J. Math. Soc. Japan
Vol. 17, No. 1, 1965

Existence of curves of genus two on a product of two elliptic curves

To Professor Y. Akizuki for the celebration of his 60th birthday

By Tsuyoshi HAYASHIDA and Mieo NISHI

(Received Sept. 2, 1964)

There have been some fragments asserting that a Riemann matrix of a curve does not decompose into a direct sum. But it seems to the authors that there have been no attempts, as far as they know, to treat the subject rigorously and systematically.

In this paper we shall examine if a product $E\times E'$ of elliptic curves E and E', with rings of endomorphisms isomorphic to the principal order of an imaginary quadratic field $Q(\sqrt{-m})$, can be a Jacobian variety of some curve of genus 2 on $E\times E'$. Rather unexpectedly the following result is obtained: $E\times E'$ can be a Jacobian variety for all values of m except 1, 3, 7 and 15 (cf. paragraph 4, Theorem). In the last paragraph we shall show that there are only a finite number of curves of genus 2 on $E\times E'$ up to isomorphism. In a forthcoming paper it will be shown that the number tends to infinity with m.

Let E and E' be two elliptic curves. We denote by $\mathrm{Hom}(E, E')$ the set of all homomorphisms of E into E'; in particular when $E=E'$, we denote $\mathrm{Hom}(E, E)$ by $\mathfrak{A}(E)$. We put $\mathfrak{A}_0(E)=\mathfrak{A}(E)\otimes Q$, where Q is the field of rational numbers. We denote by Z the ring of rational integers.

§ 1. Preliminaries.

Let $Q(\sqrt{-m})$ be an imaginary quadratic field and $\mathfrak{o}$ its principal order; when $m=0$, we may understand that $Q(\sqrt{-m})$ and $\mathfrak{o}$ coincide with Q and Z respectively. We consider an elliptic curve E for which $\mathfrak{A}_0(E)$ and $\mathfrak{A}(E)$ are isomorphic to $Q(\sqrt{-m})$ and $\mathfrak{o}$ respectively. Since in case $m\neq 0$, $Q(\sqrt{-m})$ has two automorphisms, there are two isomorphisms of $Q(\sqrt{-m})$ on $\mathfrak{A}_0(E)$. We choose and fix one of them, and denote it by ι. We can identify $\mathfrak{A}(E)$ with $\mathfrak{o}$ by ι.

For any finite number of endomorphisms $\lambda_1, \cdots, \lambda_n \in \mathfrak{o}$ of E, $\{\lambda_1, \cdots, \lambda_n\}$ $\neq \{0, \cdots, 0\}$, the correspondence

$$h_{\lambda_1,\cdots,\lambda_n}: E \ni x \to (\lambda_1 x, \cdots, \lambda_n x) \in \overbrace{E\times \cdots \times E}^{n}$$

defines a homomorphism of E into $E\times\cdots\times E$. The image of E by $h_{\lambda_1,\cdots,\lambda_n}$ is an abelian subvariety of dimension 1 on $E\times\cdots\times E$, namely an elliptic curve lying on $E\times\cdots\times E$; we denote it by $E_{\lambda_1,\cdots,\lambda_n}$.

It is clear that translations of $E_{\lambda_1,\cdots,\lambda_n}$ are also elliptic curves on $E\times\cdots\times E$; conversely we have the following

LEMMA 1. *For each elliptic curve E' lying on the product of n copies of E, there exist n endomorphisms $\lambda_1, \cdots, \lambda_n \in \mathfrak{o}$ of E such that E' is a translation of $E_{\lambda_1,\cdots,\lambda_n}$.*

PROOF. E' is a translation of an abelian subvariety of dimension 1 on $E\times\cdots\times E$ (cf. [6], Th. 9); therefore we may assume that E' itself is an abelian subvariety on $E\times\cdots\times E$. We can easily see that E' is isogenous to E; let $\alpha: E\to E'$ be an isogeny. Since E' is a subvariety on $E\times\cdots\times E$, α is a homomorphism of E into $E\times\cdots\times E$ and the image of E by α is E'. Let λ_i be the composed map of α and the projection of $E\times\cdots\times E$ to the i-th factor ($i=1, \cdots, n$). We then have $E'=E_{\lambda_1,\cdots,\lambda_n}$.

For any endomorphism $\alpha\in\mathfrak{o}$ of E, we can consider the following correspondence

$$\alpha^*: E_{\lambda_1,\cdots,\lambda_n} \ni (\lambda_1 x, \cdots, \lambda_n x) \to (\lambda_1\alpha x, \cdots, \lambda_n\alpha x) \in E_{\lambda_1,\cdots,\lambda_n},\ x\in E.$$

Since the ring $\mathfrak{o}$ is commutative, α^* is well-defined and determines an endomorphism of the elliptic curve $E_{\lambda_1,\cdots,\lambda_n}$. It is easily verified that the correspondence

$$\iota^*: \mathfrak{o} \ni \alpha \to \alpha^* \in \mathfrak{A}(E_{\lambda_1,\cdots,\lambda_n})$$

is an injective homomorphism. Now $\mathfrak{A}_0(E_{\lambda_1,\cdots,\lambda_n})$ is isomorphic to $\mathfrak{A}_0(E)$, and consequently to $Q(\sqrt{-m})$; this implies that ι^* is surjective. We may identify $\mathfrak{A}(E_{\lambda_1,\cdots,\lambda_n})$ with $\mathfrak{o}$ by ι^*. Then $h_{\lambda_1,\cdots,\lambda_n}$ is an $\mathfrak{o}$-homomorphism of E on $E_{\lambda_1,\cdots,\lambda_n}$[1].

Now we have the following

PROPOSITION 1. *Let E and E' be elliptic curves whose rings of endomorphisms are both isomorphic to the pricipal order $\mathfrak{o}$ in $Q(\sqrt{-m})$. Suppose that there is a homomorphism h of E onto E'. Then, for each endomorphism γ' of E' (resp. λ of E), we can find an endomorphism γ of E (resp. λ' of E') so that $\gamma' h = h\gamma$ (resp. $\lambda' h = h\lambda$); such an endomorphism is uniquely determined. The correspondence $\gamma'\to\gamma$ (resp. $\lambda\to\lambda'$) gives rise to an isomorphism of rings of endomorphisms of E and of E'. Moreover the above correspondence is independent on the choice of h.*

PROOF. There is a homomorphism h' of E' onto E such that $h'h=n\delta_E$

[1] Then, putting $\mathfrak{a}=(\lambda_1, \cdots, \lambda_n)$, $h_{\lambda_1,\cdots,\lambda_n}$ is an $\mathfrak{a}$-multiplication in [5] (cf. [5], p. 52).

and $hh'=n\delta_{E'}$, where $n=\nu(h)$ and δ_E (resp. $\delta_{E'}$) means the identity map of E (resp. of E'). For given γ', we put $\gamma=\frac{1}{n}h'\gamma'h$. It is easy to show that γ is integral over Z and our assertions follow immediately.

COROLLARY 1. *If we identify $\mathfrak{A}(E_{\lambda_1,\cdots,\lambda_n})$ and $\mathfrak{A}(E_{\mu_1,\cdots,\mu_l})$ with $\mathfrak{o}$ by ι^* respectively, every homomorphism of $E_{\lambda_1,\cdots,\lambda_n}$ on $E_{\mu_1,\cdots,\mu_l}$ is an $\mathfrak{o}$-homomorphism.*

PROOF. Let φ be any homomorphism of $E_{\lambda_1,\cdots,\lambda_n}$ on $E_{\mu_1,\cdots,\mu_l}$. Then $\varphi\circ h_{\lambda_1,\cdots,\lambda_n}$ is a homomorphism of E on $E_{\mu_1,\cdots,\mu_l}$. Since there exists an $\mathfrak{o}$-homomorphism $h_{\mu_1,\cdots,\mu_l}$ of E on $E_{\mu_1,\cdots,\mu_l}$, $\varphi\circ h_{\lambda_1,\cdots,\lambda_n}$ is also an $\mathfrak{o}$-homomorphism by Prop. 1. But the latter fact implies that φ is an $\mathfrak{o}$-homomorphism.

COROLLARY 2. *Assumtions being as in Prop.* 1, *let $\mathfrak{z}$ be the kernel of h. Then we have $\lambda\mathfrak{z}\subset\mathfrak{z}$ for every endomorphism λ of E.*

Starting from $E_{\lambda_1,\cdots,\lambda_n}$ in place of E, we can define $(E_{\lambda_1,\cdots,\lambda_n})_{\mu_1,\cdots,\mu_l}$, where λ_i, μ_j are elements of $\mathfrak{o}$. Then $(E_{\lambda_1,\cdots,\lambda_n})_{\mu_1,\cdots,\mu_l}$ is an elliptic curve $E_{\lambda_1\mu_1,\lambda_2\mu_1,\cdots,\lambda_n\mu_l}$ on the product of nl copies of E.

