5) for example, means that there exists an $\mathcal{O}_p$-basis x, y of L_p such that $H(x,x)=H(y,y)=0$ and $H(x,y)=1$. If $4\,\|\,d(K)$ and $(d(V), K/\mathbf{Q})_p=+1$, every unimodular lattice in (V_p, H) is normal ($m=2$). The above lemma is verified easily by the results in [14], so we omit the proof.

6.3. Summarizing the above lemmas, we have:

PROPOSITION 6.4. *Let K be an imaginary quadratic field. In the set of isometry classes of positive definite Hermitian spaces (V, H) of rank m, there exist exactly 2^{t-1} classes which contain a unimodular $\mathcal{O}$-lattice, where t is the number of distinct prime divisors of the discriminant $d(K)$ of K. They are characterized by the condition*

$$(d(V), K/\mathbf{Q})_p=+1 \qquad \text{for all places} \quad p \quad \text{with} \quad (K/p)=-1\ . \tag{6.7}$$

They are parametrized by the local norm residues $\{(d(V), K/\mathbf{Q})_p;\ p\,|\,d(K)\}$ which are *subject to the condition*

$$\prod_{p|d(K)} (d(V), K/\boldsymbol{Q})_p = +1 . \tag{6.8}$$

Moreover, for each (V, H) satisfying this condition, there exist at most two genera of unimodular lattices with respect to the unitary group; one is normal and the other is subnormal. The latter exists only if m is even and $2 \mid d(K)$.

Finally, we quote the following fundamental result:

LEMMA 6.5 (Jacobowitz [14]). *Suppose $(K/p) \neq +1$, and let L_p be an arbitrary $\mathcal{O}_p$-lattice in (V_p, H). Then there exists an orthogonal decomposition of L_p:*

$$L_p = L_1 \oplus L_2 \oplus \cdots \oplus L_r , \tag{6.9}$$

where each L_i is a modular lattice and $s(L_1) \subsetneqq s(L_2) \subsetneqq \cdots \subsetneqq s(L_r)$. The sequences

$$\operatorname{rank}(L_1), \cdots, \operatorname{rank}(L_r) , \quad \textit{and} \quad s(L_1), \cdots, s(L_r)$$

are uniquely determined by L_p.

A decomposition of this type is called a *Jordan splitting*.

REFERENCES

[1] T. ASAI, The conjugacy classes in the unitary, symplectic, and orthogonal groups over an algebraic number field, J. Math. Kyoto Univ. 16 (1976), 325–350.

[2] T. ASAI, The class numbers of positive definite quadratic forms, Japan. J. Math. 3 (1977), 239–296.

[3] A. BOREL AND HARISH-CHANDRA, Arithmetic subgroups of algebraic groups, Ann. Math. 75 (1962), 485–535.

[4] H. BRAUN, Zur Theorie der Hermitischen Formen, Abh. Math. Sem. d. Hansischen Univ. 14 (1941), 61–150.

[5] M. EICHLER, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z. 43 (1938), 102–109.

[6] K. HASHIMOTO, On Brandt matrices associated with the positive definite quaternion hermitian forms, J. Fac. Sci. Univ. of Tokyo 27 (1980), 227–245.

[7] K. HASHIMOTO, Elliptic conjugacy classes of the Sigel modular group and unimodular hermitian forms over the ring of cyclotomic integers, J. Fac. Sci. Univ. of Tokyo 33 (1986), 57–82.

[8] K. HASHIMOTO AND T. IBUKIYAMA, On class numbers of positive definite binary quaternion hermitian forms, J. Fac. Sci. Univ. of Tokyo 27 (1980), 549–601.

[9] K. HASHIMOTO AND H. KOSEKI, Class numbers of positive definite binary and ternary unimodular Hermitian forms, Proc. Japan Acad. 62, Ser. A (1986), 323–326.

[10] K. HASHIMOTO AND H. KOSEKI, Class numbers of positive definite binary and ternary unimodular Hermitian forms, to appear in Tôhoku Math. J.

[11] H. HASSE, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin (1952).

[12] T. HAYASHIDA, A class number associated with the product of an elliptic curve with itself, J. Math. Soc. Japan 20 (1968), 26–43.

[13] K. IYANAGA, Class numbers of positive definite Hermitian forms, J. Math. Soc. Japan 21 (1969), 359–374.

[14] R. Jacobowitz, Hermitian forms over local fields, Amer. J. Math. 84 (1962), 441–465.
[15] W. Landherr, Äquivalenz Hermitischer Formen über einen beliebigen algebraischen Zahlkörper, Abh. Math. Sem. Univ. Hamburg 11 (1935), 245–248.
[16] J. Milnor, On isometries of inner product spaces, Invent. Math. 8 (1969), 83–97.
[17] T. Ono, On Tamagawa numbers, AMS Proc. Symp. in Pure Math. 9 (1966), 122–132.
[18] G. Otremba, Zur Theorie der Hermitischen Formen in imaginär-quadratischen Zahlkörpern, J. reine angew. Math. 249 (1971), 1–19.
[19] G. Shimura, Arithmetic of unitary groups, Ann. Math. 79 (1964), 369–409.
[20] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, Ann. Math. 36 (1935), 527–606.
[21] T. A. Springer and R. Steinberg, Conjugacy classes, Lecture Notes in Math. 131, Springer-Verlag, Berlin, Heidelberg, New York (1970), 167–266.
[22] T. Tamagawa, On Selberg's trace formula, J. Fac. Sci. Univ. of Tokyo 8 (1960), 363–386.
[23] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Austr. Math. Soc. 3 (1963), 1–62.

Department of Mathematics
Waseda University
3–4–1 Ohkubo, Shinjuku
Tokyo 160
Japan

and

Department of Mathematics
University of Tokyo
7–3–1 Hongo
Tokyo 113
Japan