ON ABELIAN VARIETIES

HISASI MORIKAWA

In a Bourbaki seminary note, La Théorie des Fonctions Thêta, A. Weil has discussed two fundamental theorems of the general theory of Theta functions. The first, due to H. Poincaré, was proved very skilfully in the note by means of harmonic integrals on a torus and the second, due to Frobenius, was treated by the systematic use of the notion of analytic structure.

In the present paper we shall give an algebraic geometrical proof of the Second (Frobenius) Theorem and shall make clear the algebro-arithmetic structure of divisors on abelian varieties defined over fields of any characteristic.

Section 1 is to give a Picard variety of a given abelian variety and to show the duality between the Picard variety of an abelian variety satisfying a certain condition and the abelian variety itself; Picard Variety has been an object of deep and interesting researches by A. Weil, J. Igusa, W. L. Chow and T. Matsusaka. In section 2 some arithmetic preparations on rings of endomorphisms of abelian varieties are given. In section 3 we prove the main theorems and study the behaviours of divisors for the homomorphisms (or endomorphisms) between abelian varieties. In the last section we shall treat a problem on positive divisors, which was left open in Weil's book, Variétés abéliennes et courbes algébriques (1948)—quoted as [V]—, as an application of the results in § 3.

The notations and results in Weil's books [V] and Foundations of algebraic geometry (1946)—quoted as (F)—, are freely used. Beside Weil's results referred to in § 1, the Lemma[1] due to W. L. Chow plays an essential role and in § 3 the theorem on the square sum of four integers of an algebraic number field, due to C. L. Siegel,[2] is a key-point in our proof.

§ 1. Duality of abelian varieties satisfying a certain condition

LEMMA 1. (*Chow*) *Let A be an abelian variety defined over k in a projective space. Let C be an algebraic subgroup of A which is normally algebraic*

Received July 13, 1953.

[1] W. L. Chow: On the quotient variety of an abelian variety, Proc. Nat. Aca. Sci. Vol. 38, No. 12 (1952).

[2] C. L. Siegel: Additive Theorie der Zahlkörper, Math. Ann. Bd. 88 (1923).

https://doi.org/10.1017/S0027763000017086 Published online by Cambridge University Press

over k. Then there exists an abelian variety B defined over k in a projective space and a separable homomorphism from A onto B defined over k whose kernel is exactly C.

We call the abelian variety B the quotient variety of A by C.

LEMMA 2. *Let A be an abelian variety defined over k in a projective space and let B be an abelian variety defined over k from which there is a purely inseparable homomorphism λ defined over k onto A. Then B is isomorphic to an abelian variety defined over k in a projective space.*

Proof. Let x be a generic point of B over k and let $(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda)$ be the homogeneous coordinates of the generic point λx of A over k. Let $(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda, y_1, \ldots, y_m)$ be a point in a projective space of dimension $n+m$ such that $k(x)=k(\lambda x, y_1/x_0^\lambda, y_2/x_0^\lambda, \ldots, y_m/x_0^\lambda)$. Let Λ be the locus of $(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda, y_1, \ldots, y_m)$ over k in the projective space. Since Λ, A are non-singular and the function $(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda, y_1, \ldots, y_m) \to (x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda)$ is purely inseparable, this correspondence is one-to-one. Let x, z be independent generic points of B over k and let $(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda, y_1, \ldots, y_m)$, $(z_0^\lambda, z_1^\lambda, \ldots, z_n^\lambda, w_1, \ldots, w_m)$ be the independent generic points over k corresponding to $(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda)$, $(z_0^\lambda, z_1^\lambda, \ldots, z_n^\lambda)$ respectively. We introduce a law of composition such that

$$(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda, y_1, \ldots, y_m)\cdot(z_0^\lambda, z_1^\lambda, \ldots, z_n^\lambda, w_1, \ldots, w_m)$$
$$=((x+z)_0^\lambda, (x+z)_1^\lambda, \ldots, (x+z)_n^\lambda, u_1, u_2, \ldots, u_m),$$

where $((x+z)_0^\lambda, (x+z)_1^\lambda, \ldots, (x+z)_n^\lambda, u_1, u_2, \ldots, u_m)$ is the point of Λ corresponding to the point $\lambda(x+z)$ of A. Since the specialization of x over any specialization of λx is uniquely determined, the specialization of $(x_0^\lambda, x_1^\lambda, \ldots, x_n^\lambda, y_1, \ldots, y_m)$ over the specialization $\lambda(z+x)$ of $x+z$ is equal to $((x+z)_0^\lambda, (x+z)_1^\lambda, \ldots, (x+z)_n^\lambda, u_1, u_2, \ldots, u_m)$. Hence $k(\lambda x, y_1/x_0^\lambda, y_2/x_0^\lambda, \ldots, y_m/x_0^\lambda, \lambda z, w_1/z_0^\lambda, w_2/z_0^\lambda, \ldots, w_m/z_0^\lambda)=k(x, z)\supset k(x+z)=k(\lambda(x+z), u_1/(x+z)_0^\lambda, u_2/(x+z)_0^\lambda, \ldots, u_m/(x+z)_0^\lambda)$. Easily we prove the associative law and the existence of unit and inverses. Moreover Λ is complete, hence Λ is an abelian variety over k and is isomorphic to B.

Similarly we can verify the following lemma.

LEMMA 3. *Let A be an abelian variety defined over k in a projective space and let $(x_0, x_1, \ldots, x_n)$ be a generic point of A over k. Then the locus B of $(x_0^{p^\nu}, x_1^{p^\nu}, \ldots, x_n^{p^\nu})$ over k is an abelian variety defined over k, where p is the characteristic of k.*

LEMMA 4. *Any abelian variety A defined over k is isomorphic to an abelian variety defined over the algebraic closure $\bar{k}$ in a projective space.*

Proof. Since any curve is birationally equivalent to a non-singular curve in a projective space, its Jacobian variety is always constructed in a projective space by Chow's method and we can choose the algebraic closure of the field of definition for the curve as a field of definition for the Jacobian variety. On the other hand we can easily see that there exists a curve defined over $\bar{k}$ on A which does not lie on any translation of a proper abelian subvariety of A. Hence there exist a Jacobian variety J defined over k in a projective space and a homomorphism λ from J onto A. Let C be the kernel of λ on J and let B be the quotient variety of J by C, which exists in a projective space and is defined over k, by Lemma 1. We denote by ρ the separable homomorphism from J onto B whose kernel is C. Let x be a generic point of J over k and B' be the locus of $((x_0^\rho)^{\nu_i(\lambda)}, (x_1^\rho)^{\nu_i(\lambda)}, \ldots, (x_1^\rho)^{\nu_i(\lambda)})$[3] over $\bar{k}$, which is an abelian variety by Lemma 3, $(x_0^\rho, x_1^\rho, \ldots, x_n^\rho)$ being the homogeneous coordinate of the point ρx of B. Then $\bar{k}(\lambda x) \supset \bar{k}((x_1^\rho/x_0^\rho)^{\nu_i(\lambda)}, \ldots, (x_n^\rho/x_0^\rho)^{\nu_i(\lambda)}$ and $[\bar{k}(\lambda x) : \bar{k}((x_1^\rho/x_0^\rho)^{\nu_i(\lambda)}, \ldots, (x_n^\rho/x_0^\rho)^{\nu_i(\lambda)})]_s = 1$. Hence the one-to-one correspondence $\lambda x \longleftrightarrow ((x_0^\rho)^{\nu_i(\lambda)}, (x_1^\rho)^{\nu_i(\lambda)}, \ldots, (x_1^\rho)^{\nu_i(\lambda)})$ is a purely inseparable homomorphism from A onto B'. By virtue of Lemma 2 there exists an abelian variety defined over k in a projective space which is isomorphic to A.

