<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>TYPE NUMBERS OF QUATERNION HERMITIAN FORMS AND SUPERSINGULAR ABELIAN VARIETIES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Ibukiyama, Tomoyoshi</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 55(2) P.369–P.384</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>2018-04</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/68357">https://doi.org/10.18910/68357</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/68357</td>
</tr>
<tr>
<td><strong>rights</strong></td>
<td></td>
</tr>
</tbody>
</table>
TYPE NUMBERS OF QUATERNION HERMITIAN FORMS AND SUPERSINGULAR ABELIAN VARIETIES

TOMOYOSHI IBUKIYAMA

(Received June 21, 2016, revised December 16, 2016)

Abstract
The word type number of an algebra means classically the number of isomorphism classes of maximal orders in the algebra, but here we consider quaternion hermitian lattices in a fixed genus and their right orders. Instead of inner isomorphism classes of right orders, we consider isomorphism classes realized by similitudes of the quaternion hermitian forms. The number \( T \) of such isomorphism classes are called type number or \( G \)-type number, where \( G \) is the group of quaternion hermitian similitudes. We express \( T \) in terms of traces of some special Hecke operators. This is a generalization of the result announced in [5] (I) from the principal genus to general lattices. We also apply our result to the number of isomorphism classes of any polarized superspecial abelian varieties which have a model over \( \mathbb{F}_p \) such that the polarizations are in a "fixed genus of lattices". This is a generalization of [8] and has an application to the number of components in the supersingular locus which are defined over \( \mathbb{F}_p \).

1. Introduction
First we review shortly the classical theory of Deuring and Eichler, and then explain how this will be generalized to quaternion hermitian cases. Let \( B \) be a quaternion algebra central over an algebraic number field \( F \) and fix a maximal order \( \mathcal{O} \) of \( B \). The class number \( H \) of \( B \) is the number of equivalence classes of left \( \mathcal{O} \)-ideals \( a \) up to right multiplication by \( B^\times \). Any maximal order of \( B \) is isomorphic (equivalently \( B^\times \)-conjugate) to the right order of some left \( \mathcal{O} \)-ideal \( a \), and the number of such isomorphism classes is called the type number \( T \). Obviously \( T \leq H \) and the formula for \( H \) and \( T \) are known by Eichler, Deuring, Peters, and Pizer, as a part of the trace formula for Hecke operators on the adelization \( B^\times_A \) (called Brandt matrices traditionally), and also several explicit formulas have been written down (See [1], [3], [2], [12], [13]). Now for a fixed prime \( p \), an elliptic curve \( E \) defined over a field of characteristic \( p \) is called supersingular if \( \text{End}(E) \) is a maximal order of a definite quaternion algebra \( B \) over \( \mathbb{Q} \) with discriminant \( p \). The class number of \( B \) is equal to the number of isomorphism classes of supersingular elliptic curves \( E \) over an algebraically closed field. All such curves \( E \) have a model defined over \( \mathbb{F}_p^2 \) and the number of \( E \) which have a model over \( \mathbb{F}_p \) is known to be equal to \( 2T - H \) (Deuring [1]). But for \( n \geq 2 \), the class number of \( M_n(B) \) is one if \( F = \mathbb{Q} \) by the strong approximation theorem and all the maximal orders of \( M_n(B) \) are conjugate to \( M_n(\mathcal{O}) \), so there is nothing to ask. Instead, we define \( G \) to be the group of similitudes of a quaternion hermitian form, and \( G_A \) the adelization. We fix a left \( \mathcal{O} \)-lattice \( L \) in \( B^n \) and consider the \( G_A \)-orbit of \( L \) in \( B^n \). Such a set of global lattices is called

2010 Mathematics Subject Classification. Primary 11E41; Secondary 14K10, 11E12.
This work was supported by JSPS KAKENHI 25247001.
a genus $\mathcal{L}(L)$ determined by $L$. The number $h(\mathcal{L})$ of $G$-orbits in $\mathcal{L} = \mathcal{L}(L)$ is called the class number of $\mathcal{L}$ and this is a complicated object. (For some explicit formulas, see [5] (I), (II)).

Now take a complete set of representatives of classes $L = L_1, \ldots, L_h$ in $\mathcal{L}(L)$. Define the right order $R_i$ of $M_n(B)$ by

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

These are maximal orders. We say that $R_i$ and $R_j$ have the same type if $R_i = a^{-1}R_j a$ for some $a \in G$. We denote this relation by $R_i \equiv_G R_j$. The number $T$ of types in $\{R_i : 1 \leq i \leq h\}$ is called a type number of $\mathcal{L}(L)$. We give a formula to express $T$ in terms of traces of Hecke operators defined by some two sided ideals of $R_1$ (Theorem 3.6) under a general setting on $F$, $B$, and quaternion hermitian forms.

Now let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_p$. (Such a curve always exists.) The abelian variety $A = E^n$ is called superspecial, and it has a standard principal polarization $\phi_X$ associated with a divisor $X = \sum_{a+b=-1} \mathbb{P}^{a} \times \mathbb{P}^{b}$. For any polarization $\lambda$ of $A$, the map $\phi_X^{-1}\lambda$ gives a positive definite quaternion hermitian matrix in $\text{End}(A) = M_\mathbb{C}(\mathbb{C})$ for a maximal order $\mathcal{O}$ of the definite quaternion algebra $B$ over $\mathbb{Q}$ with discriminant $p$, and we can define a genus $\mathcal{L}(\phi_X^{-1}\lambda)$ of lattices to which $\phi_X^{-1}\lambda$ belongs. We denote by $\mathcal{P}(\lambda)$ the set of polarizations $\mu$ of $A$ such that $\phi_X^{-1}\mu \in \mathcal{L}(\phi_X^{-1}\lambda)$. We fix $\lambda$ and denote the class number and the type number of $\mathcal{L}(\phi_X^{-1}\lambda)$ by $H$ and $T$ respectively. Then the number of isomorphism classes of polarized abelian varieties $(E^n, \mu)$ with $\mu \in \mathcal{P}(\lambda)$ is $H$ and the number of those which have models over $\mathbb{F}_p$ is equal to $2T - H$ (Theorem 4.3). As an application, we can show that the number of irreducible components of the supersingular locus $S_{n,1}$ in the moduli of principally polarized abelian varieties $A_{n,1}$ which have models over $\mathbb{F}_p$ is equal to $2T - H$ where $H$ and $T$ are class numbers and type numbers of the principal genus (resp. the non-principal genus) when $n$ is odd (resp. $n$ is even) (Theorem 4.6).

By the way, for a prime discriminant, an explicit formula for $T$ for the principal genus for $n = 2$ has been given in [8]. The formulas for $T$ for the non-principal genus for $n = 2$ will be given in a separate paper [6]. Together with the formula in [5] (I), (II), an explicit formula for $2T - H$ for $n = 2$ for any genera of maximal lattices will be given there. 

Acknowledgment. The author thanks Professor F. Oort for his deep interest in the theory and for explaining to him a theory of supersingular locus in the moduli. He also thanks Professor Chia-Fu Yu and Academia Sinica in Taipei for giving him an excellent circumstance to finish this paper and for their kind hospitality.

2. Fundamental definitions

We review several fundamental things about quaternion hermitian forms. For the claims without proofs, see [14]. Let $F$ be an algebraic number field which is a finite extension of $\mathbb{Q}$. Let $B$ be any quaternion algebra over $F$, not necessarily totally definite. For any $a \in B$, we denote by $Tr(a)$ and $N(a)$ the reduced trace and the reduced norm over $F$, respectively. We denote by $\overline{a}$ the main involution of $B$ over $F$, so $Tr(a) = a + \overline{a}$, $N(a) = a\overline{a}$. A non-degenerate quaternion hermitian form $f$ on $B^n$ over $B$ is defined to be a map $f : B^n \times B^n \rightarrow B$ such that $f(ax + by, z) = \overline{a}f(x, z) + b\overline{f}(y, z)$ for $a, b \in B$, $f(y, x) = f(x, y)$, and $f(x, B^n) = 0$ implies $x = 0$. For any $n_1 \times n_2$ matrix $b = (b_{ij}) \in M_{n_1n_2}(B)$, we write $\overline{b} = (\overline{b}_{ji})$. It is well-known that, by a base change over $B$, we may assume that

...
where \( J = \text{diag}(e_1, \ldots, e_n) \) is a non-degenerate diagonal matrix in \( M_n(F) \). For any place \( v \) of \( F \), we denote by \( F_v \) the completion at \( v \). We denote by \( \mathbb{H} \) the division quaternion algebra over \( \mathbb{R} \). Equivalence classes of non-degenerate quaternion hermitian forms over \( \mathbb{H} \) are determined by the signature of the forms. More precisely, if we denote by \( v_1, \ldots, v_r \) the set of all infinite places of \( F \) such that \( B_v = B \otimes_F F_v \) is a division algebra, then the forms \( f \) on \( B^a \) are equivalent under the base change over \( B \) if and only if their embeddings to the maps on \( B_v^a \) are equivalent over \( B_v \) for all \( v_i (1 \leq i \leq r) \). If \( v \) is a finite place of \( F \), then any non-degenerate quaternion hermitian forms are equivalent under the base change over \( B_v \).

