On some algebraic properties of CM-types of CM-fields and their reflexes

Ryoko Oishi-Tomiyasu

High Energy Accelerator Research Organization, 1-1, Oho, Tsukuba, Ibaraki, 305-0801, Japan

A R T I C L E   I N F O

A B S T R A C T

Text. The purpose of this paper is to show that the reflex fields of a given CM-field K are equipped with a certain combinatorial structure that has not been exploited yet.

The first theorem is on the abelian extension generated by the moduli and the b-torsion points of abelian varieties of CM-type, for any natural number b. It is a generalization of the result by Wei on the abelian extension obtained by the moduli and all the torsion points. The second theorem gives a character identity of the Artin L-function of a CM-field K and the reflex fields of K. The character identity pointed out by Shimura (1977) in [10] follows from this.

The third theorem states that some Pfister form is isomorphic to the orthogonal sum of $Tr_{K^*(\Phi)/\mathbb{Q}}(\bar{a}a)$ defined on the reflex fields $\bigoplus_{\Phi \in \Lambda} K^*(\Phi)$. This result suggests that the theory of complex multiplication on abelian varieties has a relationship with the multiplicative forms in higher dimension.

Video. For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=IIwksVYV5YE.

© 2010 Elsevier Inc. All rights reserved.

0. Introduction

The moduli of abelian varieties of a CM-type and their torsion points generate an abelian extension, not of the field of complex multiplication, but of a reflex field of the field. This is the theory of Shimura and Taniyama, which determines the Galois group of the abelian extension as the kernel of the half norm map between the idele groups (*cf.* [12, Main Theorem 1, 2]).

After that, in order to give a more direct description of the Galois group, Shimura [9] and Ovseevich [5] investigated into the abelian extension generated by the class-field of the maximal totally real subfield of the CM-field K and complex multiplication. There is also the work by Kubota on the

E-mail address: ryoko.oishi@kek.jp.

abelian extension generated by one CM-type of K [3]. On the other hand, Wei proved a theorem on the abelian extension generated only by complex multiplication [13]. Our first theorem (2.1) is a generalization of the theorem by Wei, which deals the abelian extension generated by the moduli and the b-torsions for a natural number b. The proof uses a combinatorial property of the reflex fields (Corollary 1.2).

In Section 3, a set of CM-fields $K(I)$ including K is proposed as a dual set of the reflex fields of K. A character identity holds between these two sets (Theorem 3.1). The character identity mentioned in [10] is obtained from this. The set of $K(I)$ consists of only conjugate fields of K over $\mathbb{Q}$, if the degree of K is 2, 4 or 8.

The third theorem (4.1) states the relation between reflex fields and some Pfister form. Let K_0 be the maximal totally real field of a given CM-field K. Then, $K = K_0(\sqrt{-d})$ for some totally positive element $d \in K_0$. Using the embeddings $\varphi_1, \ldots, \varphi_N : K_0 \hookrightarrow \mathbb{C}$, the Pfister form $q := \langle 1, \varphi_1(d) \rangle \otimes \cdots \otimes \langle 1, \varphi_N(d) \rangle$ is defined over the Galois closure of K_0 over $\mathbb{Q}$. The third theorem states that q is isomorphic to the orthogonal sum of $2^{-N} Tr_{K^*(\Phi)/\mathbb{Q}}(\bar{a}a)$ defined on the reflex fields $K^*(\Phi)$.

In the case of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$, the Pfister form $\langle 1, d \rangle$ equals the quadratic form on $\mathbb{Q}(\sqrt{-d})$ defined by the norm $N_{\mathbb{Q}(\sqrt{-d})/\mathbb{Q}}$. Theorem 4.1 is a generalization of this to higher dimension.

Some basic notations and definitions are given in Section 1. Each following section depends on the content of Section 1.

1. Some algebraic properties of CM-fields and their reflex fields

In this section, several results on the reflex fields and their Galois groups are shown. They are used to prove the theorems in the remaining sections.

1.1. Basic notations

Here, recall the definitions of CM-types, their dual CM-types; let K be a CM field and K_0 be its maximal totally real field. Their Galois closures are denoted by K^c and K_0^c respectively. We denote the Galois groups:

$$G := \mathrm{Gal}(K^c/\mathbb{Q}), \qquad G_0 := \mathrm{Gal}(K_0^c/\mathbb{Q}),$$

$$H := \mathrm{Gal}(K^c/K), \qquad H_0 := \mathrm{Gal}(K^c/K_0), \qquad C := \mathrm{Gal}(K^c/K_0^c),$$

where $\mathbb{Q}$ is the rational number field. There is an exact sequence:

$$1 \longrightarrow C \longrightarrow G \longrightarrow G_0 \longrightarrow 1.$$

Since K^c is also a CM-field, the complex conjugation ι is a central element of G. The pair (K, Φ) is called a CM-type of K, when Φ is a set of the embeddings of $K \hookrightarrow \mathbb{C}$ over $\mathbb{Q}$ such that Φ and $\iota\Phi$ are disjoint, and every embedding is contained in $\Phi \cup \iota\Phi$. Therefore, Φ and $\Phi \cup \iota\Phi$ correspond one-to-one to the left cosets G/H_0, G/H respectively.

For a CM-type (K, Φ) and a set $S_\Phi := \bigcup_{\varphi \in \Phi} \varphi H$, define a subgroup $H^*(\Phi)$ of G by

$$H^*(\Phi) := \{\sigma \in \mathrm{Gal}(K^c/\mathbb{Q}) : \sigma S_\Phi = S_\Phi\}. \qquad (1)$$

Then, $\iota \notin H^*(\Phi)$, and $H^*(\Phi)S_\Phi = S_\Phi$. Hence, $S_\Phi = H^*(\Phi)\psi_1 \cup \cdots \cup H^*(\Phi)\psi_M$, which is a disjoint union of right cosets. Let $K^*(\Phi)$ be the fixed subfield of K^c by $H^*(\Phi)$, then, $K^*(\Phi)$ is a CM-field. If we set $\Phi^* := \{\psi_1^{-1}|_{K^*(\Phi)}, \ldots, \psi_M^{-1}|_{K^*(\Phi)}\}$, $(K^*(\Phi), \Phi^*)$ is also a CM-type. $(K^*(\Phi), \Phi^*)$ is called the dual CM-type of (K, Φ), and $K^*(\Phi)$ is called the reflex field of (K, Φ).

1.2. On the structure of the Galois groups of CM-fields and their reflex fields

In this section, we define a 1-cocycle map and an embedding $\mathrm{Gal}(K^c/\mathbb{Q}) \hookrightarrow \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0$ to see the structure of the Galois group of the reflex fields. The results in this section are already described in [2] in a similar fashion. Here, we reformulate the descriptions in [2] to clarify the relation between the structure and the action of G on the CM-types, for the proofs of the following theorems.

Let H_0 act on $\mathbb{Z}_2$ trivially. The induced module $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ can be regarded as a set of maps $\mathrm{Map}(G/H_0, \mathbb{Z}_2)$, on which G acts by $\sigma(f)(\tau H_0) = f(\sigma^{-1}\tau H_0)$. Since K_0^c is the composite field of all the conjugate fields of K_0 over $\mathbb{Q}$, $C = \bigcap_{\tau \in G} \tau H_0 \tau^{-1}$. Hence, the actions of C on G/H_0 and $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ are trivial. Therefore, $G_0 = G/C$ also acts on G/H_0 and $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$.

As an abelian group, we have $C \cong (\mathbb{Z}_2)^m$ for some integer m. In fact, since $K = K_0(\sqrt{-d})$ for some totally positive $d \in K_0$, K^c equals $K_0^c(\sqrt{-\varphi_1(d)}, \ldots, \sqrt{-\varphi_N(d)})$, where $\varphi_1, \ldots, \varphi_N$ are the embeddings of $K_0 \hookrightarrow \mathbb{C}$ over $\mathbb{Q}$.

The following lemma shows that when G acts on C by conjugation $\tau \cdot a = \tau a \tau^{-1}$ for $\tau \in G$ and $a \in C$, C can be embedded into $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ as a G-module.

Lemma 1.1. *Using a totally positive d such that $K = K_0(\sqrt{-d})$, define a map $r : C \to \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ by*

$$r(a)(\varphi_i H_0) = \begin{cases} 0 & \text{if } a(\sqrt{-\varphi_i(d)}) = \sqrt{-\varphi_i(d)}, \\ 1 & \text{otherwise.} \end{cases} \tag{2}$$

Then, r does not depend on the choice of d, and it is an injective G-homomorphism.

Proof. It is clear that r does not depend on the choice of d. Furthermore, it is an injective homomorphism of additive groups, because $K^c = K_0^c(\sqrt{-\varphi_1(d)}, \ldots, \sqrt{-\varphi_N(d)})$. For any $\tau \in G$, if we put $(-1)^{n_i} = \tau^{-1}(\sqrt{-\varphi_i(d)})/\sqrt{-\tau^{-1}\varphi_i(d)}$, then

$$\tau a \tau^{-1}\left(\sqrt{-\varphi_i(d)}\right) = (-1)^{n_i} \tau a\left(\sqrt{-\tau^{-1}\varphi_i(d)}\right)$$

$$= (-1)^{n_i + r(a)(\tau^{-1}\varphi_i H_0)} \tau\left(\sqrt{-\tau^{-1}\varphi_i(d)}\right)$$

$$= (-1)^{r(a)(\tau^{-1}\varphi_i H_0)} \sqrt{-\varphi_i(d)}.$$

So, $(\tau \cdot r)(a)(\varphi_i(d)) := r(a)(\tau^{-1}\varphi_i H_0) = r(\tau a \tau^{-1})(\varphi_i H_0)$. Hence, r is a G-homomorphism. □

The embedding r given in Lemma 1.1 can be extended to a 1-cocycle map $G \to \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$.

Definition 1. For a CM-type (K, Φ) with $\Phi = \{\varphi_1, \ldots, \varphi_N\}$, define a map $r_\Phi : G \to \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ to be

$$r_\Phi(\tau)(\varphi_i H_0) := \begin{cases} 0 & \text{if } \tau^{-1}\varphi_i \in \Phi, \\ 1 & \text{otherwise.} \end{cases} \tag{3}$$

Proposition 1.1. *The map r_Φ is a 1-cocycle that equals r on C. The cohomology class $[r_\Phi]$ in $H^1(G_0, \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2))$ is determined independently from the choice of the CM-type (K, Φ). Moreover, $(K, \Phi) \mapsto r_\Phi$ gives a map from the CM-types of K onto the cohomology class $[r_\Phi]$. For any two CM-types (K, Φ) and (K, Φ'), $r_\Phi = r_{\Phi'}$ if and only if $\Phi' = \Phi$ or $\iota\Phi$.*

Proof. For $a \in C$, $a\varphi_i H = \varphi_i H$ or $\iota\varphi_i H$, since $a\varphi_i H_0 = \varphi_i H_0$. Furthermore, $a\varphi_i H = \varphi_i H$ if and only if a fixes $\sqrt{-\varphi_i(d)}$, since $K_0^c \cdot \varphi_i(K) = K_0^c(\sqrt{-\varphi_i(d)})$. Hence, $r_\Phi|_C = r$.

For any $\tau_1, \tau_2 \in G$,

$$r_\Phi(\tau_1\tau_2)(\varphi_i H_0) = 0 \iff (\tau_1\tau_2)^{-1}\varphi_i \in \Phi$$

$$\iff r_\Phi(\tau_2)\big(\tau_1^{-1}\varphi_i H_0\big) = \begin{cases} 0 & \text{if } \tau_1^{-1}\varphi_i \in \Phi, \\ 1 & \text{if } \tau_1^{-1}\varphi_i \in \iota\Phi \end{cases}$$

$$\iff r_\Phi(\tau_2)\big(\tau_1^{-1}\varphi_i H_0\big) = \begin{cases} 0 & \text{if } r_\Phi(\tau_1)(\varphi_i H_0) = 0, \\ 1 & \text{if } r_\Phi(\tau_1)(\varphi_i H_0) = 1 \end{cases}$$

$$\iff r_\Phi(\tau_1)(\varphi_i H_0) + r_\Phi(\tau_2)\big(\tau_1^{-1}\varphi_i H_0\big) = 0$$

$$\iff \big(r_\Phi(\tau_1) + \tau_1 \cdot r_\Phi(\tau_2)\big)(\varphi_i H_0) = 0.$$

So r_Φ is a 1-cocycle. Next, we shall show the map $\Phi \mapsto r_\Phi$ is onto $[r_\Phi]$; using the CM-type Φ and $f \in \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$, any CM-types Φ' are represented by $\{\iota^{f(\varphi_1 H_0)}\varphi_1, \ldots, \iota^{f(\varphi_N H_0)}\varphi_N\}$. Then, $r_{\Phi'}(\tau) = r_\Phi(\tau) + \tau \cdot f - f$, which implies that

$$r_{\Phi'}(\tau) = r_\Phi(\tau) \text{ for all } \tau \in G \iff f \text{ equals 0 or 1 constantly.}$$

Hence, the last statement also holds. $\square$

Since $r_\Phi|_C = r$ and $G/C = G_0$, r_Φ induces a 1-cocycle of $H^1(G_0, \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)/r(C))$. There is the exact sequence of cohomology groups:

$$H^1(G_0, \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)/r(C)) \longrightarrow H^2(G_0, r(C)) \longrightarrow H^2(G_0, \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)).$$

Lemma 1.2. *Let* $[s]$ *be the image of* $[r_\Phi]$ *by* $H^1(G_0, \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)/r(C)) \to H^2(G_0, r(C))$. *Then,* $[s] \in H^2(G_0, r(C))$ *corresponds to the exact sequence*: $1 \to C \to G \to G_0 \to 1$.