PROPOSITION 2[2]. $\nu(h_{\lambda_1,\cdots,\lambda_n})=\text{Norm}\,(\lambda_1,\cdots,\lambda_n)$.

PROOF. There exists an ideal $(\mu_1,\cdots,\mu_l)$ in $\mathfrak{o}$ such that $(\lambda_1,\cdots,\lambda_n)(\mu_1,\cdots,\mu_l)=(\gamma)$, $\gamma\in\mathfrak{o}$ and that $(\nu(h_{\lambda_1,\cdots,\lambda_n}),\ N(\mu_1,\cdots,\mu_l))=1$. We consider the homomorphism:

$$h'_{\mu_1,\cdots,\mu_l}:\ E_{\lambda_1,\cdots,\lambda_n}\rightarrow(E_{\lambda_1,\cdots,\lambda_n})_{\mu_1,\cdots,\mu_l}\,.$$

Let k be a field over which E and each endomorphism are defined, and x a generic point of E over k. We can readily see that $k(\lambda_1\mu_1x,\lambda_2\mu_1x,\cdots,\lambda_n\mu_lx)=k(\gamma x)$. This implies that $\nu(h'_{\mu_1,\cdots,\mu_l}\circ h_{\lambda_1,\cdots,\lambda_n})=\nu(\gamma)$; and, since $\nu(\gamma)=N(\gamma)$, we have $\nu(h_{\lambda_1,\cdots,\lambda_n})\nu(h'_{\mu_1,\cdots,\mu_l})=N(\lambda_1,\cdots,\lambda_n)N(\mu_1,\cdots,\mu_l)$. Since $\nu(h_{\lambda_1,\cdots,\lambda_n})$ is prime to $N(\mu_1,\cdots,\mu_l)$, $\nu(h_{\lambda_1,\cdots,\lambda_n})$ divides $N(\lambda_1,\cdots,\lambda_n)$. Quite similarly $\nu(h'_{\mu_1,\cdots,\mu_l})$ also divides $N(\mu_1,\cdots,\mu_l)$. Therefore we have $\nu(h_{\lambda_1,\cdots,\lambda_n})=N(\lambda_1,\cdots,\lambda_n)$.

Let k be a field over which E and each endomorphism of E are defined; let x be a generic point of E over k. If two ideals $(\lambda_1,\cdots,\lambda_n)$, $(\mu_1,\cdots,\mu_l)$ are equal, then $k(\lambda_1x,\cdots,\lambda_nx)=k(\mu_1x,\cdots,\mu_lx)$; and hence $E_{\lambda_1,\cdots,\lambda_n}$ is isomorphic to $E_{\mu_1,\cdots,\mu_l}$. If $\gamma\neq0$ is an element of $\mathfrak{o}$, then γx is also an generic point of E over k; and hence $E_{\lambda_1,\cdots,\lambda_n}$ is equal to $E_{\lambda_1\gamma,\cdots,\lambda_n\gamma}$. We shall prove the following

PROPOSITION 3. $\text{Hom}\,(E_{\lambda_1,\cdots,\lambda_n},E_{\mu_1,\cdots,\mu_l})$ *is canonically isomorphic to* $(\lambda_1,\cdots,\lambda_n)(\mu_1,\cdots,\mu_l)^{-1}$ *as $\mathfrak{o}$-modules. Moreover, if $h\in\text{Hom}\,(E_{\lambda_1,\cdots,\lambda_n},E_{\mu_1,\cdots,\mu_l})$ corresponds to $\alpha\in(\lambda_1,\cdots,\lambda_n)(\mu_1,\cdots,\mu_l)^{-1}$ by this isomorphism, then $\nu(h)=N\alpha\cdot N(\mu_1,\cdots,\mu_l)/N(\lambda_1,\cdots,\lambda_n)$.*

PROOF. We can find an element γ in $\mathfrak{o}$ and an ideal $(\beta_1,\cdots,\beta_s)$ so that $(\lambda_1,\cdots,\lambda_n)(\beta_1,\cdots,\beta_s)=(\gamma\mu_1,\cdots,\gamma\mu_l)$. We put $E_{\lambda_1,\cdots,\lambda_n}=E'$. Then the correspondence: $(\gamma\mu_1x,\cdots,\gamma\mu_lx)\rightarrow(\beta_1(\lambda_1x,\cdots,\lambda_nx),\cdots,\beta_s(\lambda_1x,\cdots,\lambda_nx))$, $x\in E$, defines

[2] Prop. 2 is a special case of Prop. 10, Chap. II in [5]. For the convenience of readers we reproduce the proof here.

an isomorphism φ of $E_{\gamma\mu_1,\cdots,\gamma\mu_l}$ on $E'_{\beta_1,\cdots,\beta_s}$. Now let h be a homomorphism: $E_{\lambda_1,\cdots,\lambda_n}\ni(\lambda_1x,\cdots,\lambda_nx)\to(\gamma\mu_1x',\cdots,\gamma\mu_lx')\in E_{\gamma\mu_1,\cdots,\gamma\mu_l}$. Then $\varphi\circ h$ is a homomorphism of E' into $E'\times\cdots\times E'$; and the composed map of $\varphi\circ h$ and the projection of $E'\times\cdots\times E'$ to the j-th factor gives rise to an endomorphism $\alpha_j\in\mathfrak{o}$ of E'. We have $\beta_j(\lambda_1x',\cdots,\lambda_nx')=\alpha_j(\lambda_1x,\cdots,\lambda_nx)$ $(j=1,\cdots,s)$. This determines an element $\alpha'\in(\beta_1,\cdots,\beta_s)^{-1}$ such that $\alpha'\beta_j=\alpha_j$ $(j=1,\cdots,s)$. Thus we have $\varphi\circ h(\lambda_1x,\cdots,\lambda_nx)=(\alpha'\beta_1(\lambda_1x,\cdots,\lambda_nx),\cdots,\alpha'\beta_s(\lambda_1x,\cdots,\lambda_nx))$; hence $h(\lambda_1x,\cdots,\lambda_nx)=(\alpha'\gamma\mu_1x,\cdots,\alpha'\gamma\mu_lx)$. We put $\alpha=\alpha'\gamma$; then $\alpha\in(\lambda_1,\cdots,\lambda_n)(\mu_1,\cdots,\mu_l)^{-1}$ and $h(\lambda_1x,\cdots,\lambda_nx)=(\alpha\mu_1x,\cdots,\alpha\mu_lx)$. Conversely it is clear that any element $\alpha\in(\lambda_1,\cdots,\lambda_n)(\mu_1,\cdots,\mu_l)^{-1}$ gives a homomorphism of $E_{\lambda_1,\cdots,\lambda_n}$ in $E_{\mu_1,\cdots,\mu_l}$ in the manner described above.

The rest of our proposition follows immediately from Prop. 2.

COROLLARY. *$E_{\lambda_1,\cdots,\lambda_n}$ is isomorphic to $E_{\mu_1,\cdots,\mu_l}$ if and only if there exists an element $\alpha\in Q(\sqrt{-m})$ such that* .

$$(\lambda_1,\cdots,\lambda_n)=\alpha(\mu_1,\cdots,\mu_l)\qquad[\text{ideals}].$$

PROOF[3]. "If" part is obvious. Let us consider the converse. We suppose that there exists an isomorphism h of $E_{\lambda_1,\cdots,\lambda_n}$ to $E_{\mu_1,\cdots,\mu_l}$; we take $\alpha\in(\lambda_1,\cdots,\lambda_n)(\mu_1,\cdots,\mu_l)^{-1}$ which corresponds to h by the canonical isomorphism given in Prop. 3. Then we see that $N\alpha N(\mu_1,\cdots,\mu_l)=N(\lambda_1,\cdots,\lambda_n)$. Whence we obtain $\alpha(\mu_1,\cdots,\mu_l)=(\lambda_1,\cdots,\lambda_n)$.

PROPOSITION 4. *(In this Proposition we assume that $m\neq 0$.) Let E and E' be elliptic curves whose rings of endomorphisms are both isomorphic to the principal order $\mathfrak{o}$ in $Q(\sqrt{-m})$. We suppose that there is a homomorphism h of E onto E'. Then there exist a finite number of endomorphisms $\alpha_1,\cdots,\alpha_n\in\mathfrak{o}$ of E such that E' is isomorphic to $E_{\alpha_1,\cdots,\alpha_n}$.*

PROOF. By Prop. 1 we can identify $\mathfrak{o}$ with $\mathfrak{A}(E)$ and $\mathfrak{A}(E')$ respectively so that h is an $\mathfrak{o}$-homomorphism of E on E'. Then, in case that h is separable, we can apply Prop. 23 of [**5**]. On the other hand, when the characteristic p of our geometry is positive, the correspondence: $x\to x^p$ is an automorphism of the universal domain; this defines the *"p-th power"* E^p of E. According to Deuring [**1**] (pp. 219-220), we see that there is an ideal $\mathfrak{z}=(\lambda_1,\cdots,\lambda_l)$ in $\mathfrak{o}$ such that E^p is isomorphic to $E_{\lambda_1,\cdots,\lambda_l}$. Combining these facts and noticing the statement before Prop. 2, we can obtain our assertion.

