Natural Science Report, Ochanomizu University, Vol. 16, No. 2, 1965
お茶の水女子大学 自然科学報告 第16巻 第2号

On Certain Type of Jacobian Varieties of Dimension 2

Tsuyoshi Hayashida (林田 倪) **and Mieo Nishi** (西 三重雄)

Department of Mathematics, Faculty of Science
Ochanomizu University, Tokyo

(*Received September 10, 1965*)

The purpose of this paper is to show a method of constructing a Jacobian variety isogenous to a product of two non-isogenous elliptic curves. We first treat in § 1 the classical case making use of the theory of complex tori; a normal form of Riemann matrix will be given for each Jacobian variety obtained. In § 2 and the subsequent sections we treat the abstract case, where we assume that the rings of endomorphisms of the two elliptic curves are both isomorphic to the ring Z of rational integers. Any Jacobian variety of such type can be obtained by our method. Also we can determine the structure of the rings of endomorphisms of Jacobian varieties of such type; and prove, as a simple application, that the ring of endomorphisms of the Jacobian variety of a generic curve of genus 2 is isomorphic to Z.

§ 1. Let A be an abelian variety isogenous to a product of two mutually non-isogenous elliptic curves E and E'. We consider in this section the case in which the universal domain of our geometry is the field C of complex numbers. Then E (resp. E') is isomorphic to a complex torus of dimension 1 with fundamental periods $\{w_1, w_2\}$ (resp. $\{w_1', w_2'\}$), and A is isomorphic to a complex torus C^2/D of dimension 2 with the following fundamental periods matrix (Riemann matrix)

$$\Omega = \begin{pmatrix} w_1 & w_2 & 0 & 0 \\ 0 & 0 & w_1' & w_2' \end{pmatrix} T$$

where T is a non-singular 4×4 matrix with entries in Z. First we shall reduce Ω into a simpler form. Since T may be replaced by TU, where U is any unimodular matrix with entries in Z, we can assume that T is of the form

$$T = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \qquad (A, B, C \text{ are } 2\times 2 \text{ matrices}). \tag{1}$$

T may again be multiplied on the right side by any unimodular matrix $U = \begin{pmatrix} U_1 & V \\ 0 & U_2 \end{pmatrix}$, so that $A^{-1}B$ is replaced by $U_1^{-1}(VU_2^{-1} + A^{-1}B)U_2$.

Put $A^{-1}B=\frac{1}{n}\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $(a, b, c, d, n)=1$. There is an integer t such that $(a+nt, b, c, d)=1$. We take $V=\begin{pmatrix}t & 0\\ 0 & 0\end{pmatrix}U_2$. We can then take unimodular matrices U_1, U_2 such that $U_1^{-1}(VU_2^{-1}+A^{-1}B)U_2$ is of the form $\frac{1}{n}\begin{pmatrix}k & 0\\ 0 & 1\end{pmatrix}$. Hence we can assume without loss of generality that the minor matrices A, B appearing in (1) have the relation

$$A^{-1}B=\begin{pmatrix}\frac{k}{n} & 0\\ 0 & \frac{1}{n}\end{pmatrix},\quad n>0,\quad n, k\in Z.$$

Then replacing E (resp. E') by E_1 (resp. E_1') with fundamental periods $(w_1, w_2)A=(\pm\alpha, \alpha\tau)$ (resp. $(w_1', w_2')C=(\pm\beta, \beta\tau')$)[1], we know that A is isomorphic to a complex torus C^2/D with fundamental periods $\Omega_1=\begin{pmatrix}n & n\tau & k & \tau\\ 0 & 0 & 1 & \tau'\end{pmatrix}$. In the rest of this section we identify A (resp. $E_1\times E_1'$) with the complex torus C^2/D_1 (resp. C^2/D_0) with fundamental periods matrix Ω_1 $\left(\text{resp. } \Omega_0=\begin{pmatrix}1 & \tau & 0 & 0\\ 0 & 0 & 1 & \tau'\end{pmatrix}\right)$. Put $\Omega_1=\Omega_0 T_1$. Since periods of $E_1\times E_1'$ contain those of A, there is a natural isogeny μ of A on $E_1\times E_1'$ such that $\nu(\mu)=|\det T_1|=n^2$.

