

## STRUCTURE OF COMPLEX TORI WITH THE AUTOMORPHISMS OF MAXIMAL DEGREE

By

Hisao YOSHIHARA

### §0. Introduction.

There is a classical result that an elliptic curve with a non-trivial automorphism is determined uniquely by the automorphism. So that we expect also in higher dimensional cases many automorphisms will affect the structure of the base space. The formulation of this idea is as follows: Let  $T$  be an  $n$ -dimensional complex torus with an automorphism  $\varphi$  and  $A \in GL_n(\mathbb{C})$  be the complex representation of  $\varphi$ . Then  $A\Omega = \Omega N$  for a period matrix  $\Omega$  of  $T$  and  $N \in GL_{2n}(\mathbb{Z})$ . Hence we have

$$\begin{pmatrix} A & 0 \\ 0 & \bar{A} \end{pmatrix} \begin{pmatrix} \Omega \\ \bar{\Omega} \end{pmatrix} = \begin{pmatrix} \Omega \\ \bar{\Omega} \end{pmatrix} N,$$

where  $\bar{\phantom{x}}$  denotes the complex conjugate. Thus all the eigenvalues of  $A$  are units of algebraic number fields of degree  $\leq 2n$ . We shall study here the structure of  $T$  when one of the eigenvalues has the degree  $2n$ . In this case all of them have the degree  $2n$  and let us call  $\varphi$  (or  $A$ ) an *automorphism of degree  $2n$* . The main results are stated in the following section. The author would like to express his hearty thanks to Prof. K. Uchida and Prof. T. Takeuchi for valuable suggestions.

### §1. Statement of main results.

In the sequel we assume that  $\varphi$  has the degree  $2n$  except Lemma 2.1 and Theorem 2.2.

First we fix our notation as follows: We consider only the case  $n \geq 2$ ,  $\{\alpha_1, \dots, \alpha_n\}$ : the eigenvalues of  $A$ ,

$$\begin{aligned} K &= \mathbb{Q}(\alpha_1, \dots, \alpha_n, \bar{\alpha}_1, \dots, \bar{\alpha}_n), \\ G &= \text{Gal}(K/\mathbb{Q}), \end{aligned}$$

$\rho$ : the complex conjugate mapping,

$\varphi_i$ : the isomorphism  $\mathbb{Q}(\alpha_1) \rightarrow \mathbb{Q}(\alpha_i)$  over  $\mathbb{Q}$ , where  $\varphi_i(\alpha_1) = \alpha_i$  ( $i=1, \dots, n$ ),

$S$ : the set of all the elements of  $G$  inducing some  $\varphi_i$  on  $\mathbf{Q}(\alpha_1)$ ,  
 $\mathfrak{S}_m$ : the symmetric group of degree  $m$ ,  
 $\mathfrak{A}_m$ : the alternating group of degree  $m$ ,  
 $e_m = \exp(2\pi\sqrt{-1}/m)$ ,  
 $a(T)$ : the algebraic dimension of  $T$ , i. e.,  $\text{tr. deg. } \mathbf{C}(T)$ , where  $\mathbf{C}(T)$  is the field of meromorphic functions on  $T$ .

In this situation our main results are stated as follows:

**THEOREM I.** *If  $T$  has an automorphism of degree  $2n$ , then  $a(T)=0$  or  $n$ . Suppose further that  $G=\mathfrak{S}_{2n}$  or  $\mathfrak{A}_{2n}$ . Then  $a(T)=0$ .*

**THEOREM II.** *Suppose that  $T$  has an automorphism of degree  $2n$  and  $\mathbf{Q}(\alpha_1)/\mathbf{Q}$  is a Galois extension. Then we have the following when  $n$  is a prime number.*

- (i) *If a 2-Sylow group of  $G$  is normal, then  $a(T)=n$ .*
- (ii) *If a 2-Sylow group of  $G$  is not normal, then  $a(T)=n$  if and only if  $S$  is a subgroup of  $G$ .*

