J. Math. Soc. Japan
Vol. 15, No. 3, 1963

On the field of moduli of an abelian variety with complex multiplication

Dedicated to Professor Y. Akizuki on his sixtieth birthday

by Koji DOI

(Received Sept. 20, 1962)

The theory of complex multiplication of abelian varieties has been established by A. Weil, G. Shimura, and Y. Taniyama ([3], to be referred as [CM]). The main parts of them, i.e. the so-called construction of class-fields are concerned with simple abelian varieties (primitive CM-type). Naturally as the next step the extension of the theory to the case of composite varieties should be considered.

Along this line we shall begin with a very simple case, assuming the variety to be a direct product $B_1\times\cdots\times B_h$ of simple abelian varieties B_i of the same CM-type. The result of this note consists in Main Theorem of §4 and Corollary to it. Our result implies the

THEOREM. *The field of moduli of the product $B_1\times\cdots\times B_h$ (with respect to any polarization) is contained in the class-field obtained from the field of moduli of the factor B.*

This means that we can not get any different class-field to that of primitive CM-type from such product.

I would like to express my heartfelt gratitude to Prof. Shimura for his kind guidance and criticism during the preparation of this note.

We shall use the same notations and terminologies as in [CM].

§1. Let $(K;\{\varphi_i\})$ be a primitive CM-type and $[K;\boldsymbol{Q}]=2n$. We shall consider a couple (A,θ) formed by an abelian variety A defined over $\boldsymbol{C}$ and an isomorphism θ of K into $\mathcal{A}_0(A)$. Let h be a positive integer. We say that (A,θ) is of type $(K;\{\varphi_i\};h)$ if the following two conditions are satisfied.

(A 1) $\dim A=nh$.

(A 2) For any element $\alpha\in K$, the analytic representation of $\theta(\alpha)$ (cf. [CM; §3.2.]) is equivalent to the diagonal matrix whose diagonal elements are exactly h times $\alpha^{\varphi_1},\cdots,\alpha^{\varphi_n}$. If (A,θ) is of type $(K;\{\varphi_i\};1)$ then (A,θ) is of type $(K;\{\varphi_i\})$ in the sense of [CM, §5.2]. Therefore we put $(K;\{\varphi_i\};1)=(K;\{\varphi_i\})$.

PROPOSITION 1. *If (A,θ) is of type $(K;\{\varphi_i\};h)$, then A is isogenous to a* *product $B\times\cdots\times B$ of h copies of B, where B is a simple abelian variety of type $(K;\{\varphi_i\})$, and there exists an isomorphism ψ of $M_h(K)$ (= the total matric algebra of degree h over K) onto $\mathcal{A}_0(A)$ such that $\psi(\alpha 1_h)=\theta(\alpha)$ for every $\alpha\in K$, where 1_h denotes the identity element of $M_h(K)$.*

PROOF. The first assertion can be proved in the same way as in [CM, §5.1 and §6.1]. Recall that B is simple and $\mathcal{A}_0(B)$ is isomorphic to K if B is of type $(K;\{\varphi_i\})$, since $(K;\{\varphi_i\})$ is primitive. Then the second assertion follows easily from the first assertion.

Generally, let A be an abelian variety defined over $\boldsymbol{C}$. Then we can find a complex torus $\boldsymbol{C}^n/\boldsymbol{D}$ and an analytic isomorphism τ of A onto $\boldsymbol{C}^n/\boldsymbol{D}$. We call the pair $(\boldsymbol{C}^n/\boldsymbol{D},\tau)$ an analytic coordinate system of A (cf. [CM; §3.1]). Let (A,θ) be of type $(K;\{\varphi_i\})$. Put

$$\mathfrak{r}=\theta^{-1}[\mathcal{A}(A)\cap\theta(K)]\,.$$

Take an analytic coordinate system $(\boldsymbol{C}^n/\boldsymbol{D},\tau)$ of A and denote by S the analytic representation of $\mathcal{A}_0(A)$ with respect to τ. Then, we have

$$S(\theta(\alpha))\boldsymbol{D}\subset\boldsymbol{D}\,,$$

for every element α in $\mathfrak{r}$. Hence $\boldsymbol{D}$ is considered as an $\mathfrak{r}$-module.

