TYPE NUMBERS OF QUATERNION HERMITIAN FORMS AND SUPERSINGULAR ABELIAN VARIETIES

Ibukiyama, T.
Osaka J. Math.
55 (2018), 369–384

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 $\mathfrak{O}$ of B. The class number H of B is the number of equivalence classes of left $\mathfrak{O}$-ideals $\mathfrak{a}$ 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 $\mathfrak{O}$-ideal $\mathfrak{a}$, 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 $B_A^\times$ (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 $\mathrm{End}(E)$ 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 $M_n(\mathfrak{O})$, 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 $\mathfrak{O}$-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 $L = L_1, \dots, L_h$ 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 $R_i \cong_G R_j$. The number T of types in $\{R_i : 1 \le i \le h\}$ 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 ϕ_X associated with a divisor $X = \sum_{a+b=n-1} E^a \times \{0\} \times E^b$. For any polarization λ of A, the map $\phi_X^{-1}\lambda$ gives a positive definite quaternion hermitian matrix in $\mathrm{End}(A) = M_n(\mathfrak{O})$ for a maximal order $\mathfrak{O}$ 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 μ of A such that $\phi_X^{-1}\mu \in \mathcal{L}(\phi_X^{-1}\lambda)$. We fix λ 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, μ) 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 $\mathcal{A}_{n,1}$ 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 $\alpha \in B$, we denote by $Tr(\alpha)$ and $N(\alpha)$ the reduced trace and the reduced norm over F, respectively. We denote by $\overline{\alpha}$ the main involution of B over F, so $Tr(\alpha) = \alpha + \overline{\alpha}$, $N(\alpha) = \alpha\overline{\alpha}$. A non-degenerate quaternion hermitian form f on B^n over B is defined to be a map $f : B^n \times B^n \to B$ such that $f(ax + by, z) = af(x, z) + bf(y, z)$ for $a, b \in B$, $\overline{f(y, x)} = f(x, y)$, and $f(x, B^n) = 0$ implies $x = 0$. For any $n_1 \times n_2$ matrix $b = (b_{ij}) \in M_{n_1 n_2}(B)$, we write ${}^t\overline{b} = (\overline{b_{ji}})$. It is well-known that, by a base change over B, we may assume that

$$f(x, y) = xJy^* \qquad (x, y \in B^n),$$

where $J = diag(\epsilon_1, \dots, \epsilon_n)$ 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 $v_1, \dots, v_r$ 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^n are equivalent under the base change over B if and only if their embeddings to the maps on $B^n_{v_i}$ are equivalent over B_{v_i} for all v_i $(1 \le i \le r)$. 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

$$G = \{g \in GL_n(B) = M_n(B)^\times; gJ\,{}^t\overline{g} = n(g)J \text{ for some } n(g) \in F^\times\}$$

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

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

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 $c1_n \in G$ or G_A.

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

$$Lg = \bigcap_{v:\text{ finite places}} (L_v g_v \cap B^n)$$

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

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

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

$$U_v = U(L_v) = \{u \in G_v; L_v = L_v u\}$$

and write $U = G_\infty \prod_{v<\infty} U_v$, where G_∞ is the product of all G_v over the archimedean places v. Then the class number h of $\mathcal{L}(L)$ is equal to $|U\backslash G_A/G|$, 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 $\mathfrak{O}_v = \mathfrak{O} \otimes_{\mathfrak{o}} \mathfrak{o}_v$. For $1 \le i \le h$, we define left $\mathfrak{O}$-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 $M_v = \mathfrak{O}_v^n h_p$ for some $h_p \in GL_n(B_v)$ (where we can take $h_v = 1$ for almost all v), so $R_{i,v} = R_i \otimes_{\mathfrak{o}} \mathfrak{o}_v = h_v^{-1} M_n(\mathfrak{O}_v) h_v$ 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

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

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 $a^{-1}R_i a = R_j$ for some $a \in G$. We denote this relation by $R_i \cong_G R_j$. The number of equivalence classes in $\{R_1, \ldots, R_h\}$ in this sense is called the type number T of $\mathcal{L}(L)$. 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, left $\mathfrak{O}_v$-lattices correspond to quaternion hermitian matrices. We denote by $GL_n(O_v)$ the group of nonsingular elements u in $M_n(O_v)$ such that $u^{-1} \in M_n(O_v)$. We say that $X \in M_n(B)$ is a quaternion hermitian matrix if $X = X^*$. We say that two hermitian matrices $X_1, X_2 \in M_n(B_v)$ are equivalent if there exists a $u \in GL_n(O_v)$ such that $uX_1u^* = mX_2$ for some $m \in F_v^\times$. We say that two left $\mathfrak{O}_v$-lattices L_1 and L_2 are G_v-equivalent if $L_1 g = L_2$ for some $g_v \in G_v$.

Lemma 2.1. *The set of G_v-equivalence classes of left $\mathfrak{O}_v$-lattices and the set of equivalence classes of 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 $J = J_1\, {}^t\overline{J_1}$ 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 $\mathfrak{O}_v$-lattice L_v may be written as $L_v = \mathfrak{O}_v^n h$ with $h \in GL_n(B_v)$ by the elementary divisor theorem. We define a map ϕ by $\phi(L_v) = hJ\,{}^t\overline{h}$. The equivalence class of the image does not depend on the choice of h. If $\mathfrak{O}_v^n h_1 g = \mathfrak{O}_v^n h_2$ for $g \in G_v$, then we have $uh_1g = h_2$ for some $u \in GL_n(O_v)$. This means that

$$n(g)uh_1Jh_1^*u^* = uh_1gJg^*h_1^*u^* = h_2Jh_2^*.$$

So ϕ 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 $\phi(O_v^n h) = X$. The map is injective. Indeed, if $uh_1Jh_1^*u^* = mh_2Jh_2^*$ for some $m \in F_v$, then $g = h_2^{-1}uh_1 \in G_v$ with $n(g) = m$ and we have $\mathfrak{O}_v^n h_2 g = \mathfrak{O}_v^n h_1$. □

