On class numbers of positive definite binary quaternion hermitian forms

By

Ki-ichiro HASHIMOTO and Tomoyoshi IBUKIYAMA

Reprinted from the
JOURNAL OF THE FACULTY OF SCIENCE, THE UNIVERSITY OF TOKYO
Sec. IA, Vol. 27, No. 3, pp. 549-601
December, 1980

On class numbers of positive definite binary quaternion hermitian forms

By Ki-ichiro HASHIMOTO and Tomoyoshi IBUKIYAMA

In this paper, we shall study the class numbers of positive definite binary quaternion hermitian forms. Let B be a definite division quaternion algebra over the rational number field $\boldsymbol{Q}$. Let V be the n-dimensional positive definite quaternion hermitian space over B. We denote by H the class number of the principal genus of V. When $n=1$, H is nothing but the class number of the maximal orders of B, whose explicit formula has been given by Eichler [4]. In this paper, we shall give an explicit formula for H when $n=2$ (§ 5. Theorem 2). When the discriminant of B is a prime number p, the result is given as follows:

$H=1$, when $p=2$ or 3, and in other cases,

$$H=(p-1)(p^2+1)/2^6\cdot3^2\cdot5+7(p-1)^2/2^6\cdot3^2+(p-1)\left(1-\left(\frac{-1}{p}\right)\right)/2^4\cdot3$$

$$+(p-1)\left(1-\left(\frac{-3}{p}\right)\right)/2^2\cdot3^2+5(p-1)/2^5\cdot3+\left(1-\left(\frac{-1}{p}\right)\right)/2^5$$

$$+\left(1-\left(\frac{-3}{p}\right)\right)^2/3^2+\left(1-\left(\frac{-3}{p}\right)\right)/2^2\cdot3^2+(p-1)/2\cdot3^2$$

$$+\left(1-\left(\frac{-1}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right)/2^2\cdot3$$

$$+\begin{cases}1/5\cdots p=5\\ 0\quad\cdots p\equiv1,\ 2,\ 3\ (\mathrm{mod.}\ 5)\\ 4/5\cdots p\equiv4\ (\mathrm{mod.}\ 5)\end{cases}$$

$$+\begin{cases}0\quad\cdots p\equiv1\ (\mathrm{mod.}\ 8)\\ 1/4\cdots p\equiv3,\ 5\ (\mathrm{mod.}\ 8)\\ 1/2\cdots p\equiv7\ (\mathrm{mod.}\ 8)\end{cases}$$

$$+\begin{cases}0\quad\cdots p\equiv1\ (\mathrm{mod.}\ 6)\\ 1/6\cdots p\equiv5\ (\mathrm{mod.}\ 6),\end{cases}$$

where $\left(\frac{*}{p}\right)$ is the Legendre symbol.

One of our motivations to the problem is Y. Ihara's paper [12]. There, he studies the Dirichlet series defined by the Hecke operators of the binary quaternion hermitian group G of V acting on certain spherical functions, and their Euler products. Though he assumed there that $H=1$, he has kindly shown us how similar theory also holds without the assumption that $H=1$. So there is some interest to compute H, which is also considered as the dimension of 'automorphic forms with weight zero' of G. So we shall also give the dimension formula of the space of 'automorphic forms with higher weights' (Theorem 3 in § 5) as a corollary to Theorem 2.

Now we outline the content of the paper. In § 1, we give precise definitions and review the arithmetic trace formula for H given in [9]. To obtain the explicit formula for H, it is basic to classify conjugacy classes in G, which is carried out in § 2 for general n. In § 3, some Mass formulae which we need are calculated. In § 4, we calculate local data, which is the most elabolate part of the paper. In § 5, we summarize them globally and obtain the formula for H (Theorem 2). In § 6, some numerical examples of the representatives of the lattice classes are given. We also show that the 'type number' of G coincides with the class number of certain genus of quinary quadratic forms studied by T. Asai [2].

Now we explain some technical points in this paper. The class number formula for positive definite quadratic forms over algebraic number fields has been studied by several authors. For example, T. Asai has employed the Springer-Steinberg classification of conjugacy classes, expressed the class numbers by the products of masses of some groups and some hermitian lattices, and obtained explicit formulae for some quaternary and quinary quadratic forms (cf. [1], [2]). We preper to give a direct description of G-conjugacy classes by the method of Hijikata [10], and in some cases, we give another parametrization suitable for our purpose. The other point is the computation of local data $c_p=c_p(g, M_2(O_p), \Lambda_p)$. Roughly spoken, c_p is the number of distinct ways to embed a certain (not necessarily maximal) order Λ_p optimally into a certain algebra, counted up to some equivalence. As it does not seem known any standard way to calculate c_p easily, we need to calculate them case by case, which will be done in § 4. Incidentally, it turns out that $c_p=0$, 1 or 2 in our case (when g is of finite order).

The authors sincerely express their hearty thanks to Professor Y. Ihara for drawing their attention to the arithmetic of quaternion hermitian groups and related problems. They also thank to Professor H. Shimizu for his deep interest in the problem and encouragement for us.

Notations We denote, as usual, by $\boldsymbol{Z}$ (resp. $\boldsymbol{Z}_p$), $\boldsymbol{Q}$ (resp. $\boldsymbol{Q}_p$), $\boldsymbol{R}$, $\boldsymbol{C}$ the ring of rational (resp. p-adic) integers, the field of rational (resp. p-adic) numbers, the

real number field, the complex number field, respectively. For a ring A, we denote by $GL_n(A)$ the group of invertible elements in the full matrix ring $M_n(A)$, and if $n=1$, we also write $A^\times=GL_1(A)$. For an algebra B or algebraic group G over $\boldsymbol{Q}$, we write B_p, G_p for the set of $\boldsymbol{Q}_p$ rational points of B, G, and B_A, G_A for the adelized ring or group of them. We denote by $\sharp S$ or $|S|$ the cardinality of finite set S. For a group G and its subgroup H, we write $g\underset{H}{\sim}g'$ for $g, g'\in G$, if $g'=h^{-1}gh$ for some $h\in H$. We denote by $G/\underset{H}{\sim}$ the quotient set of G by this equivalence relation. For a quaternion algebra B over F, we denote by $x\to\bar{x}$ ($x\in B$) the canonical involution, and put $\mathrm{Tr}(x)=x+\bar{x}$, $N(x)=x\bar{x}$.

§ 1. Lattices in quaternion hermitian space.

In this section, we review the definitions which we need and quote the arithmetic trace formula for H given in [9] which is a starting point of this paper. We note that a systematic treatment for the arithmetic of quaternion hermitian forms has been given by G. Shimura [17], and certain Hecke theory in the binary case has been given by Y. Ihara [12].

1-1. Let B denote a quaternion algebra over $\boldsymbol{Q}$, and V be a left B-space of rank n. Let $f: V\times V\to B$ be a non-degenerate quaternion hermitian form. By definition, it satisfies:

(i) $f(ax+by, z)=af(x, z)+bf(y, z)$,

(ii) $f(x, y)=\overline{f(y, x)}$, and

(iii) $f(x, V)=0$ implies $x=0$,

for all $a, b\in B$, $x, y, z\in V$. We denote by $G=G(V, f)$ the group of all similitudes of f: namely

$$G=G(V, f)$$
$$=\{g\in GL(V);\ f(xg, yg)=n(g)f(x, y),\ x, y\in V\},$$

where $n(g)\in\boldsymbol{Q}^\times$ is a scalar depending only on g.

We take and fix, once and for all, a maximal order O of B. Then an O-lattice in V is defined to be a $\boldsymbol{Z}$-lattice in V, which is at the same time a left O-module. For an O-lattice L, the two-sided O-ideal generated by the elements $f(x, y)$ for $x, y\in L$ is called the norm of L, and denoted by $N_f(L)$. If L is maximal among the O-lattices having the same norm $N_f(L)$, then it is called a maximal O-lattice. We denote by $\mathcal{L}(O)$ the set of all maximal O-lattices. We put $V_p=V\underset{B}{\otimes}B_p$, $L_p=L\underset{O}{\otimes}O_p$, and denote by f_p the continuous prolongation of f to V_p. Two maximal O-lattices L_1, L_2 are said to belong to the same genus if for every prime p, there exists $g_p\in G_p$ such that $L_{2p}=L_{1p}g_p$. Here $G_p=G(V_p, f_p)$ is defined by replacing $V, f, \boldsymbol{Q}$ by $V_p, f_p, \boldsymbol{Q}_p$ respectively in the above definition of $G(V, f)$.

Two lattices L_1 and L_2 are said to belong to the same class and written $L_1 \cong L_2$, if there exists $g \in G(V, f)$ such that $L_2 = L_1 g$. It is known by Shimura [17] that if $n=1$, $\mathcal{L}(O)$ consists of a single genus, and if $n>1$, the genera in $\mathcal{L}(O)$ are in one to one correspondence with the set of all two-sided O-ideals of the form $q_1^{e_1} \cdots q_s^{e_s}$, where q_i's are the prime O-ideals dividing the discriminant of B, and $e_i=0$ or 1. If $\mathfrak{A}=q_1^{e_1} \cdots q_s^{e_s}$ is as above, the genus in $\mathcal{L}(O)$ corresponding with $\mathfrak{A}$ is the one which contains a maximal O-lattice L with norm $N_f(L)=\mathfrak{A}$, and it is denoted by $\mathcal{L}(O; e_1, \cdots, e_s)$. Especially, $\mathcal{L}(O; 0, \cdots, 0)$ is called the principal genus. We shall write it simply by $\mathcal{L}(O; 0)$. Now it is known that each genus consists of a finite number $H(e_1, \cdots, e_s)$ of classes, which is independent of the choice of O. Moreover, it is known by [17], [18], that if (V, f) is indefinite, we have always $H(e_1, \cdots, e_s)=1$. The purpose of this paper is to give an explicit formula for $H=H(0, \cdots, 0)$ in the case (V, f)=positive definite and $n=2$.

1-2. Throughout the following, we assume that (V, f) is positive definite (a fortiori, B is definite). Then we can assume, by a base change of V over B, that

$$f(x, y)=\sum_{i=1}^{n} x_i \bar{y}_i \quad \text{for } x=(x_1, \cdots, x_n),\ y=(y_1, \cdots, y_n) \in V=B^n,$$

(cf. [17]). Obviously, O^n is then a maximal O-lattice belonging to the principal genus $\mathcal{L}(O; 0)$. The adelized group G_A of $G=G(V, f)$ acts naturally and transitively on $\mathcal{L}(O; 0)$: namely for $L \in \mathcal{L}(O; 0)$ and $g \in G_A$, we put $Lg=\bigcap_p (L_p g_p \cap V)$. Then Lg is again a maximal O-lattice in $\mathcal{L}(O; 0)$. We denote by $\mathfrak{U}$ the stabilizer of O^n in G_A:

$$\mathfrak{U}=\{g \in G_A;\ O^n g=O^n\}$$
$$=G_\infty \times \prod_p U_p, \quad U_p=G_p \cap GL_n(O_p).$$

Then there is a natural bijection induced by $g \to O^n g$:

$$\mathfrak{U} \backslash G_A / G \xrightarrow{\sim} \mathcal{L}(O; 0)/\cong : \text{the set of classes in } \mathcal{L}(O; 0). \tag{1}$$

The class number $H=H(0)$ of $\mathcal{L}(O, 0)$ is expressed as the trace of the Brandt matrix, that is,

$$H=\operatorname{tr} B_\rho(1), \text{ for } \rho=\text{trivial}. \tag{2}$$

The general formula for $\operatorname{tr} B_\rho(m)$ is given in [9], and applying it to our case, we have:

THEOREM A

$$H=\sum_{C(g)} \sum_{L_G(\Lambda)} M_G(\Lambda) \prod_p c_p(g, M_n(O_p), \Lambda_p), \tag{3}$$

where the notations are as follows: put, for each element g of G,

$$Z(g)=\{z\in M_n(B);\ zg=gz\} \text{ and } Z_G(g)=Z(g)\cap G.$$

1) *$C(g)$ runs over the conjugacy classes represented by g, which satisfies the conditions*

(i) $n(g)=1$,

(ii) $C(g)$ is 'locally integral',

$$\text{i.e., } C(g)\cap g_i^{-1}M_n(O_A)g_i\neq\emptyset$$

for some i, where $\{g_i\}$ is a complete set of representatives of $\mathfrak{U}\backslash G_A/G$ and $O_A=B_\infty\times\prod_p O_p$. ((ii) is equivalent to $C_A(g)\cap M_n(O_A)\neq\emptyset$, where $C_A(g)$ is the conjugacy class in G_A represented by g.)

2) *$L_G(\Lambda)$ runs over the 'G-genera' of $\boldsymbol{Z}$-orders in $Z(g)$: the G-genus $L_G(\Lambda)$ containing Λ is the set of all Z-orders in $Z(g)$ which are conjugate in $Z_G(g)_p=Z(g)_p\cap G_p$ with Λ_p, where $Z(g)_p=Z(g)\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_p$: namely*

$$L_G(\Lambda)=\{\Lambda';\ \Lambda'_p=x_p\Lambda_p x_p^{-1} \text{ for some } x_p\in Z_G(g)_p \text{ for all } p\}.$$

3) *$M_G(\Lambda)$ is the 'G-Mass' of the $\boldsymbol{Z}$-order Λ of $Z(g)$, which is defined as follows. We decompose the adelized group $Z_G(g)_A$ of $Z_G(g)$ into disjoint union of double cosets*

$$Z_G(g)_A=\coprod_{k=1}^{h} Z_G(g)y_k(\Lambda_A^\times\cap G_A),\quad \Lambda_A=\Lambda\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_A,$$

and put $\Lambda_k=y_k\Lambda y_k^{-1}=\bigcap_p(y_{kp}\Lambda_p y_{kp}^{-1}\cap Z(g))$. Then we define

$$M_G(\Lambda)=\sum_{k=1}^{h}\frac{1}{[\Lambda_k^\times\cap G:1]}.$$

4) *We denote by $c_p(g,\ M_n(O_p),\ \Lambda_p)$ the number of the optimal embeddings $\varphi: Z(g)_p\hookrightarrow M_n(B_p)$ w.r.t. Λ_p and $M_n(O_p)$, counted up to the equivalence by $Z_G(g)$-conjugations. That is*

$$c_p(g,\ M_n(O_p),\ \Lambda_p)=\#(Z_G(g)_p\backslash M_p(g,\ M_n(O_p),\ \Lambda_p)/U_p),$$

where $U_p=G_p\cap GL_n(O_p)$, and

$$M_p(g,\ M_n(O_p),\ \Lambda_p)=\{x_p\in G_p;\ x_p^{-1}gx_p\in M_n(O_p),\ Z(g)_p\cap x_pM_n(O_p)x_p^{-1}\sim\Lambda_p\}.$$

Here, we write $\Lambda_{1p}\sim\Lambda_{2p}$ to indicate that $\Lambda_{2p}=y_p\Lambda_{1p}y_p^{-1}$ for some $y_p\in Z_G(g)_p$.

§ 2. Classification of conjugacy classes.

In order to evaluate more explicitly the right hand side of the formula in Theorem A, we need to classify the conjugacy classes in G, and pick up those which are 'locally integral' (i.e., $C_A(g)\cap M_n(O_A)\neq\emptyset$). As for the first problem, we follow the method of Hijikata [10] and proceed as follows: First, we see that the conjugacy classes $C(g)$ correspond bijectively with equivalence classes in $Z(g)^*_+/\approx$ of 'positive hermitian elements' of the commutor algebra $Z(g)$ (Lemma 1). Then, we reduce the problem to the case when the algebra $\boldsymbol{Q}[g]$ is a field (Lemma 2). Let $p(x)^q$ be the principal polynomial of g considered as an element of $M_n(B)$, where $p(x)$ is irreducible over $\boldsymbol{Q}$. When q is odd or $\boldsymbol{Q}[g]$ is real, $Z(g)^*_+/\approx$ is easily described (Prop. 1, 2). In the remaining cases, it is parametrized by the isomorphism classes of certain division algebras (Prop. 3). This parametrization has some advantages for our later use. After these case-studies, we summarize them as Theorem 1 and we shall note as Corollary that the Hasse principle holds for conjugacy classes in G. As for the second problem, we shall see that the condition $C_A(g)\cap M_n(O_A)\neq\emptyset$, is not equivalent to "the principal polynomial of g is integral", contrary to the case of $n=1$. In fact, in some cases, there are infinitely many conjugacy classes having the same principal polynomial, whereas the locally integral ones are finite in number. We shall treat this problem in case $n=2$.

2-1. We begin by noting that $M_n(B)$ is a central simple algebra over $\boldsymbol{Q}$ of degree $4n^2$, with an involution $x\to{}^t\bar{x}$, which will be denoted simply by ${}^t\bar{x}=x^*$. We note also that the involution $*$ is positive: namely for all $x\in M_n(B)$, we have $\mathrm{tr}(xx^*)\geqq 0$, and $\mathrm{tr}(xx^*)=0$ if and only if $x=0$. We call an element $z=z^*\in M_n(B)$ positive, $z>0$, if it defines a positive definite quaternion hermitian form in B^n, i.e., $xzx^*\geqq 0$ for all $x\in B^n$, and $xzx^*=0$ only for $x=0$. Then it is well known that, if $z=z^*\in M_n(B)$ is positive, there exists an $x\in GL_n(B)$ such that $xx^*=z$, and vice versa. Therefore the map $x\to xx^*$ induces the bijection

$$GL_n(B)/G \xrightarrow{\sim} Z^*_+/\boldsymbol{Q}^\times_+=\{z\in M_n(B);\ z=z^*>0\}/\boldsymbol{Q}^\times_+. \tag{4}$$

For $g\in G$, put $g'=x^{-1}gx$ with $x\in GL_n(B)$. Let $Z(g)$ be the commutor algebra of g in $M_n(B)$. Then a direct calculation shows that $g'\in G$ if and only if $xx^*\in Z(g)^\times$. We write $Z(g)^*_+=\{z\in Z(g);\ z=z^*>0\}$. we define an equivalence relation $\approx$ in $Z(g)^*_+$ by $z\approx z'\Leftrightarrow z'=yzy^*$ for some $y\in Z(g)^\times$. We also define an equivalence relation $\approx$ (mod. $\boldsymbol{Q}^\times_+$) by $z\approx z'$ (mod. $\boldsymbol{Q}^\times_+)\Leftrightarrow z'=ayzy^*$ for some $a\in\boldsymbol{Q}^\times_+$ and $y\in Z(g)^\times$. Then we have

LEMMA 1. *The map $x^{-1}gx\to xx^*$ induces a bijection*

$$\{g' \in G\,;\ g' \underset{GL_n(B)}{\sim} g\}/\underset{G}{\sim} \longrightarrow Z(g)^*_+/\approx (\mathrm{mod.}\ \boldsymbol{Q}^\times_+)\,, \tag{5}$$

where $\underset{G}{\sim}$ *means the equivalence by G-conjugation.*

PROOF. Injectivity is clear. Surjectivity follows form the bijection (4). q. e. d.

Since $G^1=\{g\in G\,;\ n(g)=1\}$ is contained in the compact group $G^1_\infty \cong US_p(n)$, every element of G is semi-simple. Therefore the algebra $\boldsymbol{Q}[g]$ generated by $g\in G$ over $\boldsymbol{Q}$ decomposes into a direct sum of fields:

$$\boldsymbol{Q}[g]=\bigoplus_{i=1}^{m} F_i\,. \tag{6}$$

LEMMA 2. *In the decomposition* (6), *each* F_i *is stable under* *. *Moreover, there is an* $x\in G$ *such that*

$$x^{-1}gx=\begin{bmatrix} g_1 & & 0 \\ & \ddots & \\ 0 & & g_m \end{bmatrix},\quad g_i\in M_{n_i}(B)\,,\quad g_i g_i^*=n(g)1_{n_i}\,.$$

PROOF. By $g^*=n(g)g^{-1}$, $\boldsymbol{Q}[g]$ is stable under *. If F_i were not stable, $F_i^*=F_j$ for some $j\neq i$, and * induces the permutation of the components on $F_i\oplus F_j$. Then we have, for $x=(1,\,0)\in F_i\oplus F_j$, $\mathrm{tr}(xx^*)=\mathrm{tr}(0,\,0)=0$, a contradiction. Therefore, each F_i is *-stable. Now we write $1=e_1+\cdots+e_m$, $e_i\in F_i$. Then e_i's form a set of orthogonal idempotents, and $e_i^*=e_i$. It is well known that there exists an $x\in GL_n(B)$ such that $x^{-1}e_ix=\delta_i$, $i=1,\cdots,m$, where

$$\delta_i=\begin{bmatrix} 0 & & & \\ & 1_{n_i} & & \\ & & 0 & \\ & & & \ddots \end{bmatrix}$$

By $e_i^*=e_i$, we have $\delta_i=(x^*x)\delta_i(x^*x)^{-1}$, so x^*x is of the form

$$x^*x=\begin{bmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_m \end{bmatrix},\quad x_i\in M_{n_i}(B)\,,\quad x_i=x_i^*>0\,.$$

There exists $y=\begin{bmatrix} y_1 & & 0 \\ & \ddots & \\ 0 & & y_m \end{bmatrix}\in GL_n(B)$, such that $y^*(x^*x)y=1_n$, i.e., $xy\in G$. Then we see that $(xy)^{-1}e_i(xy)=\delta_i$ for $i=1,\cdots,m$. It is now easy to see that $(xy)^{-1}g(xy)$ is of the required form. q. e. d.

According to Lemma 2, $Z(g)$ splits as:

$$Z(g)=\bigoplus_{i=1}^{m} Z_i(g)\,, \tag{7}$$

where $xZ_i(g)x^{-1}$ is the commutor algebra of g_i in $M_{n_i}(B)$. Then we have a bijection

$$Z(g)_+^*/\approx(\text{mod. } \boldsymbol{Q}_+^\times) \xrightarrow{\sim} \left(\bigoplus_{i=1}^{m} Z_i(g)_+^*/\approx\right)(\text{mod. } \boldsymbol{Q}_+^\times)\,. \tag{8}$$

Thus we can say that the problem to classify the conjugacy classes in (5) is reduced to the case where $m=1$, i.e., $F=\boldsymbol{Q}[g]$ is a field. In this case, the principal polynomial $f(x)$ has the form $f(x)=p(x)^q$, where $p(x)$ is irreducible over $\boldsymbol{Q}$ and $\boldsymbol{Q}[x]/(p(x))=F$. Call p the degree of $p(x)$. Then we see that $Z(g)$ is a simple algebra of degree pq^2 over $\boldsymbol{Q}$ with center F. As noted above, $Z(g)$ has the involution which is positive. Therefore F is either (a) totally real, or (b) a totally imaginary quadratic extension of a totally real field F_0.

2-2. First we consider the case (a).