So for a finite \( v \), we may change to \( J = 1_n \) locally by a base change over \( B_v \). We fix \( f \) once and for all. We define a group of similitudes with respect to \( f \) by

\[
G = \{ g \in GL_n(B) = M_n(B)^{\times}; gJ^T\overline{g} = n(g)J \text{ for some } n(g) \in F^\times \}
\]

call this a quaternion hermitian group with respect to \( f \). If we write \( g^TJ = Jg^{-1} \), then the condition \( g \in G \) is written simply as \( gg^T = n(g)1_n \). For any place \( v \), we put

\[
G_v = \{ g \in M_n(B_v); gg^T = n(g)1_n, n(g) \in F_v^\times \}
\]

where \( B_v = B \otimes_F F_v \). We denote by \( F_A \) and \( G_A \) the adelizations of \( F \) and \( G \), respectively. For \( c \in F \) or \( F_A \), it is clear that \( c_{1_n} \in G \) or \( G_A \).

We denote by \( v \) the ring of integers of \( F \). We fix a maximal order \( \mathcal{O} \) of \( B \). An \( \mathcal{O} \)-module \( L \) in \( B^a \) such that \( L \otimes_{\mathcal{O}} F = B^a \) is called a left \( \mathcal{O} \)-lattice if it is a left \( \mathcal{O} \)-module. For any finite place \( v \) of \( F \), we denote by \( \mathcal{O}_v \) the \( v \)-adic completion of \( \mathcal{O} \) and put \( L_v = L \otimes_{\mathcal{O}} \mathcal{O}_v \). We say that left \( \mathcal{O} \)-lattices \( L_1 \) and \( L_2 \) belong to the same class if \( L_1 = L_2g \) for some \( g \in G \). We say that \( L_1 \) and \( L_2 \) belong to the same genus if \( L_1, v = L_2, v g_v \) for some \( g_v \in G_v \) for all finite places \( v \) of \( F \). We fix a left \( \mathcal{O} \)-lattice \( L \) and denote by \( \mathcal{L}(L) \) the set of left \( \mathcal{O} \)-lattices belonging to the same genus as \( L \) and call this a genus of \( L \). In other words, if we put

\[
Lg = \bigcup_{v \text{ finite places}} (L \otimes_{\mathcal{O}} \mathcal{O}_v \cap B^a)
\]

for any \( g = (g_v) \in G_A \), then we have

\[
\mathcal{L}(L) = \{ Lg; g \in G_A \}.
\]

We fix a left \( \mathcal{O} \)-lattice \( L \). For any finite place \( v \), we define

\[
U_v = U(L_v) = \{ u \in G_v; L_v = L_au \}
\]

and write \( U = G_{\infty} \prod_{v < \infty} U_v \), where \( G_{\infty} \) is the product of all \( G_v \) over the archimedean places \( v \). Then the class number \( h \) of \( \mathcal{L}(L) \) is equal to \( |U|/G_A/G \), which is known to be finite. Now we write \( G_A = \bigcup_{i=1}^h U_{g_i}G \) (disjoint), where we assume that \( g_1 = 1 \). We write \( \mathfrak{C}_v = \mathcal{O} \otimes \mathcal{O}_v \). For \( 1 \leq i \leq h \), we define left \( \mathcal{O} \)-lattices \( L_i \) by \( L_i = Lg_i \). The ring

\[
R_i = \{ b \in M_n(B); L_i b \subset L_i \}
\]

is called the right order of \( L_i \). This is an maximal order of \( M_n(B) \), since for any prime \( v \), we have \( M_v = \mathfrak{C}_v \otimes h_p \), for some \( h_p \in GL_n(B_v) \) (where we can take \( h_v = 1 \) for almost all \( v \)), so \( R_{i,v} = R_i \otimes \mathcal{O}_v \mathcal{O}_v = h_v^{-1} M_n(\mathfrak{C}_v)h_v \) are maximal orders for any finite places \( v \). For any order \( R \) of
$M_n(B)$ and $g = (g_v) \in G_A$, we define $g^{-1}Rg$ by

$$g^{-1}Rg = \bigcap_{v \in \infty} g_v^{-1}R_vg_v \cap M_n(B).$$

So if we write $R = R_1$ (where we chose $g_1 = 1$), then $R_i = g_i^{-1}Rg_i$. We say that $R_i$ and $R_j$ have the same type (or $G$-type) if $a^{-1}Rai = R_j$ for some $a \in G$. We denote this relation by $R_i \simeq_G R_j$. The number of equivalence classes in $[R_1, \ldots, R_h]$ in this sense is called the type number $T$ of $L(L)$. When $n = 1$, since $G = B^\times$ and $G_A = B_A^\times$, this is nothing but the type number in the classical sense.

Now we give a complete set of representatives of local equivalence classes of quaternion hermitian lattices for finite places. First we show an easy result that for a finite place $v$ in the classical sense.

**Lemma 2.1.** The set of $G_v$-equivalence classes of left $\mathfrak{S}_v$-lattices and the set of equivalence classes of quaternion hermitian matrices in $M_n(B_v)$ correspond bijectively.

**Proof.** Take $J$ as before. Since $N(B_v^\times) = F_v^\times$ for any finite place $v$, there exists a diagonal matrix $J_1 \in GL_n(B_v)$ such that $J = J_1^{-1}T_1$ and we may assume that $J = 1_n$. But to avoid any likely confusion, we keep using a general $J$ here in the proof. For any finite place $v$, it is clear that any $\mathfrak{S}_v$-lattice $L_v$ may be written as $L_v = \mathfrak{S}_v^uh$ with $h \in GL_n(B_v)$ by the elementary divisor theorem. We define a map $\phi$ by $\phi(L_v) = hJ^1h_v$. The equivalence class of the image does not depend on the choice of $h$. If $\mathfrak{S}_v^uh_1g = \mathfrak{S}_v^uh_2$ for $g \in G_v$, then we have $uh_1g = h_2$ for some $u \in GL_n(O_v)$. This means that

$$n(g)uh_1J_1h_1^*u^* = uh_1gJ^1h_1^*u^* = h_2Jh_2^*.$$

So $\phi$ induces a map from a $G_v$-equivalence class to a class of hermitian matrices. The map is surjective. Indeed for any hermitian matrix $X \in GL_n(B_v)$, there exists an $x \in GL_n(B_v)$ such that $X = xx^*$, so if we put $hJ_1 = x$ for $J_1$ such that $J_1J_1^* = J$, then we have $\phi(O_v^nh) = X$. The map is injective. Indeed, if $uh_1Jh^*u^* = mh_2Jh_2^*$ for some $m \in F_v$, then $g = h_2^{-1}uh_1 \in G_v$ with $n(g) = m$ and we have $\mathfrak{S}_v^uh_2g = \mathfrak{S}_v^uh_1$. □

For a finite place $v$, we denote by $p_v$ a prime element of $O_v$. First we consider the case when $B_v$ is division. When $B_v$ is a division quaternion algebra, let $O_v$ be the maximal order of $B_v$ and $\pi$ a fixed prime element of $O_v$ such that $N_{B_v/F_v}(\pi) = p_v$ and $\pi^2 = -p_v$.