For a finite place v, we denote by p_v a prime element of $\mathfrak{o}_v$. 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 π 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*

$$uHu^* = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & 0 & \vdots \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & A_r \end{pmatrix}$$

where $A_i = p_v^{e_i}$ *or*

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

Proof. We prove this by induction of the size of H. Multiplying by a power of p_v, we may assume that $H \in M_n(\mathfrak{O}_v)$. Assume that the $\mathfrak{O}_v$ ideal spanned by the components h_{ij} of $H = (h_{ij})$ is $\pi^e\mathfrak{O}_v$. 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 $O_v^\times$. If a diagonal component belongs to $O_v^\times$, then by permuting the rows and columns, we may assume that the $(1, 1)$ component h_{11} belongs to $O_v^\times$. Since $H = H^*$, this means $h_{11} \in \mathfrak{o}_v^\times$. Since we have $N(O_v^\times) = \mathfrak{o}_p^\times$, by changing H to $\epsilon H\epsilon^*$ for $\epsilon \in O_v^\times$ with $N(\epsilon) = h_{11}^{-1}$, 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 $u_1 = 1_n - \sum_{i=2}^n h_{i1}e_{i1}$, where we write $H = (h_{ij})$, obviously $u_1 \in GL_n(O_v)$ and we have

$$u_1Hu_1^* = \begin{pmatrix} 1 & 0 \\ 0 & H_1 \end{pmatrix}.$$

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

$$p_vt + p_vsN(b) + Tr(b\overline{\epsilon}).$$

Since it is well known that $Tr(O_v) = \mathfrak{o}_v$ (e.g. the unramified extension of F_v contains an integral element whose trace is one), we take $b = \epsilon_0\overline{\epsilon}^{-1}$ for an element $\epsilon_0 \in O_v$ such that $tr(\epsilon_0) = 1$. Since $1 + p_vt + p_vsn(b) \in \mathfrak{o}_v^\times$, we reduce to the previous case. Secondly we assume that $e = 1$. Then all the diagonal components belong to $p_v\mathfrak{o}_v$ and changing rows and columns, we may assume that $h_{12} = \pi\epsilon$ with $\epsilon \in \mathfrak{O}_v^\times$. We assume that $h_{11} = p_v^et_0$ with $e \geq 1$ and $t_0 \in \mathfrak{o}_v^\times$ and $h_{22} = p_vs$ with $s \in \mathfrak{o}_v$. Again by $v_1 = 1_n + b_1e_{12}$, the $(1, 1)$ component of $v_1Hv_1^*$ is given by $p_v^et_0 + p_vsN(b_1) + Tr(\pi\epsilon\overline{b_1})$. If we put $\overline{b_1} = p_v^{e-1}\epsilon^{-1}\overline{\pi}\epsilon_0$ with $\epsilon_0 \in \mathfrak{O}_v$ such that $Tr(\epsilon_0) = -t_0$, then we have

$$p_v^et_0 + p_vsN(b_1) + Tr(\pi\epsilon\overline{b_1}) = p_v^e(t_0 + Tr(\epsilon_0)) + sp_v^{2e}N(\epsilon^{-1}\epsilon_0) = p_v^{2e}sN(\epsilon^{-1}\epsilon_0).$$

This is divisible by p_v^{2e}. Since $Tr(\pi\mathfrak{O}_v) = p_v\mathfrak{o}_v$, we see that $\epsilon_0 \in \mathfrak{O}_v^\times$ and $b_1 \in p^{e-1}\pi\mathfrak{O}_v^\times$. Repeating the same process, we can take $v_i = 1 + b_ie_{12}$ such that the $(1, 1)$ component of $v_iv_{i-1}\cdots v_1Hv_1^*\cdots v_i^*$ is of arbitrary high p_v-adic order. Since the π-adic order of b_i monotonically increases, the limit $\lim_{i\to\infty} v_i\cdots v_1$ converges to $v \in GL_n(\mathfrak{O}_v)$ and we see that the $(1, 1)$ component of vHv^* is zero. By these changes, the $(1, 2)$ components always belong to $\pi\mathfrak{O}_v^\times$, so we may assume that $h_{11} = 0$ and $h_{12} = \pi\epsilon_2 \in \pi\mathfrak{O}_v^\times$. By taking the diagonal matrix $A_0 = \mathrm{diag}(1, \epsilon_2^{-1}, 1\ldots, 1) \in GL_n(O_v)$ and $A_0^*HA_0$, 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

$$\begin{pmatrix} 0 & \pi \\ \overline{\pi} & p_vs \end{pmatrix}$$

We have

$$\begin{pmatrix}1 & 0\\ b & 1\end{pmatrix}\begin{pmatrix}0 & \pi\\ \overline{\pi} & p_v s\end{pmatrix}\begin{pmatrix}1 & \overline{b}\\ 0 & 1\end{pmatrix} = \begin{pmatrix}0 & \pi\\ \overline{\pi} & p_v s + Tr(b\pi)\end{pmatrix}.$$

Since $Tr(\pi\mathfrak{O}_v) = p_v\mathfrak{o}_v$, we can take $b \in \mathfrak{O}_v$ such that $p_v s + Tr(b\pi) = 0$, 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 $\pi\mathfrak{O}_v$, and if we put

$$w = 1_n - \sum_{j=3}^{n} \overline{\pi}^{-1} h_{2j} e_{1j} - \sum_{j=3}^{n} \pi^{-1} h_{1j} e_{2j},$$

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

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

with $H_1 = \begin{pmatrix}0 & \pi\\ \overline{\pi} & 0\end{pmatrix}$, 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 $\mathfrak{O}_v$-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 $n(U_v) = \mathfrak{o}_v^\times$.*