By virtue of Lemma 4 we get the following lemma.

LEMMA 5. *Let A be an abelian variety defined over k and let C be an algebraic subgroup which is algebraic over k. Then there exists an abelian variety B in a projective space defined over $\bar{k}$ and a separable homomorphism defined over $\bar{k}$ from A onto B whose kernel is exactly C.*

LEMMA 6. *Let X, Y be non-degenerate divisors*[4] *on a Jacobian variety satisfying $X - Y \equiv 0$.*[5] *Then there exists a point t such that $Y \sim X_t$.*

Proof. By virtue of Corollary 3 of Theorem 32, N° 62, § VII, [V] there exists an endomorphism δ'_X such that $X_t - X \sim \Theta_{\delta'_X t} - \Theta$. From $X - Y \equiv 0$, we can write $Y - X \sim \Theta_u - \Theta$ with a suitable point u. Since X is non-degenerate, δ'_X is an onto endomorphism. Hence there exists a point satisfying $\delta'_X t = u$. Therefore

$$X_t - X \sim \Theta_{\delta'_X t} - \Theta = \Theta_u - \Theta \sim Y - X.$$

Hence $X_t \sim Y$.

LEMMA 7. *Let A be an abelian variety and let X be a non-degenerate divisor*

3) $\nu_i(\lambda) = [\bar{k}(\lambda x) : \bar{k}(x)]_i$.

4) We mean by a non-degenerate divisor X a divisor such that $X_t - X \sim 0$ for only finite number of points t.

5) $Z \equiv 0$ means that $Z_t - Z \sim 0$ for all points t. We call such a divisor Z algebraically equivalent to zero.

on A. Then there exists a natural number c depending only on A such that for any divisor satisfying $Z \equiv 0$ there exists a point of A satisfying $cZ \sim X_t - X$.

Proof. Let A' be an abelian variety and let J be a Jacobian variety such that $A \times A'$ and J are isogeneous, which always exist. Let λ be a homomorphism from J onto $A \times A$ and let W be a non-degenerate divisor on A. Put $Y = Z + X$. Since $\lambda^{-1}(X \times A' + A \times W)$, by virtue of Lemma 6, there exists a point s of J such that

$$\lambda^{-1}(Y \times A' + A \times \mathrm{W}) \sim \lambda^{-1}(X \times A' + A \times W)_s.$$

Therefore

$$\lambda^{-1}(Y \times A' + A \times W) \sim \lambda^{-1}(X_u \times A + A \times W_v),$$
$$\lambda^{-1}((Y - X_u) \times A' + A \times (W - W_v)) \sim 0,$$

where u, v are the projections of λs on A, A' respectively. Hence

$$\lambda^{-1}(Y - X_u) \sim 0.$$

Let λ' be the homomorphism from $A \times A'$ onto J such that $\lambda\lambda' = \nu(\lambda)\delta_{A \times A'}$. Then

$$\lambda'^{-1}(\lambda^{-1}(Y - X_u)) = (\nu(\lambda)\delta_{A \times A'})^{-1}(Y - X_u) \sim \nu(\lambda)(Y - X_u) \sim 0.$$

Hence

$$\nu(\lambda)Z = \nu(\lambda)(Y - X) \sim \nu(\lambda)(X_u - X) \sim X_{\nu(\lambda)u} - X.$$

This proves our lemma.

We denote by $G_a(A)$ the group of all divisors algebraically equivalent to zero and by $G_l(A)$ the group of all divisors linearly equivalent to zero.

THEOREM 1. (*Existence theorem*) *Let A be an abelian variety defined over k. Then there exists an abelian variety A^* defined over $\bar{k}$ in a projective space satisfying*

$$G_a(A)/G_l(A) \cong A^*$$

and isogeneous to A. If A lies in a projective space, A^* is defined over k.

Proof. Let X be a non-degenerate divisor on A. Then there exists a natural number c depending only on A such that $cZ \sim X_t - X$ with a point t for any divisor satisfying $Z \equiv 0$. Putting $cu = t$, we have $Z = c(X_u - X) + (Z - c(X_u - X))$. Hence

$$G_a(A) = \{cZ\ ;\ Z \equiv 0\} \cup \{Z\ ;\ cZ \sim 0\},$$
$$G_l(A) \cap \{cZ\ ;\ Z \equiv 0\} = \{cZ\ ;\ cZ \sim 0\}.$$

Therefore

$$G_a(A)/G_l(A) \cong \{cZ\ ;\ Z \equiv 0\}/\{cZ\ ;\ cZ \sim 0\}.$$

Let C be the subgroup of all points t of A satisfying $X_t - X$. Then C is a finite subgroup normally algebraic over k. Let A be the quotient abelian variety of A by C and let λ be the separable homomorphism from A onto A^* whose kernel is C. Since $cZ \sim X_t - X \sim 0$ if and only if $t \in C$, $\{cZ\ ;\ Z \equiv 0\}/\{cZ\ ;\ cZ \sim 0\} \cong A^*$. Therefore

$$G_a(A)/G_l(A) \cong A^*.$$

When A lies in a projective space, A^* is defined over k by Lemma 1.

LEMMA 8. *Let V be a normal projective variety defined over a field k and let X be a V-divisor linearly equivalent to zero. Then every specialization X' of X over k is also linearly equivalent to zero.*

This can be proved in the same way as in the case of a curve.[6)]

LEMMA 9. *Let X be a divisor on an abelian variety. If X is linearly equivalent to zero, then any specialization of X' is also linearly equivalent to zero.*

This is an immediate consequence of Lemma 5 and Lemma 8.

LEMMA 10. *Let X, Y be non-degenerated divisors of an abelian variety. Then for any point t there exists at least one point s such that $X_t - X \sim Y_s - Y$.*

Proof. From Lemma 7 $c(X_u - X) \sim Y_s - Y$ with a certain s. Putting $cu = t$, we have $c(X_u - X) \sim X_{cu} - X \sim X_t - X \sim Y_s - Y$.

LEMMA 11. *Let X, Y be non-degenerate divisors on an abelian variety A defined over k and let x be a generic point of A over k. Let y be the point of A such that $X_x - X \sim Y_y - Y$. Then $k(x, y)$ is algebraic over $k(x)$, $k(y)$ and y is also a generic point of A over k.*

Proof. Let Δ be the locus of (x, y) over $\bar{k}$. Since $A \times A$ is complete, Δ is also complete. $(X_x - X) - (Y_y - Y) \sim 0$, hence by virtue of Lemma 10 $(X_{x'} - X) - (Y_{y'} - Y) \sim 0$ for any specialization (x', y') of (x, y) over k. On the other hand X, Y are non-degenerate, hence the number of the specializations of y over any specialization x' of x is always finite. This shows that y is algebraic over $k(x)$. Similarly x is algebraic over $k(y)$. Hence y is also a generic point of A over k.