We shall use the following well-known property in the theory of algebraic number fields.

LEMMA. *Let F be an algebraic number field and $\mathfrak{o}$ be the ring of integers in F. Let $\mathfrak{M}$ be a finitely generated $\mathfrak{o}$-module without torsion. Then*

$$\mathfrak{M}\cong\mathfrak{a}_1\oplus\cdots\oplus\mathfrak{a}_n\cong\mathfrak{o}\oplus\cdots\oplus\mathfrak{o}\oplus\mathfrak{a}_1\cdots\mathfrak{a}_n$$

where $\mathfrak{a}_i$ are ideals of $\mathfrak{o}$. Moreover, in these representations of $\mathfrak{M}$, the number n and the ideal class of an ideal $\mathfrak{a}_1\cdots\mathfrak{a}_n$ are uniquely determined by $\mathfrak{M}$.

For the proof of this lemma, we refer to a more general treatment [**1**; Theorem 2].

By the constructive proof of [CM; Theorem 2 of §6.1 and Theorem 3 of §6.2] and the above lemma, we can get the following proposition immediately, applying Theorem 2 with the $\mathfrak{M}$ of that theorem taken as each of the above direct summands of our $\mathfrak{M}$ in turn.

PROPOSITION 2. *Let the notations and assumptions be the same as in Proposition 1. If $\theta^{-1}[\theta(K)\cap\mathcal{A}(A)]$ coincides with the ring of integers in K, A is isomorphic to a product $B_1\times\cdots\times B_h$, where the B_i are simple abelian varieties of the same type $(K;\{\varphi_i\})$. Moreover, we can take the B_i in such a way that the B_i for $1\leqq i\leqq h-1$ are isomorphic to each other.*

REMARK. We remark that the abelian varieties B_1, B_h in Proposition 2 are *principal* [cf. CM; §7.2 and §7.4]. Hence, by [CM; Proposition 17 of §7.4], there are exactly h_0 (the number of ideal classes in K) abelian varieties such as A in Proposition 2, which are not isomorphic to each other.

§ **2.** In view of [CM; Proposition 26 of § 12.4], we assume that abelian varieties which we shall consider in the following treatment, are defined over an algebraic number field.

PROPOSITION 3. *Let* $(K^*; \{\psi_\alpha\})$ *be the dual of a primitive* CM-*type* $(K; \{\varphi_i\})$ *and* (B, ι) *be a simple abelian variety of type* $(K; \{\varphi_i\})$. *Let* $\mathcal{C}$ *be a polarization of* B *and* k_0 *be the field of moduli of* $(B, \mathcal{C})$. *Then we have*

$$k_0K^* = \text{the field of moduli of } (B, \mathcal{C}, \iota).$$

PROOF. Let k be an algebraic number field of finite degree satisfying the following conditions [CM; § 15]:

i) k is normal over K^*;

ii) B is defined over k;

iii) for every automorphism σ of k over K^*, all the elements of $\mathcal{H}(B, B^\sigma)$ are defined over k;

iv) $\mathcal{C}$ contains a basic polar divisor Y rational over k. Then the field k contains the field of moduli of $(B, \mathcal{C}, \iota)$ and also $k \supset k_0K^*$. Let τ be an isomorphism of k onto a field k', which leaves invariant the elements of the field of moduli of $(B, \mathcal{C}, \iota)$. Then, by [**2**; Proposition 5], $(B, \mathcal{C}, \iota)$ is isomorphic to $(B^\tau, \mathcal{C}^\tau, \iota^\tau)$, i.e. there exists an isomorphism η of B onto B^τ such that

$$\eta^{-1}(Y^\tau) \in \mathcal{C}$$

and

$$\eta \circ \iota(a) = \iota^\tau(a) \circ \eta$$

for every element $a \in \mathfrak{r}$, where $\mathfrak{r} = \iota^{-1}(\mathcal{A}(B))$. Remarking that $K = \boldsymbol{Q}\mathfrak{r}$, we know that τ fixes every element of K^* and also of k_0 by an essential property of fields of definition of (B, ι) [cf. CM; Proposition 31 of § 8.5].