Proof. First we show that $n(U_v) \subset \mathfrak{o}_v^\times$. Assume that $g \in U_v$ and $gg^\sigma = n(g)1_n$. Since $L_v g = L_v$ and L_v is a free 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 $g^\sigma = Jg^*J^{-1}$ is the same as that of g, this is also monic integral. In particular, the determinants of g and g^σ in this representation are integral. So $n(g)^{4n}$ 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 $n(g) \in \mathfrak{o}_v^\times$. Next we show the converse. First we assume that B_v is division. We take $h \in GL_v(B_p)$ such that $L_v = \mathfrak{O}^n h_v$ and put $H = h_v J\, {}^t\overline{h_v}$. Then for any $m \in \mathfrak{o}_v^\times$, we have an element $\alpha \in GL_n(\mathfrak{O}_v)$ such that $\alpha H \alpha^* = mH$. Indeed, we have $uHu^* = \mathrm{diag}(A_1, \ldots, A_r)$ for some $u \in GL_n(\mathfrak{O}_v)$ as in Proposition 2.2. Take $b_i \in \mathfrak{O}_v^\times$ such that $N(b_i) = m$, then if $A_i = p_v^e$, we have $b_i A_i b_i^* = mA_i$. If $A_i = \begin{pmatrix}0 & \pi\\ \overline{\pi} & 0\end{pmatrix}$, then $\mathfrak{O}_v$ is realized as $\mathfrak{O}_v = \mathfrak{o}_v^{un} + \mathfrak{o}_v^{un}\pi$ where $\pi^2 = -p$ and $\mathfrak{o}_v^{un}$ is a subring of $\mathfrak{O}_v$, which is isomorphic to the maximal order of the unique unramified quadratic extension of F_v. Here for $b \in \mathfrak{o}_v^{un}$, we have $b\pi = \pi\overline{b}$. We have $N((o_v^{un})^\times) = \mathfrak{o}_v^\times$ by local class field theory. So taking $b \in (\mathfrak{o}_v^{un})^\times \subset \mathfrak{O}_v^\times$ with $N(b) = m$, put

$$C_i = \begin{pmatrix}b & 0\\ 0 & \overline{b}\end{pmatrix}.$$

Then

$$C_i \begin{pmatrix}0 & \pi\\ -\pi & 0\end{pmatrix} C_i^* = \begin{pmatrix}0 & b\pi b\\ -\overline{b}\pi\overline{b} & 0\end{pmatrix} = m\begin{pmatrix}0 & \pi\\ -\pi & 0\end{pmatrix}.$$

So taking a diagonal matrix v consisting of diagonal blocks b_i and C_i, we have $vuHu^*v^* =$

$muHu^*$. So by $H = h_vJh_v^*$, we have $h_v^{-1}vuh_v \in G_p$ and $n(h^{-1}vuh) = m$. We also have $L_vh^{-1}vuh_v = O_v^n vuh_v = O_v^n h_v = L_v$, so $h_v^{-1}vuh_v \in U_v$. Next assume that $B_v = M_2(F_v)$. In this case, by virtue of Shimura [14] Proposition 2.10, there exists an element $X \in GL_n(B_v)$ satisfying $XX^* = 1_n$ and fractional left O_v-ideals $\mathfrak{b}_i$ such that $L_v = (\mathfrak{b}_1, \ldots, \mathfrak{b}_n)X$. Let m be any element in $\mathfrak{o}_v^\times$. we take $J_1 = \mathrm{diag}(u_1, \ldots, u_n)$ such that $J_1\, {}^t\overline{J_1} = J$. Since the right orders $\mathfrak{O}_i$ of $\mathfrak{b}_i$ are again maximal orders which are all conjugate to $M_2(o_v)$, there exist $\alpha_i \in u_i\mathfrak{O}_i^\times u_i^{-1}$ for each $1 \leq i \leq n$ such that $N(\alpha_i) = m$. Put $g = X^{-1}J_1^{-1}\mathrm{diag}(\alpha_1, \ldots, \alpha_n)J_1X$. Then we have

$$L_vg = (\mathfrak{b}_1u_1^{-1}\alpha_1, \ldots, \mathfrak{b}_nu_n^{-1}\alpha_n)J_1X = (\mathfrak{b}_1u_1^{-1}, \ldots, \mathfrak{b}_nu_n^{-1})J_1X = L_v.$$

So we have $g \in U_v$ and $gJg^* = mJ$. So $m \in n(U_v)$. □

3. G-type numbers and Hecke operators

3.1. A formula for a type number. We fix a left $\mathfrak{O}$-lattice L in B^n. We define $U \subset G_A$ by the group of stabilizers of L as before and fix representatives $L_1, \ldots, L_h$ 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 $\pi^eM_n(\mathfrak{O}_v)$ for some integer $e \geq 0$. When $B_v = M_2(F_v)$, then any two sided ideal of $M_n(\mathfrak{O}_v) \cong M_{2n}(\mathfrak{o}_v)$ in $M_n(\mathfrak{O}_v)$ is given by $p_v^eM_n(\mathfrak{O}_v)$ 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 $u_1\pi^eu_2M_n(O_p) = \pi^eM_n(O_p)$ when B_p is division.

Proposition 3.2. *When B_v is division, there exists an element $\omega_v \in R_v \cap G_v$ such that $\omega_v^2 = -p_v1_n$, $\omega_v\omega_v^* = p_v1_n$ and any two sided ideal of R_v in R_v is given by $\omega_v^eR_v$ for some $e \geq 0$.*