Proof. For $\sigma \in G_0$, fix a pre-image of $G \to G_0$, and denote it by $\hat{\sigma}$. Then, $[s]$ in $H^2(G_0, r(C))$ is given by
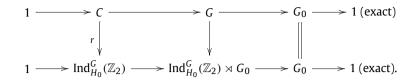
$$x(\sigma, \tau) = r_\Phi(\hat{\sigma}) - r_\Phi(\widehat{\sigma\tau}) + \hat{\sigma} \cdot r_\Phi(\hat{\tau}).$$

Let $a := \hat{\sigma}\hat{\tau}\widehat{\sigma\tau}^{-1}$, then $a \in C$, and we have

$$x(\sigma, \tau) = r_\Phi(\hat{\sigma}) - r_\Phi\big(a^{-1}\hat{\sigma}\hat{\tau}\big) + \hat{\sigma} \cdot r_\Phi(\hat{\tau})$$

$$= r_\Phi(\hat{\sigma}) - \big(-r_\Phi(a) + r_\Phi(\hat{\sigma}) + \hat{\sigma} \cdot r_\Phi(\hat{\tau})\big) + \hat{\sigma} \cdot r_\Phi(\hat{\tau})$$

$$= r(a) = r\big(\hat{\sigma}\hat{\tau}\widehat{\sigma\tau}^{-1}\big).$$

This means $x(\sigma, \tau)$ coincides with the exact sequence. $\square$

By Lemma 1.2, $[s]$ belongs to the kernel of $H^2(G_0, r(C)) \to H^2(G_0, \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2))$ in the exact sequence. Therefore, there is a commutative diagram of two exact sequences:

$$1 \longrightarrow C \longrightarrow G \longrightarrow G_0 \longrightarrow 1 \text{ (exact)}$$

$$1 \longrightarrow \operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2) \longrightarrow \operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2) \rtimes G_0 \longrightarrow G_0 \longrightarrow 1 \text{ (exact)}.$$

The group operation of the semi-direct group $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2) \rtimes G_0$ is defined by

$$(f, \sigma)(f', \sigma') = (f + \sigma \cdot f', \sigma\sigma'). \tag{4}$$

The projection on $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2)$ of the middle vertical homomorphism equals r_Φ for a CM-type (K, Φ). The corollary follows from the discussion above.

Corollary 1.1. *Let (K, Φ) be a CM-type of K. Let ρ be the canonical epimorphism $G \twoheadrightarrow G_0$. Then, the map $\rho_\Phi : G \to \operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2) \rtimes G_0$ given by $\tau \mapsto (r_\Phi(\tau), \rho(\tau))$ is an injective homomorphism.*

By the definition of r_Φ, we have for any $\tau \in G$,

$$\tau \in H^*(\Phi) \quad \Longleftrightarrow \quad r_\Phi(\tau) \text{ equals } 0 \text{ constantly.} \tag{5}$$

Therefore, using the embedding r_Φ and ρ defined in Corollary 1.1, the subgroups of G can be restated as follows:

$$C = \{\tau \in G : \rho(\tau) = id\}, \tag{6}$$

$$H^*(\Phi) = \{\tau \in G : r_\Phi(\tau) = 0 \text{ for any } \tau\}. \tag{7}$$

In particular, by the injectivity of r on C, $C \cap H^*(\Phi) = \{id\}$ for any (K, Φ). On the other hand, $C \subset H$. Hence, $H^*(\Phi)$ can equal H only when $C = \{id, \iota\}$.

1.3. The conjugacy among CM-types

It is said that two CM-types (K, Φ) and (K, Φ') are conjugate if and only if $\Phi' = \tau\Phi$ for some $\tau \in G$. Corresponding to the action of G on the CM-types of K, a new action of G on $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2)$ is introduced in this section.

Fix a CM-type $\Phi_0 := \{\varphi_1, \ldots, \varphi_N\}$ of K. Then, for $f \in \operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2)$, a CM-type Φ_f is given by

$$\Phi_f := \{\iota^{f(\varphi_1 H_0)}\varphi_1, \ldots, \iota^{f(\varphi_N H_0)}\varphi_N\}. \tag{8}$$

The set of the CM-types of K has a one-to-one correspondence with $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2)$ by $f \mapsto \Phi_f$.

Regarding G as a subgroup of $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2) \rtimes G_0$ by the embedding ρ_{Φ_0} defined in Corollary 1.1, let G act on $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2) \rtimes G_0$ by multiplication from the left-hand side. This yields a new action of G on $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2)$ given by $\tau * f := r_{\Phi_0}(\tau) + \tau \cdot f$. This action depends on Φ_0. We shall show the lemma:

Lemma 1.3. *The identification between all the CM-types and $\operatorname{Ind}_{H_0}^{G}(\mathbb{Z}_2)$ given by $f \mapsto \Phi_f$ coincides with their G-structure, i.e., $\tau\Phi_f = \Phi_{\tau*f}$ for $\tau \in G$. Hence, $H^*(\Phi_f)$ coincides with the stabilizer of f, i.e., $\tau * f = f \iff \tau \in H^*(\Phi_f)$. In addition, two CM-types $(K, \Phi_f), (K, \Phi_{f'})$ are conjugate if and only if there exists $\tau \in G$ such that $f' = \tau * f$.*

Proof. If we show $\tau \Phi_f = \Phi_{\tau * f}$ for any $\tau \in G$, it is easily seen that the remaining statements hold. For $\tau \in G$ and $\varphi \in \Phi_0$, we have

$$r_{\Phi_f}(\tau)(\varphi H_0) = 0 \quad \Longleftrightarrow \quad \iota^{f(\varphi H_0)} \varphi \in \tau \Phi_f.$$

Hence,

$$\tau \Phi_f = \left\{ \iota^{(r_{\Phi_f}(\tau) + f)(\varphi_1 H_0)} \varphi_1, \ldots, \iota^{(r_{\Phi_f}(\tau) + f)(\varphi_N H_N)} \varphi_N \right\}.$$

Since $r_{\Phi_f}(\tau) = r_{\Phi_0}(\tau) + \tau \cdot f - f$,

$$r_{\Phi_f}(\tau) + f = r_{\Phi_0}(\tau) + \tau \cdot f = \tau * f. \tag{9}$$

Therefore, $\tau \Phi_f = \Phi_{\tau * f}$. We proved the lemma. $\square$

The set of the CM-types of K is divided into the orbits by the action of G. Each orbit corresponds to a conjugacy class of the CM-types of K. The fixed subgroup of Φ is $H^*(\Phi)$. Therefore, the degree of the reflex field $K^*(\Phi)$ equals the cardinality of the orbit. From this, the following lemma follows which is also described in [11]:

Lemma 1.4. *Let Λ be a system of representatives for the conjugacy classes of the CM-types of K. Then, the sum of the degrees of the reflex fields $\{K^*(\Phi)\}_{\Phi \in \Lambda}$ equals 2^N.*

It is used in the proof of Theorem 2.1.

1.4. On a combinatorial property of half norm maps

For a CM-type (K, Φ), a half norm map $K^\times \to K^*(\Phi)^\times$ is defined by $a \mapsto \prod_{\varphi \in \Phi} \varphi(a)$. In general, for a given G-module M, a half norm map $N_\Phi : M^H \to M^{H^*(\Phi)}$ is defined by $a \mapsto \sum_{\varphi \in \Phi} \varphi(a)$, where M^H, $M^{H^*(\Phi)}$ are the subsets of M consisting of the fixed elements by H, $H^*(\Phi)$ respectively. Then, $N_\Phi(a + \iota a)$ equals the norm map $N_{G/H} : a \mapsto \sum_{\sigma \in G/H} \sigma(a)$.

The following proposition shows a characteristic property of half norm maps.

Proposition 1.2. *Let M be a G-module on which ι acts as -1. Denote the dual CM-type of (K, Φ) by $(K^*(\Phi), \Phi^*)$. Then, two maps are defined using the half norm maps:*

$$(N_\Phi)_{\Phi \in \Lambda} : M^H \to \bigoplus_{\Phi \in \Lambda} M^{H^*(\Phi)},$$

$$a \mapsto \left(\sum_{\varphi \in \Phi} \varphi(a) \right)_{\Phi \in \Lambda}, \tag{10}$$

$$\sum_{\Phi \in \Lambda} N_{\Phi^*} : \bigoplus_{\Phi \in \Lambda} M^{H^*(\Phi)} \to M^H,$$

$$(b_\Phi)_{\varphi \in \Phi} \mapsto \sum_{\Phi \in \Lambda} \sum_{\psi \in \Phi^*} \psi(b_\Phi), \tag{11}$$

where Λ ranges all the conjugacy classes of the CM-types of K. Then, the composition of the following maps equals the multiplication by 2^{N-1} on M^H, where $2N$ is the degree of K over $\mathbb{Q}$:

$$M^H \xrightarrow{(N_\Phi)_{\Phi \in \Lambda}} \bigoplus_{\Phi \in \Lambda} M^{H^*(\Phi)} \xrightarrow{\sum_{\Phi \in \Lambda} N_{\Phi^*}} M^H.$$

This lemma is generalized to Proposition 4.1 in Section 4. Hence, we omit the proof here.

Let $\mathbb{I}_L$ be the idele group of a number field L. For a natural number b, define an open subgroup $U_L((b)) \subset \mathbb{I}_L$ by

$$U_L((b)) := (L_\infty)_+^\times \times \prod_{\mathfrak{p} | (b)} (1 + b\mathcal{O}_\mathfrak{p}) \times \prod_{\mathfrak{p} \nmid (b)} \mathcal{O}_\mathfrak{p}^\times, \tag{12}$$

where $\mathcal{O}_\mathfrak{p}$ is the ring of integers of the local field $L_\mathfrak{p}$, and $(L_\infty)_+^\times$ is the connected open subgroup of 1 in $(L \otimes_\mathbb{Q} \mathbb{R})^\times$.

From Proposition 1.2, the corollary follows immediately. It will be used in the proof of Theorem 2.1.

Corollary 1.2. *The composition of the following two maps equals the multiplication by 2^{N-1} on $\mathbb{I}_K / U_K((b)) \mathbb{I}_{K_0}$:*

$$\mathbb{I}_K / \mathbb{I}_{K_0} U_K((b)) \xrightarrow{(N_\Phi)_{\Phi \in \Lambda}} \bigoplus_{\Phi \in \Lambda} \mathbb{I}_{K^*(\Phi)} / \mathbb{I}_{K_0^*(\Phi)} U_{K^*(\Phi)}((b)) \xrightarrow{\sum_{\Phi \in \Lambda} N_{\Phi^*}} \mathbb{I}_K / \mathbb{I}_{K_0} U_K((b)).$$

In particular, the elements that belong to the kernel of $(N_\Phi)_{\Phi \in \Lambda}$, has an order dividing 2^{N-1}.

Remark 1. When K is a Galois extension over $\mathbb{Q}$, all the reflex fields are contained in K. Therefore, in this case, the elements that belong to the kernel of $(N_\Phi)_{\Phi \in \Lambda}$ have an order dividing at most 2.

2. The abelian extension by complex multiplication

In this section, we shall prove the theorem on the abelian extension generated by complex multiplication.

First, we give some definitions; for a number field L, let $C_L := \mathbb{I}_L / L^\times$, and denote the connected component of the identity in C_L by D_L. By the main theorem of class field theory, there is the canonical isomorphism $\phi_L : C_L / D_L \xrightarrow{\cong} \text{Gal}(L^{ab}/L)$.

For a number field L and an integral ideal $\mathfrak{a}$ of L, define an open subgroup $U_L(\mathfrak{a}) \subset \mathbb{I}_L$ associated with $\mathfrak{a}$ by

$$U_L(\mathfrak{a}) := (L_\infty)_+^\times \times \prod_{\mathfrak{p} | \mathfrak{a}} (1 + \mathfrak{a}\mathcal{O}_\mathfrak{p}) \times \prod_{\mathfrak{p} \nmid \mathfrak{a}} \mathcal{O}_\mathfrak{p}^\times, \tag{13}$$

where $\mathcal{O}_\mathfrak{p}$ is the ring of integers of the local field $L_\mathfrak{p}$, and $(L_\infty)_+^\times$ is the connected open subgroup in $(L \otimes_\mathbb{Q} \mathbb{R})^\times$. Let $L_\mathfrak{a}$ be the ray class field of L modulo $\mathfrak{a}$, then, ϕ_L gives an isomorphism $\mathbb{I}_L / L^\times U_L(\mathfrak{a}) \to \text{Gal}(L_\mathfrak{a}/L)$.