Now suppose A is a Jacobian variety of some curve. Let θ be a thêta divisor on A. There is an isogeny λ of $E_1\times E_1'$ on A such that $\lambda\circ\mu=n^2\delta_A$, δ_A being the identity map of A; therefore, if we put $Y=\lambda^{-1}(\theta)$, then $\mu^{-1}(Y)\equiv n^4\theta$ modulo algebraic equivalence. We know that any divisor on $E_1\times E_1'$ is algebraically equivalent to a linear combination (with integral cofficients) of two elliptic curves $E_1\times 0$ and $0\times E_1'$ (Weil [3], Th. 22). Hence there are two integers x and y such that $Y\equiv x(E_1\times 0)+y(0\times E_1')$. We can write the relation[2),3)] $\varphi_{\mu^{-1}(Y)}={}^t\mu\circ\varphi_Y\circ\mu$ by a matrix equality

$$n^4E(\theta)={}^tT_1\begin{pmatrix}yI & 0\\ 0 & xI\end{pmatrix}T_1,\quad \text{where}\quad I=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

Since $E(\theta)$ is a matrix with entries in Z and $\det E(\theta)=1$, we have

$$n^{16}=n^4x^2y^2;\quad ny\equiv 0,\ ky+x\equiv 0 \pmod{n^4}.$$

Whence we have $x=y=n^3$ (Notice: since θ is positive, $x>0$ and $y>0$) and $k+1\equiv 0 \pmod n$.

We have thus seen that if $A=C^2/D_1$ is a Jacobian variety of some curve, then $k+1\equiv 0 \pmod n$. Conversely, we can see from the above

1) $\pm$ signs are determined so as to make $Im\,\tau>0$ and $Im\,\tau'>0$.

2) Let A be an abelian variety and X be a divisor on A; we take the dual variety $\hat{A}$ of A. For a point u on A, we denote by $\hat{u}$ the point on $\hat{A}$ representing the linear class of X_u-X; then the map: $u\to\hat{u}$ is a homomorphism φ_X of A into $\hat{A}$.

3) ${}^t\mu$ means the transpose of μ.

calculations that if $k\equiv -1 \pmod{n}$ (in Ω_1), then there is a positive divisor X on A such that $(X, X)=2$ (cf. Weil [5]).[4]

Next, it is easy to see that there are only two abelian subvarieties on $A=C^2/D_1$, i. e. the complex torus with fundamental periods $\left\{\begin{pmatrix} n \\ 0 \end{pmatrix}, \begin{pmatrix} n\tau \\ 0 \end{pmatrix}\right\}$ and $\left\{\begin{pmatrix} 0 \\ n/(n,k) \end{pmatrix}, \begin{pmatrix} 0 \\ n\tau' \end{pmatrix}\right\}$, and if $n>1$ they intersect at least at two points, e. g. the origin and the point represented by $\begin{pmatrix} 0 \\ \tau' \end{pmatrix}\left(\equiv\begin{pmatrix} -\tau \\ 0 \end{pmatrix}\right)$. This implies that if $n>1$, A is not a product of two elliptic curves.

Therefore, by virtue of Weil [4] Satz 2, we can conclude that $A=C^2/D_1$ can be a Jacobian variety if and only if $n>1$ and $k\equiv -1 \pmod{n}$.[5]

In case when $k\equiv -1 \pmod{n}$, we apply a coordinate transformation $u'=\frac{1}{n}(u+v)$, $v'=v$, and obtain a mormal form of Riemann matrix of $A=C^2/D_1$: $\begin{pmatrix} 1 & 0 & \frac{1}{n}(\tau+\tau') & \tau' \\ 0 & 1 & \tau' & n\tau' \end{pmatrix}$.