Proof. First we show that there exists an element $\omega_v \in R_v$ such that $\omega_v^2 = -p_v1_n$, $\omega_v\omega_v^\sigma = p_v1_n$, and $\omega_vR_v = R_v\omega_v$. Take $h_v \in GL_n(B_v)$ such that $L_v = \mathfrak{O}_v^nh_v$ and put $H = h_vJ\,{}^t\overline{h_v}$. 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 $L_v \subset O_v^n$ and $H \in M_n(\mathfrak{O}_v)$. Then by Proposition 2.2, there exists some $u \in GL_n(O_v)$ such that all the components of uHu^* are in $\mathfrak{o}_v \cup \pi\mathfrak{o}_v$. So we have $\pi(uHu^*) = (uHu^*)\pi$, so $\pi(uHu^*)\overline{\pi} = puHu^*$. So if we put $\omega_v = h_v^{-1}u^{-1}\pi uh_v$, then we have $\omega_vJ\omega_v^* = p_vJ$ and $\omega_v^2 = -p_v1_n$. We also have $\mathfrak{O}_v^nh_v\omega_v = \mathfrak{O}_v^nu^{-1}\pi uh_v = \mathfrak{O}_v^n\pi uh_v \subset \mathfrak{O}_v^nuh_v = \mathfrak{O}_vh_v$, so $\omega_v \in h_v^{-1}M_n(\mathfrak{O}_v)h_v = R_v$. We also have $R_v\omega_v = h_v^{-1}M_n(\mathfrak{O}_v)u^{-1}\pi uh_v = h_v^{-1}u^{-1}M_n(\mathfrak{O}_v)\pi uh = h_v^{-1}u^{-1}\pi uM_n(\mathfrak{O}_v)h_v = \omega_vR_v$, so $R_v\omega_v$ is a two sided ideal. By using Lemma 3.1, any two sided ideal of R_v is given by $h_v^{-1}u_1\pi^eu_2h_vR_v$ for some $e \geq 0$ and any u_1, $u_2 \in GL_n(\mathfrak{O}_v)$ and this is equal to $\omega_v^eR_v$. □

We denote by $\mathfrak{d}$ the $\mathfrak{o}_v$-ideal defined as the product of the prime ideals p_v of $\mathfrak{o}_v$ such that B_v is division. This is called the discriminant of B. We say that p_v is ramified when B_v is division and split when $B_v = M_2(F_v)$. We fix ω_v for $p_v|D$ as above and for any integral ideal $\mathfrak{m}|\mathfrak{d}$ of $\mathfrak{o}_v$, we define $\omega(\mathfrak{m}) = (g_v) \in G_A$ by setting $g_v = 1$ for all archimedean places v and finite places v such that $p_v \nmid \mathfrak{m}$, and $g_v = \omega_v$ for any places v such that $p_v|\mathfrak{m}$. We put $F_\infty = \prod_{v\,:\,\text{infinite}} F_v$ where v runs over all archimedean places of F. We choose a complete set $\mathfrak{c}_1, \ldots, \mathfrak{c}_{h_0}$ of representatives of $F_A^\times/F^\times \cdot F_\infty^\times \prod_v \mathfrak{o}_v^\times$. 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 $\mathfrak{c}_i$ as an element of G_A. We also have $(F_\infty^\times \prod_v \mathfrak{o}_v^\times)1_n \subset U$ for any $\mathfrak{O}$-lattice L. We have

Proposition 3.3. (1) *R_i and R_j have the same G-type if and only if $\mathfrak{c}_l^{-1}\omega(\mathfrak{m})^{-1}g_i \in Ug_jG$ for some $\mathfrak{m}|\mathfrak{d}$ and some $\mathfrak{c}_l$.*
(2) *Assume that the class number of F is one. Then for a fixed $\mathfrak{m}|\mathfrak{d}$, if $\omega(\mathfrak{m})^{-1}g_i \in Ug_jG$, then $\omega(\mathfrak{m})^{-1}g_j \in Ug_iG$.*

Proof. First we assume that $R_i \cong_G R_j$, so we have $a^{-1}R_ia = R_j$ for some $a \in G$. This means that $a^{-1}g_i^{-1}Rg_ia = g_j^{-1}Rg_j$, so by definition, we have $a^{-1}g_{i,v}^{-1}R_pg_{i,v}a = g_{j,v}R_pg_{j,v}$, where $g_{i,v}$ and $g_{j,v}$ are v-adic components of g_i and g_j. So $R_vg_{i,v}ag_{j,v}^{-1}$ is a two sided ideal of R_v. So if B_v is division, then $g_{i,v}ag_{j,v} = \omega_v^{e_v}u$ with $u \in U_v$. If $B_v = M_2(F_v)$, then $g_{i,v}ag_{j,v}^{-1} = p_v^{e_v}u$ with $u \in U_v$. Since $g_{i,v}ag_{j,v}^{-1}$ is the v-component of an element in G_A, we have $g_{i,v}ag_{j,v}^{-1} \in U_v$ for almost all v. So $e_v \neq 0$ only for the finitely many v. We denote by m_1 an element of $F_A^\times$ such that v component is $p_v^{e_v}$ for split primes p_v, and $p_v^{[e_v/2]}$ 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 $m_1 = u_0\mathfrak{c}_lc$ with $u_0 \in F_\infty \prod_v \mathfrak{o}_v^\times$ and $c \in F^\times$. If we define $\mathfrak{m}$ as a product of ramified p_v such that e_v is odd, we see $g_iac^{-1}g_j^{-1} \in \omega(\mathfrak{m})\mathfrak{c}_lU$, so $\mathfrak{c}_l^{-1}\omega(\mathfrak{m})^{-1}g_i \in Ug_jG$. Next we prove the converse. We assume that $\mathfrak{c}_l^{-1}\omega(\mathfrak{m})^{-1}g_i \in Ug_jG$ for some $\mathfrak{m}|\mathfrak{d}$ and l. Then $g_i = \omega(\mathfrak{m})\mathfrak{c}_lug_ja$ for some $u \in U$ and $a \in G$. Then we have

$$R_i = g_i^{-1}Rg_i = a^{-1}g_j^{-1}u^{-1}\mathfrak{c}_l^{-1}\omega(\mathfrak{m})^{-1}R\,\omega(\mathfrak{m})\mathfrak{c}_lug_ja.$$

We have $\omega(m)^{-1}R\omega(m) = R$ since conjugation is defined locally. Since $\mathfrak{c}_l1_n$ is in the center of $M_n(B_A)$ and $u^{-1}Ru = R$ by definition of U, we have $a^{-1}R_ja = R_i$, hence we have proved (1). Now if $\omega(\mathfrak{m})^{-1}g_i \in Ug_jG$ for some $\mathfrak{m}|\mathfrak{d}$, then since $\omega(\mathfrak{m})U = U\omega(\mathfrak{m})$ by definition of $\omega(\mathfrak{m})$, we have $g_i \in \omega(\mathfrak{m})Ug_jG = U\omega(\mathfrak{m})g_jG$, hence $\omega(\mathfrak{m})g_j \in Ug_iG$. Since $\omega(\mathfrak{m})^2 \in F_A1_n$ and we assumed that the class number of F_A is one, we see that $\omega(\mathfrak{m})^2 = u_0c$ for some $u_0 \in F_\infty \prod_v \mathfrak{o}_v^\times$ and $c \in F^\times$. We have $\omega(\mathfrak{m}) = \omega(\mathfrak{m})^{-1}u_0c$ and we have $\omega(\mathfrak{m})^{-1}g_j \in u_0^{-1}Ug_iGc^{-1} = Ug_iG$. $\square$