Let A be a polarized abelian variety of CM-type $(K^*(\Phi), \Phi^*)$. For a CM-type (K, Φ) and the dual CM-type $(K^*(\Phi), \Phi^*)$, we have a half norm map $K^\times \to K^*(\Phi)^\times$ defined by $a \mapsto \prod_{\varphi \in \Phi} \varphi(a)$. It also induces a half norm map $N_\Phi : C_K \to C_{K^*(\Phi)}$. By the theory of complex multiplication, the abelian extension over K generated by the moduli and $\mathfrak{a}$-torsions of A corresponds to the kernel of the map induced by N_Φ:

$$C_K \to \mathbb{I}_{K^*(\Phi)}/\big(K^*(\Phi)\big)^\times U_{K^*(\Phi)}(\mathfrak{a}),$$

$$\mathfrak{a} \mapsto \prod_{\varphi \in \Phi} \varphi(\mathfrak{a}).$$

In the sequel, let b be a natural number, and $\mathcal{M}_{K,b}$ be the subfield of K^{ab} obtained by adjoining to K, the moduli and the b-torsion points of all the polarized abelian varieties of a CM-type with the reflex field contained in K. By the theory of complex multiplication, $\mathcal{M}_{K,b}$ is contained in $K_{(b)}$, the ray class field of K modulo b. Furthermore, we have the theorem:

Theorem 2.1. *Let $\{K^*(\Phi)\}_{\Phi \in \Lambda}$ be the set of the reflex fields of all the CM-types of K, and 2^{N_0} be the maximum 2-power dividing the degrees of all the reflex fields of K. (Hence, $1 \leqslant N_0 \leqslant N$.)*
Then, there exists a subgroup $H(b)$ of $\mathrm{Gal}(K_{(b)}/\mathcal{M}_{K,b})$ satisfying the following:

(i) $2^{N-1}\mathrm{Gal}(K_{(b)}/\mathcal{M}_{K,b}) \subset H(b) \subset \mathrm{Gal}(K_{(b)}/\mathcal{M}_{K,b})$,
(ii) $2^{N_0}H(b) \subset \mathrm{Ver}(\mathrm{Gal}(K_{0,(b)}/K_0 \cdot \mathbb{Q}_{(b)})) \subset H(b)$,

where $K_{0,(b)}$ is the ray class field of K_0 modulo b, and Ver is the Verlagerung map $\mathrm{Gal}(K_{0,(b)}/K_0) \to \mathrm{Gal}(K_{(b)}/K)$.
In particular, for any odd prime p, the p-component of $\mathrm{Gal}(K_{(b)}/\mathcal{M}_{K,b})$ is isomorphic to that of $\mathrm{Ver}(\mathrm{Gal}(K_{0,(b)}/K_0 \cdot \mathbb{Q}_{(b)}))$.

Proof. For an ideal (b), take $U_K((b))$ as (13). Let $V_K((b))$ be the image of $U_K((b))$ in C_K. By class field theory, there is a commutative diagram:

$$
\begin{array}{ccc}
C_{K_0}/V_{K_0}((b)) & \xrightarrow[\cong]{\phi_{K_0}} & \mathrm{Gal}(K_{0,(b)}/K_0) \\
\downarrow & & \downarrow{\mathrm{Ver}} \\
C_K/V_K((b)) & \xrightarrow[\cong]{\phi_K} & \mathrm{Gal}(K_{(b)}/K).
\end{array}
$$

To prove the theorem, we use the commutative diagram of two exact sequences:

$$
\begin{array}{ccccccccc}
0 & \to & C_K^{\langle \iota \rangle}/V_K((b))^{\langle \iota \rangle} & \to & C_K/V_K((b)) & \to & C_K/C_K^{\langle \iota \rangle}V_K((b)) & \to & 0 \\
 & & \downarrow & & \downarrow{(N_\Phi)_{\Phi \in \Lambda}} & & \downarrow & & \\
0 & \to & \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}^{\langle \iota \rangle}/V_{K^*(\Phi)}((b))^{\langle \iota \rangle} & \to & \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}/V_{K^*(\Phi)}((b)) & \to & \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}/C_{K^*(\Phi)}^{\langle \iota \rangle}V_{K^*(\Phi)}((b)) & \to & 0
\end{array}
$$

where the superscript $\langle \iota \rangle$ means the subgroup fixed by the complex conjugation ι. We denote each kernel of the vertical maps by

$$N_{1,b} := \mathrm{Ker}\left(C_K^{\langle \iota \rangle}/V_K((b))^{\langle \iota \rangle} \to \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}^{\langle \iota \rangle}/V_{K^*(\Phi)}((b))^{\langle \iota \rangle} \right),$$

$$N_{2,b} := \mathrm{Ker}\left(C_K/V_K((b)) \to \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}/V_{K^*(\Phi)}((b)) \right),$$

$$N_{3,b} := \mathrm{Ker}\left(C_K/C_K^{\langle \iota \rangle}V_K((b)) \to \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}/C_{K^*(\Phi)}^{\langle \iota \rangle}V_{K^*(\Phi)}((b)) \right).$$

By the snake lemma, we have the exact sequence:

$$0 \longrightarrow N_{1,b} \longrightarrow N_{2,b} \longrightarrow N_{3,b}.$$

Furthermore, by the theory of complex multiplication, $\mathrm{Gal}(K_{(b)}/\mathcal{M}_{K,b})$ equals $\phi_K(N_{2,b})$. On the other hand, by Corollary 1.2, all the elements of $N_{3,b}$ have an order dividing 2^{N-1}.

Let $H(b) := \phi_K(N_{1,b})$. Then, it is clear that the assertion (i) of the theorem holds.

Next, we show (ii); since $H^1(K^\times) = 0$, we have $C_K^{\langle \iota \rangle} = \mathbb{I}_K^{\langle \iota \rangle}/(K^\times)^{\langle \iota \rangle} = C_{K_0}$. Hence, there is a commutative diagram:

$$
\begin{array}{ccccc}
C_{K_0}/V_{K_0}((b)) & \longrightarrow & C_K^{\langle \iota \rangle}/V_K((b))^{\langle \iota \rangle} & \longrightarrow & 0 \,(\text{exact}) \\
{\scriptstyle N_{K_0/\mathbb{Q}}} \downarrow & & {\scriptstyle (N_\Phi)_{\Phi \in \Lambda}} \downarrow & & \\
C_{\mathbb{Q}}/V_{\mathbb{Q}}((b)) & \longrightarrow & \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}^{\langle \iota \rangle}/V_{K^*(\Phi)}((b))^{\langle \iota \rangle}. & &
\end{array}
$$

Let $J_{K_0,b}$ be the kernel of the left vertical map in the diagram, and $J_{K,b}$ be the image of $J_{K_0,b}$ in $C_K/V_K((b))$. Then, $\phi_K(J_{K,b}) = \mathrm{Ver}(\mathrm{Gal}(K_{0,(b)}/K_0 \cdot \mathbb{Q}_{(b)}))$. Since $J_{K,b} \subset N_{1,b}$, (ii) is proved if $2^{N_0} N_{1,b} \subset J_{K,b}$.

Let n_Φ be the degree of $K^*(\Phi)$. If $a \in C_{\mathbb{Q}}$ belongs to $V_{K^*(\Phi)}((b))^{\langle \iota \rangle}$ for all CM-type (K, Φ), then, $a^{n_\Phi} = N_{G/H^*(\Phi)}(a) \in V_{\mathbb{Q}}((b))$. Hence, $a^m \in V_{\mathbb{Q}}((b))$, where m is the greatest common divisor of n_Φ ($\Phi \in \Lambda$). Since the sum of n_Φ ($\Phi \in \Lambda$) equals 2^N by Lemma 1.4, m equals 2^{N_0} in the statement of the theorem. $\quad\square$

In [13], Wei proved the following theorem on the abelian extension obtained from all the CM-types whose reflex is contained in K. In the remaining part of this section, we prove the theorem by Wei, using Theorem 2.1 and basic results of algebraic number theory.

Theorem 2.2 *(Wei). Let $\mathcal{M}_K$ be the subfield of K^{ab} obtained by adjoining to K, the moduli and the torsion points of all the polarized abelian varieties of a CM-type with the reflex field contained in K. The subgroup corresponding to $\mathcal{M}_K$ equals the image of $\mathrm{Gal}(K_0^{ab}/K_0 \cdot \mathbb{Q}^{ab})$ in $\mathrm{Gal}(K^{ab}/K)$ under the Verlagerung map.*

Proof. Denote each kernel of the maps induced by $(N_\Phi)_{\Phi \in \Lambda}$, by

$$N_1 := \mathrm{Ker}\left(C_K^{\langle \iota \rangle}/D_K^{\langle \iota \rangle} \to \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}^{\langle \iota \rangle}/D_{K^*(\Phi)}^{\langle \iota \rangle} \right),$$

$$N_2 := \mathrm{Ker}\left(C_K/D_K \to \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}/D_{K^*(\Phi)} \right),$$

$$N_3 := \mathrm{Ker}\left(C_K/C_K^{\langle \iota \rangle} D_K \to \bigoplus_{\Phi \in \Lambda} C_{K^*(\Phi)}/C_{K^*(\Phi)}^{\langle \iota \rangle} D_{K^*(\Phi)} \right).$$

These groups equal $\varprojlim_b N_{1,b}$, $\varprojlim_b N_{2,b}$, $\varprojlim_b N_{3,b}$ respectively, the inverse limits of the groups defined in the proof of Theorem 2.1. In addition, we define

$$J_{K_0} := \mathrm{Ker}(N_{K_0/\mathbb{Q}} : C_{K_0}/D_{K_0} \to C_{\mathbb{Q}}/D_{\mathbb{Q}}),$$

and denote the image in C_K/D_K by J_K. J_{K_0} is also the inverse limit of $J_{K_0,b}$ in the proof of Theorem 2.1. Then, Theorem 2.2 follows from Lemmas 2.1 and 2.2. $\square$

Lemma 2.1. $N_1 = J_K$.

Lemma 2.2. $N_3 = \{0\}$.

Lemma 2.4 is used to prove them. First, we prove Lemma 2.4 using Lemma 2.3.

Let E_L be the group of units of a number field L. For any subgroup $U \subset \mathbb{I}_L$, $\overline{U}$ means its topological closure. The image of $L_\infty^\times \subset \mathbb{I}_L$ in C_L is denoted by $\widetilde{L}_\infty^\times$.

Lemma 2.3. *Let L be a number field. If $a \in \mathbb{I}_L$ satisfies $a^m \in \overline{L^\times}$ (resp. $a^m \in \overline{L_\infty^\times L^\times}$) for a natural number m, there exists $d \in \overline{L^\times}$ such that $a^m = d^m$ (resp. $a_\mathfrak{p}^m = d_\mathfrak{p}^m$ at any finite primes $\mathfrak{p}$). In particular, if $a \in C_L$ satisfies $a^m \in D_L$ (resp. $a \in \widetilde{L}_\infty^\times D_L$), then, a corresponds to $b \in \mathbb{I}_L$ such that all the components b_ν at any primes (resp. any finite primes) ν are m-th roots of unity.*

Proof. Let $U_m \subset \mathbb{I}_L$ be an open subgroup such that $E_L \cap U_m \subset E_L^m$. Take $c \in L^\times$ such that $a^m \equiv c$ mod U_m. For any open subgroup $U' \subset U_m$, there exists a unit ϵ of L such that $a^m \equiv \epsilon^m c$ mod U'. Therefore, for any finite prime $\mathfrak{p}$ of L, $c^{1/m} \in L_\mathfrak{p}$. This means that the primes of $L(\zeta_m)$ except for a finite number, are totally split over $L(c^{1/m}, \zeta_m)$, where ζ_m is a primitive m-th root of unity. Hence, $c^{1/m}$ belongs to $L(\zeta_m)$. Then, $c^{1/m} \in L$, again since we have $c^{1/m} \in L_\mathfrak{p}$ for any finite prime $\mathfrak{p}$. Therefore, the first statement follows. (Suppose that $U_m, U' \supset L_\infty^\times$ for the case of $a^m \in \overline{L_\infty^\times L^\times}$.) The second statement follows immediately. $\square$

Lemma 2.4. *Let $L \subset M$ be number fields. If $a \in C_L$ satisfies $a \in D_M$ (resp. $a \in \widetilde{M}_\infty^\times D_M$) and $a^m \in D_L$ for a natural number m, then, $a \in D_L$ (resp. $a \in \widetilde{L}_\infty^\times D_L$).*

Proof. By Lemma 2.3, we may assume that the components of a at any primes are m-th roots of unity. Let U be an open subgroup in $\mathbb{I}_M$ such that no roots of unity of M are contained in it. Take a positive number l such that $E_M^l \subset U \cap E_M$. For any open subgroup $U' \subset U$ such that $U' \cap E_M \subset E_M^{ml}$, there exists $\epsilon \in E_M$ such that $a \equiv \epsilon$ mod U', because $a \in D_M$. Then, $\epsilon^m \in E_M^{ml}$, since $\epsilon^m \equiv a^m \equiv 1$ mod U'. Therefore, $\zeta\epsilon \in E_M^l$ for some root of unity $\zeta \in M$. In particular, $a \equiv \epsilon \equiv \zeta$ mod U. Since U is arbitrary, $a = \zeta$ for some root of unity ζ in L. Therefore, $a \in D_L$. The proof is similar for the case of $a \in \widetilde{M}_\infty^\times D_M$. $\square$

Proof of Lemma 2.1. Since $D_K^{\langle \iota \rangle} = (\widetilde{K_0})_\infty^\times D_{K_0}$, we have $C_K^{\langle \iota \rangle}/D_K^{\langle \iota \rangle} = C_{K_0}/(\widetilde{K_0})_\infty^\times D_{K_0}$. Therefore,

$$N_1 = \mathrm{Ker}\left(C_{K_0}/(\widetilde{K_0})_\infty^\times D_{K_0} \to \bigoplus_{\Phi \in \Lambda} C_{K_0^*(\Phi)}/\big(\widetilde{K_0^*(\Phi)}\big)_\infty^\times D_{K_0^*(\Phi)} \right).$$

This map is via the norm map $N_{K_0/\mathbb{Q}} : C_{K_0}/\widetilde{(K_0)}_\infty^\times D_{K_0} \to C_\mathbb{Q}/\widetilde{\mathbb{R}}^\times D_\mathbb{Q}$. Take an element $a \in C_\mathbb{Q}$ that belongs to $\widetilde{(K_0^*(\Phi))}_\infty^\times D_{K_0^*(\Phi)}$. Then, $a^2 \in D_{K_0^*(\Phi)}$. In addition, the canonical map $C_\mathbb{Q}/D_\mathbb{Q} \to C_{K_0^*(\Phi)}/D_{K_0^*(\Phi)}$ is injective, because both $K_0^*(\Phi)$ and $\mathbb{Q}$ are totally real fields [1]. Hence, $a^2 \in D_\mathbb{Q}$. Therefore, $a \in \widetilde{\mathbb{R}}^\times D_\mathbb{Q}$ by Lemma 2.4; the statement follows. $\square$

Proof of Lemma 2.2. Take $a \in C_K$ such that $N_\Phi(a) \in C_{K^*(\Phi)}^{\langle \iota \rangle} D_{K^*(\Phi)}$ for all the CM-types (K, Φ). It is enough if we can show $a \in C_K^{\langle \iota \rangle} D_K$, which is equivalent to $a^{1-\iota} \in D_K$. By Theorem 2.1, $a^{2^{N-1}} \in C_K^{\langle \iota \rangle} D_K$. Hence, $a^{2^{N-1}(1-\iota)} \in D_K$. By Lemma 2.4, there exists $b \in \mathbb{I}_K$ such that $b \equiv a^{1-\iota}$ mod D_K, and all the

components of b at the primes of K, are 2^{N-1}-th roots of unity. Moreover, $N_\Phi(b)$ is a root of unity of $K^*(\Phi)$ for any Φ, since $N_\Phi(b) \in D_{K^*(\Phi)}$. Hence, $b^{1-\iota} = b^2$ is a root of unity, and b is also a root of unity. Therefore, $a^{1-\iota} \in D_K$. □

3. A character identity

In this section, we give a proof of a character identity between the Artin L-functions of a CM-field K and the reflex of K.