§ 2. We now proceed to the case where the characteristic p of our universal domain is arbitrary; the method developed in the rest of this paper is purely algebraic.

We consider an abelian variety A of dimension 2; when A is isogenous to a product of two non-isogenous elliptic curves with rings of endomorphisms isomorphic to Z, we shall say that A is *of type* (N). If A is *of type* (N), then there are just two abelian subvarieties of dimension 1 on A, which are not isogenous to each other (cf. Weil [3], Prop. 26); we denote them by E and E'. Let u and v be independent generic points of E and E' respectively over an algebraically closed field k. (From now on we keep this meaning for k.) Then we can define an isogeny $\lambda: E\times E'\ni(u, v)\to u+v\in A$. The isogeny λ induces isomorphisms on E and E' respectively. This impies in particular that the subgroup in E (resp. E') obtained by projection of elements in the kernel Ker (λ) of λ to E (resp. E') is isomorphic to Ker (λ). Therefore the system of invariants of the abelian group Ker (λ) must be of the type (n, mn), where $n\geqq 1$, $m\geqq 1$ are rational integers; moreover if the characteristic p is positive, then p does not divide n (notice that the group of points on E whose orders are p is a cyclic group of order p).

The separable closure K of $k(u+v)$ in $k(u, v)$ is an abelian function field (cf. Serre [2]); namely there exists an abelian variety B, defined over k such that the function field of B over k is isomorphic to K. By inclusion relations between function fields we can define naturally

4) In what follows we denote by (X, Y) the interesection number of divisors X and Y.

5) It is easy to see that if $n=1$, then there is no divisor X with $(X, X)=2$, $X>0$, except $E_1\times 0+0\times E_1'$, so that A can not be a Jacobian variety.

a purely inseparable isogeny $\lambda_1 : E\times E'\to B$ and a separable isogeny $\lambda_2 : B\to A$, such that $\lambda=\lambda_2\circ\lambda_1$. We put $\nu(\lambda_1)=p^e$. In what follows we shall say that such an A is of type $[p^e, (n, mn)]$. (If the characteristic $p=0$, we put $p^e=1$)

Here we need some definitions. Let γ ; $A\to B$ be an isogeny of an abelian variety A onto another abelian variety B (the dimension of A being arbitrary). If there exists an isogeny $\mu : B\to A$ such that $\mu\circ\gamma=m\delta_A$ where m is an integer and δ_A the identity map of A, then we shall say that γ *divides* m or m is *a multiple of* γ. The smallest positive integer m which is divisible by γ will be called *the least integral multiple of* γ ; we shall denote it by $m_0(\gamma)$. It is clear that any integral multiple of γ is divisible by $m_0(\gamma)$.

We now return to our case of $\lambda : E\times E'\to A$, A being of type $[p^e, (n, mn)]$. We can state

LEMMA 1. *The least integral multiple* $m_0(\lambda)$ *of* λ *is the least common multiple* $\{p^e, mn\}$ *of* p^e *and* mn.

