Some remarks on abelian varieties

Dedicated to Professor Y. Kawada on his 60th birthday

By Tetsuji SHIODA

Introduction. Let us consider the following questions on abelian varieties:

QUESTION 1. *Given an abelian variety A and its abelian subvarieties B_1 and B_2, is it true that*

$$B_1 \cong B_2 \Rightarrow A/B_1 \cong A/B_2 \text{ ?}$$

QUESTION 2. *Let A and A' be abelian varieties of the same dimension defined over an algebraic number field K, and let $A(\mathfrak{p})$ (resp. $A'(\mathfrak{p})$) denote the reduction of A mod $\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ in K. Assume that $A \cong A'$ over an algebraic closure of K. Then, does it follow that $A(\mathfrak{p}) \cong A'(\mathfrak{p})$ for all but a finite number of prime ideals $\mathfrak{p}$?*

In this note we shall show that the answer to both questions is NO! More specifically, we are mainly concerned with 2-dimensional abelian varieties of the form $A=E\times E'$, and consider the following "cancellation problems" for elliptic curves. Let E, E' and E'' be elliptic curves defined over an algebraically closed field k.

QUESTION 3. $E\times E' \cong E\times E'' \Rightarrow E' \cong E''$?

QUESTION 4. $E\times E \cong E\times E'' \Rightarrow E \cong E''$?

Obviously any counterexample to Question 3 or 4 will give one to Question 1. The answer to these questions is summarized in the table:

char (k)	Question 3	Question 4
0 $(k=\boldsymbol{C})$	No	Yes
$p>0$	No	No

As for Question 2, we can also find a counterexample in which A and A' are abelian surfaces of product type. We remark that Question 2 is affirmative in 1-dimensional case (by looking at the absolute invariant), and would be so for higher dimensional case too if there were a nice moduli space for *unpolarized* abelian varieties. Thus the non-validity of Question 2 reflects the fact that there exists no such moduli space, but of course, is not a consequence of this

fact.

The contents of this paper are as follows. In § 1 we show that Question 3 is "generically" true, i.e. under the additional assumption that the Picard number $\rho(E\times E')$ of $E\times E'$ is less than 4. Note that we have (cf. [7] Appendix)

$$\rho(E\times E')=\begin{cases} 2 & E\not\sim E' \\ 3 & E\sim E',\ \mathrm{End}\,(E)\cong \boldsymbol{Z} \\ 4 & E\sim E',\ \mathrm{End}\,(E)\cong \boldsymbol{Z}^2 \\ 6 & E\sim E',\ \mathrm{End}\,(E)\cong \boldsymbol{Z}^4. \end{cases}$$

In § 2 and § 3, we shall construct a counterexample to Question 4 in characteristic $p>0$ by means of supersingular elliptic curves and also one to Question 2. In § 4 we study Question 3 in the complex case by using the theory of singular abelian surfaces [8], and obtain a complete answer (Theorem 4.1). In particular, we show that Question 4 is affirmative in the complex case. Finally we discuss in § 5 a related question on Kummer surfaces, which has motivated the present work.

The author wishes to thank Y. Ihara and T. Katsura for helpful conversations.

Notation. For abelian varieties, we use more or less standard notation (see e.g. [5]): in particular, $\cong$ for isomorphisms, and $\sim$ for isogenies. $A/\langle v\rangle$ denotes the quotient abelian variety of an abelian variety A by the subgroup generated by a point v of finite order on A. $\rho(A)$ denotes the Picard number of A (considered over an algebraically closed field).

§ 1.

First we shall show that Question 3 is "generically" true:

PROPOSITION 1.1. *Let E, E' and E'' be elliptic curves such that $E\times E'\cong E\times E''$. If $\rho(E\times E')\leqq 3$, then E' is isomorphic to E''.*

PROOF. We distinguish the two cases: (i) $\rho(E\times E')=2$ and (ii) $\rho(E\times E')=3$. In case (i), E and E' are not isogenous to each other. Then it is easy to see that any elliptic curve lying on $E\times E'$ is isomorphic either to E or to E'. Hence, if $E\times E'\cong E\times E''$, then E'' must be isomorphic to E'.