For any group N_0 and a normal subgroup N such that $[N_0 : N] = 2$, we denote by $\chi_{N_0/N}$ the non-trivial character of N_0 induced by the canonical homomorphisms $N_0 \twoheadrightarrow N_0/N \overset{\cong}{\to} \{\pm 1\}$.

Proposition 3.1. Let K be a CM-field. Let $\mathbf{0}$ and $\mathbf{1}$ be the elements of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ that map any $\varphi_i H_0$ to 0 and 1 respectively. For a fixed CM-type (K, Φ_0), G can be regarded as a subgroup of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0$ by ρ_{Φ_0} defined in Corollary 1.1. Then, the equation holds:

$$\mathrm{Res}_G \, \mathrm{Ind}_{\langle \mathbf{1}\rangle \times G_0}^{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0} \left(\chi_{\langle \mathbf{1}\rangle \times G_0 / \{\mathbf{0}\} \times G_0} \right) = \sum_{\Phi \in \Lambda} \mathrm{Ind}_{H_0^*(\Phi)}^G \left(\chi_{H_0^*(\Phi)/H^*(\Phi)} \right), \tag{14}$$

where $\langle \mathbf{1}\rangle$ is the subgroup of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ generated by $\mathbf{1}$, and Λ is a system of representatives for the conjugacy classes of the CM-types of K.

Proof. We have

$$\mathrm{Res}_G \, \mathrm{Ind}_{\langle \mathbf{1}\rangle \times G_0}^{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0} \left(\chi_{\langle \mathbf{1}\rangle \times G_0 / \{\mathbf{0}\} \times G_0} \right) = \sum_{s \in G \backslash \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0 / \langle \mathbf{1}\rangle \times G_0} \mathrm{Ind}_{s(\langle \mathbf{1}\rangle \times G_0)s^{-1} \cap G}^G \left(\chi^s \right),$$

where χ^s is the character of $s(\langle \mathbf{1}\rangle \times G_0)s^{-1} \cap G$ such that $\chi^s(x) = \chi_{\langle \mathbf{1}\rangle \times G_0/\{\mathbf{0}\} \times G_0}(s^{-1}xs)$ for $x \in s(\langle \mathbf{1}\rangle \times G_0)s^{-1} \cap G$. Let $\{s_i\}$ be a system of representatives for $G \backslash \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0 / \langle \mathbf{1}\rangle \times G_0$. We can choose $\{s_i\}$ from $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \times \{id\}$. Let $s_i = (f_i, id)$, and $\Phi_{f_i} := \{\iota^{f_i(\varphi_1 H_0)}\varphi_1, \ldots, \iota^{f_i(\varphi_N H_0)}\varphi_N\}$ for a fixed CM-type $\Phi_0 := \{\varphi_1, \ldots, \varphi_N\}$. Then, by Lemma 1.3, $\{\Phi_{f_i}\}$ makes a system of representatives for the conjugacy class of the CM-types of K. Moreover, we have

$$s_i\left(\langle \mathbf{1}\rangle \times G_0\right)s_i^{-1} \cap G = \{\sigma \in G : \sigma * f_i = f_i \text{ or } f_i + \mathbf{1}\} = H_0^*(\Phi_{f_i}).$$

Hence, χ^{s_i} is the character induced by $H_0^*(\Phi_{f_i}) \twoheadrightarrow H_0^*(\Phi_{f_i})/H^*(\Phi_{f_i}) \overset{\cong}{\to} \{\pm 1\}$. By this, the statement follows. □

Let I be a subset of $\{\varphi_1 H_0, \ldots, \varphi_N H_0\}$. Then, the character of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ is given by $\chi_I(f) := (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0)}$. It is clear that $I \mapsto \chi_I$ gives a bijection from the subsets of $\{\varphi_1 H_0, \ldots, \varphi_N H_0\}$ to the characters of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$. For $f \in \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ and $s = (f', \sigma) \in \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0$, we define f^s such that $(f^s, id) = s^{-1} \cdot (f, id) \cdot s$, and $\chi_I^s(f) := \chi_I(f^s)$. Then, for $s = (f', \sigma)$,

$$\chi_I^s(f) = \chi_I\left(\sigma^{-1} \cdot f + \sigma^{-1} \cdot f' - f' \right)$$
$$= \chi_I\left(\sigma^{-1} \cdot f + \sigma^{-1} \cdot f' \right) - \chi_I\left(f' \right)$$
$$= \chi_{\sigma I}\left(f + f' \right) - \chi_I\left(f' \right), \tag{15}$$

where $\sigma I := \{\sigma\varphi_1 H_0, \ldots, \sigma\varphi_N H_0\}$. Hence, $\chi_I^s = \chi_I$ means $\chi_{\sigma I}(f + f') = \chi_I(f + f')$ for any f, therefore, $\sigma I = I$.

Let $H_{0,I} := \{\sigma \in G_0 \colon \sigma I = I\}$. Then, χ_I is extended to a character of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes H_{0,I}$ by

$$\chi_I((f, \sigma)) = \chi_I(f). \tag{16}$$

This character is denoted by $\widetilde{\chi_I}$.

For an irreducible representation π of $H_{0,I}$, let $\tilde{\pi}$ be the irreducible representation of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes H_{0,I}$ given by composing π with $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes H_{0,I} \twoheadrightarrow H_{0,I}$. We denote the representation $\mathrm{Ind}_{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes H_{0,I}}^{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0}(\widetilde{\chi_I} \otimes \tilde{\pi})$ by $\theta_{I,\pi}$ and the character of $\theta_{I,\pi}$ by $\chi_{I,\pi}$.

Proposition 3.2. *Let $|I|$ be the cardinality of I. Then,*

(a) $\theta_{I,\pi}$ *is irreducible.*
(b) *If $\theta_{I,\pi}$ and $\theta_{I',\pi'}$ are isomorphic, then $I' = \sigma I$ for some $\sigma \in G_0$, and π' is isomorphic to π.*
(c) *Every irreducible representation of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0$ is isomorphic to one of the $\theta_{I,\pi}$.*

Proof. See, *e.g.*, [8, Proposition 25]. □

For any odd number d, G_0 acts on $\{\varphi_1 H_0, \ldots, \varphi_N H_0\}$ by $\varphi_i H_0 \mapsto \sigma\varphi_i H_0$, which induces an action of G_0 on the set $\{I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\} \colon |I| = d\}$ for any natural number d. Let J_d be a system of representatives for the orbits, and $J_{odd} := \bigcup_{1 \leqslant d \leqslant N \colon \text{odd}} J_d$.

Lemma 3.1. *The following gives an irreducible decomposition*:

$$\mathrm{Ind}_{\langle \mathbf{1} \rangle \times G_0}^{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0}(\chi_{\langle \mathbf{1} \rangle \times G_0 / \{\mathbf{0}\} \times G_0}) = \sum_{I \in J_{odd}} \chi_{I,id}. \tag{17}$$

Proof. In the sequel, for any representation π, we denote the character of π by χ_π. From the above proposition, it suffices if the multiplicities of $\theta_{I,\pi}$ are computed. By the Frobenius reciprocity,

$$\left\langle \mathrm{Ind}_{\langle \mathbf{1} \rangle \times G_0}^{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0}(\chi_{\langle \mathbf{1} \rangle \times G_0 / \{\mathbf{0}\} \times G_0}), \chi_{I,\pi} \right\rangle_{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0}$$

$$= \left\langle \chi_{\langle \mathbf{1} \rangle \times G_0 / \{\mathbf{0}\} \times G_0}, \mathrm{Res}_{\langle \mathbf{1} \rangle \times G_0} \mathrm{Ind}_{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes H_{0,I}}^{\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0}(\widetilde{\chi_I} \otimes \chi_{\tilde{\pi}}) \right\rangle_{\langle \mathbf{1} \rangle \times G_0}$$

$$= \left\langle \chi_{\langle \mathbf{1} \rangle \times G_0 / \{\mathbf{0}\} \times G_0}, \mathrm{Ind}_{\langle \mathbf{1} \rangle \times H_{0,I}}^{\langle \mathbf{1} \rangle \times G_0}(\widetilde{\chi_I} \otimes \chi_{\tilde{\pi}}) \right\rangle_{\langle \mathbf{1} \rangle \times G_0}$$

$$= \left\langle \chi_{\langle \mathbf{1} \rangle \times H_{0,I} / \{\mathbf{0}\} \times H_{0,I}}, \widetilde{\chi_I} \otimes \chi_{\tilde{\pi}} \right\rangle_{\langle \mathbf{1} \rangle \times H_{0,I}}.$$

Moreover,

$$\left\langle \chi_{\langle \mathbf{1} \rangle \times H_{0,I} / \{\mathbf{0}\} \times H_{0,I}}, \widetilde{\chi_I} \otimes \chi_{\tilde{\pi}} \right\rangle_{\langle \mathbf{1} \rangle \times H_{0,I}}$$

$$= \left| \langle \mathbf{1} \rangle \times H_{0,I} \right|^{-1} \sum_{t \in \langle \mathbf{1} \rangle \times H_{0,I}} \chi_{\langle \mathbf{1} \rangle \times H_{0,I} / \{\mathbf{0}\} \times H_{0,I}}(t)(\widetilde{\chi_I} \otimes \chi_{\tilde{\pi}})(t^{-1})$$

$$= \frac{1}{2}|H_{0,I}|^{-1} \sum_{t \in \{\mathbf{0}\} \times H_{0,I}} (\widetilde{\chi_I} \otimes \chi_{\tilde{\pi}})(t^{-1})(1 - (\widetilde{\chi_I} \otimes \chi_{\tilde{\pi}})((\mathbf{1}, id)^{-1}))$$

$$= \frac{1 - \chi_I(\mathbf{1})}{2} |H_{0,I}|^{-1} \sum_{t \in \{\mathbf{0}\} \times H_{0,I}} \widetilde{\chi_I} \otimes \chi_{\bar{\pi}} \left(t^{-1} \right)$$

$$= \frac{1 - \chi_I(\mathbf{1})}{2} \langle \pi, id \rangle_{H_{0,I}}.$$

Therefore,

$$\left\langle \mathrm{Ind}^{\mathrm{Ind}^G_{H_0}(\mathbb{Z}_2) \rtimes G_0}_{\langle \mathbf{1} \rangle \times G_0} (\chi_{\langle \mathbf{1} \rangle \times G_0 / \{\mathbf{0}\} \times G_0}), \ \chi_{I,\pi} \right\rangle_{\mathrm{Ind}^G_{H_0}(\mathbb{Z}_2) \rtimes G_0}$$

$$= \begin{cases} 1 & \text{if } |I| \text{ is odd and } \pi \text{ is the trivial representation of } G_0, \\ 0 & \text{otherwise.} \end{cases}$$

We obtain the lemma. $\quad\square$

Let I be a subset of $\{\varphi_1 H_0, \ldots, \varphi_N H_0\}$ such that $|I|$ is odd. Define

$$H(I) := \left\{ \sigma \in G \colon \sum_{\varphi H_0 \in I} r_{\Phi}(\sigma)(\varphi H_0) = 0, \ \rho(\sigma) \in H_{0,I} \right\}. \tag{18}$$

The definition of $H(I)$ is independent of the choice of Φ. If $I = \{H_0\}$, then, $H(I) = H$. Moreover, for $H_0(I) := (\mathrm{Ind}^G_{H_0}(\mathbb{Z}_2) \rtimes H_{0,I}) \cap G$,

$$\mathrm{Res}_H(\chi_{I,id}) = \mathrm{Res}_G \, \mathrm{Ind}^{\mathrm{Ind}^G_{H_0}(\mathbb{Z}_2) \rtimes G_0}_{\mathrm{Ind}^G_{H_0}(\mathbb{Z}_2) \rtimes H_{0,I}} (\widetilde{\chi_I}) = \mathrm{Ind}^G_{H_0(I)}(\widetilde{\chi_I}), \tag{19}$$

since $|G \setminus (\mathrm{Ind}^G_{H_0}(\mathbb{Z}_2) \rtimes G_0)/(\mathrm{Ind}^G_{H_0}(\mathbb{Z}_2) \rtimes H_{0,I})| = 1$.

We denote the field corresponding to the subgroup $H_0(I)$ by $K_0(I)$. Since $\iota \in H_0(I)$, $K_0(I)$ is a totally real field. Let $K(I)$ be the quadratic extension of $K_0(I)$ corresponding to the kernel of the character $\widetilde{\chi_I}$. Since ι does not belong to the kernel, $K(I)$ is a CM-field. For $I = \{H_0\}$, $K(I) = K$.