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

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

Then for any $z \in G_A$ and $UzU = \bigcup_{i=1}^d z_iU$, the double coset acts on $f(g) \in \mathfrak{M}_0(U)$ by

$$([UzU]f)(g) = \sum_{i=1}^d f(z_i^{-1}g) \qquad (g \in G_A).$$

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 $R(\mathfrak{m}\mathfrak{c}_l^2)$ for $\mathfrak{m}|\mathfrak{d}$ and $\mathfrak{c}_l$ for $1 \leq l \leq h_0$ by

$$R(\mathfrak{m}\mathfrak{c}_l^2) = U\omega(\mathfrak{m})\mathfrak{c}_l U.$$

(Here we write $\mathfrak{c}_l^2$ in $R(*)$ just because $\mathfrak{c}_l^2 \in F_A^\times$ gives the multiplicator of the similitude $\mathfrak{c}_l 1_n$ and fits the notation $\mathfrak{m}$.) If we denote by t the number of prime divisors of $\mathfrak{d}$, then there are $2^t h_0$ such operators. Since $\omega_v R_v = R_v \omega_v$, we have $\omega_v R_v^\times = R_v^\times \omega_v$ and $\omega_v U_v = U_v \omega_v$. Also $\mathfrak{c}_l 1_n$ is in the center of G_A. So it is clear that $U\omega(m)\mathfrak{c}_l U = \omega(m)\mathfrak{c}_l U$. So these operators are obviously commutative. By definition, this acts on $\mathfrak{M}_0(U)$ by

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

By definition, we have $R(\mathfrak{m}\mathfrak{c}_l^2)f_i = f_j$ for the unique j such that $\omega(\mathfrak{m})^{-1}\mathfrak{c}_l^{-1}g_i \in Ug_jG$. So $R(\mathfrak{m}\mathfrak{c}_l^2)$ 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 $c \in F^\times$ and this acts trivially on $\mathfrak{M}_0(U)$, so the definition of $R(\mathfrak{m}\mathfrak{c}_l^2)$ depends only on $\mathfrak{m}$ and the class of $\mathfrak{c}_l$. We have $(U\omega(\mathfrak{m})\mathfrak{c}_l U)^2 = Um\mathfrak{c}_l^2$ for some $m \in F_A^\times$ 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 $R(\mathfrak{m}\mathfrak{c}_l^2)$ for all $\mathfrak{m}$ and $\mathfrak{c}_l$ is a finite abelian group. As a whole, the action of the semi-group spanned by $R(\mathfrak{m}\mathfrak{c}_l^2)$ on $\mathfrak{M}_0(U)$ is regarded as an action of a finite abelian group Γ of order $2^t h_0$.

Now we review an easy general theory of group actions. Let Γ 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 Γ. We denote by ρ the linear representation on the formal sum $\oplus_{x\in X}\mathbb{C}x$ associated to the action of Γ on the set X.

Lemma 3.4. *The number T of transitive orbits of X by Γ is given by*

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

Proof. Let $X = \bigcup_{i=1}^T X_i$ be the decomposition into the disjoint union of transitive orbits of Γ. Then Γ acts on X_i transitively. Fix $x_i \in X_i$ for each i and denote by Γ_i the stablizer of x_i in Γ. Then we have $|X_i| = |\Gamma/\Gamma_i|$. The stablizer of any other point $\gamma x_i \in X_i$ for $\gamma \in \Gamma$ is $\gamma\Gamma_i\gamma^{-1}$, but since Γ is abelian, this is equal to Γ_i. So Γ_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 ρ_i the linear representation of Γ 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 $\rho = \sum_{i=1}^T \rho_i$, we have

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

Hence we prove the lemma. □

Now we come back to the G-type number.

Proposition 3.5. *We have $R_i \cong_G R_j$ if and only if f_i and f_j are in the same orbit of the action of the semi-group spanned by $\{R(\mathfrak{m}\mathfrak{c}_l^2); \mathfrak{m}|\mathfrak{d}, 1 \le l \le h_0\}$.*

Proof. This claim is obvious from Proposition 3.3. □

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

$$T = \sum_{l=1}^{h_0} \sum_{\mathfrak{m}|\mathfrak{d}} \frac{Tr(R(\mathfrak{m}\mathfrak{c}_l^2))}{2^t h_0},$$

where 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 is important for a geometric interpretation. 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 $J = 1_n$. Then $g^\sigma = g^* = {}^t\overline{g}$ and $n(g) > 0$ for $g \in G$. For a left $\mathfrak{O}$-lattice L, we define $U = U(L)$ as before. For $G_A = \cup_{i=1}^{h} Ug_iG$ with $g_1 = 1$, we may assume that $n(g_i) = 1$ since the class number of $\mathbb{Q}$ is one and we have $n(G_A) = n(U)n(G)$. The set of lattices $L_i = Lg_i$ $(1 \le i \le h)$ is a complete set of representatives of the classes in $\mathcal{L}(L)$. We assume $n \ge 2$. Then by the strong approximation theorem on $GL_n(B)$, we can show easily that any left $\mathfrak{O}$-lattice L may be written as $L = \mathfrak{O}^n h$ for some $h \in GL_n(B)$. 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 $u \in GL_n(O)$ and $0 < m \in \mathbb{Q}^\times$ such that $uH_1u^* = mH_2$.