THEOREM 2. *Let X, Y be non-degenerate divisors on an abelian variety A defined over k. Let A_1^* be the quotient abelian variety of A by the subgroup C_1 of points t satisfying $X_t - X \sim 0$ and let λ be the separable homomorphism from A onto A_1^* whose kernel is the subgroup C_1, and let A_2^* be the quotient abelian*

6) See Lemma 10, N° 35, § V, [V].

variety of A be the subgroup C_2 of points s satisfying $Y_s - Y \sim 0$ and μ be the separable homomorphism whose kernel is C_2. Then there exists an abelian variety from which there exist purely inseparable homomorphisms onto A_1^*, A_2^* respectively.

Proof. Using the notations in the proof of Lemma 11, (x, y) is a generic pair of points of A over k such that $X_x - X \sim Y_y - Y$. Let A^* be the locus of $(\lambda x, \mu y)$ over k. Then $k(\lambda x, \mu y)$ is purely inseparable over $k(\lambda x)$, $k(\mu y)$ and a law of composition is introduced onto A^* as follows:

$$(\lambda x, \mu y)(\lambda u, \mu v) = (\lambda(x+u), \mu(y+v)),$$

where (x, y), (u, v) are independent generic pairs of points of A satisfying $X_x - X \sim Y_y - Y$, $X_u - X \sim Y_v - Y$, which are also generic points of A^* from Lemma 11. This clearly satisfies the conditions of the law of group composition. Since A^* is complete, A^* is an abelian variety. This A^* is our abelian variety.

This theorem shows that the abelian variety A^* constructed in the proof of Theorem 1 is uniquely determined within purely inseparable homomorphisms. Therefore we call A^* a model of the Picard variety of A.

COROLLARY. *All models of the Picard variety of an abelian variety defined over a field of characteristic zero are each other isomorphic.*

THEOREM 3. (*Duality*) *Let A be an abelian variety with a non-degenerate divisor X such that there is no point t satisfying $X_t - X \sim 0$ and $p^\nu t = 0$ with a ν. Let A^* be a model of the Picard variety of A. Then A is a model of the Picard variety of A^*.*

Proof. Let λ be the separable homomorphism from A onto A^* such that $\lambda t = 0$ if and only if $X_t - X \sim 0$. Let λ' be the homomorphism from A^* onto A such that $\lambda'\lambda = \nu(\lambda)\delta_A$,[7] $\lambda\lambda' = \nu(\lambda)\delta_{A^*}$, and let $t_1, t_2, \ldots, t_{\nu(\lambda)}$ be all points of A satisfying $\lambda t = 0$, $i = 1, 2, \ldots, \nu(\lambda)$. Since $X_{t_1} + X_{t_2} + \ldots + X_{t_{\nu(\lambda)}}$ is invariant for all translations by $t_1, \ldots, t_{\nu(\lambda)}$ and p does not divide $\nu(\lambda)$, by virtue of Proposition 13, N° 78, § XI, [V], there exists a divisor Y on A such that $X_{t_1} + X_{t_2} + \ldots + X_{t_{\nu(\lambda)}} = \lambda^{-1}(Y)$. Since $X_{t_1} + X_{t_2} + \ldots + X_{t_{\nu(\lambda)}} = \nu(\lambda)X$ and $\lambda'^{-1}(\lambda^{-1}(Y)) = (\nu(\lambda)\delta_{A^*})^{-1}(Y) \equiv \nu(\lambda)^2 Y \equiv \lambda'^{-1}(\nu(\lambda)X) \equiv \nu(\lambda)\lambda'^{-1}(X)$, $\nu(\lambda)Y \equiv \lambda'^{-1}(X)$. Therefore $E_l(\lambda'^{-1}(X)) = E_l(\nu(\lambda)Y)$, $E_l(\lambda^{-1}(Y)) = E_l(\nu(\lambda)X)$. From the formula in N° 77, § XI, [V].

$E_l(\lambda^{-1}(X)) = {}^tM(\lambda)E_l(X)M(\lambda) = \nu(\lambda)E_l(Y)$, $E_l(\lambda'^{-1}(Y)) = {}^tM_l(\lambda')E_l(Y)M_l(\lambda) = \nu(\lambda)E_l(X)$. Since $X_{\nu(\lambda)t} - X \sim 0$ if and only if $\lambda\nu(\lambda)t = \nu(\lambda)\lambda t = 0$, $X_{\nu(\lambda)t} - X \sim \nu(\lambda)(X_t - X) \sim 0$ if and only if $\nu(\lambda)\lambda t = \lambda\nu(\lambda)t = 0$. Hence $\lambda^{-1}(Y_u) - \lambda^{-1}(Y)$

[7] δ_A is the identical endomorphism of A.

~ 0 if and only if $\nu(\lambda)u=0$. Denoting by $\tau_l(u)$ the l-coordinate of u on A, $\nu(\lambda)\tau_l(u)\equiv 0 \pmod{1}$ if and only if ${}^tM_l(\lambda)E_l(Y)\tau_l(u)\equiv 0 \pmod{1}$. Hence $\nu(\lambda)U = {}^tM_l(\lambda)E_l(Y)$ with an l-adic unimodular matrix U and $E_l(Y)={}^tM_l(\lambda)^{-1}\nu(\lambda)U = {}^tM_l(\lambda)^{-1}{}^t(M_l(\lambda')M_l(\lambda))U={}^tM_l(\lambda')U$. From $E_l(Y)=-E_l(Y)$ we get $E_l(Y) = -{}^tUM_l(\lambda')$. Hence, when $l^\nu u=0$, $Y_u-Y\sim 0$ if and only if $\lambda'_u=0$. On the other hand there is no point satisfying $Y_t-Y\sim 0$ and $p^\nu t=0$ with a ν. This shows that A is a model of the Picard variety of A^*.

§ 2. Arithmetic preperations

LEMMA 1. *Let k be a number field and $'$ be an involution of k such that $S_p(\alpha'\alpha)>0$. Then k is a totally real or a totally imaginary field and $\alpha'=\bar{\alpha}$, where $\bar{\alpha}$ means the complex conjugate of α.*

Proof. Let k' be the invariant subfield of k by $'$ and let $k'=k'^{(1)},\ldots, k'^{(r_1)}, k'^{(r_1+1)},\ldots, k'^{(r_1+r_2)}, k'^{(r_1+r_2+1)},\ldots, k'^{(r_1+2r_2)}$ be the conjugate fields over the rational number field, where $k'^{(r_1+i)}$ and $k'^{(r_1+r_2+i)}$ $i=1,2,\ldots,r_2$ are mutually complex conjugate fields.