We obtain the theorem from the above argument.

Theorem 3.1. *Let Λ be a system of representatives for the conjugacy classes of the CM-types of K. Then,*

$$\sum_{(K, \Phi) \in \Lambda} \mathrm{Ind}^G_{H_0^*(\Phi)}(\chi_{H_0^*(\Phi)/H^*(\Phi)}) = \sum_{I \in J_{odd}} \mathrm{Ind}^G_{H_0(I)}(\widetilde{\chi_I}). \tag{20}$$

Now, we can apply the character identity to obtain a relation formula of the Artin L-functions and relative invariants of a CM-field and its reflexes, as is done in [10].

For a field F, we denote the discriminant, the class number and the unit group of F by d_F, h_F and E_F respectively.

Corollary 3.1. *There is a relation formula of the Artin L-functions*:

$$\prod_{(K, \Phi) \in \Lambda} L(s, \chi_{H_0^*(\Phi)/H^*(\Phi)}) = \prod_{I \in J_{odd}} L(s, \widetilde{\chi_I}|_{H_0(I)}), \tag{21}$$

where Λ is a system of representatives for the conjugacy classes of the CM-types of K. Therefore,

$$\prod_{(K,\Phi)\in\Lambda}\left|\frac{d_{K^*(\Phi)}}{d_{K_0^*(\Phi)}}\right| = \prod_{I\in J_{odd}}\left|\frac{d_{K(I)}}{d_{K_0(I)}}\right|, \tag{22}$$

$$\prod_{(K,\Phi)\in\Lambda}\frac{h_{K^*(\Phi)}/h_{K_0^*(\Phi)}}{[E_{K^*(\Phi)} : E_{K_0^*(\Phi)}]} = \prod_{I\in J_{odd}}\frac{h_{K(I)}/h_{K_0(I)}}{[E_{K(I)} : E_{K_0(I)}]}. \tag{23}$$

Proof. The first equation follows from Theorem 3.1; in general, $L(s,\chi) = L(s, \mathrm{Ind}_H^G(\chi))$ holds for any character χ of a finite dimensional representation of H. We denote the number of the roots of unity in K, K_0 by w_K, w_{K_0}, and the regulator of K, K_0 by R_K, R_{K_0}. Then,

$$L(1, \chi_{K/K_0}) = \lim_{s\to 1}\frac{\zeta_K(s)}{\zeta_{K_0}(s)} = \left(\frac{(2\pi)^N h_K R_K}{w_K\sqrt{|d_K|}}\right)\left(\frac{2^N h_{K_0} R_{K_0}}{w_{K_0}\sqrt{|d_{K_0}|}}\right)^{-1}$$

$$= \pi^N\left|\frac{d_K}{d_{K_0}}\right|^{-\frac{1}{2}}\frac{h_K/h_{K_0}}{[E_K : E_{K_0}]}.$$

For a character χ of G, let $\mathfrak{f}(\chi)$ be the conductor of the character χ. Then,

$$(d_K) = \mathfrak{f}\big(\mathrm{Ind}_H^G(id_H)\big),$$

$$(d_{K_0}) = \mathfrak{f}\big(\mathrm{Ind}_{H_0}^G(id_{H_0})\big),$$

where id_H and id_{H_0} are the trivial representations of H and H_0 respectively (*cf.* [7, Chapter VI, Corollary 1 of Prop. 6]). Hence,

$$\left(\frac{d_K}{d_{K_0}}\right) = \mathfrak{f}\big(\mathrm{Ind}_H^G(id_H)\big)\mathfrak{f}\big(\mathrm{Ind}_{H_0}^G(id_{H_0})\big)^{-1} = \mathfrak{f}\big(\mathrm{Ind}_H^G(\chi_{H_0/H})\big).$$

Therefore, the corollary follows. $\square$

It is clear that $C \subset H(I)$. Therefore, $K(I)$ is different from any reflex fields of K at least when $C \neq \{id, \rho\}$, since $C \cap H^*(\Phi) = \{id\}$ by (6) and (7) in Section 1.2. By this, Example 1 is the only case when the set of $K(I)$ totally coincides with the set of the reflex fields of K, *i.e.*, the character identity is trivial.

Example 1. Suppose that $G = \langle\iota\rangle \times G_0$ and the degree N of K_0 is an odd number, *i.e.*, there is a section homomorphism $G_0 \hookrightarrow G$. Let Φ_0 be a CM-type of K such that $S_{\Phi_0} = \{id\} \times G_0$. For a subset $I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}$, define $f_I \in \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ by

$$f_I(\varphi H_0) := \begin{cases} 0, & \varphi H_0 \notin I, \\ 1, & \varphi H_0 \in I. \end{cases} \tag{24}$$

Then, for the fixed CM-type Φ_0, we have $(id, \sigma) * f_I = \sigma \cdot f_I = f_{\sigma I}$, and $(\iota, \sigma) * f_I = 1 + f_{\sigma I}$. Therefore, when the cardinality of I is odd, we have

$$H^*(\Phi_{f_I}) = \big\{(id, \sigma) \in \langle\iota\rangle \times G_0 : \sigma I = I\big\} = H(I).$$

Hence, $K(I)$ and $K^*(\Phi_{f_I})$ coincide. The set of $K(I)$ ($I \in J_{odd}$) has a one-to-one correspondence with the reflexes $K^*(\Phi_{f_I})$ of K.

Example 2. Let G be the dihedral group D_{2n} of degree $2n$. Then, G has two generators α, β such that $\alpha^{2n} = id$, $\beta^2 = id$, and $\beta\alpha\beta^{-1} = \alpha^{-1}$. Regard the central element α^n as the complex conjugation ι. Then, the fixed subfield K by $H := \{id, \beta\}$ is a CM-field and $\Phi_0 := \{id|_H, \alpha|_H, \ldots, \alpha^{n-1}|_H\}$ is a CM-type of K. We have $H^*(\Phi_0) = \{id, \alpha^{n-1}\beta\}$. When n is odd, it is the case of Example 1.

So, let n be even. In this case, K and $K^*(\Phi_0)$ are not conjugate. Nevertheless, as Shimura pointed out in [10],

$$\operatorname{Ind}_{H_0}^G(\chi_{H_0/H}) = \operatorname{Ind}_{H_0^*(\Phi_0)}^G(\chi_{H_0^*(\Phi_0)/H^*(\Phi_0)}). \tag{25}$$

In [2], this type of character identity is investigated for dihedral groups, responding to Shimura's suggestion. We shall show that Eq. (25) follows from Theorem 3.1; regard G_0 as a subgroup of the symmetry group S_n by the canonical action on $G/H_0 = \{H_0, \alpha H_0, \ldots, \alpha^{n-1} H_0\}$. A map $\rho_{\Phi_0} := (r_{\Phi_0}, \rho)$ is defined in Corollary 1.1. The image of α^i is given by

$$r_{\Phi_0}(\alpha^i) = (\underbrace{1, \ldots, 1}_{i}, \underbrace{0, \ldots, 0}_{n-i}), \qquad \rho(\alpha^i) = (1\, 2\, \ldots\, n)^i.$$

Similarly, the image of $\alpha^i\beta$ is given by

$$r_{\Phi_0}(\alpha^i\beta) = (\underbrace{0, \ldots, 0}_{i+1}, \underbrace{1, \ldots, 1}_{n-i-1}),$$

$$\rho(\alpha^i\beta) = \left(\left\lfloor\frac{n+i+1}{2}\right\rfloor\left\lceil\frac{n+i+3}{2}\right\rceil\right) \cdots (i+3\, n-1)(i+2\, n)(1\, i+1)(2\, i) \cdots \left(\left\lfloor\frac{i+1}{2}\right\rfloor\left\lceil\frac{i+3}{2}\right\rceil\right),$$

where $\lfloor * \rfloor$ and $\lceil * \rceil$ are the floor function and the ceiling function respectively.

Let k_0 be the maximum number such that $2^{k_0} \mid n$. For the CM-type Φ_0, if we define Φ_f as (8), $\sigma \in G$ is contained in $H^*(\Phi_f)$ if and only if $r_{\Phi_0}(\sigma) = \rho(\sigma) \cdot f - f$. Therefore, let $(i, 2n)$ be the greatest common divisor of i and $2n$, then,

$$\alpha^i \in H^*(\Phi) \text{ for some } \Phi \quad \Longleftrightarrow \quad \alpha^{(i,2n)} \in H^*(\Phi) \text{ for some } \Phi \quad \Longleftrightarrow \quad 2^{k_0+1} \mid i,$$

$$\alpha^i\beta \in H^*(\Phi) \text{ for some } \Phi \quad \Longleftrightarrow \quad i \text{ is odd.}$$

Similarly, for $I \subset \{H_0, \alpha H_0, \ldots, \alpha^{n-1} H_0\}$, $\sigma \in G$ is contained in $H(I)$ if and only if $\sigma I = I$ and $\sum_{\alpha^j H_0 \in I} r_{\Phi_0}(\sigma)(\alpha^j H_0) = 0$. Therefore, under the assumption that the cardinality of I is odd,

$$\alpha^i \in H(I) \quad \Longleftrightarrow \quad \alpha^{(i,2n)} \in H(I) \quad \Longleftrightarrow \quad 2^{k_0+1} \mid i \text{ and } \alpha^{(i,n)}I = I,$$

$$\alpha^i\beta \in H(I) \quad \Longleftrightarrow \quad i \text{ is even and } \alpha^i\beta I = I.$$

Hence, $H^*(\Phi)$ is conjugate to (i) $\langle\alpha^{2^{k_0+1}j}\rangle$, or (ii) $\langle\alpha^{2^{k_0+1}j}, \alpha^{n-1}\beta\rangle$ for some j such that $2^{k_0}j \mid n$. Similarly, $H(I)$ is conjugate to (iii) $\langle\alpha^{2^{k_0+1}j}\rangle$, or (iv) $\langle\alpha^{2^{k_0+1}j}, \beta\rangle$.

In the sequel, Φ_0 is replaced by the CM-type such that $\alpha^i|_H \in \Phi_0 \Longleftrightarrow i \equiv 0, \ldots, 2^{k_0} - 1 \mod 2^{k_0+1}$. For $I \subset \{H_0, \alpha H_0, \ldots, \alpha^{n-1} H_0\}$, define $f_I \in \operatorname{Ind}_{H_0}^G(\mathbb{Z}_2)$ as (24). Then, since we have $r_{\Phi_0}(\alpha^{2^{k_0+1}j}) = 0$ for any j, and $r_{\Phi_0}(\alpha^{n-1}\beta) = 0$,

$$\alpha^{2^{k_0+1}j} \in H^*(\Phi_{f_I}) \iff \alpha^{2^{k_0}j}I = I,$$

$$\alpha^{n-1}\beta \in H^*(\Phi_{f_I}) \iff \alpha^{n-1}\beta I = I.$$

For a natural number j such that $2^{k_0}j \mid n$, define

$$S_j := \left\{ I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\} : \alpha^{2^{k_0}j}I = I \text{ and } \alpha^{2^{k_0}j_0}I \neq I \text{ for any } j_0 \mid j \right\},$$

$$\tilde{S}_j := \left\{ I \in S_j : \alpha^{n-1}\beta I = I \right\},$$

$$T_j := \left\{ I \in S_j : |I| \text{ is odd} \right\},$$

$$\tilde{T}_j := \left\{ I \in S_j : |I| \text{ is odd, and } \beta I = I \right\}.$$

Let $s_j := |S_j|$, $\tilde{s}_j := |\tilde{S}_j|$, $t_j := |T_j|$, $\tilde{t}_j := |\tilde{T}_j|$. Using these variables, we can count the number of the orbits of G such that the stabilizer is conjugate to each subgroup. By Theorem 3.1,

$$\sum_{0 < j \mid 2^{-k_0}n} \frac{s_j - [G : \langle \alpha^{2^{k_0}j}, \alpha^{n-1}\beta \rangle]\tilde{s}_j}{[G : \langle \alpha^{2^{k_0+1}j} \rangle]} \mathrm{Ind}^G_{\langle \alpha^{2^{k_0}j} \rangle} \left(\chi_{\langle \alpha^{2^{k_0}j} \rangle / \langle \alpha^{2^{k_0+1}j} \rangle} \right)$$

$$+ \sum_{0 < j \mid 2^{-k_0}n} \frac{\tilde{s}_j}{[\langle \alpha^{2^{k_0}j}, \alpha^{n-1}\beta \rangle : \langle \alpha^{2^{k_0+1}j}, \alpha^{n-1}\beta \rangle]} \mathrm{Ind}^G_{\langle \alpha^{2^{k_0}j}, \alpha^{n-1}\beta \rangle} \left(\chi_{\langle \alpha^{2^{k_0}j}, \alpha^{n-1}\beta \rangle / \langle \alpha^{2^{k_0+1}j}, \alpha^{n-1}\beta \rangle} \right)$$

$$= \sum_{0 < j \mid 2^{-k_0}n} \frac{t_j - [G : \langle \alpha^{2^{k_0-1}j}, \beta \rangle]\tilde{t}_j}{[G : \langle \alpha^{2^{k_0}j} \rangle]} \mathrm{Ind}^G_{\langle \alpha^{2^{k_0}j} \rangle} \left(\chi_{\langle \alpha^{2^{k_0}j} \rangle / \langle \alpha^{2^{k_0+1}j} \rangle} \right)$$

$$+ \sum_{0 < j \mid 2^{-k_0}n} \frac{\tilde{t}_j}{[\langle \alpha^{2^{k_0-1}j}, \beta \rangle : \langle \alpha^{2^{k_0}j}, \beta \rangle]} \mathrm{Ind}^G_{\langle \alpha^{2^{k_0}j}, \beta \rangle} \left(\chi_{\langle \alpha^{2^{k_0}j}, \beta \rangle / \langle \alpha^{2^{k_0+1}j}, \beta \rangle} \right).$$

