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