It is well known that each ideal in $\mathfrak{o}$ can be generated by at most two elements; if $(\lambda_1,\cdots,\lambda_n)=(\alpha_1,\alpha_2)$, then $E_{\lambda_1,\cdots,\lambda_n}$ is isomorphic to E_{α_1,α_2}. Let τ be an homomorphism of E into E_{α_1,α_2}. Then, by Prop. 3, we can find an element $\gamma\in(\alpha_1,\alpha_2)^{-1}$ so that τ is given by the correspondence

$$\tau:\ E\ni x\to((\gamma\alpha_1)x,(\gamma\alpha_2)x)\in E_{\alpha_1,\alpha_2}\,.$$

[3] For another proof we can apply Cor. 1 of our Prop. 1 and [**5**], Prop. 14.

Now we consider an product $E\times E_{\alpha_1,\alpha_2}$. If $\lambda\in\mathfrak{o}$ and $\mu\in(\alpha_1, \alpha_2)^{-1}$, then $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ is an elliptic curve lying on $E\times E_{\alpha_1,\alpha_2}$. The above discussion enables us to show the following

LEMMA 1′. *For each elliptic curve E' lying on $E\times E_{\alpha_1,\alpha_2}$, there exist two elements $\lambda\in\mathfrak{o}$ and $\mu\in(\alpha_1, \alpha_2)^{-1}$ such that E' is a translation of $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$.*

Proof is similar to that of Lemma 1.

In order to calculate intersection numbers of divisors on $E\times E_{\alpha_1,\alpha_2}$ we need some lemmas[4].

LEMMA 2. *Let $\alpha, \beta, \gamma, \delta$ be endomorphisms of E, and k a field over which $\alpha, \beta, \gamma, \delta$ are defined; x and y be independent generic points of E over k. Assume that $\alpha\delta-\beta\gamma\neq 0$. Then*

$$[k(x, y): k(\alpha x+\gamma y, \beta x+\delta y)]=N(\alpha\delta-\beta\gamma).$$

PROOF. First we suppose that $\delta\neq 0$. We calculate the degree of the extension $k(x, y)$ over $k((\alpha\delta-\beta\gamma)x, \beta x+\delta y)$ in two ways. Noticing that $k(x, \delta y)=k(x, \beta x+\delta y)$, we have

$$\begin{aligned}&[k(x, y): k((\alpha\delta-\beta\gamma)x, \beta x+\delta y)]\\ &=[k(x, y): k(x, \delta y)][k(x, \beta x+\delta y): k((\alpha\delta-\beta\gamma)x, \beta x+\delta y)]\\ &=N\delta N(\alpha\delta-\beta\gamma)\end{aligned}$$

in one way. On the other hand, if we put $\alpha x+\gamma y=u$ and $\beta x+\delta y=v$, then $\delta u-\gamma v=(\alpha\delta-\beta\gamma)x$; noticing $k(\delta u-\gamma v, v)=k(\delta u, v)$, we have

$$\begin{aligned}&[k(x, y): k((\alpha\delta-\beta\gamma)x, \beta x+\delta y)]\\ &=[k(x, y): k(\delta u-\gamma v, v)]\\ &=[k(x, y): k(u, v)][k(u, v): k(\delta u, v)]\\ &=[k(x, y): k(u, v)]N\delta.\end{aligned}$$

Since $N\delta\neq 0$, by comparing these two equalities, we obtain our assertion.

If $\delta=0$, then $\gamma\neq 0$ and we can take γ in place of δ.

In what follows the symbol (X, Y) means the intersection number of divisors X and Y on $E\times E_{\alpha_1,\alpha_2}$.

LEMMA 3. $(E_{\lambda,\mu\alpha_1,\mu\alpha_2}, E_{\xi,\eta\alpha_1,\eta\alpha_2})=\dfrac{N(\lambda\eta-\mu\xi)N(\alpha_1, \alpha_2)}{N(\lambda, \mu\alpha_1, \mu\alpha_2)N(\xi, \eta\alpha_1, \eta\alpha_2)}$

PROOF. Since $E_{\lambda_1,\cdots,\lambda_n}=E_{\gamma\lambda_1,\cdots,\gamma\lambda_n}$ for any $\gamma\neq 0$, $\gamma\in\mathfrak{o}$, we may assume that λ, μ (resp. ξ, η) in this formula are elements of $\mathfrak{o}$, multiplying λ, μ (resp. ξ, η) by a suitable non-zero element of $\mathfrak{o}$ if necessary.

Let x and y be independent generic points of E over k, where k is a field over which endomorphisms $\alpha_1, \alpha_2, \lambda, \mu, \xi, \eta$ are defined. If $\lambda\eta-\mu\xi=0$, then

[4] Only Lemmas 2 and 3 are needed, and Propositions 5—9 are not necessary for this object.

$E_{\lambda,\mu\alpha_1,\mu\alpha_2}=E_{\xi,\eta\alpha_1,\eta\alpha_2}$ and our formula clearly holds. Hence we may assume $\lambda\eta-\mu\xi\neq 0$; then we know by Lemma 2 that $\lambda x+\xi y$ and $\mu x+\eta y$ are algebraically independent over k. We have (cf. [6], Th. 4, Cor. 2)

$$\begin{aligned}&(E_{\lambda,\mu\alpha_1,\mu\alpha_2},\ E_{\xi,\eta\alpha_1,\eta\alpha_2})\\ &=[k(\lambda x,\ \mu\alpha_1 x,\ \mu\alpha_2 x,\ \xi y,\ \eta\alpha_1 y,\ \eta\alpha_2 y):k(\lambda x+\xi y,\ \alpha_1(\mu x+\eta y),\ \alpha_2(\mu x+\eta y))]\\ &=\frac{[k(x,y):k(\lambda x+\xi y,\ \mu x+\eta y)][k(u):k(\alpha_1 u,\ \alpha_2 u)]}{[k(x):k(\lambda x,\ \mu\alpha_1 x,\ \mu\alpha_2 x)][k(y):k(\xi y,\ \eta\alpha_1 y,\ \eta\alpha_2 y)]}\end{aligned}$$

where $u=\mu x+\eta y$. Since u is a generic point of E over k, our assertion follows immediately from Lemma 2 and Prop. 2.

COROLLARY 1. $(E_{\lambda,\mu},\ E_{\xi,\eta})=\dfrac{N(\lambda\eta-\mu\xi)}{N(\lambda,\mu)N(\xi,\eta)}$.

COROLLARY 2. $E_{\lambda,\mu\alpha_1,\mu\alpha_2}=E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}$ if and only if there exists an element $\gamma\in Q(\sqrt{-m})$ such that $\lambda'=\gamma\lambda$, $\mu'=\gamma\mu$.

Our assertion follows immediately from Lemma 3.

By virtue of Prop. 3, we can see that each endomorphism of $E\times E_{\alpha_1,\alpha_2}$ is given by the correspondence:

$$(x,\ \alpha_1 y,\ \alpha_2 y)\rightarrow(\alpha x+\gamma y,\ \alpha_1(\beta x+\delta y),\ \alpha_2(\beta x+\delta y)),$$

where α and $\delta\in\mathfrak{o}$, $\beta\in(\alpha_1,\alpha_2)^{-1}$, $\gamma\in(\alpha_1,\alpha_2)$. This endomorphism may be expressed by a matrix $\begin{pmatrix}\alpha&\gamma\\ \beta&\delta\end{pmatrix}$.

PROPOSITION 5. $\nu\begin{pmatrix}\alpha&\gamma\\ \beta&\delta\end{pmatrix}=N(\alpha\delta-\beta\gamma)$.

PROOF. Let x and y be independent generic points of E over k, where k is a field over which E and each endomorphism are defined. Then, by definition, the left hand side of our proposition is given by the degree $[k(x,\ \alpha_1 y,\ \alpha_2 y):k(\alpha x+\gamma y,\ \alpha_1\beta x+\alpha_1\delta y,\ \alpha_2\beta x+\alpha_2\delta y)]$. If we multiply this number by $[k(y):k(\alpha_1 y,\ \alpha_2 y)]$ and divide the resulting number by $[k(x):k(\alpha x,\ \beta\alpha_1 x,\ \beta\alpha_2 x)][k(y):k(\gamma y,\ \delta\alpha_1 y,\ \delta\alpha_2 y)]$, then we obtain the intersection number $(E_{\alpha,\beta\alpha_1,\beta\alpha_2},\ E_{\gamma,\delta\alpha_1,\delta\alpha_2})$. Our assertion follows immediately from Lemma 3 and Prop. 2.