Since we have $\rho(\alpha) = (1\ 2\ \ldots\ n)$, $\rho(\beta) = (\frac{n}{2}\ \frac{n+4}{2}) \cdots (3\ n-1)(2\ n)$, and $\rho(\alpha^{n-1}\beta) = (1\ n)(2\ n-1) \cdots (\frac{n}{2}\ \frac{n+2}{2})$, the subsets can be restated;

$$S_j = \left\{ I \subset \{1, \ldots, n\} : 2^{k_0}j \text{ is the minimum periodicity of } I \right\},$$

$$\tilde{S}_j = \{ I \in S_j : i \in I \iff n - i + 1 \in I \},$$

$$T_j = \left\{ I \in S_j : \left| I \cap \{1, \ldots, 2^{k_0}j\} \right| \text{ is odd} \right\},$$

$$\tilde{T}_j = \left\{ I \in S_j : 1 \in I \iff \frac{n}{2} + 1 \notin I, \text{ and } i \in I \iff n - i + 2 \in I \left(2 \leqslant i \leqslant \frac{n}{2} \right) \right\}.$$

Hence, we have $s_j = 2t_j$, $\tilde{s}_j = \tilde{t}_j$. Therefore,

$$\sum_{0 < j \mid 2^{-k_0}n} \frac{\tilde{s}_j}{2} \mathrm{Ind}^G_{\langle \alpha^{2^{k_0}j}, \alpha^{n-1}\beta \rangle} \left(\chi_{\langle \alpha^{2^{k_0}j}, \alpha^{n-1}\beta \rangle / \langle \alpha^{2^{k_0+1}j}, \alpha^{n-1}\beta \rangle} \right)$$

$$= \sum_{0 < j \mid 2^{-k_0}n} \frac{\tilde{s}_j}{2} \mathrm{Ind}^G_{\langle \alpha^{2^{k_0}j}, \beta \rangle} \left(\chi_{\langle \alpha^{2^{k_0}j}, \beta \rangle / \langle \alpha^{2^{k_0+1}j}, \beta \rangle} \right).$$

By induction on j, we obtain (25).

4. Reflex fields and a Pfister form

In this section, we show Proposition 4.1, then, give a proof of the third theorem which states that some Pfister form is decomposed into quadratic forms defined on a set of reflex fields of K. Pfister forms are known as the only case of anisotropic multiplicative quadratic forms ([6], *cf.* [4]).

For a CM-type (K, Φ) and $I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}$ with odd cardinality, a CM-field $K(I)$ is introduced in Section 3. These CM-fields are also used for the proof of the third theorem. First, we give a definition of the CM-type $(K(I), \Phi(I))$; using $\rho_\Phi : G \hookrightarrow \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2) \rtimes G_0$ in Corollary 1.1, we defined the subgroups $H(I)$ and $H_0(I)$ of G by

$$H(I) := \left\{ \sigma \in G \colon \sum_{\varphi H_0 \in I} r_\Phi(\sigma)(\varphi H_0) = 0, \ \rho(\sigma)I = I \right\}, \tag{26}$$

$$H_0(I) := \left\{ \sigma \in G \colon \rho(\sigma)I = I \right\}. \tag{27}$$

Then, $H(I)$ and $H_0(I)$ are independent of the choice of the CM-type Φ, and $H_0(I) = H(I) \cup \iota H(I)$. A CM-field $K(I)$ is the fixed subfield by $H(I)$. Furthermore, if we set

$$S_{\Phi(I)} := \left\{ \sigma \in G \colon \sum_{\varphi H_0 \in I} r_\Phi(\sigma^{-1})(\varphi H_0) = 0 \right\}, \tag{28}$$

then, $H^*(\Phi)S_{\Phi(I)} = S_{\Phi(I)}$ and $S_{\Phi(I)}H(I) = S_{\Phi(I)}$. Denote the set of the embeddings $K(I) \hookrightarrow \mathbb{C}$ corresponding to the left cosets $S_{\Phi(I)}/H(I)$ by $\Phi(I)$, and the set of the embeddings $K^*(\Phi) \hookrightarrow \mathbb{C}$ given by the inverse of the right cosets $H^*(\Phi) \backslash S_{\Phi(I)}$ by $\Phi(I)^*$. $\Phi(I)$ and $\Phi(I)^*$ are CM-types of $K(I)$ and $K^*(\Phi)$ respectively. In addition, $(K(I), \Phi(I))$ contains the dual CM-type of $(K^*(\Phi), \Phi(I)^*)$, and $(K^*(\Phi), \Phi(I)^*)$ contains the dual of $(K(I), \Phi(I))$.

For $0 \leqslant d \leqslant N$, there is the canonical action of G on $\{I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\} \colon |I| = d\}$; let J_d be a system of representatives for the orbits, and $J_{odd} := \bigcup_{1 \leqslant d \leqslant N \colon odd} J_d$. Since the stabilizer of I is $\langle H(I), \iota \rangle$, there is the decomposition given by $H_0(I)\sigma \mapsto \sigma^{-1}I$:

$$\left\{ I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\} \colon |I| \text{ is odd} \right\} = \bigcup_{I \in J_{odd}} H_0(I) \backslash G. \tag{29}$$

On the other hand, for a fixed CM-type (K, Φ_0), a G-action on $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ is defined by $f \mapsto \sigma * f$ in Section 1.3. Since the stabilizer of f is $H^*(\Phi_f)$, there is the decomposition for each I, given by $\sigma H_0^*(\Phi_f) \mapsto \sigma * f$:

$$\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)/\langle \mathbf{1} \rangle = \bigcup_{\Phi_f \in \Lambda} G/H_0^*(\Phi_f), \tag{30}$$

where $\langle \mathbf{1} \rangle$ is the subgroup of $\mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ generated by $\mathbf{1} \in \mathrm{Ind}_{H_0}^G(\mathbb{Z}_2)$ that maps all G/H_0 to 1, and Λ is a system of representatives for the conjugacy classes of the CM-types of K. When the degree of K is $2N$, the dimension of $\bigoplus_{I \in J_{odd}} K(I)$ over $\mathbb{Q}$ is 2^N, which is same as that of $\bigoplus_{\Phi \in \Lambda} K^*(\Phi)$.

The following proposition also shows that the set of $(K(I), \Phi(I))$ can be regarded as the dual of the set of $(K^*(\Phi), \Phi^*)$; for a G-module M, denote by M^H, the subset of M consisting of all the fixed elements by H. Then, the half norm map $N_{\Phi(I)} : M^{H(I)} \to M^{H^*(\Phi)}$ is defined by $a \mapsto \sum_{\varphi \in \Phi(I)} \varphi(a)$. The norm map $N_{G/H} : M^H \to M^G$ is also defined by $a \mapsto \sum_{\sigma \in G/H} \sigma(a)$.

Proposition 4.1. *Let M be a G-module on which ι acts as -1. Using the half norm maps, define two maps $N_{J \to \Lambda}, N_{\Lambda \to J}$ by*

$$N_{J \to \Lambda} : \bigoplus_{I \in J_{odd}} M^{H(I)} \to \bigoplus_{\Phi_f \in \Lambda} M^{H^*(\Phi_f)},$$

$$(a_I)_{I \in J_{odd}} \mapsto \left(\sum_{I \in J_{odd}} \iota^{\sum_{\varphi H_0 \in I} f(\varphi H_0)} N_{\Phi_f(I)}(a_I) \right)_{\Phi_f \in \Lambda},$$

$$N_{\Lambda \to J} : \bigoplus_{\Phi_f \in \Lambda} M^{H^*(\Phi_f)} \to \bigoplus_{I \in J_{odd}} M^{H(I)},$$

$$(b_{\Phi_f})_{\varphi \in \Phi_f} \mapsto \left(\sum_{\Phi_f \in \Lambda} \iota^{\sum_{\varphi H_0 \in I} f(\varphi H_0)} N_{\Phi_f(I)^*}(b_{\Phi_f}) \right)_{I \in J_{odd}}.$$

Then, the compositions $N_{J \to \Lambda} \circ N_{\Lambda \to J}$ and $N_{\Lambda \to J} \circ N_{J \to \Lambda}$ equal the multiplication by 2^{N-1}.

We use the following two lemmas for the proof.

Lemma 4.1. *For any $I, I' \in J_{odd}$,*

$$\sum_{\Phi_f \in \Lambda} \iota^{\sum_{\varphi' H_0 \in I'} f(\varphi' H_0) + \sum_{\varphi H_0 \in I} f(\varphi H_0)} N_{\Phi_f(I')^*} \circ N_{\Phi_f(I)}$$

$$= \begin{cases} 2^{N-2}(id - \iota) + 2^{N-2} N_{G/H(I)} & \text{if } I = I', \\ 0 & \text{otherwise.} \end{cases} \tag{31}$$

Proof. The left-hand side of (31) equals

$$\sum_{\Phi_f \in \Lambda} \sum_{\psi' \in G/H_0^*(\Phi_f)} \iota^{\sum_{\psi H_0 \in I'} (f + r_{\Phi_f}(\psi'))(\varphi H_0)} \psi' \sum_{\psi \in H_0(I) \backslash G} \iota^{\sum_{\varphi H_0 \in I} (f + r_{\Phi_f}(\psi))(\varphi H_0)} \psi^{-1}$$

$$= \sum_{\Phi_f \in \Lambda} \sum_{\psi' \in G/H_0^*(\Phi_f)} \iota^{\sum_{\varphi H_0 \in I'} \psi' * f(\varphi H_0)} \sum_{\psi \in H_0(I) \backslash G} \iota^{\sum_{\varphi H_0 \in I} \psi * f(\varphi H_0)} \psi' \psi^{-1}$$

$$= \sum_{\Phi_f \in \Lambda} \sum_{\psi' \in G/H_0^*(\Phi_f)} \iota^{\sum_{\varphi H_0 \in I'} \psi' * f(\varphi H_0)} \sum_{\psi \in H_0(I) \backslash G} \iota^{\sum_{\varphi H_0 \in I} \psi \psi' * f(\varphi H_0)} \psi^{-1}$$

$$=: (\star).$$

Using the decomposition (30),

$$(\star) = \sum_{f \in \mathrm{Ind}_{H_0}^G (\mathbb{Z}_2)/\langle \mathbf{1} \rangle} \iota^{\sum_{\varphi H_0 \in I'} f(\varphi H_0)} \sum_{\psi \in H_0(I) \backslash G} \iota^{\sum_{\varphi H_0 \in I} \psi * f(\varphi H_0)} \psi^{-1}$$

$$= \sum_{\psi \in H_0(I) \backslash G} \iota^{\sum_{\varphi H_0 \in I} r_{\Phi_0}(\psi)(\varphi H_0)} \psi^{-1} \sum_{f \in \mathrm{Ind}_{H_0}^G (\mathbb{Z}_2)/\langle \mathbf{1} \rangle} \iota^{\sum_{\varphi H_0 \in I'} f(\varphi H_0) + \sum_{\varphi H_0 \in I} \psi \cdot f(\varphi H_0)}$$

$$= \sum_{\psi \in H_0(I) \backslash G} \iota^{\sum_{\varphi H_0 \in I} r_{\Phi_0}(\psi)(\varphi H_0)} \psi^{-1} \sum_{f \in \mathrm{Ind}_{H_0}^G (\mathbb{Z}_2)/\langle \mathbf{1} \rangle} \iota^{\sum_{\varphi H_0 \in I'} f(\varphi H_0) + \sum_{\varphi H_0 \in \psi^{-1} I} f(\varphi H_0)}$$

$$= 2^{N-1} \sum_{\psi \in H_0(I) \backslash G, \ I' = \psi^{-1} I} \psi^{-1} + 2^{N-2} \sum_{\psi \in H_0(I) \backslash G, \ I' \neq \psi^{-1} I} (1 + \iota) \psi^{-1}.$$

If $I' = \psi^{-1}I$ for some $\psi \in H_0(I) \setminus G$, then, $I = I'$ and $\psi \in H_0(I)$ since $I, I' \in J_{odd}$. Therefore,

$$(\star) = \begin{cases} 2^{N-2}(id - \iota) + 2^{N-2}N_{G/H(I)} & \text{if } I = I', \\ 0 & \text{otherwise.} \end{cases}$$

We obtain the lemma. $\square$

Lemma 4.2. *For* $\Phi_f, \Phi_{f'} \in \Lambda$,

$$\sum_{I \in J_{odd}} \iota^{\sum_{\varphi H_0 \in I}(f'+f)(\varphi H_0)} N_{\Phi_{f'}(I)} \circ N_{\Phi_f(I)^*}$$

$$= \begin{cases} 2^{N-2}(id - \iota) + 2^{N-2}N_{G/H^*(\Phi_f)} & \text{if } f = f', \\ 0 & \text{otherwise.} \end{cases} \tag{32}$$