Lemma 3.7. *Assume that $n \ge 2$. By the above mapping, the set of G equivalence classes of left 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 $h_i \in GL_n(B)$ such that $L_i = \mathfrak{O}^n h_i$ $(1 \le i \le h)$. So we have $L_i = Lg_i = O^n h_1 g_i$. Then we have $uh_i = h_1 g_i$ for some $u \in G_\infty \prod_p GL_n(\mathfrak{O}_p)$, and $uh_ih_i^*u^* = h_1h_1^*$. This means that the reduced norms of $h_ih_i^*$ and $h_1h_1^*$ are the same. Denote 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) $\omega(m)^{-1}g_i \in Ug_jG$.
(2) *There exists $\alpha \in M_n(\mathfrak{O})$ such that $\alpha M_n(\mathfrak{O}) = M_n(\mathfrak{O})\alpha$ and $\alpha h_j h_j^* \alpha^* = mh_ih_i^*$.*

Proof. Assume (1). We have $\omega(m)^{-1}g_i = ug_ja$ for some $u \in U$, $a \in G$, and $g_i = \omega(m)ug_ja$. Since all the p-adic components of $\omega(m)$ are in R_p, we have $L\omega(m) \subset L$. Hence

$$L_i = Lg_i = L\omega(m)ug_ja \subset Lg_ja = L_ja.$$

Since $L_i = \mathfrak{O}^n h_i$ and $L_j = \mathfrak{O}^n h_j$, we have $\mathfrak{O}^n h_i \subset \mathfrak{O}^n h_j a$. Hence if we put $\alpha = h_i a^{-1} h_j^{-1}$ then $\mathfrak{O}^n \alpha \subset \mathfrak{O}^n$, so $\alpha \in M_n(\mathfrak{O})$ and $\alpha h_j h_j^* \alpha^* = n(a)^{-1} h_i h_i^*$. Since we assumed $n(g_i) = n(g_j) = 1$, we have $n(a)n(u) = n(\omega(m)^{-1})$. Since $n(u) \in \mathbb{R}_+^\times \prod_p \mathbb{Z}_p^\times$, $n(\omega(m)) \in m\mathbb{R}_+^\times \prod_p \mathbb{Z}_p^\times$, and $n(a) \in \mathbb{Q}_+^\times$, we have $n(a) = m^{-1}$, and $\alpha h_j h_j^* \alpha^* = m h_i h_i^*$. By definition of a, we have $a^{-1} = g_i^{-1}\omega(m)ug_j$, so

$$a^{-1}R_j = g_i^{-1}\omega(m)ug_j(g_j^{-1}Rg_j) = g_i^{-1}\omega(m)uRg_j = g_i^{-1}R\omega(m)ug_j = g_i^{-1}Rg_ia^{-1} = R_ia^{-1}.$$

Since we have $R_k = h_k^{-1}M_n(\mathfrak{O})h_k$ for any k, we have $a^{-1}h_j^{-1}M_n(\mathfrak{O})h_j = h_i^{-1}M_n(\mathfrak{O})h_ia^{-1}$, and $h_ia^{-1}h_j^{-1}M_n(\mathfrak{O}) = M_n(\mathfrak{O})h_ia^{-1}h_j^{-1}$. Since $\alpha = h_ia^{-1}h_j^{-1}$ by definition, we see that $\alpha M_n(\mathfrak{O})$ is a two-sided ideal. Hence we have (2). Now assume (2) and define a by $a^{-1} = h_i^{-1}\alpha h_j$. Then $a \in G$ and $n(a^{-1}) = m$. By $\alpha M_n(\mathfrak{O}) = M_n(\mathfrak{O})\alpha$, $n(g_ia^{-1}g_j^{-1}) = m$, and Lemma 3.1, we have $g_ia^{-1}g_j^{-1} = \omega(m)u$ with $u \in U$. So $\omega(m)^{-1}g_i = ug_ja \in Ug_jG$. 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 $\omega(m)^{-1}g_iG \notin Ug_jG$. But $\omega(m)^{-1}g_i \in G_A = \bigcup_{j=1}^h Ug_jG$, so we have $\omega(m)^{-1}g_i \in Ug_iG$ for all $m|D$. If we assume that $D = p$ is a prime, then $R_i \cong_G R_j$ if and only if $\omega(m)^{-1}g_i \in Ug_jG$ 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 $\omega(p)^{-1}g_i \in Ug_jG$. If $R_i \cong_G R_j$ only for $j = i$, then $\omega(p)^{-1}g_i \in Ug_iG$.*

Proof. If there exist j and k such that $j \neq i$ and $k \neq i$, then $g_i \notin Ug_jG$ and $g_i \notin Ug_kG$, and if $R_i \cong_G R_j \cong_G R_k$ besides, then by Proposition 3.3, we have $\omega(p)^{-1}g_i \in Ug_jG$ and $\omega(p)^{-1}g_i \in Ug_kG$, hence $Ug_jG = Ug_kG$ so $j = k$. If there exist no $j \neq i$ such that $R_i \cong_G R_j$, then we have $\omega(p)^{-1}g_i \notin Ug_jG$ for any $j \neq i$. This means that $\omega(p)^{-1}g_i \in Ug_iG$. □

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 $\mathbb{F}_p$

4.1. Polarizations on superspecial abelian varieties. Let A be an abelian variety and A^t the dual of A. For an effective divisor D of A, we define an isogeny ϕ_D from A to A^t by

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

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 λ from A to A^t is a polarization if there exists an effective divisor D such that $\lambda = \phi_D$. We say that a polarization λ is a principal polarization if λ is an isomorphism. Two polarized abelian varieties (A_1, λ_1) and (A_2, λ_2) are said to be isomorphic if there exists an isomorphism $\phi : A_1 \to A_2$ such that $\lambda_1 = \phi^t\lambda_2\phi$, where ϕ^t is the dual map from A_2^t to A_1^t associated with ϕ.