COROLLARY. *An endomorphism*

$$\begin{pmatrix}\alpha&\gamma\\ \beta&\delta\end{pmatrix}$$

of $E\times E_{\alpha_1,\alpha_2}$ *is an automorphism if and only if* $\alpha\delta-\beta\gamma$ *is a unit of* $\mathfrak{o}$.

PROPOSITION 6. *For any* $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ *on* $E\times E_{\alpha_1,\alpha_2}$, *there exists an* $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ *such that* $(E_{\lambda,\mu\alpha_1,\mu\alpha_2},\ E_{\xi,\eta\alpha_1,\eta\alpha_2})=1$.

PROOF. By virture of Lemma 3, we have only to show that there exist ξ, $\eta\in\mathfrak{o}$ such that $(\lambda,\ \mu\alpha_1,\ \mu\alpha_2)(\xi,\ \eta\alpha_1,\ \eta\alpha_2)=(\lambda\eta-\mu\xi)(\alpha_1,\ \alpha_2)$. We put $N(\lambda,\ \mu\alpha_1,\ \mu\alpha_2)=n$ and $(\alpha_1,\alpha_2)=\mathfrak{a}$; namely $(\lambda,\ \mu\mathfrak{a})(\bar{\lambda},\ \bar{\mu}\bar{\mathfrak{a}})=(\lambda\bar{\lambda},\ \lambda\bar{\mu}\bar{\mathfrak{a}},\ \bar{\lambda}\mu\mathfrak{a},\ \mu\bar{\mu}\mathfrak{a}\bar{\mathfrak{a}})$

$=(n)$. This means that there exist $\eta\in(\bar{\lambda}, \bar{\mu}\bar{\mathfrak{a}})$ and $\xi\in(\bar{\lambda}\mathfrak{a}, \bar{\mu}\bar{\mathfrak{a}}\mathfrak{a})$ such that $\lambda\eta-\mu\xi=n$. Then we have $(\xi, \eta\mathfrak{a})\subset(\bar{\lambda}, \bar{\mu}\bar{\mathfrak{a}})\mathfrak{a}$ and hence $(\lambda, \mu\mathfrak{a})(\xi, \eta\mathfrak{a})\subset(\lambda\eta-\mu\xi)\mathfrak{a}$. But the relation $(\lambda, \mu\mathfrak{a})(\xi, \eta\mathfrak{a})\supset(\lambda\eta-\mu\xi)\mathfrak{a}$ is obvious. Hence our assertion follows.

REMARK. One can read in our proof that $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ is not unique; and that the ideal class of $(\xi, \eta\alpha_1, \eta\alpha_2)$ is uniquely determined; in fact $(\xi, \eta\alpha_1, \eta\alpha_2)(\lambda, \mu\alpha_1, \mu\alpha_2)\sim(\alpha_1, \alpha_2)$. Then Cor. of Prop. 3 shows that "partners" $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ of $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ are isomorphic to each other.

COROLLARY. *For any $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ on $E\times E_{\alpha_1,\alpha_2}$, there exists an $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ such that $E_{\lambda,\mu\alpha_1,\mu\alpha_2}\times E_{\xi,\eta\alpha_1,\eta\alpha_2}$ is isomorphic to $E\times E_{\alpha_1,\alpha_2}$; moreover the correspondence is given as follows:*

$$E_{\lambda,\mu\alpha_1,\mu\alpha_2}\times E_{\xi,\eta\alpha_1,\eta\alpha_2}\ni(P, Q)\longleftrightarrow P+Q\in E\times E_{\alpha_1,\alpha_2}.$$

PROOF. This Corollary follows immediately from Prop. 6 and [6], Th 4, Cor. 2; namely $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ in Prop. 6 has the desired property.

Here we shall give an example in which the assertion of Prop. 6 can not be generalized to the case of $E\times E'$, where E' is isogenous to E.

EXAMPLE[5]. Let E be an elliptic curve such that the ring of endomorphisms is isomorphic to the ring Z of rational integers. Let q be a prime which is different from the characteristic of our universal domain; then the subgroup of the points of E whose orders are q is a direct sum of cyclic groups $\mathfrak{z}_1$ and $\mathfrak{z}_2$ of orders q. There exist elliptic curves $E_i=E/\mathfrak{z}_i$ and separable homomorphisms $\lambda_i: E\rightarrow E_i=E/\mathfrak{z}_i$ such that the kernels of λ_i are $\mathfrak{z}_i$ $(i=1, 2)$. We can readily see that any homomorphism of E to E_i is written as $n\lambda_i$, where $n\in Z$. From this we can see that any abelian subvariety of dimension 1 on $E_1\times E_2$ is a locus of a point $(m\lambda_1 x, n\lambda_2 x)$, $x\in E$, where $m, n\in Z$ and we may suppose that $(m, n)=1$; we denote it by $E_{m\lambda_1,n\lambda_2}$. We take E_{λ_1,λ_2}. It is easy to see that, for any $E_{m\lambda_1,n\lambda_2}$ $(m\neq n)$, the intersection $E_{\lambda_1,\lambda_2}\cap E_{m\lambda_1\cdot n\lambda_2}$ contains other points than the origin $(0, 0)$.

PROPOSITION 7. *Let $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ and $E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}$ be elliptic curves on $E\times E_{\alpha_1,\alpha_2}$. If there exists an homomorphism φ of $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ onto $E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}$, then φ can be extended to an endomorphism of $E\times E_{\alpha_1,\alpha_2}$.*

PROOF. We take $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ and $E_{\xi',\eta'\alpha_1,\eta'\alpha_2}$ such that $E_{\lambda,\mu\alpha_1,\mu\alpha_2}\times E_{\xi,\eta\alpha_1,\eta\alpha_2}$ and $E_{\lambda'.\mu'\alpha_1,\mu'\alpha_2}\times E_{\xi',\eta'\alpha_1,\eta'\alpha_2}$ are both isomorphic to $E\times E_{\alpha_1,\alpha_2}$. Since $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ is isogenous to $E_{\xi',\eta'\alpha_1,\eta'\alpha_2}$, we can take an homomorphism ψ of $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ onto $E_{\xi',\eta'\alpha_1,\eta'\alpha_2}$. Then we obtain a homomorphism

$$\varphi\times\psi:\ E_{\lambda,\mu\alpha_1,\mu\alpha_2}\times E_{\xi,\eta\alpha_1,\eta\alpha_2}\rightarrow E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}\times E_{\xi',\eta'\alpha_1,\eta'\alpha_2}.$$

Since $E\times E_{\alpha_1,\alpha_2}$ is isomorphic to either of two products, we obtain an extension of φ via. $\varphi\times\psi$.

[5] This example is suggested by our friend S. Koizumi.

PROPOSITION 8. *Let $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ and $E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}$ be elliptic curves on $E\times E_{\alpha_1,\alpha_2}$. If there exists an isomorphism φ of $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ onto $E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}$, then φ can be extended to an automorphism of $E\times E_{\alpha_1,\alpha_2}$.*

PROOF. Our assertion follows from Cor. of Prop. 3, Remark at the end of Prop. 6, Cor. of Prop. 6, and our proof of Prop. 7.

We take a Z-basis (minimal basis) $\{1, \omega\}$ of $\mathfrak{o}$, where $\omega=\sqrt{-m}$ if $m\equiv 1$ or 2 (mod 4) and $\omega=\frac{1}{2}(1+\sqrt{-m})$ if $m\equiv 3$ (mod 4); then each element of $\mathfrak{o}$ can be written uniquely as a linear combination of $1, \omega$ with coefficients in Z. Let $\{\beta_1, \beta_2\}$ be a Z-basis of the ideal $(\alpha_1, \alpha_2)^{-1}$. Then $E_{1,\beta_i\alpha_1,\beta_i\alpha_2}$ are the graphs of homomorphisms: $E\ni x\rightarrow(\beta_i\alpha_1 x, \beta_i\alpha_2 x)\in E_{\alpha_1,\alpha_2}$, $(i=1, 2)$; and $E_{1,0,0}$, E_{0,α_1,α_2} mean $E\times 0$, $0\times E_{\alpha_1,\alpha_2}$ respectively. According to [6], Th. 22, we know that each divisor X on $E\times E_{\alpha_1,\alpha_2}$ is algebraically equivalent to a linear combination of these elliptic curves; namely we have

$$X\equiv aE_{1,\beta_1\alpha_1,\beta_1\alpha_2}+bE_{1,\beta_2\alpha_1,\beta_2\alpha_2}+cE_{1,0,0}+dE_{0,\alpha_1,\alpha_2} \tag{1}$$

where coefficients are rational integers[6),7)].

