Title	On the class-fields obtained by complex multiplication of abelian varieties
Author(s)	Shimura, Goro
Citation	Osaka Mathematical Journal. 1962, 14(1), p. 33-44
Version Type	VoR
URL	https://doi.org/10.18910/9592
rights	
Note	

Shimura, G.
Osaka Math. J.
14 (1962), 33–44.

ON THE CLASS-FIELDS OBTAINED BY COMPLEX MULTIPLICATION OF ABELIAN VARIETIES

Dedicated to Professor K. Shoda on his sixtieth birthday

By

Goro SHIMURA

By complex multiplication of abelian varieties, we get certain class-fields over a totally imaginary quadratic extension F of a totally real algebraic number field F_0. The corresponding ideal-groups are explicitly given in Main Theorems of [3]. On this subject, one may ask how large class-fields over F can be constructed by such a means. An answer to the question is given in [4, 5], to a certain degree, in terms of local characters attached to Grössen-characters. However, this does not give any information, for example, about unramified class-fields over F so obtained. The purpose of the present paper is to give some results concerning this problem, which are almost directly derived from the defining-relation for the ideal-groups mentioned above.

In general the ideal-class group $\mathfrak{K}$ of F is approximately decomposed into the ideal-class group $\mathfrak{K}_0$ of F_0 and its complementary part $\mathfrak{K}_1$. Adjoining the absolute class-field over F_0 to F, we get the unramified class-field over F corresponding to $\mathfrak{K}/\mathfrak{K}_1$. Now, roughly speaking, the unramified class-field over F corresponding to $\mathfrak{K}/\mathfrak{K}_0$ is generated by the fields of moduli of certain polarized abelian varieties. The ramified class-fields over F are found in a similar situation, if we consider the points of finite order on the varieties. In § 2, we show these facts under a condition on F, which is satisfied whenever F is normal over the rational number field. We shall prove that the class-fields over F_0 and complex multiplication yield at least a subfield B of the maximal abelian extension A of F such that $A \subset B(\sqrt{x} \mid x \in B)$ (Theorem 1); B contains the absolute class-field over F (Theorem 2). If F is an imaginary cyclotomic field, the results are stated in a little preciser and simpler form, as we shall see in § 3. The object of the final § 4 is the investigation of a special kind of CM-types, by which we can prove, without any condition on F, similar results for the class-fields over F obtained from complex multiplication of an abelian variety whose endomorphism-algebra contains a quadratic extension of F (Theorem 4). In all these cases, if the class-number of F is odd, the absolute class-field over F is contained in the composite of the absolute class-field over F_0 and the fields of moduli of certain polarized abelian varieties which we can specify in each case.

The author wishes to express his sincere thanks to Prof. M. Eichler whose communications gave him a chance to consider the problem, and also to Dr. Y. Akagawa, T. Honda, N. Nobusawa for their valuable discussions; in particular, the paper [2] is noticed by Nobusawa.

NOTATION AND CONVENTION. $\boldsymbol{Q}$ and $\boldsymbol{C}$ denote respectively the field of rational numbers and the field of complex numbers. For every $x \in \boldsymbol{C}$, we denote by x^ρ the complex conjugate of x. Any algebraic number field will be considered as a subfield of $\boldsymbol{C}$. If K is an algebraic number field of finite degree and $\mathfrak{b}$ is an integral ideal of K, $I_{\mathfrak{b}}(K)$ denotes the group of all ideals prime to $\mathfrak{b}$, and $P_{\mathfrak{b}}(K)$ the subgroup of $I_{\mathfrak{b}}(K)$ consisting of all principal ideals (a) such that $a \in K$, $a \equiv 1 \bmod \mathfrak{b}$. For every positive integer b, the ideal (b) generated by b (in some algebraic number field) will be often denoted simply by b. Further we denote by $C_{\mathfrak{b}}(K)$ the class-field over K corresponding to the ideal-group $P_{\mathfrak{b}}(K)$, namely, the ray-class-field modulo $\mathfrak{b}$ over K. In particular, $C_1(K)$ is the absolute class-field (Hilbert's class-field) over K.

§ 1. **Preliminaries.** Let F_0 be a totally real algebraic number field of finite degree, and F a totally imaginary quadratic extension of F_0. Define, for every positive integer b, a subgroup $I_b(F/F_0)$ of $I_b(F)$ by

$$(1) \qquad I_b(F/F_0) = \{\mathfrak{a} \in I_b(F) \mid \mathfrak{a}/\mathfrak{a}^\rho = (a) \text{ for some } a \in F \text{ such that } aa^\rho = 1,\ a \equiv 1 \bmod (b)\}.$$

We see easily that

$$(2) \qquad I_b(F/F_0) \supset P_b(F) \cdot \{\mathfrak{a} \in I_b(F) \mid \mathfrak{a}^\rho = \mathfrak{a}\} \supset P_b(F) I_b(F_0).$$

Consider the case $b=1$. If $\mathfrak{a} \in I_1(F/F_0)$, we have $\mathfrak{a}/\mathfrak{a}^\rho = (a)$ for some $a \in F$ such that $aa^\rho = 1$. By Hilbert's lemma, there exists an element w of F such that $a = w^\rho / w$. Then $(w\mathfrak{a})^\rho = w\mathfrak{a}$. It follows that

$$(3) \qquad I_1(F/F_0) = P_1(F) \cdot \{\mathfrak{a} \in I_1(F) \mid \mathfrak{a}^\rho = \mathfrak{a}\}.$$