PROPOSITION 1. *Assume that $F=\boldsymbol{Q}[g]$ is totally real. Then we have either*

(i) *$F=\boldsymbol{Q}$, and $Z(g)=M_n(B)$, $Z_G(g)=G$, or*

(ii) *F is real quadratic, $n=2n_0$ (even), and*

$$Z(g)\cong M_{n_0}(B_F)\,,\quad B_F=B\underset{\boldsymbol{Q}}{\otimes}F\,,$$

$$Z_G(g)\cong\{z\in M_{n_0}(B_F)\,;\ z^t\bar{z}=\text{scalar in } \boldsymbol{Q}^\times\}\,.$$

In both cases, the number of G-conjugacy classes in (5) *is one.*

PROOF. Note that $F=F_0=\{z\in F\,;\ z^*=z\}$ in this case. If $g\in Z(G)=$center of G, it belongs to the case (i). If not, since $g^2=gg^*=n(g)\in\boldsymbol{Q}_+^\times$, F is real quadratic. In this case, we see that $Z(g)\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{R}$ is a direct sum of two copies of a simple algebra over $\boldsymbol{R}$ of degree n^2, since $F\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{R}=\boldsymbol{R}\oplus\boldsymbol{R}$. Therefore, it is isomorphic to either $M_n(\boldsymbol{R})\oplus M_n(\boldsymbol{R})$, or $M_{n/2}(\boldsymbol{H})\oplus M_{n/2}(\boldsymbol{H})$, where $\boldsymbol{H}$ is the Hamilton quaternion algebra over $\boldsymbol{R}$. On the other hand, we have $M_n(B)\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{R}=M_n(\boldsymbol{H})$, and $Z(g)\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{R}$ is contained in it. It follows that $Z(g)\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{R}=M_{n_0}(\boldsymbol{H})\oplus M_{n_0}(\boldsymbol{H})$, $n_0=n/2$. Now we can take an element $g_0\in G(2)=\{h\in M_2(B)\,;\ hh^*=n(h)1_2,\ n(h)\in\boldsymbol{Q}^\times\}$, and put

$$g=\begin{bmatrix} g_0 & & \\ & \ddots & \\ & & g_0 \end{bmatrix}\ \begin{matrix}\uparrow\\ n_0\,.\\ \downarrow\end{matrix}$$

The commutor algebra of g_0 in $M_2(B)$ is easily seen to be isomorphic to $B\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{Q}[g_0]$

$=B\cdot\boldsymbol{Q}[g_0]$. Therefore $Z(g)\cong M_{n_0}(B\underset{\boldsymbol{Q}}{\otimes}Q[g])\cong M_{n_0}(B_F)$, and we see that this isomorphism keeps the involution *. So we have $Z_G(g)=\{z\in M_{n_0}(B_F)\,;\ zz^*=\text{scalar in } \boldsymbol{Q}^\times\}$. Finally, if we note that the bijection (4) is valid for B_F/F, we can conclude that the right hand side of (5) consists of a single class. So we get the last assertion. q. e. d.

Now we consider the case (b), where $F_0=\{x\in F\,;\ x^*=x\}$ is totally real and F is a totally imaginary quadratic extension of F_0. Obviously $p=[F:\boldsymbol{Q}]=2p_0$ is even and $pq=2n$, $p_0q=n$.

PROPOSITION 2. *Assume that F is totally imaginary and q: odd. Then*

(i) $B\underset{\boldsymbol{Q}}{\otimes}F\cong M_2(F)$, *i.e., F splits B.*

(ii) *There is an isomorphism $\phi: Z(g)\xrightarrow{\sim}M_q(F)$ and $y\in GL_q(F)$, such that $y=y^*>o$, $\phi(z^*)=y\phi(z)^*y^{-1}$ for all $z\in Z(g)$. Here, we mean by $y>0$ that $y^\sigma\in M_q(\boldsymbol{C})$ are positive definite for any embedding $\sigma: F\hookrightarrow\boldsymbol{C}$.*
Therefore

$$Z_G(g)\cong\{x\in M_q(F)\,;\ xyx^*=n(x)y,\ n(x)\in\boldsymbol{Q}^\times\}.$$

(iii) *The map $z\to\phi(z)y\to\det(\phi(z)y)$ induces the bijections*

$$Z(g)^*_+/\approx\ (\text{mod. } \boldsymbol{Q}^\times_+)\xrightarrow{\sim}M_q(F)^*_+/\approx\ (\text{mod. } \boldsymbol{Q}^\times_+)$$
$$\xrightarrow{\sim}F^\times_{0+}/(\boldsymbol{Q}^\times_+N_{F/F_0}(F^\times)).$$

PROOF. By embedding F_0 in $M_{p_0}(\boldsymbol{Q})$, and $M_{p_0}(B)$ in $M_q(M_{p_0}(B))=M_n(B)$ diagonally, we see that the commutor algebra $Z(F_0)$ of F_0 in $M_n(B)$ is isomorphic to $M_q(B_{F_0})$, where $B_{F_0}=B\underset{\boldsymbol{Q}}{\otimes}F_0$. Since $Z(g)$ is contained in $Z(F_0)$, we have an injection over F_0:

$$Z(g)\hookrightarrow M_q(B_{F_0}).$$

On the other hand, since $F\underset{F_0}{\otimes}F=F\oplus F$, we have an injection

$$Z(g)\underset{F_0}{\otimes}F\cong Z(g)\oplus Z(g)'\hookrightarrow M_q(B_{F_0})\underset{F_0}{\otimes}F\cong M_q(B_F).$$

It follows that $B_F=M_2(F)$ if $q=$odd, since $Z(g)$ and $Z(g)'$ are simple algebras over F of degree q^2. In this case, we can assume, by taking some inner automorphism if necessary, that the above inclusion is

$$Z(g)\oplus Z(g)'=\begin{bmatrix}Z(g) & 0\\ 0 & Z(g)'\end{bmatrix}\hookrightarrow M_2(M_q(F))=M_{2q}(F).$$

In particular, $Z(g)\hookrightarrow M_q(F)$, and, by compairing the degree over F, it follows that $Z(g)\cong M_q(F)$. Now it is well known, and easy to show, that any positive involu-

tion of $M_q(F)$ which induces on F the conjugation over F_0 can be written as $z\to y^{-1}z^*y$ for some $y=y^*>o$, $y\in GL_q(F)$. (ii) follows from this. Finally it is also well known, that the equivalence class of hermitian matrices in $M_q(F)$ over F_0 is determined by the determinant up to the factor $N_{F/F_0}(F^\times)$. (iii) follows from this and Lemma 1. q. e. d.

2-3. Now we assume that F is totally imaginary and $q=2q_0=$even. As in the proof of Prop. 2, we take a field K_0 in $M_{p_0}(\boldsymbol{Q})$ which is isomorphic to F_0, and take an element

$$h\in M_2(K_0)\subset M_2(M_{p_0}(\boldsymbol{Q}))\subset M_{q_0}(M_2(M_{p_0}(\boldsymbol{Q})))=M_n(\boldsymbol{Q})$$

such that $g=x^{-1}hx$ for some $x\in M_n(B)$, where the last inclusion is diagonal. Then we have $K=K_0(h)\cong\boldsymbol{Q}(g)$.

LEMMA 3. (i) *There exists* $w_0\in GL_{p_0}(\boldsymbol{Q})$ *such that* $w_0={}^tw_0>0$, *and* ${}^tx=w_0xw_0^{-1}$ *for all* $x\in K_0$.
(ii) *There exists* $w\in GL_n(\boldsymbol{Q})$ *such that* $w={}^tw>o$, *and* ${}^ty=w({}^\sigma y)w^{-1}$ *for all* $y\in K=K_0(h)$, *where* σ *denotes the conjugation of* K *over* K_0.

PROOF. (i) Take a basis $v_1,\cdots v_k$ $(k=p_0)$ of K_0 regarded as a linear space over $\boldsymbol{Q}$, and write $xv_j=\sum_{i=1}^{k}v_iz_{ij}$, $z_{ij}\in\boldsymbol{Q}$. If we denote by $\sigma_1,\cdots,\sigma_k$ the set of all isomorphisms of K_0 into $\boldsymbol{R}$, we get

$$\begin{bmatrix}\sigma_1(x) & & 0\\ & \ddots & \\ 0 & & \sigma_k(x)\end{bmatrix}A=AZ,\quad A=(\sigma_i(v_j)),\quad Z=(z_{ij}).$$

Then we have

$${}^t\begin{bmatrix}\sigma_1(x) & & 0\\ & \ddots & \\ 0 & & \sigma_k(x)\end{bmatrix}=\begin{bmatrix}\sigma_1(x) & & 0\\ & \ddots & \\ 0 & & \sigma_k(x)\end{bmatrix}={}^tA^{-1}\,{}^tZ\,{}^tA=AZA^{-1},$$

$${}^tZ=({}^tAA)Z({}^tAA)^{-1}.$$

Since $x\to Z$ defines an isomorphism of K_0 into $M_k(\boldsymbol{Q})=M_{p_0}(\boldsymbol{Q})$, we can identify them and take $w_0={}^tAA$. It is easy to see that $w_0\in M_k(\boldsymbol{Q})$, and $w_0={}^tw_0>0$. (ii) We may assume that h is of the form

$$h=\begin{pmatrix}0 & 1\\ -b & -a\end{pmatrix},\quad a,\ b\in K_0.$$

Then we take $w=\begin{pmatrix}w_0 & 0\\ 0 & w_0\end{pmatrix}\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}$, and see that it satisfies the required conditions. q. e. d.

We fix h and w as in the above proof, till the end of 2-3. We note that $b=N_{K/K_0}(h)=n(g)\in \boldsymbol{Q}_+^\times$.

First we shall show that the problem reduces to the case $q_0=1$. By a direct calculation, we see that $g=x^{-1}hx\in G\Leftrightarrow xx^*w\in Z(h)=M_{q_0}(B_K)$, where $B_K=B_{K_0}\underset{K_0}{\otimes}K$ $=B\cdot K$. We extend σ to an automorphism of $Z(h)$ over K_0 in such a way that it induces the identity on B_{K_0}, and denote it again by σ. Then ${}^\sigma z=w^{-1}({}^t z)w$ for all $z\in Z(h)$, where we put ${}^t z=({}^t z_{ij})$ for $z=(z_{ij})$, $z_{ij}\in M_p(B)$.

LEMMA 4. (i) *By the isomorphism* $\phi: Z(g)\ni z\to xzx^{-1}\in Z(h)=M_{q_0}(B_K)$, *the involution* $*$ *of* $Z(g)$ *corresponds with the involution* $\mathrm{Int}(v^{-1})\cdot\sigma\cdot *$ *of* $M_{q_0}(B_K)$; *namely*

$$\phi(z^*)=v^\sigma(\phi(z)^*)v^{-1} \quad \text{for } z\in Z(g),$$

where in the right hand side, $v=xx^*w$ *and* $*$ *denotes the involution* $\phi(z)^*={}^t\overline{\phi(z)}$ *as a matrix in* $M_{q_0}(B_K)$, *where* $-$ *is the canonical involution of* B_K *over* K.
(ii) ${}^\sigma v^*=v$, *where* $*$ *is* ${}^t-$ *of* $M_{q_0}(B_K)$.

PROOF. (i) is a direct consequence of the above remark. As for (ii), we note that $(x^{-1}vx)^*=x^{-1}vx$. Then by (i), $v^\sigma v^* v^{-1}=v$, so ${}^\sigma v^*=v$. q. e. d.

For simplility, we write ${}^\sigma y^*=y^{\circledast}$ for $y\in M_{q_0}(B_K)$. Note that it is an involution of $M_{q_0}(B_K)$ of the second kind. Now put

$$M_{q_0}(B_K)_+^{\circledast}=\{v\in M_{q_0}(B_K);\ v^{\circledast}=v,\ v>0\},$$

where $v>0$ means that the reduced trace of $zvz^{\circledast}$ (over K) is totally positive for all $z\in M_{q_0}(B_K)$, $z\neq 0$. If $q_0=1$, $v>0$ is equivalent to $\mathrm{Tr}(v)>0$ and $N(v)>0$. We define an equivalence relation $\approx(\mathrm{mod.}\ \boldsymbol{Q}_+^\times)$ in $M_{q_0}(B_K)_+^{\circledast}$: $v\approx v'\ (\mathrm{mod.}\ \boldsymbol{Q}_+^\times)\Leftrightarrow v'=axvx^{\circledast}$ for some $a\in\boldsymbol{Q}_+^\times$ and $x\in GL_{q_0}(B_K)$. Then, we get a bijection induced from the map $x^{-1}hx\to xx^*w$:

$$\{g\in G;\ g\underset{GL_n(B)}{\sim}h\}/\underset{G}{\sim}\ \xrightarrow{\sim}\ M_{q_0}(B_K)_+^{\circledast}/\approx\ (\mathrm{mod.}\ \boldsymbol{Q}_+^\times). \tag{9}$$

In fact, injectivity is clear. Surjectivity can be proved by next Lemma 5 and the last part of the proof of Lemma 7.

LEMMA 5. *The reduced norm of* $M_{q_0}(B_K)$ *over* K *induces the following bijection*:

$$M_{q_0}(B_K)_+^{\circledast}/\approx\ (\mathrm{mod.}\ \boldsymbol{Q}_+^\times)\ \xrightarrow{\sim}\ K_{0+}^\times/N_{K/K_0}(K^\times). \tag{10}$$

PROOF. Although this is known by W. Landherr [13], Ramanathan [14], we give here an outline of the proof for the convenience of the readers. First note that, if $v_2\approx v_1$ for two $^{\circledast}$-hermitian matrices, then $v_2=xv_1x^{\circledast}$ for some $x\in GL_{q_0}(B_K)$,

so that the reduced norm of v_2 is $N(v_2)=N(x)N(v_1)N(x^{\circledast})=N_{K/K_0}(N(x))N(v_1)$. So the map is well defined. Note also that any $^{\circledast}$-hermition matrix is equivalent to a diagonal matrix. Therefore we may assume that $v=v^{\circledast}$ is of the form

$$v=\begin{pmatrix} v_1 & & 0 \\ & \ddots & \\ 0 & & v_{q_0} \end{pmatrix}.$$

Put $u=(v+{}^{\sigma}v)/2$, $w=(v-{}^{\sigma}v)/2\sqrt{m}$, where m is a totally negative element of K_0 such that $K=K_0(\sqrt{m})$. Then we see that $v=u+\sqrt{m}w$, $u\in M_{q_0}(B_{K_0})$ and $w\in M_{q_0}(B_{K_0})$ is a quaternion skew hermitian matrix with respect to the canonical involution of B_{K_0}. If we write $x_i\in B_K$ as $x_i=y_i+\sqrt{m}z_i$, y_i, $z_i\in B_{K_0}$, we have

$$f_v(x)=xvx^{\circledast}=f_1(y,\ z)+\sqrt{m}f_2(y,\ z)\,;$$

$$f_1(y,\ z)\in K_{0+}\,,\quad f_2(z,\ y)=-f_2(y,\ z)\,,$$

where $f_2(y,\ z)$ is a quaternion skew hermitian form of rank $2q_0$ corresponding with the matrix

$$\begin{pmatrix} w & -u \\ u & -mw \end{pmatrix}.$$

Now it is known that any quaternion skew hermitian form of rank 4 represents 0 non-trivially (cf. [13]). Therefore, if $q_0>1$, there exists $x=(x_i)\in B_K^{q_0}$, $x\neq 0$ such that $f_2(y,\ z)=0$, $y=(y_i)$, $z=(z_i)$. By taking an orthogonal basis containing this x, we see that v is equivalent to

$$v\approx\begin{pmatrix} a & & 0 \\ & v_2' & * \\ 0 & \ddots & \\ & * & v_{q_0}' \end{pmatrix}\approx\begin{pmatrix} 1 & & 0 \\ & v_2' & * \\ 0 & \ddots & \\ & * & v_{q_0}' \end{pmatrix}$$

By continuing this process, we see that any $v\in M_{q_0}(B_K)_{+}^{\circledast}$ is equivalent to a matrix of the form

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & v_0 \end{pmatrix},\qquad {}^{\sigma}\bar{v}_0=v_0\in B_K\,.$$

Now it suffices to prove the case $q_0=1$. In this case, the space V consisting of all $^{\circledast}$-hermitian elements in B_K can be regarded as a quadratic space over K_0, by the restriction of the reduced norm of B_K. Since the even Clifford algebra of V is B_K, the proper similitude of V is given by $v\to axv^{\sigma}\bar{x}$ for $a\in K_0^{\times}$, $x\in B_K^{\times}$. The injectivity of the map in our lemma follows from this fact and the Witt theorem. Since $\dim_{K_0}V=4$, surjectivity is clear. q. e. d.

We assume that $q_0=1$, so that $Z(h)=B_K$.

LEMMA 6. *Let $v_i\in B_K^\times$, $i=1, 2$, be $\circledast$-hermitian elements. Then*
(i) *$\tau_i=\mathrm{Int}(v_i^{-1})\cdot\sigma$ is an automorphism of B_K over K_0 of order 2. The fixed subalgebra of τ_i:*

$$Z_\sigma(v_i)=\{z\in B_K\,;\ v_i{}^\sigma z v_i^{-1}=z\} \tag{11}$$

is a quaternion algebra over K_0. Conversely, any quaternion subalgebra of B_K over K_0 is associated with a $\circledast$-hermitian element of B_K in this way.
(ii) *$Z_\sigma(v_1)\cong Z_\sigma(v_2)\Leftrightarrow v_1\approx v_2$ (mod. $K_0^\times$).*

We omit the proof of this lemma, since it is easy and found in [8].

LEMMA 7. *Let $g=x^{-1}hx\in G$, $v=xx^*w\in Z(h)$ be as above. Then the quaternion algebra $Z_\sigma(v)$ defined by* (11) *is totally definite. Conversely, for any totally definite quaternion algebra Z over K_0 contained in $Z(h)$, there exists $x\in GL_n(B)$ such that $x^{-1}hx\in G$, and $Z_\sigma(v)=Z$ for $v=xx^*w$.*

PROOF. Obviously, $-$ induces the canonical involution of $Z_\sigma(v)$, and $N(z)=z\bar{z}\in K_0^\times$ for all $z\in Z_\sigma(v)$. On the other hand, we have, for any $w\in K_0^\times$, $w^2N(z)=\phi(yy^*)$, $y=\phi^{-1}(wz)$ by Lemma 4. Then, there exists a positive constant c such that $\mathrm{Tr}_{K_0/Q}(w^2N(z))=c\,\mathrm{Tr}(yy^*)$. So $N(z)$ is a positive element of K_0, that is, $N(z)$ is totally positive, which proves that $Z_\sigma(v)$ is totally definite. Conversely, let Z be any such one in $Z(h)$. By Lemma 6, we can find $v\in Z(h)^\times$ such that $v={}^\sigma\bar{v}$, $Z=Z_\sigma(v)$. Here we note that, in the correspondence of Lemma 6,

$$Z_\sigma(v)=\text{totally definite}\Leftrightarrow N(v)=\text{totally positive},$$

which is easily proved (cf. [8]). We can choose $a\in K_0^\times$ so that the reduced trace $\mathrm{Tr}(av)$ over K is a totally positive element of K_0. So we can assume that v is a positive $\circledast$-hermitian element. If we put $z=vw^{-1}$, then the remark preceeding Lemma 4 shows that $z=z^*$. We shall show that $z>0$. By the following Lemma 8, we can find $x_1\in GL_2(B_{K_0})$ such that $x_1{}^t\bar{x}_1\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}=v$. Then, by Lemma 3 (i), we have $z=vw^{-1}=x_1w_1^{-1}x_1^*$, where $w=w_1\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}$, $w_1=\begin{pmatrix}w_0 & 0\\ 0 & w_0\end{pmatrix}$, since ${}^t\bar{x}_1=w_1^{-1}x_1^*w_1$. Again by Lemma 3 (i), we have w_1, $w_1^{-1}>0$, and so $z>0$. Then there exists $x\in GL_n(B)$ such that $xx^*=z$, so $v=xx^*w$ and $x^{-1}hx\in G$.

LEMMA 8. *For any positive $\circledast$-hermitian element v in $Z(h)$, there exists $x_1\in GL_2(B_{K_0})$ such that $v=x_1^t\bar{x}_1\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}$, where $\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}$ is as in the proof of Lemma* 3.

PROOF. Put $N(v)=d\in K_{0+}^{\times}$. First, we show that there exists $x\in GL_2(B_{K_0})$ such that $N\left(x^t\bar{x}\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}\right)\in dN_{K/K_0}(K^{\times})$. If we let s vary over $B_{K_0}^0=\{s\in B_{K_0};\ \mathrm{Tr}_{B_{K_0}/K_0}(s)=0\}$, and t over K_0, we get a totally indefinite quadratic form $N(s,t)=N(s')-bN(s)=((a^2-4b)N(s)+N(t))/4$ of four variables over K_0, where we put $s'=(as+t)/2$. Then the equation $N(s,t)=n$ has a solution. Replacing s, t, d, by us, ut, u^2d ($u\in K_0^{\times}$) if necessary, we can assume that t is totally positive and $N(s,t)\in dN_{K/K_0}(K^{\times})$. Then we define $c\in K_{0+}^{\times}$, $\varepsilon\in B_{K_0}$ by

$$2bc+a\varepsilon=s'$$

$$ac+2\varepsilon=s,$$

and see that $\varepsilon+\bar{\varepsilon}=-ac$. Then we can find $\delta\in B_{K_0}^{\times}$ such that $N(\delta)=bc$, and see that $c-N(\beta)=(bc^2-N(\varepsilon))/bc>0$, where $\beta=\varepsilon\bar{\delta}^{-1}$. So we can find $\alpha\in B_{K_0}$ such that $N(\alpha)=c-N(\beta)$. Now put $x=\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix}$, then we have

$$v_0=x^t\bar{x}\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}=\begin{pmatrix}2bc+a\varepsilon & ac+2\varepsilon\\ b(ac+2\bar{\varepsilon}) & 2bc+a\bar{\varepsilon}\end{pmatrix}$$

$$=\begin{pmatrix}s' & s\\ b\bar{s} & \bar{s}'\end{pmatrix}\in Z(h),$$

$$N(v_0)=N(2bc+a\varepsilon)-bN(ac+2\varepsilon)=N(s')-bN(s)\in dN_{K/K_0}(K^{\times}),$$

and $v_0^{\circledast}=v_0$. By virtue of Lemma 5, there exists $y\in B_K^{\times}$ such that $yv_0y^{\circledast}=v$. Then, it is easy to show that $v=yv_0y^{\circledast}=yx^t\bar{x}^t\bar{y}w=x_1^t\bar{x}_1w$, $x_1=yx$. q. e. d.