As $(X, E_{\xi,\eta\alpha_1,\eta\alpha_2})$ is linear with respect to divisors X, it follows easily from Lemma 3 that there exist rational integers k, l, $l\equiv 0(\mathrm{mod}\, N(\alpha_1, \alpha_2))$, and an element α of the ideal $\overline{(\alpha_1, \alpha_2)}$ depending only on X so that

$$(X, E_{\xi,\eta\alpha_1,\eta\alpha_2})=(k\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta)/N(\xi, \eta\alpha_1, \eta\alpha_2) \tag{2}$$

for all $E_{\xi,\eta\alpha_1,\eta\alpha_2}$. Moreover, as is easily verified, constants k, l and α are uniquely determined when X is given. Now it is convenient to attach a matrix

$$M(X)=\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}, \quad \text{where} \quad k\in Z,\ l\in N(\alpha_1, \alpha_2)Z,\ \alpha\in\overline{(\alpha_1, \alpha_2)}$$

to any divisor X on $E\times E_{\alpha_1,\alpha_2}$. For an elliptic curve $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ on $E\times E_{\alpha_1,\alpha_2}$ we have

$$M(E_{\lambda,\mu\alpha_1,\mu\alpha_2})=\frac{N(\alpha_1, \alpha_2)}{N(\lambda, \mu\alpha_1, \mu\alpha_2)}\begin{pmatrix} \mu\bar{\mu} & -\lambda\bar{\mu} \\ -\mu\bar{\lambda} & \lambda\bar{\lambda} \end{pmatrix}.$$

As (X, Y) is linear with respect to Y, we can get the following formula:

$(X, Y)=(kl'+lk'-\alpha\bar{\alpha}'-\bar{\alpha}\alpha')/N(\alpha_1, \alpha_2)$, where $M(X)=\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}$ and $M(Y)=\begin{pmatrix} k' & -\bar{\alpha}' \\ -\alpha' & l' \end{pmatrix}$. In particular, putting $X=Y$, we have

$$\frac{1}{2}(X, X)=(kl-\alpha\bar{\alpha})/N(\alpha_1, \alpha_2)=\frac{\det M(X)}{N(\alpha_1, \alpha_2)}. \tag{3}$$

[6] In what follows we shall denote by $\equiv$ the algebraic equivalence.

[7] Of course, we may take the graphs of homomorphisms of E_{α_1,α_2} onto E, namely $E_{\gamma_1,\alpha_1,\alpha_2}$, $E_{\gamma_2,\alpha_1,\alpha_2}$ in stead of $E_{1,\beta_i\alpha_1,\beta_i\alpha_2}$ $(i=1, 2)$, where $\{\gamma_1, \gamma_2\}$ is a Z-basis of (α_1, α_2).

When X is expressed in the form (1), we have

$$M(X)=\begin{pmatrix} (aN\beta_1+bN\beta_2)N(\alpha_1, \alpha_2)+d & -(a\bar{\beta}_1+b\bar{\beta}_2)N(\alpha_1, \alpha_2) \\ -(a\beta_1+b\beta_2)N(\alpha_1, \alpha_2) & (a+b+c)N(\alpha_1, \alpha_2) \end{pmatrix}.$$

This implies in particular that to every matrix $M=\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}$, $k\in Z$, $\alpha\in\overline{(\alpha_1, \alpha_2)}$, $l\in N(\alpha_1, \alpha_2)Z$, there corresponds a divisor X such that $M=M(X)$.

We also know that $M(X)=M(Y)$ if and only if $X\equiv Y$.

LEMMA 4. *Let X be a divisor on $E\times E_{\alpha_1,\alpha_2}$ such that $(X, X)=2$. Then we have $l(X)\geqq 1$ or otherwise $l(-X)\geqq 1$, where $l(X)$ means the dimension of the complete linear system $|X|$ determined by X.*

PROOF. By virtue of the Riemann-Roch theorem on $E\times E_{\alpha_1,\alpha_2}$ we know that

$$l(X)+l(-X)\geqq\chi(E\times E_{\alpha_1,\alpha_2})-\chi_{E\times E_{\alpha_1,\alpha_2}}(-X).$$

Since the arithmetic genus of an abelian variety is zero, we have $\chi(E\times E_{\alpha_1,\alpha_2})=0$; and further the virtual arithmetic genus $\chi_{E\times E_{\alpha_1,\alpha_2}}(-X)$ is equal to $-\frac{1}{2}(X, X)$ (cf. [4]). Therefore we have

$$l(X)+l(-X)\geqq 1.$$

This implies either $l(X)\geqq 1$, $l(-X)=0$ or $l(X)=0$, $l(-X)\geqq 1$.

The following lemma is due to Weil (cf. [7], Satz 2).

LEMMA (Weil). *Let A be an abelian variety of dimension 2, and X be a positive divisor on A such that $(X, X)=2$. Then, if X is an irreducible curve, then X is a curve of genus 2 and A is a Jacobian variety of X; if X is not irreducible, then there exist elliptic curves E and E' on A such that $X\equiv E+E'$*[8].

LEMMA 5. *Let X be a positive divisor on $E\times E_{\alpha_1,\alpha_2}$ such that $(X, X)=2$. Then X is an irreducible curve if and only if $(X, E_{\lambda,\mu\alpha_1,\mu\alpha_2})>1$ for all elliptic curves on $E\times E_{\alpha_1,\alpha_2}$.*

PROOF. First we suppose that X is irreducible and that $(X, E_{\lambda,\mu\alpha_1,\mu\alpha_2})=1$ for some $\lambda\in\mathfrak{o}$ and $\mu\in(\alpha_1, \alpha_2)^{-1}$. Then, by virtue of Weil [6], Cor. 2, Th. 4, we know that there is a birational transformation of $E\times E_{\alpha_1,\alpha_2}$ onto $X\times E_{\lambda,\mu\alpha_1,\mu\alpha_2}$. This is a contradiction, because the dimension of the Picard variety of $X\times E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ is three (recall that genus of X is 2).

Conversely if X is not irreducible, then by Weil's lemma there are elliptic curves $E_{\lambda,\mu\alpha_1,\mu\alpha_2}$ and $E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}$ such that $X\equiv E_{\lambda,\mu\alpha_1,\mu\alpha_2}+E_{\lambda',\mu'\alpha_1,\mu'\alpha_2}$. Since $(X, X)=2$ we see that $(E_{\lambda,\mu\alpha_1,\mu\alpha_2}, E_{\lambda',\mu'\alpha_1,\mu'\alpha_2})=1$. This implies that $(X, E_{\lambda,\mu\alpha_1,\mu\alpha_2})=1$.

[8] Notice that, if $(X, X)\neq 0$, then X is non-degenerate (cf. [3]).

§ 2. Formulation of the problem.

We take a divisor X on $E\times E_{\alpha_1,\alpha_2}$ such that $(X, X)=2$. Put

$$M(X)=\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l \end{pmatrix};$$

then by (2), we have $k=(X, E_{1,0,0})$. Since either $l(X)\geqq 1$ or $l(-X)\geqq 1$ by Lemma 4, we can see that $l(X)\geqq 1$ if and only if $k>0$ $\left(\text{since } \frac{kl-\alpha\bar{\alpha}}{N(\alpha_1, \alpha_2)} = \frac{1}{2}(X, X)=1, \text{ we have } k\neq 0\right)$. By virtue of Weil's lemma, and our Lemma 5, formulas (2) and (3), we have the following

CRITERION. *Let X be a divisor on $E\times E_{\alpha_1,\alpha_2}$ such that*

(4) $$k>0\,, \qquad kl-\alpha\bar{\alpha}=N(\alpha_1, \alpha_2)$$

where $M(X)=\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}$. If the equation

(5) $$k\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta=N(\xi, \eta\alpha_1, \eta\alpha_2)$$

has a non-trivial solution $\{\xi, \eta\}\neq\{0, 0\}$ in $\mathfrak{o}$, then there exists an elliptic curve $E_{\xi',\eta'\alpha_1,\eta'\alpha_2}$ such that $X\equiv E_{\xi,\eta\alpha_1,\eta\alpha_2}+E_{\xi',\eta'\alpha_1,\eta'\alpha_2}$, $(E_{\xi,\eta\alpha_1,\eta\alpha_2}, E_{\xi',\eta'\alpha_1,\eta'\alpha_2})=1$; and otherwise there exists an irreducible curve θ of genus 2 on $E\times E_{\alpha_1,\alpha_2}$ which is linearly equivalent to X so that $E\times E_{\alpha_1,\alpha_2}$ is the Jacobian variety of θ.

