Advanced Studies in Pure Mathematics 15, 1989
Automorphic Forms and Geometry of Arithmetic Varieties
pp. 301–349

On Automorphism Groups of Positive Definite Binary Quaternion Hermitian Lattices and New Mass Formula

Tomoyoshi Ibukiyama

Dedicated to Professor Ichiro Satake on his sixtieth birthday

In this paper, we shall give some general method how to calculate the multiplicity of a given finite group which appears as the automorphism groups of the lattices, up to isometry, in a fixed genus in a positive definite metric space, and apply it to the binary quaternion hermitian cases, motivated by the theory of supersingular abelian varieties developed in Katsura-Oort [12]. Our Main Theorems are Theorems 7.1 and 7.2 in § 7. More precisely, we shall consider the following problems. Let B be either the rational number field $\boldsymbol{Q}$, an imaginary quadratic field over $\boldsymbol{Q}$, or a definite quaternion algebra over $\boldsymbol{Q}$. Let (V, h) be a pair of a finite dimensional left B-vector space V over B and a positive definite hermitian metric h on B with respect to the unique positive involution of B. Denote by $G=G(V, h)$ the group of similitudes of (V, h);

$$G=\{g \in GL_B(V);\ h(xg, yg)=n(g)h(x, y)\ (x, y \in V) \text{ for some } n(g) \in \boldsymbol{Q}^\times\}.$$

Let $\mathscr{L}$ be a fixed genus of some lattices in V.

Problem 1. Calculate the class number $H=\sharp(\mathscr{L}/G)$ of $\mathscr{L}$.

It is known that Problem 1 can be solved at least in principle by means of the trace formula (cf. Hashimoto [3]), and some explicit calculations have been done by several mathematicians. Now, our main theme in this paper is the following Problem 2. Denote by $L_1, \cdots, L_H$ a complete set of representatives of the classes in $\mathscr{L}$. For each i $(1 \leqq i \leqq H)$, put

$$\Gamma_i=\mathrm{Aut}(L_i)=\{g \in G;\ L_i g=L_i\}.$$

It is easy to see that this is a finite group for each i, because of our assumption that h is positive definite.

Received May 6, 1987.

Problem 2. Let Γ be any finite group. Count the number of classes L_i such that $\Gamma \cong \Gamma_i$.

The usual trace formula(, or its refinement in [3], [5], [6]) gives us some information also on this Problem 2. But, in general, these previously known formulae do not give us enough information to solve the above Problem 2.

In this paper, first, we give a certain new mass formula which gives us enough information to solve Problem 2 (§ 1. Theorem 1.1). This new formula is a generalization of the formula in [3] (cf. also [5], [6]), and the proof itself is obtained in a similar way. But, while the old one in [3] was more or less motivated to explain the trace formula, our new one does not appear as a summand in the usual trace formula in general. And, it does not seem to have been appreciated that such new formula should exist and be useful.

The reason why we need a new mass formula can be roughly explained as follows. We can take a certain big finite group Δ so that it acts on $\mathscr{L}/G$, and that, for each i $(1 \leqq i \leqq H)$, the subgroup of Δ consisting of all elements which stabilize the class which contains L_i is isomorphic to Γ_i. The usual trace formula is essentially the formula to give the *linear* characters of the permutation representation of Δ on $\mathscr{L}/G$ (although it might sometimes give us slightly more information). To determine each Γ_i, we need the irreducible decomposition of $(\Delta, \mathscr{L}/G)$ as a *permutation* representation. But, in general, a permutation representation *cannot* be determined by the linear representation attached to it. Our new mass formula is quite useful to fill this gap. The usual trace formula expresses some kind of masses by sum of data determined by G-conjugacy classes of elements of G. Our new mass formula expresses some kind of new masses by sum of data determined by G-conjugacy classes of elements of the *direct-product* G^r, where r is a certain natural number. By this formula, we can tell whether several elements of G are contained in a group Γ_i at the same time, or not, and this gives us a general tool in order to solve Problem 2, as we shall explain in § 1.

Secondly, we shall apply this method to some special cases. Hereafter, we shall assume that B is the definite quaternion algebra over Q with fixed prime discriminant p. We shall solve Problem 2 explicitly for arbitrary p for the (unique) non-principal genus in V in the case of $\dim_B V = 2$ (§ 7. Theorem 7.1. As for the case where the discriminant is not necessarily prime, see Theorem 7.2). When $\dim_B V = 1$, the answer to Problems 1, 2 was classically well known by Eichler [2]. When $\dim_B V = 2$, or 3, Problem 1 was solved in Hashimoto-Ibukiyama [5] and Hashimoto [4] by means of the trace formula. Our Problems 1 and 2

have also close relations to the theory of supersingular abelian varieties. For example, when $\dim_B V \geqq 2$, the class number of the principal genus in V is equal to the number of isomorphism classes of principal polarizations on E^n, where E is a supersingular elliptic curve over a field of characteristic p, p is the discriminant of B, and $n=\dim_B V$ (T. Ibukiyama-T. Katsura-F. Oort [11]). In this case, Problem 2 amounts to describe all automorphism groups of all principally polarized abelian varieties (E^n, C), where we denote by C the principal polarizations on E^n. When $n=2$, using this relation, Problem 2 was solved explicitly for all p for the principal genus in V ([11] loc. cit.). When $n=2$ and genus in question is the non-principal genus in V, another geometrical interpretation of Problems 1 and 2 was given in Katsura-Oort [12]: for any natural integer m such that $p \nmid m$, denote by $A_{2,1}(m)$ the coarse moduli space of principally polarized abelian surfaces with level m structure, and by $A_s(m)$ the locus in $A_{2,1}(m)$ of principally polarized supersingular abelian surfaces with level m structure. As shown in [12], the variety $A_s(1)$ is not irreducible in general, and the number of irreducible components of $A_s(1)$ is equal to the class number of the non-principal genus in V. In this case, if $p \neq 2$, Problem 2 amounts to give explicitly the decomposition group of each irreducible component in $A_s(2)$ for the natural covering $A_{2,1}(2) \to A_{2,1}(1)$ (which is isomorphic to the automorphism group of the Morret-Baily family in [13], [12].) Using this relation and some geometrical methods, Katsura-Oort [12] solved Problem 2 for $p \leqq 31$ in this case. Actually, they used essentially some geometrical alternatives of the usual trace (, or mass) formula, and it worked successfully for such small p. But, for general p, this does not work, and we need a new mass formula which was mentioned above. We shall solve Problem 2 for the non-principal genus in V, $\dim_B V=2$, completely for all p by a purely *number-theoretical* method. It seems to be an interesting problem to find some geometrical alternatives of our methods, or some direct geometrical interpretation of our results in this paper.

Now, we explain briefly the content of each section. In § 1, after reviewing lattices in hermitian spaces, we give general (but not explicit) new mass formula and explain how to solve Problem 2 in general, by using this formula. From § 2 until the end of this paper, we are devoted into explicit calculations in order to solve Problem 2 in the binary quaternion hermitian case. In § 2, we review the class number formula in [5] II and give some miscellaneous results obtained by that formula. In order to calculate explicit "masses" which we need, in § 3, we classify G-conjugacy classes of some elements of G^2, in § 5, we calculate some "local data", and in § 6, we give explicit "masses". This procedure is more or less similar to that of the explicit calculations of the usual trace

formula in [5], but it is more elaborate and complicated in our case. In § 4, we show that some dihedral groups cannot be isomorphic to any Γ_i $(1 \leqq i \leqq H)$, without using mass formula. The argument in this section is special to the case we are considering, but it economizes the calculations. In § 7, we gather the results in the former sections, and solve Problem 2.

The author would like to thank Professors T. Katsura and F. Oort for explaining him their problems in [12] and also for valuable conversations.

Notations. As usual, we denote by $\boldsymbol{Q}$ (resp. $\boldsymbol{Z}$) the field of rational numbers (resp. the ring of rational integers). We denote by $\boldsymbol{Q}_+$ the set of all positive rational numbers. For any algebraic group $\mathfrak{g}$ over $\boldsymbol{Q}$, we denote by $\mathfrak{g}_A$ the adelization of $\mathfrak{g}$, by $\mathfrak{g}_\infty$ (resp. $\mathfrak{g}_q$) the infinite (resp. q-adic) component of $\mathfrak{g}_A$, where q is any prime. For each prime q, we denote by $\boldsymbol{Q}_q$ (resp. $\boldsymbol{Z}_q$) the field of q-adic numbers (resp. the ring of q-adic integers), and by $\boldsymbol{F}_{q^r}$ the finite field of characteristic q with q^r elements. For any ring R, we denote by $R^\times$ the group of units of R, by $M_n(R)$ (n; natural number) the set of n by n matrices, and we put $GL_n(R) = M_n(R)^\times$. We denote by 1_n the unit matrix of $M_n(R)$, which is often denoted by $1 = 1_n$, when n is clear from the context. For any finite set S, we denote by $\sharp(S)$ the cardinality of S.

§ 1. New mass formula

1.1. First, we review on lattices in metric spaces, and formulate Problems 1, 2 in the adelic language. As in the introduction, let B be either the rational number field $\boldsymbol{Q}$, an imaginary quadratic extension of $\boldsymbol{Q}$, or a positive definite quaternion algebra over $\boldsymbol{Q}$. Let V be a finite dimensional left B-vector space. We denote by $^-$ the unique positive involution of B, which is trivial when $B = \boldsymbol{Q}$, the complex conjugation when B is imaginary quadratic, and the main involution of B when B is quaternionic. We fix a positive definite metric h on V with respect to $^-$: h is a mapping of $V \times V$ to B which satisfies the following conditions (1), (2), (3).

(1) $h(ax+by, z) = ah(x, z)+bh(y, z), \qquad (a, b \in B, x, y, z \in V),$

(2) $h(y, x) = \overline{h(x, y)} \qquad (x, y \in V),$

(3) $h(x, x) \geqq 0,$ for all $x \in V$, and
$h(x, x) = 0,$ if and only if $x = 0$.

Denote by $\mathrm{End}_B(V)$ (resp. $GL_B(V)$) the ring (resp. group) of all left B-linear endomorphisms (resp. automorphisms) of V, and by $G = G(V, h)$

the group of similitudes of (V, h):

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

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

Then, G is an algebraic group over $\boldsymbol{Q}$. We denote by G_A the adelization of G, and for any place v of $\boldsymbol{Q}$, we denote by G_v the v-component of G_A. When v is a finite prime q, we have

$$G_q=\{g \in GL_{B_q}(V_q);\ h_q(xg, yg)=n(g)h_q(x, y),\ x, y \in V_q,\ n(g) \in \boldsymbol{Q}_q^\times\}$$

where $B_q=B\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_q$, $V_q=V\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_q$ and h_q is the continuous prolongation of h to V_q. Let O be a maximal order of B. A left O-module in V is called left O-lattice, when L is a $\boldsymbol{Z}$-lattice in V (, where V is regarded as a vector space over $\boldsymbol{Q}$). Two left O-lattices L and M are said to be isomorphic, if $L=Mg$ for some $g \in G$. For each left O-lattice L and each prime p, put $L_p=L\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_p$. For a fixed left O-lattice L, the genus $\mathscr{L}(L)$ which contains L is defined to be the following set of lattices:

$$\mathscr{L}(L)=\{M \subset V:\ M \text{ is a left } O\text{-lattice such that for every prime } p,\ M_p=L_pg_p \text{ for some } g_p \in G_p\}.$$

The number $\sharp(\mathscr{L}(L)/G)$ of isomorphism classes of left O-lattices in $\mathscr{L}(L)$ is known to be finite, and called the class number of $\mathscr{L}(L)$. The class number has the following interpretation in the adelic language. For any prime p, put

$$U_p(L)=\{g \in G_p:\ L_pg=L_p\}, \quad \text{and} \quad \mathfrak{A}(L)=G_\infty \prod_p U_p(L).$$

Decompose G_A into the double cosets as follows:

$$G_A=\coprod_{i=1}^{H} \mathfrak{A}(L)g_jG \qquad \text{(disjoint)}.$$

Then, we have $H=\sharp(\mathscr{L}(L)/G)$. A complete set of representatives of classes in $\mathscr{L}(L)$ is given by $L_1, \cdots, L_H$, where

$$L_i=Lg_i=\bigcap_p (L_pg_{i,p} \cap V) \qquad (i=1, \cdots, H)$$

and $g_{i,p}$ is the p-component of $g_i \in G_A$ for each prime p. Put

$$\Gamma_i=\mathrm{Aut}\,(L_i)=\{g \in G;\ L_ig=L_i\}.$$

Then, we have $\Gamma_i=G \cap g_i^{-1}\mathfrak{A}(L)g_i$, which is a finite group.

Now, we shall explain the essential meaning of Problem 2. We

introduce some subgroup $\mathfrak{A}'$ of $\mathfrak{A}=\mathfrak{A}(L)$. Fix a prime p. It is well known that there exists a torsion-free normal subgroup U_p' of $U_p(L)$ of finite index. Put

$$\mathfrak{A}'=G_\infty U_p' \prod_{q\neq p} U_q(L) \quad \text{and} \quad \Delta=\mathfrak{A}/\mathfrak{A}'=U_p/U_p'.$$

Decompose G_A into double cosets as follows;

$$G_A=\coprod_{j=1}^{H'} \mathfrak{A}'g_j'G \qquad \text{(disjoint)}.$$

Denote by $\mathscr{L}'$ the set of H' double cosets in the above decomposition:

$$\mathscr{L}'=\{\mathfrak{A}'g_j'G;\ j=1,\ \cdots,\ H'\}.$$

Then, the finite group Δ acts on $\mathscr{L}'$ by

$$\bar{\delta}(\mathfrak{A}'g_j'G)=\delta(\mathfrak{A}'g_j'G)=\mathfrak{A}'\delta g_j'G,$$

where $\bar{\delta}\in\Delta$ and δ is any representative of $\bar{\delta}$ in U_p. It is obvious that $\bar{\delta}(\mathfrak{A}'g_j'G)=\mathfrak{A}'g_k'G$ for some $\bar{\delta}\in\Delta$, if and only if both $\mathfrak{A}'g_j'G$ and $\mathfrak{A}'g_k'G$ are contained in the same double coset $\mathfrak{A}g_iG$ for some i $(1\leqq i\leqq H)$. In other words, each Δ-orbit in $\mathscr{L}'$ corresponds one-to-one to each class of $\mathscr{L}(L)$. So, we can calculate H, if the character of the linear representation of Δ attached to the permutation representation $(\Delta, \mathscr{L}')$ is known. On the other hand, for each j $(1\leqq j\leqq H')$, define a subgroup Γ_j' of Δ by:

$$\Gamma_j'=\{\bar{\delta}\in\Delta;\ \bar{\delta}(\mathfrak{A}'g_j'G)=\mathfrak{A}'g_j'G\}.$$

It is trivial that, for each j $(1\leqq j\leqq H')$, there exists the unique i $(1\leqq i\leqq H)$ such that $\mathfrak{A}'g_j'G\subset\mathfrak{A}g_iG$. For that i, we get a group isomorphism $\Gamma_j'\cong\Gamma_i$. In fact, put $g_j'=ug_ia$ $(a\in G,\ u\in\mathfrak{A})$. Then,

$$\begin{aligned}\Gamma_j' &\cong (g_jGg_j'^{-1}\cap\mathfrak{A})/(g_jGg_j'^{-1}\cap\mathfrak{A}')\\ &\cong (G\cap g_i^{-1}\mathfrak{A}g_i)/(G\cap g_i^{-1}u^{-1}\mathfrak{A}'ug_i)\\ &\cong \Gamma_i/(G\cap g_i^{-1}u^{-1}\mathfrak{A}'ug_i).\end{aligned}$$

But, $G\cap g_i^{-1}u^{-1}\mathfrak{A}'ug_i=\{1\}$, because G is diagonally embedded in G_A and U_p' is torsion-free. So, $\Gamma_j'\cong\Gamma_i$. In other words, the stabilizer of any point in each Δ-orbit gives each Γ_i, and the irreducible decomposition of $(\Delta, \mathscr{L}')$ as *permutation* representation is given by $\bigoplus_{i=1}^{H}(\Delta, \Delta/\Gamma_i)$ through the above isomorphism, where $(\Delta, \Delta/\Gamma_i)$ is the permutation representation of Δ determined by the action of Δ on Δ/Γ_i. This is the essential difference between Problem 1 and Problem 2.

1.2. We shall explain a general method to solve Problem 2 and give a new mass formula. Let Γ be a finite subgroup of G. We would like to know for example how many Γ_i $(1 \leqq i \leqq H)$ contain Γ. If Γ is a cyclic group, the usual trace formula gives us a strong tool for this problem: fix a generator γ of Γ and denote by $\{\gamma\}_G$ the set of elements of G which are G-conjugate to γ. Then, our previous trace formula (cf. [2], [3], [5]) expresses the following "mass"

$$\sum_{i=1}^{H} \frac{\sharp\{\{\gamma\}_G \cap \Gamma_i\}}{\sharp(\Gamma_i)}$$

by some data on G-conjugacy classes. But, as Γ_i is not necessarily cyclic, we must introduce some new "mass" for non-cyclic Γ. We shall explain this below. For any natural integer r and any group $\mathfrak{g}$, denote by $\mathfrak{g}^r$ the direct product of r copies of $\mathfrak{g}$. The multiplication between elements of $\mathfrak{g}$ and $\mathfrak{g}^r$ is defined through the diagonal embedding of $\mathfrak{g}$ into $\mathfrak{g}^r$:

$$hg=(hg_1, \cdots, hg_r), \qquad gh=(g_1h, \cdots, g_rh),$$
$$(h \in \mathfrak{g},\ g=(g_1, \cdots, g_r) \in \mathfrak{g}^r).$$

Let $\mathfrak{h}$ be a subgroup of $\mathfrak{g}$. Two elements $g, g' \in \mathfrak{g}^r$ are said to be $\mathfrak{h}$-conjugate, if $g'=hgh^{-1}$ for some $h \in \mathfrak{h}$. Now, through the natural embedding $G^r \subset GL_B(V)^r$, we regard elements of G^r also elements of $GL_B(V)^r$. For $\gamma \in G^r$, denote by $\{\gamma\}_G$ (resp. $\{\gamma\}_{GL}$) the set of all elements of G^r which are G (resp. $GL_B(V)$)-conjugate to γ. For each genus $\mathscr{L}$ of lattices in V, and each $\{\gamma\}_G$ (resp. $\{\gamma\}_{GL}$), where $\gamma \in G^r$, we define a new "mass" $m(\mathscr{L}, \{\gamma\}_G)$ (resp. $m(\mathscr{L}, \{\gamma\}_{GL})$) as follows:

$$m(\mathscr{L}, \{\gamma\}_G)=\sum_{i=1}^{H} \frac{\sharp\{\{\gamma\}_G \cap \Gamma_i^r\}}{\sharp(\Gamma_i)},$$

$$m(\mathscr{L}, \{\gamma\}_{GL})=\sum_{i=1}^{H} \frac{\sharp\{\{\gamma\}_{GL} \cap \Gamma_i^r\}}{\sharp(\Gamma_i)},$$

where H and Γ_i $(1 \leqq i \leqq H)$ are defined for each $\mathscr{L}$ as in 1.1.

It is trivial that $m(\mathscr{L}, \{\gamma\}_G)=m(\mathscr{L}, \{\gamma\}_{GL})=0$, unless the group generated by all $\gamma_1, \cdots, \gamma_r$ is of finite order, where $\gamma=(\gamma_1, \cdots, \gamma_r)$. More precisely, take a (finite) subgroup Γ of G, and fix a set of generators $\gamma_1, \cdots, \gamma_r$ of Γ. Then, $h_i^{-1}\Gamma h_i \subset \Gamma_i$ for some i $(1 \leqq i \leqq H)$ and some $h_i \in G$ (resp. $h_i \in GL_B(V)$), if and only if $m(\mathscr{L}, \{\gamma\}_G) \neq 0$ (resp. $m(\mathscr{L}, \{\gamma\}_{GL}) \neq 0$) for $\gamma=(\gamma_1, \cdots, \gamma_r) \in G^r$. Then above "masses" might be called "masses" of Γ, although they depend on the choice of generators of Γ.

A formula for these masses will be given in Theorem 1.1 later. Here we explain a general method how to solve Problem 2 by using these masses. Assume that $\Delta = U_p' \backslash U_p$ is explicitly known. As each Γ_i $(1 \leqq i \leqq H)$ is isomorphic to a subgroup of Δ, we can give explicitly the candidates for the (abstract) group isomorphism classes which contain some Γ_i.

It is more convenient to consider the following refinements (a), (b) of Problem 2. For any finite subgroup Γ of G,

(a) Count the number of i $(1 \leqq i \leqq H)$ such that $h_i^{-1}\Gamma h_i = \Gamma_i$ for some $h_i \in GL_B(V)$.

(b) Count the number of i $(1 \leqq i \leqq H)$ such that $h_i^{-1}\Gamma h_i = \Gamma_i$ for some $h_i \in G$.

We can solve (a) by the following process (1), (2). (We can solve (b) virtually in the same way.)