Conversely, let σ be an isomorphism of k which leaves invariant the elements of k_0K^*. Then we can easily see that $(B, \mathcal{C}, \iota)$ is isomorphic to $(B^\sigma, \mathcal{C}^\sigma, \iota^\sigma)$ by the definition of k_0 and [CM; Proposition 1 of § 14.1]. Hence σ fixes every element of the field of moduli of $(B, \mathcal{C}, \iota)$. This completes the proof.

§ **3.** Let (B_1, ι_1) and (B_2, ι_2) be two abelian varieties which are principal and of the same primitive CM-type $(K; \{\varphi_i\})$. Then, by [CM; Proposition 16 of § 7.4.], there exists an isogeny μ of B_1 onto B_2 such that $(B_2, \iota_2; \mu)$ is an $\mathfrak{a}$-transform of (B_1, ι_1) for an integral ideal $\mathfrak{a}$ of K. Let λ be a homomorphism of B_2 onto B_1 such that

$$\lambda \circ \mu = a \circ \delta_{B_1},$$

where a is a positive integer. Let $\mathcal{C}_1$ be a polarization of B_1 and X be a divisor in $\mathcal{C}_1$. Put $\mathcal{C}_2 = \mathcal{C}(\lambda^{-1}(X))$. Put

$$\mathcal{P}_1 = (B_1, \mathcal{C}_1, \iota_1), \qquad \mathcal{P}_2 = (B_2, \mathcal{C}_2, \iota_2).$$

Then it is easy to see that μ is a homomorphism of $\mathcal{P}_1$ onto $\mathcal{P}_2$ and λ is a homomorphism of $\mathcal{P}_2$ onto $\mathcal{P}_1$. Let k_0 be the field of moduli of (B_1, C_1) and $(K^*; \{\psi_\alpha\})$ be the dual of $(K; \{\varphi_i\})$.

PROPOSITION 4. *Notations being as above, if σ is an automorphism of the algebraic closure of $\mathbf{Q}$, which is the identity on k_0K^*, then there exists an isomorphism of $\mathcal{P}_1$ onto $\mathcal{P}_1^\sigma$. Moreover, for every isomorphism η_1 of $\mathcal{P}_1$ onto $\mathcal{P}_1^\sigma$, there exists an isomorphism η_2 of $\mathcal{P}_2$ onto $\mathcal{P}_2^\sigma$ such that*

$$\eta_1 \circ \lambda = \lambda^\sigma \circ \eta_2, \qquad \eta_2 \circ \mu = \mu^\sigma \circ \eta_1 .$$

PROOF. By the same proof of [CM; Proposition 14 of §17.1], we can easily verify the existence of isomorphism η_2.

§4. Now we shall apply these preliminaries to our abelian variety $A = B_1 \times \cdots \times B_h$ (as in Proposition 2), where each simple abelian variety (B_i, ι_i) is principal and of the same primitive CM-type $(K; \{\varphi_i\})$. Let ρ_i be the projection of A onto the i-th factor B_i and ρ_i' the injection of B_i into A. For every element β of $\mathcal{A}_0(A)$, put $\beta_{ij} = \rho_i \circ \beta \circ \rho_j'$. Then $\beta_{ij} \in \mathcal{H}_0(B_j, B_i)$ and β is uniquely determined by the β_{ij}. Therefore we write

$$\beta = (\beta_{ij}) = \begin{pmatrix} \beta_{11} & \cdots & \beta_{1h} \\ \cdots & \cdots & \cdots \\ \beta_{h1} & \cdots & \beta_{hh} \end{pmatrix}.$$

Now we can find easily (cf. CM §14.1 Proposition 1 to construct λ_{ij} satisfying i)–iii)) a system $\{\lambda_{ij};\ 1 \leqq i \leqq h,\ 1 \leqq j \leqq h\}$ with the following properties:

i) for every i and j, λ_{ij} is an element of $\mathcal{H}_0(B_j, B_i)$.

ii) $\lambda_{ij} \circ \iota_j(\alpha) = \iota_i(\alpha) \circ \lambda_{ij}$ for every $\alpha \in K$;

iii) $\lambda_{ij} \circ \lambda_{jk} = \lambda_{ik}$.