**Proposition 2.2.** Let $B_v$ be a division quaternion algebra and $H = H^* \in M_n(B_v)$ be a quaternion hermitian matrix. Then there exists a $u \in GL_n(O_v)$ such that

$$uHu^* = \begin{pmatrix}
A_1 & 0 & \cdots & 0 \\
0 & A_2 & 0 & : \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & A_r
\end{pmatrix}$$
where $A_i = p_v^e$ or

$$A_i = p_v^e \begin{pmatrix} 0 & \pi \\ \pi & 0 \end{pmatrix}.$$

Proof. We prove this by induction of the size of $H$. Multiplying by a power of $p_v$, we may assume that $H \in \mathcal{M}_n(\mathbb{Q}_v)$. Assume that the $\mathcal{O}_v$ ideal spanned by the components $h_{ij}$ of $H = (h_{ij})$ is $\pi^e \mathcal{O}_v$. By replacing $H$ by $p_v^{-e/2} H$, we may assume that $e = 0$ or $e = 1$. First assume that $e = 0$. Then some component of $H$ is in $\mathcal{O}_v^\times$. If a diagonal component belongs to $\mathcal{O}_v^\times$, then by permuting the rows and columns, we may assume that the $(1, 1)$ component $h_{11}$ belongs to $\mathcal{O}_v^\times$. Since $H = H^*$, this means $h_{11} \in \mathcal{O}_v^\times$. Since we have $N(\mathcal{O}_v^\times) = \mathcal{O}_v^\times$, by changing $H$ to $eHe^*$ for $e \in \mathcal{O}_v^\times$ with $N(e) = h_{11}^{-1}$, we may assume that $h_{11} = 1$. Denote by $e_{ij}$ the $n \times n$ matrix whose $(i, j)$ component is 1 and whose other components are 0. Then if we put $u_1 = 1_n - \sum_{i=2}^n h_{1i} e_{1i}$, where we write $H = (h_{ij})$, obviously $u_1 \in \text{GL}_n(\mathcal{O}_v)$ and we have

$$u_1 H u_1^* = \begin{pmatrix} 1 & 0 \\ 0 & H_1 \end{pmatrix}.$$ 

So we reduce to the matrix $H_1$ of size $n - 1$. If all the diagonal components belong to $\mathcal{O}_v$, and there exists some off-diagonal component belonging to $\mathcal{O}_v^\times$, then, by permuting the rows and columns, we may assume that the $(1, 2)$ component is $h_{12} = e \in \mathcal{O}_v^\times$. We write $h_{11} = p_v t$ and $h_{22} = p_v s$ with $t, s \in \mathcal{O}_v$. If we put $u_2 = 1_n - be_{12}$ with $b \in \mathcal{O}_v$, then $u_2 \in \text{GL}_n(\mathcal{O}_v)$ and the $(1, 1)$ component of $u H u^*$ is given by

$$p_v t + p_v s N(b) + Tr(b \bar{e}).$$

Since it is well known that $Tr(\mathcal{O}_v) = \mathcal{O}_v$ (e.g. the unramified extension of $F_v$ contains an integral element whose trace is one), we take $b = e_0 \bar{e}^{-1}$ for an element $e_0 \in \mathcal{O}_v$ such that $tr(e_0) = 1$. Since $1 + p_v t + p_v s N(b) \in \mathcal{O}_v^\times$, we reduce to the previous case. Secondly we assume that $e = 1$. Then all the diagonal components belong to $\mathcal{O}_v$ and changing rows and columns, we may assume that $h_{12} = \pi e$ with $e \in \mathcal{O}_v^\times$. We assume that $h_{11} = p_v^e t_0$ with $e \geq 1$ and $t_0 \in \mathcal{O}_v^\times$ and $h_{22} = p_v s$ with $s \in \mathcal{O}_v$. Again by $v_1 = 1_n + b_1 e_{12}$, the $(1, 1)$ component of $v_1 H v_1^*$ is given by $p_v^e t_0 + p_v s N(b_1) + Tr(\pi e b_1)$. If we put $b_1 = p_v^{e-1} \pi e_0$ with $e_0 \in \mathcal{O}_v$ such that $Tr(e_0) = -t_0$, then we have

$$p_v^e t_0 + p_v s N(b_1) + Tr(\pi e b_1) = p_v^e t_0 + Tr(e_0) + sp_v^{2e} N(e^{-1} e_0) = p_v^{2e} s N(e^{-1} e_0).$$

This is divisible by $p_v^{2e}$. Since $Tr(\pi \mathcal{O}_v) = p_v e_0$, we see that $e_0 \in \mathcal{O}_v^\times$ and $b_1 \in p_v^{-e} \pi \mathcal{O}_v^\times$. Repeating the same process, we can take $v_i = 1_n + b_i e_{12}$ such that the $(1, 1)$ component of $v_i v_{i-1} \cdots v_1 H v_1^* \cdots v_i^*$ is of arbitrary high $p_v$-adic order. Since the $\pi$-adic order of $b_i$ monotonically increases, the limit $\lim_{i \to \infty} v_i \cdots v_1$ converges to $v \in \text{GL}_n(\mathcal{O}_v)$ and we see that the $(1, 1)$ component of $v H v^*$ is zero. By these changes, the $(1, 2)$ components always belong to $\pi \mathcal{O}_v^\times$, so we may assume that $h_{11} = 0$ and $h_{12} = \pi e_2 \in \pi \mathcal{O}_v^\times$. By taking the diagonal matrix $A_0 = \text{diag}(1, e_2^{-1}, 1, \ldots, 1) \in \text{GL}_n(\mathcal{O}_v)$ and $A_0^* H A_0$, we may assume that $h_{12} = \pi$. So now we can assume that the diagonal block of $H$ of $(i, j)$ components with $1 \leq i, j \leq 2$ is given by

$$\begin{pmatrix} 0 & \pi \\ \pi & p_v s \end{pmatrix}.$$ 

We have
So taking a diagonal matrix \( v \), we can take \( b \in \mathcal{O}_v \) such that \( p_v s + T(\pi b) = 0 \), so we may assume that \( s = 0 \). Now we will show that we can change \( H \) so that the components of the first and the second row vanish except for the \((1, 2)\) and \((2, 1)\) components. Since we assumed that \( e = 1 \), all the components belong to \( \pi \mathcal{O}_v \), and if we put

\[
w = 1 - \sum_{j=3}^{n} \pi^{-1} h_{2j}e_{1j} - \sum_{j=3}^{n} \pi^{-1} h_{1j}e_{2j},
\]

then \( w \in GL_n(\mathcal{O}_v) \) and we have

\[
w^* H w = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}
\]

with \( H_1 = \begin{pmatrix} 0 & \pi \\ \pi & 0 \end{pmatrix} \), so the claim for \( H \) reduces to the claim for \( H_2 \).

For any subset \( W \) of \( G_A \), we put

\[ n(W) = \{ n(w) \in F_{A^*}^\times : w \in W \}. \]

**Corollary 2.3.** For any finite place \( v \), let \( L_v \) be a left \( \mathcal{O}_v \)-lattice and define \( U_v \) as before as a group of elements \( g \in G_v \) such that \( L_v g = L_v \). Then we have \( n(U_v) = \mathcal{O}_v^\times \).

Proof. First we show that \( n(U_v) \subset \mathcal{O}_v^\times \). Assume that \( g \in U_v \) and \( gg^* = n(g)1_v \). Since \( L_v g = L_v \) and \( L_v \) is a free \( \mathcal{O}_v \)-module of finite rank, the characteristic polynomial of the representation of \( g \) is monic integral if we identify \( B_v \) with \( F_v^4 \). Since the characteristic polynomial of \( g^* = Jg J^{-1} \) is the same as that of \( g \), this is also monic integral. In particular, the determinants of \( g \) and \( g^* \) in this representation are integral. So \( n(g) \) is integral, and so \( n(g) \) is also integral. Since \( L_v = L_v g^{-1} \), this is also true for \( n(g)^{-1} \). So we have \( n(g) \in \mathcal{O}_v^\times \).

Next we show the converse. First we assume that \( B_v \) is division. We take \( h \in GL_n(B_v) \) such that \( L_v = \mathcal{O}_v h_{v} \) and put \( H = h_{v} J_{v} h_{v}^{-1} \). Then for any \( m \in \mathcal{O}_v^\times \), we have an element \( \alpha \in GL_n(\mathcal{O}_v) \) such that \( \alpha H \alpha^* = mH \). Indeed, we have \( uH u^* = \text{diag}(A_1, \ldots, A_n) \) for some \( u \in GL_n(\mathcal{O}_v) \) as in Proposition 2.2. Take \( b \in \mathcal{O}_v^\times \) such that \( N(b) = m \), and if \( \alpha_i = p_v e_i \), then we have \( b, \alpha_i, \alpha_i^* = m \).