PROOF. We put $N=\{p^e, mn\}$, $N=p^sN_0$, $(N_0, p)=1$. Let u, v be independent generic points of E, E' over k ; and $\mathfrak{H}$, $\mathfrak{G}$ the kernel of λ, $N\delta_{E\times E'}$ respectively. Then $k(\lambda(u, v))$ is the fixed subfield of $k(\lambda_1(u, v))$ under Galois maps induced by $\mathfrak{H}$, and $k(Nu, Nv)$ that of $k(u^{p^s}, v^{p^s})$ by $\mathfrak{G}$. Since $k(\lambda_1(u, v))\supset k(u^{p^s}, v^{p^s})$ and $\mathfrak{H}\subset\mathfrak{G}$, we have $k(\lambda(u, v))\supset k(Nu, Nv)$. This impies that N is a multiple of λ. On the other hand $m_0(\lambda)$ is a multiple of $\lambda_1 : E\times E'\to B$. Put $m_0(\lambda)=p^tN_1$, $(N_1, p)=1$. Since λ_1 is purely inseparable, we have $k(\lambda_1(u, v))\supset k(u^{p^t}, v^{p^t})$. We can readily see that u is of degree p^e over $k(\lambda_1(u, v))$ and of degree p^t over $k(u^{p^t}, v^{p^t})$. Therefore we have $p^e\,|\,m_0(\lambda)$. Next noticing that the kernel of $m_0(\lambda)\delta_{E\times E'}$ must contain a cyclic group of order mn, we have $mn\,|\,m_0(\lambda)$. This settles our assertion.

Let X be any divisor on A. Since $E\times 0$ and $0\times E'$ make a basis of the group of divisors on $E\times E'$ modulo algebraic equivalence $\equiv$, there are rational integers a, b such that

$$\lambda^{-1}(X)\equiv a(E\times 0)+b(0\times E')\,. \tag{2}$$

As an easy consequence of Lemma 1, we have

LEMMA 2. $a\equiv b\equiv 0 \pmod{\{p^e, mn\}}$

PROOF. The relation (2) means that the map $\varphi_{\lambda^{-1}(X)}$ is represented by the matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ (namely is given by the correspondence : $E\times E'\ni(u, v)\to(au, bv)\in E\times E'$). On the other hand $\varphi_{\lambda^{-1}(X)}={}^t\lambda\varphi_X\lambda$; hence $k(u+v)\supset k(au, bv)$, Noticing that if au belongs to the field $k(u+v)$, then av also does, we see that a and b are multiples of λ ; hence $a\equiv b\equiv 0$ $\pmod{\{p^e, mn\}}$.

§ 3. Since $(\lambda^{-1}(X), \lambda^{-1}(X))=\nu(\lambda)(X, X)$, it follows from the relation (2) that $\nu(\lambda)(X, X)/2=ab$; namely, if we put $m=m'p^f$, $(m', p)=1$, then

$$(X, X)/2\equiv 0 \pmod{m'p^{f-e}} \quad \text{(the case; } e\leqq f\text{)} \tag{4}$$

$$(X, X)/2\equiv 0 \pmod{m'p^{e-f}} \quad \text{(the case; } e>f\text{)}. \tag{4'}$$

These relations (4), (4') imply that if $m'>1$ or $e\neq f$, then, for any divisor X on A, $(X, X)/2\neq 1$. Since a thêta divisor on a Jacobian variety of dimension 2 has the self-intersection number 2, we see that A can not be a Jacobian variety, unless A is of type $[p^e, (n, p^e n)]$.

§ 4. We shall now determine the structure of the ring End(A) of endomorphisms of A. We suppose A is of type $[p^e, (n, mn)]$. Let α be any element of End(A). Notations being the same as in the preceding section, we know that

$$\alpha(u+v)=au+bv, \tag{3}$$

where a, b are rational integers; we also see that, for given α, rational integers a and b are uniquely determined. Denoting the identity map of A by δ_A, we have $(\alpha-b\delta_A)(u+v)=(a-b)u$. This implies that $a-b$ is a multiple of λ; $E\times E'\to A$ (see the proof of Lemma 2); therefore by Lemma 1 we have $a\equiv b \pmod{\{p^e, mn\}}$. Conversely it is easy to see that if a, b are two integers such that $a\equiv b \pmod{\{p^e, mn\}}$, then the correspondence α defined by (3) gives an endomorphism of A. We can thus state:

End(A) *is isomorhpic to the ring of matrices* $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $a\equiv b \pmod{\{p^e, mn\}}$.