We shall write, for $g=x^{-1}hx\in G$ and $v=xx^*w$,

$$Z_0(g)=\phi^{-1}(Z_\sigma(v)). \tag{12}$$

This $Z_0(g)$ does not depend on the choice of x.

PROPOSITION 3. *Assume that F is totally imaginary and q: even. Then there is a canonical bijection induced by $C(g)\to Z_\sigma(v)$:*

$$\{g\in G;\ g\underset{GL_n(B)}{\sim}h\}/\underset{G}{\sim}\ \xrightarrow{\sim}\left\{\begin{array}{l}\textit{isomorphism classes of totally}\\ \textit{definite quaternion algebras}\\ \textit{over } K_0 \textit{ contained in } Z(h)=B_K\end{array}\right\}$$

and we have

$$Z_G(g)=\{z\in M_{q_0}(B_K);\ zvz^{\circledast}=n(z)v,\ n(z)\in \boldsymbol{Q}_+^{\times}\}.$$

In particular, when $q=2$ and $F_0=\boldsymbol{Q}$,

$$Z_G(g)=F^\times\cdot Z_0(g)^\times=\{ab\in Z(g);\ a\in F^\times,\ b\in Z_0(g)^\times\}.$$

PROOF. The first two assertions follow from Lemma 5, 6, 7. To prove the last one, we first note that, by Lemma 4 (i), the canonical involution of the quaternion algebra $Z(g)/F$ is written as $z\to z'=v_0{}^\sigma(z^*)v_0^{-1}$, where we put $v_0=x^{-1}vx$, and we carry σ to an automorphism of $Z(g)$ over F_0 by ϕ. Then it is easy to show that $z^*=z'\Leftrightarrow z\in Z_0(g)$. So the right hand side of the above equality is contained in $Z_G(g)$. Conversely, let z be any element of $Z_G(g)$. Then, since $zz^*=n(z)\in\boldsymbol{Q}^\times\subset F^\times$, we have $z^*=cz'$ for some $c\in F^\times$. By using Lemma 3 and 4, we can prove ${}^\sigma z=cv_0^{-1}zv_0$, so that $z={}^\sigma({}^\sigma z)=N_{F/F_0}(c)(v_0{}^\sigma v_0)^{-1}z(v_0{}^\sigma v_0)=N_{F/F_0}(c)z$ and $N_{F/F_0}(c)=1$. By Hilbert's theorem 90, there exists $d\in F^\times$ such that $c=d^\sigma d^{-1}$. It follows $v_0{}^\sigma(dz)=(dz)v_0$, so that $dz\in Z_\sigma(v_0)=Z_0(g)$, $z\in F^\times\cdot Z_0(g)^\times$. q. e. d.

COROLLARY. *The following map induced by the inclusion map of G into G_A is injective*:

$$\{g\in G;\ g_{\widetilde{GL_n(B)}}h\}/_{\widetilde{G}}\longrightarrow\{g\in G_A;\ g_{\widetilde{GL_n(B_A)}}h\}/_{\widetilde{G_A}} \tag{13}$$

and the image is the set of all $(g_p)_p\in G_A$ such that the number of $\mathfrak{p}$'s for which $Z_0(g_p)_\mathfrak{p}$=division is congruent to $[F_0:\boldsymbol{Q}]$ mod. 2, where we put $Z_0(g_p)_p=\bigoplus_{\mathfrak{p}|p}Z_0(g_p)_\mathfrak{p}$ ($\mathfrak{p}$ is a prime ideal of F_0).

2-4. Now we summarize the above results on classification of conjugacy class in G. We also give the condition for a polynomial to be the principal polynomial of some element of G.

REMARK 1. Let $f(x)$ be a polynomial of degree $2n$ which decomposes to the product of irreducible factors over $\boldsymbol{Q}$: $f(x)=\prod_{i=1}^{m}p_i(x)^{q_i}$. Then, by virtue of Lemma 2, $f(x)$ is the principal polynomial of some element of G if and only if $p_i(x)^{q_i}$ is the principal polynomial of some element of $G(n_i)$ for all i and whose similitudes are the same, where $2n_i=p_iq_i$, $p_i=\deg(p_i(x))$. We also note that $GL_n(B)$-conjugacy class of an element g of $M_n(B)$ depends only on the principal polynomial of g.

THEOREM 1. *Let $f(x)=p(x)^q$ be a monic polynomial of degree $2n$, where $p(x)$ is an irreducible polynomial over $\boldsymbol{Q}$. Then, a necessary and sufficient condition for $f(x)$ to be the principal polynomial of some element of G is*:

(i) *$p(x)$ is linear, or*

(ii) *$p(x)=x^2-c$, $c\in\boldsymbol{Q}_+^\times$, and n is even, or*

(iii) *$\boldsymbol{Q}[x]/(p(x))$ is a totally imaginary quadratic extension F of a totally real field F_0, and $p(x)$ is of the form $\prod_\sigma(x^2+{}^\sigma ax+c)$, where $c\in\boldsymbol{Q}_+^\times$, $a\in F_0$, and σ runs through all embeddings of F_0 into $\boldsymbol{R}$, and besides, F splits B if q is odd.*

In the case (i), (ii), *the elements of* G *whose principal polynomials are* $f(x)$ *form a single* G*-conjugacy class (Prop.* 1). *In the case* (iii), *the* G*-conjugacy classes in the* $GL_n(B)$*-conjugacy class whose principal polynomial is* $f(x)$ *are classified by Prop.* 2 (iii), *or Prop.* 3, *for* q*=odd or even, respectively. By virtue of* (8) *and Remark* 1, *the case when* $f(x)=\prod_{i=1}^{m} p(x)^{q_i}$, *or* $\boldsymbol{Q}[g]$ *is not a field, reduces to the above cases.*

Next Corollary seems to be generally known by [10]:

COROLLARY. *The Hasse principle holds for conjugacy classes in* G: *namely the map in* (13) *is injective for each* $h \in G$.

PROOF. In the case (iii), q: even, this has been already shown in Corollary to Prop. 3. In the other cases, this is easily shown by virtue of Prop. 1, 2.

2-5. Now we consider the second problem to characterize the "locally integral" conjugacy classes in G, namely the ones that satisfy $C_A(g) \cap M_n(O_A) \neq \emptyset$. Since this problem seems difficult in general, we shall restrict ourselves to the case $n=2$. By what we have seen, there are 7 cases to be distinguished, according to the decomposition (6) of $\boldsymbol{Q}[g]$: namely we have

(14)
- (I) $\boldsymbol{Q}[g]=\boldsymbol{Q}$, $Z(g)=M_2(B)$,
- (II) $\boldsymbol{Q}[g]=\boldsymbol{Q}\oplus\boldsymbol{Q}$, $Z(g)=B\oplus B$,
- (III) $\boldsymbol{Q}[g]=\boldsymbol{Q}\oplus F$, $Z(g)=B\oplus F$, F=imaginary quadratic field contained in B,
- (IV) $\boldsymbol{Q}[g]=F$=imaginary quadratic, $Z(g)=B_F$,
- (V) $\boldsymbol{Q}[g]=F_1\oplus F_2=Z(g)$, F_i=imaginary quadratic field contained in B,
- (VI) $\boldsymbol{Q}[g]=F=Z(g)$=totally imaginary quadratic extension of a real quadratic field F_0,
- (VII) $\boldsymbol{Q}[g]=F$=real quadratic, $Z(g)=B_F$.

In the cases (I), (II), (III), and (VII), the conjugacy class $C(g)$ depends only on the principal polynomial $f(x)$ of g, so it is always locally integral as long as $f(x)$ is integral. Other cases will be explained below.

First we consider the case (IV). By Prop. 3, if we fix the principal polynomial $f(x)=(x^2+ax+b)^2$, $C(g)$ correspond bijectively with definite quaternion algebras $Z_0(g)$ contained in B_F.

PROPOSITION 4. *Let* $g \in G$ *belong to the case* (IV). *Assume that* $f(x)$ *is integral. Then we have an equivalence*

$$C(g)=\textit{locally integral} \Leftrightarrow D(Z_0(g)) \mid D(\boldsymbol{Z}[g])D(B),$$

where we denote by $D(\boldsymbol{Z}[g])$, $D(Z_0(g))$, $D(F)$, $D(B)$ *the discriminant of* $\boldsymbol{Z}[g]$,

$Z_0(g)$, F, B, *respectively.*

PROOF. We use the notations of 2-3. We may assume that h is of the form

$$h=\begin{pmatrix}0 & 1\\ -b & -a\end{pmatrix}\in M_2(\boldsymbol{Z}),\quad \text{and}\quad w=\begin{pmatrix}2b & a\\ a & 2\end{pmatrix}.$$

Let p be a prime such that $p\mid D(Z_0(g))$, $p\nmid D(F)D(B)$, and assume that $\boldsymbol{Z}_p[g]$ is maximal in F_p. Then $K_p\cong F_p$ is the unramified quadratic extension of $\boldsymbol{Q}_p$, and $B_p=M_2(\boldsymbol{Q}_p)$. We can assume: $O_p=M_2(\boldsymbol{Z}_p)$. Take any $x\in GL_2(B_p)$ such that $g=x^{-1}hx\in G_p\cap M_2(O_p)$. By multiplying an element of $Z(h)_p^\times$ from the left, we can assume that x is of the form $x=\begin{pmatrix}\alpha & \beta\\ 0 & 1\end{pmatrix}u$, $\alpha=\begin{pmatrix}p^m & 0\\ 0 & p^n\end{pmatrix}\in B_p^\times$, $m\geqq n$, $u\in GL_2(O_p)$. Then it is not difficult to see that $p\mid D(Z_0(g))$ is equivalent to $N(\alpha)=p^{n+m}\notin N_{K_p/\boldsymbol{Q}_p}(K_p^\times)$, i.e., $n+m=$odd. We have

$$\begin{pmatrix}\alpha & \beta\\ 0 & 1\end{pmatrix}^{-1}h\begin{pmatrix}\alpha & \beta\\ 0 & 1\end{pmatrix}=\begin{pmatrix}\alpha^{-1}(b\beta)\alpha & \alpha^{-1}(b\beta^2+a\beta+1)\\ -b\alpha & -(a+b\beta)\end{pmatrix}\in M_2(O_p).$$

Then we can write $b\beta=\begin{pmatrix}X & Y\\ Z & W\end{pmatrix}\in O_p=M_2(Z_p)$, and see that $\alpha^{-1}(b\beta)\alpha\in O_p$ implies $Y\equiv 0\ (\mathrm{mod}.\ p^{m-n})$. On the other hand, from $(b\beta)^2+a(b\beta)+b\in b\alpha O_p$, we see that $X^2+aX+b\in bp^m\boldsymbol{Z}_p$. But $b\alpha\in O_p$, so bp^n, $bp^m\in\boldsymbol{Z}_p$, and $bp^m\in p\boldsymbol{Z}_p$ because $m-n=$odd>0. So we see that $X^2+aX+b\equiv 0\ (\mathrm{mod}.\ p)$, which is impossible by the assumption that g is a root of x^2+ax+b and $\boldsymbol{Z}_p[g]$ is the maximal order of $F_p\cong K_p$. Thus, we have proved: $\Rightarrow$. The converse assertion can be proved by giving an example of $g_p\in G_p$ which is p-integral, i.e., $g_p\in G_p\cap M_2(O_p)$: If $F_p=\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p$, g_p can be always taken to be p-integral. If F_p is a field, the following two elements form a representatives of G_p-conjugacy classes correponding to $f(x)=(x^2+ax+b)^2$.

(i) $g_p=\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}$

$$Z_0(g)_p=\begin{cases}\text{split if } -1\in N_{F/\boldsymbol{Q}}(F_p),\\ \text{division, otherwise,}\end{cases}$$

(ii) $g_p=\begin{pmatrix}\omega & 0\\ 0 & \eta^{-1}\omega\eta\end{pmatrix}$

$$Z_0(g)_p=\begin{cases}\text{division if } -1\in N_{F/\boldsymbol{Q}}(F_p)\\ \text{split, otherwise,}\end{cases}$$

where $\omega \in O_p$ is a root of $x^2+ax+b=0$, and $\eta \in B_p^\times$ is any element such that $N(\eta) \notin N_{F/Q}(F_p)$. In (ii), we can assume $\eta^{-1}\omega\eta \in O_p$ if B_p is division or F_p is ramified or $\boldsymbol{Z}_p[g_p]$ is not maximal. Then we see, by Corollary to Prop. 3, that $g \underset{G_p}{\sim} g_p$ for all p, i.e., g is locally integral. q.e.d.

Now let $g \in G$ belong to the case (V) in (14). By (8) and Prop. 2, we have the following diagram:

$$
\begin{array}{ccc}
\{g' \in G\,;\ g' \underset{GL_2(B)}{\sim} g\}/\underset{G}{\sim} & \xrightarrow{\sim} & \boldsymbol{Q}_+^\times/(N_{F_1/Q}(F_1^\times)N_{F_2/Q}(F_2^\times)) \\
\cap\downarrow & & \phi\downarrow\cap \\
\{g' \in G_A\,;\ g' \underset{GL_2(B_A)}{\sim} g\}/\underset{G_A}{\sim} & \xrightarrow{\sim} & \boldsymbol{Q}_{+A}^\times/(N_{F_1/Q}(F_{1A}^\times)N_{F_2/Q}(F_{2A}^\times))\,.
\end{array} \tag{15}
$$

PROPOSITION 5. *Let $g \in G$ belong to the case* (V), *and assume that $F_1 \ncong F_2$. Then the vertical maps in* (15) *are surjective, hence bijective.*

The proof is easy and will be omitted. By this proposition, we see that, given any $(g_p)_p \in G_A$, there exists $g \in G$ such that $g \underset{G_p}{\sim} g_p$ for all p. Then $C(g)$ is locally integral if and only if g_p's are p-integral. Thus our problem reduces to the purely local ones, which will be treated in 4-5.

PROPOSITION 6. *Let $g \in G$ belong to the case* (V), *and assume that $F_1 \cong F_2$. Then the image of ϕ in* (15) *is a subgroup of index* 2.

The proof is easy and will be omitted.

2-6. Finally we consider the case (VI) in (14): F is a totally imaginary quadratic extension of a real quadratic field F_0. As is well known, only three cases can occur: $F/\boldsymbol{Q}$ is either a cyclic extension of degree 4, an abelian extension of type (2, 2), or a non-Galois extension of degree 4 whose normal closure has the Galois group isomorphic to the dihedral group of order 8. We have a diagram;

$$
\begin{array}{ccc}
\{g' \in G\,;\ g' \underset{GL_2(B)}{\sim} g\}/\underset{G}{\sim} & \xrightarrow{\sim} & F_{0+}^\times/(\boldsymbol{Q}_+^\times N_{F/F_0}(F^\times)) \\
\cap\downarrow & & \phi\downarrow\cap \\
\{g' \in G_A\,;\ g' \underset{GL_2(B_A)}{\sim} g\}/\underset{G_A}{\sim} & \xrightarrow{\sim} & F_{0+A}^\times/(\boldsymbol{Q}_{+A}^\times N_{F/F_0}(F_A^\times))\,.
\end{array} \tag{16}
$$

PROPOSITION 7. *Let $g \in G$ belong to the case* (VI). *Assume that $F/\boldsymbol{Q}$ is a cyclic or non Galois extension. Then the vertical maps in* (16) *are surjective, hence bijective.*

On the other hand, if $F/\boldsymbol{Q}$ is an extension of type (2, 2), then the images

are subgroups of index 2. More precisely, the image of $\phi: F_{0+}^{\times}/N_{F/F_0}(F^{\times})\boldsymbol{Q}_{+}^{\times} \to \bigoplus_p F_{0p}^{\times}/N_{F_p/F_{0p}}(F_p^{\times})\boldsymbol{Q}_p^{\times}$ is those $(x_p)_p$ such that $x_p \notin N_{F_p/F_{0p}}(F_p^{\times})$ for even number of p's. The proofs of these facts are tiresome exercises of class field theory, and we omit them.

PROPOSITION 8. *Let $g \in G$ belong to the case* (VI), *and assume that $F/\boldsymbol{Q}$ is of type* (2, 2). *Let F_1, F_2 be the quadratic subfields of $F=\boldsymbol{Q}[g]$ other than F_0. Then* (i) *$g_i=N_{F/F_i}(g)$ is an element of $Z_G(g)$ and belongs to the case* (IV). *Moreover, if $g' \to g_i'$ is another such correspondence, we have the equivalence*

$$g \underset{G}{\sim} g' \Leftrightarrow g_1 \underset{G}{\sim} g_1' \Leftrightarrow g_2 \underset{G}{\sim} g_2'.$$

(ii) *Tne image of the vertical map of* (16) *is those $(g_p)_p \in G_A$ such that* $\sum_p \operatorname{inv} Z_0(g_{1p})_p=0$.

(iii) *Assume that $\boldsymbol{Z}[g]$ is maximal in F. Then we have an equivalence*

$$C(g): \textit{locally integral} \Leftrightarrow C(g_i): \textit{locally integral}$$

for $i=1$ and 2.

PROOF. When $g_1 \underset{G}{\sim} g_1'$, we can assume $g_1=g_1'$. So $g, g' \in \boldsymbol{Z}_G(g_1)=F_1^{\times} \cdot Z_0(g_1)$. Of course, we have assumed that g, g' have the same principal polynomial. Then we can write $g=ah$, $g'=ah'$ ($a \in F_1^{\times}$, $h, h' \in Z_0(g_1)^{\times}$), and h, h' have the same principal polynomial over $\boldsymbol{Q}$. So $\gamma h \gamma^{-1}=h'$ for some $\gamma \in Z_0(g_1)$ and $\gamma g \gamma^{-1}=g'$. The converse is obvious. So we have (i). As for (ii), the necessity is clear. The sufficiency easily follows from the structure of image of ϕ and above (i). (iii) is a consequence of explicit presentations of local conjugacy classes, and we omit the proof because we do not use the fact any after. q. e. d.

§ 3. Explicit formula of $M_G(\Lambda)$

In this section, we shall give a formula for $M_G(\Lambda)$ which appears in our trace formula in theorem A. Our method of calculation is essentially based on the theory of Tamagawa numbers of semisimple algebraic groups, which is treated in Tamagawa [19], Weil [20].

3-1. First, we shall show how the calculation of $M_G(\Lambda)$ is related to the theory of Tamagawa numbers. Let k be an algebraic number field and G be a semisimple algebraic group over k. Then the Tamagawa number $\tau(G)$ of G is defined by

$$\tau(G)=|D(k)|^{-\dim G/2} \int_{G_A/G_k} \omega_A, \tag{17}$$

where, $D(k)$ is the discriminant of k, ω is an invariant algebraic differential form of G of degree $\dim G$, and ω_A is the Tamagawa measure of G_A associated to ω. It is known, by Weil [20] Th. 4.4.1, that if G is the special unitary group of a hermitian form, or a quaternion hermitian form, then $\tau(G)=1$.

Now let G be our group, $g\in G$, and put, according to (7),

$$Z^1_G(g)=\bigoplus_{i=1}^{m} Z^1_{G_i}(g)\,, \tag{18}$$

$$Z^1_{G_i}(g)=\{z_i\in Z_i(g)^\times\cap G\,;\ n_i(z_i)=1,\ N_i(z_i)=1\},$$

where $N_i(z_i)$ is the reduced norm of $z_i\in Z_i(g)$ over F_i, the center of $Z_i(g)$. As we have seen in § 2, each $Z^1_{G_i}(g)$ is a semisimple algebraic group over $\boldsymbol{Q}$, and it is either one of the two types noted above, with the only exception for the case treated in 2-3. Therefore, if $Z^1_{G_i}(g)$'s do not contain the exceptional case, we have

$$\tau(Z^1_G(g))=\prod_{i=1}^{m}\tau(Z^1_{G_i}(g))=1\,. \tag{19}$$

Let Λ be a $\boldsymbol{Z}$-order of $Z(g)$ of the form $\Lambda=\bigoplus_{i=1}^{m}\Lambda_i$, where Λ_i is a $\boldsymbol{Z}$-order of $Z_i(g)$. Put

$$\Lambda_i^1=\{z_i\in\Lambda_i\,;z_iz_i^*=1\}\,.$$

LEMMA 9. *Assume that* $\tau(Z^1_G(g))=1$, and $n(Z_G(g))=\boldsymbol{Q}^\times$, $n(\Lambda_A^\times)=Z_A^\times$. *Then*

$$M_G(\Lambda)=\Big[\prod_{i=1}^{m}\prod_{p}\int_{\Lambda^1_{ip}}\omega_p\cdot\int_{Z^1_{G_i}(g)_\infty}\omega_\infty\Big]^{-1}.$$

This follows immediately from the definition. q. e. d.

3-2. Let $g\in Z(G)$=the center of G, so that $Z(g)=M_n(B)$. We shall now give a formula for $M_G(\Lambda)$ for $\Lambda=M_n(O)$, which will constitute the main term of our trace formula. For the convenience of the later use, we shall give a more general form: namely we assume that k is a totally real number field whose class number in the narrow sense is one, B is a totally definite quaternion algebra over k, and O is a maximal order of B.

PROPOSITION 9.[1] *Let* $\Lambda=M_n(O)$. *Then*

$$M_G(\Lambda)=\frac{|D(k)|^{n(2n+1)/2}\zeta_k(2)\zeta_k(4)\cdots\zeta_k(2n)}{\Big(\dfrac{(2\pi)^{n(n+1)}}{1!\,3!\cdots(2n-1)!}\Big)^{[K:\boldsymbol{Q}]}}\times\prod_{\mathfrak{l}\mid D(B/k)}\prod_{i=1}^{n}((N\mathfrak{l})^i+(-1)^i) \tag{20}$$

[1] We learned this formula and the proof from Prof. Y. Ihara.

where $\zeta_k(s)$ denotes the Dedekind zeta function of k.