Let $(F; \{\sigma_1, \cdots, \sigma_n\})$ be a CM-type and $(F^*; \{\tau_j\})$ be its dual (cf. [3, §§ 5.2, 8.3]). Let $\mathfrak{b}$ be an integral ideal of F^*, and b the smallest positive integer divisible by $\mathfrak{b}$. We denote by $I_{\mathfrak{b}}(F; \{\sigma_i\})$ the subgroup of $I_b(F)$ consisting of all ideals $\mathfrak{a}$ such that there exists an element u of F^* for which we have

$$(4)\qquad \prod_{i=1}^{n} \mathfrak{a}^{\sigma_i}=(u)\,,\quad N(\mathfrak{a}) = uu^{\rho}\,,\quad u\equiv 1 \bmod \mathfrak{b}\,.$$

Further we denote by $C_b(F/F_0)$ and $C_{\mathfrak{b}}(F;\ \{\sigma_i\})$ the class-fields over F corresponding to the ideal-groups $I_b(F/F_0)$ and $I_{\mathfrak{b}}(F;\ \{\sigma_i\})$, respectively. If $\mathfrak{a}\in I_b(F;\ \{\sigma_i\})$, we have $N(\mathfrak{a})\equiv 1 \bmod (b)$. It follows that $C_b(F;\ \{\sigma_i\})$ *contains the cyclotomic field* $\boldsymbol{Q}(\zeta)$ *for a primitive b-th root of unity* ζ.

Now Main Theorems 1 and 2 of [3] assert that if $(K^*;\ \{\psi_\alpha\})$ is a primitive CM-type, we get the class-fields $C_{\mathfrak{b}}(K^*;\ \{\psi_\alpha\})$ by means of complex multiplication of an abelian variety belonging to the dual of $(K^*;\ \{\psi_\alpha\})$. This result holds in a little more general form:

Proposition 1. *The assertions of Main Theorems* 1 *and* 2 *of* [3] *are true even in case where* $(K^*;\ \{\psi_\alpha\})$ *is not primitive.*

Proof. Let $(K^*;\ \{\psi_\alpha\})$ be a CM-type which is not necessarily primitive. Let $(K;\ \{\varphi_\lambda\})$ be the dual of $(K^*;\ \{\psi_\alpha\})$, and $(K_1^*;\ \{\chi_\nu\})$ be the dual of $(K;\ \{\varphi_\lambda\})$. Then $(K;\ \{\varphi_\lambda\})$ and $(K_1^*;\ \{\chi_\nu\})$ are primitive; and $(K;\ \{\varphi_\lambda\})$ is the dual of $(K_1^*;\ \{\chi_\nu\})$ (cf. [3, § 8. 3]). Let L be a Galois extension of $\boldsymbol{Q}$ containing K^*. Then K and K_1^* are subfields of L. Let G be the Galois group of L over $\boldsymbol{Q}$, and H^*, H_1^* be respectively the subgroups of G corresponding to K^*, K_1^* by Galois theory. We have $K^*\supset K_1^*$, $H^*\subset H_1^*$, in view of the result of [3, § 8. 3]. Extend ψ_α and χ_ν to elements of G and denote them again by the same letters. We have then

$$(5)\qquad \bigcup_\alpha H^*\psi_\alpha = \bigcup_\nu H_1^*\chi_\nu\,.$$

Let $\mathfrak{b}$ be an integral ideal of K and b the smallest positive integer divisible by $\mathfrak{b}$. Considering an abelian variety belonging to $(K;\ \{\varphi_\lambda\})$, we get the class-field $C_{\mathfrak{b}}(K_1^*;\ \{\chi_\nu\})$ over K_1^*. The composite of K^* and $C_{\mathfrak{b}}(K_1^*;\ \{\chi_\nu\})$ is a class-field over K^*; and by the "theorem of translation" of class-field theory, the corresponding ideal-group is the group of ideals $\mathfrak{a}\in I_b(K^*)$ such that $N_{K^*/K_1^*}(\mathfrak{a})\in I_{\mathfrak{b}}(K_1^*;\ \{\chi_\nu\})$. By the relation (5), this ideal-group is just $I_{\mathfrak{b}}(K^*;\ \{\psi_\alpha\})$; so we get our proposition.

For convenience, we state here a part of [3, § 8. 3, Prop. 28] as

Proposition 2. *Let* $(F;\ \{\sigma_i\})$ *be a CM-type and* $(F^*;\ \{\tau_j\})$ *its dual. Then* F^* *is generated over* $\boldsymbol{Q}$ *by the elements* $\sum_{i=1}^{n} x^{\sigma_i}$ *for* $x\in F$.

§ 2. **Class-fields obtained from two CM-types.** F and F_0 being as in § 1, let $(F;\ \{\sigma_1, \cdots, \sigma_n\})$ be a CM-type such that σ_1 is the identity mapping of F. Consider the condition:

(A) *If* $(F^*;\ \{\tau_j\})$ *is the dual of* $(F;\ \{\sigma_i\})$, *then* $F\supset F^*$.

This is satisfied whenever F is normal over $\boldsymbol{Q}$. Now we observe that $(F; \{\rho, \sigma_2, \cdots, \sigma_n\})$ is a CM-type. Let $(F_1^*; \{\varphi_\lambda\})$ be the dual of this CM-type. If $(F; \{\sigma_i\})$ satisfies the condition (A), we have $F_1^* \subset F$. In fact, by Proposition 2, for every $x \in F$, we see that $\sum_{i=1}^{n} x^{\sigma_i} \in F^* \subset F$, so that $x^\rho + \sum_{i=2}^{n} x^{\sigma_i} = x^\rho - x + \sum_{i=1}^{n} x^{\sigma_i} \in F$; this implies, again by Proposition 2, $F_1^* \subset F$.