§ 5. We shall now show that, for arbitrarily given integers $e\geqq 0$, $m\geqq 1$, $n\geqq 1$, $(n, p)=1$, there exist abelian varieties of type $[p^e, (n, mn)]$. It is easy to see that there are abelian varieties of type $[1, (n, mn)]$. To treat the case when $e>0$, we need

LEMMA 3. *Let A be an abelian variety of type $[1, (1, p^e)]$. Then the dual variety (Picard variety) $\hat{A}$ of A is of type $[p^e, (1, 1)]$.*

PROOF. We denote by E, E' the two elliptic curves on A and by λ the isogeny of $E\times E'$ on A defined by $\lambda(u, v)=u+v$, $u\in E$, $v\in E'$. By definition we know that Ker(λ) is a cyclic group of order $\nu(\lambda)=p^e$; if Ker(λ) is generated by a point (z, z') on $E\times E'$, then the point z (resp. z') on E (resp. E') is of order p^e. We put $E_1=E/\{z\}$ (resp. $E'_1=E'/\{z'\}$) where $\{z\}$ (resp. $\{z'\}$) is the cyclic group generated by z (resp. z') and denote by u_1 (resp. v_1) the canonical image of the point u (resp. v). Then there exists an isogeny μ of A on $E_1\times E'_1$ such that $\mu(u+v)=(u_1, v_1)$. We put $X=E_1\times 0+0\times E'_1$; then we can see that $\mu^{-1}(X)=E+E'$ (cf. Weil [3], Prop. 33) and also that $\lambda^{-1}(\mu^{-1}(X))=(\mu\lambda)^{-1}(X)\equiv p^e(E\times 0+0$

$\times E'$). Thus we have the following commutative diagram:

$$\begin{array}{ccccc} E\times E' & \xrightarrow{\lambda} & A & \xrightarrow{\mu} & E_1\times E_1' \\ \downarrow{\scriptstyle \varphi_{\lambda^{-1}\mu^{-1}(X)}} & & \downarrow{\scriptstyle \varphi_{\mu^{-1}(X)}} & & \downarrow{\scriptstyle \delta=\text{identity}} \\ E\times E' & \xleftarrow{{}^t\lambda} & \hat{A} & \xleftarrow{{}^t\mu} & E_1\times E_1' \end{array}$$

here $\varphi_{\lambda^{-1}\mu^{-1}(X)}=\begin{pmatrix} p^e & 0 \\ 0 & p^e \end{pmatrix}$. Put $\varphi_{\mu^{-1}(X)}(u+v)=u^*+v^*$. Then $k(u^*)\subset k(u_1)$ and $k(v^*)\subset k(v_1)$. Suppose $k(u^*)$ is not equal to $k(u_1)$. Then $k(u^*)$ is isomorphic to the function field of an elliptic curve (say) E^*; and we have two isogenies $\kappa_1: E_1\times E_1'\ni(u_1, v_1)\to(u^*, v_1)\in E^*\times E_1'$ and $\kappa_2: E^*\times E_1'\ni(u^*, v_1)\to u^*+v^*\in\hat{A}$, such that ${}^t\mu=\kappa_2\circ\kappa_1$. This implies that μ is the composition of two isogenies ${}^t\kappa_2$ and ${}^t\kappa_1$: $\mu={}^t\kappa_1\circ{}^t\kappa_2$, ${}^t\kappa_2: A\to E^*\times E_1'$, ${}^t\kappa_1: E^*\times E_1'\to E_1\times E_1'$. If we put ${}^t\kappa_2(u+v)=(u_0^*, v_1)$, then we have $k(u_1)\subset k(u_0^*)\subset k(u)\cap k(u+v)$ and $k(u_1)\neq k(u_0^*)$ (Notice that $\nu({}^t\kappa_1)=\nu(\kappa_1)>1$). Noticing that $k(u)/k(u_1)$ is a separable cyclic extention of degree p^e, we know that $k(u)/k(u_0^*)$ is a separable cyclic extention of degree p^t, $t<e$; therefore $k(u_0^*)\supset k(p^tu)$. Consequently we have $k(u+v)\supset k(p^tu)$; this means that the least integral multiple of λ divides p^t. Since $t<e$, this is a contradiction. Hence we have $k(u^*)=k(u_1)$ and similarly $k(v^*)=k(v_1)$. Since ${}^t\lambda{}^t\mu$ and (consequently) ${}^t\mu$ are purely inseparable (cf. Serre [2]) and $\nu(\mu)=p^e$, the proof of our Lemma is completed.