(1) Classify $GL_B(V)$-conjugacy classes of all finite subgroups Γ of G which are isomorphic to any subgroup of Δ, satisfying $m(\mathscr{L}, \{\gamma\}_{GL}) \neq 0$ for $\gamma = (\gamma_1, \cdots, \gamma_r)$, where $\gamma_1, \cdots, \gamma_r$ are some generators of Γ.

Denote by $\{\mathscr{G}_\varphi ; \varphi \in \Phi\}$ a complete set of representatives of the conjugacy classes in (1). For each such class $\mathscr{G}_\varphi$, fix once and for all, a representative $\Gamma_\varphi \subset G$ and a set of generators $\gamma_1^{(\varphi)}, \cdots, \gamma_{r(\varphi)}^{(\varphi)}$ of Γ_φ, and calculate $m(\mathscr{L}, \{\gamma_\varphi\}_{GL})$ for each $\gamma_\varphi = (\gamma_1^{(\varphi)}, \cdots, \gamma_{r(\varphi)}^{(\varphi)}) \in G^{r(\varphi)}$. Now, put $I = \{1, 2, \cdots, H\}$, and for each $\mathscr{G}_\varphi$, define subsets $I(\mathscr{G}_\varphi)$ and $J(\mathscr{G}_\varphi)$ of I as follows:

$$I(\mathscr{G}_\varphi) = \{i \in I ;\ \Gamma_i \in \mathscr{G}_\varphi\},$$
$$J(\mathscr{G}_\varphi) = \{j \in I ;\ \Gamma_j \supsetneqq \Gamma \text{ for some } \Gamma \in \mathscr{G}_\varphi\}.$$

We want to know $\sharp(I(\mathscr{G}_\varphi))$ for each $\mathscr{G}_\varphi$. It is obvious that $\{\gamma_\varphi\}_{GL} \cap \Gamma_i^{r(\varphi)} \neq \emptyset$, if and only if $i \in I(\mathscr{G}_\varphi) \cup J(\mathscr{G}_\varphi)$. So we have

$$(*) \qquad m(\mathscr{L}, \{\gamma_\varphi\}_{GL}) - \sum_{j \in J(\mathscr{G}_\varphi)} \frac{\sharp\{\{\gamma_\varphi\}_{GL} \cap \Gamma_j^{r(\varphi)}\}}{\sharp(\Gamma_j)} = \sharp(I(\mathscr{G}_\varphi)) \times \frac{\sharp\{\{\gamma_\varphi\}_{GL} \cap \Gamma_\varphi^{r(\varphi)}\}}{\sharp(\Gamma_\varphi)}.$$

(2) (i) Define the order of Φ as follows: $\varphi < \varphi'$ $(\varphi, \varphi' \in \Phi)$, if and only if $\Gamma \subsetneqq \Gamma'$ for some $\Gamma \in \mathscr{G}_\varphi$ and $\Gamma' \in \mathscr{G}_{\varphi'}$. If φ is maximal with respect to this order among those such that $m(\mathscr{L}, \{\gamma_\varphi\}_{GL}) \neq 0$, then $J(\mathscr{G}_\varphi) = \emptyset$, and we have

$$\sharp(I(\mathscr{G}_\varphi)) = m(\mathscr{L}, \{\gamma_\varphi\}_{GL}) \times \frac{\sharp(\Gamma_\varphi)}{\sharp\{\{\gamma_\varphi\}_{GL} \cap \Gamma_\varphi^{r(\varphi)}\}}.$$

(ii) Fix $\varphi \in \Phi$, and assume that $\sharp(I(\mathscr{G}_{\varphi'}))$ are known for all φ' such

that $\varphi' > \varphi$. As far as we have a good description for $\{\gamma_\varphi\}_{GL}$ and $\Gamma^{r(\varphi)}_{\varphi'}$, we can calculate $\#\{\{\gamma_\varphi\}_{GL} \cap \Gamma^{r(\varphi)}_{\varphi'}\}$, and the left hand side of (*), which is equal to

$$m(\mathscr{L}, \{\gamma_\varphi\}_{GL}) - \sum_{\substack{\varphi' \in \Phi \\ \varphi' > \varphi}} \#(I(\mathscr{G}_{\varphi'})) \times \frac{\#\{\{\gamma_\varphi\}_{GL} \cap \Gamma^{r(\varphi)}_{\varphi'}\}}{\#(\Gamma_{\varphi'})}.$$

So, we get $\#(I(\mathscr{G}_\varphi))$ also in this case.

1.3. We shall give a mass formula. First, the relation between $m(\mathscr{L}, \{\gamma\}_G)$ and $m(\mathscr{L}, \{\gamma\}_{GL})$ is given as follows: fix $\gamma \in G^r$, and denote by $\{\gamma_\psi;\ \psi \in \Psi\}$ a complete set of representatives of G-conjugacy classes in $\{\gamma\}_{GL}$. The set Ψ might be infinite, but it is trivial that

$$m(\mathscr{L}, \{\gamma\}_{GL}) = \sum_{\psi \in \Psi} m(\mathscr{L}, \{\gamma_\psi\}_G),$$

and $m(\mathscr{L}, \{\gamma_\psi\}_G) = 0$, except for finitely many $\psi \in \Psi$. We shall give a formula for $m(\mathscr{L}, \{\gamma_\psi\}_G)$.

Theorem 1.1. *Notations and assumptions being as above,*

$$m(\mathscr{L}, \{\gamma\}_G) = \sum_{L_G(\Lambda)} M_G(\Lambda) \prod_q c_q(\gamma, U_q, \Lambda),$$

where the product is taken over all primes q and $L_G(\Lambda)$, $M_G(\Lambda)$, and $c_q(\gamma, U_q, \Lambda)$ will be defined below.

Definition of $L_G(\Lambda)$, $M_G(\Lambda)$, and $c_q(\gamma, U_q, \Lambda)$. These are defined almost in the same way as in [3], or [5] p. 553, except for the small change caused by the fact that $\gamma \notin G$ but $\gamma \in G^r$. We write down their definition here for the sake of completeness. *For any $g = (g_1, \cdots, g_r) \in G^r$, put*

$$Z(g) = \{z \in \mathrm{End}_B(V);\ zg_i = g_i z \text{ for all } i = 1, \cdots, r\},$$

and $Z_G(g) = Z(g) \cap G$.

Denote by $Z_G(g)_A$ the adelization of $Z_G(g)$, and by $Z_G(g)_q$ the q-component of $Z_G(g)_A$.

(1) *$L_G(\Lambda)$ runs over the 'G-genera' of Z-orders of $Z(\gamma)$: for any Z-order $\Lambda \subset Z(\gamma)$,*

$$L_G(\Lambda) = \{\Lambda';\ \Lambda' \text{ is a } \mathbf{Z}\text{-order of } Z(\gamma) \text{ such that, for every prime } q,\ \Lambda'_q = x_q \Lambda_q x_q^{-1} \text{ for some } x_q \in Z_G(\gamma)_q\}.$$

(2) *$M_G(\Lambda)$ is the 'G-mass' of the Z-order Λ of $Z(\gamma)$ which is defined as follows: we decompose $Z_G(\gamma)_A$ into disjoint union of double cosets as*

$$Z_G(\gamma)_A = \coprod_{k=1}^{h(\Lambda)} Z_G(\gamma) z_k (\Lambda_A^\times \cap G_A),$$

where $\Lambda_A = Z_G(g)_\infty \prod_q \Lambda_q \subset Z_G(g)_A$. *Put*

$$\Lambda_k = z_k \Lambda z_k^{-1} = \bigcap_q (z_{k,q} \Lambda_q z_{k,q}^{-1} \cap Z(\gamma)).$$

We define

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

(3) *For any prime* q *and any* $\boldsymbol{Z}$*-order of* $Z(\gamma)$, *we define the number* $c_q(\gamma, U_q, \Lambda)$ *by*:

$$c_q(\gamma, U_q, \Lambda) = \sharp(Z_G(\gamma)_q \backslash M_q(\gamma, U_q, \Lambda_q)/U_q),$$

where

$$M_q(\gamma, U_q, \Lambda) = \{x_q \in G_q;\ x_q^{-1}\gamma x_q \in U_q^\gamma \text{ and } Z(\gamma)_q \cap x_q R_q x_q^{-1} = z_q \Lambda_q z_q^{-1} \text{ for some } z_q \in Z_G(\gamma)_q\},$$

and $R_q = \{g_q \in \mathrm{End}_{B_q}(V_q);\ L_q g_q \subset L_q\}$.

Proof of Theorem 1.1. The proof is obtained virtually in the same way as in the proof of Theorem 1 in [3]. We only need to change carefully the objects $Z(g)$, $Z_G(g)$, and $M_q(g, U_q, \Lambda)$ for $g \in G$ in [3] by the new objects $Z(\gamma)$, $Z_G(\gamma)$, and $M_q(\gamma, U_q, \Lambda)$ for $\gamma \in G^r$. The details will be omitted here. q.e.d.

§ 2. Review on quaternion hermitian lattices and some miscellaneous results

From now on unitil the end of this paper, we denote by B the definite quaternion algebra over $\boldsymbol{Q}$ with arbitrary fixed prime discriminant p (except for Theorem 7.2, where the discriminant is not necessarily prime), and by V the two dimensional left B-vector space. Some part of our results is valid also for left B-vector spaces of arbitrary dimension, but we shall not mention on such details.

2.1. First, we review on maximal lattices in V, according to Shimura [16]. The positive definite quaternion hermitian metric on V is unique up to base changes, and we can assume that $V = B^2$ and

$$h(x, y) = x_1 \bar{y}_1 + x_2 \bar{y}_2 \qquad (x = (x_1, x_2),\ y = (y_1, y_2) \in B^2).$$

As in the introduction, we denote by G the group of similitudes of

(B^2, h). Fix a maximal order O of B. For each left O-lattice L, the norm $N(L)$ of L is defined to be the two sided O-ideal spanned by all $h(x, y)$ $(x, y \in L)$. A left O-lattice is called maximal, when L is maximal among those left O-lattices which have the same norm as L. For example, O^2 is a maximal lattice with $N(O^2)=O$. There exists a maximal left O-lattice $M' \subset V$ such that $N(M')=\mathfrak{P}$, where $\mathfrak{P}$ is the unique prime ideal of O dividing p. The set of maximal left O-lattices in V is the disjoint union of $\mathscr{L}(O^2)$ and $\mathscr{L}(M')$, where $\mathscr{L}(O^2)$ (resp. $\mathscr{L}(M')$) is the genus of left O-lattices in V which contains O^2 (resp. M'). The genus $\mathscr{L}(O^2)$ (resp. $\mathscr{L}(M')$) is called the principal (resp. non-principal) genus in V. Our concern in this paper is $\mathscr{L}(M')$, and we describe it more explicitly here. For each prime q, sometimes we use the metric h_q^* defined by:

$$h_q^*(x, y)=x\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}{}^t\bar{y} \qquad (x, y \in B_q^2).$$

We denote by G_q^* the group of similitudes of (B_q^2, h_q^*):

$$G_q^*=\left\{g \in M_2(B_q);\, g\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}{}^t\bar{g}=n(g)\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ n(g) \in \boldsymbol{Q}_q^\times\right\}.$$

The above h_q^* is obtained from h_q by a base change of B_q^2. In fact, for each prime q, there exists $\xi_q \in GL_2(O_q)$ such that $\xi_q\,{}^t\bar{\xi}_q=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. We fix such ξ_q for each q once and for all. It is trivial that $h_q^*(x, y)=h(x\xi_q, y\xi_q)$ and the mapping $G_q \ni g \to \xi_q g \xi_q^{-1} \in G_q^*$ defines an isomorphism $G_q \cong G_q^*$. We often identify G_q with G_q^* by this fixed isomorphism without mentioning it. Now, by Shimura [16], there exists $M \in \mathscr{L}(M')$ such that $M_q=M\otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q=O_q^2$ for every prime $q \neq p$, and that

$$M_p=M\otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p=\{(a\pi, b)\xi_p \in B_p^2;\, a, b \in O_p\},$$

where π is a prime element of O_p. Definite $\mathfrak{A}(M)=G_\infty \prod_q U_q(M)$ as in § 1.1. This $U_q(M)$ is explicitly given as follows: for each prime $q \neq p$, put

$$U_q=G_q \cap GL_2(O_q), \quad \text{and} \quad U_q^*=G_q^* \cap GL_2(O_q)=\xi_q U_q \xi_q^{-1},$$

and for p, put

$$U_p^*=G_q^* \cap \begin{pmatrix}O_p & \pi^{-1}O_p\\ \pi O_p & O_p\end{pmatrix}^\times.$$

Then, $U_q(M)=U_q$ and $U_p(M)=\xi_p^{-1}U_p^*\xi_p$. Denote by H the class number of $\mathscr{L}(M)$, and decompose G_A as in § 1:

$$G_A = \coprod_{i=1}^{H} \mathfrak{A}(M) g_i G \qquad \text{(disjoint)}.$$

For each i $(1 \leqq i \leqq H)$, define L_i and Γ_i as in § 1 for this genus $\mathscr{L}(M)$ and the above decomposition.

2.2. In this subsection, we shall give a purely number-theoretical alternative proof of the following Lemma 2.1 which was first obtained by Katsura-Oort [12] by an algebro-geometrical method.

Lemma 2.1 (Katsura-Oort, loc. cit.,). *Assume that $p \geqq 7$. Then, each $\Gamma_i/\{\pm 1\}$ $(1 \leqq i \leqq H)$ is isomorphic (as an abstract group) to one of the following groups*:

$$\begin{aligned} &\boldsymbol{Z}/n\boldsymbol{Z} && (1 \leqq n \leqq 6), \\ &D_{2n} && (1 \leqq n \leqq 6), \\ &A_4,\ S_4,\ A_5, \end{aligned}$$

where D_{2n} is the dihedral group of order $2n$, S_n (resp. A_n) is the n-th symmetric (resp. alternative) group, and $\pm 1 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(B)$.

Proof. For any element g of $M_2(B)$, the algebra $\boldsymbol{Q}(g)$ is at most of rank 4 over $\boldsymbol{Q}$. Hence, it is easy to list up all possible characteristic polynomials of elements of $M_2(B)$ which are of finite order, as has been done in [5] p. 590. By this list, we can see that every element of every $\Gamma_i/\{\pm 1\}$ is at most of order 6. Now, put

$$(U_p^*)^1 = \left\{ u \in U_p^*;\ u \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} {}^t\bar{u} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

We can embed each Γ_i $(1 \leqq i \leqq H)$ into $(U_p^*)^1$ by the mapping:

$$g_i \Gamma_i g_i^{-1} \subset \mathfrak{A}(M) \xrightarrow{\text{pr}} U_p \cong U_p^*,$$

where pr is the natural projection. We denote by Γ_i' the image of Γ_i in $(U_p^*)^1$ by this embedding. Define a subgroup V_p of $(U_p^*)^1$ by:

$$V_p = (U_p^*)^1 \cap \begin{pmatrix} 1+\pi O_p & O_p \\ \pi^2 O_p & 1+\pi O_p \end{pmatrix}^{\times}.$$

Then, V_p is a normal subgroup of $(U_p^*)^1$, and we get a group isomorphism

$$(U_p^*)^1 / V_p \cong SL_2(\boldsymbol{F}_{p^2}).$$

In fact, it is well known that $O_p/\pi O_p \cong \boldsymbol{F}_{p^2}$, and we can show easily that the following map

$$(U_p^*)^1/V_p \ni \begin{pmatrix} a & b\pi^{-1} \\ c\pi & d \end{pmatrix} \longrightarrow \begin{pmatrix} a & b \\ \bar{c} & \bar{d} \end{pmatrix} \bmod \pi \in M_2(\boldsymbol{F}_{p^2})$$

induces the above isomorphism. Now, we want to embed Γ_i into $SL_2(\boldsymbol{F}_{p^2})$. We can show that the order m of any torsion element g of V_p is some multiple of p. In fact, we have

$$g = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} + \pi X$$

for some $r \in O_p$ and $X \in M_2(O_p)$, and

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = g^m \equiv \begin{pmatrix} 1 & mr \\ 0 & 1 \end{pmatrix} \bmod \pi.$$

So, $mr \in \pi O_p$, and if $p \nmid m$, then $r \in \pi O_p$. So, $g \in 1+\pi M_2(O_p)$. But, it is well known and easy to see that the multiplicative group $1+\pi M_2(O_p)$ has no torsion element whose order is prime to p. So, we get a contradiction. Next, assume that $p \geqq 7$. Then, by the above considerations, we can show that $\Gamma_i \cap V_p = \{1\}$. In other words, we get an injective group homomorphism $\Gamma_i \hookrightarrow (U_p^*)^1/V_p \cong SL_2(\boldsymbol{F}_{p^2})$. The complete set of subgroups of $PSL_2(\boldsymbol{F}_{p^2})$ is classically wellknown (cf. Huppert [9] p. 213). Besides, the orders of elements $\Gamma_i/\{\pm 1\}$ are at most 6, and not divisible by p. Such subgroups of $PSL_2(\boldsymbol{F}_{p^2})$ are just those listed in Lemma 2.1.

q.e.d.

2.3. Now, we shall review the class number formula for $\mathscr{L}(M)$ and give some miscellaneous results obtained by that formula. The $GL_2(B)$-conjugacy classes $\{g\}_{GL}$ of semi-simple elements of G is parametrized by principal polynomials of g. (The principal polynomial of $g \in M_2(B)$ is defined to be the characteristic polynomial of the image of g by the regular representation $M_2(B) \hookrightarrow M_4(\boldsymbol{C})$.) More precisely, for a polynomial $f(x) \in \boldsymbol{Q}[x]$ of degree 4, define a subset of G by:

$$C_f = \{g \in G;\ g \text{ is semi-simple and the principal polynomial of } g \text{ is } f(x)\}.$$

It is well known and easy to prove that

$$C_f = \{g\}_{GL}$$

for any $g \in C_f$. So, we sometimes denote $m(\mathscr{L}(M), \{g\}_{GL})$ by $m(\mathscr{L}(M), f(x))$, where $g \in C_f$. We have $m(\mathscr{L}(M), f(x)) = m(\mathscr{L}(M), f(-x))$, because

any lattice in V is stable under the action of $\{\pm 1\}$. Define polynomials $f^{(m)}(x)$ $(1 \leqq m \leqq 6)$ as follows:

$$f^{(1)}(x)=(x-1)^4,$$
$$f^{(2)}(x)=(x^2+1)^2,$$
$$f^{(3)}(x)=(x^2+x+1)^2,$$
$$f^{(4)}(x)=x^4+1,$$
$$f^{(5)}(x)=x^4+x^3+x^2+x+1,$$
$$f^{(6)}(x)=x^4-x^2+1.$$

For each m $(1 \leqq m \leqq 6)$, define $H(m)$ by:

$$H(m)=\begin{cases} m(\mathscr{L}(M), f^{(m)}(x)), & \text{if } f^{(m)}(x)=f^{(m)}(-x) \text{ (i.e., } m=2, 4, 6), \\ 2\times m(\mathscr{L}(M), f^{(m)}(x)), & \text{if } f^{(m)}(x)\neq f^{(m)}(-x) \text{ (i.e., } m=1, 3, 5). \end{cases}$$

We quote the class number formula for $\mathscr{L}(M)$ in [5].

Theorem 2.2 ([5] II). *Assume that* $p \geqq 7$. *Then,* $m(\mathscr{L}(M), f(x))=0$ *except for the case that* $f(x)=f^{(m)}(x)$, *or* $f(x)=f^{(m)}(-x)$ *for some* $m=1, \cdots, 6$, *and*

$$H(1)=\frac{p^2-1}{2880},$$
$$H(2)=\frac{1}{96}\left(4+\left(\frac{-1}{p}\right)\right)\left(p-\left(\frac{-1}{p}\right)\right),$$
$$H(3)=\frac{1}{72}\left(3+\left(\frac{-3}{p}\right)\right)\left(p-\left(\frac{-3}{p}\right)\right),$$
$$H(4)=\begin{cases} \frac{1}{4} & \cdots \text{ if } p\equiv 3 \text{ or } 5 \bmod 8, \\ 0 & \cdots \text{ if } p\equiv 1 \text{ or } 7 \bmod 8, \end{cases}$$
$$H(5)=\begin{cases} \frac{2}{5} & \cdots \text{ if } p\equiv 2 \text{ or } 3 \bmod 5, \\ 0 & \cdots \text{ if } p\equiv 1 \text{ or } 4 \bmod 5, \end{cases}$$
$$H(6)=\begin{cases} \frac{1}{6} & \cdots \text{ if } p\equiv 5 \bmod 12, \\ 0 & \cdots \text{ if } p\equiv 1, 7, \text{ or } 11 \bmod 12, \end{cases}$$

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

The class number H of $\mathscr{L}(M)$ is given by:

$$H=\sum_{m=1}^{6} H(m).$$

Remark. In the notations in [5] II, $H(1)=H_1$, $H(2)=H_6$, $H(3)=H_7$, $H(4)=H_{11}$, $H(5)=H_{10}$, and $H(6)=H_{12}$.