Proposition 3. *Notation being as above, suppose that the condition (A) is satisfied. Then, for every positive integer b, we have*

$$I_b(F; \{\sigma_i\}) \cap I_b(F; \{\rho, \sigma_2, \cdots, \sigma_n\}) \subset I_b(F/F_0).$$

Proof. If $\mathfrak{a} \in I_b(F; \{\sigma_i\}) \cap I_b(F; \{\rho, \sigma_2, \cdots, \sigma_n\})$, we have $\mathfrak{a}\mathfrak{a}^{\sigma_2} \cdots \mathfrak{a}^{\sigma_n} = (u)$, $\mathfrak{a}^\rho \mathfrak{a}^{\sigma_1} \cdots \mathfrak{a}^{\sigma_n} = (v)$, $N(\mathfrak{a}) = uu^\rho = vv^\rho$ for an element u of F^* and an element v of F_1^* such that $u \equiv 1 \bmod (b)$, $v \equiv 1 \bmod (b)$. Put $a = u/v$. By our assumption and by the above consideration, a is an element of F; and we have $\mathfrak{a}/\mathfrak{a}^\rho = (a)$, $aa^\rho = 1$, $a \equiv 1 \bmod (b)$. This proves our proposition.

Theorem 1. *Let F_0 be a totally real algebraic number field of degree $n > 1$, and F a totally imaginary quadratic extension of F_0. Then, the composite D_b of $C_b(F/F_0)$ and $C_b(F_0)$ contains the class-field over F corresponding to the ideal-group $\{\mathfrak{a} \in I_b(F) \mid \mathfrak{a}^2 \in P_b(F)\}$. Let further $(F; \{\sigma_1, \cdots, \sigma_n\})$ be a CM-type such that σ_1 is the identity mapping of F. Suppose that the condition* (A) *is satisfied. Then, for every positive integer b, the composite of $C_b(F; \{\sigma_i\})$ and $C_b(F; \{\rho, \sigma_2, \cdots, \sigma_n\})$ contains $C_b(F/F_0)$.*

In other words, *if there exists a CM-type satisfying the condition* (A), *then, adjoining the ray-class-field modulo* (b) *over F_0, we get, by complex multiplication of abelian varieties, at least a subfield D_b of the ray-class-field $C_b(F)$ modulo* (b) *over F such that the Galois group of $C_b(F)/D_b$ is of exponent* 1 *or* 2.

Proof. The composite of $C_b(F_0)$ and F is the class-field over F corresponding to the ideal-group $\{\mathfrak{a} \in I_b(F) \mid \mathfrak{a}\mathfrak{a}^\rho \in P_b(F_0)\}$. If $\mathfrak{a}\mathfrak{a}^\rho \in P_b(F_0)$ and $\mathfrak{a}/\mathfrak{a}^\rho \in P_b(F)$, we have $\mathfrak{a}^2 \in P_b(F)$. This proves the first assertion. The second assertion is an immediate consequence of Proposition 3.

REMARK 1. If F is a non-abelian imaginary extension of $\boldsymbol{Q}$ of degree 4, the condition (A) is never satisfied by any CM-type $(F; \{\sigma_i\})$. In § 4, we shall give an example of a primitive CM-type $(F; \{\sigma_i\})$ satisfying (A) with an F which is not normal over $\boldsymbol{Q}$.

The author is ignorant of the difference between the maximal abelian extension $A=\bigcup_{b=1}^{\infty} C_b(F)$ and $B=\bigcup_{b=1}^{\infty} C_b(F_0)C_b(F;\ \{\sigma_i\})C_b(F;\ \{\rho, \sigma_2, \cdots, \sigma_n\})$[1]. If we put $D=\bigcup_{b=1}^{\infty} D_b$, we have $A\supset B\supset D$, and $A\subset D(\sqrt{x}\,|\,x\in D)$. We can at least prove:

Theorem 2. *F, F_0 and D_b being as in Theorem* 1, *the absolute class-field over F is contained in D_b for a suitable b.*

Proof. Let $E_1, \cdots, E_r$ be cyclic unramified extentions of F such that the composite of them is the maximal one among the unramified abelian extensions of F whose degrees are powers of 2. By [2, Satz 1b], we can find, for each i, a cyclic extension E_i' of F containing E_i such that $[E_i':E_i]=2$. Let b be a positive integer such that the ideal-groups corresponding to the E_i' are all defined modulo (b). Now let E_0 be the maximal one among the unramified abelian extensions of F of odd degree. Let $\mathfrak{H}$, $\mathfrak{K}$, $\mathfrak{L}$ denote respectively the subgroups of $I_b(F)$ corresponding to E_0, $E_0E_1\cdots E_r$, $E_0E_1'\cdots E_r'$. We have clearly $I_b(F)\supset\mathfrak{H}\supset\mathfrak{K}\supset\mathfrak{L}\supset P_b(F)$. If $\mathfrak{a}\in I_b(F)$ and $\mathfrak{a}^2\in P_b(F)$, then $\mathfrak{a}^2\in\mathfrak{L}$. As $\mathfrak{H}/\mathfrak{L}$ is the 2-Sylow subgroup of $I_b(F)/\mathfrak{L}$, we obtain $\mathfrak{a}\in\mathfrak{H}$. By our construction of the E_i', we must have $\mathfrak{a}\in\mathfrak{K}$. This shows that $\mathfrak{K}$ contains the ideal-group $\{\mathfrak{a}\in I_b(F)\,|\,\mathfrak{a}^2\in P_b(F)\}$. It follows that D_b contains the field $E_0E_1\cdots E_r$, the absolute class-field over F.

If either one or both of the groups

$$\{\mathfrak{a}\in I_b(F)\,|\,\mathfrak{a}\mathfrak{a}^\rho\in P_b(F_0)\}/P_b(F), \qquad I_b(F/F_0)/P_b(F)$$

have odd orders, then $D_b=C_b(F)$.