If \( A_i = \begin{pmatrix} 0 & \pi \\ \pi & 0 \end{pmatrix} \), then \( \mathcal{O}_v \) is realized as \( \mathcal{O}_v = \mathcal{O}_v^u + \mathcal{O}_v^w \pi \) where \( \pi^2 = -p \) and \( \mathcal{O}_v^u \) is a subring of \( \mathcal{O}_v \), which is isomorphic to the maximal order of the unique unramified quadratic extension of \( F_v \). Here for \( b \in \mathcal{O}_v^u \), we have \( b \pi = \pi b \). We have \( N((\alpha_i^u)^{\mathcal{O}_v}) = \alpha_i^v \) by local class field theory. So taking \( b \in (\mathcal{O}_v^u)^{\mathcal{O}_v} \subset \mathcal{O}_v^\times \) with \( N(b) = m \), put

\[
C_i = \begin{pmatrix} b & 0 \\ 0 & \frac{1}{b} \end{pmatrix}.
\]

Then

\[
C_i \begin{pmatrix} 0 & \pi \\ -\pi & 0 \end{pmatrix} C_i^* = \begin{pmatrix} 0 & b \pi b^-1 \\ -b \pi b^{-1} & 0 \end{pmatrix} = m \begin{pmatrix} 0 & \pi \\ -\pi & 0 \end{pmatrix}.
\]

So taking a diagonal matrix \( v \) consisting of diagonal blocks \( b_i \) and \( C_i \), we have \( vuHu^*v^* = \ldots \).
In this case, by virtue of Shimura [14] Proposition 2.10, there exists an element \( o \) of \( \mathfrak{o} \) such that all the components of \( u_i \) of \( \mathfrak{o} \) are division and split when \( g \) is division, this is equal to \( \pi \) by \( \mathfrak{o} \) and right orders \( \mathfrak{o} \) of \( \mathfrak{o} \). Let \( m \) be any element in \( \mathfrak{o} \); we take \( J_1 = \text{diag}(u_1, \ldots, u_n) \) such that \( J_1 \mathcal{T}_1 = J \). So we have \( L_v = (1, J_1) \mathcal{T}_1 \mathcal{J}_1 = L_v \). Then we have

\[
L_v g = (b_1 u_1^{-1} \alpha_1, \ldots, b_n u_n^{-1} \alpha_n) J_1 X = (b_1 u_1^{-1}, \ldots, b_n u_n^{-1}) J_1 X - L_v.
\]

3. G-type numbers and Hecke operators

3.1. A formula for a type number. We fix a left \( \mathcal{O} \)-lattice \( L \) in \( B^\alpha \). We define \( U \subset G_\alpha \) by the group of stabilizers of \( L \) as before and fix representatives \( L_1, \ldots, L_n \) of classes in \( \mathcal{L}(L) \) and right orders \( R_i \) of \( L_i \). We set \( L_1 = L \) and \( R_1 = R \). We denote by \( L_v \) and \( R_v \) the tensor of \( L \) and \( R \) over \( \mathfrak{o} \) and \( \mathfrak{o}_v \), respectively. First, to define some good Hecke operators, we see there exist some special elements in \( R_v \cap G_v \). When \( B_v \) is division, we fix an element \( \pi \) in \( \mathfrak{o}_v \) with \( \pi^2 = -p_v \) as before. First we recall the following well-known fact.

**Lemma 3.1.** When \( B_v \) is division, any two sided ideal of \( M_n(\mathfrak{o}_v) \) in \( M_n(\mathfrak{O}_v) \) is given by \( \pi^e M_{n}(\mathfrak{o}_v) \) for some integer \( e \geq 0 \). When \( B_v = M_{2}(F_v) \), then any two sided ideal of \( M_n(\mathfrak{o}_v) \) is given by \( \pi^e M_{n}(\mathfrak{o}_v) \) for some integer \( e \geq 0 \).

The proof is well-known and straightforward by using the elementary divisor theorem in both cases and omitted here. It is also clear that for any \( u_1, u_2 \in GL_n(\mathfrak{o}_v) \), we have

\[
u_1 \pi^e u_2 M_n(\mathfrak{O}_p) = \pi^e M_n(\mathfrak{O}_p)\text{ when } B_p \text{ is division.}
\]

**Proposition 3.2.** When \( B_v \) is division, there exists an element \( \omega_v \in R_v \cap G_v \) such that \( \omega_v^2 = -p_v 1_n \), \( \omega_v \omega_v^* = p_v 1_n \) and any two sided ideal of \( R_v \) in \( R_v \) is given by \( \omega_v^e R_v \) for some \( e \geq 0 \).

Proof. First we show that there exists an element \( \omega_v \in R_v \) such that \( \omega_v^2 = -p_v 1_n \), \( \omega_v \omega_v^* = p_v 1_n \), and \( \omega_v R_v = R_v \omega_v \). Take \( h_v \in GL_n(B_v) \) such that \( L_v = \mathfrak{O}_v h_v \) and put \( H_v = h_v J_1^\top h_v \). By changing a representative of the \( G_v \)-equivalence class of \( L_v \) by multiplying an element of \( \mathfrak{o}_v \), we may assume that \( L_v \subset \mathcal{O}_v \) and \( H_v = M_n(\mathfrak{O}_v) \). Then by Proposition 2.2, there exists some \( u \in GL_n(\mathfrak{O}_v) \) such that all the components of \( uH_v^\alpha \) are in \( \mathfrak{o}_v \cup \pi \mathfrak{o}_v \). So we have \( \pi(uH_v^\alpha) = (uH_v^\alpha) \pi \) for \( \pi \). Put \( \omega_v = h_v^{-1} u^{-1} \pi u_h \), then we have \( \omega_v^2 = h_v^{-1} u^{-1} \pi u_h \), and \( \omega_v \omega_v^* = p_v 1_n \). We also have \( \mathfrak{O}_v h_v \omega_v^* = \mathfrak{O}_v h_v^\pi u_h = \mathfrak{O}_v \pi u_h = \mathfrak{O}_v \omega_v \). So \( \omega_v R_v \) is a two sided ideal of \( R_v \) is given by \( \omega_v^e R_v \) for some \( e \geq 0 \) and any \( u_1, u_2 \in GL_n(\mathfrak{o}_v) \) and this is equal to \( \omega_v^e R_v \).
ideal \( m \mid b \) of \( a_v \), we define \( \omega(m) = (g_v) \in G_A \) by setting \( g_v = 1 \) for all archimedean places \( v \) and finite places \( v \) such that \( p_v \nmid m \), and \( g_v = \omega_v \) for any places \( v \) such that \( p_v \mid m \). We put \( F_{\infty} = \prod_v \text{finite } F_v \) where \( v \) runs over all archimedean places of \( F \). We choose a complete set \( c_1, \ldots, c_h \) of representatives of \( F_{\infty}^x \cap F_{\infty} \prod_v \omega_v \). This set of course corresponds to a complete set of representatives of ideal classes of \( F \) and \( h_0 \) is the class number of \( F \). By embedding \( F_A 1_n \subset G_A \), we regard \( \epsilon_i \) as an element of \( G_A \). We also have \( (F_{\infty}^x \prod_v \omega_v) 1_n \subset U \) for any \( \mathbb{C} \)-lattice \( L \). We have

**Proposition 3.3.** (1) \( R_i \) and \( R_j \) have the same \( G \)-type if and only if \( \epsilon_i^{-1} \omega(m)^{-1} g_i \in U g_j G \) for some \( m \mid b \) and some \( \epsilon_i \).

(2) Assume that the class number of \( F \) is one. Then for a fixed \( m \mid b \), if \( \omega(m)^{-1} g_i \in U g_j G \) then \( \omega(m)^{-1} g_j \in U g_i G \).

Proof. First we assume that \( R_i \equiv_G R_j \), so we have \( a^{-1} R_i a = R_j \) for some \( a \in G \). This means that \( a^{-1} g_i^{-1} R g_i a = g_j^{-1} R g_j \), so by definition, we have \( a^{-1} g_i^{-1} R g_i a = g_j^{-1} R g_j \), where \( g_{i,v} \) and \( g_{j,v} \) are \( v \)-adic components of \( g_i \) and \( g_j \). So \( R g_i g_{i,v}^{-1} g_{j,v} \) is a two sided ideal of \( R_v \). If \( B_i \) is division, then \( g_{i,v} g_{i,v}^{-1} = \omega_v^{-1} u \) with \( u \in U_v \). If \( B_i = \mathbb{M}_2(F_v) \), then \( g_{i,v} g_{i,v}^{-1} = \omega_v^{-1} u \) with \( u \in U_v \). Since \( g_{i,v} g_{i,v}^{-1} \) is the \( v \)-component of an element in \( G_A \), we have \( g_{i,v} g_{i,v}^{-1} \in U_v \) for almost all \( v \). So \( \epsilon_i \neq 0 \) only for the finitely many \( v \). We denote by \( m_1 \) an element of \( F_{\infty}^x \) such that \( v \) component is \( p_v^e \) for split primes \( p_v \), and \( p_v^{[e/2]} \) for ramified primes \( p_v \), where \( [x] \) is the least integer which does not exceed \( x \). For some \( l \) with \( 1 \leq l \leq h_0 \), we have \( m_1 = 0 \) for some \( u \) in \( U \) and \( c \in F_{\infty}^x = \prod_v \omega_v \). If we define \( m \) as a product of ramified \( p_v \) such that \( \epsilon_i \) is odd, we see \( g_{i,v} a^{-1} g_{j,v}^{-1} = \omega(v)^{-1} g_i \in U g_j G \). Next we prove the converse. We assume that \( \epsilon_i^{-1} \omega(m)^{-1} g_i \in U g_j G \) for some \( m \mid b \) and \( l \). Then \( g_i = \omega(m)^{-1} u g_j a \) for some \( u \in U \) and \( a \in G \). Then we have

\[ R_i = g_i^{-1} R g_i = a^{-1} g_j^{-1} u^{-1} \epsilon_i^{-1} \omega(m)^{-1} R \omega(m)^{-1} g_i \epsilon_i u g_j a. \]

We have \( \omega(m)^{-1} R \omega(m) = R \) since conjugation is defined locally. Since \( \epsilon_i 1_n \) is in the center of \( M_n(B_A) \) and \( u^{-1} Ru = R \) by definition of \( U \), we have \( a^{-1} R_i a = R_i \), hence we have proved (1).