Let p be a prime. An elliptic curve E over a field of characteristic p such that $\mathrm{End}(E)$ is a maximal order of a definite quaternion algebra B with discriminant p is called supersingular. There exists a supersingular elliptic curve defined over $\mathbb{F}_p$ such that $\mathrm{End}(E)$ contains an element π with $\pi^2 = -p \cdot id_E$. We fix such an E once and for all. Then we can regard π as the Frobenius endomorphism of E and every element of 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 $O = \mathrm{End}(E)$. Then we have identifications $\mathrm{End}(E^n) = M_n(O)$ and $Aut(E^n) = M_n(O)^\times = GL_n(O)$. For any $\phi \in \mathrm{End}(E^n)$, the Rosati involution is defined by $\phi_X^{-1}\phi^t\phi_X$. Then this is equal to ϕ^* under the identification of $\mathrm{End}(E^n)$ with $M_n(O)$. In particular, if we put $H_\lambda = \phi_X^{-1}\lambda$ for a polarization λ, then $H_\lambda^* = H_\lambda$ and H_λ is a positive definite quaternion hermitian matrix in $M_n(O)$. It is easy to show that two polarized abelian varieties (E^n, λ_1) and (E^n, λ_2) are isomorphic if and only if there exists an $\alpha \in GL_n(O)$ such that $\alpha H_{\lambda_1}\alpha^* = H_{\lambda_2}$.

Any polarization λ of E^n is defined over $\mathbb{F}_{p^2}$ since ϕ_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, λ_1) and (E^n, λ_2) are isomorphic, then they are isomorphic over $\mathbb{F}_{p^2}$ since any element of $Aut(E^n)$ is defined over $\mathbb{F}_{p^2}$. Now we denote by σ 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, λ) has a model defined over $\mathbb{F}_p$ if and only if (E^n, λ) and (E^n, λ^σ) are isomorphic.*

Proof. Assume that there is a model (A, η) of (E^n, λ) defined over $\mathbb{F}_p$. We write an isomorphism $(A, \eta) \to (E^n, \lambda)$ by ψ. Here ψ is defined over the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. Anyway, for any element $\tau \in Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, 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 ψ gives an isomorphism $(E^n, \lambda) \cong (E^n, \lambda^\sigma)$, then $\psi \in Aut(E^n)$ is defined over $\mathbb{F}_{p^2}$ and $\psi^\sigma\psi$ is an automorphism of (E^n, λ) since $\lambda^{\sigma^2} = \lambda$. Since $\psi^\sigma\psi$ fixes a polarization (corresponding to a positive definite lattice), it is well-known that this is of finite order. So $(\psi^\sigma\psi)^r = (\psi\psi^\sigma)^r = 1$ for some positive integer r, where 1 means the identity map of E^n. Now we regard σ as a generator of the Galois group $Gal(\mathbb{F}_{p^{2r}}/\mathbb{F}_p)$. Since ψ is defined over $\mathbb{F}_{p^2}$, we have $\psi^{\sigma^2} = \psi$ and $(\psi^\sigma\psi)^{\sigma^{2i}} = \psi^\sigma\psi$. So if we put $f_1 = 1$, $f_\sigma = \psi$, and $f_{\sigma^i} = \psi^{\sigma^{i-1}}\psi^{\sigma^{i-2}}\cdots\psi$ for $1 \le i \le 2r-1$, then we have

$$f_{\sigma^i}^{\sigma^j} f_{\sigma^j} = \psi^{\sigma^{i+j-1}}\cdots\psi^{\sigma^j}\psi^{\sigma^{j-1}}\cdots\psi = f_{\sigma^{i+j}}.$$

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

$$\psi^{\sigma^{i+j-1-2r}}\cdots\psi^\sigma\psi,$$

since we have

$$\psi^{\sigma^{i+j-1}}\cdots\psi^{i+j-2r} = (\psi^\sigma\psi)^{\sigma^{i+j-2}}(\psi^\sigma\psi)^{\sigma^{i+j-4}}\cdots = ((\psi^\sigma\psi)^r)^{\sigma^\delta} = 1,$$

where $\delta = 0$ or 1 according as $i + j$ is even or odd. So we have $f_{\sigma^{i+j-2r}} = f_{\sigma^{i+j}}$ and the set of maps $\{f_{\sigma^i}; 0 \le i \le 2r - 1\}$ satisfies the descent condition for $Gal(\mathbb{F}_{p^{2r}}/\mathbb{F}_p)$ (See [15]). So we have a model over $\mathbb{F}_p$. $\square$

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

Proof. Let F be the Frobenius endomorphism of E^n over $\mathbb{F}_p$ and set $F = \pi 1_n$ where π is a prime element of O over p with $\pi^2 = -p$. Let F_1 be the Frobenius map of $(E^n)^t$ over $\mathbb{F}_p$. (Actually it is the same as F if we identify $(E^n)^t$ with E^n.) For a polarization λ of E^n, we have $\lambda^\sigma F = F_1\lambda$ by definition. In particular, since ϕ_X is defined over $\mathbb{F}_p$, we have $\phi_X F = F_1\phi_X$. So we have $(\phi_X^{-1}\lambda^\sigma)F = F(\phi_X^{-1}\lambda)$. Now assume that (E^n, λ^σ) and (E^n, λ) are isomorphic. This means that there exists an automorphism ϕ of E^n such that $\lambda^\sigma = \phi^t\lambda\phi$. So we have $\phi_X^{-1}\lambda^\sigma = \phi_X^{-1}\phi^t\phi_X\phi_X^{-1}\lambda\phi$. We have $\phi_X^{-1}\phi^t\phi_X = \phi^*$, identifying $\mathrm{End}(E^n)$ with $M_n(O)$ and writing $g^* = {}^t\overline{g}$ 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 $F^*F = p1_n$, we have $pH_\lambda = \alpha^* H_\lambda \alpha$ 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 $pH_\lambda = \alpha^* H_\lambda \alpha$ 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 $bF^r M_n(O)$ with positive rational number b and some non-negative integer r. So we have $\alpha = bF^r\epsilon$ for some $\epsilon \in GL_n(O) = M_n(O)^\times$. By taking the reduced norm of the both sides of $pH_\lambda = \alpha^* H_\lambda \alpha$, we see that the reduced norm $N(\alpha)$ of α is p^n. Since $N(F) = p^n$ and $N(\epsilon) = 1$, we see that $p^n = b^{2n}p^{nr}$, so $b = p^{n(1-r)/2}$. Since $F^2 = -p$, this is equal to $\pm F^{n(1-r)}$, and $\alpha = \phi F^s$ for some $\phi \in GL_n(O)$. Here comparing the reduced norm, we have $s = 1$ and this ϕ gives an isomorphism of (E^n, λ) to (E^n, λ^σ). $\square$