Lemma 1. *F and F_0 being as in Theorem* 1, *let h and h_0 be respectively the class-numbers of F and F_0. Then h is a multiple of h_0, and h/h_0 is the order of the group* $\{\mathfrak{a}\in I_1(F)\,|\,\mathfrak{a}\mathfrak{a}^\rho\in P_1(F_0)\}/P_1(F)$.

Proof. Let K be the absolute class-field over F_0. As the infinite prime spots of F_0 ramify in F, F is not contained in K, so that $[FK:F]=[K:F_0]=h_0$. Our lemma follows easily from this and class-field theory.

We call h/h_0 *the relative class-number of F*. Then we can conclude that, *if the relative class-number of F is odd, D_1 is the absolute class-field over F.* Further we obtain

Proposition 4. *F and F_0 being as in Theorem* 1, *let h and h_0 be respectively the class-numbers of F and F_0. Suppose that every prime ideal of F ramified in F/F_0 is a principal ideal. Then we have*

1) It would be meaningful to take account of the infinite prime spots of F_0, though we have not used them in the present investigation.

$$I_1(F/F_0) = P_1(F)I_1(F_0), \quad [C_1(F/F_0):F] \geqq h/h_0 .$$

Moreover, if h_0 is odd, the composite D_1 of $C_1(F/F_0)$ and $C_1(F_0)$ is the absolute class-field over F.

Proof. The equality $I_1(F/F_0)=P_1(F)I_1(F_0)$ follows easily from our assumption and the relation (3) of § 1. Now the injection of $I_1(F_0)$ into $I_1(F)$ gives a homomorphism of $I_1(F_0)/P_1(F_0)$ onto $I_1(F/F_0)/P_1(F)$; so we have $[I_1(F/F_0): P_1(F)] \leqq h_0$, and hence $[I_1(F): I_1(F/F_0)] \geqq h/h_0$, which implies $[C_1(F/F_0):F] \geqq h/h_0$. If h_0 is odd, the order of the group $I_1(F/F_0)/P_1(F)$ must be odd; as remarked above, this implies $D_1=C_1(F)$.

§ 3. **Class-fields over cyclotomic fields.** Let F be an imaginary cyclotomic field and F_0 the maximal real subfield of F. As F is normal over $\boldsymbol{Q}$, we can apply to F the result of § 2. In particular, we get the following assertion. *If the relative class-number of an imaginary cyclotomic field F is odd, then the absolute class-field over F is generated by the absolute class-field over the maximal real subfield of F and the unramified class-fields over F obtained from the fields of moduli of certain two polarized abelian varieties having subfields of F as endomorphism algebras.* Several criteria for the oddness of relative class-number of imaginary cyclotomic fields are given in [1, Satz 38, 42, 46].

F being still an imaginary cyclotomic field, if $(F; \{\sigma_i\})$ is primitive, the dual of $(F; \{\sigma_i\})$ is $(F; \{\sigma_i^{-1}\})$ in virtue of [3, § 8. 4, (1)]. By (1) and (4) of § 1, we see easily

$$(6) \qquad I_b(F/F_0) \cap I_b(F; \{\sigma_i\}) = I_b(F/F_0) \cap I_b(F; \{\tau_i\})$$

for any two primitive CM-types $(F; \{\sigma_i\})$ and $(F; \{\tau_i\})$. For every automorphism γ of F and for every $(F; \{\sigma_i\})$, we have

$$(7) \qquad I_b(F; \{\sigma_i\}) = I_b(F; \{\gamma\sigma_i\}) .$$

Theorem 3. *Let F be an imaginary cyclic extension of $\boldsymbol{Q}$ of degree $2n$ and F_0 the maximal real subfield of F; let σ be a generator of the Galois group of F over $\boldsymbol{Q}$. Then we have*

$$C_b(F; \{1, \sigma, \cdots, \sigma^{n-1}\}) \supset C_b(F/F_0) ,$$
$$C_b(F; \{1, \sigma, \cdots, \sigma^{n-1}\}) \supset C_b(F; \{\tau_i\})$$

for every positive integer b and for every primitive CM-type $(F; \{\tau_i\})$. Moreover, if every prime ideal of F ramified in F/F_0 is a principal ideal, then, we have, for every CM-type $(F; \{\tau_i\})$,

$$C_1(F; \{1, \sigma, \cdots, \sigma^{n-1}\}) = C_1(F/F_0) \supset C_1(F; \{\tau_i\}) .$$

Proof. It is easy to see that $(F; \{1, \sigma, \cdots, \sigma^{n-1}\})$ is a primitive CM-type. By (7), we have $I_b(F; \{1, \sigma, \cdots, \sigma^{n-1}\}) = I_b(F; \{\sigma^n, \sigma, \sigma^2, \cdots, \sigma^{n-1}\})$. Then by Proposition 3, we have $I_b(F; \{1, \sigma, \cdots, \sigma^{n-1}\}) \subset I_b(F/F_0)$. This proves the first inclusion. The second inclusion follows from this and (6). Now assume that every prime ideal of F ramified in F/F_0 is a principal ideal. By Proposition 4, $I_1(F/F_0) = P_1(F)I_1(F_0)$. We can easily verify that $I_1(F_0) \subset I_1(F; \{\tau_i\})$ for every CM-type $(F; \{\tau_i\})$, so that $I_1(F/F_0) \subset I_1(F; \{\tau_i\})$, which implies $C_1(F/F_0) \supset C_1(F; \{\tau_i\})$. Apply this to the case $\{\tau_i\} = \{1, \sigma, \cdots, \sigma^{n-1}\}$. As we have already seen the inverse inclusion, we must have $C_1(F; \{1, \sigma, \cdots, \sigma^{n-1}\}) = C_1(F/F_0)$.