Now if \( \omega(m)^{-1} g_i \in U g_j G \) for some \( m \mid b \), then since \( \omega(m) U = U \omega(m) \) by definition of \( \omega(m) \), we have \( g_i \in \omega(m) U g_j G = U \omega(m) g_j G \), hence \( \omega(m) g_j \in U g_j G \). Since \( \omega(m)^2 \in F_A 1_n \) and we assumed that the class number of \( F_A \) is one, we see that \( \omega(m)^2 = u_0 c \) for some \( u_0 \in F_{\infty} \prod_v \omega_v \) and \( c \in F_{\infty}^x \). We have \( \omega(m) = \omega(m)^{-1} u_0 c \) and we have \( \omega(m)^{-1} g_j \in u_0^{-1} U g_j G c^{-1} = U g_j G \).

\[ \square \]

Now we review the definition of the action of Hecke operators on functions on the double coset \( U \setminus G_A / G \). In particular when \( G_{\infty} \) is compact, this is nothing but the space of automorphic forms of trivial weight (See [4] and [5] (1)). We define the space \( \mathcal{M}_0(U) \) by

\[ \mathcal{M}_0(U) = \{ f : G_A \to \mathbb{C} ; f(uga) = f(g) \text{ for any } u \in U, a \in G, g \in G_A \}. \]

Then for any \( \varepsilon \in G_A \) and \( U \varepsilon U \subset \bigcup_{j=1}^{d} \varepsilon_j U \), the double coset acts on \( f(g) \in \mathcal{M}_0(U) \) by

\[ ([U \varepsilon U] f)(g) = \sum_{j=1}^{d} f(\varepsilon_j^{-1} g) \quad (g \in G_A). \]

For the class number \( h = h(\mathcal{L}) \) of \( \mathcal{L} = \mathcal{L}(L) \) and \( 1 \leq i \leq h \), we denote by \( f_i \) the element in
$M_0(U)$ such that $f_i(g) = 1$ for any $g \in Ug_iG$ and $= 0$ for any $g \in Ug_jG$ with $j \neq i$. Then since $\mathfrak{M}_0(U)$ is the set of functions on $G_A$ which are constant on each double coset $Ug_iG$, we see that $(f_1, \ldots, f_h)$ is a basis of $\mathfrak{M}_0(U)$ and $h = \dim \mathfrak{M}_0(U)$. To count the type number by traces of Hecke operators, we define Hecke operators $R(m\epsilon^2_l)$ for $m|\mathfrak{d}$ and $\epsilon_l$ for $1 \leq l \leq h_0$ by

$$R(m\epsilon^2_l) = U\omega(m)\epsilon_lU.$$ 

(Here we write $\epsilon^2_l$ in $R(*)$ just because $\epsilon^2_l \in F_A^x$ gives the multiplicator of the similitude $\epsilon_l1_n$ and fits the notation $m$.) If we denote by $t$ the number of prime divisors of $\mathfrak{d}$, then there are $2^{t}h_0$ such operators. Since $\omega_cR_c = R_c\omega_c$, we have $\omega_cR^* = R^*\omega_c$ and $\omega_cU_c = U_c\omega_c$. Also $\epsilon_l1_n$ is in the center of $G_A$. So it is clear that $U\omega(m)\epsilon_lU = \omega(m)\epsilon_lU$. So these operators are obviously commutative. By definition, this acts on $\mathfrak{M}_0(U)$ by

$$R(m\epsilon^2_l)f = [U\omega(m\epsilon^2_l)U]f = f(\omega(m)^{-1}\epsilon^2_lg).$$

By definition, we have $R(m\epsilon^2_l)f_j = f_j$ for the unique $j$ such that $\omega(m)^{-1}\epsilon^2_lg_j \in Ug_jG$. So $R(m\epsilon^2_l)$ induces a permutation of $(f_1, \ldots, f_h)$. If $c \in F_A$ belongs to the trivial ideal class, then we have $U(c1_n)U = (c1_n)U$ with $c \in F^x$ and this acts trivially on $\mathfrak{M}_0(U)$, so the definition of $R(m\epsilon^2_l)$ depends only on $m$ and the class of $\epsilon_l$. We have $(U\omega(m)\epsilon_lU)^2 = Um\epsilon^2_l$ for some $m \in F_A^x$ and this also acts as a permutation on $(f_1, \ldots, f_h)$. We also see by this that the image of the action of the algebra of $R(m\epsilon^2_l)$ for all $m$ and $\epsilon_l$ is a finite abelian group. As a whole, the action of the semi-group spanned by $R(m\epsilon^2_l)$ on $\mathfrak{M}_0(U)$ is regarded as an action of a finite abelian group $\Gamma$ of order $2^{t}h_0$.

Now we review an easy general theory of group actions. Let $\Gamma$ be a finite abelian group acting on a finite set $X$ (faithful or not.) We would like to count the number of the transitive orbits of $X$ under $\Gamma$. We denote by $\rho$ the linear representation on the formal sum $\oplus_{x \in X}\mathbb{C}x$ associated to the action of $\Gamma$ on the set $X$.

**Lemma 3.4.** The number $T$ of transitive orbits of $X$ by $\Gamma$ is given by

$$T = \frac{1}{|\Gamma|} \sum_{g \in \Gamma} Tr(\rho(g)).$$

**Proof.** Let $X = \bigcup_{i=1}^{\Gamma} X_i$ be the decomposition into the disjoint union of transitive orbits of $\Gamma$. Then $\Gamma$ acts on $X_i$ transitively. Fix $x_i \in X_i$ for each $i$ and denote by $\Gamma_i$ the stabilizer of $x_i$ in $\Gamma$. Then we have $|X_i| = |\Gamma/\Gamma_i|$. The stabilizer of any other point $\gamma x_i \in X_i$ for $\gamma \in \Gamma$ is $\gamma\Gamma_i\gamma^{-1}$, but since $\Gamma$ is abelian, this is equal to $\Gamma_i$. So $\Gamma_i$ acts trivially on $X_i$. Also, any $\gamma \in \Gamma$ with $\gamma \notin \Gamma_i$ has no fixed point in $X_i$. So if we denote by $\rho_i$ the linear representation of $\Gamma$ associated with the action on $X_i$, then we have

$$Tr(\rho_i(g)) = \begin{cases} |X_i| & \text{if } g \in \Gamma_i, \\ 0 & \text{if } g \notin \Gamma_i. \end{cases}$$

In other words, we have

$$\sum_{g \in \Gamma} Tr(\rho_i(g)) = |X_i||\Gamma_i| = |\Gamma|.$$ 

Since we have $\rho = \sum_{i=1}^{\Gamma} \rho_i$, we have
\[
\sum_{g \in \Gamma} \text{Tr} (\rho(g)) = \sum_{i=1}^{T} |\Gamma| = |\Gamma| \times T.
\]

Hence we prove the lemma. □

Now we come back to the G-type number.

**Proposition 3.5.** We have \( R_i \cong_c R_j \) if and only if \( f_i \) and \( f_j \) are in the same orbit of the action of the semi-group spanned by \( \{ R(\text{mc}_i^2) ; m|d, 1 \leq l \leq h_0 \} \).

Proof. This claim is obvious from Proposition 3.3. □

**Theorem 3.6.** The G-type number \( T \) is given by

\[
T = \sum_{i=1}^{h_0} \sum_{m|b} \text{Tr} (R(\text{mc}_t^2)) \frac{2^h}{h_0},
\]

where \( \text{Tr} \) means the trace of the action of the \( U \)-double cosets on \( M_0(U) \).