Proof. The left-hand side of (32) equals

$$\sum_{I \in J_{odd}} \sum_{\psi' \in H_0(I) \setminus G} \iota^{\sum_{\varphi H_0 \in I}(f+f'+r_{\Phi_{f'}}(\psi'))(\varphi H_0)} \psi'^{-1} \sum_{\psi \in G/H_0^*(\Phi_f)} \iota^{\sum_{\varphi H_0 \in I} r_{\Phi_f}(\psi)(\varphi H_0)} \psi$$

$$= \sum_{I \in J_{odd}} \sum_{\psi' \in H_0(I) \setminus G} \iota^{\sum_{\varphi H_0 \in I}(f+f'+r_{\Phi_{f'}}(\psi'))(\varphi H_0)} \sum_{\psi \in G/H_0^*(\Phi_f)} \iota^{\sum_{\varphi H_0 \in I} r_{\Phi_f}(\psi'\psi)(\varphi H_0)} \psi$$

$$=: (\star).$$

Since $r_{\Phi_{f'}}(\tau) = r_{\Phi_f}(\tau) + \tau \cdot (f - f') - (f - f')$,

$$\begin{aligned}\left(f + f' + r_{\Phi_{f'}}(\psi') + r_{\Phi_f}(\psi'\psi)\right)(\varphi H_0) &= \left(\psi' \cdot (f - f') + r_{\Phi_f}(\psi') + r_{\Phi_f}(\psi'\psi)\right)(\varphi H_0) \\ &= \left(\psi' \cdot (f - f') + \psi' \cdot r_{\Phi_f}(\psi)\right)(\varphi H_0) \\ &= \psi' \cdot \left(\psi * f - f'\right)(\varphi H_0). \end{aligned}$$

Then, by the decomposition (29),

$$(\star) = \sum_{I \in J_{odd}} \sum_{\psi' \in H_0(I) \setminus G} \sum_{\psi \in G/H_0^*(\Phi_f)} \iota^{\sum_{\varphi H_0 \in \psi'^{-1}I}(\psi*f-f')(\varphi H_0)} \psi$$

$$= \sum_{\psi \in G/H_0^*(\Phi_f)} \psi \sum_{I \subset \{\varphi_1 H_0, \dots, \varphi_N H_0\}, |I|: \text{ odd}} \iota^{\sum_{\varphi H_0 \in I}(\psi*f-f')(\varphi H_0)}$$

$$= 2^{N-1} \sum_{\psi \in G/H_0^*(\Phi_f),\, f'=\psi*f} \psi + 2^{N-1} \sum_{\psi \in G/H_0^*(\Phi_f),\, f'=\iota\psi*f} \iota\psi + 2^{N-2} \sum_{\psi \in G/H_0^*(\Phi_f),\, f'=\iota\psi*f} (id + \iota)\psi.$$

If $\psi * f = f'$ for some $\psi \in G/H^*(\Phi_f)$, then, $f' = f$ and $\psi \in H^*(\Phi_f)$ since $f, f' \in \Lambda$. Therefore,

$$(\star) = \begin{cases} 2^{N-2}(id - \iota) + 2^{N-2}N_{G/H^*(\Phi_f)} & \text{if } f = f', \\ 0 & \text{otherwise.} \end{cases}$$

We obtain the lemma. $\square$

Proof of Proposition 4.1. Denote the canonical embedding $M^{H(I')} \hookrightarrow \bigoplus_{I \in J_{odd}} M^{H(I)}$ by $i_{I'}$, and the canonical projection $\bigoplus_{I \in J_{odd}} M^{H(I)} \twoheadrightarrow M^{H(I')}$ by $p_{I'}$. Then, for $I', I'' \in J_{odd}$ by Lemma 4.1,

$$p_{I''} \circ N_{\Lambda \to J} \circ N_{J \to \Lambda} \circ i_{I'} = \sum_{\Phi_f \in \Lambda} \iota^{\sum_{\varphi'' H_0 \in I''} f(\varphi'' H_0) + \sum_{\varphi' H_0 \in I'} f(\varphi' H_0)} N_{\Phi_f(I'')^*} \circ N_{\Phi_f(I')}$$

$$= \begin{cases} 2^{N-1} \, id & \text{if } I'' = I', \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, denote the canonical embedding $M^{H^*(\Phi')} \hookrightarrow \bigoplus_{\Phi \in \Lambda} M^{H^*(\Phi)}$ and the projection $\bigoplus_{\Phi \in \Lambda} M^{H^*(\Phi)} \twoheadrightarrow M^{H^*(\Phi')}$ by $i_{\Phi'}$ and $p_{\Phi'}$. Then, for $\Phi_{f'}, \Phi_{f''} \in \Lambda$ by Lemma 4.2,

$$p_{\Phi_{f''}} \circ N_{J \to \Lambda} \circ N_{\Lambda \to J} \circ i_{\Phi_{f'}} = \sum_{I \in J_{odd}} \iota^{\sum_{\varphi H_0 \in I} (f' + f'')(\varphi H_0)} N_{\Phi_{f''}(I)} \circ N_{\Phi_{f'}(I)^*}$$

$$= \begin{cases} 2^{N-1} \, id & \text{if } f' = f'', \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, the assertion holds. □

For a given CM-field L, we denote by $L^{1-\iota}$, the subspace consisting of $a \in L$ such that $\iota a = -a$. Then, $N_{\Lambda \to J}$ defined in Proposition 4.1 induces an isomorphism as $\mathbb{Q}$-linear spaces:

$$N_{\Lambda \to J} : \bigoplus_{\Phi \in \Lambda} K^*(\Phi)^{1-\iota} \xrightarrow{\cong} \bigoplus_{I \in J_{odd}} K(I)^{1-\iota}. \tag{33}$$

Even if the cardinality of I is even, $H(I)$, $H_0(I)$ and $S_{\Phi(I)}$ are well defined by (26), (27) and (28). $\Phi(I)$ and $\Phi(I)^*$ are also defined similarly. When the cardinality of I is odd, we have $\iota \in H(I)$, hence, the fixed field $K(I)$ by $H(I)$ is a totally real field. $[H_0(I) : H(I)] = 1$ or 2 in this case.

Let M be a 2-divisible G-module M on which ι acts as -1. Then, for $I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}$ with odd cardinality, the half norm map $N_{\Phi(I)}, N_{\Phi(I)^*}$ satisfies on $M^{H(I)}, M^{H^*(\Phi)}$ respectively,

$$N_{\Phi(I)} = \frac{1}{2} \sum_{\psi \in H(I) \backslash G} (-1)^{\sum_{\varphi H_0 \in I} r_\Phi(\psi)(\varphi H_0)} \psi^{-1}, \tag{34}$$

$$N_{\Phi(I)^*} = \frac{1}{2} \sum_{\psi \in G/H^*(\Phi)} (-1)^{\sum_{\varphi H_0 \in I} r_\Phi(\psi)(\varphi H_0)} \psi. \tag{35}$$

In the sequel, we use (34), (35) as the definition of the half norm map $N_{\Phi(I)}$ and $N_{\Phi(I)^*}$. It is well defined since $\sum_{\varphi H_0 \in I} r_\Phi(\sigma)(\varphi H_0)$ depends only on the double coset of $H(I)\sigma H^*(\Phi)$. By this, we can calculate $N_{\Phi(I)}, N_{\Phi(I)^*}$ for $I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}$ with even cardinality. It is also possible to omit the assumption that ι acts on M as -1.

$N_{\Phi(I)}$ gives a map from $M^{H(I)}$ to $M^{H^*(\Phi)}$ because we have for $\sigma \in H^*(\Phi)$,

$$\sigma N_{\Phi(I)} = \frac{1}{2} \sum_{\psi \in H(I) \backslash G} (-1)^{\sum_{\varphi H_0 \in I} r_\Phi(\psi)(\varphi H_0)} \sigma \psi^{-1}$$

$$= \frac{1}{2} \sum_{\psi \in H(I) \backslash G} (-1)^{\sum_{\varphi H_0 \in I} r_\Phi(\psi \sigma)(\varphi H_0)} \psi^{-1} = N_{\Phi(I)}.$$

Similarly, $N_{\Phi(I)^*}(M^{H^*(\Phi)}) \subset M^{H(I)}$, $\iota N_{\Phi(I)} = (-1)^{|I|} N_{\Phi(I)}$ and $\iota N_{\Phi(I)^*} = (-1)^{|I|} N_{\Phi(I)^*}$ also hold.

For a G-module M, we denote the complex conjugation of $a \in M$ by $\bar{a}$. Let L be a CM-field or a totally real field, and F be a subfield of L. Then, a positive definite quadratic form over L is defined by $a \mapsto Tr_{L/F}(\bar{a}a)$.

On each direct sum $\bigoplus_{\Phi \in \Lambda} K^*(\Phi)$ and $\bigoplus_{I \in J_{odd}} K(I)$, a quadratic form is defined by the orthogonal sum of $Tr_{K(I)/\mathbb{Q}}(\bar{a}a)$, $Tr_{K^*(\Phi)/\mathbb{Q}}(\bar{a}a)$ respectively. Denote them by Q_J and Q_Λ. They have canonical linear extensions to $K_0^c \otimes_{\mathbb{Q}} (\bigoplus_{I \in J_{odd}} K(I))$, $K_0^c \otimes_{\mathbb{Q}} (\bigoplus_{\Phi \in \Lambda} K^*(\Phi))$, which are denoted by $K_0^c \otimes_{\mathbb{Q}} Q_J$ and $K_0^c \otimes_{\mathbb{Q}} Q_\Lambda$.

For the maximum totally real field K_0 of K, take a totally positive element $d \in K_0$ such that $K = K_0(\sqrt{-d})$. Then, we have the Pfister form defined over K_0^c:

$$q := \langle 1, \varphi_1(d) \rangle \otimes \cdots \otimes \langle 1, \varphi_N(d) \rangle, \tag{36}$$

where $\langle 1, a \rangle$ represents the quadratic form $x^2 + ay^2$. This quadratic form can be regarded as a tensor product of the norm $N_{K_0^c(\sqrt{-\varphi_i(d)})/K_0^c}$ defined on

$$V := K_0^c(\sqrt{-\varphi_1(d)}) \otimes_{K_0^c} \cdots \otimes_{K_0^c} K_0^c(\sqrt{-\varphi_N(d)}), \tag{37}$$

which is a K_0^c-algebra.

For $I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}$, let

$$v_I := c_1 \otimes \cdots \otimes c_N, \quad c_i := \begin{cases} \sqrt{-\varphi_i(d)} & \text{if } \varphi_i H_0 \in I, \\ 1 & \text{otherwise.} \end{cases} \tag{38}$$

Then, $\{v_I : I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}\}$ makes a basis of V as a linear space over K_0^c.

Now, we have $\prod_{\varphi H_0 \in I} \sqrt{-\varphi(d)} \in K(I)$, since $H(I)$ fixes it. Let $[I] := \{\sigma I : \sigma \in G\}$. Then, there is the canonical isomorphism:

$$K_0^c \otimes_{\mathbb{Q}} K(I) \xrightarrow{\cong} \bigoplus_{I' \in [I]} K_0^c\left(\prod_{\varphi \in I'} \sqrt{-\varphi(d)} \right). \tag{39}$$

We denote by J, a system of representatives for the orbits of the action of G on $\{\varphi_1 H_0, \ldots, \varphi_N H_0\}$. Then,

$$K_0^c \otimes_{\mathbb{Q}} \left(\bigoplus_{I \in J} K(I) \right) \cong \bigoplus_{I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}} K_0^c\left(\prod_{\varphi \in I} \sqrt{-\varphi(d)} \right). \tag{40}$$

This map gives an embedding $\phi_{J_{odd}} : K_0^c \otimes_{\mathbb{Q}} (\bigoplus_{I \in J_{odd}} K(I)^{1-\iota}) \hookrightarrow V$. Hence, by (33), there is also an embedding $\phi_{J_{odd}} \circ N_{\Lambda \to J} : K_0^c \otimes_{\mathbb{Q}} (\bigoplus_{\Phi \in \Lambda} K^*(\Phi)^{1-\iota}) \hookrightarrow V$.

Theorem 4.1 shows that $\phi_{J_{odd}} \circ N_{\Lambda \to J}$ is extended to an isomorphism between $K_0^c \otimes_{\mathbb{Q}} (\bigoplus_{\Phi \in \Lambda} K^*(\Phi))$ and V, conserving their quadratic forms.

Theorem 4.1. *For a totally positive $d \in K_0$ such that $K = K_0(\sqrt{-d})$, define a Pfister form q and K_0^c-algebra V by* (36) *and* (37) *respectively. Then, there is an isomorphism as K_0^c-algebras:*

$$\phi_\Lambda : K_0^c \otimes_{\mathbb{Q}} \left(\bigoplus_{\Phi \in \Lambda} K^*(\Phi) \right) \xrightarrow{\cong} V.$$

Furthermore, such isomorphisms satisfy $q(\phi_\Lambda(w)) = 2^{-N} K_0^c \otimes_{\mathbb{Q}} Q_\Lambda(w)$, where Q_Λ is the orthogonal sum of the quadratic form $Tr_{K^*(\Phi)/\mathbb{Q}}(\bar{a}a)$.

The following lemma is used for the proof.