PROOF. We prove the case $k=\boldsymbol{Q}$, since the general case requires nothing more than a careful change of notations. By Lemma 9, it suffices to evaluate the integral $\int_{A_A^1}\omega_A$. First we note that the Lie algebra $\mathfrak{g}$ of G^1 is:

$$\mathfrak{g}=\{x\in M_n(B);\ x+x^*=0\}.$$

We can write

$$B=Q+Q\alpha+Q\beta+Q\alpha\beta,\ \alpha^2=-m,\ \beta^2=-q,\ \alpha\beta=-\beta\alpha,$$

where $m,\ q\in\boldsymbol{Z}$ are such that $m=D(B)$, $(m,\ q)=1$, $q>0$. We can take, as a basis of $\mathfrak{g}$ over $\boldsymbol{Q}$, the following set of $n(2n+1)$ elements

$$x_{ii,\xi}=\begin{bmatrix}0 & \vdots & 0\\ \cdots & \xi & \cdots\\ 0 & \vdots & 0\end{bmatrix}(i,\quad \xi=\alpha,\ \beta,\ \alpha\beta,\ 1\leqq i\leqq n,$$

$$x_{ij,\eta}-x_{ji,\eta}=\begin{pmatrix}0 & \vdots & 0 & \vdots & 0\\ \cdots\cdots & & \cdots\cdots & \eta & \cdots\\ 0 & \vdots & 0 & \vdots & 0\\ \cdots & -\bar{\eta} & \cdots\cdots & & \cdots\\ 0 & \vdots & 0 & \vdots & 0\end{pmatrix}\begin{matrix}(i\\ \\ \\ (j\end{matrix},\quad \eta=1,\ \alpha,\ \beta,\ \alpha\beta,\ 1\leqq i<j\leqq n.$$

Then we can take, as an invariant form on G^1, the following

$$\omega=\overset{\triangle}{i,\xi}\, dx_{ii,\xi}\ \overset{\triangle}{i<j,\eta}(dx_{ij,\eta}-dx_{ji,\eta}),$$

where $dx_{..}$ denotes the dual of the vector field which takes the value $x_{..}$ above at the origin 1_n of G^1.

(i) *The integral at ∞:*

We can express $\mathfrak{g}_\infty$ in $M_{2n}(\boldsymbol{C})$:

$$\mathfrak{g}_\infty=\left\{x=\begin{pmatrix}X & Y\\ -{}^tY & -{}^t\bar{X}\end{pmatrix}\in M_{2n}(\boldsymbol{C});\ {}^t\bar{X}=-X,\ {}^tY=Y\right\},$$

and define a volume element $\omega_\infty^{\mathrm{can}}$ of $G_\infty^1=USp(n)$, which is induced from the Riemannian metric defined by the Killing form multiplied by -1:

$$-B(x,\ y)=-\mathrm{tr}(adx\cdot ady)=-2(n+1)\mathrm{tr}(xy).$$

Then a straight forward calculation shows that we have

$$\omega_\infty=(mq)^{n(n+1)}(4n+4)^{-n(2n+1)/2}\omega_\infty^{\mathrm{can}},\quad \text{and}$$

$$\int_{USp(n)}\omega_\infty^{\mathrm{can}}=(4n+4)^{n(2n+1)/2}2^{n(n-1)}\prod_{i=1}^{n}2\cdot\pi^{2i}/(2i-1)!.$$

This is found, for example, in Gelfand-Neumark [7].

(ii) *The integral at p, $B_p=M_2(\boldsymbol{Q}_p)$:*

We have $G_p^1\cong Sp(2n, \boldsymbol{Q}_p)$. By this isomorphism, we can identify: $\Lambda_p^1=Sp(2n, \boldsymbol{Z}_p)$. We express $\mathfrak{g}_p$ in $M_{2n}(\boldsymbol{Q}_p)$:

$$\mathfrak{g}_p=\left\{x=\begin{pmatrix}X & Y\\ Z & -{}^tX\end{pmatrix}\in M_{2n}(\boldsymbol{Q}_p);\ Y={}^tY,\ Z={}^tZ\right\},$$

and define a Haar measure ω_p^{can} of $Sp(2n, \boldsymbol{Q}_p)$ by the similar way as ω_p, from the Chevalley basis:

$$\underset{1\leqq i\leqq j\leqq n}{\begin{pmatrix}E_{ii} & 0\\ 0 & -E_{ii}\end{pmatrix}},\ \underset{1\leqq i<j\leqq n}{\begin{pmatrix}0 & E_{ij}+E_{ji}\\ 0 & 0\end{pmatrix}},\ \begin{pmatrix}0 & 0\\ E_{ij}+E_{ji} & 0\end{pmatrix},\ \underset{1\leqq i\leqq n}{\begin{pmatrix}0 & E_{ii}\\ 0 & 0\end{pmatrix}},\ \begin{pmatrix}0 & 0\\ E_{ii} & 0\end{pmatrix}.$$

Then by a straight forward calculation, we have

$$\omega_p=\left|2^{n^2}(qm)^{n(n+1)/2}\right|_p^{-1}\omega_p^{\mathrm{can}}.$$

Following equality is well known:

$$\int_{Sp(2n, \boldsymbol{Z}_p)}\omega_p^{\mathrm{can}}=p^{-n(2n+1)}\sharp(Sp(2n, F_p)),\quad F_p=\boldsymbol{Z}/(p).$$

Therefore we have

$$\int_{\Lambda_p^1}\omega_p=\left|2^{n^2}(qm)^{n(n+1)/2}\right|_p^{-1}\prod_{i=1}^{n}(1-p^{-2i}).$$

(iii) *The integral at p, B_p: division:*

If $p\neq 2$, we may assume that α, β were so chosen that 1, α, β, $\alpha\beta$ form a basis of O_p over $\boldsymbol{Z}_p$. We then put $\omega_p^{\mathrm{can}}=\omega_p$. If $p=2$, we take a basis of O_p and define ω_p^{can} as above. Then an easy calculation shows that

$$\omega_p=|2|_p^{-n^2}\omega_p^{\mathrm{can}},$$

which is valid also for $p\neq 2$. Now we have

$$\int_{\Lambda_p^1}\omega_p^{\mathrm{can}}=p^{-n(2n+1)}\sharp(\Lambda_p^1/\{z\in\Lambda_p^1;\ z\equiv 1\ (\mathrm{mod.}\ p)\}).$$

If we note that $\Lambda_p^1/\{z\in\Lambda_p^1;\ z\equiv 1\ (\mathrm{mod.}\ p)\}$ is isomorphic to

$$\left\{\begin{pmatrix}X & Y\\ 0 & \overline{X}\end{pmatrix};\ X,\ Y\in M_n(F_{p^2}),\ {}^t\overline{X}X=1_n,\ {}^t\overline{X}Y-{}^tY\overline{X}=0\right\},$$

we have, since $\sharp(U_n(F_{p^2}))=p^{n(n-1)/2}\prod_{i=1}^{n}(p^i-(-1)^i)$,

$$\int_{\Lambda_p^1}\omega_p=|2|_p^{-n^2}\prod_{i=1}^{n}(1-p^{-2i})\Big[\prod_{i=1}^{n}(1+(-1)^ip^{-i})\Big]^{-1}.$$

Multiplying these integrals and applying Lemma 9, we get the required formula of $M_G(\Lambda)$. q. e. d.

REMARK 2. (i) If $g\in Z(G)$, the only G-genus of Z-orders of $Z(g)=M_n(B)$, which appears in our trace formula is the one containing $M_n(O)$, since $c_p(g, M_n(O_p), \Lambda_p)=0$ if $\Lambda_p\nsim M_n(O_p)$.
(ii) In some cases, we can conclude that $H=1$, by Prop. 9. To be more precise, we have, by the definition of $M_G(\Lambda)$,

$$M_G(M_n(O))=\sum_{i=1}^{H}\frac{1}{[\Lambda_i^\times\cap G^1:1]}.$$

By Prop. 9, we have $M_G(M_n(O))=1/1152$, $1/288$, $1/82944$, $1/28800$, according as $(n, k, D(B))=(2, \boldsymbol{Q}, 2)$, $(2, \boldsymbol{Q}, 3)$, $(3, \boldsymbol{Q}, 2)$, $(2, \boldsymbol{Q}(\sqrt{5}), 1)$. Since the denominators are equal to $|O^1|^n\cdot n!=$(the order of the unit group of O^n), we conclude that the class of O^n is the only maximal O-lattices in the principal genus.

3-3. Now we assume that $n=2$. Let $g\in G$ belong to the case (II) of (14). Then $Z(g)=B\oplus B$, and any Z-order Λ of $Z(g)$ is contained in a maximal one, so we may assume that $\Lambda\subseteq O\oplus O$.

PROPOSITION 10. *Notations being as above, we have*

$$M_G(\Lambda)=\Big[\frac{1}{24}\prod_{l\mid D(B)}(l-1)\Big]^2\prod_p[(O_p^2)^\times\cap G_p:\Lambda_p^\times\cap G_p]. \tag{21}$$

PROOF. By Theorem 3, for $n=1$, we have the $Ma\beta$ formula of B:

$$M_G(O)=\frac{1}{24}\prod_{l\mid D(B)}(l-1), \tag{22}$$

which has been known by [4]. Then we apply Lemma 9, and get the formula for $\Lambda=O^2$. The general case follows from this, if we note the equality:

$$\tau(Z_G(g)/\boldsymbol{Q}^\times)=2M_G(\Lambda)\Big(\int_{Z_G(g)_\infty/R^\times}\bar{\omega}_\infty\Big)\prod_p\int_{(\Lambda_p^\times\cap G_p)/\boldsymbol{Z}_p^\times}\bar{\omega}_p$$

$$=2M_G(O^2)\Big(\int_{Z_G(g)_\infty/R^\times}\bar{\omega}_\infty\Big)\prod_p\int_{((O_p^2)^\times\cap G_p)/\boldsymbol{Z}_p^\times}\bar{\omega}_p$$

where $\bar{\omega}$ is the Tamagawa measure on the semi-simple group $Z_G(g)/\boldsymbol{Q}^\times$.

Let $g\in G$ belong to the case (III), so that $Z(g)=B\oplus F$, $F=$imaginary quadratic field in B. Let $\mathcal{O}$ denote the ring of integers of F.

PROPOSITION 11. *Notation being as above, let Λ be a $\boldsymbol{Z}$-order of $Z(g)$ such that $g\in\Lambda\subseteq O\oplus\mathcal{O}$. Then we have*

$$M_G(\Lambda)=\frac{h(F)}{24[\mathcal{O}^\times:1]}\prod_{l\mid D(B)}(l-1)\prod_p[(O\oplus\mathcal{O})_p^\times\cap G_p:\ \Lambda_p^\times\cap G_p] \tag{23}$$

where $h(F)$ denote the class number of F.

PROOF. If we write

$$F_A^\times=\coprod_{i=1}^{h(F)}F^\times a_i\mathcal{O}_A^\times,$$

we have a disjoint decomposition:

$$Z_G(g)_A=\coprod_{i=1}^{h(F)}((B^\times,\ F^\times)\cap G)(B_A^1a_i,\ a_i)((O_A^\times,\ \mathcal{O}_A^\times)\cap G_A).$$

Therefore we have

$$Z_G(g)\backslash Z_G(g)_A/(\Lambda_A^\times\cap G_A)\cong\coprod_{i=1}^{h(F)}Z_G^1(g)\backslash Z_G^1(g)_A(a_i,\ a_i)/\Lambda_A^1,$$

for $\Lambda=O\oplus\mathcal{O}$. Then we can apply Lemma 9 and proceed in the same way as in Prop. 10. q. e. d.

Now let $g\in G$ belong to the case (IV). By Prop. 3, we have $Z(g)=B_F$, and $Z_G(g)=F^\times\cdot Z_0(g)^\times$, where $F=\boldsymbol{Q}[g]$=imaginary quadratic field, and $Z_0(g)$ is the definite quaternion algebra over $\boldsymbol{Q}$. Let Λ be a $\boldsymbol{Z}$-order of $Z(g)$ such that $g\in\Lambda$, and put:

$$\Lambda_0=\Lambda\cap Z_0(g).$$

Then we see that Λ_0 is an order of $Z_0(g)$, so it is contained in some maximal order $\Lambda_{0,\max}$ of $Z_0(g)$.

PROPOSITION 12. *Notations being as above, we have*

$$M_G(\Lambda)=\frac{h(\mathcal{O})}{12[\mathcal{O}^\times:1]}\prod_{l\mid D(Z_0(g))}(l-1)\prod_p d_p(\Lambda)/e_p(\Lambda), \tag{24}$$

where

$$\begin{aligned}d_p(\Lambda)&=[(\Lambda_{0,\max})_p^\times:\ \Lambda_{0p}^\times]\ [\mathcal{O}_p^\times:\boldsymbol{Z}_p[g]^\times],\\ e_p(\Lambda)&=[\Lambda_p^\times\cap G_p:\ \boldsymbol{Z}_p[g]^\times\Lambda_{0p}^\times].\end{aligned} \tag{25}$$

PROOF. First we assume that $\Lambda=\Lambda_{0,\max}\otimes\mathcal{O}$. Since the elements of $F^\times$ and $Z_0(g)^\times$ mutually commute, we have

$$Z_G(g)\backslash Z_G(g)_A/(\Lambda_A^\times\cap G_A)=(F^\times\backslash F_A^\times/\mathcal{O}_A^\times)\cdot(Z_0(g)^\times\backslash Z_0(g)_A^\times/\Lambda_{0A}^\times).$$

Therefore we have a bijection

$$Z_G^1(g)\backslash Z_G^1(g)_A/\Lambda_A^1 \cong \coprod_{i=1}^{h(F)} \coprod_{j=1}^{h(Z_0(g))} (F^\times a_i \mathcal{O}_A^\times)(Z_0(g)^1 b_j \Lambda_{0A}^1),$$

where

$$F_A^\times = \coprod_{i=1}^{h(F)} F^\times a_i \mathcal{O}_A^\times,$$

$$Z_0(g)_A^1 = \coprod_{j=1}^{h(Z_0(g))} Z_0(g)^1 b_j \Lambda_{0A}^1$$

From this, we get the formula of $M_G(\Lambda)$ for $\Lambda = \Lambda_{0,\max} \otimes \mathcal{O}$. In the general case, we have, as in the proof of Prop. 10,

$$\tau(Z_G(g)/\boldsymbol{Q}^\times) = 2M_G(\Lambda_{0,\max}\otimes\mathcal{O}) \int_{Z_G(g)_\infty/\boldsymbol{R}^\times} \bar{\omega}_\infty \prod_p \int_{(\Lambda_{0,\max}\otimes\mathcal{O})_p^\times \cap G_p/\boldsymbol{Z}_p^\times} \bar{\omega}_p$$

$$= 2M_G(\Lambda) \int_{Z_G(g)_\infty/\boldsymbol{R}^\times} \bar{\omega}_\infty \prod_p \int_{\Lambda_p^\times \cap G_p/\boldsymbol{Z}_p^\times} \bar{\omega}_p$$

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

§ 4. Calculation of $c_p(g, M_2(O_p), \Lambda_p)$ for g: torsion element.

We shall now evaluate the factor $c_p(g, M_2(O_p), \Lambda_p)$, which appeared in the trace formula, in the case where g has a finite order. This is sufficient for the calculation of the class number of G, since $C(g)$ locally integral implies that it is of finite order: in fact, the locally integral g's with $n(g)=1$ form a discrete subgroup $G^1 \cap \mathfrak{U}^1$ of the compact group $\mathfrak{U}^1$. As we defined in § 1, $c_p(g, M_2(O_p), \Lambda_p)$ is the number of distinct ways to embed Λ_p optimally into $M_2(O_p)$, up to some equivalence relations. In this section, we denote the set $\{x \in G_p;\ x^{-1}gx \in U_p\}$ by $M(g, U_p)$.

4-1. First, let $g = \pm 1$. As noted in § 3-2, Remark 2, the only G-genus of Z-orders of $Z(g) = M_2(B)$ which takes part in the trace formula is the one containing $M_2(O)$. In this case we have obviously, $Z_G(g) = G$, so $c_p(g, M_2(O_p), M_2(O_p)) = 1$.

Let now g belong to the case (II) in (14). We see that $g^2 = 1$, and by the result of § 2, g is conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in G.

PROPOSITION 13. *Let* $g = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. *Then*

(26) $$c_p(g, M_2(O_p), \Lambda_p)=\begin{cases} 1 \cdots \textit{if } \Lambda_p \sim \Lambda(k)_p,\ 0 \leqq k \leqq \mathrm{ord}_p(2), \\ 0 \cdots \textit{otherwise,} \end{cases}$$

$$[\Lambda(0)_p^1 : \Lambda(1)_p^1]=\begin{cases} p^2(p+1) \cdots \textit{if } B_p=\textit{division}, \\ p(p^2-1) \cdots \textit{if } B_p=\textit{split}, \end{cases}$$

where $\Lambda(k)_p=\left\{\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in Z(g)_p ;\ \alpha \equiv \delta \pmod{p^k},\ \alpha, \delta \in O_p\right\}$.

PROOF. First we note that $Z(g)=\begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}$, and $Z_G(g)=\left\{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix};\ Nx=Ny \neq 0\right\}$. We shall write $x_1 \sim x_2$ for $x_i \in G_p$, if $Z_G(g)_p x_1 U_p = Z_G(g)_p x_2 U_p$. Now, given an element $x \in M_p(g, U_p)=\{x \in G_p ;\ x^{-1}gx \in U_p\}$, we can assume that it is of the form $x=\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$: in fact, by multiplying an element of U_p from the right, we have $x \sim \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\alpha \neq 0$, then we multiply $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}^{-1} \in Z_G(g)_p$ from the left and see that $x \sim \begin{pmatrix} 1 & * \\ * & * \end{pmatrix}$. Since the last element belongs to G_p, it is of the form $\begin{pmatrix} 1 & \beta \\ -\delta\bar{\beta} & \delta \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$. Moreover, we see that β can be taken arbitrary from $O_p^1 \beta O_p^1$, because of the following equality:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\delta} \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}\begin{pmatrix} \bar{\alpha} & 0 \\ 0 & \delta \end{pmatrix}=\begin{pmatrix} 1 & \alpha\beta\delta \\ -\overline{\alpha\beta\delta} & 1 \end{pmatrix}, \quad \alpha, \delta \in O_p^1 .$$

Now, we assume that B_p is division. We multiply, if necessary, x by some power of p and make it of the form $\begin{pmatrix} a & \beta \\ -\bar{\beta} & a \end{pmatrix}$, $a=p^n$, $\beta \in O_p - pO_p$. If $n(x)=a^2+N\beta \in \boldsymbol{Z}_p^\times$, we have $x \sim 1$. If $n(x) \in p\boldsymbol{Z}_p$, and $a \in p\boldsymbol{Z}_p$, then $\beta=\pi\beta_0$, where π is a prime element of O_p such that $N\pi \in p\boldsymbol{Z}_p^\times$ and $\beta_0 \in O_p^\times$. Then we see that $\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}^{-1} x \in U_p$, so that $x \sim 1$. Thus we can assume, if $x \not\sim 1$, that it is of the form $x=\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$, $\beta \in O_p$, $n(x)=1+N\beta=p^k u$, $k \geqq 1$, $u \in \boldsymbol{Z}_p^\times$. Now we have

(27) $$x_1^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} x_2=\frac{1}{p^k u_1}\begin{pmatrix} \alpha+\beta_1\delta\bar{\beta}_2 & \alpha\beta_2-\beta_1\delta \\ \bar{\beta}_1\alpha-\delta\bar{\beta}_2 & \bar{\beta}_1\alpha\beta_2+\delta \end{pmatrix},$$

$$\text{for} \quad x_i=\begin{pmatrix} 1 & \beta_i \\ -\bar{\beta}_i & 1 \end{pmatrix}.$$

If we put $\beta=\beta_1=\beta_2$, $\alpha=1$, $\delta=-1$, then we see that the condition $x\in M_p(g, U_p)$ is equivalent to $2\beta\equiv 0 \pmod{p^k}$. Since we have assumed that $\beta\in O_p^\times$, $k\geqq 1$, this occurs if and only if $p=2$, $k=1$. Moreover, if $x_i=\begin{pmatrix} 1 & \beta_i \\ -\bar{\beta}_i & 1 \end{pmatrix}$, $i=1, 2$, satisfy these conditions, we can find an element $\varepsilon\in O_p$ such that $\varepsilon\equiv 1 \pmod{p^k}$ and $N\varepsilon=N(\beta_2\beta_1^{-1})$, since $N(\beta_2\beta_1^{-1})\equiv 1 \pmod{p^k}$. Then if we put $\alpha=\bar{\beta}_2$, $\delta=\bar{\beta}_1\varepsilon$, we have, in (27), $x_1^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}x_2\in U_p$, so that $x_2\sim x_1$. So we have $M_p(g, U_p)=Z_G(g)_p\left\{1, \begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}\right\}U_p$, where $\beta=1$ if $p=2$, and $\beta=0$ otherwise. We put $\Lambda_p=Z(g)_p\cap xM_2(O_p)x^{-1}$, for each $x\in M_p(g, U_p)$. From (27), we see easily that $\Lambda_p=\Lambda(0)_p$, if $x=1$, and $\Lambda_p=\Lambda(1)_p$, if $x=\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$. We have $\Lambda(0)_p^1/\Lambda(1)_p^1\cong O_p^1/\{z\in O_p^1;\ z\equiv 1 \pmod{p}\}\cong\left\{\begin{pmatrix} x & y \\ 0 & \bar{x} \end{pmatrix};\ x, y\in F_{p^2},\ x\bar{x}=1\right\}$, and therefore, $[\Lambda(0)_p^1:\Lambda(1)_p^1]=p^2(p+1)$.