### 3.2. Relation with global integral elements.

**Interpretation of the above results in terms of global quaternion hermitian matrices.**

For that purpose, we specialize the situation. From now on, we assume that \( F = \mathbb{Q} \) and \( B \) is a definite quaternion algebra over \( \mathbb{Q} \). We assume that the quaternion hermitian form is positive definite, so \( J = 1 \). Then \( g^* = g' = \overline{g} \) and \( n(g) > 0 \) for \( g \in G \). For a left \( \mathcal{O} \)-lattice \( L \), we define \( U = U(L) \) as before. For \( \mathbb{G}_A = \bigcup_{i=1}^{h} U g_i G \) with \( g_1 = 1 \), we may assume that \( n(g_i) = 1 \) since the class number of \( \mathbb{Q} \) is one and we have \( n(G_A) = n(G) \). The set of lattices \( L_i = Lg_i (1 \leq i \leq h) \) is a complete set of representatives of the classes in \( \mathcal{L}(L) \). We assume \( n \geq 2 \). Then by the strong approximation theorem on \( \text{GL}_n(B) \), we can show easily that any left \( \mathcal{O} \)-lattice \( L \) may be written as \( L = \mathcal{O}^r h \) for some \( h \in \text{GL}_n(B) \). We define the associated quaternion hermitian matrix by \( H = hh^* \). This is positive definite. We say that two quaternion hermitian matrices \( H_1 \) and \( H_2 \) are equivalent if there exists \( u \in \text{GL}_n(O) \) and \( 0 < m \in \mathbb{Q}^x \) such that \( uH_1u^* = mh_2 \).

**Lemma 3.7.** Assume that \( n \geq 2 \). By the above mapping, the set of \( G \) equivalence classes of left \( \mathbb{O} \)-lattices and the set of equivalence classes of positive definite quaternion hermitian matrices correspond bijectively.

A proof is the same as in Lemma 2.1 and omitted here. For representatives \( L = L_1 \ldots L_h \) of the genus \( \mathcal{L}(L) \), where \( L_i = Lg_i \), we can take \( h_i \in \text{GL}_n(B) \) such that \( L_i = \mathcal{O}^r h_i \) \((1 \leq i \leq h)\). So we have \( L_i = Lg_i = \mathcal{O}^r h_i g_i \). Then we have \( uh_i = h_1 g_i \) for some \( u \in \text{GL}_n(\mathbb{O}) \). We define \( \text{GL}_n(\mathbb{O}) \) by \( D \) the discriminant of \( B \). For \( m|D \), we define \( \omega(m) \) as before. We denote by \( R \) the right order of \( L \) as before.

**Proposition 3.8.** For \( 0 < m \) with \( m|D \), the following conditions (1) and (2) are equivalent.

1. \( \omega(m)^{-1} g_i \in U g_j G \).
2. There exists \( \alpha \in M_n(\mathbb{O}) \) such that \( \alpha M_n(\mathbb{O}) = M_n(\mathbb{O}) \alpha \) and \( ah_i h_j^* \alpha^* = mh_i h_j \).

Proof. Assume (1). We have \( \omega(m)^{-1} g_i = u g_j a \) for some \( u \in U \), \( a \in G \), and \( g_i = \omega(m) u g_j a \).

Since all the \( p \)-adic components of \( \omega(m) \) are in \( R_p \), we have \( L \omega(m) \subset L \). Hence
Since $L_i = \mathcal{O}^n h_i$ and $L_j = \mathcal{O}^n h_j$, we have $\mathcal{O}^n h_i \subset \mathcal{O}^n h_j$. Hence if we put $\alpha = h_i a^{-1} h_j^{-1}$ then $\mathcal{O}^n \alpha \subset \mathcal{O}^n$, so $\alpha \in M_n(\mathcal{O})$ and $h_i a^{-1} \alpha^* = n(a)^{-1} h_i h_j^*$. Since we assumed $n(g_j) = n(g_i) = 1$, we have $n(u(m(u) = n(\omega(m)^{-1})$. Since $n(u) \in \mathbb{R}^n \prod_p \mathbb{Z}_p^*$, $n(\omega(m)) \in \mathbb{R}^n \prod_p \mathbb{Z}_p^*$, and $n(a) \in \mathbb{Q}^n$, we have $n(a) = m^{-1}$, and $h_i h_j^{-1} h a^{-1} = m h_i h_j^*$. By definition of $a$, we have $a^{-1} = g_i^{-1} \omega(m) u g_j$, so

$$a^{-1} R_j = g_i^{-1} \omega(m) u g_j (g_j^{-1} R g_j) = g_i^{-1} \omega(m) u R g_j = g_i^{-1} R \omega(m) u g_j = g_i^{-1} R g_j a^{-1} = R_j a^{-1}.$$ 

Since we have $R_k = h_i^{-1} M_n(\mathcal{O}) h_k$ for any $k$, we have $a^{-1} h_j^{-1} M_n(\mathcal{O}) h_j = h_i^{-1} M_n(\mathcal{O}) h_i a^{-1}$, and $h_i a^{-1} h_j^{-1} M_n(\mathcal{O}) = M_n(\mathcal{O}) h_i a^{-1} h_j^{-1}$. Since $\alpha = h_i a^{-1} h_j^{-1}$ by definition, we see that $\alpha M_n(\mathcal{O})$ is a two-sided ideal. Hence we have (2). Now assume (2) and define $a$ by $a^{-1} = h_i^{-1} a h_j$. Then $a \in G$ and $n(a^{-1}) = m$. By $\alpha M_n(\mathcal{O}) = M_n(\mathcal{O}) \alpha$, $n(g_i a^{-1} g_j^{-1}) = m$, and Lemma 3.1, we have $g_i a^{-1} g_j^{-1} = \omega(m) u$ with $u \in U$. So $\omega(m)^{-1} g_i = u g_j a \in U g_j G$. So we have (1).

Now for a fixed $i$, if there exists no $j \neq i$ such that $R_j \cong G R_i$, then by Proposition 3.3, for any $j \neq i$ and $m|D$, we have $\omega(m)^{-1} g_i G \not\subset Ug_j G$. But $\omega(m)^{-1} g_i \in G_A = \bigcup_{j=1}^{k} U g_j G$, so we have $\omega(m)^{-1} g_i \in U g_j G$ for all $m|D$. If we assume that $D = p$ is a prime, then $R_i \cong G R_j$ if and only if $\omega(m)^{-1} g_i \in U g_j G$ for $m = 1$ or $p$. So we have

**Lemma 3.9.** Assume that $D = p$ is a prime. We fix $i$. Then there exists at most one $j \neq i$ such that $R_j \cong G R_i$. If there exist such $j \neq i$, then we have $\omega(p)^{-1} g_i \in U g_j G$. If $R_i \cong G R_j$ only for $j = i$, then $\omega(p)^{-1} g_i \in U g_i G$.

Proof. If there exist $j$ and $k$ such that $j \neq i$ and $k \neq i$, then $g_i \not\in U g_j G$ and $g_j \not\in U g_k G$, and if $R_i \cong G R_j \cong G R_k$ besides, then by Proposition 3.3, we have $\omega(p)^{-1} g_i \in U g_j G$ and $\omega(p)^{-1} g_j \in U g_i G$, hence $U g_j G \not\subset U g_i G$ so $j = k$. If there exist no $j \neq i$ such that $R_i \cong G R_j$, then we have $\omega(p)^{-1} g_i \not\in U g_j G$ for any $j \neq i$. This means that $\omega(p)^{-1} g_i \in U g_i G$. So, when $D = p$ is a prime, then the $G$-type of any genus is either a subset of a pair of maximal orders or a subset of single element in $\{R_i; 1 \leq i \leq h\}$.

**4. Models of polarizations defined over $\overline{\mathbb{F}}_p$**

**4.1. Polarizations on superspecial abelian varieties.** Let $A$ be an abelian variety and $A'$ the dual of $A$. For an effective divisor $D$ of $A$, we define an isogeny $\phi_D$ from $A$ to $A'$ by

$$\phi_D(t) = Cl(D_t - D) (t \in A),$$

where $D_t$ is the translation of $D$ by $t$ and $Cl$ denotes the linear equivalence class of the divisor. We say that an isogeny $\lambda$ from $A$ to $A'$ is a polarization if there exists an effective divisor $D$ such that $\lambda = \phi_D$. We say that a polarization $\lambda$ is a principal polarization if $\lambda$ is an isomorphism. Two polarized abelian varieties $(A_1, \lambda_1)$ and $(A_2, \lambda_2)$ are said to be isomorphic if there exists an isomorphism $\phi : A_1 \to A_2$ such that $\lambda_1 = \phi' \lambda_2 \phi$, where $\phi'$ is the dual map from $A_1'$ to $A_2'$ associated with $\phi$.