When  $n=2$ , we can state in detail the relation between  $a(T)$  and the structure of  $K$ , that is,

**THEOREM III.** *Let  $D_4$  (resp.  $C_k$ ) be the dihedral group of order 8 (resp. the cyclic group of order  $k$ .) Then*

- (1)  *$a(T)=0$  if and only if (i)  $G=\mathfrak{S}_4$ , or (ii)  $G=\mathfrak{A}_4$ , or (iii)  $G=D_4$  and  $\mathbf{Q}(\alpha_1) \neq \mathbf{Q}(\alpha_2)$ .*
- (2)  *$a(T)=2$  if and only if (iv)  $G=D_4$  and  $\mathbf{Q}(\alpha_1)=\mathbf{Q}(\alpha_2)$ , or (v)  $G=C_2 \times C_2$ , or (vi)  $G=C_4$ .*

Of course there exist many complex tori with each structure of  $K$  listed above. Moreover in case  $a(T)=2$ , we have the following results for the structure of  $T$ .

**THEOREM IV.** *Suppose that  $T$  is a non-simple abelian surface with an automorphism of degree 4. Then  $T$  is isogenous to  $E \times E$ , where  $E$ , is an elliptic curve with a period  $(1, \lambda)$  such that  $\lambda$  is an imaginary quadratic integer  $\text{tr}(A)$  or  $\det(A)$ . On the other hand, suppose that  $T$  is a simple abelian surface with an automorphism of degree 4. Then  $T$  is isogenous to  $V=\mathbf{C}^2/A$ , where*

$$A = \begin{pmatrix} 1 & \zeta & \zeta^2 & \zeta^3 \\ 1 & \zeta^2 & \zeta^4 & \zeta \end{pmatrix}, \quad \zeta = e_5.$$

**THEOREM V.** *Under the same assumption and notation as in the latter part of Theorem IV, suppose further  $|\alpha_i| < 2$  ( $i=1, 2$ ). Then  $T$  is isomorphic to  $V$ .*

This theorem provides an extension of the classical fact for the elliptic curves mentioned in the Introduction. Of course the assumption  $|\alpha_i| < 2$  ( $i=1, 2$ ) is necessary, for we have an example that two distinct simple abelian surfaces have the same automorphism of degree 4 (Remark 3.8). Unfortunately the latter part of Theorem IV cannot be extended to 3-dimensional abelian varieties. Such an example will be given in § 4. By Theorem III, the latter part of Theorem IV is also false when  $T$  is not algebraic.

**§ 2. n-dimensional case.**

Recall that we do not assume that  $\varphi$  has the degree  $2n$  in Lemma 2.1 and Theorem 2.2.

LEMMA 2.1. *Let  $H$  be a dominant Riemann form on  $T$  (Ch. VI, [3]). Then for any Riemann form  $H'$  on  $T$ , there exists a constant  $c > 0$  such that  $cH(z, z) \geq H'(z, z)$  for any  $z \in \mathbb{C}^n$ .*

PROOF. See Ch. VI in [3].

THEOREM 2.2. *Let  $d = \max\{d_i \mid d_i = |\mathbf{Q}(\alpha_i) : \mathbf{Q}|, i=1, \dots, n\}$  and  $r = a(T)$ . Then  $d \leq \max\{2r, 2(n-r)\}$ .*

PROOF. Let  $H$  be a dominant Riemann form on  $T$ , and put  $(A^*H)(z, w) = H(Az, Aw)$ . Then  $A^*H$  is also a Riemann form on  $T$ . Hence  $0 \leq H(Az, Az) \leq cH(z, z)$  for some  $c > 0$ . Thus  $AW = W$ , where  $W$  is the kernel of  $H$ . Taking a suitable basis, we may assume

$$A = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix},$$

where the size of  $A_2$  is  $r$ . Let  $T^*$  be the algebraic reduction of  $T$ . Then it is easy to see that  $A_2$  induces an automorphism of  $T^*$ . This proves the Theorem.