By the above Theorem 2.2, we see that the natural projection on $\Gamma_i/\{\pm 1\}$ of any element γ of any Γ_i $(1\leqq i\leqq H)$ is of order m, if and only if the characteristic polynomial of γ is equal to $f^{(m)}(x)$, or $f^{(m)}(-x)$. For each (abstract) finite group Γ', and each m $(1\leqq m\leqq 6)$, define a rational number $M(\Gamma', m)$ by:

$$M(\Gamma', m)=\frac{\sharp\{\gamma'\in\Gamma';\ \gamma' \text{ is of order } m\}}{\sharp(\Gamma')}.$$

Then, for each $p\geqq 7$, we have

$$H(m)=\sum_{i=1}^{H} M(\Gamma_i/\{\pm 1\}, m)=\sum_{\Gamma'} \sharp(I(\Gamma'))M(\Gamma', m), \tag{2.3}$$

where Γ' runs over a complete set of representatives of all group isomorphism classes of all (abstract) finite groups, and

$$I(\Gamma')=\{i\in I;\ \Gamma_i/\{\pm 1\}\cong\Gamma' \text{ as } \textit{abstract} \text{ groups}\},$$

$I=\{1, \cdots, H\}$. In § 1, we defined the notation $I(\mathscr{G})$ for each $GL_2(B)$-conjugacy class $\mathscr{G}$ of finite subgroups of G. In the case $\mathscr{L}(M)$, the use of the above (new) notation $I(\Gamma')$ is consistent with the old one in § 1 by the following reason: we can show that $\Gamma_i/\{\pm 1\}\cong\Gamma_j/\{\pm 1\}$ for i, j $(1\leqq i, j\leqq H)$, if and only if $h^{-1}\Gamma_i h=\Gamma_j$ for some $h\in GL_2(B)$. In fact, if $\Gamma_i/\{\pm 1\}$ is cyclic, this is obvious by Theorem 2.2 and the Skolem-Noether Theorem. The proof in the case where $\Gamma_i/\{\pm 1\}$ is not cyclic is easily obtained by (3.2) in § 3, the proof of Corollary 4.2 in § 4, and by Lemma 6.7 in § 6, using the Skolem-Noether Theorem. By using Lemma 2.2 and some geometrical alternatives of Theorem 2.2 and (2.3), Katsura-Oort [12] derived some information on Problem 2 in the case of $\mathscr{L}(M)$ and solved it for $p\leqq 31$. For example, we get $M(Z/4Z, 4)=\frac{1}{2}$, $M(Z/5Z, 5)=\frac{4}{5}$, $M(Z/6Z, 6)=\frac{1}{3}$. But, for each prime $p\geqq 7$, we have $H(4)\leqq\frac{1}{4}$, $H(5)\leqq\frac{2}{5}$, and $H(6)\leqq\frac{1}{6}$. So, we see easily that $I(Z/4Z)=I(Z/5Z)=I(Z/6Z)=\varnothing$. In the same way, by Lemma 2.1, Theorem 2.2, and (2.3), we get

$$\sharp(I(D_{12}))=\begin{cases}1 & \cdots \text{ if } p\equiv 5 \bmod 12, \quad (p\neq 5)\\ 0 & \cdots \text{ if } p\equiv 1, 7, \text{ or } 11 \bmod 12.\end{cases}$$

(As for details, see [12] loc. cit.)

If p is very small, Lemma 2.1, Theorem 2.2, and (2.3) give us enough information to solve Problem 2, as was executed in [12]. But, as for general p, it is indispensable to give some new mass formula in order to solve Problem 2. For example, we have $M(D_8, 4)=M(S_4, 4)=\frac{1}{4}$, and $M(D_{10}, 5)=M(A_5, 5)=\frac{2}{5}$, and at least for big prime p, we can not tell which of D_8 or S_4 (, or D_{10} or A_5) appears as $\Gamma_i/\{\pm 1\}$, unless we have some new formula. The rest of this paper will be devoted to a calculation of the new mass formula.

§ 3. Classification of conjugacy classes

In order to calculate the mass $m(\mathscr{L}(M), \{\gamma\}_{GL})$ explicitly for each $\gamma \in G^r$ (r: natural integer) by using Theorem 1.1, first we must classify the G-conjugacy classes in $\{\gamma\}_{GL}=\{h^{-1}\gamma h \in G;\ h \in GL_2(B)\}$. We shall give a general (but not explicit) parametrization in 3.1, imitating the method in Hijikata [8] (see also [5]), and more explicit theory in the cases we need will be given in 3.2.

3.1. For any natural integer s and any element $g=(g_1, \cdots, g_s) \in M_2(B)$, put ${}^t\bar{g}=({}^t\bar{g}_1, \cdots, {}^t\bar{g}_s)$. Any element $z \in M_2(B)$ is called positive symmetric, $z>0$, if $z={}^t\bar{z}$ and $\mathrm{tr}(xz\,{}^t\bar{x})>0$ for all $x \in M_2(B)$, $x \neq 0$, where tr is the reduced trace of $M_2(B)$. Now, fix a natural number r and an element $\gamma=(\gamma_1, \cdots, \gamma_r) \in G^r$. Denote by $Z(\gamma) \subset M_2(B)$ the "commutor algebra" of γ in $M_2(B)$ as in § 1.2, and denote by $Z(\gamma)_+^*$ the set of all positive symmetric elements in $Z(\gamma)$:

$$Z(\gamma)_+^*=\{z \in Z(\gamma);\ z={}^t\bar{z}>0\}.$$

We define an equivalence relation $\approx$ in $Z(\gamma)_+^*$ by putting $z \approx z'$, if and only if $axz\,{}^t\bar{x}=z'$ for some $x \in Z(\gamma)^\times$ and $a \in \boldsymbol{Q}_+^\times$.

Lemma 3.1. *The mapping $g^{-1}\gamma g \to g\,{}^t\bar{g}$ induces a bijection:*

$$\{\gamma\}_{GL}/\underset{G}{\sim} \approx Z(\gamma)_+^*/\approx,$$

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

Proof. For $g \in GL_2(B)$, we have $g^{-1}\gamma g \in G^r$, if and only if $(g^{-1}\gamma g)({}^t\bar{g}\,{}^t\bar{\gamma}\,{}^t\bar{g}^{-1})=(1, \cdots, 1) \in G^r$, taking the product in G^r. Namely, $g^{-1}\gamma g \in G^r$, if and only if $g\,{}^t\bar{g} \in Z(\gamma)_+^* \subset Z(\gamma)$. Next, if $g_1^{-1}\gamma g_1,\ g_2\,{}^1\gamma g_2 \in G^r$ and $g_1^{-1}\gamma g_1=h^{-1}g_2^{-1}\gamma g_2 h$ for some $g_1, g_2 \in GL_2(B)$ and $h \in G$, then $g_2 h g_1^{-1} \in Z(\gamma)^\times$. In other words, we have $g_2\,{}^t\bar{g}_2=cx(g_1\,{}^t\bar{g}_1)\,{}^t\bar{x}$ for some $c \in \boldsymbol{Q}_+^\times$ and $x \in Z(\gamma)^\times$. So the mapping is well defined. It is well known that any

positive symmetric element of $M_2(B)$ is of the form $g\,{}^t\bar{g}$ for some $g \in GL_2(B)$. Hence we get the surjectivity. For any $c \in \boldsymbol{Q}_+^\times$, there exists $h \in G$ such that $h\,{}^t\bar{h} = cI_2$. So the injectivity is clear. q.e.d.

3.2. In this subsection, we treat some special cases we need. We assume here that $p \geqq 5$. When $r=1$, the mass formulae were given in the class number formula. So, we treat the case $r \geqq 2$, or those $\gamma = (\gamma_1, \cdots, \gamma_r) \in G^r$ such that the group spanned by $\gamma_1, \cdots, \gamma_r$ is not cyclic. Now, we assume that there exists an injective group homomorphism $D_{2n} \hookrightarrow \Gamma_i/\{\pm 1\}$ for some i $(1 \leqq i \leqq H)$ and some n $(2 \leqq n \leqq 6)$. For each fixed n $(2 \leqq n \leqq 6)$, denote by σ_n', τ_n' the generators of D_{2n} such that $\sigma_n'^2 = 1$, $\tau_n'^n = 1$, and $\sigma_n'\tau_n' = \tau_n'^{-1}\sigma_n'$. Fix a representative σ_n (resp. τ_n) of σ_n' (resp. τ_n') in Γ_i. First, we examine the structure of the subalgebra $\boldsymbol{Q}(\sigma_n, \tau_n)$ of $M_2(B)$ spanned by σ_n, τ_n. As $\sigma_n'^2 = 1$, we have $\sigma_n^2 = \pm 1$.

If $\sigma_n^2 = 1$, then, by Theorem 2.2, we have $\sigma_n = \pm 1$, and hence $\sigma_n' = 1$, which is a contradiction. So, we have $\sigma_n^2 = -1$. We get also $\sigma_n\tau_n = \tau_n^{-1}\sigma_n$. In fact, if $\sigma_n\tau_n = -\tau_n^{-1}\sigma_n$, then $(\sigma_n\tau_n)^2 = -(\sigma_n\tau_n)(\tau_n^{-1}\sigma_n) = -\sigma_n^2 = 1$, and hence $\sigma_n'\tau_n' = 1$, which is a contradiction. By easy calculation, we can show that $\boldsymbol{Q}(\tau_n + \tau_n^{-1})$ is the center of $\boldsymbol{Q}(\sigma_n, \tau_n)$. Besides, it is easy to see that $\boldsymbol{Q}(\sigma_n, \tau_n)$ is the totally definite quaternion algebra over $\boldsymbol{Q}(\tau_n + \tau_n^{-1})$, and ${}^t\bar{x}$ induces on $\boldsymbol{Q}(\sigma_n, \tau_n)$ the main involution over $\boldsymbol{Q}(\tau_n + \tau_n^{-1})$. More precisely, we get

(3.2) for each $n=2$, or 3, $\boldsymbol{Q}(\sigma_n, \tau_n)$ is the definite quaternion algebra over $\boldsymbol{Q}$, and the discriminant is 2 (resp. 3) when $n=2$ (resp. 3).

(3.3) for each $n=4$, 5, or 6, $\boldsymbol{Q}(\sigma_n, \tau_n)$ is the totally definite quaternion algebra over $\boldsymbol{Q}(\sqrt{2})$, $\boldsymbol{Q}(\sqrt{5})$, or $\boldsymbol{Q}(\sqrt{3})$, respectively, and the discriminant is 1.

The proof consists of standard exercises of the classfield theory, and will be omitted here. Incidentally, by Eichler [2], it can be easily shown that the class number of each $\boldsymbol{Q}(\sigma_n, \tau_n)$ $(2 \leqq n \leqq 5)$ is equal to one. Now, for each n $(2 \leqq n \leqq 6)$, put $\gamma_n = (\sigma_n, \tau_n)$. When $n=6$, the mass $m(\mathscr{L}(M), \{\gamma_6\}_{GL})$ was already known in § 2. When $n=4$, or 5, we have some special method to calculate the masses $m(\mathscr{L}(M), \{\gamma_n\}_{GL})$, as will be shown in the next section. So, we shall give here an explicit parametrization for $\{\gamma_n\}/\sim_G$ only when $n=2$, or 3.

For each $n=2$, or 3, and for each pair (α, β) of elements of $M_2(B)$, or $M_2(B_q)$ (q: prime), we consider the following conditions:

(3.4) (i) $\alpha\beta = \beta^{-1}\alpha$,
(ii) the principal polynomial of α is $f^{(2)}(x)$,
(iii) the principal polynomial of β is $f^{(n)}(x)$.

For each $n=2$, or 3, define a subset C_n of G^2 by:

$$C_n=\{(\alpha, \beta) \in G^2;\ \text{the pair } (\alpha, \beta) \text{ satisfies (3.4)}\},$$

and for each prime q, define a subset $C_n(q)$ of G_q^2 by:

$$C_n(q)=\{(\alpha, \beta) \in G_q^2;\ \text{the pair } (\alpha, \beta) \text{ satisfies (3.4)}\}.$$

We sometimes regard $C_n(q)$ also as a subset of G_q^* by the fixed identification $G_q^* \cong G_q$. By the Skolem-Noether Theorem and (3.2), it is easy to show that C_n (resp. $C_n(q)$) forms a single $GL_2(B)$ (resp. $GL_2(B_q)$)-conjugacy class for each n and q, if $C_n \neq \emptyset$ (resp. $C_n(q) \neq \emptyset$). Actually, we can show that $C_n \neq \emptyset$ for each $p \geqq 5$. In fact, there exist integers $\lambda, \mu \in Z$ such that

$$\left(\frac{-(1+\lambda^2)}{p}\right) \neq 1, \quad \text{and} \quad \left(\frac{-3(1+\mu^2)}{p}\right)=1,$$

where $\left(\frac{*}{p}\right)$ is the Legendre symbol. Fix such λ, μ. There exist $c, d \in B$ such that $c^2=-1/(1+\lambda^2)$ and $d^2=-3/(1+\mu^2)$. Define elements α, β_2, $\beta_3 \in G$ by:

$$\alpha=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \quad \beta_2=c\begin{pmatrix}1 & \lambda\\ \lambda & -1\end{pmatrix}, \quad \beta_3=\frac{1}{2}\begin{pmatrix}-1+d & d\mu\\ d\mu & -1-d\end{pmatrix}.$$

Then, $(\alpha, \beta_2) \in C_2$ and $(\alpha, \beta_3) \in C_3$. Now, for each $n=2$ or 3, fix $\gamma=(\alpha, \beta) \in C_n$. As we have $\boldsymbol{Q}(\alpha, \beta) \otimes Z(\gamma) \cong M_2(B)$, we can show by (3.2) that $Z(\gamma)$ is the *indefinite* quaternion algebra over $\boldsymbol{Q}$ with discriminant $2p$ (resp. $3p$), when $n=2$ (resp. 3). The algebra $Z(\gamma)$ is stable under the action $x \to {}^t\bar{x}$, but this does not induce the main involution ρ of $Z(\gamma)$. As ${}^t\bar{x}$ induces a positive involution on $Z(\gamma)$, there exists $a \in Z(\gamma)^\times$ such that ${}^t\bar{x}=a^{-1}x^\rho a$ for any $x \in Z(\gamma)$ and $a^2 \in \boldsymbol{Q}^\times$, $a^2>0$ (Shimura [15]). By the Skolem-Noether Theorem, there exists $b \in Z(\gamma)$ such that $ba=-ab$ and $b^2 \in \boldsymbol{Q}^\times$. As $Z(\gamma)$ is indefinite, we get $b^2>0$. It is obvious that 1, a, b, ab form a basis of $Z(\gamma)$. For an element $z \in Z(\gamma)$, we have $z={}^t\bar{z}$, if and only if $z=x_1+x_2b+x_3ab$ for some $x_1, x_2, x_3 \in \boldsymbol{Q}$. It is easy to see that $z={}^t\bar{z}>0$, if and only if $n(z)>0$ and $\mathrm{tr}(z)>0$, where n (resp. tr) is the reduced norm (resp. trace) of $Z(\gamma)$. Namely, we have

$$Z(\gamma)_+^*=\{z \in Z(\gamma);\ n(z)>0,\ \mathrm{tr}(z)>0,\ \mathrm{tr}(za^{-1})=0\}.$$

So, for each $z \in Z(\gamma)_+^*$ there eixsts the unique square-free positive integer $m(z)$ such that $\boldsymbol{Q}(za^{-1}) \cong \boldsymbol{Q}(\sqrt{-m(z)})$.

Proposition 3.5. *The mapping* $Z(\gamma)_+^* \ni z \to \boldsymbol{Q}(\sqrt{-m(z)})$ *induces the following bijection*:

$$Z(\Upsilon)_+^*/\approx \approx \left\{\begin{matrix}\textit{the isomorphism classes of imaginary quadratic}\\ \textit{field which can be embedded into } Z(\Upsilon)\end{matrix}\right\}.$$

Proof. If $z_1, z_2 \in Z(\Upsilon)_+^*$ and $z_1 \approx z_2$, then $z_1 a^{-1} = cd(z_2 a^{-1})d^e$ for some $c \in \boldsymbol{Q}_+^\times$ and $d \in Z(\Upsilon)$. So, we have $\boldsymbol{Q}(z_1 a^{-1}) \cong \boldsymbol{Q}(z_2 a^{-1})$. So, the mapping factors through $Z(\Upsilon)_+^*/\approx$. If K is an imaginary quadratic field contained in $Z(\Upsilon)$, and if $K \cong \boldsymbol{Q}(\sqrt{-m})$ for some square-free integer $m>0$, then there exists the unique element $y \in K$ such that $y^2 = -m$ and $\mathrm{tr}(ya)>0$. If we put $z = ya$, then ${}^t\bar{z} = {}^t\bar{a}\,{}^t\bar{y} = a^{-1}a^e a a^{-1} y^e a = a^{-1}(ay)a = ya = z$, and $\mathrm{tr}(z)>0$, $n(z) = n(a)n(y)>0$. So, $z \in Z(\Upsilon)_+^*$, and $m(z) = m$. Hence, the surjectivity is proved. The injectivity is proved as follows: If $\boldsymbol{Q}(z_1 a^{-1}) \cong \boldsymbol{Q}(z_2 a^{-1})$ for $z_1, z_2 \in Z(\Upsilon)_+^*$, then there exists $c \in \boldsymbol{Q}_+^\times$ such that $(z_1 a^{-1})^2 = c^2 (z_2 a^{-1})^2$. Hence, by the Skolem-Noether Theorem, there exists $z_0 \in Z(\Upsilon)^\times$ such that $z_0^{-1}(z_1 a^{-1}) z_0 = c z_2 a^{-1}$. This means that $z_1 = cn(z_0)^{-1} z_0 z_2 {}^t\bar{z}_0$. q.e.d.

Now, we show that the above parametrization in Proposition 3.5 is "canonical", that is, it does not depend on the choice of initial $\Upsilon \in C_n$. Fix $\Upsilon \in C_n$ as before, and for each $\Upsilon' = g^{-1}\Upsilon g \in \{\Upsilon\}_{GL}$ ($g \in GL_2(B)$), define an imaginary quadratic subfield $K(\Upsilon')$ of $M_2(B)$ by:

$$K(\Upsilon') = \boldsymbol{Q}({}^t\bar{g} a^{-1} g).$$

As $K(\Upsilon') = g^{-1}\boldsymbol{Q}(g\,{}^t\bar{g} a^{-1})g$, the "parameter" of Υ' in Proposition 3.5 is given by the isomorphism class which contains $K(\Upsilon')$. We have $Z(\Upsilon') = g^{-1}Z(\Upsilon)g \supset K(\Upsilon')$, and the involution ${}^t\bar{g}$ induces the complex conjugation on $K(\Upsilon')$. As $Z(\Upsilon')$ is indefinite, by the Skolem-Noether Theorem, there exists $y \in Z(\Upsilon')$ which satisfies the following condition:

(3.6) $\qquad yk = {}^t\bar{k}y$ for any $k \in K(\Upsilon')$, and $0 < y^2 \in \boldsymbol{Q}$.

For any such y, we have $Z(\Upsilon') = K(\Upsilon') + yK(\Upsilon')$.

Proposition 3.7. *Notations and assumptions being as above, $K(\Upsilon')$ is the unique quadratic subfield of $Z(\Upsilon')$ such that its non-trivial automorphism over $\boldsymbol{Q}$ is given by the action $x \to {}^t\bar{x}$. We have also*

$$Z_G(\Upsilon') = Z(\Upsilon') \cap G = K(\Upsilon')^\times \cup yK(\Upsilon')^\times,$$

where y is any element of $Z(\Upsilon')$ which satisfies (3.6).

Proof. First, we show that $y = {}^t\bar{y}$. We have $y = g^{-1}y_0 g$ for some $y_0 \in Z(\Upsilon)$, and by definition of a, ${}^t\bar{y}_0 = a^{-1}y_0^e a = -a^{-1}y_0 a$. As ${}^t\bar{g}ag \in K(\Upsilon')$, we have $y = -({}^t\bar{g}a^{-1}g)y(g^{-1}a\,{}^t\bar{g}^{-1}) = {}^t\bar{g}\,{}^t\bar{y}_0\,{}^t\bar{g}^{-1} = {}^t\bar{y}$. Hence, the action $x \to {}^t\bar{x}$ induces the identity mapping on $yK(\Upsilon')$. This proves the first

assertion. Now, it is clear that $K(\gamma')$, $yK(\gamma')\subset Z_G(\gamma')$. On the contrary, if $z\in Z_G(\gamma')$, then $z\,{}^t\bar{z}=c1_2$ for some $c\in \boldsymbol{Q}_+^\times$. By easy calculation, we get ${}^t\bar{z}=({}^t\bar{g}a^{-1}g)z^{\rho'}(g^{-1}a\,{}^t\bar{g})$, where ρ' is the main involution of $Z(\gamma')$. Hence, we get $zk=cn(z)^{-1}kz$ for any $k\in K(\gamma')$, where $n(z)$ is the reduced norm. Taking the norm of both sides, we see that $cn(z)^{-1}=\pm 1$. Hence, $z\in K(\gamma')\cup yK(\gamma')$. q.e.d.

The local version of Propositions 3.5 and 3.7 is obtained in a similar way.