In case (ii), E, E' and E'' are mutually isogenous and have no complex multiplications. Let $\varphi: E\to E''$ be a fundamental homomorphism, i.e., a generator of $\mathrm{Hom}\,(E, E'')\cong \boldsymbol{Z}$. Similarly we fix fundamental homomorphisms $\psi: E\to E'$ and $\mu: E'\to E''$. Denoting by μ' etc. the transpose of μ etc., we can find a unique integer n such that

(1.1) $$\mu'\circ\varphi=n\psi\,,\qquad \text{i.e.}\quad \begin{array}{ccc} E & \xrightarrow{\varphi} & E'' \\ {\scriptstyle\psi}\downarrow & \curvearrowright & \downarrow{\scriptstyle\mu'} \\ E' & \xrightarrow[n]{} & E' \end{array}$$

Considering the degrees of both sides, we have

(1.2) $$\deg\mu\cdot\deg\varphi=n^2\deg\psi\,.$$

On the other hand, there is an isomorphism $f: E\times E'\simeq E\times E''$, and f and f^{-1} can be expressed as follows:

(1.3) $$f=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix},\qquad f^{-1}=\begin{pmatrix}\alpha_1 & \beta_1\\ \gamma_1 & \delta_1\end{pmatrix},$$

where α, β, γ and δ are respectively homomorphisms $E\to E$, $E'\to E$, $E\to E''$ and $E'\to E''$ and similarly for $\alpha_1,\cdots,\delta_1$. From the relation $f^{-1}\circ f=1$, it follows that

(1.4) $$\gamma_1\beta+\delta_1\delta=1\,.$$

Writing γ_1, β, δ_1 and δ in terms of the fundamental homomorphisms ψ, μ and their transpose, we have from (1.4) that

(1.5) $$(\deg\psi,\ \deg\mu)=1\,.$$

Hence $\deg\psi$ divides $\deg\varphi$ by (1.2). Interchanging the role of φ and ψ, we have then

(1.6) $$\deg\psi=\deg\varphi\,,\qquad \deg\mu=n^2\,.$$

Assume for a moment that the characteristic is 0. We claim that $\operatorname{Ker}\varphi\subset\operatorname{Ker}\psi$. In fact, take an element $x\in\operatorname{Ker}\varphi$ and let m be the order of x. Then $\psi(x)$ is a point of E' of order dividing m. Moreover (1.1) shows $n\cdot\psi(x)=\mu'\circ\varphi(x)=0$. But since m and n are relatively prime by (1.5) and (1.6), we conclude that $\psi(x)=0$, i.e., $x\in\operatorname{Ker}\psi$, proving our claim. Therefore it follows from (1.6) that $\operatorname{Ker}\psi=\operatorname{Ker}\varphi$, which proves $E'\cong E''$ (in characteristic 0 case).

In the general case, the above argument shows

$$(\operatorname{Ker}\psi)_{\text{red}}=(\operatorname{Ker}\varphi)_{\text{red}}\,.$$

Then, replacing E by $E/$(this subgroup) in the diagram (1.1), we may assume that both ψ and φ are purely inseparable homomorphisms. Note that n and μ are separable by (1.5) and (1.6). Hence, by the uniqueness of the separable closure in the extension of function fields $k(E)/(n\psi)^*k(E')$, we conclude that $E'\cong E''$. This completes the proof.

§ 2. Our first construction of counterexamples to Question 3 or 4 is based on the following observation. Suppose that we have an elliptic curve E and

two points v, w of E of finite order. Assume that

(i) there exists an automorphism of the abelian surface $E\times E$, sending the point $(v, 0)$ to the point $(0, w)$;

(ii) $E/\langle v\rangle \cong E/\langle w\rangle$.

Then we obtain a counterexample to Question 3:

$$(E/\langle v\rangle)\times E\cong E\times(E/\langle w\rangle) \qquad \text{but} \quad E/\langle v\rangle \ncong E/\langle w\rangle .$$

Moreover, if we have $E/\langle v\rangle\cong E$, then this gives a counterexample to Question 4.