The former part of Theorem I is a corollary of the above Theorem. In what follows we assume that  $\varphi$  has the degree  $2n$ . Then set  $\hat{T} = \mathbb{C}^n / \hat{\Omega}$ , where

$$\hat{\Omega} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{2n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{2n-1} \end{pmatrix}.$$

It is easy to see that  $\hat{T}$  is a finite covering of  $T$ . Hence in particular  $a(\hat{T}) = a(T)$ . Then we have the following

THEOREM 2.3. *If there is a pair  $(i, j)$  such that  $|\mathcal{Q}(\alpha_i, \alpha_j): \mathcal{Q}(\alpha_i)|=2n-1$ , then  $a(T)=0$ .*

PROOF. Suppose  $a(T)=n$ , i. e.,  $a(\hat{T})=n$ . Then there exists an alternating matrix  $C \in GL_{2n}(\mathcal{Q})$  such that  $\hat{\Omega}C^t\hat{\Omega}=0$ . Which implies

$$\sum_{k,m=1}^{2n} c_{km} \alpha_i^{k-1} \alpha_j^{m-1} = 0, \text{ where } C = (c_{km}).$$

Hence

$$\begin{aligned} & \sum_{k < m} c_{km} (\alpha_i \alpha_j)^{k-1} (\alpha_j^{m-k} - \alpha_i^{m-k}) \\ &= (\alpha_j - \alpha_i) \sum_{k < m} c_{km} (\alpha_i \alpha_j)^{k-1} (\alpha_j^{m-k-1} + \alpha_j^{m-k-2} \alpha_i + \dots + \alpha_i^{m-k-1}) \\ &= 0. \end{aligned}$$

Since  $\alpha_j \neq \alpha_i$ , we obtain

$$\sum_{1 \leq k < m \leq 2n} c_{km} (\alpha_j^{m-2} \alpha_i^{k-1} + \alpha_j^{m-3} \alpha_i^k + \dots + \alpha_i^{k-1} \alpha_j^{m-2}) = 0.$$

In this equation the degree of  $\alpha_j$  is at most  $2n-2$ , hence we infer that  $c_{km}=0$  for all  $k, m$ . This is a contradiction. Hence  $a(T) \neq n$ , i. e., we have  $a(T)=0$  by the former part of Theorem I.

The latter part of Theorem I is an easy consequence of the above Theorem.

LEMMA 2.4 (§ 8.1, [2]).  *$(\mathcal{Q}(\alpha_1); \{\varphi_i\})$  is a CM-type if and only if we have  $G = S \cup S\sigma\rho\sigma^{-1}$  and  $S\sigma\rho\sigma^{-1} = \sigma\rho\sigma^{-1}S$  for every  $\sigma \in G$ .*

LEMMA 2.5. *If  $S$  is a subgroup of  $G$ , then  $(\mathcal{Q}(\alpha_1); \{\varphi_i\})$  is a CM-type and hence  $a(T)=n$ .*

PROOF. We have only to check the conditions in the above Lemma. Since  $|G:S|=2$ ,  $S$  is a normal subgroup of  $G$ . Suppose  $S \cap S\sigma\rho\sigma^{-1} \neq \emptyset$  for some  $\sigma \in G$ . Then we get a relation  $\sigma\rho\sigma^{-1} \in S$ , i. e.,  $\rho \in \sigma^{-1}S\sigma = S$ . This is a contradiction, for  $S$  cannot contain  $\rho$ .