Proposition 3.8. *For each prime q and each $\gamma=(\alpha,\beta)\in C_n(q)$ ($n=2$, or 3), there exists the unique commutative semi-simple subalgebra $K(\gamma)_q$ of $Z(\gamma)_q=\{z\in M_2(B_q);\ z\alpha=\alpha z,\ z\beta=\beta z\}$ of rank 2 over $\boldsymbol{Q}_q$ such that ${}^t\bar{x}$ induces the non-trivial automorphism over $\boldsymbol{Q}_q$ on it. We have*

$$Z_G(\gamma)_q=K(\gamma)_q^\times\cup yK(\gamma)_q^\times,$$

where y is any element of $Z(\gamma)_q$ such that $yk={}^t\bar{k}y$ for any $k\in K(\gamma)_q$. Two elements $\gamma,\gamma'\in C_n(q)$ are G_q-conjugate, if and only if $K(\gamma)\cong K(\gamma')$.

The proof is virtually the same as that of Proposition 3.7, and will be omitted here.

By Propositions 3.7 and 3.8, we get the following "Hasse principle".

Proposition 3.9. *For elements $\gamma,\gamma'\in C_n$ (for fixed $n=2$, or 3), γ is G-conjugate to γ', if and only if γ is G_A-conjugate to γ'.*

Proof. The "only if" part is trivial. Now, we prove the converse. If $\gamma=g^{-1}\gamma' g$ for some $g\in G_A$, then by Proposition 3.8, $K(\gamma)\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_q\cong K(\gamma')\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_q$ for every prime q. So, $K(\gamma)\cong K(\gamma')$. q.e.d.

Remark. As was explained in Hijikata [7], in many cases, the Hasse principle on G-conjugacy classes can be reduced to that on various forms, that is, in our cases, those forms defined by $*$-symmetric positive definite elements of $Z(g)$, where $*$ is the natural involution of $Z(g)$ induced by that of B. For example, the proof of Proposition 3.9 was reduced to the Hasse principle on quaternion anti-hermitian forms of degree one in a "multiplicative" sense (i.e. (H-III) in Hijikata [6]). This method works also in general cases, unless $*$-symmetric elements of $Z(g)$ is equivalent to quaternion anti-hermitian forms (cf. [7]). As the Hasse principle on quaternion anti-hermitian forms is false for general degree (Hijikata [6], Bayer-Fluckiger [1]), we do not know at present whether the Hasse principle on G-conjugacy classes in G^r is valid or not for the remaining cases.

§ 4. Non-existence of D_8 and D_{10}

We assume that $p \geqq 7$. In this section, we shall prove that $I(D_8) = I(D_{10}) = \emptyset$ for $\mathscr{L}(M)$ by showing that, if $\Gamma_i/\{\pm 1\} \longleftarrow\!\supset D_8$ (resp. D_{10}), then $\Gamma_i/\{\pm 1\} \cong S_4$ (resp. A_5). We denote by R_i the right order of L_i:

$$R_i = \{g \in M_2(B);\ L_i g \subset L_i\}.$$

Proposition 4.1. *Assume that* $\Gamma_i/\{\pm 1\} \longleftarrow\!\supset D_{2n}$ *for* $n = 4$, *or* 5. *Then,* $R_i \cap \boldsymbol{Q}(\sigma_n, \tau_n)$ *is a maximal order of* $\boldsymbol{Q}(\sigma_n, \tau_n)$, *where* σ_n *and* τ_n *are defined for each n as in* § 3.2.

The proof of this proposition will be given later in this section. Here, we shall give Corollaries to this Proposition.

Corollary 4.2. *If* $\Gamma_i/\{\pm 1\}$ *contains a subgroup which is isomorphic to* D_8 (*resp.* D_{10}), *then* $\Gamma_i/\{\pm 1\} \cong S_4$ (*resp.* A_5).

Proof. For each $n = 4$, or 5, define σ_n, τ_n as before, and put $\Omega_n = R_i \cap \boldsymbol{Q}(\sigma_n, \tau_n)$. Denote by W_n the group of units of $\boldsymbol{Z}[\tau_n + \tau_n^{-1}]$, and denote by E_n the subgroup of Ω_n defined by:

$$E_n = \{\gamma \in \Omega_n^{\times};\ \gamma\, {}^t\bar{\gamma} = 1\}.$$

Then, $E_n/\{\pm 1\} \cong \Omega_n/W_n$. In fact, if $x \in \Omega_n^{\times}$, then $x\, {}^t\bar{x} = \varepsilon \in W_n$, but as the norm of the fundamental unit of $\boldsymbol{Q}(\tau_n + \tau_n^{-1})$ is -1, there exists $\varepsilon_0 \in W_n$ such that $\varepsilon_0^2 = \varepsilon$. Hence $(\varepsilon_0 x)\, {}^t\overline{(\varepsilon_0 x)} = 1$. By the usual mass formula (Eichler [1]), we have

$$\frac{1}{\sharp(\Omega_4/W_4)} \leqq \frac{1}{24} \quad \text{and} \quad \frac{1}{\sharp(\Omega_5/W_5)} \leqq \frac{1}{60}.$$

As $\Gamma_i \supset E_4$, or E_5, we get $\Gamma_i/\{\pm 1\} \cong S_4$, or A_5, by Lemma 3.1. q.e.d.

Corollary 4.3. *For* $\mathscr{L}(M)$ *and each* $p \geqq 7$,

$$\sharp(I(S_4)) = \begin{cases} 1 & \cdots \text{ if } p \equiv 3, 5 \bmod 8, \\ 0 & \cdots \text{ if } p \equiv 1, 7 \bmod 8, \end{cases}$$

$$\sharp(I(A_5)) = \begin{cases} 1 & \cdots \text{ if } p \equiv 2, 3 \bmod 5, \\ 0 & \cdots \text{ if } p \equiv 1, 4 \bmod 5. \end{cases}$$

Proof. By Lemma 3.1, we get

$$H(4) = M(S_4, 4)\sharp(I(S_4)) + M(D_8, 4)\sharp(I(D_8)),$$
$$H(5) = M(A_5, 5)\sharp(I(A_5)) + M(D_{10}, 5)\sharp(I(D_{10})).$$

As $I(D_8)=I(D_{10})=\varnothing$ by Corollary 4.2, we get Corollary 4.3. q.e.d.

Proof of Proposition 4.1. For each $n=4$, or 5, put $\Omega_n=R_i\cap \boldsymbol{Q}(\sigma_n,\tau_n)$ as before, and put $\delta_n=\tau_n+\tau_n^{-1}$. Then, $Z(\delta_n)=\boldsymbol{Q}(\sigma_n,\tau_n)$. It is sufficient to show that $\Omega_n\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_q$ is maximal in $Z(\delta_n)\otimes_{\boldsymbol{Q}}\boldsymbol{Q}_q$ for every prime q. By easy calculation, we can show that the discriminant of the order $\boldsymbol{Z}[\sigma_n,\tau_n]$ of $\boldsymbol{Z}(\delta_n)$ over $\boldsymbol{Z}[\delta_n]$ is equal to $n\boldsymbol{Z}[\delta_n]$ for each $n=4$, or 5. Hence, $\Omega_n\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_q$ is maximal for each prime $q\neq 2$ (resp. $\neq 5$), if $n=4$ (resp. 5). So, we must show that $\Omega_4\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_2$ and $\Omega_5\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_5$ are maximal. Denote by δ_5' the natural projection of $g_i\delta_5 g_i^{-1}\in M_2(O_A)$ in $M_2(O_5)$. Taking $\xi_5\in GL_2(O_5)$ such that $\xi_5\,{}^t\bar{\xi}_5=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ as in § 3.1, put $\zeta_5=\xi_5\delta_5'\bar{\xi}_5^{-1}$. It is obvious that $\Omega_5\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_5$ is maximal, if and only if $Z(\zeta_5)_5\cap M_2(O_5)$ is a maximal order of $Z(\zeta_5)_5$. To show that $Z(\zeta_5)\cap M_2(O_5)$ is maximal, it is sufficient to show that $Z(u^{-1}\zeta_5 u)_5\cap M_2(O_5)=u^{-1}Z(\zeta_5)_5 u\cap M_2(O_5)$ is maximal for some $u\in U_5^*$. Now, fix an identification $O_5=M_2(\boldsymbol{Z}_5)$, and define an elements ζ of $M_2(O_5)$ by:

$$\zeta=\begin{pmatrix}h&0\\0&\bar{h}\end{pmatrix},$$

where $h=\begin{pmatrix}0&1\\1&-1\end{pmatrix}$ and $\bar{h}=\begin{pmatrix}-1&-1\\-1&0\end{pmatrix}\in M_2(\boldsymbol{Z}_5)$. We show that $\zeta_5=u^{-1}\zeta u$ for some $u\in U_5^*$. As $2\delta_5+1\in G$, we have $2\zeta_5+1\in G_5^*$. As $2\zeta+1\in G_5^*$, by [4] Theorem 1, we have $x^{-1}(2\zeta+1)x=2\zeta_5+1$ for some $x\in G_5^*$, and hence $x^{-1}\zeta x=\zeta_5$. Now, we show that $x\in Z_G(\zeta)_5\cdot U_5^*$, where $Z_G(\zeta)_5=\{z\in G_5^*;\ z\zeta=\zeta z\}$. For $x,x'\in G_5^*$, we shall write $x\sim x'$, if $x\in Z_G(\zeta)x'U_5^*$. By the Iwasawa decomposition of G_5^* with respect to the compact group U_5^*(cf. [5] p. 579, where 1 is a misprint for 0), and by the fact that $\begin{pmatrix}c&0\\0&1\end{pmatrix}\in Z_G(\zeta)$ for any $c\in\boldsymbol{Q}_5^\times$, we get $x\sim\begin{pmatrix}\bar{\alpha}^{-1}&\beta\\0&\alpha\end{pmatrix}$ for some $\alpha\in B_5^\times$, $\beta\in B_5$ such that $\mathrm{tr}(\bar{\alpha}\beta)=0$. If we put $F=\boldsymbol{Q}_5(h)\subset M_2(\boldsymbol{Q}_5)=B_5$, then by [4] Lemma 10, we have $\alpha\in F^\times\begin{pmatrix}1&0\\0&5^m\end{pmatrix}GL_2(Z_5)$ for some $m\in\boldsymbol{Z}$. As $\begin{pmatrix}\bar{a}^{-1}&0\\0&a\end{pmatrix}\in Z_G(\zeta)$ and $\begin{pmatrix}\bar{b}^{-1}&0\\0&b\end{pmatrix}\in U_5^*$ for any $a\in F^\times$ and $b\in GL_2(\boldsymbol{Z}_5)$, we can also assume that $\alpha=\begin{pmatrix}1&0\\0&5^m\end{pmatrix}$. As $x^{-1}\zeta x\in M_2(O_5)$, we get $\alpha^{-1}\bar{h}\alpha=\begin{pmatrix}-1&5^m\\-5^{-m}&0\end{pmatrix}\in M(\boldsymbol{Z}_5)$. Hence $m=0$, that is, $x\sim\begin{pmatrix}1&\beta\\0&1\end{pmatrix}$ for some $\beta\in B_5$ such that $\mathrm{tr}(\beta)=0$. Now, put $\beta=\begin{pmatrix}a&b\\c&-a\end{pmatrix}\in M_2(Q_5)$. As $\begin{pmatrix}1&-\beta\\0&1\end{pmatrix}\begin{pmatrix}h&0\\0&\bar{h}\end{pmatrix}\begin{pmatrix}1&\beta\\0&1\end{pmatrix}=\begin{pmatrix}h&h\beta-\beta\bar{h}\\0&\bar{h}\end{pmatrix}\in M_2(O_5)$, we have $h\beta-\beta h=(a+b+c)1_2\in M_2(\boldsymbol{Z}_5)$. Put $d=(a+b+c)/3$,

and $\beta_0=d\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. As $\begin{pmatrix}1 & \beta_0\\ 0 & 1\end{pmatrix}\in U_5^*$ and $\begin{pmatrix}1 & \beta-\beta_0\\ 0 & 1\end{pmatrix}\in Z_G(\zeta)$, we get $\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}\sim\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. This means that ζ is U_5^*-conjugate to ζ_5. By easy calculation, we see that

$$Z(\zeta)_5=\begin{pmatrix}1 & 0\\ 0 & y\end{pmatrix}M_2(F)\begin{pmatrix}1 & 0\\ 0 & y\end{pmatrix}^{-1},$$

and

$$Z(\zeta)_5\cap M_2(O_5)=\begin{pmatrix}1 & 0\\ 0 & y\end{pmatrix}M_2(o_F)\begin{pmatrix}1 & 0\\ 0 & y\end{pmatrix}^{-1}$$

where o_F is the maximal order of F and $y=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\in M_2(\boldsymbol{Z}_5)$. Thus, we proved that $\Omega_5\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_5$ is maximal. The proof of the maximality of $\Omega_4\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_2$ can be obtained in a similar way, and will be omitted here.

q.e.d.

§ 5. Calculation of local data

In this section, we calculate the "local data" $c_q(\gamma, U_q, \Lambda)$ which are the most important and complicated terms in the mass formula in Theorem 1.1. For each prime q and each $n=2$ or 3, define the subset $C_n(q)$ of G_q^2 as in § 3.2. For each $\gamma=(\alpha, \beta)\in C_n(q)$, put

$$Z(\gamma)_q=\{z\in M_2(B_q);\ z\alpha=\alpha z,\ z\beta=\beta z\},$$

and $Z_G(\gamma)_q=Z(\gamma)_q\cap G_q$. For each order $\Lambda\subset Z(\gamma)_q$, we define $c_q(\gamma, U_q, \Lambda)$ as in Theorem 1.1. For the sake of convenience for calculations, we often identify some elements of $C_n(q)\subset G_q^2$ with some elements of $(G_q^*)^2$ through the fixed isomorphism $G_q\cong G_q^*$ defined by $G_q\ni g\to\xi_q g\xi_q^{-1}\in G_q^*$ as in § 2.1. In such cases, in order to treat everything in G_q^*, we consider G_q^*-conjugacy classes instead of G_q-conjugacy classes, and modify also the definitions of the notations: For each $\gamma\in(G_q^*)^2$, we define $Z(\gamma)_q$ as before, and put $Z_G(\gamma)_q=Z(\gamma)_q\cap G_q^*$. For each order $\Lambda\subset Z(\gamma)_q$, we put

$$c_q(\gamma, U_q^*, \Lambda)=\#(Z_G(\gamma)_q\backslash M(\gamma, U_q^*, \Lambda)/U_q^*),$$

where

$$M(\gamma, U_q^*, \Lambda)=\{g\in G_q^*;\ g^{-1}\gamma g\in(U_q^*)^2,\text{ and}$$
$$Z(\gamma)_q\cap gR_qg^{-1}=x\Lambda x^{-1}\text{ for some }x\in Z_G(\gamma)_q\},$$

and $R_q=M_2(O_q)$, if $q\neq p$, and $R_p=\begin{pmatrix}O_p & \pi^{-1}O_p\\ \pi O_p & O_p\end{pmatrix}$, π is a prime element of O_p.

It is easy to see that, for any $\gamma \in (G_q^*)^2$, $Z_G(\xi_q^{-1}\gamma\xi_q)_q = \xi_q^{-1}Z_G(\gamma)_q\xi_q$, and $c_q(\xi_q^{-1}\gamma\xi_q, U_q, \xi_q^{-1}\Lambda\xi_q) = c_q(\gamma, U_q^*, \Lambda)$.

In this section, we calculate $c_q(\gamma, U_q, \Lambda)$ for each representative γ of G_q-conjugacy class in $C_n(q)$ and each order Λ of $Z(\gamma)_q$. We are interested only in those such that $c_q(\gamma, U_q, \Lambda) \neq 0$ for some Λ, or equivalently, $g^{-1}\gamma g \in U_q^2$ for some $g \in G_q$. We say that $\gamma \in G^r$ is q-integral, if $g^{-1}\gamma g \in U_q^r$ for some $g \in G_q$. If $\gamma = (\alpha, \beta) \in C_n(q)$ is q-integral, then α and β are also q-integral. For orders Λ, $\Lambda' \subset Z(\gamma)_q (\gamma \in C_n(q))$, we write $\Lambda \sim \Lambda'$, if $\Lambda' = x^{-1}\Lambda x$ for some $x \in Z_G(\gamma)$. We assume that $p \geqq 5$ throughout this section.

5.1. First, we assume that $q \neq 2, n, p$. In this case, we fix, once and for all, an isomorphism $\varphi: B_q \cong M_2(\boldsymbol{Q}_q)$ such that $\varphi(O_q) = M_2(\boldsymbol{Z}_q)$, and identify B_q (resp. O_q) with $M_2(\boldsymbol{Q}_q)$ (resp. $M_2(\boldsymbol{Z}_q)$). There exist ω, η_2, $\eta_3 \in O_q$ such that $\omega^2 = -1$, $\eta_2^2 = -1$, $\eta_3^2 + \eta_3 + 1 = 0$, $\omega\eta_2 = -\eta_2\omega$ and $\omega\eta_3 = \bar{\eta}_3\omega$, where $^-$ denotes the main involution of B_q. For each $n = 2$ or 3, put $\gamma_n = (\alpha, \beta_n) \in C_n(q)$, where $\alpha = \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$ and $\beta_n = \begin{pmatrix} \eta_n & 0 \\ 0 & \eta_n \end{pmatrix}$. Then, $Z(\gamma_n)_q = M_2(Q_q) \subset M_2(B_q)$. By Proposition 3.8, it is easy to see that a complete set of representatives of G_q-conjugacy classes in $C_n(q)$ are given by $x_i^{-1}\gamma_n x_i$ $(i = 1, \cdots, 4)$, where x_i $(1 \leqq i \leqq 4)$ are any fixed elements of $GL_2(B_q)$ such that $x_i\,{}^t\bar{x}_i = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -\varepsilon \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -q \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -\varepsilon q \end{pmatrix}$ for $i = 1, 2, 3$, or 4, respectively, where ε is a fixed element of $\boldsymbol{Z}_q$ such that $\varepsilon \notin (\boldsymbol{Z}_q)^2$. The G_q-conjugacy classes which contains $x_1^{-1}\gamma_n x_1$ and $x_2^{-1}\gamma_n x_2$ are q-integral, because, by [4] Lemma 11, we can take x_1, x_2 so that x_1, $x_2 \in GL_2(O_q)$ and $x_1\,{}^t\bar{x}_1 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, $x_2\,{}^t\bar{x}_2 = \begin{pmatrix} 1 & 0 \\ 0 & -\varepsilon \end{pmatrix}$, and $x_i^{-1}\gamma_n x_i \in U_q^2$ for these x_i $(i = 1, 2)$. We shall show that $x_3^{-1}\gamma_n x_3$ and $x_4^{-1}\gamma_n x_4$ are not q-integral. First, assume that $\left(\frac{-1}{q}\right) = -1$. Fix $g \in GL_2(B_q)$ such that $g\,{}^t\bar{g} = \begin{pmatrix} 1 & 0 \\ 0 & -q \end{pmatrix}$, or $\begin{pmatrix} 1 & 0 \\ 0 & -\varepsilon q \end{pmatrix}$. If $g^{-1}\gamma_n g$ is q-integral, then $g^{-1}\alpha g$ is also q-integral, and by [4] Proposition 4 and p. 565 (i), there exists $g_1 \in G_q$ such that $g_1^{-1}g^{-1}\alpha g g_1 = \alpha$. Namely, $gg_1 \in Z(\alpha) = M_2(F)$, where $F = \boldsymbol{Q}_q(\alpha)$. So, $g\,{}^t\bar{g} = cz\,{}^t\bar{z}$ for some $c \in \boldsymbol{Q}_q^\times$ and $z \in GL_2(F)$. Hence, $\det(g\,{}^t\bar{g}) \in c^2 N_{F/\boldsymbol{Q}_q}(F^\times)$, which is a contradiction, because F is unramified over $\boldsymbol{Q}_q$. Next, we assume that $\left(\frac{-1}{q}\right) = 1$. In this case, $N_{F/\boldsymbol{Q}_q}(\boldsymbol{Z}_q[\omega]) = \boldsymbol{Z}_q$, because $\boldsymbol{Q}_q(\omega) \cong \boldsymbol{Q}_q \oplus \boldsymbol{Q}_q$. Fix elements x, $y \in \boldsymbol{Z}_q$ such that $x^2 + y^2 = -q$, or $-\varepsilon q$. Put $u = x + y\omega$, and $g_1 = \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}$. We must show that $\delta = g_1^{-1}\gamma_n g_1$ is not q-integral. Assume that $g^{-1}\delta g \in U_q^2$ for some fixed $g \in G_q$. As $g^{-1}\alpha g \in U_q$, we get $g \in Z_G(\alpha) \cdot U_q$ by [5] Proposition 15 (i). We can assume $g \in Z_G(\alpha)$. By [5] Proposition 3, we have

$$Z_G(\alpha)=F^\times\left\{\begin{pmatrix} c & d \\ -\bar{d} & \bar{c}\end{pmatrix};\ c,\ d\in F\right\},$$

where $F=\boldsymbol{Q}_q(\omega)$ and $^-$ is the non-trivial automorphism of F. So, we can write $g=f\begin{pmatrix} c & d \\ -\bar{d} & \bar{c}\end{pmatrix}$, f, c, $d\in F$. Put $\eta'=2\eta_3-1$ when $n=3$, and put $\eta'=\eta$, when $n=2$. Then, $g^{-1}\begin{pmatrix}\eta_n & 0 \\ 0 & u^{-1}\eta_n u\end{pmatrix}g\in U_q$, if and only if

$$g^{-1}\begin{pmatrix}\eta' & 0 \\ 0 & u^{-1}\eta' u\end{pmatrix}g\in U_q.$$

As $\eta'\varphi=\bar{\varphi}\eta'$ for any $\varphi\in F$, we get $u^{-1}\eta' u=u^{-1}\bar{u}\eta'$ and $g^{-1}\begin{pmatrix}\eta' & 0 \\ 0 & u^{-1}\eta' u\end{pmatrix}g\in U_q$, if and only if $g^{-1}\begin{pmatrix}1 & 0 \\ 0 & u^{-1}\bar{u}\end{pmatrix}\bar{g}\in U_q$, where $\bar{g}=\bar{f}\begin{pmatrix}\bar{c} & \bar{d} \\ -d & c\end{pmatrix}$. Hence, if δ is q-integral, we get $\overline{(u\det g)}/(u\det g)\in \boldsymbol{Z}_q[\omega]^\times$. By definition, $\det g=f^2(n(c)+n(d))$, and $\overline{(\det g)}/\det g=(\bar{f}/f)^2$. Namely, $(\bar{f}/f)^2\cdot q/u^2\in \boldsymbol{Z}_q[\omega]^\times$. Hence, $q\in \boldsymbol{Z}_q[\omega]^\times(F^\times)^2$. As $F\cong \boldsymbol{Q}_q\oplus\boldsymbol{Q}_q$ and $\boldsymbol{Z}_q[\omega]^\times\cong Z_q^\times\oplus Z_q^\times$, this is a contradiction. This proves that δ is not q-integral.