In general, for every positive integer b, we see that

$$I_b(F; \{\sigma_i\}) \supset P_b(F) \cdot \{\mathfrak{a} \in I_b(F_0) \mid N(\mathfrak{a}) \equiv 1 \bmod (b)\} .$$

If $(F; \{\sigma_i\}) = (F; \{1, \sigma, \cdots, \sigma^{n-1}\})$, *the factor group*

$$I_b(F; \{\sigma_i\}) / [P_b(F) \cdot \{\mathfrak{a} \in I_b(F_0) \mid N(\mathfrak{a}) \equiv 1 \bmod (b)\}]$$

is of exponent 1 *or* 2. In fact, in this case, if $\mathfrak{a} \in I_b(F; \{\sigma_i\})$, we have $\mathfrak{a} \in I_b(F/F_0)$ by Theorem 3, so that $\mathfrak{a}/\mathfrak{a}^\rho \in P_b(F)$; on the other hand, it is clear that $N_{F_0/\boldsymbol{Q}}(\mathfrak{a}\mathfrak{a}^\rho) \equiv 1 \bmod (b)$; therefore, we have

$$\mathfrak{a}^2 = (\mathfrak{a}/\mathfrak{a}^\rho)(\mathfrak{a}\mathfrak{a}^\rho) \in P_b(F) \cdot \{\mathfrak{a} \in I_b(F_0) \mid N(\mathfrak{a}) \equiv 1 \bmod (b)\} .$$

Let l^ν be a power of an odd prime number l and ζ a primitive l^ν-th root of unity. Put $F = \boldsymbol{Q}(\zeta)$, $F_0 = \boldsymbol{Q}(\zeta + \zeta^{-1})$. Then F is cyclic over $\boldsymbol{Q}$ and every prime ideal of F ramified in F/F_0 is a principal ideal. Therefore, we can apply Proposition 4 and Theorem 3 to the present case. In particular, *if the class-number of* F_0 *is odd, then, the field of moduli of a certain polarized abelian variety having* F *as endomorphism-algebra, together with the absolute class-field over* F_0, *generates the absolute class-field over* F. By a theorem of Kummer, the class-number of $F = \boldsymbol{Q}(\zeta)$ is odd if and only if the relative class-number of F is odd (cf. [1, Satz 45]). Hence, the class-number of $F_0 = \boldsymbol{Q}(\zeta + \zeta^{-1})$ is odd whenever the relative class-number of F is odd; the table of [1] shows that the relative class-number of $\boldsymbol{Q}(\zeta)$ is odd for $l^\nu < 100$, $l^\nu \neq 29$.

Remark 2. In Theorem 3, it may happen that $C_1(F/F_0) \neq C_1(F; \{\tau_i\})$ for some $\{\tau_i\}$. In fact, let l be a prime number ≥ 5 and ζ a primitive l-th root of unity. Choose as τ_i the automorphism of F defined by $\zeta^{\tau_i} = \zeta^i$ for $1 \leq i \leq n = (l-1)/2$. As observed in [3, § 8. 4, (1)], $(F; \{\tau_i\})$ is primitive; further by [3, § 15. 4, Example 2)], we have $C_1(F; \{\tau_i\}) = F$, so that $I_1(F; \{\tau_i\}) = I_1(F)$. Therefore, $C_1(F/F_0) \neq C_1(F; \{\tau_i\})$ if the relative class-number of F is greater than 1; the latter is of course the case for many l.

Now if we put $\{\sigma_i\}=\{\tau_1\sigma, \tau_2, \cdots, \tau_n\}$, we must have $I_1(F; \{\sigma_i\})\subset I_1(F/F_0)$ in view of Proposition 3. We can prove that this CM-type $(F; \{\sigma_i\})$ is primitive. In fact, if $l\neq 17$, the trick of [3, § 8. 4, (1)] is applicable; and if $l=17$, this is shown by means of [3, § 8. 2, Prop. 26]. Then, by Theorem 3 and by what we have just proved, we get $I_1(F; \{\sigma_i\})=I_1(F/F_0)$, which implies $C_1(F; \{\sigma_i\})=C_1(F/F_0)$. In general, it is not necessarily true that there exists an automorphism γ of F such that $\{\gamma\sigma_i\}=\{1, \sigma, \cdots, \sigma^{n-1}\}$.

§ 4. A CM-type obtained from two CM-types. The argument of § 2 is powerless when F has no CM-type satisfying (A). In order to treat such a case, we consider a special kind of CM-type. We begin with an easy

Lemma 2. *Let F be a totally imaginary quadratic extension of a totally real algebraic number field F_0. Let L be the smallest normal extension of $\boldsymbol{Q}$ containing F, and G the Galois group of L over $\boldsymbol{Q}$. Then ρ, considered as an element of G, belongs to the center of G; and L is a totally imaginary quadratic extension of a totally real subfield.*

Proof. We can find an element z of F such that $F=F_0(z)$ and z^2 is a totally negative element of F_0. For every $\gamma\in G$, $(z^\gamma)^2$ is a totally negative element of F_0, so that $z^{\gamma\rho}=-z^\gamma=(-z)^\gamma=z^{\rho\gamma}$. Further, for every $x\in F_0$, we have $x^{\gamma\rho}=x^\gamma=x^{\rho\gamma}$. Therefore, for every $\gamma, \delta\in G$ and for every $x\in F_0$, we have $(x^\delta)^{\gamma\rho}=(x^\delta)^{\rho\gamma}$, $(z^\delta)^{\gamma\rho}=(z^\rho)^{\delta\gamma}=(z^\delta)^{\rho\gamma}$. These relations imply $y^{\gamma\rho}=y^{\rho\gamma}$ for every $y\in L$, since L is generated by F_0^δ and z^δ; this proves the first assertion. If we denote by L_0 the set of elements y of L such that $y^\rho=y$, we have $(y^\gamma)^\rho=y^{\rho\gamma}=y^\gamma$ for every $y\in L_0$. It follows that L_0 is totally real; this proves the last assertion.