Now we proceed to the proof of Theorem II. Suppose that  $\mathcal{Q}(\alpha_1)/\mathcal{Q}$  is a Galois extension and  $n=p$  is a prime number. When  $p=2$ , the assertion is clear. So that we assume  $p \neq 2$ . Then there are exactly  $n$  or one 2-Sylow subgroups in  $G$ . If there is only one 2-Sylow subgroup, then  $\{1, \rho\}$  is the unique 2-Sylow group and hence it is normal, i. e.,  $\sigma\rho = \rho\sigma$  for every  $\sigma \in G$ . Thus  $a(T)=n$  by Lemma 2.4. On the other hand, suppose the 2-Sylow group is not normal. Then  $G$  is generated by  $\rho$  and  $\sigma$ , where  $\sigma^p=1$ ,  $\rho\sigma\rho = \sigma^r$ ,  $r^2 \equiv 1 \pmod{p}$ ,  $r \not\equiv 1 \pmod{p}$ , (Ch. 4, [1]). If  $a(T)=n$ , then  $(\mathcal{Q}(\alpha_1); \{\varphi_i\})$  is a CM-type. By Lemma 2.4, we have  $S\sigma\rho\sigma^{-1}\rho = S$ . Since  $\sigma\rho\sigma^{-1}\rho = \sigma^k$  for  $1 < k < p$  and  $S \ni 1$ , we obtain  $S \ni \sigma^k$ , whence  $S \ni \sigma^{m \cdot k}$  for all  $m$ . As  $\#S=p$ , we conclude that  $S = \{1, \sigma, \dots, \sigma^{p-1}\}$ . By

Lemma 2.5 we have the "only if" part of (ii).

REMARK 2.6. *If the order of  $A$  is finite, then  $G$  is an abelian group. Hence  $a(T)=n$ . As an application of this, we have  $a(T)=n$  if  $|\alpha_i| \leq 1$  for all  $i$ .*

### § 3. 2-dimensional case.

First we shall prove some lemmas.

LEMMA 3.1 (T. Takeuchi). *Let  $F$  be a CM-field of degree 4. If  $F$  has an imaginary unit, then  $F/\mathbf{Q}$  is a Galois extension.*

PROOF. If  $F$  has a non-trivial root of unity, then  $F/\mathbf{Q}$  is a Galois extension. Thus we assume that  $F$  has only trivial roots of unity. In this case the degree of an imaginary unit  $\alpha$  is 4 and  $F=\mathbf{Q}(\alpha)$ . Let  $\varepsilon$  (resp.  $\varepsilon_0$ ) be the fundamental unit of  $F$  (resp.  $F \cap \mathbf{R}$ ). Then  $\alpha = \pm \varepsilon^m$  and  $\varepsilon_0 = \pm \varepsilon^k$  for some integers  $m, k$ . Thus  $\alpha^k$  is real. Now let  $\alpha, \beta, \bar{\alpha}$ , and  $\bar{\beta}$  be the conjugates of  $\alpha$ . Then we see  $(\bar{\alpha}/\alpha)^k = 1$  and so  $\alpha + \bar{\alpha} = 0$ . Similarly  $\beta + \bar{\beta} = 0$ . Therefore, as  $N_{F/\mathbf{Q}}(\alpha) = 1$ , we see  $\alpha\beta = \pm 1$ . Hence  $F/\mathbf{Q}$  is a Galois extension.

LEMMA 3.2. *Under the same assumption and notation as in Lemma 3.1, suppose further that  $F/\mathbf{Q}$  is a cyclic extension. Then  $F = \mathbf{Q}(e_s)$ .*

PROOF. As  $F$  contains no imaginary quadratic elements, it suffices to show that  $F$  has a non-trivial root of unity. Now let  $\sigma$  be a generator of  $\text{Gal}(F/\mathbf{Q})$  and put  $\beta = \sigma(\alpha)$ , where  $\alpha$  is an imaginary unit. Since  $N_{F/\mathbf{Q}}(\alpha) = 1$ , we have  $|\alpha\beta| = |\sigma(\alpha\beta)| = |\sigma^2(\alpha\beta)| = |\sigma^3(\alpha\beta)| = 1$ . Thus  $\alpha\beta$  is a root of unity. If  $\alpha\beta = \pm 1$ , then  $\bar{\alpha} = \sigma^2(\alpha) = \alpha(\beta) = \sigma(\pm 1/\alpha) = \pm 1/\beta = \alpha$ . This contradicts the assumption that  $\alpha$  is an imaginary unit of  $F$ , and we can conclude  $\alpha\beta$  is a non-trivial root of unity.