Proposition 5.1. *If $q\neq 2$, p, n, then there exist exactly two q-integral G_q-conjugacy classes in $C_n(q)$ for each n and q. A complete set of representatives δ_1, δ_2 of these classes and $K(\delta_i)_q$, $Z_G(\delta_i)_q$ $(i=1, 2)$ are given as follows: We fix $z\in Z_q[\omega]$ such that $z\bar{z}=-\varepsilon$.*

(i) $\delta_1=\left(\begin{pmatrix}\omega & 0 \\ 0 & \omega\end{pmatrix}, \begin{pmatrix}\eta_n & 0 \\ 0 & \eta_n\end{pmatrix}\right)\in (U_q^*)^2$, $K(\delta_1)_q=\left\{\begin{pmatrix}a & 0 \\ 0 & b\end{pmatrix};\ a,\ b\in \boldsymbol{Q}_q\right\}$,

and $Z_G(\delta_1)_q=K(\delta_1)_q^\times\cup y_1K(\delta_1)_q^\times$,

where $y_1=\begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}$,

(ii) $\delta_2=\left(\begin{pmatrix}\omega & 0 \\ 0 & \omega\end{pmatrix}, \begin{pmatrix}\eta_n & 0 \\ 0 & z^{-1}\eta_n z\end{pmatrix}\right)\in U_q^2$, $K(\delta_2)_q=\boldsymbol{Q}_q\left(\begin{pmatrix}0 & z \\ -\bar{z} & 0\end{pmatrix}\right)$,

and $Z_G(\delta_2)_q=K(\delta_2)_q^\times\cup y_2K(\delta_2)_q^\times$,

where $y_2=\begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}$.

Proof. Taking γ_n as before, two q-integral G_q-conjugacy classes are represented by $x_i^{-1}\gamma_n x_i$ $(i=1, 2)$, where x_1, x_2 are any elements of $GL_2(O_q)$ such that $x_1{}^t\bar{x}_1=\begin{pmatrix}0 & -1 \\ -1 & 0\end{pmatrix}$, $x_2{}^t\bar{x}_2=\begin{pmatrix}1 & 0 \\ 0 & -\varepsilon\end{pmatrix}$. Put $x_2=\begin{pmatrix}1 & 0 \\ 0 & z\end{pmatrix}$. Then, $\delta_2=x_2^{-1}\gamma_n x_2$. Next, take $a\in O_q^\times=M_2(\boldsymbol{Z}_q)^\times$ so that $a^2=-1$, and put $x=\begin{pmatrix}a & 0 \\ 0 & a\end{pmatrix}$. If we put $x_1=x\xi_q$ (where $\xi_q\in GL_2(O_q)$, $\xi_q{}^t\bar{\xi}_q=\begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}$), then

$x_1{}^t\bar{x}_1=\begin{pmatrix}0&-1\\-1&0\end{pmatrix}$, and we get $\xi_q(x_1^{-1}\gamma_n x_1)\xi_q^{-1}=x^{-1}\gamma_n x\in(U_q^*)^2$. As $x\in U_q^*$, identifying $x_1^{-1}\gamma_n x_1$ with $x^{-1}\gamma_n x=\delta_1$ by the isomorphism $U_q\cong U_q^*$, δ_1 represents the class which contains $x_1^{-1}\gamma_n x_1$. The rest is easy by noting that

$$Z(\delta_1)=M_2(\boldsymbol{Q}_q)\subset M_2(B_q),\quad\text{and}\quad Z(\delta_2)=\begin{pmatrix}1&0\\0&z\end{pmatrix}^{-1}M_2(\boldsymbol{Q}_q)\begin{pmatrix}1&0\\0&z\end{pmatrix}.$$

q.e.d.

Proposition 5.2. *Assume that $q\neq 2$, p, n, and take δ_1, δ_2 as in Proposition* 5.1.

(i) $$c_q(\delta_1, U_q^*, \Lambda)=\begin{cases}1 & \cdots \textit{ if } \Lambda\sim M_2(\boldsymbol{Z}_q),\\ 0 & \cdots \textit{ otherwise,}\end{cases}$$

(ii) $$c_q(\delta_2, U_q, \Lambda)=\begin{cases}1 & \cdots \textit{ if } \Lambda\sim\begin{pmatrix}1&0\\0&z\end{pmatrix}^{-1}M_2(\boldsymbol{Z}_q)\begin{pmatrix}1&0\\0&z\end{pmatrix},\\ 0 & \cdots \textit{ otherwise.}\end{cases}$$

Proof. First, we prove (i). Denote the component of δ_1 by α, β: $\delta_1=(\alpha,\beta)\in(G_q^*)^2$. If $g^{-1}\delta_1 g\in(U_q^*)^2$ for some $g\in G_q^*$, then $g^{-1}\alpha g\in U_q^*$. By [4] Proposition 15 (i), (ii), we get $g\in Z_G(\alpha)_q U_q^*$. Now, we write $g_1\sim g_2$ for $g_1, g_2\in G_q^*$, if $g_2\in Z_G(\delta_1)_q g_1 U_q^*$. If we put $F=\boldsymbol{Q}_q(\omega)$, then

$$Z_G(\alpha)_q=F^\times\begin{pmatrix}\boldsymbol{Q}_q & \boldsymbol{Q}_q\omega\\ \boldsymbol{Q}_q\omega & \boldsymbol{Q}_q\end{pmatrix}^\times.$$

(See [5] p. 579.) First, we treat the case where F is a field. In this case, $F^\times=\{q^n; n\in\boldsymbol{Z}\}\cdot\boldsymbol{Z}_q[\omega]^\times$, hence we have $g\sim\begin{pmatrix}a&b\omega\\c\omega&d\end{pmatrix}$ for some $a, b, c, d\in\boldsymbol{Q}_q$ such that $ab+bd\neq 0$. We can also assume that $ad\neq 0$. As $\begin{pmatrix}a&0\\0&d\end{pmatrix}\in Z_G(\delta_1)_q$, we get $g\sim\begin{pmatrix}1&b'\omega\\c'\omega&1\end{pmatrix}$ ($b', c'\in\boldsymbol{Q}_q$ and $b'c'+1\neq 0$). Now,

$$\begin{pmatrix}1&b'\omega\\c'\omega&1\end{pmatrix}^{-1}\beta\begin{pmatrix}1&b'\omega\\c'\omega&1\end{pmatrix}=\frac{1}{1+b'c'}\begin{pmatrix}\eta_n+b'c'\bar{\eta}_n & b'\omega(\bar{\eta}_n-\eta_n)\\ c'\omega(\bar{\eta}_n-\eta_n) & b'c'\bar{\eta}_n+\eta_n\end{pmatrix}\in U_q^*.$$

As $q\neq 2$, n, we get $B_q=\boldsymbol{Z}_q+\boldsymbol{Z}_q\omega+\boldsymbol{Z}_q\eta_n+\boldsymbol{Z}_q\omega\eta_n$. Hence, b', c', $1-b'c'\in(1+b'c')\boldsymbol{Z}_q$. Put $m=\mathrm{ord}_q(1+b'c')$ (the q-adic order). If $m>0$, then $b', c'\in q^m\boldsymbol{Z}_q$ and $1+b'c'\in\boldsymbol{Z}_q^\times$, which is a contradiction. Now, assume that $m<0$. Then, $m=\mathrm{ord}_q(b'c')$. Put $s=\mathrm{ord}_q(b')$ and $t=\mathrm{ord}_q(c')$. Then, $s+t=m$. If $s>0$, then $\mathrm{ord}_q(c')=t=m-s<m$, and hence $c'\in q^m\boldsymbol{Z}_q$, which is a contradiction. So, $s\leqq 0$, and by the same way, we get $t\leqq 0$. Hence

$$g\sim\begin{pmatrix}q^{-s} & 0\\ 0 & q^{-t}\end{pmatrix}\begin{pmatrix}1 & b'\omega\\ c'\omega & 1\end{pmatrix}\in U_q^*.$$

If $m=0$, then $\begin{pmatrix}1 & b'\omega\\ c'\omega & 1\end{pmatrix}\in U_q^*$. Thus, we get $g\sim 1$ in any case. Next, we treat the case where $F\cong \boldsymbol{Q}_q\oplus\boldsymbol{Q}_q$. If $g^{-1}\delta_1 g\in (U_q^*)^2$, then $g\sim g_1=x\begin{pmatrix}1 & b\omega\\ c\omega & 1\end{pmatrix}$, for some $b, c\in \boldsymbol{Q}_q$, $x\in F^\times$, as before. Put $\beta'=2\beta-1$ when $n=3$, and $\beta'=\beta$, when $n=2$. As we have assumed $q\neq 2$, n, $g^{-1}\beta' g\in U_q^*$, if and only if $g^{-1}\beta g\in U_q^*$. We get $g_1^{-1}\beta' g_1=g_1^{-1}\bar{g}_1\beta'\in U_q^*$, hence $g_1^{-1}\bar{g}_1\in U_q^*$, where $\bar{g}_1=\bar{x}\begin{pmatrix}1 & -b\omega\\ -c\omega & 1\end{pmatrix}$. We get

$$g_1^{-1}\bar{g}_1=\frac{\bar{x}}{x(1+bc)}\begin{pmatrix}1-bc & -2b\omega\\ -2c\omega & 1-bc\end{pmatrix}\in GL_2(\boldsymbol{Z}_q[\omega]).$$

We fix an isomorphism of $\boldsymbol{Z}_q[\omega]$ onto $\boldsymbol{Z}_q\oplus\boldsymbol{Z}_q$ such that ω is mapped to $(1, -1)$. As $N_{F/\boldsymbol{Q}_q}(\bar{x}/x)=1$, we can assume that $\bar{x}/x=(q^e, q^{-e})\in \boldsymbol{Q}_q\oplus\boldsymbol{Q}_q$ for some $e\in \boldsymbol{Z}$. Put $m=\mathrm{ord}_q(1+bc)$. Then, $1-bc, b, c\in q^{m+|e|}\boldsymbol{Z}_q$.

If $m>0$, then $2=(1+bc)+(1-bc)\in q^m\boldsymbol{Z}_q$, which is a contradiction, because $q\neq 2$. So, $m\leqq 0$. Put $t=\mathrm{ord}_q(b)$ and $s=\mathrm{ord}_q(c)$. If $m<0$, then $t+s=m$ and $1-bc\in q^m\boldsymbol{Z}_q$. Hence $c=0$, and we can show $g\sim 1$ virtually in the same way as in the case where F is a field. If $m=0$, then $b, c\in q^{|e|}\boldsymbol{Z}_q$ and $1-bc\in q^{|e|}\boldsymbol{Z}$. Hence $e=0$, so $g\sim 1$. Thus, we have proved (i). The proof of (ii) is obtained virtually in the same way as in the proof of (i), and we shall omit it here. q.e.d.

5.2. Next, we treat the case $q=p$. If $\gamma=(\alpha, \beta)\in C_n(p)$ is p-integral, then by [5] (III) Propositions 2.5 and 2.6, we can assume (up to G_q^*-conjugation) that

(5.3) (i) in the case $\left(\frac{-1}{p}\right)=-1$,

$$\gamma\in (G_q^*)^2,\qquad \alpha=\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}\in G_q^*,$$

where ω is a fixed element of $O_q^\times$ such that $\omega^2=-1$,

(ii) in the case $\left(\frac{-1}{p}\right)=1$,

$$\gamma\in (G_q^*)^2,\qquad \alpha=\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix}\in G_q^*,$$

where $\omega'\in \boldsymbol{Z}_p$, $\omega'^2=-1$.

First, we treat the case $n=2$.

Proposition 5.4. *There are exactly two p-integral G_p^*-conjugacy classes in $C_2(p)$. The representatives δ_1, δ_2 of such classes and $K(\delta_i)_p$, $Z_G(\delta_i)_p$ $(i=1, 2)$ are given as follows:*

(i) *When* $\left(\frac{-1}{p}\right)=-1$,

$$\delta_1=\left(\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}, \begin{pmatrix}0 & -\pi^{-1}\\ \pi & 0\end{pmatrix}\right) \in (U_p^*)^2,$$

$$K(\delta_1)_p=\boldsymbol{Q}_p\left(\begin{pmatrix}0 & \omega\\ -p\omega & 0\end{pmatrix}\right),$$

$$Z_G(\delta_1)_p=K(\delta_1)_p^\times \cup yK(\delta_1)_p^\times, \quad \textit{and}$$

$$\delta_2=\left(\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}, \begin{pmatrix}0 & \pi^{-1}u\\ \pi u & 0\end{pmatrix}\right) \in (U_p^*)^2,$$

$$K(\delta_2)_p=\boldsymbol{Q}_p\left(\begin{pmatrix}0 & \omega\\ p\omega & 0\end{pmatrix}\right),$$

$$Z_G(\delta_2)_p=K(\delta_2)_p^\times \cup yK(\delta_2)_p^\times,$$

where π is a fixed element of O_q such that $\pi^2=-p$, $\pi\omega=-\omega\pi$, u is a fixed element of $Z_p[\omega]$ such that $u\bar{u}=-1$, and $y=\begin{pmatrix}\omega & 0\\ 0 & -\omega\end{pmatrix}$.

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

$$\delta_1=\left(\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix}, \begin{pmatrix}0 & -\pi^{-1}\\ \pi & 0\end{pmatrix}\right) \in (U_p^*)^2$$

$$K(\delta_1)_p=\boldsymbol{Q}_p\left(\begin{pmatrix}\pi & 0\\ 0 & \pi\end{pmatrix}\right),$$

$$Z_G(\delta_1)_p=K(\delta_1)_p^\times \cup y'K(\delta_1)_p^\times, \quad \textit{and}$$

$$\delta_2=\left(\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix}, \begin{pmatrix}0 & \pi^{-1}u\\ \pi u & 0\end{pmatrix}\right) \in (U_q^*)^2,$$

$$K(\delta_2)_p=Q_p\left(\begin{pmatrix}\pi u & 0\\ 0 & \pi u\end{pmatrix}\right),$$

$$Z_G(\delta_2)_p=K(\delta_2)_p^\times \cup y'K(\delta_2)_p^\times,$$

where π is as in (i), *u is an element of $O_q^\times$ such that $u\pi=\pi\bar{u}$ and $n(u)=-1$, and* $y'=\begin{pmatrix}u & 0\\ 0 & -u\end{pmatrix}$.

Proof. First, we assume that $\left(\frac{-1}{p}\right)=-1$. Take δ_1 as in (i). By easy calculation, we get

$$Z(\delta_1)_p=\left\{\begin{pmatrix} a & b \\ p\bar{b} & \bar{a}\end{pmatrix};\ a,\ b\in \boldsymbol{Q}_p(\omega)\right\}.$$

The main involution ρ of $Z(\delta_1)$ is given by:

$$\begin{pmatrix} a & b \\ p\bar{b} & \bar{a}\end{pmatrix}^{\rho}=\begin{pmatrix} \bar{a} & -b \\ -p\bar{b} & a\end{pmatrix}.$$

Put $c=\begin{pmatrix} 0 & -\omega \\ p\omega & 0\end{pmatrix}$. As we are dealing with elements of G_p^*, we put $z^*=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}{}^t\bar{z}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ for $z\in M_2(B_p)$. Then, $z^*=c^{-1}z^{\rho}c$ for any $z\in Z(\delta_1)_p$, and $z^*=z$, if and only if $z=\begin{pmatrix} a & b \\ pb & \bar{a}\end{pmatrix}$ for some $a\in \boldsymbol{Q}_p(\omega)$, $b\in \boldsymbol{Q}_p$. A quadratic semisimple algebra K over $\boldsymbol{Q}_p$ can be embedded into $Z(\delta_1)$, if and only if $K=\boldsymbol{Q}_p(\sqrt{-1})$, $\boldsymbol{Q}_p(\sqrt{p})$, or $\boldsymbol{Q}_p(\sqrt{-p})$. Hence, by Proposition 3.5, representatives of G_p^*-conjugacy classes in $C_2(p)$ is given by $x_i^{-1}\delta_1 x_i$ $(i=1, 2, 3)$, where

$$x_1x_1^*=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix} 0 & -\omega \\ p\omega & 0\end{pmatrix}^{-1}c,\qquad x_2x_2^*=\begin{pmatrix}u & 0\\ 0 & \bar{u}\end{pmatrix}=\begin{pmatrix} 0 & b' \\ p\bar{b}' & 0\end{pmatrix}^{-1}c,$$

and $x_3x_3^*=\begin{pmatrix}\omega & 0\\ 0 & -\omega\end{pmatrix}c=\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}$, where b' is a fixed element of $\boldsymbol{Z}_p[\omega]$ such that $b'\bar{b}'=-1$ and $u=\bar{b}'^{-1}\omega$. If we put $x_2=\begin{pmatrix}u & 0\\ 0 & 1\end{pmatrix}$, then

$$x_2x_2^*=x_2\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}{}^t\bar{x}_2\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}u & 0\\ 0 & \bar{u}\end{pmatrix}.$$

Hence, δ_1 or $\delta_2=x_2^{-1}\delta_1 x_2$ is p-integral, and corresponds with $\boldsymbol{Q}_p(\sqrt{p})$, or $\boldsymbol{Q}_p(\sqrt{-p})$, respectively. Now, we show that $x_3^{-1}\delta_1 x_3$ is not p-integral. If this is p-integral, then, by [5] (iii) Proposition 2.5 (i), we have

$$g^{-1}x_3^{-1}\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}x_3g=\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}$$

for some $g\in G_p^*$. Hence, $x_3g\in M_2(F)$, where $F=\boldsymbol{Q}_p(\omega)$. This means that $dx_3x_3^*=ff^*$ for some $f\in GL_2(F)$ and $d\in \boldsymbol{Q}_p^{\times}$. Hence, $-d^2p=(\det f)(\det f^*)$ $=(\det f)\ (\det {}^t\bar{f})\in N_{F/\boldsymbol{Q}_p}(F)$. As F is unramified over $\boldsymbol{Q}_p$, this is a contradiction. This proves (i).

Next, we prove the case (ii). Taking δ_1 as in (ii), we get

$$Z\left(\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix}\right)_p=\left\{\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix};\ a,\ b\in B_p\right\},\quad\text{and}$$

$$Z(\delta_1)_p=\left\{\begin{pmatrix}a & 0\\ 0 & \pi a\pi^{-1}\end{pmatrix};\ a\in B_p\right\}.$$

A complete set of representatives of G_p^*-conjugacy classes in $C_2(p)$ is given by $x_i^{-1}\delta_1 x_i$ $(i=1, 2, 3)$, where

$$x_1x_1^*=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad x_2x_2^*=\begin{pmatrix}u & 0\\ 0 & u\end{pmatrix},\quad \text{and}\quad x_3x_3^*=\begin{pmatrix}u\pi & 0\\ 0 & u\pi\end{pmatrix},$$

taking u as in (ii). For $i=1, 2$, $x_i^{-1}\delta_1 x_i$ is G_p-conjugate to δ_i. Now, we show that $x_3^{-1}\delta_1 x_3$ is not p-integral. By [4] (III) Proposition 2.6 (i), if $g^{-1}x_3^{-1}\delta_1 x_3 g \in U_p^*$ for some $g \in G_p^*$, then $g^{-1}x_3^{-1}\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix}x_3 g$ is U_p^*-conjugate to $\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix}$. Namely, we can assume $x_3 g \in Z\left(\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix}\right)$, and hence $x_3 g=\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}$ for some $a, b \in B_p^\times$. In other words,

$$\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}^{-1}\begin{pmatrix}0 & -\pi^{-1}\\ \pi & 0\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}=\begin{pmatrix}0 & -a^{-1}\pi^{-1}b\\ b^{-1}\pi a & 0\end{pmatrix}\in U_p^*.$$

So, we get $a^{-1}b \in O_p^\times$. On the other hand, we get $dx_3x_3^*=d\begin{pmatrix}u\pi & 0\\ 0 & u\pi\end{pmatrix}=\begin{pmatrix}a\bar{b} & 0\\ 0 & b\bar{a}\end{pmatrix}$ for some $d \in \boldsymbol{Q}_p^\times$. That is, $\mathrm{ord}_\pi(a\bar{b})$ is odd, which is a contradiction. q.e.d.