Let now A_1 be an abelian variety of type $[p^e, (1, 1)]$; we denote by E and E' the two elliptic curves on A_1 and by λ_1 the isogeny of $E\times E'$ on A_1, dnfined by the correspondence $\lambda_1(u, v)=u+v(u\in E, v\in E')$. We can take a subgroup $\mathfrak{H}$ of $E\times E'$, with invariants (n, mn), such that $E\times 0\cap\mathfrak{H}=0\times E'\cap\mathfrak{H}=\{(0, 0)\}$. We put $\lambda_1(\mathfrak{H})=\mathfrak{H}_1$; then since λ_1 is purely inseparable, also $E\cap\mathfrak{H}_1=E'\cap\mathfrak{H}_1=\{0\}$. We consider $A=A_1/\mathfrak{H}_1$ and the canonical isogeny $\lambda_2: A_1\to A$; namely λ_2 is separable and its kernel is $\mathfrak{H}_1$. Put $\lambda=\lambda_2\lambda_1$. We shall show that λ induces isomorphisms on E and on E'. We denote by E_1 (resp. E_1') the image variety of E (resp. E') by λ_2, and by u_1 (resp. v_1) the image point of u (resp. v). On accounts of our construction of the group $\mathfrak{H}_1$ we see that λ_2 induces purely inseparable homomorphisms on E and on E'; namely $k(u)$ (resp. $k(v)$) is a purely inseparable extension of $k(u_1)$ (resp. $k(v_1)$). This implies that $k(u_1, v)\supset k(u+v)$; since $k(u+v)(v)=k(u, v)$, we see that $k(u_1, v)=k(u, v)$ and consequently $k(u_1)=k(u)$; similarly $k(v_1)=k(v)$. Our assertion is thereby proved. We thus have seen that A is of type $[p^e, (n, nm)]$.

§ 6. In this section we shall prove a preliminary result. Let λ be an isogeny of an abelian variety A onto an abelian variety B; let $m_0(\lambda)$ be the least integral multiple of λ. If $\nu(\lambda)=m_0(\lambda)$, then we shall say that λ is *cyclic*. It is easy to see that when λ is separable, the

kernel of λ is a cyclic group if and only if λ is cyclic in our sense.

LEMMA 4. *If $\lambda: A\to B$ is cyclic, then ${}^t\lambda: \hat{B}\to\hat{A}$ is also cyclic.*

PROOF. By definition there exists an isogeny $\mu: B\to A$ such that $\mu\lambda=m_0(\lambda)\delta_A$. We can readily see that $\lambda\mu=m_0(\lambda)\delta_B$. This implies that ${}^t\mu{}^t\lambda=m_0(\lambda)\delta_{\hat{B}}$ and therefore $m_0(\lambda)$ is a multiple of ${}^t\lambda$. Since the dual variety of $\hat{A}$ is isomorphic to A and the same for $\hat{B}$, it follows that $m_0(\lambda)$ is the least integral multiple of ${}^t\lambda$. Noticing that $\nu({}^t\lambda)=\nu(\lambda)$, we see that ${}^t\lambda$ is also cyclic.

§ 7. We shall now show that, for arbitrarily given two integers $e\geqq 0$ and $n>0$, $(n, p)=1$, $np^e>1$, we can find out Jacobian varieties among abelian varieties of type $[p^e, (n, p^en)]$.