Let $p$ be a prime. An elliptic curve $E$ over a field of characteristic $p$ such that $\text{End}(E)$ is a maximal order of a definite quaternion algebra $B$ with discriminant $p$ is called supersingular. There exists a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$ such that $\text{End}(E)$ contains an
element $\pi$ with $\pi^2 = -p \cdot id_E$. We fix such an $E$ once and for all. Then we can regard $\pi$ as the Frobenius endomorphism of $E$ and every element of $\text{End}(E)$ is defined over $\mathbb{F}_p^2$. An abelian variety $A$ which is isogenous to $E^n$ is called supersingular. An abelian variety which is isomorphic to $E^n$ is called superspecial. It is well known that any product of various supersingular elliptic curves are all isomorphic (Shioda, Deligne). The superspecial abelian variety $E^n$ has a principal polarization defined over $\mathbb{F}_p$ (See [7]). Indeed, if we take a divisor $X$ defined by

$$X = \sum_{i=0}^{n-1} E^i \times [0] \times E^{n-1-i},$$

then the $n$-fold self-intersection $X^n = n!$, so det $\phi_X = 1$, and this is defined over $\mathbb{F}_p$. We put $O = \text{End}(E)$. Then we have identifications $\text{End}(E^n) = M_n(O)$ and $\text{Aut}(E^n) = M_n(O)^\times = GL_n(O)$. For any $\phi \in \text{End}(E^n)$, the Rosati involution is defined by $\phi^{-1}_X \phi \phi_X$. Then this is equal to $\phi^\sigma$ under the identification of $\text{End}(E^n)$ with $M_n(O)$. In particular, if we put $H_1 = \phi^{-1}_X \phi$ for a polarization $\lambda$, then $H_1 = H_2$ and $H_2$ is a positive definite quaternion hermitian matrix in $M_n(O)$. It is easy to show that two polarized abelian varieties $(E^n, A_1)$ and $(E^n, A_2)$ are isomorphism if and only if there exists an $\alpha \in GL_n(O)$ such that $\alpha H_2 \alpha^* = H_1$.

Any polarization $\lambda$ of $E^n$ is defined over $\mathbb{F}_p^2$ since $\phi_X$ is defined over $\mathbb{F}_p$ and any endomorphism of $E$ is defined over $\mathbb{F}_p^2$ by the choice of our $E$. We also see that if polarized abelian varieties $(E^n, A_1)$ and $(E^n, A_2)$ are isomorphic, then they are isomorphic over $\mathbb{F}_p^2$ since any element of $\text{Aut}(E^n)$ is defined over $\mathbb{F}_p^2$. Now we denote by $\sigma$ the Frobenius automorphism of the algebraic closure $\overline{\mathbb{F}_p}$ over $\mathbb{F}_p$.

**Lemma 4.1.** Notation being as before, a polarized abelian variety $(E^n, \lambda)$ has a model defined over $\mathbb{F}_p$ if and only if $(E^n, \lambda)$ and $(E^n, \lambda^r)$ are isomorphic.

Proof. Assume that there is a model $(A, \eta)$ of $(E^n, \lambda)$ defined over $\mathbb{F}_p$. We write an isomorphism $(A, \eta) \to (E^n, \lambda)$ by $\psi$. Here $\psi$ is defined over the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. Anyway, for any element $\tau \in \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, we have

$$(E^n, \lambda) \cong (A, \tau) = (A^\tau, \eta^\tau) \cong (E^n, \lambda^\tau).$$

So the condition is necessary. On the other hand, if $\psi$ gives an isomorphism $(E^n, \lambda) \cong (E^n, \lambda^r)$, then $\psi \in \text{Aut}(E^n)$ is defined over $\mathbb{F}_p^2$ and $\psi^\sigma \psi$ is an automorphism of $(E^n, \lambda)$ since $\lambda^\sigma \gamma = \lambda$. Since $\psi^\sigma \psi$ fixes a polarization (corresponding to a positive definite lattice), it is well-known that this is of finite order. So $(\psi^\sigma \psi)^r = (\psi^\sigma \psi)^{r^2} = 1$ for some positive integer $r$, where $1$ means the identity map of $E^n$. Now we regard $\sigma$ as a generator of the Galois group $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. Since $\psi$ is defined over $\mathbb{F}_p^2$, we have $\psi^\sigma = \psi$ and $(\psi^\sigma \psi)^{r^2} = \psi^\sigma \psi$. So if we put $f_1 = 1$, $f_\sigma = \psi$, and $f_{i\sigma} = \psi^r f_{i\sigma} \psi^r \cdots \psi f_{i\sigma}$ for $1 \leq i \leq 2r - 1$, then we have

$$f_{i\sigma} = \psi^r f_{i\sigma} \psi^r \cdots \psi^r f_{i\sigma} \psi^r = f_{i\sigma}.\$$

This is obvious if $i + j < 2r$. If $2r \leq i + j \leq 4r - 1$, then this is equal to

$$\psi^{r(i + j - 2r)} \cdots \psi^r \psi f_{i\sigma},$$

since we have

$$\psi^{r(i + j - 2r)} \cdots \psi^r \psi f_{i\sigma} = ((\psi^\sigma \psi)^{r^2} \cdots (\psi^\sigma \psi)^{r^4} \cdots = 1,$$
where $\delta = 0$ or $1$ according as $i + j$ is even or odd. So we have $f_{\alpha^r,\tau} = f_{\alpha^r,\sigma}$ and the set of maps $\{f_{\alpha^r}; 0 \leq i \leq 2r - 1\}$ satisfies the descent condition for $\text{Gal}(\overline{\mathbb{F}_p}, \mathbb{F}_p)$ (See [15]). So we have a model over $\mathbb{F}_p$.

\textbf{Proposition 4.2.} Notation being the same as before, the polarized abelian varieties $(E^n, \lambda)$ and $(E^n, \lambda')$ are isomorphic if and only if $\alpha^r H_\lambda \alpha = pH_\lambda$ for some $\alpha \in \text{End}(E^n) = M_n(O)$ such that $\alpha M_n(O) = M_n(O)\alpha$.

\textbf{Proof.} Let $F$ be the Frobenius endomorphism of $E^n$ over $\mathbb{F}_p$ and set $F = \pi 1_n$ where $\pi$ is a prime element of $O$ over $p$ with $\pi^2 = -p$. Let $F_1$ be the Frobenius map of $(E^n)'$ over $\mathbb{F}_p$. (Actually it is the same as $F$ if we identify $(E^n)'$ with $E^n$.) For a polarization $\lambda$ of $E^n$, we have $\lambda' F = F_1 \lambda$ by definition. In particular, since $\phi_X$ is defined over $\mathbb{F}_p$, we have $\phi_X F = F_1 \phi_X$. So we have $(\phi_X^{-1} \lambda') F = F(\phi_X^{-1} \lambda)$. Now assume that $(E^n, \lambda')$ and $(E^n, \lambda)$ are isomorphic. This means that there exists an automorphism $\phi$ of $E^n$ such that $\lambda^\phi = \phi' \lambda$. So we have $\phi_X^{-1} \lambda' = T_{\phi_X^{-1}} \phi_X^{-1} \lambda$. We have $\phi_X^{-1} \phi_X = \phi^*$, identifying $\text{End}(E^n)$ with $M_n(O)$ and writing $g' = T_{\phi_X^{-1}}$ for any $g \in M_n(B)$. So if we put $H_\lambda = \phi_X^{-1} \lambda$, then we have $FH_\lambda = \phi^* H_\lambda \phi F$. Since $F^2 F = p 1_n$, we have $FH_\lambda = \alpha^r H_\lambda \alpha$ for $\alpha = \phi F$. We have $\alpha M_n(O) = \phi F M_n(O) = \phi M_n(O) F = M_n(O) F = M_n(O) \phi F = M_n(O) \alpha$. So we have proved the “only if” part. Conversely, assume that $\alpha H_\lambda = \alpha^r H_\lambda \alpha$ for some $\alpha \in M_n(O)$ such that $\alpha M_n(O)$ is a two sided ideal. Since we assumed that the two sided prime ideal of $O$ over $p$ is generated by $F \in O$, it is classically well-known that any two sided ideal of $M_n(O)$ is given by $b F^r M_n(O)$ with positive rational number $b$ and some non-negative integer $r$. So we have $\alpha = b F^r \epsilon$ for some $\epsilon \in GL_n(O) = M_n(O)^\times$. By taking the reduced norm of both sides of $p H_\lambda = \alpha^r H_\lambda \alpha$, we see that the reduced norm $N(\alpha)$ of $\alpha$ is $p^r$. Since $N(F) = p^r$ and $N(\epsilon) = 1$, we see that $p^r = b^{2n} p^{nr}$, so $b = p^{r(1-r)/2}$. Since $F^2 = -p$, this is equal to $\pm p^{(1-r)}$, and $\alpha = \phi F^s$ for some $\phi \in GL_n(O)$. Here comparing the reduced norm, we have $s = 1$ and this $\phi$ gives an isomorphism of $(E^n, \lambda)$ to $(E^n, \lambda')$.