§ 3. The case: $m=0$. (The case without complex multiplications.)

We are now going to solve the equation (5) under the condition (4). First we treat the case $m=0$. In this case we may assume $\alpha_1=1$, $\alpha_2=0$, $\beta_1=1$, $\beta_2=0$, $b=0$, and we have

$$M(X)=\begin{pmatrix} a+d & -a \\ -a & a+c \end{pmatrix}, \quad \text{where} \quad X\equiv aE_{1,1}+cE_{1,0}+dE_{0,1}\,.$$

The conditions (4), (5) are written in the following form:

(4′) $$a+d>0\,, \qquad ac+cd+da=1$$

(5′) $$(a+d)x^2-2axy+(a+c)y^2=1\,.$$

It is easy to see that under the condition (4′) the equation (5′) has always solutions in Z (cf. e.g. [2], p. 160). Namely, in this case $E\times E$ can not be a Jacobian variety.

§ 4. The case: $m>0$. (The case with complex multiplications.)

Case I. First we shall consider the case in which the ideal $(\alpha_1, \alpha_2)\subset\mathfrak{o}$ is not principal. We put $k=2$; and take an element α in the ideal $\overline{(\alpha_1, \alpha_2)}$ such that the ideal $\mathfrak{B}\subset\mathfrak{o}$ defined by $(\bar{\alpha})=(\alpha_1, \alpha_2)\mathfrak{B}$, is prime to 2; then the condition $kl-\alpha\bar{\alpha}=N(\alpha_1, \alpha_2)$ determines a number $l\in N(\alpha_1, \alpha_2)Z$. Let X be a divisor on $E\times E_{\alpha_1,\alpha_2}$ such that

$$M(X)=\begin{pmatrix} 2 & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}.$$

Since $(\mathfrak{B}, 2)=1$, we have $N(\bar{\alpha}, 2\alpha_1, 2\alpha_2)=N(\alpha_1, \alpha_2)$, and the following relations holds (cf. Preliminaries):

$$2X\equiv E_{1,0,0}+E_{\bar{\alpha},2\alpha_1,2\alpha_2}. \tag{6}$$

Now we shall show that $(X, E_{\xi,\eta\alpha_1,\eta\alpha_2})>1$ for all elliptic curves $E_{\xi,\eta\alpha_1,\eta\alpha_2}$. Suppose there is an elliptic curve $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ such that $(X, E_{\xi,\eta\alpha_1,\eta\alpha_2})=1$. Then (6) implies $(E_{1,0,0}, E_{\xi,\eta\alpha_1,\eta\alpha_2})+(E_{\bar{\alpha},2\alpha_1,2\alpha_2}, E_{\xi,\eta\alpha_1,\eta\alpha_2})=2$. If $(E_{1,0,0}, E_{\xi,\eta\alpha_1,\eta\alpha_2})=0$, then we have $E_{1,0,0}=E_{\xi,\eta\alpha_1,\gamma\alpha_2}$ by Lemma 3, so that $(E_{\bar{\alpha},2\alpha_1,2\alpha_2}, E_{1,0,0})=2$. On the other hand, by our construction we have $(X, X)=2$, which means $(E_{\bar{\alpha},2\alpha_1,2\alpha_2}, E_{1,0,0})=4$. This is a contradiction. Similarly we know that $(E_{\bar{\alpha},2\alpha_1,2\alpha_2}, E_{\xi,\eta\alpha_1,\eta\alpha_2})$ can not be zero. Hence we must have $(E_{1,0,0}, E_{\xi,\eta\alpha_1,\eta\alpha_2})=(E_{\bar{\alpha},2\alpha_1,2\alpha_2}, E_{\xi,\eta\alpha_1,\eta\alpha_2})=1$. Then by Remark of Prop. 6, ideals $(1, 0, 0)$ and $(\bar{\alpha}, 2\alpha_1, 2\alpha_2)$ belong to the same ideal class. But we have $(\bar{\alpha}, 2\alpha_1, 2\alpha_2)=(\mathfrak{B}, 2)(\alpha_1, \alpha_2)=(\alpha_1, \alpha_2)$ and the ideal (α_1, α_2) is not principal by our assumption. This is a contradiction. Thus we know that $(X, E_{\xi,\eta\alpha_1,\eta\alpha_2})>1$ for all elliptic curves $E_{\xi,\eta\alpha_1,\eta\alpha_2}$ on $E\times E_{\alpha_1,\alpha_2}$.

Case II. We shall treat the case in which (α_1, α_2) is a principal ideal. In this case we may assume, without loss of generality, that $\alpha_1=1$, $\alpha_2=0$ (cf. Cor. of Prop. 3). Since $E_{1,0}$ is isomorphic to E, we may consider $E\times E$ in place of $E\times E_{1,0}$. (And $E_{\lambda,\mu}$ in place of $E_{\lambda,\mu,0}$.)

Let k, l be rational integers and α be an element of $\mathfrak{o}$ such that $k>0$, $kl-\alpha\bar{\alpha}=1$; and X be a divisor on $E\times E$ with $M(X)=\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}$. We have similarly as in case I the following relation

$$kX\equiv E_{1,0}+E_{\bar{\alpha},k}.$$

First we shall test the value $k=2$. Suppose there exists an elliptic curve $E_{\xi,\eta}$ such that $(X, E_{\xi,\eta})=1$. Then we have $(E_{1,0}, E_{\xi,\eta})+(E_{\bar{\alpha},2}, E_{\xi,\eta})=2$. We easily see as in case I, that neither $(E_{1,0}, E_{\xi,\eta})$ nor $(E_{\bar{\alpha},2}, E_{\xi,\eta})$ can be zero. Hence we must have $(E_{1,0}, E_{\xi,\eta})=(E_{\bar{\alpha},2}, E_{\xi,\eta})=1$. Then by Remark of Prop. 6, (ξ, η) must be a principal ideal; therefore we may assume $(\xi, \eta)=\mathfrak{o}$, multiplying a suitable non-zero element $\gamma\in Q(\sqrt{-m})$ to ξ and η, if necessary. Then by Cor. 1 of Lemma 3 we know that η and $2\xi-\bar{\alpha}\eta$ are units of $\mathfrak{o}$; this means that α must be congruent to a unit of $\mathfrak{o}$ modulo 2. We can conclude from this that if we can find α so that $\alpha\bar{\alpha}+1\equiv 0 \pmod 2$ and that α is not congruent to a unit modulo 2, then we can find $l\in Z$ such that $2l-\alpha\bar{\alpha}=1$ and for such values of α and l the equation $2\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta=N(\xi, \eta)$ has no solution $\{\xi, \eta\}\neq\{0, 0\}$ in $\mathfrak{o}$. Such α exists in the following cases:

$$\begin{aligned} &\alpha=1+\sqrt{-m} && \text{if } m\equiv 2 \pmod 4)\\ &\alpha=\sqrt{-m} && \text{if } m\equiv 1 \pmod 4),\ m>1\\ &\alpha=\frac{1}{2}(\pm 1+\sqrt{-m}) && \text{if } m\equiv 3 \pmod 8),\ m>3. \end{aligned}$$

To treat the case: $m\equiv 7 \pmod 8$, we put $k=8$. Let α be an element of $\mathfrak{o}$ such that $\alpha\bar{\alpha}+1\equiv 0 \pmod 8$; X be a divisor such that

$$M(X)=\begin{pmatrix} 8 & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}, \quad \text{where } l=\frac{1}{8}(\alpha\bar{\alpha}+1).$$

We have $(X, X)=2$ and $8X\equiv E_{1,0}+E_{\bar{\alpha},8}$. Suppose there exists an elliptic curve $E_{\xi,\eta}$ such that $(X, E_{\xi,\eta})=1$. Then the above relation gives

$$(E_{1,0}, E_{\xi,\eta})+(E_{\bar{\alpha},8}, E_{\xi,\eta})=8. \tag{7}$$

We can find ideals $\mathfrak{a}, \mathfrak{b}$ in $\mathfrak{o}$ so that $(\eta)=(\xi, \eta)\mathfrak{a}$ and $(8\xi-\bar{\alpha}\eta)=(\xi, \eta)\mathfrak{b}$ respectively; by Cor. 1 of Lemma 3, (7) can be written in the following form:

$$N\mathfrak{a}+N\mathfrak{b}=8.$$

Similarly as in preceding cases we see that neither $(E_{1,0}, E_{\xi,\eta})$ nor $(E_{\bar{\alpha},8}, E_{\xi,\eta})$ can be zero; this implies that neither η nor $8\xi-\bar{\alpha}\eta$ can be zero. We put $\gamma=N\mathfrak{a}/\eta$. Then we have $(\gamma\xi, \gamma\eta)=\bar{\mathfrak{a}}$. Therefore taking $\gamma\xi, \gamma\eta$ in place of ξ, η, if necessary, we may suppose that $(\xi, \eta)=\bar{\mathfrak{a}}$, $\eta=N\mathfrak{a}$. Now we can write the condition for the existence of $E_{\xi,\eta}$ such that $(X, E_{\xi,\eta})=1$ in the following form:

$$N(8\xi-\bar{\alpha}\eta)=\eta(8-\eta)>0, \qquad N(\xi, \eta)=\eta\,; \ \xi, \eta\in\mathfrak{o}. \tag{8}$$