Proposition 5.5. *Let notations and assumptions be as in Proposition* 5.4.

(i) *If* $\left(\frac{-1}{p}\right)=-1$, *then for each* $i=1, 2$,

$$c_p(\delta_i, U_p^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

where $\Lambda(i)$ *is the unique maximal order of* $Z(\delta_i)_p$.

(ii) *If* $\left(\frac{-1}{p}\right)$, *then for each* $i=1, 2$,

$$c_p(\delta_i, U_p^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

where $\Lambda(i)$ *is the unique maximal order of* $Z(\delta_i)_p$.

Proof. We assume $\left(\frac{-1}{p}\right)=-1$, and give the proof for δ_1. If $g^{-1}\delta_1 g \in (U_p^*)^2$ for some $g \in G_p^*$, then by [5] III Proposition 2.5 (i), $g \in$

$(GL_2(F)\cap G_p^*)\cdot U_p^*$, where $F=\boldsymbol{Q}_p(\omega)$. By a similar argument as in the proof of Proposition 5.4, we can assume $g=\begin{pmatrix}1 & b\omega\\ c\omega & d\end{pmatrix}$ for some $b, c, d\in \boldsymbol{Q}_p$. As $\begin{pmatrix}1 & c\omega/p\\ -c\omega & 1\end{pmatrix}\in K(\delta_1)_p$, we get $g\sim\begin{pmatrix}1 & c\omega/p\\ -c\omega & 1\end{pmatrix}g\sim\begin{pmatrix}1 & x\omega\\ 0 & y\end{pmatrix}$ for some $x, y\in \boldsymbol{Q}_p$. Now,

$$\begin{pmatrix}1 & x\omega\\ 0 & y\end{pmatrix}^{-1}\begin{pmatrix}0 & -\pi^{-1}\\ \pi & 0\end{pmatrix}\begin{pmatrix}1 & x\omega\\ 0 & y\end{pmatrix}=\begin{pmatrix}-xy^{-1}\omega\pi, & -x^2y^{-1}\pi-y\pi^{-1}\\ y^{-1}\pi, & xy^{-1}\pi\omega\end{pmatrix}\in U_p^*.$$

Hence, $y^{-1}\in \boldsymbol{Z}_p$, $xy^{-1}\in \boldsymbol{Z}_p$, and $x^2y^{-1}p-y\in \boldsymbol{Z}_p$. Then, $-(xy^{-1})^2p+1\in y^{-1}\boldsymbol{Z}_p$. So, $y^{-1}\notin p\boldsymbol{Z}_p$. This means that $y\in \boldsymbol{Z}_p^\times$ and $x\in \boldsymbol{Z}_p$. Hence, $g\sim 1$. This proves the assertion. The proof for δ_2 is virtually the same, and will be omitted here. Next, assume that $\left(\frac{-1}{p}\right)=1$. If $g^{-1}\delta_1 g\in U_p^*$ for some $g\in G_p^*$, then $g\sim\begin{pmatrix}a & 0\\ 0 & da\end{pmatrix}$ ($d\in \boldsymbol{Q}_p^\times$, $a\in B_p^\times$), by [5] III Proposition 2.5 (i). As

$$\begin{pmatrix}a & 0\\ 0 & da\end{pmatrix}^{-1}\begin{pmatrix}0 & -\pi^{-1}\\ \pi & 0\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & da\end{pmatrix}=\begin{pmatrix}0 & -da^{-1}\pi^{-1}a\\ d^{-1}a^{-1}\pi a & 0\end{pmatrix}\in U_p^*,$$

we get $d\in \boldsymbol{Z}_p^\times$. Besides, $B_p=\{\pi^r; r\in \boldsymbol{Z}\}\times O_p^\times$. Hence, $g\sim 1$. The proof for δ_2 is virtually the same, and will be omitted here. q.e.d.

Next, we treat the case $n=3$ and $q=p$. In this case, the representatives of p-integral G_p^*-conjugacy classes have not so simple form. Here, it is more convenient to proceed as follows. Take $\alpha\in G_p^*$ as in (5.3) in each case. We shall find all $\beta\in G_p^*$ such that $(\alpha, \beta)\in C_3(p)$ for this α, and investigate whether (α, β) is p-integral, or not. For this purpose, it is more convenient to replace each element $(\alpha, \beta)\in C_3(p)$ by $(\alpha, 2\beta-1)$. Namely, for each q, put

$$C_3'(q)=\{(\alpha, \beta')\in (G_q^*)^2;\ \alpha\beta'=-\beta'\alpha,\ (\beta')^2=-3\}.$$

Then, $C_3'(q)$ corresponds bijectively to $C_3(q)$ by the mapping $(\alpha, \beta)\in C_3(q)$ to $(\alpha, 2\beta-1)\in C_3'(q)$. Besides, if $q\neq 2, 3$, (α, β) is q-integral, if and only if $(\alpha, 2\beta-1)$ is q-integral.

Proposition 5.6. *There are exactly two p-integral G_p^*-conjugacy classes in $C_3'(p)$, and the representatives δ_1, δ_2 of such classes and $K(\delta_i)_p$, $Z_G(\delta_i)_p$ ($i=1, 2$) are given as follows:*

(i) *When* $\left(\frac{-1}{p}\right)=-1$, *for each* $i=1, 2$,

$$\delta_i=\left(\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix},\begin{pmatrix}0 & -\pi^{-1}\\ \varepsilon_i\pi & 0\end{pmatrix}b_i\right)\in (U_p^*)^2,$$

$$K(\delta_i)_p=\boldsymbol{Q}_p\left(\begin{pmatrix}0 & \omega\\ -p\varepsilon_i\omega & 0\end{pmatrix}\right),$$

$$Z_G(\delta_i)_p=K(\delta_i)_p^\times\cup yK(\delta_i)_p^\times,$$

where $\varepsilon_1=1$, $\varepsilon_2=-1$, b_1, b_2 *are fixed elements of* $Z_p[\omega]$ *such* $N(b_1)=3$, $N(b_2)=-3$, π *is a prime element of* O_p *such that* $\pi^2=-p$, $\pi\omega=-\omega\pi$, *and* $y=\begin{pmatrix}\omega & 0\\ 0 & -\omega\end{pmatrix}$.

(ii) *When* $\left(\frac{-1}{p}\right)=1$, *for each* $i=1, 2$,

$$\delta_i=\left(\begin{pmatrix}\omega' & 0\\ 0 & -\omega'\end{pmatrix},\begin{pmatrix}0 & \pi_i^{-1}\\ -3\pi_i & 0\end{pmatrix}\right)\in (U_p^*)^2,$$

$$K(\delta_i)_p=\boldsymbol{Q}_p\left(\begin{pmatrix}\pi_i & 0\\ 0 & \pi_i\end{pmatrix}\right),$$

$$Z_G(\delta_i)_p=K(\delta_i)_p^\times\cup y'K(\delta_i)_p^\times,$$

where π_1, π_2 *and* y' *are defined as follows: Fix an element* $\varepsilon\in Z_p^\times\backslash(Z_p^\times)^2$, *and* $c\in O_p^\times$ *such that* $c^2=\varepsilon$. *We denote by* π_1, π_2 *any fixed elements of* O_p *such that* $\pi_i c=-c\pi_i$ $(i=1, 2)$ *and* $\pi_1^2=p$, $\pi_2^2=p\varepsilon$. *We put* $y'=\begin{pmatrix}c & 0\\ 0 & -c\end{pmatrix}$.

Proof. First, assume that $\left(\frac{-1}{p}\right)=-1$. Put $\alpha=\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}$. If $(\alpha, \beta')\in C_3'(p)$, then by easy calculation, we can show that $\beta'=\pi b\begin{pmatrix}\mu\omega & 1\\ \lambda & \mu\omega\end{pmatrix}$ for some λ, $\mu\in\boldsymbol{Q}_p$ and $b\in\boldsymbol{Q}_p(\omega)$ such that $N(b)(\mu^2+\lambda)=3/p$. If we put $\gamma=(\alpha, \beta')$, then

$$K(\gamma)_p=\boldsymbol{Q}_p+\boldsymbol{Q}_p\begin{pmatrix}-\mu & \omega\\ -\lambda\omega & \mu\end{pmatrix}\cong\boldsymbol{Q}_p(\sqrt{m}),$$

where $m=\mu^2+\lambda$. As we have assumed $p\geq 5$, and $\boldsymbol{Q}_p(\omega)$ is unramified over $\boldsymbol{Q}_p$, we get $mp\in N_{F/\boldsymbol{Q}_p}(\boldsymbol{Q}_p(\omega))$, and hence $m\in p(\boldsymbol{Q}_p)^2\cup(-p)(\boldsymbol{Q}_p)^2$. Putting $\mu=0$ and $\lambda=\pm p$, we get the required results. The proof for the case $\left(\frac{-1}{p}\right)=1$ is similarly obtained, and the details will be omitted here. q.e.d.

Proposition 5.7. *Let notations and assumptions be as in Proposition* 5.6.

(i) *If* $\left(\frac{-1}{p}\right)=-1$, *then for each* $i=1, 2$

$$c_p(\delta_i, U_p^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

where $\Lambda(i)=\left\{\begin{pmatrix} a & b\\ \varepsilon_i p\bar{b} & \bar{a}\end{pmatrix};\ a, b\in \boldsymbol{Z}_p[\omega]\right\}$ *for each* $i=1, 2$.

(ii) *If* $\left(\frac{-1}{p}\right)=1$, *then, for each* $i=1, 2$.

$$c_p(\delta_i, U_p^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise}\end{cases}$$

where $\Lambda(i)=\boldsymbol{Z}_p+\boldsymbol{Z}_p\pi_i 1_2+\boldsymbol{Z}_p y+\boldsymbol{Z}_p y\pi_i 1_2$, *for each* $i=1, 2$.

Proof. The proof is more or less similar as the proof of Proposition 5.5, and will be omitted here. q.e.d.

5.3. Now, we treat the case $q=n=3$.

Proposition 5.8. *There exist exactly two 3-integral* G_q^**-conjugacy classes in* $C_3(3)$. *The representatives* δ_1, δ_2 *of such classes, and* $K(\delta_i)_3$, $Z_G(\delta_i)_p$ $(i=1, 2)$ *are given as follows*:

$$\delta_1=\left(\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1 & \varepsilon\\ -3\varepsilon & 1\end{pmatrix}\right)\in (U_3^*)^2,$$

$$K(\delta_1)_3=\boldsymbol{Q}_3\left(\begin{pmatrix}0 & \omega\\ 3\omega & 0\end{pmatrix}\right),$$

$$Z_G(\delta_1)_3=K(\delta_1)_3^\times\cup yK(\delta_1)^\times, \quad \textit{and}$$

$$\delta_2=\left(\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}, \frac{b}{3}\begin{pmatrix}1 & \varepsilon\\ 3\varepsilon & 1\end{pmatrix}\right)\in (U_3^*)^2,$$

$$K(\delta_2)_3=\boldsymbol{Q}_3\left(\begin{pmatrix}0 & \omega\\ -3\omega & 0\end{pmatrix}\right),$$

$$Z_G(\delta_2)_3=K(\delta_2)_3^\times\cup yK(\delta_2)_3^\times,$$

where

$$\omega=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, \quad \varepsilon=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\in M_2(\boldsymbol{Q}_3)=B_3, \quad y=\begin{pmatrix}\omega & 0\\ 0 & -\omega\end{pmatrix}\in M_2(B_3),$$

and b *is a fixed element of* $\boldsymbol{Q}_3(\omega)$ *such that* $N(b)=-1$.

The local data are given as follows: *for each* $i=1, 2$,

$$c_3(\delta_i, U_3^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

where

$$\Lambda(1)=\left\{\begin{pmatrix} x & y\\ 3\bar{y} & \bar{x}\end{pmatrix};\ x, y\in \boldsymbol{Z}_3[\omega]\right\},\quad \text{and}$$

$$\Lambda(2)=\left\{\begin{pmatrix} x & y\\ -3\bar{y} & \bar{x}\end{pmatrix};\ x, y\in \boldsymbol{Z}_3[\omega]\right\}.$$

Proof. The proof is more or less similar to the proof of Proposition 5.5, and will be omitted here. q.e.d.

5.4. Finally, we treat the case $q=2$ (and $n=2$ or 3). This is the most elaborate case, but here we shall omit the proofs, because it seems too lengthy to write them down. First, we treat $C_3(2)$. There exist elements $\omega, \eta\in O_2$ such that $\eta^2+\eta+1=0$, $\omega^2=-1$, and $\omega\eta=\eta^{-1}\omega$. We fix such pair η, ω once and for all, and put $\eta'=2\eta+1$.

Proposition 5.9. *There exists exactly four 2-integral G_2^*-conjugacy classes in $C_3(2)$. The representatives $\delta_1, \delta_2, \delta_3, \delta_4$ of such classes and $K(\delta_i)_2$, $Z_G(\delta_i)_2$ $(i=1, \cdots, 4)$ are given as follows*:

$$\delta_i=\left(\omega b_i\begin{pmatrix}0 & 1\\ \lambda_i & 0\end{pmatrix}, \begin{pmatrix}\eta & 0\\ 0 & \eta\end{pmatrix}\right)\in (U_2^*)^2 \quad (i=1, \cdots, 4),$$

$$K(\delta_i)_2=\boldsymbol{Q}_2\left(\begin{pmatrix}0 & \eta'\\ -\lambda_i\eta' & 0\end{pmatrix}\right),$$

$$Z_G(\delta_i)_2=K(\delta_i)_2^\times\cup yK(\delta_i)_2^\times \quad (i=1, \cdots, 4),$$

where $\lambda_1=1$, $\lambda_2=-1$, $\lambda_3=\dfrac{1}{3}$, $\lambda_4=\dfrac{-1}{3}$, *each* b_i $(1\leqq i\leqq 4)$ *is a fixed element of* $\boldsymbol{Z}_2[\eta]_2^\times$ *such that* $N(b_i)=\lambda$, *and* $y=\begin{pmatrix}\eta' & 0\\ 0 & -\eta'\end{pmatrix}$.

The local data are given as follows:

$$c_2(\delta_1, U_2^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(1),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

$$c_2(\delta_2, U_2^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(2),\\ 1 & \cdots \text{ if } \Lambda\sim\Lambda'(2),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

$$c_2(\delta_3, U_2^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(3),\\ 1 & \cdots \text{ if } \Lambda\sim\Lambda'(3),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

$$c_4(\delta_4, U_2^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(4),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

where

$$\Lambda(i)=\left\{\begin{pmatrix} x & y\\ \lambda_i\bar{y} & \bar{x}\end{pmatrix};\ x, y\in \boldsymbol{Z}_2[\eta]\right\}\quad (i=1, \cdots, 4),$$

and

$$\Lambda'(i)=\begin{pmatrix}1 & -\eta'\\ 0 & 2\end{pmatrix}^{-1} M_2(O_2)\begin{pmatrix}1 & -\eta'\\ 0 & 2\end{pmatrix}\cap (K(\delta_i)_2+yK(\delta_i)_2)\quad (i=2, 3).$$

Next, we consider $C_2(2)$. In this case, $Z(\gamma)_2$ is the division quaternion algebra over $\boldsymbol{Q}_2$ for any $C_2(2)$. So, by Proposition 3.6, $C_2(2)$ consists of seven G_2-conjugacy classes. Fix an isomorphism O_2 with $M_2(\boldsymbol{Z}_2)$, and identify O_2 with $M_2(\boldsymbol{Z}_2)$. Put $\omega=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $\varepsilon=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\in O_2$.

Proposition 5.10. *Any G_2-conjugacy classes in $C_2(2)$ are 2-integral. The representatives $\delta_1, \cdots, \delta_7$ of conjugacy classes in $C_2(2)$, and $K(\delta_i)_2$, $Z_G(\delta_i)_2$ $(i=1, \cdots, 7)$ are given as follows (, identifying G_2 with G_2^* for some of them)*:

$$\delta_i=\left(\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}, \varepsilon\begin{pmatrix}a_i & b_i\\ b_i & d_i\end{pmatrix}\right)\in (U_2^*)^2\quad (i=1, 2, 3),$$

$$K(\delta_i)_2=\boldsymbol{Q}_2\left(\begin{pmatrix}1 & -\bar{a}_i/\bar{b}_i\\ -a_i/b_i & -1\end{pmatrix}\right),$$

and

$$Z_G(\delta_i)_2=K(\delta_i)_2^\times\cup y_iK(\delta_i)_2^\times\quad (i=1, 2, 3),$$

where a_i, b_i $(i=1, 2, 3)$ are fixed elements of $\boldsymbol{Z}_2[\omega]$ such that $N(a_i)+N(b_i)=-1$, $N(b_1)=2$, $N(b_2)=10$, $N(b_3)=5$, $d_i=-\bar{b}_i^{-1}\bar{b}_i\bar{a}_i$ $(i=1, 2, 3)$, and $y_i=\begin{pmatrix}0 & \bar{a}_i/\bar{b}_i\\ a_i/b_i & 0\end{pmatrix}$

$$\delta_j=\left(\begin{pmatrix}\omega & 0\\ 0 & \omega\end{pmatrix}, \begin{pmatrix}0 & 1\\ \lambda_j & 0\end{pmatrix}\right)\in (U_2^*)^2\quad (j=4, 5),$$

$$K(\delta_j)_2=\boldsymbol{Q}_2\left(\begin{pmatrix}0 & \omega\\ -\lambda_j\omega & 0\end{pmatrix}\right),$$

$$Z_G(\delta_j)_2=K(\delta_j)_2^\times\cup\begin{pmatrix}\omega & 0\\ 0 & -\omega\end{pmatrix}K(\delta_j)^\times\quad (j=4, 5),$$

where $\lambda_4=-1$, $\lambda_5=-5$, and

$$\delta_k=\left(\begin{pmatrix}\omega & \bar{\pi}\omega\varepsilon\\ 0 & \omega\end{pmatrix}, \begin{pmatrix}-b_k\lambda_k & \pi^{-1}(\pi\bar{b}_k-\pi^{-1}\bar{b}_k^{-1})\varepsilon\\ \varepsilon\pi\lambda_k b_k & \bar{b}_k\lambda_k\end{pmatrix}\right)\in (U_2^*)^2,\quad (k=6,7),$$

$$K(\delta_k)_2=\left\{\begin{pmatrix}x+y\lambda_k\pi^{-1}\omega\varepsilon, & y\omega(2^{-1}\lambda_k-1)\\ y\lambda_k\omega, & x+y\lambda_k\omega\pi^{-1}\varepsilon\end{pmatrix};\ x,\ y\in \boldsymbol{Q}_2\right\},$$

$$Z_G(\delta_k)_2=K(\delta_k)^\times\cup\begin{pmatrix}\omega & 0\\ 0 & -\omega\end{pmatrix}K(\delta_k)^\times\quad (k=6,7),$$

where $\lambda_6=-2$, $\lambda_7=-10$, $\pi=1+\omega$, *and* b_6, b_7 *are fixed elements of* $\boldsymbol{Q}_2[\omega]$ *such that* $N(b_6)=\dfrac{1}{2}$, $N(b_7)=\dfrac{1}{10}$.

Proposition 5.11. *Notations being as in Proposition* 5.10, *local data for* δ_i $(i=1,\cdots,7)$ *are given as follows:*

For each $i=1$, 2, *or* 3,

$$c_2(\delta_i, U_2, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise.}\end{cases}$$

where $\Lambda(i)=M_2(O_2)\cap(K(\delta_i)+y_iK(\delta_i))$ $(i=1,2,3)$.

For each $i=4$, 5,

$$c_2(\delta_i, U_2^*, \Lambda)=\begin{cases}3 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

where $\Lambda(i)=\left\{\begin{pmatrix}a & b\\ -\lambda_i\bar{b} & \bar{a}\end{pmatrix};\ a,\ b\in \boldsymbol{Z}_2[\omega]\right\}$ $(i=4,5)$.

For each $i=6$, 7,

$$c_2(\delta_i, U_2^*, \Lambda)=\begin{cases}1 & \cdots \text{ if } \Lambda\sim\Lambda(i),\\ 0 & \cdots \text{ otherwise,}\end{cases}$$

where $\Lambda(i)=\left(K(\delta_i)_2+\begin{pmatrix}\omega & 0\\ 0 & -\omega\end{pmatrix}K(\delta_i)_2\right)\cap M_2(O_2)$ $(i=6,7)$.

For each $i=1,\cdots,7$, put $\delta_i=(\alpha_i,\beta_i)\in C_2(2)$, where δ_i are as in Proposition 10. Then, $\boldsymbol{Q}_2(\alpha_i,\beta_i)$ is the division quaternion algebra over $\boldsymbol{Q}_2$. In the next section, we shall use the following Lemma.