COROLLARY 3.3. *Let  $F$  be a CM-field of degree 4. If it contains no imaginary quadratic elements and contains an imaginary unit, then  $F = \mathbf{Q}(e_s)$ .*

PROOF. By Lemma 3.1,  $F/\mathbf{Q}$  is a Galois extension of  $\mathbf{Q}$ . Suppose  $\text{Gal}(F/\mathbf{Q}) = C_2 \times C_2$ . Then  $F$  contains an imaginary quadratic subfield. Thus  $\text{Gal}(F/\mathbf{Q})$  has to be cyclic.

Next we consider  $\mathbf{Q}(\alpha_i)$  when  $n=2$ .

LEMMA 3.4. *Suppose that  $n=2$ . Then  $\mathbf{Q}(\alpha)$ ,  $\alpha = \alpha_1$  or  $\alpha_2$ , is a Galois extension over  $\mathbf{Q}$  if and only if  $\mathbf{Q}(\alpha) \ni \bar{\alpha}$ .*

PROOF. If  $\mathcal{Q}(\alpha) \ni \bar{\alpha}$ , then  $\mathcal{Q}(\alpha) \ni k = \mathcal{Q}(\alpha + \bar{\alpha}, \alpha\bar{\alpha}) \neq \mathcal{Q}$ . Since  $k$  is a real quadratic field,  $\mathcal{Q}(\alpha)$  turns out to be a CM-field. Hence  $\mathcal{Q}(\alpha)/\mathcal{Q}$  is a Galois extension by Lemma 3.1.

Now we proceed to the proof of Theorem III. If  $G = \mathfrak{S}_4$ , or  $\mathfrak{A}_4$ , then  $a(T) = 0$  by Theorem I. When  $K$  is of type (iii),  $T$  is not a simple abelian surface owing to Lemma 3.1. Hence suppose that  $T$  is a non-simple abelian surface. Then  $\hat{T}$  which is defined in §2 is also a non-simple abelian surface, i.e.,  $\hat{T}$  is isogeneous to  $E \times E'$ , where  $E$  and  $E'$  are elliptic curves whose period matrices are  $(1, \mu)$  and  $(1, \mu')$  respectively. Hence we have

$$P \begin{pmatrix} 1 & \mu & 0 & 0 \\ 0 & 0 & 1 & \mu' \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 \end{pmatrix} M,$$

where  $P \in GL(2, \mathcal{C})$ ,  $M \in M_4(\mathcal{Z})$ . Thus we have a polynomial  $f(x) \in \mathcal{Z}[x]$  with degree  $\leq 3$  such that  $f(\alpha_1) \neq 0$ ,  ${}^t(f(\alpha_1), f(\alpha_2)) \in \hat{L}$  and  ${}^t(\lambda f(\alpha_1), \lambda f(\alpha_2)) \in \hat{L}$ , where  $\lambda$  is an imaginary number  $\mu$  or  $\mu'$  and  $\hat{L}$  is the lattice generated by the column vectors of  $\hat{\mathcal{Q}}$ . Thus we get  $\lambda \in \mathcal{Q}(\alpha_1) \cap \mathcal{Q}(\alpha_2)$ . Since  $\mathcal{Q}(\alpha_1) \neq \mathcal{Q}(\alpha_2)$ , we have  $\mathcal{Q}(\lambda) = \mathcal{Q}(\alpha_1) \cap \mathcal{Q}(\alpha_2)$ . Then  $\mathcal{Q}(\lambda)$  is an imaginary quadratic field and  $\mathcal{Q}(\lambda) = \mathcal{Q}(\alpha_1 + \bar{\alpha}_2, \alpha_1 \bar{\alpha}_2)$  by Lemma 3.4. As  $\alpha_1$  and  $\bar{\alpha}_2$  are the conjugate of each other over  $\mathcal{Q}(\lambda)$ , the isomorphism  $\alpha_1 \mapsto \alpha_2$  induces the complex conjugate mapping on  $\mathcal{Q}(\lambda)$ . Hence we have  ${}^t(\lambda f(\alpha_1), \bar{\lambda} f(\alpha_2)) \in \hat{L}$ . This means  ${}^t(0, (\lambda - \bar{\lambda})f(\alpha_2)) \in \hat{L}$ . Thus we obtain  $\lambda = \bar{\lambda}$ . This is a contradiction. Consequently  $a(T) = 0$ . Next we consider the case where  $K$  is of type (iv) or (v). Then we infer readily that  $\mathcal{Q}(\alpha_1 + \alpha_2, \alpha_1 \alpha_2)$  is an imaginary quadratic field by Lemma 3.4. Hence  $\alpha_1 \alpha_2 = e_m$ ,  $m = 1, 2, 3, 4$ , or  $6$ . If  $m = 1$  or  $2$ , put  $\lambda = \alpha_1 + \alpha_2$ . If not so, put  $\lambda = \alpha_1 \alpha_2$ . Note that  $\alpha_1 + \alpha_2$  can be expressed like  $h e_m + k$ ,  $h, k \in \mathcal{Z}$  in the latter case. Since  $\lambda$  is an algebraic integer,