We take an A_1 of type $[p^e, (1, n)]$, where $(n, p)=1$; let E and E' be elliptic curves on A_1, and λ_1 be the isogeny of $E\times E'$ on A_1 defined by $\lambda_1(u, v)=u+v$, $u\in E$, $v\in E'$. By Lemma 1 the least integral multiple $m_0(\lambda_1)$ of λ_1 is p^en; therefore λ_1 is cyclic. Hence by Lemma 4, ${}^t\lambda_1$ is cyclic. It is known that ${}^t\lambda_1$ is separable (cf. Serre [2]); therefore $\mathrm{Ker}({}^t\lambda_1)$ is a cyclic group of order p^en. We consider the divisor $E+E'$ on A_1. Then we know that $\lambda_1^{-1}(E+E')\equiv p^en(E\times 0+0\times E')$; this implies that the following diagram:

$$\begin{array}{ccc} E\times E' & \xrightarrow{\lambda_1} & A_1 \\ \left(\begin{smallmatrix} p^en & 0 \\ 0 & p^en \end{smallmatrix}\right)\downarrow & & \downarrow \varphi_{E+E'} \\ E\times E' & \xleftarrow{{}^t\lambda_1} & \hat{A}_1 \end{array}$$

is commutative. By elementary group-theoretic considerations it follows that the system of invariants of the abelian group $\mathrm{Ker}\,\varphi_{E+E'}$ is (n, p^en).

We can see that the subgroup $\mathfrak{Z}_1=E\cap E'$ of $\mathrm{Ker}\,\varphi_{E+E'}$ is cyclic and of order n; consequently there exists a cyclic group $\mathfrak{Z}_2$ of order p^en such that $\mathrm{Ker}\,\varphi_{E+E'}=\mathfrak{Z}_1+\mathfrak{Z}_2$ (direct sum). We consider $A=A_1/\mathfrak{Z}_2$ and the canonical isogeny λ_2 of A_1 on A. It is clear that A is of type $[p^e, (n, p^en)]$. According to [Nishi [1], Lemma 1], there exists a positive divisor Y on A_1 such that $Y\sim E+E'$ and $Y_\xi=Y$ for all points ξ in $\mathfrak{Z}_2$. Then by virtue of (Weil [3], Prop. 33), there exists a positive divisor θ on A such that $Y=\lambda_2^{-1}(\theta)$. By conputing self-intersection numbers we see that $(\theta, \theta)=2$. Since A is of type $[p^e, (n, p^en)]$, A is not isomorphic to a product of two elliptic curves, provided $np^e>1$. Therefore, by virtue of (Weil [4], Satz 2), A must be a Jacobian variety, θ being a thêta divisor on it.

Now we shall consider the converse. Suppose that J is a Jacobian variety of type (N); we have seen in preceding § 3 that J must be of type $[p^e, (n, p^en)]$. Let E and E' be two elliptic curves on J; let λ:

$E\times E'\to J$ be the isogeny defined by $\lambda(u, v)=u+v$, $u\in E$, $v\in E'$. There exists an abelian variety A_1 of type $[p^e, (1, n)]$ and isogenies $\lambda_1: E\times E' \to A_1$ and $\lambda_2: A_1\to J$ such that $\lambda=\lambda_2\lambda_1$. It follows from Lemma 2 that elliptic curves on A_1, which we denote by the same notations E, E', make a basis of the group of divisors modulo algebraic equivalence. Consequently there are positive integers a and b such that $\lambda_2^{-1}(\theta)\equiv aE+bE'$, where θ is a thêta divisor on J. By computing self-intersection numbers, we easily see that $a=b=1$; namely $\lambda_2^{-1}(\theta)\equiv E+E'$. This means that Ker $\varphi_{E+E'}$ must contain Ker (λ_2). On the other hand the isogeny λ must induce identity maps on E and on E'; therefore $E\cap E'\cap \mathrm{Ker}\,(\lambda_2)=\{0\}$. Taking orders of these groups into account we see Ker $\varphi_{E+E'}=(E\cap E')+\mathrm{Ker}\,(\lambda_2)$ (direct sum).

