48. *On the Structure of Singular Abelian Varieties*

By Toshiyuki KATSURA

(Comm. by Kunihiko KODAIRA, April 12, 1975)

1. By a singular abelian variety we mean a complex abelian variety of dimension g ($g \geqq 2$) whose Picard number equals the maximum possible number g^2. In this note we prove

Theorem. *A singular abelian variety is isomorphic to a product of mutually isogenous elliptic curves with complex multiplications.*

Let us remark that the following two facts have been known:

(i) A complex abelian variety of dimension g is singular if and only if it is isogenous to a product of g mutually isogenous elliptic curves with complex multiplications (see Mumford [1] and Shioda [2]).

(ii) The theorem is true for the dimension $g=2$ (see Shioda and Mitani [3]).

These facts depend, respectively, on the structure theorem of the endomorphism algebra of abelian varieties and on the analysis of the period map of abelian surfaces. Our proof of the theorem is based on the statements (i), (ii) and proceeds by induction on the dimension g.

2. Let A be a singular abelian variety of dimension g. Since the theorem is true for $g=2$ by (ii), we can assume that it is true for the dimension $\leqq g-1$. In view of (i), there exist g mutually isogenous elliptic curves $E_1, \cdots, E_g$ with complex multiplications and a finite subgroup N of $E_1 \times \cdots \times E_g$ such that

$$A \cong E_1 \times \cdots \times E_g / N. \tag{1}$$

To prove the theorem, we can assume that N is a cyclic group of a prime order, say p. Let

$$a=(a_1, \cdots, a_g), \qquad a_i \in E_i \tag{2}$$

denote a generator of N.

If $a_i=0$ for some i, then the assertion follows from the induction hypothesis. So the idea of the proof is to show that there is an automorphism ψ of $E_1 \times \cdots \times E_g$ such that

$$\psi(a)=(b_1, \cdots, b_g), \quad b_i \in E_i, \quad b_{i_0}=0 \qquad \text{for some } i_0. \tag{3}$$

To carry out this idea we need a few lemmata on elliptic curves.

3. We fix the following notation:

$\boldsymbol{Z}$: the ring of rational integers,

$\boldsymbol{C}$: the field of complex numbers,

$\boldsymbol{F}_p$: a finite field with p elements,

E, E_1, E_2, E_3, etc.: elliptic curves over $\boldsymbol{C}$,

p_E: the multiplication by p on E,

$(E)_p = \mathrm{Ker}\,(p_E)$: the group of points of order p of E; this group can be regarded as a two dimensional vector space over F_p,

$\mathrm{Hom}\,(E_1, E_2)$: the group of homomorphisms of E_1 into E_2.

Furthermore, we denote by r_{ij} the natural homomorphism of $\mathrm{Hom}\,(E_i, E_j)$ into $\mathrm{Hom}\,((E_i)_p, (E_j)_p)$, and by I_{ij} its image. For any $x \in E$, $\langle x \rangle$ denotes the cyclic group generated by x, and $\langle x \rangle^*$ the set of non-zero elements of $\langle x \rangle$.

Lemma 1. *Let E_i and E_j be isogenous elliptic curves with complex multiplications. Then, $\dim_{F_p} I_{ij} = 2$.*

Proof. By the assumption, $\mathrm{Hom}\,(E_i, E_j)$ is a free abelian group of rank 2. An element f of $\mathrm{Hom}\,(E_i, E_j)$ belongs to $\mathrm{Ker}\,(r_{ij})$ if and only if $f = p_{E_j} \circ g$ for some $g \in \mathrm{Hom}\,(E_i, E_j)$. Hence, we have $I_{ij} \cong \mathrm{Hom}\,(E_i, E_j)/p\,\mathrm{Hom}\,(E_i, E_j) \cong (\boldsymbol{Z}/p\boldsymbol{Z})^2$. q.e.d.

Definition. We call $x \in E_1$ *a zero of* $\mathrm{Hom}\,(E_1, E_2)$, if $x \neq 0$ and $f(x) = 0$ for all $f \in \mathrm{Hom}\,(E_1, E_2)$.

Lemma 2. *Let E_1 be isogenous to E_2 with complex multiplication. If there exists a zero $a_1 \in (E_1)_p$ of* $\mathrm{Hom}\,(E_1, E_2)$, *then there exist no zeros of* $\mathrm{Hom}\,(E_2, E_1)$ *in $(E_2)_p$.*

Proof. Suppose there exists a zero of $\mathrm{Hom}\,(E_2, E_1)$ in $(E_2)_p$, say a_2. Choose suitable elements $b_1 \in (E_1)_p$ and $b_2 \in (E_2)_p$ such that $(E_1)_p \cong \langle a_1 \rangle \times \langle b_1 \rangle$ and $(E_2)_p \cong \langle a_2 \rangle \times \langle b_2 \rangle$. Since a_1 is a zero of $\mathrm{Hom}\,(E_1, E_2)$, we have $I_{12} \cong \mathrm{Hom}_{F_p}(\langle b_1 \rangle, (E_2)_p)$ by Lemma 1. So there exists $f \in \mathrm{Hom}\,(E_1, E_2)$ such that

$$f : \begin{cases} a_1 \to 0 \\ b_1 \to b_2. \end{cases} \tag{4}$$

We also have $I_{21} \cong \mathrm{Hom}_{F_p}(\langle b_2 \rangle, (E_1)_p)$. So there exist two homomorphisms $g_i \in \mathrm{Hom}\,(E_2, E_1)$ $(i=1,2)$ such that

$$g_1 : \begin{cases} a_2 \to 0 \\ b_2 \to a_1, \end{cases} \qquad g_2 : \begin{cases} a_2 \to 0 \\ b_2 \to b_1. \end{cases} \tag{5}$$

Thus, we have two endomorphisms $g_i \circ f \in \mathrm{End}\,(E_1)$ $(i=1,2)$ such that

$$g_1 \circ f : \begin{cases} a_1 \to 0 \\ b_1 \to a_1, \end{cases} \qquad g_2 \circ f : \begin{cases} a_1 \to 0 \\ b_1 \to b_1. \end{cases} \tag{6}$$

The matrices associated with $r_{11}(id_{E_1})$, $r_{11}(g_1 \circ f)$, $r_{11}(g_2 \circ f)$ (relative to the basis $\{a_1, b_1\}$) are respectively given as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{7}$$

Hence, $\dim I_{11} \geqq 3$, which contradicts Lemma 1. q.e.d.

Lemma 3. *Let E_1 and E_2 be two elliptic curves, and $a_i \in E_i$ $(i=1,2)$ be two points of order p. Moreover, we assume there exists a homomorphism $f \in$* $\mathrm{Hom}\,(E_1, E_2)$ *such that $f(a_1) \in \langle a_2 \rangle^*$. Then, there exists an automorphism φ of $E_1 \times E_2$ such that $\varphi(a_1, a_2) = (a_1, 0)$.*

Proof. Since $f(a_1) \neq 0$ and $f(a_1) \in \langle a_2 \rangle$, there exists an integer n such that $a_2 = nf(a_1)$. The automorphism φ of $E_1 \times E_2$ defined by

$$(8) \qquad \varphi(x_1, x_2) = (x_1, x_2 - nf(x_1))$$

has the required property. q.e.d.

Lemma 4. *Let E_1, E_2 and E_3 be three elliptic curves, and $a_i \in E_i$ $(i=1,2,3)$ be three points of order p. Moreover, we assume there exist homomorphisms $f_i \in \mathrm{Hom}(E_i, E_3)$ $(i=1,2)$ such that $f_i(a_i)$ $(i=1,2)$ are linearly independent over F_p in $(E_3)_p$. Then, there exists an automorphism ψ of $E_1 \times E_2 \times E_3$ such that $\psi(a_1, a_2, a_3) = (a_1, a_2, 0)$.*

Proof. By the assumption, there exist two integers n_1, n_2 such that $a_3 = n_1 f_1(a_1) + n_2 f_2(a_2)$. Therefore, it is sufficient to define ψ by

$$(9) \qquad \psi(x_1, x_2, x_3) = (x_1, x_2, x_3 - n_1 f_1(x_1) - n_2 f_2(x_2)). \qquad \text{q.e.d.}$$

4. Reduction of the proof of the theorem. We use the same notations as in (1), (2) of 2, and assume $a_i \neq 0$ for $i = 1, 2, \cdots, g$. By Lemma 2, we can assume a_1 is not a zero of $\mathrm{Hom}(E_1, E_2)$, i.e., there exists $f \in \mathrm{Hom}(E_1, E_2)$ such that $f(a_1) \neq 0$. If $f(a_1) \in \langle a_2 \rangle^*$, there exists by Lemma 3 an automorphism $\varphi \times id_{E_3 \times \cdots \times E_g}$ of $E_1 \times \cdots \times E_g$ such that $\varphi \times id_{E_3 \times \cdots \times E_g}(a_1, a_2, \cdots, a_g) = (a_1, 0, a_3, \cdots, a_g)$. Hence, the assertion follows by induction hypothesis. Therefore, we can assume $(E_2)_p \cong \langle a_2 \rangle \times \langle f(a_1) \rangle$.

Applying Lemma 3 or Lemma 4, we can find an automorphism ψ of $E_1 \times \cdots \times E_g$ satisfying the condition (3) of 2 in each of the following cases:

(i) There exists $g \in \mathrm{Hom}(E_2, E_3)$ such that $g(a_2) \in \langle a_3 \rangle^*$.

(ii) There exists $g \in \mathrm{Hom}(E_2, E_3)$ such that $g(f(a_1)) \in \langle a_3 \rangle^*$.

(iii) a_2 is a zero of $\mathrm{Hom}(E_2, E_3)$.

(iv) $f(a_1)$ is a zero of $\mathrm{Hom}(E_2, E_3)$.

(v) There exist two homomorphisms $g_1, g_2 \in \mathrm{Hom}(E_2, E_3)$ such that $g_1(f(a_1))$ and $g_2(a_2)$ are linearly independent in $(E_3)_p$.

For instance, in the case (iii), there exists $g \in \mathrm{Hom}(E_2, E_3)$ such that $g(f(a_1)) = a_3$ by the fact that $I_{23} \cong \mathrm{Hom}(\langle f(a_1) \rangle, (E_3)_p)$. So the assertion follows by Lemma 3. Putting these together, we have only to consider the case satisfying the following two conditions:

(A) For any $g \in \mathrm{Hom}(E_2, E_3)$, neither $g(a_2)$ nor $g(f(a_1))$ is not contained in $\langle a_3 \rangle^*$, and neither a_2 nor $f(a_1)$ is a zero of $\mathrm{Hom}(E_2, E_3)$.

(B) $V = \{g(a) \mid g \in \mathrm{Hom}(E_2, E_3), a \in (E_2)_p\}$ is a one dimensioal linear subspace of $(E_3)_p$.

If there exists $g \in \mathrm{Hom}(E_3, E_2)$ such that $g(a_3) \notin \langle f(a_1) \rangle$, then we have $(E_2)_p \cong \langle f(a_1) \rangle \times \langle g(a_3) \rangle$. So, there exist two integers n_1, n_2 such that $a_2 = n_1 f(a_1) + n_2 g(a_3)$. In this case, the assertion follows by Lemma 4. So we can assume one more condition:

(C) For any $g \in \mathrm{Hom}\,(E_3, E_2)$, we have $g(a_3) \in \langle f(a_1) \rangle$.

5. In this last section, we shall prove that there exists no case satisfying the conditions (A) (B) (C). Let v be a basis of a one dimensional vector space V in (B). Then, $(E_3)_p \cong \langle a_3 \rangle \times \langle v \rangle$. Let g_1, g_2 be two homomorphisms of $\mathrm{Hom}\,(E_2, E_3)$ inducing a basis of I_{23}. By the condition (B), it is easy to see that they can be normalized in the following form:

$$g_1 : \begin{cases} a_2 \quad \to 0 \\ f(a_1) \to k_1 v, \end{cases} \qquad g_2 : \begin{cases} a_2 \quad \to k_2 v \\ f(a_1) \to 0, \end{cases} \tag{10}$$

where k_i $(i=1, 2)$ are non-zero integers.

On the other hand, let h_1, h_2 be two homomorphisms of $\mathrm{Hom}\,(E_3, E_2)$ such that h_i $(i=1, 2)$ inducing a basis of I_{32}. By the condition (C), they can be normalized in the following form:

$$h_1 : \begin{cases} a_3 \to 0 \\ v \to m_1 f(a_1) + m_2 a_2, \end{cases} \qquad h_2 : \begin{cases} a_3 \to n_1 f(a_1) \\ v \to \begin{cases} n_2 a_2 & \text{if } m_1 \neq 0 \\ n_2 f(a_1) & \text{if } m_1 = 0, \end{cases} \end{cases} \tag{11}$$

where m_i $(i=1, 2)$, n_j $(j=1, 2)$ are rational integers and at least one of m_i is not zero.

First, suppose $n_1 \neq 0$. Then, we have an endomorphism $g_1 \circ h_2 \in \mathrm{End}\,(E_3)$ such that

$$g_1 \circ h_2 : \begin{cases} a_3 \to k_1 n_1 v \\ v \to \begin{cases} 0 & \text{if } m_1 \neq 0 \\ k_1 n_2 v & \text{if } m_1 = 0. \end{cases} \end{cases} \tag{12}$$

Moreover, we have an endomorphism of $\mathrm{End}\,(E_3)$ such that

$$g_1 \circ h_1 : \begin{cases} a_3 \to 0 \\ v \to k_1 m_1 v, \end{cases} \quad \text{if } m_1 \neq 0, \tag{13}$$

$$g_2 \circ h_1 : \begin{cases} a_3 \to 0 \\ v \to k_2 m_2 v, \end{cases} \quad \text{if } m_1 = 0.$$

Thus, $\{r_{33}(g_1 \circ h_2), r_{33}(g_1 \circ h_1)\}$ if $m_1 \neq 0$ or $\{r_{33}(g_1 \circ h_2), r_{33}(g_2 \circ h_1)\}$ if $m_1 = 0$ is a basis of two dimensional vector space I_{33}. On the other hand, $id_{E_3} \in \mathrm{End}\,(E_3)$ induces a nontrivial element of I_{33}, and it is clear that the element cannot be expressed by the linear combination of such a basis, which is a contradiction.

Hence, we have $n_1 = 0$. But in this case, a_3 is a zero of $\mathrm{Hom}\,(E_3, E_2)$. Therefore, as before, we have two homomorphisms $h_1', h_2' \in \mathrm{Hom}\,(E_2, E_2)$ such that

$$h_1' : \begin{cases} a_3 \to 0 \\ v \to a_2, \end{cases} \qquad h_2' : \begin{cases} a_3 \to 0 \\ v \to f(a_1). \end{cases} \tag{14}$$

So we have four non-trivial endomorphisms $r_{22}(h_1' \circ g_1)$, $r_{22}(h_2' \circ g_1)$, $r_{22}(h_1' \circ g_2)$, $r_{22}(h_2' \circ g_2)$. The matrices associated with them relative to the basis $\{a_2, f(a_1)\}$ are respectively as follows:

$$
\begin{pmatrix} 0 & k_1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & k_1 \end{pmatrix}, \quad \begin{pmatrix} k_2 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ k_2 & 0 \end{pmatrix}. \tag{15}
$$

They are linearly independent in I_{22}, which contradicts Lemma 1. Hence, there exists no case satisfying the conditions (A) (B) (C), and we complete our proof.

References

[1] D. Mumford: Abelian Variety. Oxford Univ. Press (1970).
[2] T. Shioda: Algebraic Cycles on Certain $K3$ Surfaces in Characteristic p. Proc. Int. Conf. on Manifolds. Tokyo (1973).
[3] T. Shioda and N. Mitani: "Singular abelian surfaces and binary quadratic forms," in Classification of Algebraic Varieties and Compact Complex Manifold, Lecture Notes in Mathematics 412. Berlin-Heidelberg-New York, Springer (1974).