$$B = \begin{pmatrix} \alpha_1 + \alpha_2 & \alpha_1 \alpha_2 \\ -1 & 0 \end{pmatrix}$$

defines an automorphism of  $E \times E$ , where  $E = \mathcal{C}/(1, \lambda)$ . Then  $T$  is isogenous to  $E \times E$ , because the eigenvalues of  $B$  are  $\alpha_1, \alpha_2$ . Finally if  $G = C_4$ , then  $K$  is a CM-field. Hence  $a(T) = 2$  by Remark 2.6. Since the Galois group of any irreducible equation of degree 4 with rational coefficients is isomorphic to one of  $\mathfrak{S}_4$ ,  $\mathfrak{A}_4$ ,  $D_4$ ,  $C_2 \times C_2$ , and  $C_4$ , we have proved Theorem III.

COROLLARY 3.5. *Suppose  $T$  has an automorphism  $A$  of degree 4. Then  $T$  is an abelian variety if and only if  $\det(A)$  is a root of unity.*

PROOF. If  $K$  is of type (i), (ii), or (iii), then  $\alpha_1 \bar{\alpha}_1$  is a conjugate of  $\alpha_1 \alpha_2$ .

Thus  $\alpha_1\alpha_2$  is not a root of unity, for we have  $\alpha_1\bar{\alpha}_1 \neq 1$  by Lemma 3.4. By Theorem III, this implies  $a(T)=2$  if  $\det(A)$  is a root of unity. The converse is wellknown.

Now let us consider the structure of the abelian surfaces in detail. The former part of Theorem IV has been proved during the proof of Theorem III. So that we study the structure when  $T$  is simple. Then  $\text{End}_0(T)=K$  is a cyclic extension. Hence  $K=Q(e_s)$  by Lemma 3.2. By the way, we may assume  $A$  and a period matrix  $\Omega$  of  $T$  as follows:

$$A = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}, \quad \Omega = \begin{pmatrix} 1 & \omega_{12} & \omega_{13} & \omega_{14} \\ 1 & \omega_{22} & \omega_{23} & \omega_{24} \end{pmatrix}.$$

Since  $T$  has the automorphism  $A$ , we have  $L \supset \hat{L}$ , where  $L$  is the lattice generated by the column vectors of  $\Omega$ . We also define  $V' = C^2/A'$ , where

$$A' = \begin{pmatrix} 1 & \zeta & \zeta^2 & \zeta^3 \\ 1 & \zeta^3 & \zeta & \zeta^4 \end{pmatrix}.$$

And let  $L_A$  (resp.  $L_{A'}$ ) denote the lattice generated by the column vectors of  $A$  (resp.  $A'$ ). Since  $\{1, \zeta, \zeta^2, \zeta^3\}$  is a basis of algebraic integers of  $Q(\zeta)$ , we have  $L_A \supset \hat{L}$  or  $L_{A'} \supset \hat{L}$ . It is easy to see that  $V$  is isomorphic to  $V'$ . Thus  $\hat{T}$  turns out to be a finite covering of  $V$ . In consequence  $T$  is isogenous to  $V$ . Thus we have proved the latter part of Theorem IV.