Let F_0 be a totally real algebraic number field of degree $n>1$. Let F and M be totally imaginary quadratic extensions of F_0. We assume $F\neq M$. Let K be the composite of F and M. Obviously, K contains a totally real algebraic number field K_0 such that $[K_0:F_0]=2$. Let $(F; \{\sigma_i\})$ and $(M; \{\tau_i\})$ be CM-types. We assume $\sigma_i=\tau_i$ on F_0. This is not an essential restriction, since for any $\{\sigma_i\}$ and $\{\tau_i\}$, we can reorder them so that $\sigma_i=\tau_i$ on F_0.

Now fix an integer r such that $1\leq r\leq n$, and define $2n$ isomorphisms $\alpha_1, \beta_1, \cdots, \alpha_n, \beta_n$ of K into $\boldsymbol{C}$ by

$$(8)\qquad \begin{cases} \alpha_i=\sigma_i \text{ on } F,\ \alpha_i=\tau_i \text{ on } M \text{ for } 1\leq i\leq n, \\ \beta_j=\sigma_j \text{ on } F,\ \beta_j=\tau_j\rho \text{ on } M \text{ for } 1\leq j\leq r, \\ \beta_k=\sigma_k\rho \text{ on } F,\ \beta_k=\tau_k \text{ on } M \text{ for } r<k\leq n. \end{cases}$$

It can be easily seen that $(K; \{\alpha_1, \beta_1, \cdots, \alpha_n, \beta_n\})$ is a CM-type. We assume henceforth that σ_1 is the identity mapping of F and τ_1 is the identity mapping of M, and consider only the case $r=1$.

Let $(M^*; \{\chi_\mu\})$ be the dual of $(M; \{\tau_i\})$; let M^{**} be the field generated over $\boldsymbol{Q}$ by the elements $\sum_{\nu=2}^{n} x^{\tau_\nu}$ for $x \in M$. By Proposition 2, M^* is generated over $\boldsymbol{Q}$ by the elements $\sum_{i=1}^{n} x^{\tau_i}$ for $x \in M$. It follows that

$$M^*M = M^{**}M. \tag{9}$$

Proposition 5. *Let $(K^*; \{\varphi_\lambda\})$ be the dual of $(K; \{\alpha_i, \beta_i\})$. Then we have $K^*=FM^{**}$.*

Proof. Put $g(y)=\sum_{i=1}^{n}(y^{\alpha_i}+y^{\beta_i})$ for $y \in K$. By Proposition 2, K^* is generated over $\boldsymbol{Q}$ by the elements $g(y)$ for $y \in K$. For any $y \in K$, we see easily $y^{\alpha_1}+y^{\beta_1}=\mathrm{Tr}_{K/F}(y)$, $y^{\alpha_\nu}+y^{\beta_\nu}=\mathrm{Tr}_{K/M}(y)^{\tau_\nu}$ for $\nu>1$, so that

$$g(y) = \mathrm{Tr}_{K/F}(y)+\sum_{\nu=2}^{n}\mathrm{Tr}_{K/M}(y)^{\tau_\nu}.$$

This implies $K^* \subset FM^{**}$. Now take elements z and w so that $F=F_0(z)$, $M=F_0(w)$, $z^2 \in F_0$, $w^2 \in F_0$. If $x \in F_0$, we have

$$g(x) = 2\mathrm{Tr}_{F_0/\boldsymbol{Q}}(x),\ g(xz) = 2xz,\ g(xw) = 2\sum_{\nu=2}^{n}(xw)^{\tau_\nu}.$$

These relations show that K^* contains F and M^{**}; this completes the proof.

Proposition 6. *M^{**} is a totally imaginary quadratic extension of a totally real algebraic number field containing F_0. Moreover, for every $x \in M$, we have $x^{\tau_2} \cdots x^{\tau_n} \in M^{**}$; and for every ideal $\mathfrak{c}$ of M, $\mathfrak{c}^{\tau_2} \cdots \mathfrak{c}^{\tau_n}$ is an ideal of M^{**}.*

Proof. If $x \in F_0$, we have $x=\mathrm{Tr}_{F_0/\boldsymbol{Q}}(x)-\sum_{\nu=2}^{n} x^{\tau_\nu} \in M^{**}$, so that $F_0 \subset M^{**}$. Now let L be the smallest normal extension of $\boldsymbol{Q}$ containing K and G the Galois group of L over $\boldsymbol{Q}$. Denote by H the set of elements $\gamma \in G$ such that $\{\tau_2\gamma, \cdots, \tau_n\gamma\}$ coincides with $\{\tau_2, \cdots, \tau_n\}$ on M as a whole. Then, by the same argument as in the proof of [3, § 8. 3, Prop. 28], we can prove that $H=\{\gamma \in G \mid x^\gamma=x$ for every $x \in M^{**}\}$. Using this fact, the second and last assertions are proved in the same manner as in the proof of [3, § 8. 3, Prop. 28]. Now, by the definition of CM-type, $\tau_2\rho$ does not coincide with any τ_ν on M; so ρ is not contained in H. If we put $H_1=H \cup H\rho$, then H_1 is a subgroup of G on account of Lemma 2. Call M_1 the subfield of L corresponding to H_1 by Galois theory. Then we see easily that M_1 is totally real and M^{**} is a totally imaginary quadratic extension of M_1.