First we assume that $r_2\neq 0$. We take a number β of k' such that $|\beta^{(r_1+1)}| = |\beta^{(r_1+r_2+1)}|>2(r_1+2r_2)$, $|\beta^{(j)}|<1/2(r_1+2r_2)$ $(j\neq r_1+1, r_1+r_2+1)$ and $\pi/2\geqq \operatorname{Arg}\beta^{(r_1+1)}>3/8\pi$. This is always possible, for the numbers of $k'^{(r_1+1)}$ are dense on the complex plane and there exists a unit η_0 of k' such that

$$|\eta_0^{(r_1+1)}|=|\eta_0^{(r_1+r_2+1)}|>1,\ |\eta_0^{(j)}|<1 \qquad (j\neq r_1+1,\ r_1+r_2+1),$$

therefore there exists η satisfying for arbitrary positive ε_0 and M,

$$|\eta^{(r_1+1)}|=|\eta^{(r_1+r_2+1)}>M,\quad |\eta^{(j)}|<\frac{1}{M} \qquad (j\neq r_1+1,\ r_1+r_2+1),$$
$$\pi\geqq \operatorname{Arg}\eta^{(r_1+1)}>\pi-\varepsilon_0.$$

Hence

$$S_{p_k}(\beta'\beta)=2\sum_{i=1}^{r_1+2r_2}\beta^{(i)^2}<2(-(2(r_1+2r_2)/\sqrt{2})$$
$$+((r_1+2(r_2-1))/2(r_1+2r_2)))<0.$$

This contradicts to the assumption in Lemma. Hence $r_2=0$.

Let $\sqrt{\alpha_0}$ be the canonical generater of k over k' and let be $\alpha_0^{(1)},\ldots, \alpha_0^{(r)}>0$ and $\alpha_0^{(r+1)},\ldots,\alpha_0^{(n/2)}<0$, where n is the (absolute) degree of k'. We take a number β of k' satisfying

$$|\beta^{(i)}|>\sqrt{2n/\alpha^{(i)}} \qquad (i=1,2,\ldots,r),$$
$$|\beta^{(j)}|<\sqrt{-1/\alpha^{(j)}} \qquad (j=r+1,\ldots,n/2).$$

Then $\beta^{(i)^2}\alpha_0^{(i)}>2n$ $(i=1,2,\ldots,r), 0<-\beta^{(j)^2}\alpha_0^{(j)}<1$ $(j=r+1,\ldots,n/2)$. Hence

$$S_{p_k}((1+\beta\sqrt{\alpha_0})'(1+\beta\sqrt{\alpha_0}))=2S_{p_{k'}}((1+\beta\sqrt{\alpha_0})(1-\beta\sqrt{\alpha_0}))$$
$$=2\sum_{i=1}^{r}(1-\beta^{(i)^2}\alpha_0^{(i)})+2\sum_{j=r+1}^{n/2}(1-\beta^{(j)^2}\alpha_0^{(j)})\leqq 2r(1-2n)+2\cdot 2(n/2-r).$$

Therefore $r=0$.

This shows that if $k\neq k'$ then k is totally imaginary. Hence $\alpha'=\bar{\alpha}$ for either case $k=k'$ or $k\neq k'$.

PROPOSITION 1. *The center $\mathfrak{z}$ of the ring of endomorphisms $\mathfrak{A}(A)$ of a simple abelian variety is totally real or totally imaginary.*

Proof. Let $M_l(\beta)$ be an l-adic representation by l-coordinates with $l\neq p$. As we see in §X, [V] the characteristic polynomial of $M_l(\beta)$ has rational coefficients. Therefore there exists a non-singular matrix F of an extension of the l-adic field such that

$$F^{-1}M_l(\beta)F=\begin{pmatrix} \beta^{(1)} & & & & & & & & \\ & \cdot & & & & & & & \\ & & \cdot & & & & & & \\ & & & \beta^{(1)} & & & & & \\ & & & & \cdot & & & & \\ & & & & & \beta^{(r)} & & & \\ & & & & & & \cdot & & \\ & & & & & & & \cdot & \\ & & & & & & & & \beta^{(r)} \end{pmatrix}$$

where $\beta=\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(r)}$ are mutually conjugate over the rational field. If β is in $\mathfrak{z}$, then β' also belongs to $\mathfrak{z}$. Moreover we can take the same F for all elements β of the center, hence

$$F^{-1}M_l(\beta')F=\begin{pmatrix} \beta'^{(1)} & & & & & & & & \\ & \cdot & & & & & & & \\ & & \cdot & & & & & & \\ & & & \beta'^{(1)} & & & & & \\ & & & & \cdot & & & & \\ & & & & & \beta'^{(r)} & & & \\ & & & & & & \cdot & & \\ & & & & & & & \cdot & \\ & & & & & & & & \beta'^{(r)} \end{pmatrix}$$

https://doi.org/10.1017/S0027763000017086 Published online by Cambridge University Press

$$F^{-1}M_l(\beta\beta')F=\begin{pmatrix}\beta^{(1)}\beta'^{(1)} & & & & & \\ & \ddots & & & & \\ & & \beta^{(1)}\beta'^{(1)} & & & \\ & & & \ddots & & \\ & & & & \beta^{(r)}\beta'^{(r)} & \\ & & & & & \ddots \\ & & & & & & \beta^{(r)}\beta'^{(r)}\end{pmatrix}$$

Each conjugate field $\mathfrak{z}^{(i)}$ has a function $\hat{\sigma}(\beta^{(i)})=\sigma(\beta)=S_pM_l(\beta)=nSp_{\mathfrak{z}^{(i)}}(\beta)$, where n is the multiplicity of β' in the characteristic equations $\sigma(\beta\beta')=\hat{\sigma}((\beta\beta')^{(i)})$ $=nSp_{\mathfrak{z}^{(i)}}(\beta\beta')>0$. This shows that $\beta^{(i)\prime}=\overline{\beta^{(i)}}$ and $\mathfrak{z}$ is totally real or totally imaginary from Lemma 1.

Proposition 2. *Let α be a symmetric element of the ring of endomorphism $\mathfrak{A}(A)$ of an abelian variety. Then the roots of the characteristic equation of $M_l(\alpha)$ are all real.*

This is an immediate consequence from the fact that $M_l(\alpha)$ can be transformed into a diagonal form and Lemma 1.

Proposition 3. *Let X be a positive divisor on a Jacobian variety. Then the roots of the chacteristic equation of $M_l(\delta'_X)$ are non-negative.*

Proof. By Corollaire 1 of Théorèm 31, N° 61, § VIII, [V], $\sigma(\lambda'\delta'_X\lambda)\geqq 0$ for all endomorphisms λ of J. Let $\mathfrak{B}$ be a commutative subring of symmetric elements in $\mathfrak{A}(J)$ containing δ'_X. Then all matrices $M_l(\beta)$ with β in $\mathfrak{B}$ are transformed into a diagonal form with a matrix F, so as, in particular

$$F^{-1}M_l(\delta'_X)F=\begin{pmatrix}\chi_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \chi_n & & & & & & \\ & & & \chi_1^{(1)} & & & & & \\ & & & & \ddots & & & & \\ & & & & & \chi_n^{(1)} & & & \\ & & & & & & \chi_1^{(r)} & & \\ & & & & & & & \ddots & \\ & & & & & & & & \chi_n^{(r)}\end{pmatrix}$$

where $(\chi_\nu, \chi_\nu^{(1)}, \ldots, \chi_\nu^{(r)})$ is a complete set of conjugates over the rational number field. By virtue of Proposition 2 all diagonal elements of $F^{-1}M_l(\beta)F$ with $\beta \in \mathfrak{B}$ are real. From the independence of valuations, $\{(\beta/m, \beta^{(1)}/m, \ldots, \beta^{(r)}/m)\}$ is dense in $r+1$ dimensional euclidean space, where m runs over all rational integers.

$$\sigma(\beta'/m \cdot \delta'_X \beta/m) = 1/m^2 \sum_{\nu, i} \chi_\nu^{(i)} \beta_\nu^{(i)^2} = \sum_{\nu, i} \chi_\nu^{(i)} (\beta^{(i)}/m)^2 \geqq 0,$$

hence

$$\chi_\nu^{(i)} \geqq 0, \qquad i = 1, 2, \ldots, r\ ;\ \nu = 1, 2, \ldots, n.$$

§ 3. Proof of the main theorem.