It is easy to see that λ_{ii} is the identity element of $\mathcal{A}_0(B_i)$. Fix such a system $\{\lambda_{ij}\}$ and define a mapping θ_0 of the total matric ring $M_h(K)$ of degree h over K to $\mathcal{A}_0(A)$ by

$$\theta_0((\alpha_{ij})) = (\lambda_{ij} \circ \iota_j(\alpha_{ij}))$$

for every $(\alpha_{ij}) \in M_h(K)$. We can easily verify that θ_0 is an isomorphism of $M_h(K)$ onto $\mathcal{A}_0(A)$ by the proof of [CM §14.1 Proposition 1]. Further, if we denote by θ the restriction of θ_0 to K, then (A, θ) is of type $(K; \{\varphi_i\}; h)$.

MAIN THEOREM. *Let $(K^*; \{\psi_\alpha\})$ be the dual of a primitive* CM-*type $(K; \{\varphi_i\})$. Let (A, θ_1) be of type $(K; \{\varphi_i\}; h)$ and $\mathcal{D}$ a polarization of A. Suppose that $\theta_1^{-1}[\theta_1(K) \cap \mathcal{A}(A)]$ is the ring of all integers in K. Let θ be an isomorphism of $M_h(K)$ onto $\mathcal{A}_0(A)$ whose restriction to K coincides with θ_1 (cf. Proposition 1). Let further (B, ι) be a simple abelian variety of type $(K; \{\varphi_i\})$ and $\mathcal{C}$ be a polarization of B. Denote by k_0 the field of moduli of $(B, \mathcal{C})$. Then we have*

$$k_0K^* = \textit{the field of moduli of } (A, \mathcal{D}, \theta).$$

PROOF. We first prove that the field of moduli of $(A, \mathcal{D}, \theta)$ is independent of the choice of a polarization $\mathcal{D}$ of A. Let $\mathcal{D}, \mathcal{D}'$ be two polarizations of A and X, X' be non-degenerate divisors in $\mathcal{D}$ and $\mathcal{D}'$, respectively. Let σ be an automorphism of the algebraic closure of $\boldsymbol{Q}$, which is the identity on the field of moduli of $(A, \mathcal{D}, \theta)$. Then, there exists an isomorphism η of $(A, \mathcal{D}, \theta)$ onto $(A^\sigma, \mathcal{D}^\sigma, \theta^\sigma)$. We shall show that η is also an isomorphism of $(A, \mathcal{D}', \theta)$ onto $(A^\sigma, \mathcal{D}'^\sigma, \theta^\sigma)$. Now define, as usual, the isogeny φ_X of A onto $\hat{A}$ (= the Picard variety of A) by the relation $\varphi_X(u) = Cl(X_u - X)$, for $u \in A$. As $\varphi_X^{-1} \circ \varphi_{X'} \in \mathcal{A}_0(A)$, there exists an element $\alpha \in M_h(K)$ such that

$$\varphi_X^{-1} \circ \varphi_{X'} = \theta(\alpha).$$

Then we have $\varphi_{X'} = \varphi_X \circ \theta(\alpha)$ and $\varphi_{X'}^\sigma = \varphi_X^\sigma \circ \theta^\sigma(\alpha)$. As $\eta^{-1}(X^\sigma) \in \mathcal{D}$, there exist positive integers m and n such that $m \cdot {}^t\eta \circ \varphi_{X^\sigma} \circ \eta = n\varphi_X$. Multiplying this by $\theta(\alpha)$, we get, on account of the relation $\eta \circ \theta(\alpha) = \theta^\sigma(\alpha) \circ \eta$, $m \cdot {}^t\eta \circ \varphi_{X'}^\sigma \circ \eta = n\varphi_{X'}$. Hence we have

$$\eta^{-1}(X'^\sigma) \in \mathcal{D}'.$$

This implies that σ is the identity on the field of moduli of $(A, \mathcal{D}', \theta)$. Repeating the same arguments to the field of moduli of $(A, \mathcal{D}', \theta)$, we see that the field of moduli of $(A, \mathcal{D}', \theta)$ is equal to that of $(A, \mathcal{D}, \theta)$.