We thus have seen that any Jacobian variety of type (N) can be obtained by the method described above.

REMARK 1. Let J be a Jacobian variety of type (N). Notations being the same as above, we have observed that $\lambda_2^{-1}(\theta)\equiv E+E'$; and this is true for every positive divisor X on J with self-intersection number 2; hence $\lambda_2^{-1}(\theta)\equiv\lambda_2^{-1}(X)$ and consequently $\theta\equiv X$ for such divisor X. This implies that *the structure of J as a Jacobian variety of some curve of genus 2 is uniquely determined. In other words a curve having J as its Jacobian variety is uniquely determined up to isomorphism.*

REMARK 2. Suppose two non-isogenous elliptic curves E and E' are given. We construct a Jacobian variety J (resp. J') of type (N) starting from $E\times E'$; let λ (resp. λ') be the isogeny of $E\times E'$ on J (resp. J') described in § 2. Then it can be proved that J and J' are isomorphic to each other if and only if λ and λ' have the same kernel. Whence we see that for given $E\times E'$ and p^en, $(n, p)=1$, there are $\phi(p^e)n^3\prod_{\substack{q\mid n\\ q:\text{ a prime}}}\left(1-\frac{1}{q^2}\right)$ mutually non-isomorphic Jacobian varieties of type $[p^e, (n, np^e)]$, where ϕ is Euler's function and when $p=0$, we put $p^e=1$.

§ 8. We can now show that the ring End $(J(C))$ of endomorphisms of the Jacobian variety of a generic curve C of genus 2 is isomorphic to the ring Z of rational integers. We have seen in § 3 and in § 6 that for any positive integer n there exists a curve C_1 of genus 2 such that End $(J(C_1))$ of the Jacobian variety of C_1 is isomorphic to the ring R_n: $R_n=\left\{\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix};\ a, b\in Z,\ a\equiv b \pmod n\right\}$. We know that there is an injection map ι of End $(J(C))$ into End $(J(C_1))$ induced by a specialization of C to C_1. Since the identity element δ of End $(J(C))$ is the linear extension of the diagonal correspondence of C, the identity element of End $(J(C))$ is mapped on that of End $(J(C_1))$ by ι. Suppose End $(J(C))$ is not isomorphic to Z. Then there is an element $\alpha\in$End $(J(C))$ which is

not an integral multiple of the identity element δ. Take a curve C_1 mentioned above; put $\iota(\alpha)=\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in \mathrm{End}(J(C_1))$. Then by our assumption, we have $a \neq b$. Put $a-b=c \in Z$; $\alpha - b\delta = \gamma \in \mathrm{End}(J(C))$. Then $\gamma \notin Z$, $\gamma^2 = c\gamma$, $c \neq 0$. Now, we know that, for any positive integer m, there is an injection map ι_m of $\mathrm{End}(J(C))$ into the ring $R_m = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix};\ a, b \in Z,\ a \equiv b \pmod{m} \right\}$. Put $\iota_m(\gamma) = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$. We have $x \neq y$, $x^2 = cx$, $y^2 = cy$; consequently $x=0$, $y=c$; or $x=c$, $y=0$. Therefore we have $c = \pm(x-y) \equiv 0 \pmod{m}$. Since m can be arbitrarily large, this is a contradiction.

Bibliography

[1] M. Nishi, The Frobenius theorem and the duality theorem on an abelian variety, Mem. Coll. Univ. of Kyoto, Vol. XXXII. No. 2, 1959.

[2] J. S. Serre, Quelque propriété des variétés abéliennes en caracteristique p, Amer. J. of Math. 80, 1958, p. 715-739.

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

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

[5] A. Weil, Théorèmes fondamentaux de la théories des fonctions thêta, Séminaire Bourbaki, Mai 1949.