Consider a particular case where F_0 is normal over $\boldsymbol{Q}$. Take an element w of M so that $M=F_0(w)$. Choose $n-1$ elements $x_2, \cdots, x_n$ of F_0 in such a way that $\det(x_\mu^{\tau_\nu})_{\mu,\nu=2,\cdots,n} \neq 0$. We have $\sum_{\nu=2}^{n} x_\mu^{\tau_\nu} w^{\tau_\nu} \in M^{**}$ for every μ, so that $w^{\tau_2}, \cdots, w^{\tau_n}$ are contained in M^{**} since $F_0 \subset M^{**}$. This shows that M^{**} is the composite of $M^{\tau_2}, \cdots, M^{\tau_n}$. We can similarly prove that $F_0 M^*$ is the composite of $M^{\tau_1}, \cdots, M^{\tau_n}$. Now assume that the composite of $M^{\tau_1}, M^{\tau_2}, \cdots, M^{\tau_n}$ is of degree 2^n over F_0. This is the case for example, if there exists a prime ideal $\mathfrak{p}$ of F_0 of absolute degree 1 such that $\mathfrak{p}$ is inertial in M while the conjugates of $\mathfrak{p}$, other than $\mathfrak{p}$ itself, decompose in M. Then, we have $[F_0 M^* : \boldsymbol{Q}] = 2^n \cdot n$, and hence $[M^* : \boldsymbol{Q}] \geqq 2^n$.[2] This gives an example of CM-type $(M : \{\tau_i\})$ such that $[M^* : \boldsymbol{Q}] > [M : \boldsymbol{Q}]$ for the dual $(M^* ; \{\chi_\mu\})$ of $(M ; \{\tau_i\})$. This shows also that the case $[K^* : F] > 2$ may happen.

Coming back to the general case, we get

Proposition 7. *Three CM-types $(F ; \{\sigma_i\})$, $(M ; \{\tau_i\})$, $(K ; \{\alpha_i, \beta_i\})$ being as above, let $(K^* ; \{\varphi_\lambda\})$ be the dual of $(K ; \{\alpha_i, \beta_i\})$. Then, for every positive integer b, the composite of $C_b(M)$ and $C_b(K ; \{\alpha_i, \beta_i\})$ contains the class-field H_b over F corresponding to the ideal group $I_b(F) \cap P_b(K^*)$.*

Proof. Let $\mathfrak{a}$ be an ideal of K. In the same way as in the proof of Proposition 5, we see that

$$(10) \qquad \mathfrak{a}^{\alpha_1}\mathfrak{a}^{\beta_1} \cdots \mathfrak{a}^{\alpha_n}\mathfrak{a}^{\beta_n} = N_{K/F}(\mathfrak{a}) \prod_{\nu=2}^{n} N_{K/M}(\mathfrak{a})^{\tau_\nu} .$$

The composite of $C_b(M)$ and $C_b(K ; \{\alpha_i, \beta_i\})$ is a class-field over K; denote by $\mathfrak{H}$ the corresponding ideal-group. If $\mathfrak{a} \in \mathfrak{H}$, we have $\mathfrak{a}^{\alpha_1}\mathfrak{a}^{\beta_1} \cdots \mathfrak{a}^{\alpha_n}\mathfrak{a}^{\beta_n} \in P_b(K^*)$ and $N_{K/M}(\mathfrak{a}) \in P_b(M)$; so we see that $\prod_{\nu=2}^{n} N_{K/M}(\mathfrak{a})^{\tau_\nu} \in P_b(M^{**})$ in view of Proposition 6. By (10) and by Proposition 5, we have $N_{K/F}(\mathfrak{a}) \in P_b(K^*)$. This shows that $\mathfrak{H}$ is contained in the ideal-group corresponding to the composite of K and H_b; our proposition is thereby proved.

If we put $m=[K^* : F]$, we see easily that

$$P_b(F) \subset I_b(F) \cap P_b(K^*) \subset \{\mathfrak{a} \in I_b(F) \mid \mathfrak{a}^m \in P_b(F)\} .$$

Therefore, the exponent of the Galois group of $C_b(F)/H_b$ is a divisor of $m=[K^* : F]$.

---

2) In reality we can show that $[M^* : \boldsymbol{Q}] = 2^n$.

If we fix M (and hence F_0) and consider M and $C_b(M)$ auxiliary, Proposition 7 may be regarded as a statement concerning the class-fields over the variant field F, which can be obtained by complex multiplication of abelian varieties having a certain overfield K^* of F as endomorphism-algebra.[3] In order to get a more transparent result, we consider a restrictive case.

Proposition 8. *$(M:\{\tau_i\})$ satisfies the condition (A) if and only if $M \supset M^{**}$; and if this is satisfied, we have $M=M^{**}$, $K=K^*$.*

Proof. The first assertion is a direct consequence of (9). If $M \supset M^{**}$, we must have $M=M^{**}$ on account of Proposition 6, so that $K^*=FM=K$ by Proposition 5.

In particular, if M is normal over $\boldsymbol{Q}$, then $(K; \{\alpha_i, \beta_i\})$ satisfies (A); in this case, K is normal over $\boldsymbol{Q}$ if and only if F is normal over $\boldsymbol{Q}$; and if we take as F a non-abelian extension of $\boldsymbol{Q}$ of degree 4, we see easily that $(K; \{\alpha_i, \beta_i\})$ is primitive.