In what follows, we shall show that the above condition (i) is satisfied when E is a *supersingular elliptic curve* in characteristic $p>0$ with suitably chosen points v and w. By definition, we have

$$\operatorname{End}(E)\cong \boldsymbol{Z}^4 . \tag{2.1}$$

Fix a prime number $l\neq p$, and denote by E_l the subgroup of points of order l on E. Then E_l can be considered as a vector space of dimension 2 over the finite field $\boldsymbol{Z}/l\boldsymbol{Z}$:

$$E_l\cong(\boldsymbol{Z}/l\boldsymbol{Z})^2 . \tag{2.2}$$

Since any endomorphism of E induces by restriction one of E_l, we have a natural homomorphism:

$$r: \operatorname{End}(E)\longrightarrow \operatorname{End}(E_l) . \tag{2.3}$$

LEMMA 2.1. *r is a surjective homomorphism.*

PROOF. The kernel of r consists of those endomorphisms φ of E which vanish at all points of order l on E. As is well-known, φ has this property if and only if φ is of the form $\varphi=l\psi$ for some $\psi\in\operatorname{End}(E)$. Hence r induces an injective homomorphism:

$$\bar{r}: \operatorname{End}(E)/l\cdot\operatorname{End}(E)\hookrightarrow \operatorname{End}(E_l) .$$

By (2.1) and (2.2), both groups are vector spaces over $\boldsymbol{Z}/l\boldsymbol{Z}$ of the same dimension 4. Thus $\bar{r}$ is an isomorphism, and hence r is surjective, q. e. d.

LEMMA 2.2. *Let v, w be a basis of E_l over $\boldsymbol{Z}/l\boldsymbol{Z}$. Then there exist φ and $\psi\in\operatorname{End}(E)$ such that*

$$\begin{cases} \varphi(v)=w \\ \varphi(w)=0 \end{cases} \quad \textit{and} \quad \begin{cases} \psi(v)=0 \\ \psi(w)=v . \end{cases} \tag{2.4}$$

PROOF. Obviously we can find endomorphisms φ and ψ of E_l satisfying (2.4). Then we apply Lemma 2.1, q. e. d.

PROPOSITION 2.3. *Let E be a supersingular elliptic curve in characteristic p. Let v, w be a basis of E_l, l being a prime number $\neq p$. Then there exists an*

automorphism f of $E\times E$ such that

$$f((v, 0))=(0, w)\,. \tag{2.5}$$

Furthermore f induces an isomorphism:

$$\bar{f}\colon E/\langle v\rangle\times E \xrightarrow{\sim} E\times E/\langle w\rangle\,. \tag{2.6}$$

PROOF. Let us denote by (x, y) a general point of $A=E\times E$. We consider the automorphisms f_1 and f_2 of A defined by

$$f_1(x, y)=(x, y+\varphi(x))$$

$$f_2(x, y)=(x+\psi(y), y)\,,$$

φ and ψ being as in Lemma 2.2. Since we have

$$f_1(v, 0)=(v, w)=f_2(0, w)\,,$$

the automorphism $f=f_2^{-1}\circ f_1$ of A satisfies (2.5). Consequently we also have (2.6), q. e. d.

REMARK 2.4. For the later use, we remark the following fact. With the same notation as in Proposition 2.3, we assume further that E is defined over a field k such that

(i) the ring $\mathrm{End}_k(E)$ of k-rational endomorphisms of E is of rank 4, and

(ii) the points v and w are k-rational.

Then the automorphism f of $E\times E$ can be chosen to be k-rational. Hence the induced isomorphism $\bar{f}$ of (2.6) is also defined over k.

Indeed, since an element $\varphi\in\mathrm{End}_k(E)$ vanishing on E_l is of the form $\varphi=l\psi$ with some $\psi\in\mathrm{End}_k(E)$, Lemma 2.1 holds good if we replace $\mathrm{End}\,(E)$ by $\mathrm{End}_k(E)$. Thus our assertion is clear from the construction of f in the proof of Proposition 2.3.

§ 3.