REMARK 3.6. *Since  $AL_A=L_A$  or  $AL_{A'}=L_{A'}$ ,  $V$  or  $V'$  has also the automorphism  $A$  when  $T$  is a simple abelian surface.*

Before proceeding to the proof of Theorem V, let us fix some notation. Since  $(1+\sqrt{5})/2$  is a fundamental unit of  $Q(\zeta)$ , we can express as  $\alpha_1 = \zeta^k \{(1+\sqrt{5})/2\}^m$  and  $\alpha_2 = \sigma(\alpha_1)$  for  $\sigma \in \text{Gal}(Q(\zeta)/Q)$ . Then, let us write  $\alpha_1 = \delta_m$ ,  $\alpha_2 = \varepsilon_m$ ,  $A = A_m$  and  $\hat{T} = T_m$  by using suffix  $m$ . In this notation we have the following

THEOREM 3.7. (1) *If two abelian surfrces have the same automorphism  $A_m$  ( $m=0, \pm 1$ ), then they are isomorphic to each other.*

(2) *If  $T_m$  and  $V$  are isomorphic to each other, then  $m=0, \pm 1$ .*

PROOF. Define

$$\Delta(m) = \frac{\Delta(1, \delta_m, \delta_m^2, \delta_m^3)}{\Delta(1, \zeta, \zeta^2, \zeta^3)}.$$

Then  $\Delta(m) = \pm \{u_m^2 + (-1)^m u_m - 1\} / 5$  where  $u_m = \{(1+\sqrt{5})/2\}^{2m} + \{(1-\sqrt{5})/2\}^{2m}$ . Hence we see that  $\Delta(m) = \pm 1$  if and only if  $m=0, \pm 1$ . Thus  $\{1, \delta_m, \delta_m^2, \delta_m^3\}$  is

a basis of algebraic integers of  $K=\mathbf{Q}(\zeta)$  if and only if  $m=0, \pm 1$ . Now, let  $M$  (resp.  $M_m$ ) be the free  $\mathbf{Z}$ -module generated by  $\{1, \omega_{12}, \omega_{13}, \omega_{14}\}$  ( $\{1, \delta_m, \delta_m^2, \delta_m^3\}$ ). Then,  $M$  and  $M_m$  are ideals of  $K$  if  $m=0, \pm 1$ , because  $T$  and  $T_m$  have the same automorphism  $A_m$ . Since the class number of  $K$  is 1, we have  $M=\mu M_m$  for some  $\mu \in K$ . Thus  $L=PL_{T_m}$  for  $P=\mu \dot{+} \sigma(\mu)$ , where  $\dot{+}$  indicates the direct sum of matrices and  $L_{T_m}=L$ . This means that  $T$  and  $T_m$  are isomorphic to each other when  $m=0, \pm 1$ . Next assume that  $T_m$  is isomorphic to  $V$ . Then  $T_m$  has also an automorphism  $B$  of order 5. Since all the elements of  $\text{End}_0(T_m)$  are represented by diagonal matrices, we may assume  $B=\zeta \dot{+} \sigma(\zeta)$  for some  $\sigma \in \text{Gal}(K/\mathbf{Q})$ . Then we have  $L_{T_m}=L_A$ . Whence we obtain  $m=0, \pm 1$ .

Now, let us prove Theorem V. Note that  $|\delta_m| < 2$ ,  $|\varepsilon_m| < 2$  are equivalent to  $m=0, \pm 1$ . Combining Remark 3.6 and Theorem 3.7, (1), we see immediately that  $T_m$  is isomorphic to  $V$  when  $m=0, \pm 1$ .