Now we assume that B_p is split. As above, we can start with $x=\begin{pmatrix} a & \beta \\ -\bar{\beta} & a \end{pmatrix}$, where $a=p^m$, $\beta\in O_p-pO_p$, and any β in $O_p^1\beta O_p^1=SL_2(\boldsymbol{Z}_p)\beta SL_2(\boldsymbol{Z}_p)$ gives an equivalent x. By the theory of elementary divisors, we can assume that β is either one of the forms $\begin{pmatrix} v & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} v & 0 \\ 0 & p^n \end{pmatrix}$, where $v\in\boldsymbol{Z}_p^\times$. For $x_i=\begin{pmatrix} a & \beta_i \\ -\bar{\beta}_i & a \end{pmatrix}$, $\beta_1=\begin{pmatrix} v & 0 \\ 0 & 0 \end{pmatrix}$, we have

$$x_1^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}x_2=\frac{1}{p^{2m}}\begin{pmatrix} p^{2m}\alpha+\beta_1\delta\bar{\beta}_2 & p^m(\alpha\beta_2-\beta_1\delta) \\ p^m(\bar{\beta}_1\alpha-\delta\bar{\beta}_2) & \bar{\beta}_1\alpha\beta_2+p^{2m}\delta \end{pmatrix}. \tag{28}$$

Therefore, we see that $x_1\in M_p(g, U_p)$ implies $2v\equiv 0 \pmod{p^m}$, so $m=0$, $x_1\sim 1$, if $p\neq 2$, or $m=1$, $p=2$. In both cases, we see that $x_1\sim x_2$ if β_1 is as above and $\beta_2=\begin{pmatrix} v_2 & 0 \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} v_2 & 0 \\ 0 & p^n \end{pmatrix}$, $n>2m$, since $x_1^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}x_2\in U_p$, for $\alpha=\begin{pmatrix} v & 0 \\ 0 & v_2 \end{pmatrix}$, $\delta=\begin{pmatrix} v_2 & 0 \\ 0 & v \end{pmatrix}$. Also, we have $x_1^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}x_2\in U_p$ for $x_1=1$, $x_2=\begin{pmatrix} p^m & \beta \\ -\bar{\beta} & p^m \end{pmatrix}$, $\beta=\begin{pmatrix} v & 0 \\ 0 & p^n \end{pmatrix}$, $1\leqq n\leqq m$, with $\alpha=\begin{pmatrix} 1 & 0 \\ 0 & p^{-n} \end{pmatrix}$, $\delta=\begin{pmatrix} p^{-n} & 0 \\ 0 & 1 \end{pmatrix}$, so that $x_2\sim 1$. Finally, assume that $m<n\leqq 2m$ for x_2 in the last expression. Then a direct calculation similar to (28) shows that $x_2\in M_p(g, U_p)$ if and only if $n=2m$, and $2p^m\equiv 0 \pmod{p^{2m}(1+v)}$. If $p\neq 2$, this happens only if $n=m=0$, $1+v\in\boldsymbol{Z}_p^\times$, so that $x_2\sim 1$. If $p=2$, then either

$m=0$, $1+v\in p\boldsymbol{Z}_p^\times$, or $m=1$, $1+v\in\boldsymbol{Z}_p^\times$. In the first case we have $x_2\sim x_1=\begin{pmatrix} p & \beta_1 \\ -\bar{\beta}_1 & p \end{pmatrix}$, $\beta_1=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, by (28) with $\alpha=\bar{\delta}=\begin{pmatrix} 1 & 0 \\ 0 & -pv \end{pmatrix}$, and in the second case we have also $x_2\sim x_1$, with $\alpha=\bar{\delta}=\begin{pmatrix} 1 & 0 \\ 0 & -v \end{pmatrix}$. Thus we have $M_p(g, U_p)=Z_G(g)_p\left\{1, \begin{pmatrix} p & \beta \\ -\bar{\beta} & p \end{pmatrix}\right\}U_p$, where $\beta=0$ if $p\neq 2$, and $\beta=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} p & \beta \\ -\bar{\beta} & p \end{pmatrix}\sim\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ if $p=2$. In the latter case, we see that $\Lambda_p=Z(g)_p\cap xM_2(O_p)x^{-1}=\Lambda(1)_p$. We have $\Lambda(0)_p^1/\Lambda(1)_p^1\cong O_p^1/\{z\in O_p^1;\ z\equiv 1 \pmod{p}\}\cong SL_2(F_p)$, and therefore, $[\Lambda(0)_p^1:\ \Lambda(1)_p^1]=p(p^2-1)$.

q. e. d.

4-2. Let g be an element of G of finite order that belongs to the case (III) in (14). Then we see that g is conjugate in G to $\pm\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$, where $\omega\neq\pm 1$ is an element of B of finite order. As is well known, the order of ω is either 4, or 3, 6, and we can assume that $\omega\in O$. We put $F=Q[\omega]$, $\mathcal{O}=Z[\omega]$.

PROPOSITION 14. *Let* $g=\pm\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$, $\omega\in O$. *Then,*

(i) *If* $\left(\frac{F}{p}\right)=1$, *then* B_p *is split and*

$$c_p(g, M_2(O_p), \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim O_p\oplus\mathcal{O}_p, \\ 0\cdots \textit{otherwise,} \end{cases}$$

(ii) *If* $\left(\frac{F}{p}\right)=0$,

$$c_p(g, M_2(O_p), \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim O_p\oplus\mathcal{O}_p, \\ 0\cdots \textit{otherwise,} \end{cases}$$

(iii) *If* $\left(\frac{F}{p}\right)=-1$,

$$c_p(g, M_2(O_p), \Lambda_p)=\begin{cases} 2\cdots \textit{if } \Lambda_p\sim O_p\oplus\mathcal{O}_p,\ B_p=\textit{division}, \\ 1\cdots \textit{if } \Lambda_p\sim O_p\oplus\mathcal{O}_p,\ B_p=\textit{split}, \\ 0\cdots \textit{otherwise.} \end{cases}$$

PROOF. We note that $Z(g)=\begin{pmatrix} B & 0 \\ 0 & F \end{pmatrix}$, and $Z_G(g)=\left\{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}\in Z(g);\ Nx=Ny\neq 0\right\}$. As in the proof of Prop. 13, we shall write $x_2\sim x_1$, if $x_2=zx_1u$ for some $z\in Z_G(g)_p$, $u\in U_p$. Then we see, as in the proof of Prop. 13, that any $x\in G_p$ can be deformed to $x\sim\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$ or $\begin{pmatrix} \eta & 0 \\ 0 & \eta\delta \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$, where η is an element

of $B_p^\times$ such that $N\eta \notin N(F_p^\times)$, and $\delta \in F_p^1 \backslash B_p^1$, $\beta \in O_p^1 \backslash B_p^\times / O_p^1$. First assume that B_p is division. Then we have

$$\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}=\begin{pmatrix} 1 & \beta\bar{\delta} \\ -\overline{(\beta\delta)} & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} \in U_p,$$

so that $x \sim \begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$, or $\begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$. If $\left(\frac{F}{p}\right)=0$, then we can assume that $N\eta \in Z_p^\times$, and

$$\begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}=\begin{pmatrix} 1 & \eta\beta\eta^{-1} \\ -\overline{(\eta\beta\eta^{-1})} & 1 \end{pmatrix}\times\begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix},\ \begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix} \in U_p,$$

so by changing the notation we have always $x \sim \begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$. Then we can proceed in the same way as in Prop. 13. If $\left(\frac{F}{p}\right)=-1$, we can take as η, a prime element of O_p such that $\mathrm{Int}(\eta)$ induces on F_p the nontrivial conjugation. Then it is easy to see that $x \in M_p(g, U_p)$ if and only if $\begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix} x \in M_p(g, U_p)$, and they determine the same order of $Z_G(g)_p : Z(g)_p \cap xM_2(O_p)x^{-1}=Z(g)_p \cap \begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix} xM_2(O_p)x^{-1}\begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix}^{-1}$. Therefore we get our assertion from the above result. Now we assume that B_p is split, and so $B_p=M_2(\boldsymbol{Q}_p)$, $O_p=M_2(\boldsymbol{Z}_p)$. We see that, if $x=\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$ $\in M_p(g, U_p)$ then $\begin{pmatrix} 1 & \beta \\ -\bar{\beta} & 1 \end{pmatrix}$ can be reduced to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, by the proof of Prop. 13, and that we have $\delta^{-1}\omega\delta \in O_p$. Then we see, by the following well known lemma, that the last condition is equivalent to $\delta \in F_p^\times \cdot O_p^\times$, hence $\delta \in F_p^1 \cdot O_p^1$. It follows easily that $x \sim 1$, if $x \in M_p(g, U_p)$. q. e. d.

LEMMA 10. *Let F be a subalgebra of $M_2(\boldsymbol{Q}_p)$ such that $[F : \boldsymbol{Q}_p]=2$ and $F \cap M_2(\boldsymbol{Z}_p)=\mathcal{O}_p$ is a maximal order of F.*

(i) *If $F=\boldsymbol{Q}_p \oplus \boldsymbol{Q}_p$, we assume that $F=\begin{pmatrix} \boldsymbol{Q}_p & 0 \\ 0 & \boldsymbol{Q}_p \end{pmatrix}$. Then*

$$GL_2(\boldsymbol{Q}_p)=\coprod_{n \geq 0} F^\times \begin{pmatrix} 1 & 0 \\ 1 & p^n \end{pmatrix} GL_2(\boldsymbol{Z}_p).$$

(ii) *If F is a field, we assume that* $F=\boldsymbol{Q}_p+\boldsymbol{Q}_p\begin{pmatrix}0 & 1\\ -b & -a\end{pmatrix}$, *where* 1, $\omega=\begin{pmatrix}0 & 1\\ -b & -a\end{pmatrix}$ *is a basis of* $\mathcal{O}_p$. *Then*

$$GL_2(\boldsymbol{Q}_p)=\coprod_{n\geq 0}F^\times\begin{pmatrix}1 & 0\\ 0 & p^n\end{pmatrix}GL_2(\boldsymbol{Z}_p)\,.$$

PROOF. Although this is well known, we give here a proof, for the sake of convenience. Any $x\in GL_2(\boldsymbol{Q}_p)$ is reduced, by a right multiplication of an element of $GL_2(\boldsymbol{Z}_p)$, to $a\cdot\begin{pmatrix}p^m & 0\\ c & p^n\end{pmatrix}$, where $a\in\boldsymbol{Q}_p^\times$, m, $n\geqq 0$ and $c\in\boldsymbol{Z}_p/(p^n)$. (i) follows from this. Assume, in (ii), that $n>0$ in $x=\begin{pmatrix}p^m & 0\\ c & p^n\end{pmatrix}$. Then $c\in\boldsymbol{Z}_p^\times$, and $\omega x=\begin{pmatrix}c & *\\ * & *\end{pmatrix}$. Therefore x is reduced to an element of the form $\begin{pmatrix}1 & 0\\ c & p^n\end{pmatrix}$. We have $x\sim\begin{pmatrix}b+ac & c\\ -bc & b\end{pmatrix}\begin{pmatrix}1 & 0\\ c & p^n\end{pmatrix}=\begin{pmatrix}c^2+ac+b & cp^n\\ 0 & bp^n\end{pmatrix}$. We note that c^2+ac+b divides cp^n, since x^2+ax+b is the equation of ω. So we have $x\sim\begin{pmatrix}c^2+ac+b & 0\\ 0 & bp^n\end{pmatrix}\sim\begin{pmatrix}1 & 0\\ 0 & p^m\end{pmatrix}$. The disjointness is clear if we note that $F\cap\begin{pmatrix}1 & 0\\ 0 & p^n\end{pmatrix}M_2(\boldsymbol{Z}_p)\begin{pmatrix}1 & 0\\ 0 & p^n\end{pmatrix}^{-1}=\boldsymbol{Z}_p+p^n\boldsymbol{Z}_p\omega$ is the order of F of conductor p^n, which is also true in (i). q. e. d.

4-3. In order to make some part of calculation in the remaining cases easier, consider, instead of G_p, an isomorphic group

$$G_p^*=\left\{g\in M_2(B_p)\,;\ g\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}g^*=n(g)\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right\}.$$

LEMMA 11. *Let* $\begin{pmatrix}t & r\\ \bar{r} & s\end{pmatrix}\in M_2(B_p)$ *be a hermitian matrix such that* t, $s\in Z_p$, $r\in O_p$ *and* $ts-r\bar{r}\in\boldsymbol{Z}_p^\times$. *Then there exists an element* $x\in GL_2(O_p)$ *such that* $xx^*=\begin{pmatrix}t & r\\ \bar{r} & s\end{pmatrix}$.

PROOF. If either t or s is in $\boldsymbol{Z}_p^\times$, we can assume, by taking the conjugation by $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, that $s\in\boldsymbol{Z}_p^\times$; take a, b, $d\in O_p$ such that $d\bar{d}=s$, $b\bar{d}=r$, $a\bar{a}=(ts-r\bar{r})/s$. Then $x=\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}$ satisfies the condition. Assume that s, $t\in p\boldsymbol{Z}_p$. Then

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}\begin{pmatrix} 1 & \bar{c} \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} t & r+t\bar{c} \\ ct+\bar{r} & c\bar{c}t+Tr(cr)+s \end{pmatrix}.$$

we can find $c\in O_p$ such that $\mathrm{Tr}(cr)\in \boldsymbol{Z}_p^\times$, hence $c\bar{c}t+\mathrm{Tr}(cr)+s\in \boldsymbol{Z}_p^\times$. So the problem is reduced to the first case. q. e. d.

Now it is clear that there exists an isomorphism $\phi: G_p \xrightarrow{\sim} G_p^*$ such that $\phi(U_p)=G_p^*\cap GL_2(O_p)=U_p^*$; in fact take $x\in GL_2(O_p)$ such that $xx^*=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and put $\phi=\mathrm{Int}(x^{-1}): g\to xgx^{-1}$. In G_p^*, the Iwasawa decomposition takes a simpler form: namely

$$G_p^*=\coprod_{n\in \boldsymbol{Q}_p^\times}\bigcup_{\alpha\in B_p^\times}\bigcup_{\beta}\begin{pmatrix} n\bar{\alpha}^{-1} & \beta \\ 1 & \alpha \end{pmatrix}U_p^*, \tag{29}$$

where β runs over the set $B(\alpha)=\{\beta\in B;\ \mathrm{Tr}(\bar{\alpha}\beta)=0\}$ (c.f. Satake [15])

Now let g belong to the case (IV) in (14). Then g generates over $\boldsymbol{Q}$ an imaginary quadratic field, so if it is of finite order, its order is either 3, 6, or 4. By Prop. 3, the conjugacy class of g is determined by the structure of $Z_0(g)$ which depends only on $\boldsymbol{Q}(g)$. First we treat the case where $Z_0(g)_p$ is split. Then we can take, as a representative of the conjugacy class, $g=\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}\in G_p^*$, where $\omega\in O_p$ is a root of unity of order 3, 6, or 4 if $\boldsymbol{Q}_p[g]$ is a field. We have $Z(g)_p=M_2(F)$, $F=\boldsymbol{Q}_p(\omega)\cong \boldsymbol{Q}_p(g)$, and $Z_0(g)=\begin{pmatrix} \boldsymbol{Q}_p & \boldsymbol{Q}_p\rho \\ \boldsymbol{Q}_p\rho & \boldsymbol{Q}_p \end{pmatrix}$, where $\rho\in F$ is an element such that $\rho^2\in \boldsymbol{Q}_p^\times$, so we can put $\rho=\sqrt{-3}, \sqrt{-1}$, according as $F=\boldsymbol{Q}_p(\sqrt{-3})$, $\boldsymbol{Q}_p(\sqrt{-1})$. We denote by $\mathcal{O}_p$ the ring of integers of F.

PROPOSITON 15. *Notations being as above, we have*:

(i) *If* $\left(\frac{F}{p}\right)=1$,

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim M_2(\mathcal{O}_p), \\ 0\cdots \textit{otherwise}, \end{cases}$$

$d_p=e_p=1$, *for* $\Lambda_p=M_2(\mathcal{O}_p)$.

(ii) *If* $\left(\frac{F}{p}\right)=-1$,

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 2\cdots \textit{if } \Lambda_p\sim M_2(\mathcal{O}_p),\ B_p=\textit{division}, \\ 1\cdots \textit{if } \Lambda_p\sim M_2(\mathcal{O}_p),\ B_p=\textit{split}, \\ 0\cdots \textit{otherwise}, \end{cases}$$

$d_p=e_p=1$, *for* $\Lambda_p=M_2(\mathcal{O}_p)$.

(iii) *If* $\left(\frac{F}{p}\right)=0$, *and* $F=\boldsymbol{Q}_p(\sqrt{-3})$, $(p=3)$

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim M_2(\mathcal{O}_p)=\Lambda_1, \\ 1\cdots \textit{if } \Lambda_p\sim\begin{pmatrix}1 & \rho^{-1}\varepsilon\\ 0 & 1\end{pmatrix}M_2(O_p)\begin{pmatrix}1 & \rho^{-1}\varepsilon\\ 0 & 1\end{pmatrix}^{-1}\cap M_2(F) \\ \qquad =\Lambda_2,\ \textit{and } B_p=\textit{division}, \\ 0\cdots \textit{otherwise}, \end{cases}$$

$d_p(\Lambda_1)=4$, $e_p(\Lambda_1)=2$, $d_p(\Lambda_2)=6$, $e_p(\Lambda_2)=1$,

where ε *is an element of* $O_p^\times$ *such that* $\varepsilon^2=-1$, $\varepsilon\rho=-\rho\varepsilon$.

(iii)′ *If* $\left(\frac{F}{p}\right)=0$, *and* $F=\boldsymbol{Q}_p(\sqrt{-1})$, $(p=2)$

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim\begin{pmatrix}1 & \pi^{-1}\varepsilon\\ 0 & 1\end{pmatrix}M_2(O_p)\begin{pmatrix}1 & \pi^{-1}\varepsilon\\ 0 & 1\end{pmatrix}^{-1}\cap M_2(F)=\Lambda_1, \\ 1\cdots \textit{if } \Lambda_p\sim M_2(O_p)=\Lambda_2, \\ 1\cdots \textit{if } \Lambda_p\sim\begin{pmatrix}1 & \varepsilon/2\\ 0 & 1\end{pmatrix}M_2(O_p)\begin{pmatrix}1 & \varepsilon/2\\ 0 & 1\end{pmatrix}^{-1}\cap M_2(F)=\Lambda_3 \\ \qquad \textit{and } B_p=\textit{division}, \\ 0\cdots \textit{otherwise}, \end{cases}$$

$d_p(\Lambda_1)=3$, $e_p(\Lambda_1)=2$, $d_p(\Lambda_2)=e_p(\Lambda_2)=1$, $d_p(\Lambda_3)=3$, $e_p(\Lambda_3)=1$, *where* ε *is an element of* $O_p^\times$ *such that* $\varepsilon^2=-1$, $\varepsilon\rho=-\rho\varepsilon$ *if* B_p *is division*, : $\varepsilon^2=1$, $\varepsilon\rho=-\rho\varepsilon$ *if* B_p *if split, and* $\pi=1+\rho$ *is a prime element of* F.

PROOF. (i) Note first that this case occurs only if B_p is split. We can assume that $F=\begin{pmatrix}\boldsymbol{Q}_p & 0\\ 0 & \boldsymbol{Q}_p\end{pmatrix}$ $B_p=M_2(\boldsymbol{Q}_p)$, and $g=\begin{pmatrix}\omega_1 & 0\\ 0 & \omega_2\end{pmatrix}$, $\omega_1, \omega_2\in\boldsymbol{Z}_p^\times$. By (29), any element x of G_p^* is reduced to $x\sim\begin{pmatrix}n\bar{\alpha}^{-1} & \beta\\ 0 & \alpha\end{pmatrix}$, in the coset $Z_G(g)xU_p^*$, where $Z_G(g)$ =the centralizer of g in G_p^*. Since $\begin{pmatrix}n & 0\\ 0 & 1\end{pmatrix}\in Z_G(g)$, we can replace n by 1. By Lemma 10 (i), $\alpha=y\begin{pmatrix}1 & 0\\ 1 & p^n\end{pmatrix}u$ for some $y\in F^\times$ and $u\in O_p^\times=GL_2(\boldsymbol{Z}_p)$. Then by changing the notations, we see $x\sim\begin{pmatrix}\bar{\alpha}^{-1} & \beta\\ 0 & \alpha\end{pmatrix}$, $\alpha=\begin{pmatrix}1 & 0\\ 1 & p^n\end{pmatrix}$. Writing down the condition $x^{-1}gx\in U_p^*$, we see that it implies $\alpha^{-1}\omega\alpha\in O_p$, hence $c(\omega_2-\omega_1)=0$ (mod. p^n). From this we have $n=0$, so we can replace α by 1, since $\omega_2-\omega_1\in\boldsymbol{Z}_p^\times$.

Then we have $x\sim\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$, $\mathrm{Tr}(\beta)=0$, and $x^{-1}gx=\begin{pmatrix}\omega & \omega\beta-\beta\omega\\ 0 & \omega\end{pmatrix}$. We write $\beta=\begin{pmatrix}r & s\\ t & -r\end{pmatrix}$, and see $\omega\beta-\beta\omega=\begin{pmatrix}0 & -(\omega_2-\omega_1)s\\ (\omega_2-\omega_1)t & 0\end{pmatrix}\in O_p$, hence $s,\ t\in \boldsymbol{Z}_p$. Thus we have $x\sim\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1_2 & \begin{pmatrix}r & 0\\ 0 & -r\end{pmatrix}\\ 0 & 1_2\end{pmatrix}\begin{pmatrix}1_2 & \begin{pmatrix}0 & s\\ t & 0\end{pmatrix}\\ 0 & 1_2\end{pmatrix}\sim 1$.

(ii) First assume that B_p is division. We have $B_p^\times=F^\times O_p^\times\cup F^\times\pi O_p^\times$, where π is a prime element of O_p. Then, as in (i), we can reduce $x\in G_p^*$ to $\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$, or $\begin{pmatrix}\pi^{-1} & \beta\\ 1 & \pi\end{pmatrix}\sim\pi\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$. For $x=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$, we have $x^{-1}gx=\begin{pmatrix}\omega & \omega\beta-\beta\omega\\ 0 & \omega\end{pmatrix}$. We can take, as a prime element π of O_p, one such that $\pi^2=p$, $\pi\omega=\bar{\omega}\pi$, so that we can write $B_p=F+F\pi$. We write $\beta=a\rho+y\pi$, $a\in\boldsymbol{Q}_p$, $y\in F$, and see $\omega\beta-\beta\omega=y(\omega-\bar{\omega})\pi$. Therefore, if $x^{-1}gx\in U_p^*$, we have $y\in F\cap O_p=\mathcal{O}_p$, hence $x=\begin{pmatrix}1 & a\rho\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & y\pi\\ 0 & 1\end{pmatrix}\sim 1$. It is easy to see that $x\in M_p(g,\ U_p^*)$ if and only if $\pi x\in M_p(g,\ U_p^*)$, and they determine the same order of $Z(g)=M_2(F)$. So we have proved our assertions. Now assume that B_p is split. As in (i), we can start with $x=\begin{pmatrix}\bar{\alpha}^{-1} & \beta\\ 0 & \alpha\end{pmatrix}$. By Lemma 10, (ii), $\alpha=y\begin{pmatrix}1 & 0\\ 0 & p^n\end{pmatrix}u$, for some $y\in F^\times$, $u\in GL_2(\boldsymbol{Z}_p)$, so we see, by changing the notation, that $x\sim\begin{pmatrix}\bar{\alpha}^{-1} & \beta\\ 0 & \alpha\end{pmatrix}$, $\alpha=\begin{pmatrix}1 & 0\\ 0 & p^n\end{pmatrix}$. We have $x^{-1}gx=\begin{pmatrix}\bar{\alpha}\omega\bar{\alpha}^{-1} & \bar{\alpha}\omega\beta-\beta\omega\alpha\\ 0 & \alpha^{-1}\omega\alpha\end{pmatrix}$, so $n=0$, $\alpha=1$, if $x\in M_p(g,\ U_p^*)$. From this, we deduce $x\sim 1$, in the same way as above.