Now we consider the elliptic curve

$$E\colon Y^2=X^3-X \tag{3.1}$$

over a field k of characteristic $p\neq 2$, containing a primitive 4-th root of unity $i=\sqrt{-1}$. We take the point at infinity as the origin of group law on E. Then the points

$$v=(0, 0)\,,\qquad w=(1, 0) \tag{3.2}$$

form a basis of the group E_2 of points of order 2. The translation on E by the point v or w is expressed as follows:

$$\begin{aligned}&(X, Y)\longrightarrow(-1/X,\ Y/X^2)\\ &(X, Y)\longrightarrow((X+1)/(X-1),\ -2Y/(X-1)^2)\end{aligned} \tag{3.3}$$

(cf. [6] p. 147). Hence the quotient $E/\langle v\rangle$ and $E/\langle w\rangle$ can be easily determined:

$$E/\langle v\rangle = E' : \ \eta^2=\xi(\xi^2+4) \tag{3.4}$$

$$E/\langle w\rangle = E'' : \ \eta^2=(\xi+1)(\xi^2-4\xi-4), \tag{3.5}$$

together with 2-isogenies of E to E' or to E'':

$$\begin{cases} \xi=X-X^{-1} \\ \eta=Y(1+X^{-2}) \end{cases} \quad \text{or} \quad \begin{cases} \xi=(X^2+1)(X-1)^{-1} \\ \eta=Y(1-2(X-1)^{-2}) . \end{cases}$$

Moreover the coordinate transformation $\xi=2iX_1$ and $\eta=2(i-1)Y_1$ gives an isomorphism of E' to E over k (since $k\ni i$):

$$E'=E/\langle v\rangle \cong E \quad (\text{over } k). \tag{3.6}$$

Looking at the absolute invariants of E and $E''=E/\langle w\rangle$

$$j(E)=2^6\cdot 3^3, \quad j(E'')=(2\cdot 3\cdot 11)^3, \tag{3.7}$$

we have

$$E\cong E'' \ (\text{over } \bar{k}) \Leftrightarrow p=3 \text{ or } 7, \tag{3.8}$$

where $\bar{k}$ denotes an algebraic closure of k.

On the other hand, it is known (cf. [2]) that

$$E: \text{supersingular} \Leftrightarrow p\equiv 3 \pmod 4. \tag{3.9}$$

In this case, k contains the field $\boldsymbol{F}_{p^2}=\boldsymbol{F}_p(\sqrt{-1})$, and the zeta-function of the elliptic curve E over $\boldsymbol{F}_{p^2}$ is given as follows:

$$Z(E/\boldsymbol{F}_{p^2}, T)=(1+pT)^2/(1-T)(1-p^2T). \tag{3.10}$$

In view of a result of Tate ([9] Theorem 2 (d)), we have then

$$\mathrm{End}_k(E)\supset \mathrm{End}_{\boldsymbol{F}_{p^2}}(E)\cong \boldsymbol{Z}^4. \tag{3.11}$$

Hence, by applying Proposition 2.3 (with $l=2$), Remark 2.4 and (3.6), we obtain the following *counterexample to Question* 4 (in a somewhat refined form):

Example I. Let E and E'' be respectively the elliptic curves (3.1) and (3.5), defined over a field k of characteristic p with $p\equiv 3 \pmod 4$, $p>7$ and $k\ni\sqrt{-1}$. Then we have

$$E\times E\cong E\times E'' \quad (\text{over } k) \tag{3.12}$$

$$E\ncong E'' \quad (\text{over } \bar{k}). \tag{3.13}$$

Next we give a *counterexample to Question* 2:

Example II. Consider the same elliptic curves E and E'' as above over the

quadratic field $K=\boldsymbol{Q}(\sqrt{-1})$, and put

$$A=E\times E, \qquad A'=E\times E''.$$

Then we claim

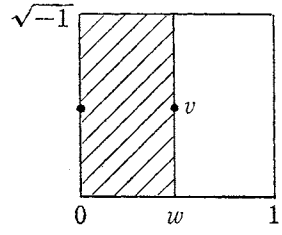
$$A\not\cong A' \quad (\text{over } \boldsymbol{C}), \tag{3.14}$$

$$A \bmod p\cong A' \bmod p \quad (\text{over } \boldsymbol{F}_{p^2}) \tag{3.15}$$

for every p with $p\equiv 3 \pmod 4$.