For any totally real algebraic number field F_0, we can find a CM-type $(M; \{\tau_i\})$ such that $[M:F_0]=2$ and $M \supset M^*$. In fact, for any positive integer s, put $M=F_0(\sqrt{-s})$ and define $\tau_1, \cdots, \tau_n$ so that $(\sqrt{-s})^{\tau_\nu}=\sqrt{-s}$. Then it is easy to see $M^*=\boldsymbol{Q}(\sqrt{-s})$.

Theorem 4. *Let F_0 be a totally real algebraic number field of degree $n>1$. Let F and M be distinct totally imaginary quadratic extensions of F_0, and K the composite of F and M. Let $(F; \{\sigma_i\})$ and $(M; \{\tau_i\})$ be CM-types such that σ_1 is the identity on F, τ_1 is the identity on M, and $\sigma_i=\tau_i$ on F_0. Define a CM-type $(K; \{\alpha_i, \beta_i\})$ by the relation (8) with $r=1$. Suppose that $(M; \{\tau_i\})$ satisfies the condition (A) of § 2. Then, for every positive integer b, $C_b(K; \{\alpha_i, \beta_i\})$ contains the class-field $C_b(F/F_0)$ over F.*

Proof. For every ideal $\mathfrak{a}$ of K, the equality (10) is also written in the form

$$(11) \qquad \mathfrak{a}^{\alpha_1}\mathfrak{a}^{\beta_1} \cdots \mathfrak{a}^{\alpha_n}\mathfrak{a}^{\beta_n} = N_{K/F}(\mathfrak{a})N_{K/M}(\mathfrak{a})^{-1} \prod_{i=1}^{n} N_{K/M}(\mathfrak{a})^{\tau_i}.$$

By our assumption and Proposition 8, we have $K=K^*$. Hence, if $\mathfrak{a} \in I_b(K; \{\alpha_i, \beta_i\})$, there exists an element u of K such that

$$\mathfrak{a}^{\alpha_1}\mathfrak{a}^{\beta_1} \cdots \mathfrak{a}^{\alpha_n}\mathfrak{a}^{\beta_n} = (u), \quad N(\mathfrak{a}) = uu^\rho, \quad u \equiv 1 \bmod (b).$$

3) In fact, the abelian varieties belonging to $(K; \{\alpha_i, \beta_i\})$ are special members of an analytic family of polarized abelian varieties whose moduli are given by certain automorphic functions of one variable.

Put $v=N_{K/F}(u)$, $\mathfrak{c}=N_{K/F}(\mathfrak{a})$. Now take $N_{K/F}$ of the both sides of (11). We note that for any ideal $\mathfrak{e}$ of M, $N_{K/F}(\mathfrak{e})=N_{M/F_0}(\mathfrak{e})$; especially,

$$N_{K/F}(N_{K/M}(\mathfrak{a})) = N_{M/F_0}(N_{K/M}(\mathfrak{a})) = N_{K/F_0}(\mathfrak{a}) = N_{F/F_0}(\mathfrak{c}) = \mathfrak{c}\mathfrak{c}^{\rho},$$

and

$$N_{K/F}\left(\prod_{i=1}^{n} N_{K/M}(\mathfrak{a})^{\tau_i}\right) = N_{M/F_0}\left(\prod_{i=1}^{n} N_{K/M}(\mathfrak{a})^{\tau_i}\right) = \prod_{i=1}^{n} N_{K/M}(\mathfrak{a})^{\tau_i} N_{K/M}(\mathfrak{a})^{\tau_i\rho}$$
$$= N_{M/Q}(N_{K/M}(\mathfrak{a})) = N_{K/Q}(\mathfrak{a}) = (uu^{\rho}).$$

Therefore, we obtain from (11), $(v)=\mathfrak{c}^2(\mathfrak{c}\mathfrak{c}^{\rho})^{-1}(uu^{\rho})$. Put $w=v(uu^{\rho})^{-1}$. Then w is an element of F, and $\mathfrak{c}/\mathfrak{c}^{\rho}=(w)$, $ww^{\rho}=1$, $w\equiv 1 \bmod (b)$. Thus we have shown $N_{K/F}[I_b(K;\{\alpha_i,\beta_i\})]\subset I_b(F/F_0)$. This proves our theorem.

By means of Theorem 4, we obtain several assertions concerning the class-fields over F similar to those given in §2. In particular, the absolute class-field $C_1(F)$ is contained in the composite $C_b(K;\{\alpha_i,\beta_i\})$ and $C_b(F_0)$ for a suitable positive integer b. As another example of specializations (or degenerations) of Theorem 4, we get the following conclusion: *F and F_0 being as in Theorem 4, let s be a positive integer such that $\sqrt{-s}\notin F$. Then the field of moduli of a certain polarized abelian variety having $F(\sqrt{-s})$ as endomorphism-algebra, together with the absolute class-field over F_0, generates a class-field over $F(\sqrt{-s})$ containing the absolute class-field over F, if the class-number of F is odd.*

OSAKA UNIVERSITY

(Received March 19, 1962)

References.

[1] H. Hasse: Über die Klassenzahl Abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.
[2] H. Richter: *Über die Lösbarkeit einiger Nicht-Abelscher Einbettungs-probleme*, Math. Ann. **112** (1936), 69–84.
[3] G. Shimura and Y. Taniyama: Complex multiplication of abelian varieties and its applications to number theory, Publications of Math. Soc. Japan, No. **6**, 1961.
[4] Y. Taniyama: *L-functions of number fields and zeta functions of abelian varieties*, J. Math. Soc. Japan **9** (1957), 330–366.
[5] A. Weil: *On a certain type of characters of the idèle-class group of an algebraic number-field*, Proceedings of the International Symposium on Algebraic Number Theory, Tokyo-Nikko, 1955 (1956), 1–7.