(iii) The case when B_p is split can be proved by exactly the same way as (ii). So we assume that B_p is division. Since $B_p^\times=F^\times O_p^\times$, we can start with $x=\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}$, $\mathrm{Tr}(\beta)=0$. If ε is as in the assertion, we can write $B_p=F+F\varepsilon$, so $\beta=a\rho+y\varepsilon$, $a\in\boldsymbol{Q}_p$, $y\in F$. Since $\begin{pmatrix}1 & a\rho\\ 0 & 1\end{pmatrix}\in Z_G(g)$, we can assume $a=0$, $\beta=y\varepsilon$. If $x\in M_p(g,\ U_p^*)$, we have as above $\omega\beta-\beta\omega=y(\omega-\bar{\omega})\varepsilon=y\rho\varepsilon\in O_p$, $y\in\rho^{-1}\mathcal{O}_p$, where $\rho=\sqrt{-3}$ is a prime element of $\mathcal{O}_p$. If $y\in\mathcal{O}_p$, then $x\in U_p^*$, $x\sim 1$. So we assume $y=\rho^{-1}u$, $u\in\mathcal{O}_p^\times$. Then we can write $u=av^2$, $a\in\boldsymbol{Z}_p^\times$, $v\in\mathcal{O}_p^\times$, since $\mathcal{O}_p^\times=\boldsymbol{Z}_p^\times(\mathcal{O}_p^\times)^2$. We have $x=\begin{pmatrix}1 & av^2\rho^{-1}\varepsilon\\ 0 & 1\end{pmatrix}=\begin{pmatrix}av & 0\\ 0 & \bar{v}^{-1}\end{pmatrix}\begin{pmatrix}1 & \rho^{-1}\varepsilon\\ 0 & 1\end{pmatrix}\begin{pmatrix}a^{-1}v^{-1} & 0\\ 0 & \bar{v}\end{pmatrix}\sim\begin{pmatrix}1 & \rho^{-1}\varepsilon\\ 0 & 1\end{pmatrix}$. If $x=1$,

then $\Lambda_1=Z(g)_p\cap M_2(O_p)=M_2(\mathcal{O}_p)$, and $\Lambda_{10}=\Lambda_1\cap Z_0(g)_p=\begin{pmatrix} \boldsymbol{Z}_p & \rho\boldsymbol{Z}_p \\ \rho\boldsymbol{Z}_p & \boldsymbol{Z}_p \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}^{-1}$ $\begin{pmatrix} \boldsymbol{Z}_p & \boldsymbol{Z}_p \\ 3\boldsymbol{Z}_p & \boldsymbol{Z}_p \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}$, and so, by taking $\Lambda_{10,\max}=\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}^{-1} M_2(\boldsymbol{Z}_p)\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}$, we see $d_p(\Lambda_1)=4$, $e_p(\Lambda_1)=2$: in fact, we have $\Lambda_1^\times\cap G_p^*=\Lambda_{10}^\times\cdot\mathcal{O}_p^\times\cup\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\Lambda_{10}^\times\cdot\mathcal{O}_p^\times$. In the same way, we have $\Lambda_2=Z(g)_p\cap\begin{pmatrix} 1 & \rho^{-1}\varepsilon \\ 0 & 1 \end{pmatrix}M_2(O_p)\begin{pmatrix} 0 & \rho^{-1}\varepsilon \\ 1 & 1 \end{pmatrix}^{-1}=\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}$ $\left\{\begin{pmatrix} s & t \\ r & w \end{pmatrix}\in M_2(\mathcal{O}_p);\ s\equiv\bar{w},\ r\equiv-\bar{t}\ (\mathrm{mod.}\ (\rho))\right\}\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}^{-1}$, and so $\Lambda_{20}=\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}$ $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in M_2(\boldsymbol{Z}_p);\ a\equiv d,\ b\equiv-c\ (\mathrm{mod.}\ 3)\right\}\begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix}^{-1}$. From this, we see easily $d_p(\Lambda_2)=6$, $e_p(\Lambda_2)=1$.

(iii)′ We omit the proof in this case, since it can be proved in the same way as in (iii). q. e. d.

Secondly we assume that $Z_0(g)$ is division. In this case, the representative of the conjugacy class which is p-integral does not take a simple form, so we work again in G_p, if $\boldsymbol{Q}_p[g]$ is a field. Let $\omega\in O_p$ be as above, and $F=\boldsymbol{Q}_p(\omega)$. If $\left(\frac{F}{p}\right)=-1$, we take $\eta\in O_p$ such that $N(\eta)=-\eta^2=-p$, and $\eta\omega=\bar{\omega}\eta$. Then we can take $g=\begin{pmatrix} \omega & 0 \\ 0 & \eta^{-1}\omega\eta \end{pmatrix}=\begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}$, and see $Z(g)=h^{-1}M_2(F)h$, $h=\begin{pmatrix} 1 & 0 \\ 0 & \eta \end{pmatrix}$, $Z_0(g)$ $=\left\{\begin{pmatrix} x & \bar{y}\eta \\ \eta y & x \end{pmatrix};\ x,\ y\in F\right\}$. If $\left(\frac{F}{p}\right)=0$, we can take $g=\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$, and see $Z(g)=$ $M_2(F)$, $Z_0(g)=\left\{\begin{pmatrix} x & \bar{y} \\ -y & \bar{x} \end{pmatrix};\ x,\ y\in F\right\}$. If $\left(\frac{F}{p}\right)=1$, then we take $g=\begin{pmatrix} \omega_1 & 0 \\ 0 & \omega_2 \end{pmatrix}\in G_p^*$ as in Prop. 15.

PROPOSITION 16. *Notations being as above, we have*:

(i) *If* $\left(\frac{F}{p}\right)=1$,

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim Z(g)_p\cap M_2(O_p), \\ 0\cdots \textit{otherwise}, \end{cases}$$

$d_p(\Lambda_p)=e_p(\Lambda_p)=1$ *for* $\Lambda_p=Z(g)_p\cap M_2(O_p)$.

(ii) *If* $\left(\frac{F}{p}\right)=-1$, *then* B_p *is division, and*

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim Z(g)_p\cap M_2(O_p), \\ 0\cdots \textit{otherwise,}\end{cases}$$

$d_p(\Lambda_p)=e_p(\Lambda_p)=1$ *for* $\Lambda_p=Z(g)_p\cap M_2(O_p)$.

(iii) *If* $\left(\frac{F}{p}\right)=0$ *and* $F=\boldsymbol{Q}_p(\sqrt{-3})$, $(p=3)$

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim Z(g)_p\cap M_2(O_p), \\ 0\cdots \textit{otherwise,}\end{cases}$$

$d_p(\Lambda_p)=1$, $e_p(\Lambda_p)=2$ *for* $\Lambda_p=Z(g)_p\cap M_2(O_p)$.

(iii)′ *If* $\left(\frac{F}{p}\right)=0$ *and* $F=\boldsymbol{Q}_p(\sqrt{-1})$, $(p=2)$

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p\sim Z(g)_p\cap M_2(O_p)=\Lambda_1, \\ 1\cdots \textit{if } \Lambda_p\sim Z(g)_p\cap \begin{pmatrix}1 & \varepsilon\\ \varepsilon & 1\end{pmatrix}M_2(O_p)\begin{pmatrix}1 & \varepsilon\\ \varepsilon & 1\end{pmatrix}^{-1}=\Lambda_2, \\ \quad \textit{and } B_p=\textit{division}, \\ 0\cdots \textit{otherwise.}\end{cases}$$

$d_p(\Lambda_1)=3$, $e_p(\Lambda_1)=2$, $d_p(\Lambda_2)=e_p(\Lambda_2)=1$,

where ε *is an element of* O_p *such that* $\varepsilon^2=-1$, $\varepsilon\omega=-\omega\varepsilon$.

We omit the proof of this proposition, since it can be proved in the same way as Prop. 15.

4-4. Here, we quote a theorem of Chevalley(-Hasse-Noether) from Chevalley [3]. Let k be a local field of characteristic 0, and let B be a division algebra, central over k. We consider a commutative semisimple algebra Z over k, which is contained in $K=M_{n'}(B)$ and maximal in K. Let O, $\mathcal{O}_Z$ be maximal orders of K, Z, respectively such that $O\supset\mathcal{O}_Z$. We call a right O-ideal A "optimal to $\mathcal{O}_Z$", if the left order of A contains $\mathcal{O}_Z$, i.e. if $\mathcal{O}_ZA\subset A$.

We note that, we can write $A=aO$, $a\in K^\times$, and that A being optimal to $\mathcal{O}_Z$ is equivalent to $Z\cap aOa^{-1}=\mathcal{O}_Z$. Thus the classification of the optimal embeddings of $\mathcal{O}_Z$ to O is equivalent to the determination of all right O-ideals optimal to $\mathcal{O}_Z$, which has been solved in Chevalley [3].

Following Chevalley [3], we can reduce the problem to the case where Z is a maximal commutative field in $K=M_{n'}(B)$. In fact, Z is a direct sum of fields: $Z=Z_1\oplus\cdots\oplus Z_g$. We write the orthogonal idempotents corresponding to the decomposition of Z by $e^{(1)}, \cdots, e^{(g)}$. Then we have:

LEMMA 12. (Chevalley [3]) (i) *If A is a right O-ideal, optimal to $\mathcal{O}_Z$, then*

$A_i=e^{(i)}Ae^{(i)}$ is an optimal right $O_i=e^{(i)}Oe^{(i)}$-ideal to $\mathfrak{O}_{Z_i}$ for $i=1, \cdots, g$, and vice versa.

Now we assume that Z is a maximal commutative field in K. We denote by d, e, the relative degree, and the ramification index of Z/k, respectively. We write $[B: k]=\rho^2$, $\delta=(d, \rho)=g\cdot c\cdot d$. of d, ρ. Then B contains the unramified extension of degree ρ, Z contains the unramified extension of degree d over k. We may assume, by applying an inner automorphism of $K^\times$, that

$$L=\left\{\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}\in K;\ a\in B\right\}\cap(\text{the unramified extension of } k \text{ of degree } d)$$

is the unramified extension of k of degree δ. Moreover we may assume that $\mathfrak{O}_Z\subset M_{n'}(O_B)=O$. Let k_ρ be the unramified extension of degree ρ over k and O_ρ its ring of integers. Then $K\otimes_k k_\rho$ is isomorphic to $M_n(k_\rho)$, where we put $n=n'\rho$. We can assume, by taking a suitable isomorphism, that O is contained in $M_n(O_\rho)$, and a prime element π of O_B has the form $\begin{pmatrix} \bar{\pi} & & 0 \\ & \ddots & \\ 0 & & \bar{\pi} \end{pmatrix}$, $\bar{\pi}=\begin{pmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & & & 1 \\ p & 0 & \cdots & 0 \end{pmatrix}\in M_\rho(O_\rho)$, and that an element ω of the unramified extension contained in B has the form $\begin{pmatrix} \bar{\omega} & & 0 \\ & \ddots & \\ 0 & & \bar{\omega} \end{pmatrix}$, $\bar{\omega}=\begin{pmatrix} \omega & & 0 \\ & \ddots & \\ 0 & & \sigma^{\rho-1}(\omega) \end{pmatrix}\in M_\rho(k_\rho)$, where σ is a generator of $\mathrm{Gal}(k_\rho/k)$. Then $Z\otimes_k k_\rho$ decomposes into a sum of fields $Z_1\oplus\cdots\oplus Z_\delta$, and the corresponding orthogonal idempotents has the form

$$e_i=\begin{pmatrix} \bar{e}_i & & 0 \\ & \ddots & \\ 0 & & \bar{e}_i \end{pmatrix},\quad \bar{e}_i=\begin{pmatrix} 0 & & & & 0 \\ & \ddots & & & \\ & & 0 & & \\ \cdots & \cdots & 1 & \cdots & \cdots \\ & & & 0 & \\ & & & & \ddots \\ 0 & & & & 0 \end{pmatrix}\begin{matrix} \\ \\ \\ \overset{i}{\smile} \\ \\ \\ \\ \end{matrix}.$$

LEMMA 12. (Chevalley [3]) *Notations and assumptions being as above, the necessary and sufficient condition for an O-ideal A to be optimal to $\mathfrak{O}_Z$ is:*

(ii) *$A'=AM_n(O_\rho)$ is of the form $\bigoplus_{i=1}^{\delta} P^{x_i}e_iM_n(O_\rho)$,*

where P is the prime ideal of $\mathfrak{O}_Z$ and $x_i\in\boldsymbol{Z}$, $x_1\leqq x_2\leqq\cdots\leqq x_\delta$, and $x_\delta-x_1\leqq n'\delta/d$. In particular,

(iii) *if $\delta=1$, (ii) is equivalent to: $A=P^aO$, $a\in\boldsymbol{Z}$.*

(iv) *if $d=n'\delta$, (ii) is equivalent to: $A=\mathfrak{p}^a$, where $\mathfrak{p}$ is the prime ideal of O and $a\in\boldsymbol{Z}$.*

4-5. Now we assume that $g\in G$ belong to the case (V) in (14). Then $\boldsymbol{Q}[g]=F_1\oplus F_2$, F_i being imaginary quadratic fields contained in B. First we consider the case $F_{1p}\neq F_{2p}$. Then, by the result of §2, all elements in G_p having the same principal polynomial as g are conjugate in G_p to g. We can take $g=\begin{pmatrix}\omega_1 & 0\\ 0 & \omega_2\end{pmatrix}$ as a representative, where $\omega_i\in\mathcal{O}_i$, $\mathcal{O}_i$ being the ring of integers in F_i. We assume that $\boldsymbol{Z}_p[g]=\mathcal{O}_{1p}\oplus\mathcal{O}_{2p}$. If g is of finite order, this assumption is satisfied (when $F_{1p}\neq F_{2p}$).

PROPOSITION 17. *Notations being as above, we have*:

(i) *If* $\left(\frac{F_1}{p}\right)=1$, $\left(\frac{F_2}{p}\right)=-1$, *then* B_p *is split and*

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases}1\cdots \textit{if } \Lambda_p=\mathcal{O}_{1p}\oplus\mathcal{O}_{2p},\\ 0\cdots \textit{otherwise.}\end{cases}$$

(ii) *If* $\left(\frac{F_1}{p}\right)=0$, $\left(\frac{F_2}{p}\right)=-1$,

$$c_p(g,\ M_2(O_p),\ \Lambda_p)=\begin{cases}2\cdots \textit{if } \Lambda_p=\mathcal{O}_{1p}\oplus\mathcal{O}_{2p} \textit{ and } B_p=\textit{division},\\ 1\cdots \textit{if } \Lambda_p=\mathcal{O}_{1p}\oplus\mathcal{O}_{2p}, \textit{ and } B_p=\textit{split},\\ 0\cdots \textit{otherwise.}\end{cases}$$

PROOF. We prove only (ii), since (i) is easier. We note that if $M_p(g, M_2(O_p), \Lambda_p)\neq\varnothing$, then we have $g\in\Lambda_p$. So by the assumption, $c_p(g, M_2(O_p), \Lambda_p)\neq\varnothing$ only for $\Lambda_p=\mathcal{O}_{1p}\oplus\mathcal{O}_{2p}$. Then we can apply the theorem of Chevalley: $x\in M_p(g, M_2(O_p), \Lambda_p)$ if and only if $xM_2(O_p)$ is a right $M_2(O_p)$-ideal, optimal to Λ_p. If B_p is split, we see that, for F_1, $\rho=1$, $n'=2$, $d=1$, $\delta=1$, and for F_2, $\rho=1$, $n'=2$, $d=2$, $\delta=1$, in the notation of lemma 12. Then x can be written as $x=\begin{pmatrix}\pi^{e_1} & 0\\ 0 & p^{e_2}\end{pmatrix}\varepsilon$, $\varepsilon\in GL_2(O_p)$, where π is a prime element of F_{1p}. Since $x\in G_p$, we have $xx^*=a\in\boldsymbol{Q}_p^\times$, $a\begin{pmatrix}N\pi^{-e_1} & 0\\ 0 & p^{-2e_2}\end{pmatrix}=\varepsilon\varepsilon^*\in GL_2(O_p)$. It follows that $e_1=2e_2$, and $x\sim p^{-e_2}xU_p$, so $x\sim 1$. Next assume that B_p is division. Then we see that for F_1, $\rho=2$, $n'=1$, $d=1$, $\delta=1$, and for F_2, $\rho=2$, $n'=1$, $d=2$, $\delta=2$. By Lemma 12, we can write $x=\begin{pmatrix}\pi^{e_1} & 0\\ 0 & \pi^{e_2}\end{pmatrix}\varepsilon$, $\varepsilon\in GL_2(O_p)$, where π is a prime element of F_{1p} (and B_p). Since $x\in G_p$, we have

$$a\begin{pmatrix}N\pi^{-e_1} & 0\\ 0 & N\pi^{-e_2}\end{pmatrix}=\varepsilon\varepsilon^*\in GL_2(O_p),\quad a\in\boldsymbol{Q}_p^\times.$$

So we have $e_1=e_2$, and $x\sim 1$, or π. If $\pi\sim 1$, we can write $\pi=\begin{pmatrix}c & 0\\ 0 & d\end{pmatrix}u$, $u\in U_p$,

$c\in F_{1p}^{\times}$, $d\in F_{2p}^{\times}$. Then $N\pi\cdot\begin{pmatrix} Nc^{-1} & 0 \\ 0 & Nd^{-1}\end{pmatrix}=uu^{*}\in \boldsymbol{Z}_p^{\times}$, which is impossible, since F_{2p} is unramified. So we have $M_p(g, M_2(O_p), \Lambda_p)=Z_G(g)\cdot\{1, \pi\}\cdot U_p$, and $c_p(g, M_2(O_p), \Lambda_p)=2$, for $\Lambda_p=\mathcal{O}_{1p}\oplus\mathcal{O}_{2p}$. This proves (ii). q. e. d.

We omit the case when both F_{1p} and F_{2p} ramify, which does not appear if g is of finite order.

Next we consider the case $F_{1p}\cong F_{2p}$ $(=F_p)$. In this case, there are two G_p-conjugacy classes for each principal polynomial, except for the case $F_p=\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p$. If we take, as one of the representative of the conjugacy classes, $g_1=\begin{pmatrix}\omega_1 & 0 \\ 0 & \omega_2\end{pmatrix}$, $\omega_i\in\mathcal{O}_i$, then the other can be taken as $g_2=\begin{pmatrix}\omega_1 & 0 \\ 0 & a^{-1}\omega_2 a\end{pmatrix}$, where $a\in B_p^{\times}$ is any element of $B_p^{\times}$ such that $N(a)\notin N_{F_p/\boldsymbol{Q}_p}(F_p^{\times})$. We assume that $g\in G$ is of finite order.

PROPOSITION 18. *Notation being as above, we have*:

(i) *If* $\left(\frac{F_p}{p}\right)=1$.

$$c_p(g, M_2(O_p), \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p=\mathcal{O}_p\oplus\mathcal{O}_p, \\ 0\cdots \textit{otherwise.}\end{cases}$$

(ii) *If* $\left(\frac{F_p}{p}\right)=-1$, *and* $p\neq 2$,

$$c_p(g_1, M_2(O_p), \Lambda_p)=\begin{cases} 2\cdots \textit{if } \Lambda_p=\mathcal{O}_p\oplus\mathcal{O}_p \textit{ and } B_p=\textit{division}, \\ 1\cdots \textit{if } \Lambda_p=\mathcal{O}_p\oplus\mathcal{O}_p \textit{ and } B_p=\textit{split}, \\ 0\cdots \textit{otherwise},\end{cases}$$

$$c_p(g_2, M_2(O_p), \Lambda_p)=\begin{cases} c_p(g_1, M_2(O_p), \Lambda_p)\cdots \textit{if } B_p=\textit{division}, \\ 0 \qquad\qquad\qquad\quad \cdots \textit{if } B_p=\textit{split}.\end{cases}$$

(iii) *If* $\left(\frac{F_p}{p}\right)=-1$, *and* $p=2$.

$$c_p(g_1, M_2(O_p), \Lambda_p)=\begin{cases} 2\cdots \textit{if } \Lambda_p=\mathcal{O}_p\oplus\mathcal{O}_p \textit{ and } B_p=\textit{division}, \\ 2\cdots \textit{if } \Lambda_p=\Lambda(1)_p \textit{ and } B_p=\textit{division}, \\ 1\cdots \textit{if } \Lambda_p=\mathcal{O}_p\oplus\mathcal{O}_p \textit{ and } B_p=\textit{split}, \\ 1\cdots \textit{if } \Lambda_p=\Lambda(1)_p \textit{ and } B_p=\textit{split}, \\ 0\cdots \textit{otherwise},\end{cases}$$

$$c_p(g_2, M_2(O_p), \Lambda_p)=\begin{cases} c_p(g_1, M_2(O_p), \Lambda_p)\cdots \textit{if } \Lambda_p=\mathcal{O}_p\oplus\mathcal{O}_p \textit{ and } B_p=\textit{division}, \\ 0 \qquad\qquad\qquad\quad \cdots \textit{otherwise},\end{cases}$$

where $\Lambda(1)_p=\{(x, y)\in\mathcal{O}_p\oplus\mathcal{O}_p\,;\ x\equiv y \pmod{p}\}$.

(iv) *If* $\left(\frac{F_p}{p}\right)=0$,

$$c_p(g_i,\ M_2(O_p),\ \Lambda_p)=\begin{cases} 1\cdots \textit{if } \Lambda_p=\mathfrak{O}_p\oplus\mathfrak{O}_p, \\ 0\cdots \textit{otherwise.} \end{cases} \quad \textit{for } i=1,\ 2.$$

PROOF. If Λ_p is maximal in $Z(g)_p$, then we proceed in the same way as in Prop. 17, making use of the theorem of Chevalley. Since $g\in G$ is of finite order, we see that $\boldsymbol{Z}_p[g]$ is not maximal only if $F_1=F_2=\boldsymbol{Q}(\sqrt{-3})$ and $p=2$. In this case we proceed as in Prop. 14, 15. We omit the details. q. e. d.

4-6. Finally, we assume that $g\in G$ belong to the case (VI) in (14). If g is of finite order, its order is either 5, 10, 8, or 12, since the principal polynomial of g has degree 4. As in §2, we write $F=\boldsymbol{Q}[g]$, $F_0=\boldsymbol{Q}[g+g^*]$. Then the number of the conjugacy classes of the elements in G_p, having the same principal polynomial, is equal to $[F_{0p}^{\times}:\boldsymbol{Q}_p^{\times}N_{F/F_0}(F_p^{\times})]$ which is 1 or 2. We note also that $\boldsymbol{Z}_p[g]$ is always maximal in F_p, if g is of finite order. Therefore, $c_p(g,\ M_2(O_p),\ \Lambda_p)=0$ for $\Lambda_p\neq\mathfrak{O}_{F_p}=\boldsymbol{Z}_p[g]$. In the following propositions, we shall use the simplified notations:

$$t=[F_{0p}^{\times}:\boldsymbol{Q}_p^{\times}N_{F/F_0}(F_p^{\times})],\ c_p(g)=c_p(g,\ M_2(O_p),\ \boldsymbol{Z}_p[g]).$$

First we treat the case where g has order 5 or 10.