DEFINITION. *Let X be a divisor on an algebraic variety V over k and let K be a field containing k over which X is rational. We denote by $l(X)$ the dimension over K of the module of functions $f(x)$ on V defined over K satisfying $(f(x)) \succ -X$.*

By virtue of Theorem 10, [3], [VIII], [F], $l(X)$ does not depend on K.

PROPOSITION 4. *Let X, Y be divisors on algebraic varieties A and B respectively. Then $l(X \times B + A \times Y) = l(X) \cdot l(Y)$.*

This is an immediate consequence from the definition of $l(X)$.

LEMMA 1. *Let J be a Jacobian variety and let Θ[8] be the theta divisor on J. Then $l(\Theta) = 1$.*

Proof. Let Γ be the non-singular curve corresponding to J and let φ be the canonical function. Let k be a common field of definition for J, φ, Θ and let x be a generic point of J over k. Then by virtue of Theorem 20, § V, [V], $\varphi(\Gamma) \cdot \theta_x$ is a non-special divisor on $\varphi(\Gamma)$. Suppose that y is present in $\varphi(\Gamma) \cdot \Theta_x$ with a positive multiplicity. Then $y - x$ is in Θ, and $y - x$ is a generic point of Θ over k, for the dimension of y over k is one and the dimension of x over k is equal to the dimension of J. Let Y be a positive divisor defined over k such that $Y \sim \Theta$. Since $\varphi(\Gamma) \cdot \Theta_x$ is non-special, $\varphi(\Gamma) \cdot Y_x = \varphi(\Gamma) \cdot \Theta_x$. Hence $y - x$ is in a component of Y. On the other hand $y - x$ is a generic point of Θ over k and Y is rational over k, hence Θ is present in Y with a positive multiplicity. Since $Y \sim \Theta$, necessarily $Y = \Theta$. This shows $l(\Theta) = 1$.

LEMMA 2. *Let X be a divisor on an abelian variety. If $u = u_1 + u_2 + \ldots + u_n$, $l_1^{e_1} u_1 = l_2^{e_2} u_2 = \ldots = l_n^{e_n} u_n = 0$ and $(l_i, p) = 1$, $(l_i, l_j) = 1(i, j = 1, 2, \ldots,$*

8) See N° 40 § V, [W].

n). Then $X_u - X \sim 0$, if and only if $E_{l_i}(X)\tau_{l_i}(u_i) \equiv 0 \mod 1$ $(i = 1, 2, \ldots, n)$, where $\tau_{l_i}(u_i)$ means the l_i-coordinate of u_i.

Proof. The case $n = 1$ is the result in 76°, § XI, [V]. We shall apply the induction on n. We assume that this is true for $n-1$. If $X_u - X \sim 0$, $l_j^{e_j}(X_u - X) \sim (X_{l_j^{e_j}u} - X) = X_{l_j^{e_j}(u_1+u_2+\ldots+u_n)} - X = X_{l_j^{e_j}(u_1+\ldots+u_{j-1}+u_{j+1}+\ldots+u_n)} - X \sim 0$. By virtue of the assumption of indution

$$E_{l_i}(X)\tau_{l_i}(l_j^{ej}u_i) \equiv l_j^{ej}E_{l_i}(X)\tau_{l_i}(u_i) \equiv 0 \mod 1 \text{ for } i \neq j.$$

Since $(l_i, l_j) = 1$,

$$E_{l_i}(X)\tau_{l_i}(u_i) \equiv 0 \mod 1 \qquad (i = 1, 2, \ldots, n).$$

The convers is clear.

THEOREM 4. *Let A, B be abelian varieties, let λ be a homomorphism from A onto B satisfying $p \nmid \nu(\lambda)$ and let X be a positive non-degenerate divisor of B. Then $l(\lambda^{-1}(X)) = \nu(\lambda)l(X)$.*

Proof. Let k be a common field of definition for A, B, λ over which all the points satisfying $\lambda t = 0$ and the divisors $X_t - X$, $\lambda^{-1}(X_u - X)$ satisfying $X_t - X \sim 0$, $\lambda^{-1}(X_u - X) \sim 0$ are rational. Let x be a generic point of A over k. Then, by virtue of Theorem 12 and its Corollary, N° 27, § IV, [V], $k(x)$ is normaly algebraic over $k(\lambda x)$ and the galois group is isomorphic to the group of all points t_i satisfying $\lambda t_i = 0$; $x + t_1, x + t_2, \ldots, x + t_{\nu(\lambda)}$ $(i = 1, 2, \ldots, \nu(\lambda))$ is the complete set of conjugates of x over $k(\lambda x)$. From the formula $E_l(\lambda^{-1}(X)) = {}^tM_l(\lambda)E_l(X)M_l(\lambda)$ in N° 76, § XI, [V] and Lemma 2, there exist points $u_1, u_2, \ldots, u_{\nu(\lambda)}$ of B such that $\lambda^{-1}(X_{u_i} - X) \sim 0$ and $X_{u_i} - X_{u_j} \nsim 0$ for $i \neq j$ $(i, j = 1, 2, \ldots, \nu(\lambda))$. Since $\lambda^{-1}(X_{u_i} - X)$ $(i = 1, 2, \ldots, \nu(\lambda))$ are rational over k, there exist functions $\phi_1(x), \phi_2(x), \ldots, \phi_{\nu(\lambda)}(x)$ in $k(x)$ such that

$$(\phi_1(x)) = \lambda^{-1}(X_{u_1} - X), \quad (\phi_2(x)) = \lambda^{-1}(X_{u_2} - X), \ldots, (\phi_{\nu(n)}(x))\lambda^{-1}(X_{u_{\nu(\lambda)}} - X).$$

From $\lambda^{-1}(X)_t = \lambda^{-1}(X_{\lambda t})$, $\lambda^{-1}(X_{u_i} - X)_{t_j} = \lambda^{-1}(X_{u_i} - X)$ $(i, j = 1, 2, \ldots, \nu(\lambda))$. Hence

$$\phi_i(x + t_j) = e_i(t_j)\phi_i(x),$$

where $e_i(t_j)$ $(i, j = 1, 2, \ldots, \nu(\lambda))$ are roots of unit.

Since $X_{u_i} \nsim X_{u_j}$ for $i \neq j$, $e_i(t_j)$ $(i = 1, 2, \ldots, \nu(\lambda))$ are different with each other as functions of t_j $(j = 1, 2, \ldots, \nu(\lambda))$.