Since $\eta>0$ and $8-\eta>0$, we have $1\leqq\eta\leqq 7$. First we consider the case when η is odd. We put $8\xi-\bar{\alpha}\eta=x+y\omega$, where $x, y\in Z$, and $\omega=\frac{1}{2}(1+\sqrt{-m})$; we then have $x^2+xy+\frac{1}{4}(1+m)y^2=\eta(8-\eta)\equiv 1 \pmod 2$. From this we know that y must be even. Therefore we have

$$\left(x+\frac{y}{2}\right)^2+m\left(\frac{y}{2}\right)^2+(\eta-4)^2=16\ ;$$

and, if $m\geqq 23$ (namely if $m\neq 7$, 15), we can conclude that $y=0$. But this is impossible since $(\eta-4)^2=1$ or 9. Thus we see that if $m\geqq 23$, η can not be odd.

Second we consider the case: $\eta=2$ or 6. We put $\frac{1}{2}(8\xi-\bar{\alpha}\eta)=x+y\omega$; then we have $x^2+xy+\frac{1}{4}(1+m)y^2=3$; multiplying both sides by 4 we have $(2x+y)^2+my^2=12$. If $m\geqq 23$, this equation is unsolvable; namely η can not be 2 nor 6.

Finally we consider the case $\eta=4$. From the first equation of (8) we have

$N(2\xi-\bar{\alpha})=1$; this implies $2\xi-\bar{\alpha}=\pm 1$. Combining this with the second equation of (8), we get $N(\alpha\pm 1)\equiv 0 \pmod{16}$.

Therefore we can conclude that if we can find α so that $\alpha\bar{\alpha}+1\equiv 0 \pmod 8$, and $\pm(\alpha+\bar{\alpha})\not\equiv\alpha\bar{\alpha}+1 \pmod{16}$, then we can find $l\in Z$ such that $8l-\alpha\bar{\alpha}=1$ and for such values of α and l the equation $8\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta=N(\xi,\eta)$ has no solution $\{\xi,\eta\}\neq\{0,0\}$ in $\mathfrak{o}$, provided $m\neq 7$, 15. Now we can easily see that

$$\alpha=\pm\sqrt{-m}\,,\, 4\pm 3\sqrt{-m} \quad \text{when} \quad m\equiv 7 \pmod{16}$$

$$\alpha=\pm 3\sqrt{-m}\,,\, 4\pm\sqrt{-m} \quad \text{when} \quad m\equiv -1 \pmod{16}$$

satisfy the required conditions. Namely, if $m\equiv 7 \pmod 8$ and $m\geqq 23$, then there exists a divisor X on $E\times E$ such that $(X,X)=2$ and $(X,E_{\xi,\eta})>1$ for all $E_{\xi,\eta}$.

Our problem is settled except when m is 1, 3, 7 or 15. In these cases we shall show that

$$(5') \qquad k\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta=N(\xi,\eta)$$

has a solution $\{\xi,\eta\}\neq\{0,0\}$ whenever $k,l\in Z$, $\alpha\in\mathfrak{o}$ satisfy the condition

$$(4') \qquad k>0\,, \qquad kl-\alpha\bar{\alpha}=1\,.$$

Put $\xi=x+y\omega$, $\eta=z+u\omega$ $(x,y,z,u\in Z)$; then the left hand side of (5′) becomes a positive definite quadratic form with real coefficients in four variables x,y,z and u. We denote its discriminant by Δ; then it is easy to see that $\Delta=D^2/16$, where D means the discriminant of the imaginary quadratic field $Q(\sqrt{-m})$. By virtue of Theorem 106 in Dickson's book [2], p. 185, the minimum of this quadratic form is not greater than $\sqrt[4]{4\Delta}$. Since $\sqrt[4]{4\Delta}=\sqrt{|D|/2}$, we can see that the minimum is 1 when m is 1, 3, or 7, and that the minimum is 1 or 2 when m is 15.

A pair $\{\xi,\eta\}$ of elements in $\mathfrak{o}$ for which the left hand side of (5′) takes the minimum 1 gives a solution of (5′), because $N(\xi,\eta)=1$ for such a pair $\{\xi,\eta\}$. Now we shall consider the case when the minimum is 2. If $N(\xi,\eta)=2$, then clearly $\{\xi,\eta\}$ is a solution of (5′). Suppose that $N(\xi,\eta)=1$. This implies that $(\xi,\eta)=1$. Then we can find $\lambda,\mu\in\mathfrak{o}$ so that $\xi\lambda-\eta\mu=1$; and we have

$$\begin{pmatrix}\bar{\xi} & \bar{\eta}\\ \bar{\mu} & \bar{\lambda}\end{pmatrix}\begin{pmatrix}k & -\bar{\alpha}\\ -\alpha & l\end{pmatrix}\begin{pmatrix}\xi & \mu\\ \eta & \lambda\end{pmatrix}=\begin{pmatrix}2 & -\bar{\alpha}_1\\ -\alpha_1 & l_1\end{pmatrix}, \qquad \alpha_1\in\mathfrak{o}\,, \qquad l_1\in Z\,,$$

$2l_1-\alpha_1\bar{\alpha}_1=1$; namely $N\alpha_1\equiv 1 \pmod 2$. Since $m=15$, this means that $\alpha_1\equiv 1 \pmod 2$; we can put $\alpha_1=1+2\beta$, where $\beta\in\mathfrak{o}$. Again we have

$$\begin{pmatrix}1 & 0\\ \beta & 1\end{pmatrix}\begin{pmatrix}2 & -\bar{\alpha}_1\\ -\alpha_1 & 1\end{pmatrix}\begin{pmatrix}1 & \bar{\beta}\\ 0 & 1\end{pmatrix}=\begin{pmatrix}2 & -1\\ -1 & l_2\end{pmatrix}.$$

Since $2l_2-1=1$, we have $l_2=1$. This implies that the minimum of the left hand side of (5′) must be 1; this is a contradiction. Namely this case can not happen.

Thus we have the following

THEOREM. *Let E and E' be elliptic curves whose rings of endomorphisms $\mathfrak{A}(E)$ and $\mathfrak{A}(E')$ are both isomorphic to the principal order $\mathfrak{o}$ of an imaginary quadratic field $Q(\sqrt{-m})$. Suppose there exist a finite number of elements $\lambda_1, \cdots, \lambda_n$ of $\mathfrak{A}(E)$ such that E' is isomorphic to $E_{\lambda_1,\cdots,\lambda_n}$. Then the product $E\times E'$ can not be a Jacobian variety when E' is isomorphic to E and m is equal to one of* 0, 1, 3, 7 *and* 15. *In all other cases there exist curves of genus two, with the self intersection number* 2, *on $E\times E'$; in other words $E\times E'$ is a Jacobian variety of some curve of genus* 2.

§ 5. The number of classes of curves of genus 2 on $E\times E_{\alpha_1,\alpha_2}$.

Assumptions for E being the same, we suppose that $E\times E_{\alpha_1,\alpha_2}$ is the Jacobian variety of an irreducible curve X and also that of another irreducible curve X', X and X' being on $E\times E_{\alpha_1,\alpha_2}$. According to the theorem of Torelli (cf. [7]) we can say that X and X' are birationally equivalent to each other if and only if there exists an automorphism Λ of $E\times E_{\alpha_1,\alpha_2}$ such that $X'\equiv\Lambda^{-1}(X)$. Now there arises naturally a problem to find out the number of classes of curves of genus 2 on $E\times E_{\alpha_1,\alpha_2}$ modulo birational equivalence. We are going to show that this number is finite.