PROPOSITION 19. *Notation being as above, we have*:

(i) *If* $p\equiv 1$ (mod. 5), *then* $B_p=$*split*, $t=1$, *and* $c_p(g)=1$.

(ii) *If* $p\equiv 2,\ 3$ (mod. 5), *then* $t=1$, *and*

$$c_p(g)=\begin{cases} 1\cdots \textit{if } B_p=\textit{split}, \\ 0\cdots \textit{if } B_p=\textit{division}. \end{cases}$$

(iii) *If* $p\equiv 4$ (mod. 5), *then* $t=2$, *and*

$$c_p(g_1)=\begin{cases} 1 \\ 2 \end{cases},\quad c_p(g_2)=\begin{cases} 0\cdots \textit{if } B_p=\textit{split}, \\ 2\cdots \textit{if } B_p=\textit{division}. \end{cases}$$

(iv) *If* $p=5$, *then* $t=1$, *and* $c_p(g)=1$.

PROOF. (i) Since $F_p=\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p$, $F_{0p}=\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p$, we have $t=[(\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p)^{\times}:(\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p)^{\times}]=1$, and we can take

$$g=\begin{pmatrix} \omega_1 & & & 0 \\ & \omega_2 & & \\ & & \omega_3 & \\ 0 & & & \omega_4 \end{pmatrix},\quad \omega_i\in Q_p,\quad \omega_1\omega_2=\omega_3\omega_4\,.$$

By the theorem of Chevalley (Lemma 12), any $x\in M_p(g, U_p)$ can be written as

$$x=a\begin{pmatrix} p^{e_1} & & & 0 \\ & p^{e_2} & & \\ & & p^{e_3} & \\ 0 & & & p^{e_4} \end{pmatrix}\varepsilon, \quad a\in Q_p^\times, \quad \varepsilon\in GL_2(O_p).$$

Then since $x\in G_p$, we have

$$b\begin{pmatrix} p^{-(e_1+e_2)} & & & 0 \\ & p^{-(e_1+e_2)} & & \\ & & p^{-(e_3+e_4)} & \\ 0 & & & p^{-(e_3+e_4)} \end{pmatrix}=\varepsilon\varepsilon^*\in GL_2(O_p), \quad b\in Q_p^\times$$

so $e_1+e_2=e_3+e_4=\mathrm{ord}_p(b)$. Therefore $x\in Z_G(g)U_p$, $x\sim 1$.

(ii) F_p is the unramified extension of degree 4 over $\boldsymbol{Q}_p$. So we have $t=[F_{op}^\times : F_{op}^\times]=1$, since $\boldsymbol{Q}_p^\times N_{F/F_0}(F_p^\times)=F_{op}^\times$. We assume first that B_p is split. Then we have, $\rho=1$, $\delta=1$, in the notation of Lemma 12. So any $x\in M_p(g, U_p)$ can be written as $x=\pi^e\cdot\varepsilon$, $\varepsilon\in GL_2(O_p)$, where π is a prime element of F_{op}. Then $n(x)N_{F/F_0}(\pi)^{-e}=\varepsilon\varepsilon^*\in GL_2(O_p)\cap F_{op}=\mathcal{O}_{F_0}^\times$. Since F_p/F_{op} is unramified, we have $\mathcal{O}_{F_0}^\times=N_{F/F_0}(\mathcal{O}_{F_p}^\times)$, $\varepsilon\varepsilon^*=N_{F/F_0}(a)$ for some $a\in\mathcal{O}_{F_p}^\times$. Then $a^{-1}\varepsilon\in U_p$, so $x=(\pi^e a)(a^{-1}\varepsilon)\in Z_G(g)U_p$, $x\sim 1$. Now we assume that B_p=division. We shall show that the conjugacy class of g is not p-integral. We take a prime element π of O_p such that $\pi a=\bar{a}\pi$ for all $a\in F_{op}$. We take $\omega\in O_p$ which has the same principal polynomial over $\boldsymbol{Q}_p$ (in B_p) as $g+g^*\in F_0$, and put $\zeta=\begin{pmatrix} 0 & -1 \\ 1 & \omega \end{pmatrix}$. Then ζ has the same principal polynomial as g, so we can write $g=x^{-1}\zeta x$ for some $x\in GL(B_p)$. It is easy to see that $b\in G_p\Leftrightarrow xx^*=\begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix}\pi^{-1}$ for some $a\in\boldsymbol{Q}_p(\omega)\cong F_{op}$. If $g\in M_2(O_p)$, then $xM_2(O_p)$ is an optimal $M_2(O_p)$-ideal to $\boldsymbol{Z}_p[\zeta]$, and we can apply the theorem of Chevalley: $\rho=n'=2$, $d=4$, $\delta=(2, 4)=2$, so $n'\delta=d$ in the notation of Lemma 12, and x can be written as $x=\pi^e\varepsilon_1=\varepsilon\pi^e$, ε_1, $\varepsilon\in GL_2(O_p)$, since (π) is two-sided. Then we have $\varepsilon\varepsilon^*=\begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix}N(\pi)^{-e}\pi^{-1}\in GL_2(O_p)$, which is impossible, since $F_{op}=\boldsymbol{Q}_p(\omega)$ is unramified.

(iii) We have $F_{op}\cong\boldsymbol{Q}_p\oplus\boldsymbol{Q}_p$, and $F_p\cong K_p\oplus K_p$, where K_p is the unramified quadratic extension of $\boldsymbol{Q}_p$. The principal polynomial of g splits as $f(x)=(x^2+ax+1)(x^2+bx+1)$, $a, b\in\boldsymbol{Q}_p$. Therefore our assertion can be reduced to the case where g belongs to the case (V) (Prop. 18). We omit the details.

(iv) We can preceed in the same way as in (ii), so we omit the details. q. e. d.

Now we assume that g has order 8, or 12. Then $F=\boldsymbol{Q}[g]$ is an abelian extension of type (2,2) of $\boldsymbol{Q}$, and it has two imaginary quadratic subfields F_1, F_2:

$F_1=\boldsymbol{Q}(\sqrt{-1})$, $F_2=\boldsymbol{Q}(\sqrt{-2})$ if g has order 8, and $F_1=\boldsymbol{Q}(\sqrt{-1})$, $F_2=\boldsymbol{Q}(\sqrt{-3})$ if g has order 12. As we have seen in § 2, they correspond to the quaternion algebra $Z_0(h_1)$, $Z_0(h_2)$ over $\boldsymbol{Q}$, where h_i denote a generator of F_i. In the following two propositions, we shall give the structure of $Z_0(h_i)_p$ which will be necessary in § 5.

PROPOSITION 20. *Assume that g has order* 8.

(i) *If* $p\equiv 1 \pmod 8$, *then* $B_p=split$, $t=1$, $c_p(g)=1$, *and* $Z_0(h_1)_p=split$, $Z_0(h_2)_p=split$.

(ii) *If* $p\equiv 3 \pmod 8$, *then* $t=1$, *and* $c_p(g)=1$ (*resp.* 2), $Z_0(h_1)_p=split$, $Z_0(h_2)_p=split$ (*resp. division*) *if* $B_p=split$ (*resp. division*).

(iii) *If* $p\equiv 5 \pmod 8$, *then* $t=1$, *and* $c_p(g)=1$ (*resp.* 2), $Z_0(h_1)_p=split$ (*resp. division*), $Z_0(h_2)_p=split$, *if* $B_p=split$ (*resp. division*).

(iv) *If* $p\equiv 7 \pmod 8$, *then* $t=2$, *and we denote by* g, g' *the two representatives of the conjugacy classes in* G_p. *Then we have*:

$$c_p(g)=\begin{cases}1\\2\end{cases},\quad Z_0(h_1)_p=\begin{cases}+1\\+1\end{cases},\quad Z_0(h_2)_p=\begin{cases}+1\cdots \text{if } B_p=+1\\-1\cdots \text{if } B_p=-1,\end{cases}$$

$$c_p(g')=\begin{cases}0\\2\end{cases},\quad Z_0(h_1')=\begin{cases}-1\\-1\end{cases},\quad Z_0(h_2')=\begin{cases}-1\cdots \text{if } B_p=+1\\+1\cdots \text{if } B_p=-1.\end{cases}$$

(v) *If* $p=2$, *then* $t=2$, *and we have*:

$$c_p(g)=\begin{cases}1\\1\end{cases},\quad Z_0(h_1)_p=\begin{cases}+1\\+1\end{cases},\quad Z_0(h_2)_p=\begin{cases}-1\cdots \text{if } B_p=+1\\+1\cdots \text{if } B_p=-1,\end{cases}$$

$$c_p(g')=\begin{cases}1\\1\end{cases},\quad Z_0(h_1')_p=\begin{cases}-1\\-1\end{cases},\quad Z_0(h_2')_p=\begin{cases}+1\cdots \text{if } B_p=+1\\-1\cdots \text{if } B_p=-1\end{cases}$$

where, for simplicity, we write $B_p=+1$ (*resp.* -1) *is* B_p *is split* (*resp. division*), *and similarly for* $Z_0(h_i)_p$.

PROPOSITION 21. *Assume that g has order* 12.

(i) *If* $p=1 \pmod{12}$, *then* $B_p=split$, $t=1$, $c_p(g)=1$, $Z_0(h_1)_p=split$, $Z_0(h_2)_p=split$.

(ii) *If* $p\equiv 5 \pmod{12}$, *then* $t=1$, *and* $c_p(g)=1$ (*resp.* 2), $Z_0(h_1)_p=split$ (*resp. division*), $Z_0(h_2)_p=split$, *if* $B_p=split$ (*resp. division*).

(iii) *If* $p\equiv 7 \pmod{12}$, *then* $t=1$, $c_p(g)=1$ (*resp.* 2), $Z_0(h_1)_p=split$, $Z_0(h_2)_p=split$ (*resp. division*) *if* $B_p=split$ (*resp. division*).

(iv) *If* $p\equiv 11 \pmod{12}$, *then* $t=2$, *and we denote by* g, g' *the two representatives of the conjugacy classes in* G_p. *Then we have*:

$$c_p(g)=\begin{cases}1\\2\end{cases},\quad Z_0(h_1)_p=\begin{cases}+1\\+1\end{cases},\quad Z_0(h_2)_p=\begin{cases}+1\cdots \text{if } B_p=+1\\-1\cdots \text{if } B_p=-1,\end{cases}$$

$$c_p(g')=\begin{cases}0\\2\end{cases},\quad Z_0(h_1')=\begin{cases}-1\\-1\end{cases},\quad Z_0(h_2')_p=\begin{cases}-1\cdots \textit{if } B_p=+1\\+1\cdots \textit{if } B_p=-1.\end{cases}$$

(v) *If* $p=2$, *then* $t=2$, *and we have*:

$$c_p(g)=\begin{cases}1\\2\end{cases},\quad Z_0(h_1)_p=\begin{cases}+1\\-1\end{cases},\quad Z_0(h_2)_p=\begin{cases}+1\cdots \textit{if } B_p=+1\\+1\cdots \textit{if } B_p=-1\end{cases}$$

$$c_p(g')=\begin{cases}0\\1\end{cases},\quad Z_0(h_1')_p=\begin{cases}-1\\+1\end{cases},\quad Z_0(h_2')_p=\begin{cases}-1\cdots \textit{if } B_p=+1\\-1\cdots \textit{if } B_p=-1\end{cases}$$

(iv) *If* $p=3$, *then* $t=2$, *and we have*:

$$c_p(g)=\begin{cases}1\\2\end{cases},\quad Z_0(h_1)_p=\begin{cases}+1\\+1\end{cases},\quad Z_0(h_2)_p=\begin{cases}-1\cdots \textit{if } B_p=+1\\+1\cdots \textit{if } B_p=-1,\end{cases}$$

$$c_p(g')=\begin{cases}0\\1\end{cases},\quad Z_0(h_1')_p=\begin{cases}-1\\-1\end{cases},\quad Z_0(h_2')=\begin{cases}+1\cdots \textit{if } B_p=+1\\-1\cdots \textit{if } B_p=-1.\end{cases}$$

We omit the proof of the above two propositions, since they can be proved in the same way as in Prop. 19.

§ 5. Explicit formula for the class number of the principal genus.

Gathering together all data in § 3 and § 4, we shall finally get the explicit formula for the class number of the principal genus $\mathcal{L}(O;0)$ in the quaternion hermitian space (B^2, f).

5-1. The principal polynomials of conjugacy classes that take parts in the formula of Theorem A, are the following:

$f_1(x)=(x-1)^4$, $f_1(-x)$ ....case (I)
$f_2(x)=(x-1)^2(x+1)^2$ ....case (II)
$f_3(x)=(x-1)^2(x^2+1)$, $f_3(-x)$ ....case (III)
$f_4(x)=(x-1)^2(x^2+x+1)$, $f_4(-x)$ ....case (III)
$f_5(x)=(x-1)^2(x^2-x+1)$, $f_5(-x)$ ....case (III)
$f_6(x)=(x^2+1)^2$ ....case (IV)
$f_7(x)=(x^2+x+1)^2$, $f_7(-x)$ ....case (IV)
$f_8(x)=(x^2+1)(x^2+x+1)$, $f_8(-x)$ ....case (V)
$f_9(x)=(x^2+x+1)(x^2-x+1)$ ....case (V)
$f_{10}(x)=(x^4+x^3+x^2+x+1)$, $f_{10}(-x)$ ....case (VI)
$f_{11}(x)=(x^4+1)$ ....case (VI)
$f_{12}(x)=(x^4-x^2+1)$ ....case (VI)

We denote by H_i the total contribution to the formula in Theorem A, of those conjugacy classes whose principal polynomials are of the form $f_i(\pm x)$. Note that, the contribution of g and $-g$ are equal, and $H_4=H_5$ by Prop. 14.

THEOREM 2. *The class number H of the principal genus of the positive definite binary quaternion hermitian forms over B is given by*

$$H=\sum_{i=1}^{12} H_i,$$

where H_i are as follows:

$$H_1=\frac{1}{2^6 3^2 5}\prod_{p\mid D(B)}(p-1)(p^2+1),$$

$$H_2=\frac{1}{2^6 3^2}\prod_{p\mid D(B)}(p-1)^2\times\begin{cases} 7\cdots \text{if } 2\nmid D(B),\\ 13\cdots \text{if } 2\mid D(B),\end{cases}$$

$$H_3=\frac{1}{2^4 3}\prod_{p\mid D(B)}(p-1)\left(1-\left(\frac{-1}{p}\right)\right),$$

$$H_4=H_5=\frac{1}{2^3 3^2}\prod_{p\mid D(B)}(p-1)\left(1-\left(\frac{-3}{p}\right)\right),$$

$$H_6=\sum_{D^*\mid 2D(B)}^{*}\frac{1}{2^5 3}\prod_{p\mid D^*}(p-1)\prod_{p\mid 2D/D^*}\left(1-\left(\frac{-1}{p}\right)\right)$$
$$\times\begin{cases} 3\cdots \text{if } 2\nmid D(B),\ 2\mid D^*\\ 5\cdots \text{if } 2\mid D(B),\ 2\mid D^*\\ 5\cdots \text{if } 2\nmid D(B),\ 2\nmid D^*\\ 11\cdots \text{if } 2\mid D(B),\ 2\nmid D^*,\end{cases}$$

where D^* runs through the set of divisors of $2D(B)$ which are product of odd number of primes.

$$H_7=\sum_{D^*\mid 3D(B)}^{*}\frac{1}{2^3 3^2}\prod_{p\mid D^*}(p-1)\prod_{p\mid 3D/D^*}\left(1-\left(\frac{-3}{p}\right)\right)$$
$$\times\begin{cases} 1\cdots \text{if } 3\mid D^*\\ 4\cdots \text{if } 3\nmid D(B),\ 3\nmid D^*\\ 16\cdots \text{if } 3\mid D(B),\ 3\nmid D^*,\end{cases}$$

where D^* is as in H_6.

$$H_8=\frac{1}{2^2 3}\prod_{p\mid D(B)}\left(1-\left(\frac{-1}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right)$$

$$H_9=\frac{1}{2^2 3^2}\prod_{p\mid D(B)}\left(1-\left(\frac{-3}{p}\right)\right)^2+\frac{1}{2^2 3}\prod_{\substack{p\mid D(B)\\ p\neq 2}}\left(1-\left(\frac{-3}{p}\right)\right)^2$$
$$\times\begin{cases}2\cdots \textit{if } 2\mid D(B)\\ 1\cdots \textit{if } 2\nmid D(B)\end{cases}$$

$$H_{10}=\frac{1}{10}\prod_{p\mid D(B)}2\prod_{p\in D(-1;\,5)}2\times\begin{cases}0\cdots \textit{if } \bigcup_{i=1}^{3} D(i;\,5)\neq\emptyset\\ 1\cdots \textit{if } \bigcup_{i=1}^{3} D(i;\,5)=\emptyset,\ 5\mid D(B)\\ 2\cdots \textit{otherwise,}\end{cases}$$

where we put $D(i;\,j)=\{p\mid D(B);\ p\equiv i \pmod{j}\}$.

$$H_{11}=\frac{1}{2^3}\prod_{\substack{p\mid D(B)\\ p\neq 2}}2\prod_{p\in D(-1;\,8)}2\times\begin{cases}0\cdots \textit{if } D(1;\,8)\neq\emptyset\\ 1\cdots \textit{otherwise}\end{cases}$$

$H_{12}=0$ *if* $D(1;\,12)\neq\emptyset$. *In other cases, it is as follows*:

(i) *if* $6\nmid D(B)$,

$$H_{12}=\frac{1}{2^3 3}\prod_{p\mid D(B)}2\prod_{p\in D(-1;\,12)}2\times\begin{cases}0\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5,\,12)=\textit{even}\\ 1\cdots \textit{if } D(-1;\,12)\neq\emptyset\\ 2\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5,\,12)=\textit{odd}\end{cases}$$

(ii) *if* $2\nmid D(B)$, $3\mid D(B)$,

$$H_{12}=\frac{1}{2^4 3}\prod_{p\mid D(B)}2\prod_{p\in D(-1;\,12)}2\times\begin{cases}2\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5;\,12)=\textit{even}\\ 3\cdots \textit{if } D(-1;\,12)\neq\emptyset\\ 4\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5;\,12)=\textit{odd}\end{cases}$$

(iii) *if* $2\mid D(B)$, $3\nmid D(B)$,

$$H_{12}=\frac{1}{2^4 3}\prod_{p\mid D(B)}2\prod_{p\in D(-1;\,12)}2\times\begin{cases}4\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5;\,12)=\textit{even}\\ 3\cdots \textit{if } D(-1;\,12)\neq\emptyset\\ 2\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5;\,12)=\textit{odd}\end{cases}$$

(iv) *if* $6\mid D(B)$,

$$H_{12}=\frac{1}{2^5 3}\prod_{p\mid D(B)}2\prod_{p\in D(-1;\,12)}2\times\begin{cases}10\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5;\,12)=\textit{even}\\ 9\cdots \textit{if } D(-1;\,12)\neq\emptyset\\ 8\cdots \textit{if } D(-1;\,12)=\emptyset,\ \sharp D(5;\,12)=\textit{odd}\end{cases}$$

(*The formula for* $D(B)=$*prime has been reproduced in Introduction*).

5-2. PROOF OF THEOREM 2.

H_1: The formula for H_1 is a direct consequence of Prop. 9 and Remark 2.

H_2: We see from Prop. 13, that the G-genera which appear are $L_G(\Lambda_i)$, $i=1, 2$: $\Lambda_{ip}=\Lambda(0)_p$ for $p\neq 2$, and $\Lambda_{1p}=\Lambda(0)_p$, $\Lambda_{2p}=\Lambda(1)_p$ for $p=2$. From theo-

rem A, we have

$$H_2=M_G(\Lambda_1)\prod_p c_p(g,\ M_2(O_p),\ \Lambda_{1p})+M_G(\Lambda_2)\prod_p c_p(g,\ M_2(O_p),\ \Lambda_{2p})$$
$$=M_G(\Lambda_1)+M_G(\Lambda_2)\,,$$

since, by Prop. 13, $c_p(\cdots)$ is always 1. Then from Prop. 10, we get our assertion.

H_3: We see from Prop. 14 that only one G-genus appears: $L_G(\Lambda)$, $\Lambda=O\oplus\mathcal{O}$. We have by Prop. 14 that $c_p(g,\ M_2(O_p),\ \Lambda_p)=1$ if B_p=split, and $=1-\left(\frac{-1}{p}\right)$ if B_p=division. Then we have by Prop. 11,

$$H_3=2M_G(\Lambda)\prod_{p\mid D(B)}\left(1-\left(\frac{-1}{p}\right)\right)=\frac{1}{48}\prod_{p\mid D(B)}\left(1-\left(\frac{-1}{p}\right)\right).$$

$H_4=H_5$: We can proceed in the same way as in H_3, and omit the details.

H_6: By Prop. 4, the set of locally integral conjugacy classes are in one to one correspondence with the set of isomorphism classes of definite quaternion algebras over $\boldsymbol{Q}$ whose discriminant divide $2D(B)$. Take one such g, $Z_0(g)$, and put $D^*=D(Z_0(g))$. From Prop. 15, 16, we see that the G-genera which appear to the contribution of $C(g)$ are:

$$L_G(\Lambda_1);\ d_2/e_2=3/2,\ L_G(\Lambda_2);\ d_2/e_2=1,\ L_G(\Lambda_3);\ d_2/e_2=3,$$
$$d_p/e_p=1 \text{ for } p\neq 2,\ \Lambda_{1p},\ \Lambda_{2p},\ \Lambda_{3p},$$

where Λ_2 appears if and only if B_2=division or $Z_0(g)_2$=split, and Λ_3 appears if and only if B_2=division, $Z_0(g)_2$=split. By the same propositions, we have $c_p(g,\ M_2(O_p),\ \Lambda_{ip})=1$ if B_p=split or $Z_0(g)_p$=division, and $c_p(\cdots)=1-\left(\frac{-1}{p}\right)$ if B_p=division and $Z_0(g)$=split. Thus the contribution of $C(g)$ is:

$$\sum_{i=1}^{3}{}^{*}M_G(\Lambda_i)\prod_p c_p(g,\ M_2(O_p),\ \Lambda_{ip})\cdot d_p(\Lambda_{ip})/e_p(\Lambda_{ip})$$
$$=\frac{1}{48}\prod_{p\mid D^*}(p-1)\prod_{\substack{p\nmid D^*\\ p\mid D(B)}}\left(1-\left(\frac{-1}{p}\right)\right)\times\begin{cases}3/2 & \cdots \text{if } 2\nmid D(B),\ 2\mid D^*\\ 3/2+1 & \cdots \text{if } 2\mid D(B),\ 2\mid D^* \text{ or } 2\nmid D(B),\ 2\nmid D^*\\ 3/2+1+3 & \cdots \text{if } 2\mid D(B),\ 2\nmid D^*,\end{cases}$$

where $\sum^*$ indicates that the term for i appears according to the remark above. This proves our assertion.