From this result we can conclude that $\{\phi_1(x), \ldots, \phi_{\nu(\lambda)}(x)\}$ is a base of $k(x)$ over $k(\lambda x)$ and $\{e_i(t) ; i = 1, 2, \ldots, \nu(\lambda)\}$ is the character group $\chi(\mathfrak{G})$ of the galois group $\mathfrak{G} = \{t_1, \ldots, t_{\nu(\lambda)} ; \lambda t_i = 0\}$.

By virtue of the fundamental theorem of abelian group, $\mathfrak{G} = \mathfrak{Z}_1 + \mathfrak{Z}_2 + \ldots + \mathfrak{Z}_h$, where $\mathfrak{Z}_i$ are cyclic groups of prime power order. Let $\{1, e_1(t), e_2(t),$

$\ldots, e_{l_1^{n_1}-1}(t)\}$ be the annihilator of $\mathfrak{Z}_2+\ldots+\mathfrak{Z}_h$ after suitable permutations of suffices of $e_i(t)$. Let t be a generator of z_1.

Let $f(x)$ be a function defined over k satisfying $f(x) \succ -X$. We write

$$f(x)=\sum_{i=1}^{\nu(\lambda)} a_i(\lambda x)\phi_i(x)$$

by the above base.

$$f(x+t)-f(x)=\sum_{j=1}^{l_1^{n_1}-1}(e_j(t)-1)a_j(\lambda x)\phi_j(x)$$

$$f(x+2t)-f(x+t)=\sum_{j=1}^{l_1^{n_1}-1}(e_j(t)-1)e_j(t)a_j(\lambda x)\phi_j(x)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f(x)-f(x+(l_1^{n_1}-1)t)=\sum_{j=1}^{l_1^{n_1}-1}(e_j(t)-1)e_j(t)^{l_1^{n_1}-1}a_j(\lambda x)\phi_j(x).$$

Since $e_j(t)=e(t)^{f_j}$, where $e(t)$ is a generator of $\{1, e_1(t), e_2(t), \ldots, e_{l_1^{n_1}-1}(t)\}$ and $f_i \neq f_j$ for $i \neq j$,

$$\begin{vmatrix} e_1(t), & e_2(t) & \ldots & e_{l_1^{n_1}-1}(t) \\ e_1(t)^2 & e_2(t)^2 & \ldots & e_{l_1^{n_1}-1}(t)^2 \\ \vdots & \vdots & & \vdots \\ e_1(t)^{l_1^{n_2}-1} & & \ldots & e_{l_1^{n_1}-1}(t)^{l_1^{n_1}-1} \end{vmatrix} = \pm\prod_j e_j(t)\prod_{h>k}(e_h(t)-e_k(t))$$

$$=\pm\prod_j e(t)\prod_{h>k}^{f_j}(e(t)^{f_h}-e(t)^{f_k})\neq 0.$$

This shows that the above system of linear equations are uniquely solvable with respect to $a_1(\lambda x)\phi_1(x), a_2(\lambda x)\phi_2(x), \ldots, a_{l_1^{n_1}-1}(\lambda x)\phi_{l_1^{n_1}-1}(x)$. Hence

$$a_j(\lambda x)\phi_j(x)=\sum_{k=0}^{l_1^{n_1}-1}c_k f(x+kt) \qquad (j=1, 2, \ldots, l_1^{n_1}-1).$$

By the same method we can determine all $a_i(\lambda x)\phi_i(x)$ $(i=1, 2, \ldots, \nu(\lambda)-1)$ except $a_{\nu(\lambda)}(\lambda x)\phi_{\nu(\lambda)}(x)$ where we assume that $e_{\nu(\lambda)}(t)\equiv 1$.

Let $(a_i(x))=A_i-B_i$ $(i=1, 2, \ldots, \nu(\lambda))$. Since $(f(x+kt_i))\succ -\lambda^{-1}(X)_{kt}=-\lambda^{-1}(X)$ for $i=1, 2, \ldots, \nu(\lambda)-1$, we have

$$(a_i(\lambda x)\phi_i(x))=\lambda^{-1}(A_i)+\lambda^{-1}(X_{u_i})-\lambda^{-1}(B_i)-\lambda^{-1}(X)\succ -\lambda^{-1}(X).$$

Hence

$$\lambda^{-1}(A_i)-\lambda^{-1}(B_i)\succ -\lambda^{-1}(X_{u_i}))$$

and $A_i-B_i\succ -X_{u_i}$. This shows that the dimension of the module $\{a_i(\lambda x)\}$ over k is exactly $l(X)$ for $i=1, 2, \ldots, \nu(\lambda)-1$.

$$(a_{\nu(\lambda)}(\lambda x)\phi_{\nu(\lambda)}(x)) = (f(x) - \sum_{i=1}^{\nu(\lambda)-1} a_i(\lambda x)\phi_i(x)) \succ -\lambda^{-1}(X),$$

hence $\lambda^{-1}(A_{\nu(\lambda)}) + \lambda^{-1}(X_{\nu(\lambda)}) - \lambda^{-1}(B_{\nu(\lambda)}) - \lambda^{-1}(X) \succ -\lambda^{-1}(X)$,

$$\lambda^{-1}(A_{\nu(\lambda)}) - \lambda^{-1}(B_{\nu(\lambda)}) \succ -\lambda^{-1}(X_{\nu(\lambda)}).$$

This shows that the dimension of the module $\{a_{\nu(\lambda)}(\lambda x)\}$ over k is also $l(X)$. Therefore $l(\lambda^{-1}(X)) = \nu(\lambda)l(X)$.

LEMMA 3 (*Siegel*). *Let k be a totally real number field. Then there exists an integral in k such that every totally positive integer in it is expressed as a sum of four squares of integers. In other words, there exists a uniquely determined natural number $c = c(k)$ such that, for every totally positive integer α, $c\alpha$ is expressible as a sum of four squares of integers.*

$c(k)$ shall be called Siegel's constant of k in the following.

LEMMA 4. *Let α be a symmetric element of $\mathfrak{A}(J)$ satisfying $\sigma(\beta'\alpha\beta) \geqq 0$ for all $\beta \in \mathfrak{A}(J)$. Then there exist a natural number c and an emdomorphism λ in $\mathfrak{A}(J^{(4)}) = \mathfrak{A}(J \times J \times J \times J)$ such that*

$$\begin{pmatrix} c\alpha & & & \\ & c\alpha & & \\ & & c\alpha & \\ & & & c\alpha \end{pmatrix} = \lambda'\lambda = \delta'_{\lambda^{-1}(\theta^{(4)})},$$

where $\theta^{(4)} = \theta \times J \times J \times J + J \times \theta \times J \times J + J \times J \times \theta \times J + J \times J \times J \times \theta$.