We denote by G the group of all matrices $\begin{pmatrix} p & r \\ q & s\end{pmatrix}$ whose entries sarisfy the conditions: p and $s\in\mathfrak{o}$, $r\in(\alpha_1, \alpha_2)$, $q\in(\alpha_1, \alpha_2)^{-1}$ and $ps-qr$ is a unit of $\mathfrak{o}$. We can write an automorphism Λ of $E\times E_{\alpha_1,\alpha_2}$ by an element $\begin{pmatrix} p & r \\ q & s\end{pmatrix}$ of G (cf. Cor. of Prop. 5). Then we can easily see that $M(\Lambda^{-1}X)=\begin{pmatrix} \bar{p} & \bar{q} \\ \bar{r} & \bar{s}\end{pmatrix}M(X)\begin{pmatrix} p & r \\ q & s\end{pmatrix}$; the condition $X'\equiv\Lambda^{-1}(X)$ is expressed by the relation

$$M(X')=\begin{pmatrix} \bar{p} & \bar{q} \\ \bar{r} & \bar{s}\end{pmatrix}M(X)\begin{pmatrix} p & r \\ q & s\end{pmatrix}.$$

Now we consider an equivalence relation

$$M\sim\begin{pmatrix} \bar{p} & \bar{q} \\ \bar{r} & \bar{s}\end{pmatrix}M\begin{pmatrix} p & r \\ q & s\end{pmatrix}, \qquad \begin{pmatrix} p & r \\ q & s\end{pmatrix}\in G,$$

in the set of matrices $M=\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l\end{pmatrix}$, where $k\in Z$, $\alpha\in\overline{(\alpha_1, \alpha_2)}$, $l\in N(\alpha_1, \alpha_2)\cdot Z$, $k>0$ and $\det M=kl-\alpha\bar{\alpha}=N(\alpha_1, \alpha_2)$; and we shall show that the number of equivalence classes is finite. (It is clear that this includes the assertion mentioned above[9].)

[9] We can see that the number of classes of divisors X such that $X\equiv E'+E''$, $(E', E'')=1$, is equal to the number of pairs $\{C', C''\}$ of ideal classes such that the product $C'C''$ contains the ideal (α_1, α_2).

We put $\xi=x+y\omega$, $\eta=z\beta_1+u\beta_2$, where $x, y, z, u\in Z$ and $\{\beta_1, \beta_2\}$ is a Z-basis of the ideal $(\alpha_1, \alpha_2)^{-1}$; then the left hand side of (5) becomes a positive definite quadratic form in four variables x, y, z, u with real coefficients. Its discriminant is equal to $D^2/16$ and hence depends only on m. This implies that the minimum k_0 of $k\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta$ ($\xi\in\mathfrak{o}$, $\eta\in(\alpha_1, \alpha_2)^{-1}$) does not exceed a constant depending only on m (cf. Minkowski's well-known theorem on a convex body and lattice points; or Dickson [2] loc. cit.). Now we can choose and fix an integral ideal $\mathfrak{a}_j$ with the smallest norm out of each ideal class C_j of $\mathfrak{o}$, $j=1, \cdots, h$, where h is the number of ideal classes. Again we choose and fix $\gamma_j\in\mathfrak{o}$ and $\delta_j\in(\alpha_1, \alpha_2)^{-1}$ such that $(\gamma_j, \delta_j\alpha_1, \delta_j\alpha_2)=\mathfrak{a}_j$ for each j, $1\leqq j\leqq h$.

Suppose that $\xi=\xi_0\in\mathfrak{o}$, $\eta=\eta_0\in(\alpha_1, \alpha_2)^{-1}$ give the minimum k_0 of $k\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta$. Then there exist a number j, $1\leqq j\leqq h$, and an element $\gamma\in Q(\sqrt{-m})$, $\gamma\neq 0$, such that $(\gamma\xi_0, \gamma\eta_0\alpha_1, \gamma\eta_0\alpha_2)=\mathfrak{a}_j$; since $\xi=\gamma\xi_0$, $\eta=\gamma\eta_0$ give the value $k_0N\gamma$ of $k\xi\bar{\xi}+l\eta\bar{\eta}-\alpha\xi\bar{\eta}-\bar{\alpha}\bar{\xi}\eta$, it follows from definitions of k_0 and $\mathfrak{a}_j$ that $N\gamma=1$. Hence we may assume that $(\xi_0, \eta_0\alpha_1, \eta_0\alpha_2)=\mathfrak{a}_j$, taking $\gamma\xi_0$, $\gamma\eta_0$ in place of ξ_0, η_0, if necessary. Then we have $(\gamma_j, \delta_j\alpha_1, \delta_j\alpha_2)=(\xi_0, \eta_0\alpha_1, \eta_0\alpha_2)$. Therefore there exists an isomorphism $\varphi: (\gamma_jx, \delta_j\alpha_1x, \delta_j\alpha_2x)\rightarrow(\xi_0x, \eta_0\alpha_1x, \eta_0\alpha_2x)$, $x\in E$, of $E_{\gamma_j,\delta_j\alpha_1,\delta_j\alpha_2}$ on $E_{\xi_0,\eta_0\alpha_1,\eta_0\alpha_2}$; and by Prop. 8, φ can be extended to an automorphism of $E\times E_{\alpha_1,\alpha_2}$. Therefore there exists a matrix $P\in G$ such that $\begin{pmatrix}\xi_0\\ \eta_0\end{pmatrix}=P\begin{pmatrix}\gamma_j\\ \delta_j\end{pmatrix}$. Hence we have

$$(\bar{\gamma}_j, \bar{\delta}_j){}^t\bar{P}\begin{pmatrix}k & -\bar{\alpha}\\ -\alpha & l\end{pmatrix}P\begin{pmatrix}\gamma_j\\ \delta_j\end{pmatrix}=k_0\,.$$

We choose and fix $\lambda_j\in\mathfrak{o}$, $\mu_j\in(\alpha_1, \alpha_2)$ such that $\gamma_j\lambda_j-\delta_j\mu_j=N\mathfrak{a}_j$. Again we choose and fix a set of representatives $\sigma_1, \cdots, \sigma_t$ of $\mathfrak{o}$ modulo $k_0(\alpha_1, \alpha_2)$. Then we can find an element $\beta\in(\alpha_1, \alpha_2)$ so that

$$\begin{pmatrix}1 & 0\\ \bar{\beta} & 1\end{pmatrix}\begin{pmatrix}\bar{\gamma}_j & \bar{\delta}_j\\ \bar{\mu}_j & \bar{\lambda}_j\end{pmatrix}{}^t\bar{P}\begin{pmatrix}k & -\bar{\alpha}\\ -\alpha & l\end{pmatrix}P\begin{pmatrix}\gamma_j & \mu_j\\ \delta_j & \lambda_j\end{pmatrix}\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}=\begin{pmatrix}k_0 & -\bar{\alpha}_0\\ -\alpha_0 & l_0\end{pmatrix},$$

where $-\bar{\alpha}_0$ is one of σ_i's.

Now, denoting $\begin{pmatrix}\gamma_j & \mu_j\\ \delta_j & \lambda_j\end{pmatrix}$ by Λ_j, the double coset $G\Lambda_jG$ can be divided into right cosets:

$$G\Lambda_jG=\sum_i GR_i\,. \tag{9}$$

We shall show that the number of these right cosets is finite. In fact this number is equal to the index $[G:\Lambda_j^{-1}G\Lambda_j\cap G]$; and if we denote by $\Gamma(N\mathfrak{a}_j)$ the set of elements $\begin{pmatrix}p & r\\ q & s\end{pmatrix}$ of G such that $p\equiv s\equiv 1$ $(\operatorname{mod} N\mathfrak{a}_j)$, $r\equiv 0$ $(\operatorname{mod}(\alpha_1, \alpha_2)N\mathfrak{a}_j)$, $q\equiv 0$ $(\operatorname{mod}(\alpha_1, \alpha_2)^{-1}N\mathfrak{a}_j)$, then $\Gamma(N\mathfrak{a}_j)$ is a (normal) subgroup of finite index of G, and contained in $\varLambda_j^{-1}G\varLambda_j$; this implies that the number of right cosets in (9) is finite.

Thus we can find a matrix Q in G so that

$$
{}^t\bar{Q}\begin{pmatrix} k & -\bar{\alpha} \\ -\alpha & l \end{pmatrix}Q = {}^t\bar{R}_i^{-1}\begin{pmatrix} k_0 & -\bar{\alpha}_0 \\ -\alpha_0 & l_0 \end{pmatrix}R_i^{-1}.
$$

Since the number of matrices appearing in the right hand side is finite, the proof is completed.

Ochanomizu University

Bibliography

[1] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, 1941.

[2] L. E. Dickson, Studies in the theory of numbers, 1930.

[3] W. L. Hoyt, On products and algebraic families of Jacobian varieties, Ann. of Math., 77 (1963), 415-423.

[4] M. Nishi, Some results on abelian varieties, Nat. Sci. Rep., Ochanomizu Univ., 9 (1958), 1-12.

[5] G. Shimura and Y. Taniyama, Complex multiplication of Abelian varieties, 1961.

[6] A. Weil, Variétés abéliennes et courbes algébriques, Actualités Sci. Indust., 1948.

[7] A. Weil, Zum Beweis des Torellischen Satzes, Nachr. Akad. Wiss. Göttingen, 1957.