Now by Proposition 2, A is expressed in the form

$$A = B_1 \times \cdots \times B_h$$

and we can find an isomorphism ι_j of K onto $\mathcal{A}_0(B_j)$ such that (B_j, ι_j) is of type $(K; \{\varphi_i\})$ for each j. Further, the (B_j, ι_j) are principal. Define an isomorphism θ_0 of $M_h(K)$ onto $\mathcal{A}_0(A)$ using these (B_j, ι_j) and a system $\{\lambda_{ij}\}$ as above. We see easily that $\theta^{-1} \circ \theta_0$ gives an automorphism of $M_h(K)$ onto itself. Restricting this to K, we get an automorphism γ of K. Then we have $\theta_0(\alpha) = \theta(\alpha^\gamma)$ for every $\alpha \in K$. As both (A, θ) and (A, θ_0) belong to $(K; \{\varphi_i\}; h)$, $\{\gamma\varphi_1, \cdots, \gamma\varphi_n\}$ must coincide with $\{\varphi_1, \cdots, \varphi_n\}$ as a whole. Then γ must be the identity mapping of K, since $(K; \{\varphi_i\})$ is primitive [CM; § 8.2, Proposition 26]. It follows that $\theta^{-1} \circ \theta_0(\alpha) = \alpha$ for every $\alpha \in K$. Therefore $\theta^{-1} \circ \theta_0$ is an inner automorphism of $M_h(K)$. Namely, there exists an element ξ of $M_h(K)$ such that $\theta(\alpha) = \theta_0(\xi\alpha\xi^{-1})$ for every $\alpha \in M_h(K)$. Using this fact, we can easily verify that the fields of moduli of $(A, \mathcal{D}, \theta)$ and $(A, \mathcal{D}, \theta_0)$ are the same. Therefore, it is sufficient to show that

$$k_0K^* = \text{the field of moduli of } (A, \mathcal{D}, \theta_0)$$

for a certain polarization $\mathcal{D}$ of A. For every i and j take a positive integer a_{ij} such that $a_{ij} \circ \lambda_{ij} \in \mathcal{H}(B_j, B_i)$. Put then $\mu_{ij} = a_{ij} \circ \lambda_{ij}$. Let $\mathcal{C}_1$ be a polarization of B_1 and X_1 be a divisor in $\mathcal{C}_1$. For every $i > 1$, call $\mathcal{C}_i$ the polarization of B_i containing $\mu_{1i}^{-1}(X_1)$. Then it is easy to see that μ_{ij} is a homomorphism of (B_j, C_j, ι_j) onto (B_i, C_i, ι_i). By Proposition 3, k_0K^* is the field of moduli of (B_i, C_i, ι_i) for every i. Let σ be an automorphism of the algebraic closure of $\boldsymbol{Q}$ which is the identity on k_0K^*. Then there exists an isomorphism η_1 of (B_1, C_1, ι_1) onto $(B_1^\sigma, C_1^\sigma, \iota_1^\sigma)$. By Proposition 4, for each $i>1$, we get an isomorphism η_i of (B_i, C_i, ι_i) onto $(B_i^\sigma, C_i^\sigma, \iota_i^\sigma)$ such that $\eta_i \circ \mu_{i1} = \mu_{i1}^\sigma \circ \eta_1$. Then, by the properties $\lambda_{ij} \circ \lambda_{jk} = \lambda_{ik}$ and $\lambda_{ij} = a_{ij}^{-1}\mu_{ij}$, we see that $\eta_i \circ \lambda_{ij} = \lambda_{ij}^\sigma \circ \eta_j$ for every i and j. Let $\mathcal{D}$ be the polarization of A containing the divisor