PROOF. First we note that the elliptic curve E is isomorphic over $\boldsymbol{C}$ to the complex torus $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}\sqrt{-1}$. In view of (3.6), we have

$$E''=E/\langle w\rangle\cong\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}2\sqrt{-1}. \tag{3.16}$$



Therefore A and A' are singular abelian surfaces, which correspond, in the sense of [8] § 3, to the matrices

$$Q_A=\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} \quad \text{and} \quad Q_{A'}=\begin{pmatrix}4 & 0\\ 0 & 4\end{pmatrix}. \tag{3.17}$$

This implies the assertion (3.14). On the other hand, (3.15) was proved in (3.12) of the previous example, because we could take $k=\boldsymbol{F}_{p^2}$ there, q. e. d.

§ 4. In this section we shall consider Question 3 more closely in the complex case. In view of Proposition 1.1, we can assume that $E\times E'$ has Picard number 4. Then E and E' are mutually isogenous elliptic curves, whose endomorphism rings $\mathrm{End}(E)$ and $\mathrm{End}(E')$ are orders of one and the same imaginary quadratic field K:

$$K=\mathrm{End}(E)\otimes\boldsymbol{Q}=\mathrm{End}(E')\otimes\boldsymbol{Q}. \tag{4.1}$$

We fix some notation. For what follows, we refer to [3] § 1 or [1]. We denote by $\mathfrak{O}$ the principal order of K, and by $\mathfrak{O}_f$ the order with conductor f (i. e. the unique subring of $\mathfrak{O}$ with index f). A submodule M of K of rank 2 is called a module of conductor f, or a proper $\mathfrak{O}_f$-ideal, if $\{x\in K;\ xM\subset M\}=\mathfrak{O}_f$. The set of proper $\mathfrak{O}_f$-ideal classes forms a finite abelian group $\mathfrak{I}_f$; its order $h(\mathfrak{O}_f)$ is the class number of $\mathfrak{O}_f$. For two modules M and M' of conductor f

and f', the product module MM' is defined and of conductor (f, f'). Moreover the map $M \to \mathfrak{O}M$ induces a surjective homomorphism of $\mathfrak{I}_f$ to $\mathfrak{I}_1$, whose kernel has the order

$$h(\mathfrak{O}_f)/h(\mathfrak{O}_1)=f[\mathfrak{O}_1^\times : \mathfrak{O}_f^\times]^{-1} \cdot \prod_{p \mid f}\left(1-\frac{\chi(p)}{p}\right). \tag{4.2}$$

Here $\mathfrak{O}_1^\times$ (resp. $\mathfrak{O}_f^\times$) denotes the group of units of $\mathfrak{O}_1$ (resp. $\mathfrak{O}_f$), and $\chi(p)=\left(\frac{K}{p}\right)$ is the Legendre symbol of K.

Now let f (or f') be the conductor of $\mathrm{End}(E)$ (or $\mathrm{End}(E')$):

$$\mathrm{End}(E)=\mathfrak{O}_f, \qquad \mathrm{End}(E')=\mathfrak{O}_{f'}, \tag{4.3}$$

and put $d=\mathrm{g.c.d.}(f, f')$. With these notation, we have

THEOREM 4.1. *Given E and E' as above, the number N of the isomorphism classes of elliptic curves E'' such that*

$$E \times E'' \cong E \times E' \tag{4.4}$$

is finite, and is given by the formula:

$$N=h(\mathfrak{O}_{f'})/h(\mathfrak{O}_d)=(f'/d)\cdot[\mathfrak{O}_d^\times : \mathfrak{O}_{f'}^\times]^{-1} \cdot \prod_{p \mid (f'/d)}\left(1-\frac{\chi(p)}{p}\right). \tag{4.5}$$

PROOF. This follows immediately from the theory of singular abelian surfaces [8], combined with the facts on quadratic fields recalled above. In fact, we can write

$$E=\boldsymbol{C}/M, \qquad E'=\boldsymbol{C}/M' \qquad \text{and} \qquad E''=\boldsymbol{C}/M''$$

with some modules M, M' and M'' in K. By Proposition 4.5 of [8], E'' satisfies (4.4) if and only if

$$MM'' \sim MM' \qquad \text{and} \qquad f''=f',$$

f'' being the conductor of M''. Therefore the number N of E'' satisfying (4.4) is equal to the number of proper $\mathfrak{O}_{f'}$-ideal classes $\{M''\} \in \mathfrak{I}_{f'}$ such that $\{MM''\}$ coincides with the given $\{MM'\} \in \mathfrak{I}_d$. Hence $N=h(\mathfrak{O}_{f'})/h(\mathfrak{O}_d)$, and the other expression of (4.5) follows from (4.2), q. e. d.