Lemma 4.3. *Let I, I' be subsets of $\{\varphi_1 H_0, \ldots, \varphi_N H_0\}$, and denote their exclusive disjunction by $I \veebar I'$. For any 2-divisible G-module M and Φ_f, $\Phi_{f'} \in \Lambda$, let a, b be elements of M fixed by $H^*(\Phi_f)$, $H^*(\Phi_{f'})$ respectively. Then,*

$$\sum_{I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}} (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0) + \sum_{\varphi H_0 \in I \veebar I'} f'(\varphi H_0)} N_{\Phi_f(I)^*}(a) N_{\Phi_{f'}(I \veebar I')^*}(b)$$

$$= \begin{cases} 2^{N-1} (-1)^{\sum_{\varphi H_0 \in I'} f(\varphi H_0)} N_{\Phi_f(I')^*}(a \times \sigma(b)) & \text{if } f = \sigma * f' \text{ for some } \sigma \in G, \\ 0 & \text{otherwise.} \end{cases} \tag{41}$$

Proof. The left-hand side of (41) equals

$$\frac{1}{4} \sum_{\psi \in G/H^*(\Phi_f)} \sum_{\psi' \in G/H^*(\Phi_{f'})} \psi(a) \psi'(b)$$

$$\times \sum_{I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}} (-1)^{\sum_{\varphi H_0 \in I} (f + r_{\Phi_f}(\psi))(\varphi H_0) + \sum_{\varphi H_0 \in I \veebar I'} (f' + r_{\Phi_{f'}}(\psi'))(\varphi H_0)} =: (\star).$$

We have

$$\sum_{\varphi H_0 \in I} \left(f + r_{\Phi_f}(\psi)\right)(\varphi H_0) + \sum_{\varphi H_0 \in I \veebar I'} \left(f' + r_{\Phi_{f'}}(\psi')\right)(\varphi H_0)$$

$$= \sum_{\varphi H_0 \in I} \left(f + r_{\Phi_f}(\psi)\right)(\varphi H_0) + \sum_{\varphi H_0 \in I'} \left(f + r_{\Phi_f}(\psi)\right)(\varphi H_0)$$

$$+ \sum_{\varphi H_0 \in I'} \left(f + r_{\Phi_f}(\psi)\right)(\varphi H_0) + \sum_{\varphi H_0 \in I \veebar I'} \left(f' + r_{\Phi_{f'}}(\psi')\right)(\varphi H_0)$$

$$= \sum_{\varphi H_0 \in I \veebar I'} \left(f + f' + r_{\Phi_f}(\psi) + r_{\Phi_{f'}}(\psi')\right)(\varphi H_0) + \sum_{\varphi H_0 \in I'} \left(f + r_{\Phi_f}(\psi)\right)(\varphi H_0). \tag{42}$$

Furthermore, since $r_{\Phi_{f'}}(\tau) = r_{\Phi_f}(\tau) + \tau \cdot (f' - f) - (f' - f)$, we have

$$f + f' + r_{\Phi_f}(\psi) + r_{\Phi_{f'}}(\psi') = \psi \cdot (f - f') + r_{\Phi_{f'}}(\psi) + r_{\Phi_{f'}}(\psi')$$

$$= \psi \cdot (f - f') + r_{\Phi_{f'}}(\psi) + r_{\Phi_{f'}}(\psi) + \psi \cdot r_{\Phi_{f'}}(\psi^{-1}\psi')$$

$$= \psi \cdot (f - (\psi^{-1}\psi') * f').$$

Hence,

$$(\star) = \frac{1}{4} \sum_{\psi \in G/H^*(\Phi_f)} \sum_{\psi' \in G/H^*(\Phi_{f'})} (-1)^{\sum_{\varphi H_0 \in I'} (f + r_{\Phi_f}(\psi))(\varphi H_0)} \psi(a) \psi'(b)$$

$$\times \sum_{I \subset \{\varphi_1 H_0, \ldots, \varphi_N H_0\}} (-1)^{\sum_{\varphi H_0 \in I \veebar I'} \psi \cdot (f - (\psi^{-1}\psi') * f')(\varphi H_0)}.$$

Hence, let $\sigma = \psi^{-1}\psi'$, then,

$$(\star) = \begin{cases} 2^{N-2} \sum_{\psi \in G/H^*(\Phi_f)} (-1)^{\sum_{\varphi H_0 \in I'}(f + r_{\Phi_f}(\psi))(\varphi H_0)} \psi(a \times \sigma(b)) & \text{if } f = \sigma * f' \text{ for some } \sigma \in G, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, Eq. (41) follows. □

Proof of Theorem 4.1. If there is an isomorphism ϕ_Λ such that $q(\phi_\Lambda(w)) = 2^{-N} Q_\Lambda(w)$, the other isomorphisms also have the property, because $Q_\Lambda \circ \sigma = Q_\Lambda$ holds for any automorphisms σ of $K_0^c \otimes_{\mathbb{Q}} (\bigoplus_{\Phi \in \Lambda} K^*(\Phi))$.

For $(a_{\Phi_f}) \in \bigoplus_{\Phi_f \in \Lambda} K^*(\Phi_f)$, define ϕ_Λ by

$$\phi_\Lambda((a_{\Phi_f})) := 2^{-N+1} \sum_I \frac{v_I}{\prod_{\varphi H_0 \in I} \sqrt{-\varphi(d)}} \sum_{\Phi_f \in \Lambda} (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0)} N_{\Phi_f(I)^*}(a_{\Phi_f}). \tag{43}$$

The coefficient of v_i is an element of K_0^c, because we have $c N_{\Phi_f(I)^*} = (-1)^{\sum_{\varphi H_0 \in I} r_{\Phi_f}(c)(\varphi H_0)} N_{\Phi_f(I)^*}$ for $c \in C$, and furthermore, by Lemma 1.1 and Proposition 1.1,

$$c\left(\prod_{\varphi H_0 \in I} \sqrt{-\varphi(d)} \right) = (-1)^{\sum_{\varphi H_0 \in I} r_{\Phi_f}(c)(\varphi H_0)} \prod_{\varphi H_0 \in I} \sqrt{-\varphi(d)}. \tag{44}$$

Hence, (43) is well defined.

Let's see that ϕ_Λ satisfies the assertion of the theorem. It is clear that ϕ_Λ is K_0^c-linear. We divide the proof into two parts.

(i) ϕ_Λ is a homomorphism between K_0^c-algebras; it is enough if we can show $\phi_\Lambda((a_\Phi))\phi_\Lambda((b_\Phi)) = \phi_\Lambda((a_\Phi b_\Phi))$ for any $(a_\Phi)_{\Phi \in \Lambda}, (b_\Phi)_{\Phi \in \Lambda} \in \bigoplus_{\Phi \in \Lambda} K^*(\Phi)$. Denote the exclusive disjunction of I and I' by $I \veebar I'$. Then, we have

$$\phi_\Lambda((a_{\Phi_f}))\phi_\Lambda((b_{\Phi_f}))$$

$$= 2^{-2N} \sum_{\Phi_f \in \Lambda} \sum_{\Phi_{f'} \in \Lambda} \sum_I \sum_{I'} \frac{v_{I \veebar I'}}{\prod_{\varphi H_0 \in I \veebar I'} \sqrt{-\varphi(d)}}$$

$$\times \sum_{\psi \in G/H^*(\Phi_f)} (-1)^{\sum_{\varphi H_0 \in I}(f + r_{\Phi_f}(\psi))(\varphi H_0)} \psi(a_{\Phi_f})$$

$$\times \sum_{\psi' \in G/H^*(\Phi_{f'})} (-1)^{\sum_{\varphi H_0 \in I'}(f' + r_{\Phi_{f'}}(\psi'))(\varphi H_0)} \psi'(b_{\Phi_{f'}})$$

$$= 2^{-2N} \sum_{\Phi_f \in \Lambda} \sum_{\Phi_{f'} \in \Lambda} \sum_I \sum_{I'} \frac{v_{I'}}{\prod_{\varphi H_0 \in I'} \sqrt{-\varphi(d)}}$$

$$\times \sum_{\psi \in G/H^*(\Phi_f)} (-1)^{\sum_{\varphi H_0 \in I}(f + r_{\Phi_f}(\psi))(\varphi H_0)} \psi(a_{\Phi_f})$$

$$\times \sum_{\psi' \in G/H^*(\Phi_{f'})} (-1)^{\sum_{\varphi H_0 \in I \veebar I'}(f' + r_{\Phi_{f'}}(\psi'))(\varphi H_0)} \psi'(b_{\Phi_{f'}})$$

$$= 2^{-2N+2} \sum_{\Phi_f \in \Lambda} \sum_{\Phi_{f'} \in \Lambda} \sum_{I'} \frac{\nu_{I'}}{\prod_{\varphi H_0 \in I'} \sqrt{-\varphi(d)}}$$

$$\times \sum_I (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0) + \sum_{\varphi H_0 \in I \searrow I'} f'(\varphi H_0)} N_{\Phi_f(I)^*}(a_{\Phi_f}) N_{\Phi_{f'}(I)^*}(b_{\Phi_{f'}}).$$

Therefore, by Lemma 4.3,

$$\phi_\Lambda(a_{\Phi_f}) \phi_\Lambda(b_{\Phi_f}) = 2^{-N+1} \sum_{\Phi_f \in \Lambda} \sum_{I'} \frac{\nu_{I'}}{\prod_{\varphi H_0 \in I'} \sqrt{-\varphi(d)}} (-1)^{\sum_{\varphi H_0 \in I'} f(\varphi H_0)} N_{\Phi_f(I')^*}(a_{\Phi_f} b_{\Phi_f})$$

$$= \phi_\Lambda(a_{\Phi_f} b_{\Phi_f}).$$

(ii) $q(\phi_\Lambda(w)) = 2^{-N} K_0^c \otimes_\mathbb{Q} Q_\Lambda(w)$; it is enough if we can show $q(\phi_\Lambda((a_\Phi))) = 2^{-N} Q_\Lambda((a_\Phi))$ for $(a_\Phi)_{\Phi \in \Lambda} \in \bigoplus_{\Phi \in \Lambda} K^*(\Phi)$. We have

$$q\big(\phi_\Lambda((a_{\Phi_f}))\big) = 2^{-2N+2} \sum_I \frac{q(\nu_I)}{\prod_{\varphi H_0 \in I}(-\varphi(d))} \left(\sum_{\Phi_f \in \Lambda} (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0)} N_{\Phi_f(I)^*}(a_{\Phi_f}) \right)^2$$

$$= 2^{-2N+1} \sum_I (-1)^{|I|} \sum_{\Phi_f \in \Lambda} (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0)} N_{\Phi_f(I)^*}(a_{\Phi_f})$$

$$\times \sum_{\Phi_{f'} \in \Lambda} \sum_{\psi' \in G/H^*(\Phi_{f'})} (-1)^{\sum_{\varphi H_0 \in I} (f' + r_{\Phi_{f'}}(\psi))(\varphi H_0)} \psi'(a_{\Phi_{f'}}).$$

Since $\iota * f(\varphi H_0) = (r_{\Phi_0}(\iota) + \iota \cdot f)(\varphi H_0) = f(\varphi H_0) + 1$ for any f,

$$q\big(\phi_\Lambda((a_{\Phi_f}))\big)$$

$$= 2^{-2N+1} \sum_I \sum_{\Phi_f \in \Lambda} (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0)} N_{\Phi_f(I)^*}(a_{\Phi_f})$$

$$\times \sum_{\Phi_{f'} \in \Lambda} \sum_{\psi' \in G/H^*(\Phi_{f'})} (-1)^{\sum_{\varphi H_0 \in I} (\iota * f' + r_{\Phi_{\iota * f'}}(\psi))(\varphi H_0)} \psi'(a_{\Phi_{f'}})$$

$$= 2^{-2N+2} \sum_I \sum_{\Phi_f \in \Lambda} \sum_{\Phi_{f'} \in \Lambda} (-1)^{\sum_{\varphi H_0 \in I} f(\varphi H_0) + \sum_{\varphi H_0 \in I} \iota * f'(\varphi H_0)} N_{\Phi_f(I)^*}(a_{\Phi_f}) N_{\Phi_{\iota * f'}(I)^*}(a_{\Phi_f}).$$

Therefore, by Lemma 4.3,

$$q\big(\phi_\Lambda((a_{\Phi_f}))\big) = 2^{-N+1} \sum_{\Phi_f \in \Lambda} N_{\Phi_f(\emptyset)^*}(a_{\Phi_f} \overline{a_{\Phi_f}})$$

$$= 2^{-N} \sum_{\Phi_f \in \Lambda} \sum_{\psi \in G/H^*(\Phi_f)} \psi(a_{\Phi_f} \overline{a_{\Phi_f}}) = 2^{-N} Q_\Lambda((a_{\Phi_f})).$$

It is clear that q and $Q_\Lambda(w)$ are positive definite. Since $q(\phi_\Lambda(w)) = 2^{-N} K_0^c \otimes_\mathbb{Q} Q_\Lambda(w)$ for any $w \in K_0^c \otimes_\mathbb{Q} (\bigoplus_{\Phi \in \Lambda} K^*(\Phi))$, ϕ_Λ must be injective. Hence, by comparing the dimensions, it is an isomorphism. Therefore, the assertion holds. $\square$

Acknowledgments

Supplementary material

The online version of this article contains additional supplementary material.
Please visit doi:10.1016/j.jnt.2010.03.021.

References

[1] E. Artin, J. Tate, Class Field Theory, Harvard University Press, 1961.
[2] B. Dodson, The structure of Galois groups of CM-fields, Trans. Amer. Math. Soc. 283 (1984) 1–32.
[3] T. Kubota, On the field extension by complex multiplication, Trans. Amer. Math. Soc. 118 (1965) 113–122.
[4] T.Y. Lam, Introduction to Quadratic Forms over Fields, American Mathematical Society, 2004.
[5] A.I. Ovseevich, Abelian extensions of fields of CM-type, Funktsional. Anal. i Prilozhen. 8 (1) (1974) 16–24.
[6] A. Pfister, Zur Darstellung definiter Funcktionen als Summe von Quadraten, Invent. Math. 4 (1967) 229–237.
[7] J.P. Serre, Corps Locaux, Hermann, Paris, 1968.
[8] J.P. Serre, Linear Representations of Finite Groups, Springer-Verlag, Berlin, New York, 1977.
[9] G. Shimura, On the class-fields obtained by complex multiplication of abelian varieties, Osaka Math. J. 14 (1962) 33–44.
[10] G. Shimura, On abelian varieties with complex multiplication, Proc. London Math. Soc. 34 (1977) 63–86.
[11] G. Shimura, Automorphic forms and the periods of abelian varieties, J. Math. Soc. Japan 31 (3) (1979) 561–591.
[12] G. Shimura, Abelian Varieties with Complex Multiplication and Modular Functions, Princeton Math. Ser., vol. 46, 1998.
[13] W. Wei, Moduli fields of CM-motives applied to Hilbert's 12-th problem, preprint, 1994.