$$\sum_{i=1}^{h} B_1 \times \cdots \times B_{i-1} \times X_i \times B_{i+1} \times \cdots \times B_h\,,$$

where X_i is a divisor in C_i for each i. Let $\eta = (\eta_1, \cdots, \eta_h)$ be an isomorphism of A onto A whose restriction to B_i is η_i for every i. Then, by the definition of θ_0 and $\mathcal{D}$, we can easily see that η is an isomorphism of $(A, \mathcal{D}, \theta_0)$ onto $(A^\sigma, \mathcal{D}^\sigma, \theta_0^\sigma)$. Hence σ is the identity on the field of moduli of $(A, \mathcal{D}, \theta_0)$.

Conversely, let σ be an automorphism of the algebraic closure of $\boldsymbol{Q}$ which is the identity on the field of moduli of $(A, \mathcal{D}, \theta_0)$. Then there exists an isomorphism η of $(A, \mathcal{D}, \theta_0)$ onto $(A^\sigma, \mathcal{D}^\sigma, \theta_0^\sigma)$. Put

$$\eta = \begin{pmatrix} \eta_{11}, \cdots, \eta_{1h} \\ \cdots\cdots\cdots\cdots \\ \eta_{h1}, \cdots, \eta_{hh} \end{pmatrix},$$

where η_{ij} is a homomorphism of B_j to B_i. By the definition, η satisfies the relation

$$\eta \circ \theta_0(a) = \theta_0^\sigma(a) \circ \eta$$

for any $\theta_0(a) \in \mathcal{A}(A)$. Let $(x) = (x_1, \cdots, x_h)$ be a generic point of A, then

$$\eta(x) = (\eta_{11}(x_1) + \cdots + \eta_{1h}(x_h), \cdots, \eta_{h1}(x_1) + \cdots + \eta_{hh}(x_h))\,.$$

As a special case, if we take

$$\theta_0(a) = \begin{pmatrix} 0, \cdots, \nu_{1h} \\ 0, \cdots, 0 \\ \cdots\cdots \\ 0, \cdots, 0 \end{pmatrix},$$

where ν_{1h} is an isogeny of B_h to B_1, we have

$$\eta \circ \theta_0(a)(x) = (\eta_{11} \circ \nu_{1h}(x_h), \cdots, \eta_{h1} \circ \nu_{1h}(x_h))\,.$$

On the other hand,

$$\theta_0^\sigma(a) \circ \eta(x) = (\nu_{1h}^\sigma[\eta_{h1}(x_1) + \cdots + \eta_{hh}(x_h)], 0, \cdots, 0)\,.$$

Hence, it follows that

$$\eta_{21} = \eta_{31} = \cdots = \eta_{h1} = 0\,.$$

If we take another set of special endomorphisms such as the above $\theta_0(a)$, we see that

$$\eta_{ij}=0, \qquad \text{for} \qquad i\neq j\,.$$

It follows that η_{ii} is an isomorphism of B_i onto B_i^σ for each i such that

$$\eta_{ii}\circ\iota_i=\iota_i^\sigma\circ\eta_{ii}\,,$$

for $i=1,\cdots,h$. By the choice of the polarization $\mathcal{D}$ of A and the result

$$\eta=\begin{pmatrix}\eta_{ii} & & 0\\ & \ddots & \\ 0 & & \eta_{hh}\end{pmatrix},$$

we can easily see that η_{ii} is an isomorphism of (B_i, C_i, ι_i) onto $(B_i^\sigma, C_i^\sigma, \iota_i^\sigma)$. This proves our main theorem.

COROLLARY. *Notations being as above, k_0K^* contains the field of moduli of $(A, \mathcal{D})$.*

PROOF. This is a direct consequence of the general theory [**2**; Proposition 8].

Osaka University

References

[1] I. Kaplansky, Modules over Dedekind Rings and valuation rings, Trans. Amer. Math. Soc., **72** (1952), 327-340.

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

[3]=[CM] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, no. 6, 1961.