\textbf{4.2. Relation to the type number.} For any polarization $\lambda$ of $E^n$, $\phi_X^{-1} \lambda$ is a positive definite quaternion hermitian matrix in $M_n(O)$. If $L$ is the genus of quaternion hermitian lattices to which $\phi_X^{-1} \lambda$ belongs, we write $L = L(\lambda)$ and we say that $\lambda$ belongs to $L$ by abuse of language. We denote by $P(\lambda)$ the set of polarizations of $E^n$ which belong to the same genus as $\lambda$ belongs to. We denote by $H(\lambda)$ and $T(\lambda)$ the class number and the type number of $L(\lambda)$, respectively.

\textbf{Theorem 4.3.} Assume that $n \geq 2$ and fix a polarization $\lambda$ of $E^n$. Then the number of isomorphism classes of polarizations in $P(\lambda)$ is equal to $H(\lambda)$. The number of isomorphism classes of $(E^n, \mu)$ with $\mu \in P(\lambda)$ which have a model over $\mathbb{F}_p$ is equal to $2T(\lambda) - H(\lambda)$.

\textbf{Proof.} The first assertion is obvious so we prove the second assertion. We define $U$ as the stabilizer in $G_A$ of a lattice corresponding to $H_\lambda = \phi_X^{-1} \lambda$ and write $G_A = \bigcup_j U g_j G$. The isomorphism classes of $\mu \in P(\lambda)$ correspond bijectively to the set $\{g_j\}$, so assume that $\mu$ corresponds to $g_j$. Write $H_\mu = \phi_X^{-1} \mu$ as before. The condition that $\alpha H_\mu \alpha^r = p H_\mu$ for some $\alpha \in M_n(O)$ with $\alpha M_n(O) = M_n(O) \alpha$ is equivalent to the condition that $\omega(p) g_j \in U g_j G$ by Proposition 3.8. The number of isomorphism classes of such $\mu$ is equal to $T(r(p))$ by Lemma 3.9. Since $T(\lambda) = (Tr(R(p)) + Tr(R(1)))/2 = (Tr(R(p)) + H(\lambda))/2$, we prove the assertion.
We note that even if \((E^n, \lambda)\) has a model over \(\mathbb{F}_p\), it is not necessarily true that \(E^n\) has a polarization equivalent to \(\lambda\) defined over \(\mathbb{F}_p\). We give such an example below. If a polarization \(\lambda\) of \(E^n\) is defined over \(\mathbb{F}_p\), this means that \(F(\phi^{-1}_X \lambda) = (\phi^{-1}_X) F\), so the quaternion hermitian matrix associated with \(\lambda\) should be realized as a matrix which commutes with \(\pi\). Now when the discriminant of \(B\) is a prime \(p\), there are two genera of quaternion hermitian maximal left \(O\)-lattices in \(B^n\), the one which contains \(O^n\), and the other which does not contain \(O^n\). We call the former a principal genus, denoted by \(\mathcal{L}_{pr}\), and the latter a non-principal genus denoted by \(\mathcal{L}_{npr}\). Now we consider the case \(\mathcal{L}_{npr}\). If \(n = 2\) and \(O\) contains \(\pi\), then any quaternion hermitian matrix associated with a lattice in \(\mathcal{L}_{npr}\) is given by

\[
H_1 = m \left( \begin{array}{cc} pt & \pi r \\ \overline{pt} & ps \end{array} \right)
\]

with \(0 < m \in \mathbb{Q}\), \(t, s \in \mathbb{Z}\) and \(r \in O\) such that \(pts - N(r) = 1\). If \(p = 3\), the maximal order \(O\) of \(B\) is concretely given up to conjugation by

\[
O = \mathbb{Z} + \mathbb{Z} \frac{1 + \pi}{2} + \mathbb{Z} \beta + \mathbb{Z} \frac{(1 + \pi)\beta}{2},
\]

where \(\pi^2 = -3\), \(\beta^2 = -1\), \(\pi \beta = -\beta \pi\). If \(H_1\) commutes with \(\pi\), then \(r\) should be in \(\mathbb{Q}(\pi)\). So we should have \(3ts - N(r) = 1\) for some positive integers \(t\), \(s\) and an element \(r = (a + b\pi)/2\) with \(a, b \in \mathbb{Z}\), \(a \equiv b \mod 2\). Here \(N(r) = (a^2 + 3b^2)/4\) but we should have \(N(r) \equiv -1 \mod 3\) by the above relation. This means that \(a^2 \equiv -1 \mod 3\) but this is impossible. So there is no such polarization. On the other hand, since the class number \(H\) is 1 for this genus, and hence the type number \(T\) is also 1, we have \(2T - H = 1\). More concretely, if we put

\[
H = \left( \begin{array}{cc} 3 & \pi(1 + \beta) \\ -\pi(1 + \beta) & 3 \end{array} \right),
\]

\[
\alpha = \left( \begin{array}{ccc} \beta & 0 \\ 0 & \pi \\ 0 & 1 \end{array} \right) = \left( \begin{array}{cc} \beta \pi & 0 \\ 0 & \pi \end{array} \right),
\]

then \(H\) corresponds with a lattice in \(\mathcal{L}_{npr}\), and we have \(aH\alpha^* = 3H\) and \(aM_2(O) = M_2(O)\alpha\). This means that the corresponding polarized abelian surface has a model over \(\mathbb{F}_3\). Besides, for any \(n \geq 2\), if we take \([n/2]\) copies of \(H\) and take

\[
H_n = H \perp \cdots \perp H \perp p
\]

where \(p\) appears only when \(n\) is odd, then the corresponding \(n\)-dimensional polarized abelian variety also has a model over \(\mathbb{F}_3\). By the way, for \(n = 2\), we will see in \([6]\) that \(2T(\mathcal{L}_{npr}) - H(\mathcal{L}_{npr}) > 0\) for all \(p\). So in the same argument, we see that

**Proposition 4.4.** For all primes \(p\), there exists a polarized abelian variety, whose polarization belongs to \(\mathcal{L}_{npr}\), that has a model over \(\mathbb{F}_p\).

### 4.3. Components of the supersingular locus which have models over \(\mathbb{F}_p\)

We denote by \(A_{n,1}\) the moduli of principally polarized abelian varieties and by \(S_{n,1}\) the locus of principally polarized supersingular abelian varieties in \(A_{n,1}\). The author learned the following theorem from Professor F. Oort.

**Theorem 4.5** (Li-Oort [10], Oort [11], Katsura-Oort [9]). (1) The set of irreducible components of \(S_{n,1}\) corresponds bijectively with equivalence classes of polarizations of \(E^n\) be-
Type Numbers of Quaternion Hermitian Forms

longing to \( L_{pr} \) if \( n \) is odd, and to \( L_{npr} \) if \( n \) is even, respectively.

(2) The locus \( S_{n,1} \) is defined over \( \mathbb{F}_p \). Each irreducible component of \( S_{n,1} \) is defined over \( \mathbb{F}_p \). The irreducible component corresponding to the polarization \( \lambda \) in the sense of (1) has a model defined over \( \mathbb{F}_p \) if and only if \( (E^n, \lambda) \) has a model over \( \mathbb{F}_p \).

For any genus \( L \) of quaternion hermitian lattices, we denote by \( H(L) \) and \( T(L) \) the class number and the type number of \( L \) as before. As a corollary of our previous Theorems 4.3 and 4.5 and Proposition 4.4, the following theorem is obvious.

**Theorem 4.6.** Assume that \( n \geq 2 \). Then the number of irreducible components of \( S_{n,1} \) which have models over \( \mathbb{F}_p \) is equal to \( 2T(L_{pr}) - H(L_{pr}) \) when \( n \) is odd and to \( 2T(L_{npr}) - H(L_{npr}) \) when \( n \) is even. In particular, there always exists an irreducible component of \( S_{n,1} \) defined over \( \mathbb{F}_p \).

Proof. Except for the last claim, the assertion has been already proved. It is obvious that \( 2T(L_{pr}) - H(L_{pr}) > 0 \) for all \( n \), since \( E^n \) has a principal polarization defined over \( \mathbb{F}_p \). So by Proposition 4.4 and Theorem 4.5, we have the claim. \( \square \)

When \( n = 2 \), the number \( 2T(L_{npr}) - H(L_{npr}) \) is concretely given in [6] and is always positive, as we remarked.

References

T. IBUKIYAMA

Department of Mathematics
Graduate School of Science
Osaka University
Machikaneyama 1-1, Toyonaka, Osaka, 560-0043
Japan
e-mail: ibukiyam@math.sci.osaka-u.ac.jp