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

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

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 $G_A = \bigcup_i Ug_iG$. The isomorphism classes of $\mu \in \mathcal{P}(\lambda)$ correspond bijectively to the set $\{g_i\}$, so assume that μ corresponds to g_i. Write $H_\mu = \phi_X^{-1}\mu$ as before. The condition that $\alpha H_\mu \alpha^* = pH_\mu$ for some $\alpha \in M_n(O)$ with $\alpha M_n(O) = M_n(O)\alpha$ is equivalent to the condition that $\omega(p)g_i \in Ug_iG$ by Proposition 3.8. The number of isomorphism classes of such μ is equal to $Tr(R(p))$ by Lemma 3.9. Since $T(\lambda) = (Tr(R(p)) + Tr(R(1)))/2 = (Tr(R(p)) + H(\lambda))/2$, we prove the assertion. $\square$

We note that even if (E^n, λ) has a model over $\mathbb{F}_p$, it is not necessarily true that E^n has a polarization equivalent to λ defined over $\mathbb{F}_p$. We give such an example below. If a polarization λ of E^n is defined over $\mathbb{F}_p$, this means that $F(\phi_X^{-1}\lambda) = (\phi_X^{-1}\lambda)F$, so the quaternion hermitian matrix associated with λ should be realized as a matrix which commutes with π. 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 π, then any quaternion hermitian matrix associated with a lattice in $\mathcal{L}_{npr}$ is given by

$$H_1 = m\begin{pmatrix} pt & \pi r \\ \overline{\pi r} & ps \end{pmatrix}$$

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 π, 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 $a, b \in \mathbb{Z}$, $a \equiv b \bmod 2$. Here $N(r) = (a^2 + 3b^2)/4$ but we should have $N(r) \equiv -1 \bmod 3$ by the above relation. This means that $a^2 \equiv -1 \bmod 3$ 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

$$H = \begin{pmatrix} 3 & \pi(1+\beta) \\ -\pi(1+\beta) & 3 \end{pmatrix},$$

$$\alpha = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix} = \begin{pmatrix} \beta\pi & 0 \\ 0 & \pi \end{pmatrix},$$

then H corresponds with a lattice in $\mathcal{L}_{npr}$, and we have $\alpha H \alpha^* = 3H$ and $\alpha M_2(O) = M_2(O)\alpha$. 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 $\mathcal{A}_{n,1}$ the moduli of principally polarized abelian varieties and by $\mathcal{S}_{n,1}$ the locus of principally polarized supersingular abelian varieties in $\mathcal{A}_{n,1}$. 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 $\mathcal{S}_{n,1}$ corresponds bijectively with equivalence classes of polarizations of E^n be-*

longing to $\mathcal{L}_{pr}$ *if* n *is odd, and to* $\mathcal{L}_{npr}$ *if* n *is even, respectively.*
(2) *The locus* $\mathcal{S}_{n,1}$ *is defined over* $\mathbb{F}_p$. *Each irreducible component of* $\mathcal{S}_{n,1}$ *is defined over* $\mathbb{F}_{p^2}$. *The irreducible component corresponding to the polarization* λ *in the sense of* (1) *has a model defined over* $\mathbb{F}_p$ *if and only if* (E^n, λ) *has a model over* $\mathbb{F}_p$.

For any genus $\mathcal{L}$ of quaternion hermitian lattices, we denote by $H(\mathcal{L})$ and $T(\mathcal{L})$ the class number and the type number of $\mathcal{L}$ 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* $\mathcal{S}_{n,1}$ *which have models over* $\mathbb{F}_p$ *is equal to* $2T(\mathcal{L}_{pr}) - H(\mathcal{L}_{pr})$ *when* n *is odd and to* $2T(\mathcal{L}_{npr}) - H(\mathcal{L}_{npr})$ *when* n *is even. In particular, there always exists an irreducible component of* $\mathcal{S}_{n,1}$ *defined over* $\mathbb{F}_p$.

Proof. Except for the last claim, the assertion has been already proved. It is obvious that $2T(\mathcal{L}_{pr}) - H(\mathcal{L}_{pr}) > 0$ 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. □

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

References

[1] M. Deuring: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

[2] M. Deuring: *Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl*, Jber. Deutsch. Math. Verein. **54**, (1950). 24–41.

[3] M. Eichler: *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151 (1956).

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

[5] K. Hashimoto and T. Ibukiyama: *On class numbers of positive definite binary quaternion hermitian forms* (I), J. Fac. Sci. Univ. Tokyo, Sec. IA Math. **27** (1980), 549–601; (II) **28** (1981), 695–699 (1982), (III) **30** (1983), 393–401.

[6] T. Ibukiyama: *Quinary lattices and binary quaternion hermitian lattices*, to appear in Tohoku Math. J.

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

[8] T. Ibukiyama and T. Katsura: *On the field of definition of superspecial polarized abelian varieties and type numbers*, Compositio Math. **91** (1994), 37–46.

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

[10] K.Z. Li and F. Oort: Moduli of supersingular abelian varieties, Lecture Notes in Mathematics, **1680**. Springer-Verlag, Berlin, 1998.

[11] F. Oort: *Newton polygon strata in the moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999), 417–440, Progr. Math. **195**, Birkhäuser, Basel, 2001.

[12] M. Peters: *Ternäre quadratische Formen und Quaternionenalgebra*, Acta Arith. **15**, (1968/69), 329–365.

[13] A.K. Pizer: *Type numbers of Eichler orders*, J. Reine Angew. Math. **264** (1973), 76–102.

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

[15] A. Weil: *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524.

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