REMARK 3.8. *Though  $V$  (or  $V'$ ) and  $T_m$  have the same automorphism  $A_m$ , they are not isomorphic to each other when  $|m| \geq 2$ .*

As a result of Theorem V, we have the following

THEOREM 3.9. *Let  $X$  be a simple abelian surface of CM-type. Then  $X$  has a non-trivial automorphism of finite order if and only if  $X$  is isomorphic to  $V$ .*

PROOF. We have only to prove the "only if" part. Since  $F=\text{End}_0(X)$  is a CM-field, it is a Galois extension over  $\mathbf{Q}$  by Lemma 3.1. Referring to 8.4, ([2]), we see  $F/\mathbf{Q}$  has to be a cyclic extension. Then  $F=\mathbf{Q}(\varepsilon_5)$  by Lemma 3.2. Now, let  $m$  be the order of the automorphism. Then we have  $m=3, 4, 5, 6, 8, 10$ , or 12. But  $F$  does not contain any imaginary quadratic elements, so that  $m=5$  or 10. Thus the above Theorem is an easy consequence of Theorem V.

#### § 4. Some examples.

EXAMPLE 4.1. We shall give examples of (iii) and (iv) in Theorem III. Let  $\alpha, \beta$  be the two roots of  $x^2-(1+\sqrt{-1})x+1=0$ . Then, define

$$X_1=\mathbf{C}^2/\left(\begin{array}{cccc} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \beta & \beta^2 & \beta^3 \end{array}\right), X_2=\mathbf{C}^2/\left(\begin{array}{cccc} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \bar{\beta} & \bar{\beta}^2 & \bar{\beta}^3 \end{array}\right).$$

Since  $\alpha\beta=1$  and  $\alpha\bar{\beta}$  is not a root of unity, we have  $a(X_1)=2$  and  $a(X_2)=0$  by Corollary 3.5. Of course  $\text{Gal}(\mathbf{Q}(\alpha, \beta, \bar{\alpha}, \bar{\beta})/\mathbf{Q})=D_4$ .

EXAMPLE 4.2. There is a 3-dimensional simple abelian variety  $T$  such that



it has an automorphism of degree 6, but  $\text{End}_0(T)/\mathbf{Q}$  is not a Galois extension. In fact, let  $a_i$  ( $i=1, 2, 3$ ) be the roots of an equation  $x^3-4x+1=0$ . And let  $K=\mathbf{Q}(\lambda, a_i)$  where  $\lambda=e_3$  or  $e_4$ . Then  $K$  is a non-Galois CM-field. Define embeddings  $\varphi_i: K \hookrightarrow \mathbf{C}$  ( $i=1, 2, 3$ ) as follows  $\varphi_1(\lambda)=\varphi_2(\lambda)=\lambda$ ,  $\varphi_3(\lambda)=\bar{\lambda}$ ,  $\varphi_i(a_1)=a_i$ . Referring to Proposition 26 (Ch. II, [2]), we see that the CM-type  $(K; \{\varphi_1, \varphi_2, \varphi_3\})$  is primitive. Thus, if we put  $T=\mathbf{C}^3/\Omega$  where

$$\Omega = \begin{pmatrix} 1 & a_1\lambda & (a_1\lambda)^2 & \cdots & (a_1\lambda)^5 \\ 1 & a_2\lambda & (a_2\lambda)^2 & \cdots & (a_2\lambda)^5 \\ 1 & a_3\bar{\lambda} & (a_3\bar{\lambda})^3 & \cdots & (a_3\bar{\lambda})^5 \end{pmatrix}.$$

then  $\text{End}_0(T) \cong K$  and  $T$  has an automorphism  $a_1\lambda \dagger a_2\lambda \dagger a_3\bar{\lambda}$ .

### References

- [ 1 ] Hall, M., The theory of groups. Macmillan, 1959.
- [ 2 ] Shimura, G. and Taniyama, Y., Complex multiplication of abelian varieties and its application to number theory. Publ. Math. Soc. Japan 6, Tokyo, (1961).
- [ 3 ] Weil, A., Introduction à l'étude des variétés kähleriennes. Paris, (1958).

Department of Mathematics  
Faculty of General Education  
Niigata University,  
Niigata-shi, 950-21 Japan.