Lemma 5.12. *The order* $\boldsymbol{Q}_2(\alpha_i,\beta_i)\cap M_2(O_2)$ *is the* (*unique*) *maximal order of* $\boldsymbol{Q}_2(\alpha_i,\beta_i)$ *for each* $i=1$, 2, 6, *or* 7, *and not maximal for each* $i=3$, 4, 5.

Proof. The unique maximal order of $\boldsymbol{Q}_2(\alpha_i,\beta_i)$ is explicitly given by

$$\boldsymbol{Z}_2+\boldsymbol{Z}_2\alpha_i+\boldsymbol{Z}_2\beta_i+\boldsymbol{Z}_2\frac{1+\alpha_i+\beta_i+\alpha_i\beta_i}{2}.$$

By direct calculation, we can show that $(1+\alpha_i+\beta_i+\alpha_i\beta_i)/2 \in M_2(O_2)$, if and only if $i=1, 2, 6$, or 7. q.e.d.

§ 6. Explicit mass formulae

In this section, we give the explicit mass formulae for $m(\mathscr{L}(M), \{\gamma\}_{GL})$ for any $\gamma \in C_2$ or C_3, gathering local data in § 5 together. Any element $g \in G^r$, or the G-conjugacy class which contains g is called locally integral, if g is q-integral for every prime q.

Proposition 6.1. *For any $g \in C_2$, g is locally integral, if and only if $K(g) \cong \boldsymbol{Q}(\sqrt{-p})$ and $p \not\equiv 7 \bmod 8$, or $K(g) \cong \boldsymbol{Q}(\sqrt{-2p})$. For any $g \in C_3$, g is locally integral, if and only if $K(g) \cong \boldsymbol{Q}(\sqrt{-3p})$.*

Proof. If $g \in C_2$ is locally integral, then by Proposition 5.4, $K(g) \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_p$ is ramified over $\boldsymbol{Q}_p$, and by Proposition 5.1, $K(g) \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_q$ is not ramified over $\boldsymbol{Q}_q$ for any $q \neq 2$. As $K(g)$ is imaginary quadratic, and $K(g)_2 \not\cong \boldsymbol{Q}_2 \oplus \boldsymbol{Q}_2$, we get the assertion for C_2. The assertion for $g \in C_3$ is obtained similarly by Propositions 5.1, 5.6, and 5.8. q.e.d.

Now, we shall calculate $M_G(\Lambda)$ for each locally integral $g \in C_2$, or C_3, and $\Lambda \subset Z(g) = K(g) + yK(g)$, where $y \in G$ is taken as in Proposition 3.7 for each g. We have

$$\Lambda^\times \cap G = \Lambda^\times \cap Z_G(g) = (\Lambda^\times \cap K(g)^\times) \cup (\Lambda^\times \cap yK(g)^\times).$$

For any order Λ, we get $\Lambda^\times \cap G = \{\pm 1\}$. In fact, as g is locally integral, $K(g) \cong \boldsymbol{Q}(\sqrt{-p})$, $\boldsymbol{Q}(\sqrt{-2p})$, or $\boldsymbol{Q}(\sqrt{-3p})$. Denote by o_K the maximal order of $K(g)$. Then, as we assumed $p \geqq 5$, $o_K^\times = \{\pm 1\} = K(g)^\times \cap \Lambda^\times$. On the other hand, any element $y_1 \in yK(g)^\times$ satisfies $0 < y_1^2 \in \boldsymbol{Q}^\times$, because $Z(g)$ is indefinite and $K(g)$ is imaginary. As $Z(g)$ is division, $y_1^2 \neq 1$ and $y_1 y_1^\rho \neq -1$, where ρ is the main involution of $Z(g)$. If y_1 is integral, then $(y_1 y_1^\rho)^{-1} \notin \boldsymbol{Z}$, so y_1^{-1} is not integral. Hence we get $\Lambda^\times \cap yK(g)^\times = \varnothing$. By definition of $M_G(\Lambda)$, we get

$$M_G(\Lambda) = \frac{1}{2} h(\Lambda),$$

where

$$h(\Lambda) = \sharp(Z_G(g) \backslash Z_G(g)_A / (\Lambda_A^\times \cap G_A)).$$

Now, we calculate $h(\Lambda)$ for each locally integral $g \in C_2$, or C_3, and each $\Lambda \subset Z(g)$ such that $c_q(g, U_q, \Lambda) \neq 0$ for all primes q. We denote by $h(-m)$ the class number of the imaginary quadratic field $\boldsymbol{Q}(\sqrt{-m})$.

Proposition 6.2. *Assume that* $g \in C_2$ *and* $K(g) \cong \boldsymbol{Q}(\sqrt{-p})$, $p \not\equiv 7 \bmod 8$. *Then, the G-genus which contains* Λ *such that* $c_q(g, U_q, \Lambda) \neq 0$ *for all primes* q *is unique, and for that* Λ, *we get*

$$h(\Lambda) = \begin{cases} \dfrac{h(-p)}{2} & \cdots \text{ if } p \equiv 1, \text{ or } 5 \bmod 8, \\ 3h(-p) & \cdots \text{ if } p \equiv 3 \bmod 8. \end{cases}$$

Proof. The first assertion is obvious by Propositions 5.2, 5.5, and 5.11. To show the rest, first, assume that $p \equiv 1$, or $5 \bmod 8$.

Then, by Propositions 5.2, 5.5, 5.11, there exists $y_q \in yK(g)_q^\times \cap \Lambda_q^\times$ for each prime q. Besides, it is easy to see that

$$\Lambda_q^\times \cap K(g)_q^\times = (o_K \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q)^\times \quad \text{and} \quad \Lambda_q^\times \cap yK(g)_q^\times = y_q(o_K \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q)^\times$$

for any prime q, where o_K is the maximal order of $K(g)$. Hence, it is easy to see that the representatives of $Z_G(g)\backslash Z_G(g)_A/(\Lambda_A^\times \cap G_A)$ can be taken in $K(g)_A^\times$. Two elements $a, b \in K(g)_A^\times$ belong to the same double coset, if and only if $kau = b$ for some $k \in K(g)^\times$, $u \in \Lambda_A^\times \cap K(g)^\times$, or $kya(u_v') = b$ for some $k \in K(g)^\times$ and $(u_v') \in \Lambda_A^\times \cap G_A$ such that $u_q' = y_q u_q \in y_q(\Lambda_q^\times \cap K(g)_q^\times)$ for all primes q. It is easy to see that $kya(u_v') = k\bar{a}(yu_v') = k\bar{a}(yy_q)(u_v)$, where $^-$ denotes the non-trivial automorphism of $K(g)_A^\times$ which is induced from the complex conjugation of $K(g)$. Deote by $\mathfrak{y}$ the fractional ideal of $K(g)$ defined by:

$$\mathfrak{y} = \bigcap_q (yy_q(o_K \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q) \cap K(g)).$$

Denote by $C(K(g))$ the ideal class group of $K(g)$. For any classes c_1, $c_2 \in C(K(g))$, write $c_1 \sim c_2$, if $c_1 = \bar{c}_2 c(\mathfrak{y})$, where $c(\mathfrak{y})$ is the ideal class which contains $\mathfrak{y}$. It is obvious that $h(\Lambda) = \sharp(C(K(g))/\sim)$. Now, we shall show that, if $c_1 \sim c_2$, then $c_1 \neq c_2$. Take a prime p' such that $\left(\dfrac{-p}{p'}\right) = 1$ and $p' \equiv 3 \bmod 4$. Then, it is easy to see that the Hilbert symbol $(-p, p')_v = -1$ for $v = 2$ and p, and $(-p, p')_v = 1$ for all the other places v of $\boldsymbol{Q}$. As the discriminant of $Z(g)$ is $2p$, we can assume $y^2 = p'$ and $y_q = y$ for any prime $q \neq p'$. So, $c(\mathfrak{y})$ is the class which contains the prime ideal $\mathfrak{p}'$ such that $\mathfrak{p}'\bar{\mathfrak{p}}' = (p')$. For $c \in C(K(g))$, assume that $c \sim c$. Take an ideal $\mathfrak{a} \in c$. Then, $\mathfrak{a}(k) = \bar{\mathfrak{a}}\mathfrak{p}'$ for some $k \in K(g)^\times$. Taking the norm of both sides, we get $N(k) = N(\mathfrak{p}') = p'$. This contradicts to the fact that $\left(\dfrac{p'}{p}\right) = -1$. Thus, we get $h(\Lambda) = h(-p)/2$. Next, assume that $p \equiv 3 \bmod 8$. In this case, by Proposition 5.11, we can show that $\Lambda_2 \cap yK(g_2) = \varnothing$.

Besides, we can assume that $y^2=2$. So, $y \in \Lambda_q^\times \cap yK(g)_q = y(o_K \otimes_Z Z_q)^\times$ for any prime $q \neq 2$. Hence, it is obvious that the representatives of $Z_G(g)\backslash Z_G(g)_A/(\Lambda_A^\times \cap G_A)$ can be taken in $K(g)_A^\times$. As $\Lambda_2 \cap yK(g)_2 = \emptyset$, we can see that for any $a, b \in K(g)_A^\times$, $b \in Z_G(g)a(\Lambda_A^\times \cap G_A)$, if and only if $b \in K(g)a(\Lambda_A^\times \cap K(g)_A^\times)$. By Propositions 5.2, 5.5, 5.11, we get $\Lambda_q^\times \cap K(g)_q^\times = (o_K \otimes_Z Z_q)^\times$ for any prime $q \neq 2$, and

$$[(o_K \otimes_Z Z_2)^\times : \Lambda_2^\times \cap K(g)_2^\times] = \left[Z_2\left[\frac{1+\sqrt{-3}}{2}\right]^\times : Z_2[\sqrt{-3}]^\times\right] = 3.$$

Hence, $h = 3h(-p)$. q.e.d.

Proposition 6.3. *Assume that $g \in C_2$ and $K(g) \cong \boldsymbol{Q}(\sqrt{-2p})$. Then, the G-genus which contains Λ such that $c_q(g, U_q, \Lambda) \neq 0$ for all primes q is unique, and for that Λ, we get*

$$h(\Lambda) = \frac{h(-2p)}{2}.$$

Proof. Take a prime p' such that $p' \equiv 5 \bmod 8$ and $\left(\frac{p'}{p}\right) = -1$. We can assume that $y^2 = p'$, where y is as before. As

$$\Lambda_q^\times \cap K(g)_q^\times = (o_K \otimes_Z Z_q)^\times \quad \text{and} \quad \Lambda_q^\times \cap yK(g)_q = y_q(o_K \otimes_Z Z_q)^\times$$

for some $y_q \in \Lambda_q^\times$ for every prime q, the proof is obtained virtually in the same way as in the case $K(g) \cong \boldsymbol{Q}(\sqrt{-p})$ and $p \equiv 1 \bmod 4$. The details will be omitted here. q.e.d.

Proposition 6.4. *Assume that $g \in C_3$ and $K(g) \cong \boldsymbol{Q}(\sqrt{-3p})$. If $p \equiv 3 \bmod 4$, the G-genus which contains Λ such that $c_q(g, U_q, \Lambda) \neq 0$ for all primes q is unique, and for that Λ, we get*

$$h(\Lambda) = \frac{h(-3p)}{2}.$$

If $p \equiv 1 \bmod 4$, there are exactly two G-genera $L_G(\Lambda)$, $L_G(\Lambda')$ such that $c_q(g, U_q, \Lambda) \neq 0$ and $c_q(g, U_q, \Lambda') = 0$ for all primes q. We can assume $\Lambda_2 \sim \Lambda(i)$ and $\Lambda_2' \sim \Lambda'(i)$, where $i = 2$ (resp. 3), if $p \equiv 5$ (resp. 1) $\bmod 8$ and $\Lambda(i)$ and $\Lambda'(i)$ are as in Proposition 5.9. For these orders, we get

$$h(\Lambda) = \begin{cases} \dfrac{h(-3p)}{2} & \cdots \text{ if } p \equiv 5 \bmod 8, \\ \dfrac{3h(-3p)}{2} & \cdots \text{ if } p \equiv 1 \bmod 8, \end{cases}$$

$$h(\Lambda')=\frac{h(-3p)}{2} \quad \cdots \text{ if } p\equiv 1 \bmod 4.$$

Proof. Take a prime p' such that $p'\equiv 5 \bmod 12$ and $\left(\frac{p'}{p}\right)=-1$. We can assume $y^2=p'$. If $p\not\equiv 1 \bmod 8$, or $q\neq 2$, we get

$$\Lambda_q^\times \cap K(g)_q^\times=(\Lambda'_q)^\times \cap K(g)_q^\times=(o_K\otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q)^\times,$$

and

$$\Lambda_q^\times \cap yK(g)_q^\times=(\Lambda'_q)^\times \cap yK(g)_q^\times=y_q(o_K\otimes_{\boldsymbol{Z}} \boldsymbol{Z}_q)^\times$$

for some $y_q \in \Lambda_q$. When $p\equiv 1 \bmod 8$, we get $(\Lambda'_2)^\times \cap K(g)_2^\times=(o_K\otimes_{\boldsymbol{Z}} \boldsymbol{Z}_2)^\times$,

$$(\Lambda'_2)^\times \cap yK(g)_2^\times=y(o_K\otimes_{\boldsymbol{Z}} \boldsymbol{Z}_2)^\times, \quad \text{and} \quad \Lambda_2^\times \cap K(g)_2\cong \boldsymbol{Z}_2[\sqrt{-3}]^\times.$$

So, the proof is obtained virtually in the same way as in the proof of Proposition 6.2. q.e.d.

Theorem 6.5. *Assume that* $p\geqq 5$. *Then,*

$$m(\mathscr{L}(M), C_2)=\begin{cases} \dfrac{3h(-p)}{4}+\dfrac{h(-2p)}{4} & \cdots \text{ if } p\equiv 1, \text{ or } 5 \bmod 8, \\ \dfrac{3h(-p)}{2}+\dfrac{h(-2p)}{4} & \cdots \text{ if } p\equiv 3 \bmod 8, \\ \dfrac{h(-2p)}{4} & \cdots \text{ if } p\equiv 7 \bmod 8, \end{cases}$$

and

$$m(\mathscr{L}(M), C_3)=\begin{cases} h(-3p) & \cdots \text{ if } p\equiv 1 \bmod 8, \\ \dfrac{h(-3p)}{4} & \cdots \text{ if } p\equiv 3, \text{ or } 7 \bmod 8, \\ \dfrac{h(-3p)}{2} & \cdots \text{ if } p\equiv 5 \bmod 8. \end{cases}$$

Proof. This is easily obtained by Theorem 1.1 and Propositions in § 5 and Propositions 6.2, 6.3, 6.4. q.e.d.

Finally, we shall give some refinement of Proposition 6.1. Assume that $\Gamma_i \ni \alpha, \beta$ for some $\gamma=(\alpha, \beta) \in C_2$ and some i $(1\leqq i\leqq H)$. By Proposition 6.1, we have $K(\gamma)=\boldsymbol{Q}(\sqrt{-p})$, or $\boldsymbol{Q}(\sqrt{-2p})$. More precisely, we have

Proposition 6.6. *Assumptions being as above, Γ_i has a subgroup Γ such that $\Gamma \ni \alpha, \beta$ and $\Gamma/\{\pm 1\} \cong A_4$, if and only if $K(\gamma) \cong \boldsymbol{Q}(\sqrt{-2p})$.*

Proof. Put $R_i = \{g \in M_2(B);\ L_i g \subset L_i\}$ as before. By Lemma 5.12, $\Lambda = \boldsymbol{Q}(\alpha, \beta) \cap R_i$ is a maximal order of $\boldsymbol{Q}(\alpha, \beta)$, if and only if $K(\gamma) \cong \boldsymbol{Q}(\sqrt{-2p})$. If Λ is maximal, then, noting that $\Lambda \supset Z[\alpha, \beta]$, we can see easily that

$$\Lambda = Z + Z\alpha + Z\beta + Z\frac{1+\alpha+\beta+\alpha\beta}{2},$$

and

$$\Lambda^\times \cap G = \left\{\pm 1, \pm\alpha, \pm\beta, \frac{\pm 1 \pm \alpha \pm \beta \pm \alpha\beta}{2}\right\},$$

and $(\Lambda^\times \cap G)/\{\pm 1\} \cong A_4$. This proves that the condition $K(\gamma) \cong \boldsymbol{Q}(\sqrt{-2p})$ is sufficient. Now, we show that the condition is necessary. Assume that there exists a subgroup $\Gamma \subset \Gamma_i$ such that $\Gamma \ni \alpha, \beta$, and $\Gamma/\{\pm 1\} \cong A_4$. As we shall see in the next Lemma 6.7, we get $\Gamma \subset \boldsymbol{Q}(\alpha, \beta)$. If $K(\gamma) \cong \boldsymbol{Q}(\sqrt{-p})$, then $\Lambda = \boldsymbol{Z}[\alpha, \beta]$, and $\Lambda^\times \cap G = \{\pm 1, \pm\alpha, \pm\beta, \pm\alpha\beta\}$. As $(\Lambda^\times \cap G)/\{\pm 1\} = (\boldsymbol{Z}/2\boldsymbol{Z})^2$ in this case, we get a contradiction. Hence, $K(\gamma) \cong \boldsymbol{Q}(\sqrt{-2p})$. q.e.d.

Lemma 6.7. *Assume that there exists a subgroup $\Gamma \subset \Gamma_i$ such that $\Gamma/\{\pm 1\} \cong A_4$. Then, there exists $\gamma = (\alpha, \beta) \in C_2$ such that $\alpha, \beta \in \Gamma$. For any such $\gamma = (\alpha, \beta) \in C_2$, we get $\Gamma \subset \boldsymbol{Q}(\alpha, \beta)$.*

Proof. Fix an isomorphism $\Gamma/\{\pm 1\} \cong A_4$ and fix any representatives σ (resp. τ) in Γ of (12) (34) (resp. (123)) $\in A_4$. Replacing σ by $-\sigma$, or τ by $-\tau$, if necessary, we can assume that $\tau^3 = 1$ and $(\sigma\tau)^3 = 1$. Then, by Theorem 3.1, we have $\sigma^2 = -1$, $\tau^2 + \tau + 1 = 0$, and $(\sigma\tau)^2 + (\sigma\tau) + 1 = 0$. So, we get $\tau\sigma\tau^{-1} = -\tau^2 + \sigma\tau$ and $\sigma\tau\sigma\tau^{-1} = -\sigma\tau^2 - \tau$. Now, put $\alpha = \sigma$, $\beta = \tau\sigma\tau^{-1}$. Then $(\alpha, \beta) \in C_2$, and $(-1 + \alpha + \beta - \alpha\beta)/2 = (-1 + \tau - \tau^2 + \sigma(1 + \tau + \tau^2)) = \tau$. Hence, $\tau \in \boldsymbol{Q}(\alpha, \beta)$. As A_4 is generated by (12) (34), (13) (24), and (123), we get $\Gamma \subset \boldsymbol{Q}(\alpha, \beta)$. q.e.d.