COROLLARY 4.2. *Let K be an imaginary quadratic field with discriminant D. Let E and E' be elliptic curves with complex multiplications in K, and let f or f' be the conductor of* $\mathrm{End}(E)$ *or* $\mathrm{End}(E')$. *Then the cancellation*

$$E \times E' \cong E \times E'' \Rightarrow E' \cong E''$$

holds if and only if one of the following conditions is satisfied:

(a) $f' \mid f$,

(b) $f'=2(f, f')$ *and* $D \equiv 1 \pmod 8$

(c) $K=\boldsymbol{Q}(\sqrt{-1})$, $f'\leqq 2$ *and* $(f,f')=1$,

(d) $K=\boldsymbol{Q}(e^{2\pi i/3})$, $f'\leqq 3$ *and* $(f,f')=1$.

PROOF. We have only to determine the case where $N=1$ in (4.5), and the verification is immediate, q. e. d.

THEOREM 4.3. *Question* 4 *is true in the complex case. Namely, for any elliptic curves* E *and* E' *over* $\boldsymbol{C}$, *we have*

$$E\times E\cong E\times E' \Rightarrow E\cong E'.$$

PROOF. If E has no complex multiplications ($\mathrm{End}(E)=\boldsymbol{Z}$), the assertion follows from Proposition 1.1. If E has complex multiplications, this is a special case of Corollary 4.2 (a). In fact, replacing E' and E'' there by E and E', we have $f=f'=d$, q. e. d.

We close this section by writing down an explicit *counterexample to Question* 3 in characteristic 0:

Example III. Denoting by $C(\tau)$ the elliptic curve $\boldsymbol{C}/\boldsymbol{Z}+\boldsymbol{Z}\tau$, we put

$$E=C(\sqrt{-1}),\quad E'=C(3\sqrt{-1})\quad\text{and}\quad E''=C\left(\frac{-1+3\sqrt{-1}}{2}\right).$$

Then we have

$$E\times E'\cong E\times E''\quad\text{but}\quad E'\ncong E''.$$

We note however that the following holds:

$$E\times E'\cong E\times C \Rightarrow C\cong E'\ \text{or}\ E''.$$

§ 5. We shall discuss in this section a related question on Kummer surfaces, which has motivated the present work. In general, let A denote an abelian variety of dimension $g\geqq 2$, defined over an algebraically closed field of characteristic $\neq 2$. The inversion automorphism ι_A of A, defined by $\iota_A(u)=-u$, has the 2^{2g} fixed points which are exactly the points of order 2 of A. The minimal resolution of the quotient variety $A/\langle\iota_A\rangle$ will be called the (desingularized) *Kummer variety* of A, and denoted by $\mathrm{Km}(A)$. Let D_ν denote the 2^{2g} exceptional divisors (all isomorphic to $\boldsymbol{P}^{g-1}$) arising from the resolution. Then the Kummer variety $X=\mathrm{Km}(A)$ has a unique effective canonical divisor K_X for g even:

$$K_X=(g/2-1)D \qquad (D=\sum_{i=1}^{2^{2g}} D_i), \tag{5.1}$$

and a unique effective bicanonical divisor K'_X for any g:

$$K'_X=(g-2)D \qquad (D\ \text{same}) \tag{5.2}$$

(cf. [10] Lemma 16.11.1). Note that, for $g=2$, the Kummer surface $\mathrm{Km}(A)$ is

a $K3$ surface.