H_7: This is proved in the same way as H_6. The details are omitted.

H_8: We see from Prop. 17, 18 that for each locally integral conjugacy class, the only G-genus appears: $L_G(\Lambda)$, $\Lambda=\mathcal{O}_{F_1}\oplus\mathcal{O}_{F_2}$. Moreover, the values $c_p(g,\ M_2(O_p),\ \Lambda_p)$ are independent of the conjugacy classes in G_p, if they are integral. Therefore we have, by Prop. 17, 18,

$$H_8=2M_G(\Lambda)\sum_{C(g):\text{ locally integral}}\prod_p c_p(g_2,\ M_2(O_p),\ \Lambda_p)$$

$$=\frac{2}{24}\prod_{\substack{p\mid D(B)\\ (\frac{-1}{p})=(\frac{-3}{p})=-1}}(c_p(g_1,\ M_2(O_p),\ \Lambda_p)+c_p(g_2,\ M_2(O_p),\ \Lambda_p))\times c_2(g,\ \cdots)c_3(g,\ \cdots)$$

$$=\frac{1}{12}\prod_{p\mid D(B)}\left(1-\left(\frac{-1}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right),$$

since the map ϕ in (15), § 2 is surjective. (Note that $h(F_1)=h(F_2)=1$).

H_9: We see from Prop. 18, (iii), that two G-genera $L_G(\Lambda_1)$, $L_G(\Lambda_2)$ appear: $\Lambda_{ip}=\mathcal{O}_p\oplus\mathcal{O}_p$ for $p\neq 2$, and $\Lambda_{1p}=\mathcal{O}_p^2$, $\Lambda_{2p}=\Lambda(1)_p$ for $p=2$. For $L_G(\Lambda_1)$, we can proceed in the same way as H_8, except that the image of ϕ in (15) is now a subgroup of index 2. However, since $c_p(\cdots)$ does not depend on the conjugacy class in G_p, we have only to multiply $1/2$ to the value above. As for $L_G(\Lambda_2)$, it is easy to see that $\Lambda_2^\times\cap G=\{(x,\ y);\ x,\ y\in\mathcal{O}^\times,\ x\equiv y\ (\text{mod. } 2)\}$ has order 12, and $M_G(\Lambda_2)=1/\sharp(\Lambda_2^\times\cap G)$. Then we get our assertion.

H_{10}, H_{11}: We see from Prop. 19, 20, that $c_p(g_1)=c_p(g_2)$ if g_1, g_2 are both p-integral. Therefore we can prove our assertion in the same way as H_8 or H_{12}. So we omit the details.

H_{12}: In this case $c_p(g)$ does depend on the conjugacy class, if $p=2$ or 3, even in the assumption that they are p-integral. We have

$$H_{12}=\sum_{C(g):\text{ locally integral}}M_G(\mathcal{O}_F)\prod_p c_p(g)$$

$$=\frac{1}{12}\prod_p{}^*(c_p(g)+c_p(g')),$$

where, $\prod^*$ indicates that the product is taken over all combinations of G_p-conjugacy classes $(g'')_p$, $g''=g$ or g', such that the number of p's for which $Z_0(g_1'')_p$ =division is odd. Then we can easily get to the assertion, by distinguishing the cases according as whether $2\mid D(B)$, $3\mid D(B)$, or not. This completes the proof of Theorem 2.

As a corollary to the above investigation, we have:

COROLLARY. *The number C_i of the locally integral conjugacy classes in G whose principal polynomial is $f_i(x)$ is given as*:

$$C_1=C_2=C_3=C_4=C_5=1,$$

$$C_6=\frac{1}{2}\prod_{\substack{p\mid 2D(B)\\ (\frac{-1}{p})\neq 1}}2,\quad C_7=\frac{1}{2}\prod_{\substack{p\mid 3D(B)\\ (\frac{-3}{p})\neq 1}}2,$$

$$C_8=\prod_{p\mid D(B)}\frac{1}{2}\left(1-\left(\frac{-1}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right),$$

$$C_8=\prod_{p\mid D(B)}\frac{1}{2}\left(1-\left(\frac{-1}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right),$$

$$C_9=\prod_{p\mid D(B)}\left(1-\left(\frac{-3}{p}\right)\right)\times\begin{cases}1\cdots \textit{if } 3\nmid D(B)\\ 2\cdots \textit{if } 3\mid D(B),\end{cases}$$

$$C_{10}=\prod_{p\mid D(-1;\,5)}2\times\begin{cases}0\cdots \textit{if } \bigcup_{i=1}^{3} D(i;\,5)\neq\varnothing\\ 1\cdots \textit{otherwise,}\end{cases}$$

$$C_{11}=\prod_{p\mid D(-1;\,8)}2\times\begin{cases}0\cdots \textit{if } D(1,\,8)\neq\varnothing\\ 1\cdots \textit{otherwise,}\end{cases}$$

$$C_{12}=\frac{1}{2}\prod_{p\mid D(-1;\,12)\cup(\{2,3\}\cap D(B))}2\times\begin{cases}0\cdots \textit{if } D(1;\,12)\neq\varnothing,\ D(-1;\,12)\cup(\{2,3\}\cap D(B))=\varnothing,\ \sharp D(5;\,12)=\textit{even}\\ 2\cdots \textit{if } D(1;\,12)=\varnothing,\ \textit{and } D(-1;\,12)\cup(\{2,3\}\cap D(B))=\varnothing,\ \sharp D(5;\,12)=\textit{odd}\\ 1\cdots \textit{otherwise.}\end{cases}$$

5-3.

Numerical examples

The values of H for small discriminants are as follows:

(i) $D(B)$=prime

$D(B)$	2	3*)	5	7	11	13	17	19	23	29	31	37
H	1	1	2	2	5	4	8	10	16	24	26	37

(ii) $D(B)\neq$prime

$D(B)$	2.3.5	2.3.7	2.3.11	2.3.13	2.3.17	2.5.7	2.5.11
H	12	22	69	94	203	75	283

$D(B)$	2.5.13	3.5.7	3.5.11	3.5.13	3.7.11	5.7.11
H	432	255	1014	1601	2760	13956

REMARK 3.*) The fact that $H=1$ for $D(B)=2$ and 3 has been proved by Y. Ihara and used in [12]. He proved it in two different ways; one by using Mass formula (cf. Remark 2 in § 3), and the other by using modular forms of one variable with weight 4.

5-4. For the convenience of the later use, we give here the formula for the dimension of the space $\bigoplus_{i=1}^{H}\mathfrak{M}_i$ defined in [9], where $(\rho, \mathfrak{M})$ is the irreducible representation of $G_\infty^1=USp(2)$ corresponding to the Young diagram:

1	2	⋯	k
1	2	⋯	k

(cf. [12]).

THEOREM 3. *Let g_j, $j=1, \cdots, 12$, be any element of G having the principal polynomial $f_j(x)$. Then*

$$\dim \bigoplus_{i=1}^{H} {}_i\mathfrak{M} = \sum_{j=1}^{12} \operatorname{tr} \rho(g_j) H_j ,$$

where H_j is as in Theorem 2, and $\operatorname{tr} \rho(g_j)$ *is given as follows*:

$$\operatorname{tr} \rho(g_1) = \dim \mathfrak{M} = (k+1)(k+2)(2k+3)/6,$$

$$\operatorname{tr} \rho(g_2) = (-1)^k (k+1)(k+2)/2,$$

$$\operatorname{tr} \rho(g_3) = \frac{1}{2} \times \begin{cases} k+2 & \cdots k \equiv 0 \\ k+1 & \cdots k \equiv 1 \\ -(k+2) & \cdots k \equiv 2 \\ -(k+1) & \cdots k \equiv 3 \end{cases} \pmod 4$$

$$\operatorname{tr} \rho(g_4) = \frac{1}{3} \times \begin{cases} 2k+3 & \cdots k \equiv 0 \\ -(k+2) & \cdots k \equiv 1 \\ -(k+1) & \cdots k \equiv 2 \end{cases} \pmod 3$$

$$\operatorname{tr} \rho(g_5) = \begin{cases} 1 & \cdots k \equiv 0 \\ k+2 & \cdots k \equiv 1 \\ k+1 & \cdots k \equiv 2 \\ -1 & \cdots k \equiv 3 \\ -(k+2) & \cdots k \equiv 4 \\ -(k+1) & \cdots k \equiv 5 \end{cases} \pmod 6$$

$$\operatorname{tr} \rho(g_6) = \frac{1}{2} \times \begin{cases} k+2 & \cdots k \equiv 0 \\ k+1 & \cdots k \equiv 1 \end{cases} \pmod 2$$

$$\operatorname{tr} \rho(g_7) = \frac{1}{3} \times \begin{cases} 2k+3 & \cdots k \equiv 0 \\ 2k+4 & \cdots k \equiv 1 \\ 2k+2 & \cdots k \equiv 2 \end{cases} \pmod 3$$

$$\text{tr } \rho(g_8)=\begin{cases} 1 & \cdots k\equiv 0, 1, 2, 3 \\ 0 & \cdots k\equiv 4, 5, 10, 11 \\ -1 & \cdots k\equiv 6, 7, 8, 9 \end{cases} \quad (\text{mod. } 12)$$

$$\text{tr } \rho(g_9)=\begin{cases} 1 & \cdots k\equiv 0 \\ 0 & \cdots k\equiv 1, 2, 4, 5 \\ -1 & \cdots k\equiv 3 \end{cases} \quad (\text{mod. } 6)$$

$$\text{tr } \rho(g_{10})=\begin{cases} 1 & \cdots k\equiv 0 \\ 0 & \cdots k\equiv 1, 3, 4 \\ -1 & \cdots k\equiv 2 \end{cases} \quad (\text{mod. } 5)$$

$$\text{tr } \rho(g_{11})=\begin{cases} 1 & \cdots k\equiv 0 \\ -1 & \cdots k\equiv 1 \\ 0 & \cdots k\equiv 2, 3 \end{cases} \quad (\text{mod. } 4)$$

$$\text{tr } \rho(g_{12})=\begin{cases} 1 & \cdots k\equiv 0 \\ -2 & \cdots k\equiv 1 \\ 2 & \cdots k\equiv 2 \\ -1 & \cdots k\equiv 3 \\ 0 & \cdots k\equiv 4, 5 \end{cases} \quad (\text{mod. } 6)$$

PROOF. The first formula is a direct consequence of Theorem A. The formula for tr $\rho(g_j)$ is easily calculated by the character formula of Weyl [21].

§ 6. Concluding remarks.

6-1. Construction of maximal lattices.

We shall give a method of finding all maximal O-lattices in B^2, belonging to the principal genus $\mathfrak{L}(O\,;0)$, where O is a maximal order of B. It is well known that the class number of $M_2(B)$ is one, since the strong approximation theorem holds. Therefore any O-lattice in B^2 can be written as

$$L=(O,\ O)x\,,\quad x\in GL_2(B)\,.$$

PROPOSITION 22. (i) *$L=(O,\ O)x$ belongs to $\mathfrak{L}(O\,;0)$ if and only if x satisfies the condition*:

$$xx^*=m\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix};\quad t,\ s>0,\quad \in Z,\quad r\in O,\quad ts-N(r)=1,\quad m\in \boldsymbol{Q}^{\times}_{+}\,. \tag{30}$$

(ii) *If L is as in* (i), *then the norm $N_f(L)$ of L is $N_f(L)=mO$.*
(iii) *$L_1=(O, O)x_1$, $L_2=(O, O)x_2\in\mathcal{L}(O; 0)$ belong to the same class if and only if there exists $y\in GL_2(O)$ such that*

$$y(x_1x_1^*)y^*=nx_2x_2^*, \quad n\in\boldsymbol{Q}_+^\times. \tag{31}$$

PROOF. (i) If $L=(O, O)x\in\mathcal{L}(O; 0)$, then there exists, for each prime p, an element $g\in G_p$ such that $(O_p, O_p)x=(O_p, O_p)g$. Then $g=ux$ for some $u\in GL_2(O_p)$, and $u(xx^*)u^*=gg^*\in\boldsymbol{Q}_p^\times$, $(u^*u)^{-1}=(gg^*)^{-1}xx^*\in GL_2(O_p)$, so the condition is necessary. Sufficiency is easily shown by using Lemma 11.
(ii) It is easy to show that $N_f(L_p)=mO_p$ for all p, hence $N_f(L)=mO$. q. e. d.

We see, in particular, that if $N_f(L)=O$, then the class of $L=(O, O)x$ depends only on $\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}$. So we write,

$$L=L(t, s, r) \quad \text{for} \quad L=(O, O)x, \quad xx^*=\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}. \tag{32}$$

We note here that, if t, s, r satisfies the condition in (30), there always exists an $x\in GL_2(B)$ such that $xx^*=\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}$. Since any maximal O-lattice in $\mathcal{L}(O; 0)$ is equivalent to a maximal O-lattice with norm O, we can reduce our problem to find all representatives of the classes in $\mathcal{L}(O; 0)$, to the problem to find all $\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}$ satisfying (30), up to the equivalence by $GL_2(O)$.

LEMMA 13. (i) *The equivalence class of $\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}$ depends only on r mod s for fixed s.*
(ii) *If $a, b\in O^\times$, then $\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}$ and $\begin{pmatrix} t & arb \\ \overline{arb} & s \end{pmatrix}$ are equivalent.*
(iii) $\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}$ *and* $\begin{pmatrix} s & \bar{r} \\ r & t \end{pmatrix}$ *are equivalent.*

PROOF. (i) We have for $u\in O$, $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \bar{u} & 1 \end{pmatrix}=\begin{pmatrix} * & r+su \\ \bar{r}+s\bar{u} & s \end{pmatrix}$.
(ii) $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}\begin{pmatrix} \bar{a} & \\ & \bar{b} \end{pmatrix}=\begin{pmatrix} t & arb \\ \overline{arb} & s \end{pmatrix}$.
(iii) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} t & \bar{r} \\ r & s \end{pmatrix}$. q. e. d.

By using the basis of O over $\boldsymbol{Z}$, we can thus find all triples (t, s, r) satisfying the condition in (30), in the following steps:

1) Let $s=1, 2, 3, \cdots$
2) To each s, find all $r \in O/(sO)$ such that $N(r)+1 \equiv 0 \pmod{s}$.
3) Let $t=(N(r)+1)/s$.

We give here an example of a basis of a maximal order $O(q, c)$ which is given in [11]:

$$O(q, c)=\boldsymbol{Z}+\boldsymbol{Z}(1+\beta)/2+\boldsymbol{Z}\alpha(1+\beta)/2+\boldsymbol{Z}(c+\alpha)\beta/q\,, \tag{33}$$

where, we write $B=\boldsymbol{Q}+\boldsymbol{Q}\alpha+\boldsymbol{Q}\beta+\boldsymbol{Q}\alpha\beta$, $\alpha^2=-m=-D(B)$, $\beta^2=-q$, $\alpha\beta=-\beta\alpha$, and q, c satisfy

(i) q is a prime such that $q \equiv 3 \pmod{8}$, and $\left(\frac{-q}{p}\right)=-1$ for all primes $p \mid m$, $p \neq 2$,

(ii) $c^2+m \equiv 0 \pmod{q}$.

Examples of lattices: In the notations of (32), (33), following two lattices form a set of representatives of classes in $\mathcal{L}(O\,;\,0)$.

(i) $D(B)=5$, $H=2$, $O=O(3, 1)$;

$$L_1=L(1, 1, 0), \quad L_2=L(2, 2, 1+(1+\alpha)\beta/2).$$

(ii) $D(B)=7$, $H=2$, $O=O(11, 2)$;

$$L_1=L(1, 1, 0), \quad L_2=L(2, 2, (1+\beta)/2).$$

6-2. The relation between G and $O(5)$.

We have a natural question about how our results are connected to that of T. Asai [2], since the two grougs G^1 and $O(5)$ are isogenous.

Let (V, Q) be a quinary quadratic space over $\boldsymbol{Q}$. Assume that it is non-degenerate. Then it is well known that the even Clifford algebra $C^+(V)$ of (V, Q) is a central simple algebra over $\boldsymbol{Q}$ of degree 16, with the main involution. It is also easy to see that $C^+(V) \cong M_2(B)$ as algebras with involutions, if and only if V is similar to a quinary space spanned by an orthogonal basis $e_1, \cdots, e_5$ of the form:

$$e_1^2=mq, \quad e_2^2=m, \quad e_3^2=q, \quad e_4^2=e_5^2=1, \tag{34}$$

where m, q are as in (33). Then we see that (V, Q) is realized in $M_2(B)$, as a subspace:

$$V=\left\{\begin{pmatrix} t & r \\ \bar{r} & -t \end{pmatrix};\ t \in \boldsymbol{Q},\ r \in B,\ Q\left(\begin{pmatrix} t & r \\ \bar{r} & -t \end{pmatrix}\right)=t^2+N(r)\right\}. \tag{35}$$

Note that the discriminant of (V, Q) belongs to $(\boldsymbol{Q}^\times)^2$.

PROPOSITION 23. *Notations being as above, assume that the discriminant* $D(B)=m$ *of* B *is prime to* 2. *Then we have,*

(i) $SO(V, Q)$ *is isomorphic (as an algebraic group) to*

$$G/\boldsymbol{Q}^\times=\{g\in M_2(B);\ gg^*\in\boldsymbol{Q}^\times\}/\boldsymbol{Q}^\times=\{g\in M_2(B);\ g^{-1}Vg=V\}/\boldsymbol{Q}^\times,$$

(ii) *Let* O *be a maximal order of* B. *and put*

$$L_V=\left\{\begin{pmatrix} t & r \\ \bar{r} & -t \end{pmatrix};\ t\in Z,\ r\in O\right\}.$$

Then L_V *is a maximal lattice in* V *with reduced discriminant* $2m^2$ *in the sense of Eichler* [6].

(iii) *The number of the classes in the genus containing* L_V *is given by*:

$$T=\#(\{g^{-1}M_2(O)g;\ g\in G_A\}/\widetilde{G})=\#(L_G(M_2(O))/\widetilde{G}).$$

PROOF. (i) and (ii) are proved by direct calculations. Besides, we can show that the ring generated by L_V in $M_2(B)$ is $M_2(O)$. Then (iii) follows immediately from (i), (ii). q. e. d.

Thus the class number of the genus of L_V in (V, Q), whose explicit formula has been given in T. Asai [2], can be interpreted in our terminology as the number of G-conjugacy classes in the G-genus $L_G(M_2(O))$ of maximal orders containing $M_2(O)$ (the 'type number' of G). Note that the same relation between the type number of B and the class number of some ternary quadratic forms is well known.

Finally we give a formula, which expresses T as a sum of traces of some modified Brandt matrices. Let $L_1, \cdots, L_H$ be a complete set of representatives of the classes in the principal genus $\mathcal{L}(O; 0)$, and let R_i be the right order in $M_2(B)$ of L_i: $R_i=\{z\in M_2(B);\ L_iz\subseteq L_i\}$. For each $n\mid D(B)$, we define an element $T^*(n)$ of Hecke algebra H_Q of G:

$$T^*(n)=(T^*_{ij})_{1\le i,j\le H},$$

$$T^*_{ij}=\{g\in G;\ n(g)=n,\ gR_i=R_jg,\ L_jg\subseteq L_i\}.$$

Then we have the following formula, which can be proved by the same way as in Eichler [5], Satz 11.

PROPOSITION 24. *Let* t *be the number of the primes dividing* $D(B)$. *Then we have*

$$T=\frac{1}{2^t}\sum_{n\mid D(B)}\operatorname{tr} B^*(n),$$

where $B^*(n)$ is the modified Brandt matrix defined by $T^*(n)$ in the similar way as in [9], *with ρ: trivial.*

References

[1] Asai, T., The Conjugacy classes in the unitary, symplectic, and orthogonal groups over an algebraic number field, J. Math. Kyoto Univ. **16** (1976), 325-350.
[2] Asai, T., The class number of positive definite quadratic forms, Japan. J. Math. **3** (1977), 239-296.
[3] Chevalley, C., Sur certains idéaux d'une algèbre simple, Abh. Math. Sem. Univ. Hamburg, 1934, 83-105.
[4] Eichler, M., Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z. **43** (1938), 102-109.
[5] Eichler, M., Zur Zahlentheorie der Quaternion-Algebren, J. Reine Angew. Math. **195** (1955), 127-151.
[6] Eichler, M., Quadratische Formen und Orthogonale Gruppen, Springer-Verlag, 1952.
[7] Gelfand, L.M. and M.A. Neumark, Unitäre Darstellungen der klassischen Gruppen, Akademie-Verlag, Berlin, 1957.
[8] Hashimoto, K., On the arithmetic of the quadratic extension of quaternion algebras (in Japanese), Master thesis, Univ. of Tokyo, 1977.
[9] Hashimoto, K., On Brandt matrices associated with the positive definite quaternion hermitian forms, J. Fac. Sci. Univ. Tokyo Sect. IA, **27** (1980), 227-245.
[10] Hijikata, H., Hasse principle for the conjugacy classes of the orthogonal group (in Japanese), Reports of the symposium on algebraic groups held at Yamanaka-Kyodo-Kensyujo, 1973.
[11] Ibukiyama, T., A basis and maximal orders in quaternion algebra over the rational number field (in Japanese), Sugaku **24** (1972), 316-318.
[12] Ihara, Y., On certain arithmetical Dirichlet series, J. Math. Soc. Japan, **16** (1964), 214-235.
[13] Landherr, W., Lie Ringe vom Typus A über einem algebraischen Zahlkörper, Abh. Math. Sem. Univ. Hamburg **12** (1938), 200-241.
[14] Ramanathan, K.G., Quadratic forms over involutive division algebras, J. Indian Math. Soc., **20** (1956), 227-257.
[15] Satake, I., Theory of spherical functions on reductive algebraic groups over p-adic fields, I.H.E.S. Publ. Math. No. 18, 1963, pp. 5-69.
[16] Shimizu, H., On zeta functions of quaternion algebras, Ann. of Math. **81** (1965). 166-193.
[17] Shimura, G., Arithmetic of alternating forms and quaternion hermitian forms, J. Math. Soc. Japan **15** (1963), 33-65.
[18] Shimura, G., Arithmetic of Unitary Groups, Ann. of Math. **79** (1964), 369-409.
[19] Tamagawa, T., Adeles, Proc. Sympos. Pure Math. Vol. 9, Amer. Math. Soc., 1966, pp. 113-121.
[20] Weil, A., Adeles and algebraic groups, Lecture Notes, Institute for Advanced Study, Princeton, 1959-60.
[21] Weyl, H., Classical groups, Princeton Univ. Press, 1939.

(Received October 15, 1979)

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan