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 $\boldsymbol{C}$,