§ 7. Main Theorems

Here, we give our main results. For the readers' convenience, we recall here the notations and assumptions in the previous sections. We denote by B the definite quaternion algebra with prime discriminant p. We denote by $L_1, \cdots, L_H$ a complete set of representatives of classes of lattices in the *non-principal* genus $\mathscr{L}(M)$ of the positive definite binary

quaternion hermitian space V over B. For each i $(1 \leqq i \leqq H)$, define a subgroup Γ_i of G by:

$$\Gamma_i = \{g \in G;\ L_i g = L_i\},$$

where G is the group of similitudes of V. For any (abstract) finite group Γ, we put

$$I(\Gamma) = \{i \in \{1, \cdots, H\};\ \Gamma_i/\{\pm 1\} \cong \Gamma\}.$$

Theorem 7.1. *Assume that $p \geqq 7$. Then, for each prime p,*

$$\sharp(I(\{1\})) = \frac{p^2-1}{2880} - \frac{1}{96}\left(4+\left(\frac{-1}{p}\right)\right)\left(p-\left(\frac{-1}{p}\right)\right)$$
$$-\frac{1}{144}\left(3+\left(\frac{-3}{p}\right)\right)\left(p-\left(\frac{-3}{p}\right)\right)+\frac{1}{8}(1-\chi(2))h(-p)$$
$$+\frac{1}{8}h(-2p)+\begin{cases}\frac{1}{8}(3-\chi'(2))h(-3p) & \cdots \text{ if } p\equiv 1 \bmod 4,\\ \frac{1}{8}h(-3p) & \cdots \text{ if } p\equiv 3 \bmod 4,\end{cases}$$
$$-\frac{5}{12}\sharp(I(D_{12}))-\frac{1}{2}\sharp(I(S_4))-\frac{3}{5}\sharp(I(A_5)),$$

$$\sharp(I(\boldsymbol{Z}/2\boldsymbol{Z})) = \frac{1}{48}\left(4+\left(\frac{-1}{p}\right)\right)\left(p-\left(\frac{-1}{p}\right)\right)-\frac{3}{8}(1-\chi(2))h(-p)$$
$$-\frac{h(-2p)}{8}-\begin{cases}\frac{1}{4}(3-\chi'(2))h(-3p) & \cdots \text{ if } p\equiv 1 \bmod 4,\\ \frac{h(-3p)}{4} & \cdots \text{ if } p\equiv 3 \bmod 4,\end{cases}$$
$$+\frac{5}{4}\sharp(I(S_4))+\frac{4}{3}\sharp(I(D_{12}))+\sharp(I(A_5)),$$

$$\sharp(I(\boldsymbol{Z}/3\boldsymbol{Z})) = \frac{1}{48}\left(3+\left(\frac{-3}{p}\right)\right)\left(p-\left(\frac{-3}{p}\right)\right)-\frac{h(-2p)}{4}$$
$$-\begin{cases}\frac{1}{8}(3-\chi'(2))h(-3p) & \cdots \text{ if } p\equiv 1 \bmod 4,\\ \frac{h(-3p)}{8} & \cdots \text{ if } p\equiv 3 \bmod 4.\end{cases}$$
$$+\frac{1}{4}\sharp(I(D_{12}))+\frac{1}{2}\sharp(I(S_4))+\sharp(I(A_5)),$$

$$\sharp(I((\boldsymbol{Z}/2\boldsymbol{Z})^2))=\frac{1}{4}(1-\chi(2))h(-p)-\sharp(I(D_{12}))-\frac{1}{2}\sharp(I(S_4)),$$

$$\sharp(I(S_3))=\begin{cases}\dfrac{1}{4}(3-\chi'(2))h(-3p) & \cdots \text{ if } p\equiv 1 \bmod 4,\\ \dfrac{h(-3p)}{4} & \cdots \text{ if } p\equiv 3 \bmod 4,\end{cases}$$
$$-\sharp(I(A_5))-\sharp(I(D_{12}))-\sharp(I(S_4)),$$

$$\sharp(I(A_4))=\frac{h(-2p)}{4}-\sharp(I(A_5))-\frac{1}{2}\sharp(I(S_4)),$$

$$\sharp(I(D_{12}))=\begin{cases}1 & \cdots \text{ if } p\equiv 5 \bmod 12,\\ 0 & \cdots \text{ if } p\equiv 1,\ 7, \text{ or } 11 \bmod 12,\end{cases}$$

$$\sharp(I(S_4))=\begin{cases}1 & \cdots \text{ if } p\equiv 3, \text{ or } 5 \bmod 8,\\ 0 & \cdots \text{ if } p\equiv 1, \text{ or } 7 \bmod 8,\end{cases}$$

$$\sharp(I(A_5))=\begin{cases}1 & \cdots \text{ if } p\equiv 2, \text{ or } 3 \bmod 5,\\ 0 & \cdots \text{ if } p\equiv 1, \text{ or } 4 \bmod 5,\end{cases}$$

and $\sharp(I(\Gamma))=0$, unless Γ is isomorphic to one of the above groups, where $h(-m)$ is the class number of the field $\boldsymbol{Q}(\sqrt{-m})$, and $\left(\frac{*}{p}\right)$ is the Legendre symbol, χ (resp. χ') is the Kronecker symbol of $\boldsymbol{Q}(\sqrt{-p})$ (resp. $\boldsymbol{Q}(\sqrt{-3p})$), that is,

$$\chi(2)=\begin{cases}1 & \cdots \text{ if } p\equiv 7 \bmod 8,\\ -1 & \cdots \text{ if } p\equiv 3 \bmod 8,\\ 0 & \cdots \text{ if } p\equiv 1 \bmod 4,\end{cases}\qquad \chi'(2)=\begin{cases}1 & \cdots \text{ if } p\equiv 5 \bmod 8,\\ -1 & \cdots \text{ if } p\equiv 1 \bmod 8,\\ 0 & \cdots \text{ if } p\equiv 3 \bmod 4.\end{cases}$$

Remark 1. If $p=2$, 3, or 5, then $H=1$ ([5]). If $p=2$, then $\sharp(\Gamma_1)=1920$ and Γ_1 was explicitly given in [10] p. 592. It was shown in Katsura-Oort [12] that, if $p=3$, then $\Gamma_1/\{\pm 1\}\cong A_6$, and if $p=5$, then $\Gamma_1/\{\pm 1\}\cong PGL(2, \boldsymbol{F}_5)$.

Remark 2. By Theorem 7.1 and the fact that $\sharp(I(A_4))$ and $\sharp(I((\boldsymbol{Z}/2\boldsymbol{Z})^2)$ are integers, we can show that $h(-p)\equiv 0$ (resp. 2) mod 4, if $p\equiv 1$ (resp. 5) mod 8, and that $h(-2p)\equiv 0$ (resp. 2) mod 4, if $p\equiv \pm 1$ (resp. ± 3) mod 8. These results are actually well known. (cf. Redei-Reichart [14])

Proof. The results on D_{12}, S_4, and A_5 have been already given in § 3 and § 4. Now, we show the rest. For each (abstract) finite group Γ and for each $n=2$, or 3, define a number $c_n(\Gamma)$ as follows:

$$c_n(\Gamma)=\#\{(\alpha,\beta)\in\Gamma^2;\ \alpha^2=\beta^n=1,\ \alpha\beta=\beta^{-1}\alpha,\ \alpha\neq\beta\}/\#(\Gamma)\times\begin{cases}2 & \cdots \text{ if } n=2,\\ 1 & \cdots \text{ if } n=3.\end{cases}$$

By the argument in § 3.2, we can easily show that

$$\begin{aligned}c_n(\Gamma_i/\{\pm 1\})&=\#(C_n\cap\Gamma_i^2)/\#(\Gamma_i)\\&=\#\{\gamma=(\alpha,\beta)\in C_n;\ \alpha,\beta\in\Gamma_i\}/\#(\Gamma_i)\quad (i=1,\cdots,H).\end{aligned}$$

We have $c_3(S_3)=c_3(D_{12})=c_3(S_4)=c_3(A_5)=1$. Hence, by Lemma 2.1 and by definition of the "mass", we get

$$m(\mathscr{L}(M),C_3)=\#(I(S_3))+\#(I(D_{12}))+\#(I(S_4))+\#(I(A_5)).$$

Hence, by Theorem 6.5, we get the assertion for $I(S_3)$. We get $c_2((\boldsymbol{Z}/2\boldsymbol{Z})^2)=c_2(D_{12})=3$, $c_2(A_4)=c_2(A_5)=1$, and $c_2(S_4)=2$. Now, define a number $c_2'(\Gamma)$ for each Γ by

$$c_2'(\Gamma)=\frac{2}{\#(\Gamma)}\times\#\left\{(\alpha,\beta)\in\Gamma^2;\ \begin{array}{l}\alpha^2=\beta^2=1,\ \alpha\beta=\beta\alpha,\ \alpha\neq\beta\\ \alpha,\beta \text{ are contained in a subgroup}\\ \text{of } \Gamma \text{ which is isomorphic to } A_4\end{array}\right\}.$$

Then, $c_2'((\boldsymbol{Z}/2\boldsymbol{Z})^2)=c_2'(D_{12})=0$, $c_2'(A_4)=c_2'(A_5)=1$, and $c_2'(S_4)=\frac{1}{2}$. By Lemma 2.1, Theorem 6.5, and Proposition 6.6, we get

$$3\#(I((\boldsymbol{Z}/2\boldsymbol{Z})^2)+\frac{3}{2}\#(I(S_4))+3\#(I(D_{12}))=\frac{1}{4}(1-\chi(2))h(-p),$$

and

$$\#(I(A_4))+\frac{1}{2}\#(I(S_4))+\#(I(A_5))=\begin{cases}\frac{1}{4}(3-\chi'(2))h(-3p), & \text{if } p\equiv 1 \bmod 4,\\ \frac{h(-3p)}{4} & \text{if } p\equiv 3 \bmod 4.\end{cases}$$

Hence, we get the assertion for $(\boldsymbol{Z}/2\boldsymbol{Z})^2$ and A_4. The rest is easily obtained by Theorem 2.2 and (2.3), noting that $M(\Gamma,1)=\frac{1}{\#(\Gamma)}$ for any finite group Γ, and

$$M(\boldsymbol{Z}/2\boldsymbol{Z}, 2)=\frac{1}{2},\quad M((\boldsymbol{Z}/2\boldsymbol{Z})^2, 2)=\frac{3}{4},\quad M(S_3, 2)=\frac{1}{2},$$

$$M(A_4, 2)=\frac{1}{4},\quad M(D_{12}, 2)=\frac{7}{12},\quad M(S_4, 2)=\frac{3}{8},\quad M(A_5, 2)=\frac{1}{4},$$

$$M(\boldsymbol{Z}/3\boldsymbol{Z}, 3)=\frac{2}{3},\quad M(S_3, 3)=\frac{1}{3},\quad M(A_4, 3)=\frac{2}{3},\quad M(D_{12}, 3)=\frac{1}{6},$$

$$M(S_4, 3)=\frac{1}{3},\quad \text{and}\quad M(A_5, 3)=\frac{1}{3}.$$ q.e.d.

Numerical examples. For small primes p, the explicit values of $\sharp(I(\Gamma))$ for each finite group Γ are given in the following table. When $p\leqq 31$ and $p\neq 23$, such table has been already given in Katsura-Oort [12], but we include also these cases below for the readers' convenience. In order to calculate the following table by Theorem 7.1, we used the table of class numbers of imaginary quadratic fields by H. Wada [17].

p \ Γ	$\{1\}$	$\boldsymbol{Z}/2\boldsymbol{Z}$	$\boldsymbol{Z}/3\boldsymbol{Z}$	$(\boldsymbol{Z}/2\boldsymbol{Z})^2$	S_3	A_4	S_4	D_{12}	A_5
7	0	0	0	0	0	0	0	0	1
11	0	0	0	0	0	0	1	0	0
13	0	0	0	0	0	0	1	0	1
17	0	0	0	0	0	0	0	1	1
19	0	0	0	0	0	1	1	0	0
23	0	0	0	0	1	0	0	0	1
29	0	0	0	0	1	0	1	1	0
31	0	0	0	0	1	2	0	0	0
37	0	0	0	0	2	1	1	0	1
41	0	0	0	1	1	1	0	1	0
43	0	0	1	0	1	1	1	0	1
47	0	1	0	0	1	1	0	0	1
53	0	1	0	0	2	0	1	1	1
59	0	1	1	1	0	1	1	0	0
61	0	0	1	1	3	2	1	0	0
67	0	1	2	0	1	2	1	0	1
71	0	2	1	0	2	1	0	0	0
73	0	1	1	1	3	3	0	0	1
79	0	1	3	0	3	2	0	0	0
83	1	1	1	1	1	1	1	0	1
89	0	3	1	2	1	2	0	1	0
97	0	3	2	1	3	4	0	0	1
101	1	2	1	2	3	1	1	1	0
103	1	2	3	0	2	4	0	0	1
107	2	1	2	1	3	0	1	0	1
109	0	3	4	1	5	2	1	0	0
113	1	4	1	1	4	1	0	1	1
127	2	2	5	0	4	3	0	0	1

Now, we give here explicit answers to Problem 2 also in some other cases. Consider the definite quaternion algebra B over $\boldsymbol{Q}$ with discriminant D, where D is not necessarily prime. Let O be a maximal order of B. Take any positive divisor D_2 of D and put $D_1=D/D_2$. Let $\mathscr{L}(D_1, D_2)$ be the set of all maximal O-lattices $L\subset B^2$ such that $L\otimes_{\boldsymbol{Z}}\boldsymbol{Z}_q\cong O_q^2$, if and only if $p\nmid D_2$. This $\mathscr{L}(D_1, D_2)$ forms a single genus (Shimura [16]). Take a complete set of representatives $L_1, \cdots, L_H$ of the classes in $\mathscr{L}(D_1, D_2)$, and put $\Gamma_i=\mathrm{Aut}(L_i)$ $(1\leqq i\leqq H)$. For any finite group Γ, put $I(\Gamma)=\#\{i;\ \Gamma_i/\{\pm 1\}\cong\Gamma,\ 1\leqq i\leqq H\}$.

Theorem 7.2. *Assume that* 2, 3, $5\nmid D$ *and* $D_2\neq 1$. *Put* $t=\#\{p; p\mid D\}$ *and* $r=\#\{p; p\mid D_1\}$. *Then,*

$$\#(I(\boldsymbol{Z}/5\boldsymbol{Z}))=\begin{cases}2^{t+r-2}, & \text{if } p\equiv -1 \bmod 5 \text{ for all } p\mid D_1\ (D_1\neq 1)\\ & \text{and } p\equiv \pm 2 \bmod 5 \text{ for all } p\mid D_2,\\ 0 & \text{otherwise,}\end{cases}$$

$$\#(I(A_5))=\begin{cases}2^{t-1}, & \text{if } D_1=1 \text{ and } p\equiv \pm 2 \bmod 5 \text{ for all } p\mid D,\\ 0 & \text{otherwise,}\end{cases}$$

$$\#(I(\boldsymbol{Z}/4\boldsymbol{Z}))=\begin{cases}2^{t+s-1}, & \text{if } D_1\neq 1,\ p\not\equiv 1 \bmod 8 \text{ for all } p\mid D_1\\ & \text{and } p\equiv \pm 3 \bmod 8 \text{ for all } p\mid D_2,\\ 0 & \text{otherwise,}\end{cases}$$

where $s=\#\{p\mid D_1;\ p\equiv -1 \bmod 8\}$,

$$\#(I(S_4))=\begin{cases}2^{t-1}, & \text{if } D_1=1 \text{ and } p\equiv \pm 3 \bmod 8, \text{ for all } p\mid D,\\ 0 & \text{otherwise,}\end{cases}$$

$$\#(I(\boldsymbol{Z}/6\boldsymbol{Z}))=\begin{cases}2^{t+u-3}, & \text{if } D_1(-1; 12)\neq\emptyset \text{ and}\\ & D(1; 12)=D_2(-1: 12)=\emptyset,\\ 2^{t-2}, & \text{if } D_1\neq 1,\ D(1; 12)=D(-1; 12)=\emptyset \text{ and}\\ & \#(D(5; 12))=\text{odd},\\ 0 & \text{otherwise,}\end{cases}$$

where for any integers i, j, $D(i; j)=\{p\mid D;\ p\equiv i \bmod j\}$, $D_2(i; j)=\{p\mid D_2;\ p\equiv i \bmod j\}$, *and* $u=\#\{p\mid D_1;\ p\equiv -1 \bmod 12\}$,

$$\#(I(D_{12}))=\begin{cases}2^{t-1}, & \text{if } D_1=1,\ D(1; 12)=D(-1; 12)=\emptyset, \text{ and}\\ & \#(D(5; 12))=\text{odd},\\ 0 & \text{otherwise,}\end{cases}$$

$$\#(I(A_4))=\begin{cases}2^{r-2}h(-2D_2)-\#(I(A_5))-2^{-1}\#(I(S_4)),\\ \qquad\qquad \text{if } \left(\dfrac{-2D_2}{p}\right)=-1 \text{ for all } p\mid D_1,\\ 0 \qquad \text{otherwise},\end{cases}$$

$$\#(I((\boldsymbol{Z}/2\boldsymbol{Z})^2))=\begin{cases}2^{r-2}h(-D_2), & \text{if } \left(\dfrac{-D_2}{p}\right)=-1 \text{ for all } p\mid D_1,\\ & D_2\not\equiv -1 \bmod 8, \text{ and } D_1\neq 1,\\ \dfrac{h(-D_2)}{4}, & \text{if } D_1=1 \text{ and } D_2\equiv 1 \bmod 4,\\ \dfrac{h(-D_2)}{2}, & \text{if } D_1=1 \text{ and } D_2\equiv 3 \bmod 8,\end{cases}$$
$$-\#(I(D_{12}))-2^{-1}\#(I(S_4)),$$

$$\#(I(S_3))=0, \text{ if } \left(\frac{-3D_2}{p}\right)=1 \text{ for some } p\mid D_1. \quad \text{In other cases,}$$

$$\#(I(S_3))=\begin{cases}2^r h(-3D_2), & \text{if } -3D_2\equiv 5 \bmod 8,\\ 2^{r-1}h(-3D_2), & \text{if } -3D_2\equiv 1 \bmod 8,\\ 2^{r-2}h(-3D_2), & \text{if } -3D_2\equiv 3 \bmod 4,\end{cases}$$
$$-\#(I(S_4))-\#(I(A_5))-\#(I(D_{12})),$$

$$\#(I(\boldsymbol{Z}/3\boldsymbol{Z}))=\frac{3}{2}H_6-\frac{1}{2}\#(I(S_3))-\#(I(A_4))-\frac{1}{2}\#(I(S_4))$$
$$-\frac{1}{4}\#(I(D_{12}))-\frac{1}{2}\#(I(A_5))-\frac{1}{2}\#(I(\boldsymbol{Z}/6\boldsymbol{Z})),$$

where H_6 *is given in* [5] (II) *Theorem* (p. 696) *for each* D_1, D_2,

$$\#(I(\boldsymbol{Z}/2\boldsymbol{Z}))=2H_7-\frac{3}{2}\#(I((\boldsymbol{Z}/2\boldsymbol{Z})^2)-\#(I(S_3))-\#(I(A_4))$$
$$-\frac{3}{4}\#(I(S_4))-\frac{7}{6}\#(I(D_{12}))-\frac{1}{2}\#(I(A_5))$$
$$-\#(I(\boldsymbol{Z}/4\boldsymbol{Z}))-\frac{1}{3}\#(I(\boldsymbol{Z}/6\boldsymbol{Z})),$$

where H_7 *is given in* [5] (II) *Theorem for each* D_1, D_2,

$$\#(I(\{1\}))=\frac{1}{2^6 3^2 5}\prod_{q\mid D_1}(p-1)(p^2+1)\prod_{p\mid D_2}(p^2-1)$$

$$-\sum_{k=2}^{6}\frac{1}{k}\sharp(I(\boldsymbol{Z}/k\boldsymbol{Z}))-\frac{1}{6}\sharp(I(S_3))-\frac{1}{12}\sharp(I(A_4))$$
$$-\frac{1}{24}\sharp(I(S_4))-\frac{1}{12}\sharp(I(D_{12}))-\frac{1}{60}\sharp(I(A_5)).$$

Proof. The proof is similar to that of Theorem 7.1. So, we only sketch it and omit the details here. By the assumption that $D_2\neq 1$ and 2, 3, $5\nmid D$, Lemma 2.1 is also valid, and almost all the results in § 2, 3, and 4 are valid also in this case. Now, the local data at $q\nmid D_1$ in § 5 can be used without any change. The calculation of local data at $q\mid D_1$ can be done virtually in the same way as in § 5. Finally, we obtain mass formulae and $\sharp(I(\Gamma))$ for each Γ. q.e.d.

References

[1] E. Bayer-Fluckiger, Principe de Hasse faible pour les systèmes des formes quadratiques, J. reine angew. Math., **378** (1987), 53–59.

[2] M. Eichler, Über die Idealklassenzahl totaler definiter Quaternionen Algebren, Math. Z., **43** (1938), 127–151.

[3] K. Hashimoto, On Brandt matrices associated with the positive definite quaternion hermitian forms, J. Fac. Sci. Univ. Tokyo Sect. IA, **27** (1980), 227–245.

[4] ——, Class numbers of positive definite ternary quaternion hermitian forms, Proc. Japan Acad., **59** Ser. A no. 10 (1983), 490–493.

[5] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms (I): J. Fac. Sci. Univ. Tokyo Sect. IA, **27** (1980), 549–601; (II) J. Fac. Sci. Univ. Tokyo Sect. IA, **28** (1983), 695–699; (III) J. Fac. Sci. Univ. Tokyo Sect. IA, **30** (1983), 393–401.

[6] ——, On relations of dimensions of automorphic forms of $Sp(2, R)$ and its compact twist $Sp(2)$ (II), Advanced Studies in Pure Math., **7** (1985), 31–102.

[7] H. Hijikata, Hasse principle on quaternionic anti-hermitian forms, J. Math. Soc. Japan, **15** (1963), 165–175.

[8] ——, Hasse principle for the conjugacy classes of the orthogonal group (in Japanese), Reports of the Symposium on algebraic groups held at Yamanaka-Kyodo-Kenshujo, 1973.

[9] B. Huppert, Endliche Gruppen I, Springer-Verlag, Berlin, Heidelberg, New York, 1979.

[10] T. Ibukiyama, On symplectic Euler factors of genus two, J. Fac. Sci. Univ. Tokyo Sect. IA, **30** (1984), 587–614.

[11] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, Compositio Math., **57** (1986), 127–152.

[12] T. Katsura and F. Oort, Families of supersingular abelian surfaces, Compositio Math., **62** (1987), 107–167.

[13] L. Moret-Bailly, Familles de courbes et de variétés abéliennes sur P^1, Astérisque, **86** (1981), 109–140.

[14] L. Redei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. reine angew. Math., **170** (1933), 69–74.

[15] G. Shimura, On the theory of automorphic functions, Ann. Math., **70** (1959), 101–144.

[16] ——, Arithmetic of alternating forms and quaternion hermitian forms, J. Math. Soc. Japan, **15** (1963), 33–65.

[17] H. Wada, The table of the class numbers of the quadratic field $Q(\sqrt{-m})$, $1 \leqq m < 24{,}000$, Sūriken-Kōkyūroku.

Department of Mathematics
College of General Education
Kyushu University
Ropponmatsu, Fukuoka
810, Japan