QUESTION 5. *Does the Kummer variety* $\mathrm{Km}(A)$ *uniquely determine the abelian variety* A *(up to isomorphisms), i.e.,*

$$\mathrm{Km}(A)\cong\mathrm{Km}(A')\Rightarrow A\cong A'\ ? \tag{5.3}$$

The answer is YES for $g\geqq 3$, but is not completely known for $g=2$ (even in the complex case $k=\boldsymbol{C}$)! Indeed, given a Kummer variety $X=\mathrm{Km}(A)$ of dimension $g\geqq 3$, we can uniquely identify the exceptional divisors D_ν from (5.1) or (5.2), and then the assertion follows from the following proposition:

PROPOSITION 5.1. *Given abelian varieties* A *and* A' *of dimension* $g\geqq 2$ *(char.* $\neq 2$*), we have*

$$A/\langle\iota_A\rangle\cong A'/\langle\iota_{A'}\rangle\Rightarrow A\cong A'\ . \tag{5.4}$$

The proof is based on the fact that the morphism

$$A\xrightarrow{\text{mult. by } 2}A\xrightarrow{\text{can.}}A/\langle\iota_A\rangle \tag{5.5}$$

can be uniquely characterized as the maximal abelian covering of $A/\langle\iota_A\rangle$ of exponent 2, which is ramified exactly at the singular points of $A/\langle\iota_A\rangle$. We omit the detail.

In case $g=2$, the above proof breaks down, because a Kummer surface $\mathrm{Km}(A)$ contains in general an infinite number of non-singular rational curves and hence the exceptional divisors D_ν corresponding to the singular points of $A/\langle\iota_A\rangle$ cannot be identified. Moreover $\mathrm{Km}(A)$ has in general infinitely many automorphisms which are not induced by that of A. (More precisely, the natural inclusion $\mathrm{Aut}(A)/\langle\iota_A\rangle\subset\mathrm{Aut}(\mathrm{Km}(A))$ has in general an *infinite* index.) At any rate, it is known in the complex case that Question 5 is true in the following cases:

(i) $\rho(A)=1$ and A has a principal polarization (Inose),
(ii) $\rho(A)=4$ ([8] Theorem 5.1).

Therefore we expect a positive answer to Question 5 at least for $k=\boldsymbol{C}$.

On the other hand, we suspected that Question 5 might be false in characteristic $p>0$. We knew the following:

(a) The Kummer surface $\mathrm{Km}(E\times E)$, E as in (3.1), is isomorphic to the elliptic modular surface of level 4, B, for any $p\neq 2$ ([7] Theorem 1).

(b) The Kummer surface $\mathrm{Km}(E\times E'')$, E'' as in (3.5), is isomorphic to the Fermat quartic surface $F\colon\sum_{i=1}^{4}x_i^4=0$, for any $p\neq 2$ (cf. [4]).

(c) When $p\equiv 3\pmod 4$, B and F are isomorphic ([7] Theorem 3).

Thus, if Question 4 or 2 in the introduction were *affirmative*, we would have had a "counterexample" of Question 5 in characteristic $p>0$. This observation has motivated our work. In view of Example I in § 3, Question 5 ($g=2$) looks plausible even in characteristic $p>0$ ($p\neq 2$).

References

[1] Borevich, Z. I. and I. R. Shafarevich, Number Theory, Academic Press, 1966.
[2] Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionen-körper, Abh. Math. Sem. Hamburg, **14** (1941), 197-272.
[3] Ihara, Y., Hecke polynomials as congruence ζ functions in elliptic modular case, Ann. of Math., **85** (1967), 267-295.
[4] Mizukami, M., Birational morphisms from certain non-singular quartic surfaces to Kummer surfaces, Master Thesis, University of Tokyo, 1976.
[5] Mumford, D., Abelian Varieties, Oxford Univ. Press, 1970.
[6] Shioda, T., On rational points of the generic elliptic curve, J. Math. Soc. Japan, **25** (1973), 144-157.
[7] Shioda, T., Algebraic cycles on certain $K3$ surfaces in characteristic p, Proc. Int. Conf. on Manifolds (Tokyo 1973), Univ. Tokyo Press, 1975.
[8] Shioda, T. and N. Mitani, Singular abelian surfaces and binary quadratic forms, in "Classification of algebraic varieties and compact complex manifolds", Springer Lecture Notes **412** (1974), 259-287.
[9] Tate, J., Endomorphisms of abelian varieties over finite fields, Inventiones Math., **2** (1966), 134-144.
[10] Ueno, K., Classification theory of algebraic varieties and compact complex spaces, Springer Lecture Notes **439**, 1975.

(Received April 2, 1976)

Department of Mathematics
Faculty of Science
University of Toky
Hongo, Tokyo
113 Japan