Proof. From the proof of Proposition 3, § 2, the roots of the characteristic equation of $M_l(\alpha)$ are all real and non-negative. Let $\mathfrak{B}$ be a maximal commutative subring of $\mathfrak{A}(J)$ of symmetric elements containing α. Then by a suitable non-singular matrix F

$$F^{-1}M_l(\beta)F = \begin{pmatrix} \beta_1^{(1)} & & & & & & \\ & \ddots & & & & & \\ & & \beta_n^{(1)} & & & & \\ & & & \ddots & & & \\ & & & & \beta_1^{(r)} & & \\ & & & & & \ddots & \\ & & & & & & \beta_1^{(r)} \end{pmatrix},$$

for all $\beta \in \mathfrak{B}$, where $(\beta_\nu^{(1)}, \beta_\nu^{(2)}, \ldots, \beta_\nu^{(r)})$ is the complete set of conjugates of β over the rational number field.[9] By virtue of Proposition 1, § 2, β_ν, $\beta_\nu^{(i)}$ $(i = 1,$

[9] Let $\mathfrak{B}_0$ be the ring generated by $\frac{\gamma}{n}$, $n = 1, 2, 3, \ldots$, $\gamma \in \mathfrak{B}$. Then $\mathfrak{B}_0$ is an algebra of type S. Therefore $\mathfrak{B}_0$ is semi-simple. This shows that there is a non-singular matrix with l-adic element F such that $F^{-1}M_l(\beta)F$ is diagonal for every $\beta \in \mathfrak{B}_0$.

$\ldots, r\,;\ \nu=1, \ldots, n)$ are all real. $\mathfrak{B}$ is a integral demain of a direct sum of real number fields and the elements on the diagonal of $F^{-1}M_l(\beta)F$ are all totally positive or zero ; for them Siegel's Lemma can be applied.

$$c\alpha=\gamma_1^2+\gamma_2^2+\gamma_3^2+\gamma_4^2 \quad \text{with} \quad \gamma_1,\ \gamma_2,\ \gamma_3,\ \gamma_4 \in \mathfrak{A}(A),$$

where c is the product of Siegel's constants of our components of $\mathfrak{B}$. This shows that

$$\begin{pmatrix} c\alpha & & & \\ & c\alpha & & \\ & & c\alpha & \\ & & & c\alpha \end{pmatrix}=\begin{pmatrix} \gamma_1 & -\gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_2 & \gamma_1 & -\gamma_4 & \gamma_3 \\ \gamma_3 & -\gamma_4 & -\gamma_1 & -\gamma_2 \\ \gamma_4 & \gamma_3 & \gamma_2 & -\gamma_1 \end{pmatrix}\begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ -\gamma_2 & \gamma_1 & -\gamma_4 & \gamma_3 \\ \gamma_3 & -\gamma_4 & -\gamma_1 & \gamma_2 \\ \gamma_4 & \gamma_3 & -\gamma_2 & -\gamma_1 \end{pmatrix}$$

$$={}^t\begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ -\gamma_2 & \gamma_1 & -\gamma_4 & \gamma_3 \\ \gamma_3 & -\gamma_4 & -\gamma_1 & \gamma_2 \\ \gamma_4 & \gamma_3 & -\gamma_2 & -\gamma_1 \end{pmatrix}\begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ -\gamma_2 & \gamma_1 & -\gamma_4 & \gamma_3 \\ \gamma_3 & -\gamma_4 & -\gamma_1 & \gamma_2 \\ \gamma_4 & \gamma_3 & -\gamma_2 & -\gamma_1 \end{pmatrix}$$

$$={}^t\begin{pmatrix} \gamma_1' & \gamma_2' & \gamma_3' & \gamma_4' \\ -\gamma_2' & \gamma_1' & -\gamma_4' & \gamma_3' \\ \gamma_3' & -\gamma_4' & -\gamma_1' & \gamma_2' \\ \gamma_4' & \gamma_3' & -\gamma_2' & -\gamma_1' \end{pmatrix}\begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ -\gamma_2 & \gamma_1 & -\gamma_4 & \gamma_3 \\ \gamma_3 & -\gamma_4 & -\gamma_1 & \gamma_2 \\ \gamma_4 & \gamma_3 & -\gamma_2 & -\gamma_1 \end{pmatrix}=\lambda'\lambda$$

where

$$\lambda=\begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ -\gamma_2 & \gamma_1 & -\gamma_4 & \gamma_3 \\ \gamma_3 & -\gamma_4 & -\gamma_1 & \gamma_2 \\ \gamma_4 & \gamma_3 & -\gamma_2 & -\gamma_1 \end{pmatrix}, \quad \lambda'={}^t\begin{pmatrix} \gamma_1' & \gamma_2' & \gamma_3' & \gamma_4' \\ -\gamma_2' & \gamma_1' & -\gamma_4' & \gamma_3' \\ \gamma_3' & -\gamma_4' & -\gamma_1' & \gamma_2' \\ \gamma_4' & \gamma_3' & -\gamma_2' & -\gamma_1' \end{pmatrix}$$

is the conjugate of λ as an element $\mathfrak{A}(J^{(4)})$ from Proposition 5. Hence

$$\begin{pmatrix} c\alpha & & & \\ & c\alpha & & \\ & & c\alpha & \\ & & & c\alpha \end{pmatrix}=\lambda'\lambda=\delta'_{\lambda^{-1}(\theta^{(4)})}\,.$$

DEFINITION. *A base divisor of an abelian variety A is the positive divisor of A satisfying* i) $l(U)=1$, ii) *for any divisor X of A there is an endomorphism δ_X' of A such that $X_t-X\sim U_{\delta_X' t}-U$.*

We shall denote by U always a base divisor and briefly shall call an abelian variety with a base divisor a *special abelian variety.*

LEMMA 5. *Let A be a special abelian variety. Then the ring of all square matrices of a certain degree, say n, over $\mathfrak{A}(A)$ is considered as the ring of endomorphisms of $A^{(n)}=\overbrace{A\times A\times \ldots \times A}^{n}$. Put $U^{(n)}=U\times A^{(n-1)}+A\times U\times A^{(n-2)}+\ldots+A^{(n-1)}\times U$. Then an involution $(\alpha_{ij})'={}^t(\alpha'_{ij})$ is introduced into $\mathfrak{A}(A^{(n)})$ such that $(\alpha_{ij})^{-1}(U_t^{(n)}-U^{(n)})\sim U^{(n)}_{(\alpha_{ij})'t}-U^{(n)}$.*

Proof. Let t be a generic point of A over a definition field k for A over which U is rational. Since $U_s-U\sim 0$ if and only if $s=0$, the point t^* such that

$(\alpha_{ij})^{-1}(U_t^{(n)} - U^{(n)}) \sim U_{t^*}^{(n)} - U^{(n)}$ is uniquely determined. Let $\varDelta$ be the locus of (t, t^*) over $\bar{k}$. Then by vertue of Lemma 11, § 1. $\bar{k}\ (t, t^*)$ is purely inseparable over $\bar{k}(t)$. Therefore $\bar{k}(t, p^\nu t^*) \supset \bar{k}(t)$ with a suitably large ν. Putting $t^* = (\alpha_{ij})^* t$, we have $p^\nu(\alpha_{ij})^* \in \mathfrak{A}(A^{(n)})$. Similarly as for θ on J, we have

$M_l(p^\nu(\alpha_{ij})^*) = E_l(U^{(n)})^{-1\,t} M_l(p^\nu(\alpha_{ij})) E_l(U^{(n)})$. After a suitable change of the l-coordinates of A,

$$E_l(U^{(n)}) = \begin{pmatrix} E_l(U) & & & & \\ & E_l(U) & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & E_l(U) \end{pmatrix}$$

and $M_l((\alpha_{ij})) = (M_l(\alpha_{ij}))$. Hence $M_l(p^\nu(\alpha_{ij})^*) = p^\nu M_l({}^t(\alpha'_{ij})) = p^\nu M_l((\alpha_{ij})')$ i.e. $(\alpha_{ij})^* = (\alpha_{ij})'$.

We can prove the following lemma similarly as for Θ on J.

LEMMA 6. *Let A be a special abelian variety. Then for every symmetric element α of $\mathfrak{A}(A)$ (by an involution induced by a basic divisor U) there exists a divisor X such that*

$$2\alpha = \delta'_X, \quad \text{where} \quad X_t - X \sim U_{\delta'_X t} - U.$$

Moreover, if $p \neq 2$, we can choose X such that $\alpha = \delta'_X$.

LEMMA 7. *Let A, B be abelian varieties and let λ be a separable homomorphism from A onto B satisfying $\nu(\lambda) \neq 0$. Let X be a divisor on B. Then $l(\lambda^{-1}(X)) \geqq 1$ if and only if $l(X) \geqq 1$.*

Proof. Let k be a common field of definition for A, B and λ over which all points $t_1, \ldots, t_{\nu(\lambda)}$ satisfying $\lambda t_i = 0$ are rational. Let x be a generic point of A over k. Let $f(x)$ be a function defined over k satisfying $(f(x)) \succ -\lambda^{-1}(X)$. Let $(f(x) = f_1(x), f_2(x), \ldots, f_{\nu(\lambda)}(x))$ be the complete set of conjugates over $k(\lambda x)$. Then the representation $M_l(t_j)$ of the Galois group $\{t_1, t_2, \ldots, t_{\nu(\lambda)}\,;\ \lambda t_i = 0\}$ by permutations of $f_1(x), f_2(x), \ldots, f_{\nu(\lambda)}(x)$ can be considered.

From the theory of representation of abelian groups $\{M(t_j)\}$ is equivalent to

$$\left\{\begin{pmatrix} e_1(t_j) & & & & \\ & e_2(t_j) & & & 0 \\ & & \cdot & & \\ & * & & \cdot & \\ & & & & e_{\nu(\lambda)}(t_j) \end{pmatrix}\right\}$$

where $e_h(t_j)$ $(j = 1, 2, \ldots, \nu(\lambda),\ h = 1, 2, \ldots, \nu(\lambda))$ are roots of the unit. Let the equivalence is effected by the matrix F. We put $(f_1(x), \ldots, f_{\nu(\lambda)}(x))F$

$= (g_1(x), \ldots, g_{\nu(\lambda)}(x))$. Then

$$g_{\nu(\lambda)}(x+t_j) = e_{\nu(\lambda)}(t_j) g_{\nu(\lambda)}(x) \quad (j = 1, 2, \ldots, \nu(\lambda)),$$
$$(f_1(x)) = (f(x)) \succ -\lambda^{-1}(X),$$
$$(f_2(x)) = (f(x+t_2)) \succ -\lambda^{-1}(X)_{t_2} = -\lambda^{-1}(X), \ldots,$$
$$(f_{\nu(\lambda)}(x)) = (f(x+t_{\nu(\lambda)})) \succ -\lambda^{-1}(X)_{t_{\nu(\lambda)}} = -\lambda^{-1}(X),$$

hence

$$(g_{\nu(\lambda)}(x)) \succ -\lambda^{-1}(X).$$

We put $Z = (g_{\nu(\lambda)}(x)) + \lambda^{-1}(X)$. Then $Z \succ 0$ and $Z \sim \lambda^{-1}(X)$. Since $\lambda t_i = 0$ and $k(x)/k(\lambda x)$ is separable, $Z_{t_i} = (g_{\nu(\lambda)}(x))_{t_i} + \lambda^{-1}(X)_{t_i} = (g_{\nu(\lambda)}(x+t_i)) + \lambda^{-1}(X) = (g_{\nu(\lambda)}(x)) + \lambda^{-1}(X) = Z$.

Hence, by virtue of Proposition 33, $N°$ 78, § XI, [V], there exists a divisor Y on B such that $Z = \lambda^{-1}(Y)$. From $Z \succ 0$, $Y \succ 0$. Since $Z \sim \lambda^{-1}(X)$, $\lambda^{-1}(Y) - \lambda^{-1}(X) \sim \lambda^{-1}(Y - X) \sim 0$. Hence $Y \equiv X$. Therefore $l(X) = l(Y) \geqq 1$.

LEMMA 8. *Let A be a special abelian variety with a positive basic divisor U. Then the operation $'$ on $\mathfrak{A}(A)$ which is defined by $\alpha^{-1}(U_t - U) \sim U_{\alpha' t} - U$ is an involution satisfying* i) $\sigma(\alpha') = \overline{\sigma(\alpha)}$, ii) $\sigma(\alpha'\alpha) = \sigma(\alpha\alpha') > 0$ *for* $\alpha \neq 0$, *where* $\sigma(\alpha) = S_p M_l(\alpha)$.

Proof. Similarly for Θ on a Jacobian variety we get $M_l(\alpha') = E_l(U)^{-1\,t}M_l(\alpha) E_l(U)$, $M_l(\delta'_X) = E_l(U)^{-1} E_l(X)$. Hence

$$\sigma(\alpha') = s_p M_l(\alpha') = s_p E_l(U)^{-1\,t} M_l(\alpha) E_l(U) = s_p M_l(\alpha) = \sigma(\alpha).$$

Since $\sigma(\alpha)$ is a rational integer by Weil's result, $\sigma(\alpha') = \sigma(\alpha) = \overline{\sigma(\alpha)}$.

The proof of ii) is rather difficult. Let J be a Jacobian variety from which there exists a homomorphism λ onto A. Let B be an abelian variety such that J and $A \times B$ are isogeneous and let μ be a homomorphism from J onto B. Let W be a non-degenerate positive divisor on B. we put

$$\rho = (\lambda \times \mu) \quad \text{i.e.} \quad \rho t = \lambda t \times \mu t.$$

Since

$$U \times B + A \times W \succ 0, \qquad \rho^{-1}(U \times B + A \times W) \succ 0.$$

From Proposition 3, § 2, $\sigma(\gamma'\alpha\gamma) \geqq 0$ for all $\gamma \in \mathfrak{A}(J)$ where $\alpha = \delta'_{\rho^{-1}(U \times B + A \times W)}$.[10] By virtue of Lemma 2 there exists a natural number c and an endomorphism ξ of $J^{(4)}$ such that

$$\begin{pmatrix} c\alpha & & & \\ & c\alpha & & \\ & & c\alpha & \\ & & & c\alpha \end{pmatrix} = \xi'\xi.$$

[10] For δ'_Z see Definition in preceding Lemma 5.

In the following we denote

$$(\rho)^{(4)} = \begin{pmatrix} \rho & & & \\ & \rho & & \\ & & \rho & \\ & & & \rho \end{pmatrix}, \quad (\rho'_Z)^{(4)} = \begin{pmatrix} \rho'_Z & & & \\ & \rho'_Z & & \\ & & \rho'_Z & \\ & & & \rho'_Z \end{pmatrix}$$

and

$$\begin{pmatrix} \alpha\alpha' & \\ & \delta_B \end{pmatrix}^{(4)} = \begin{pmatrix} \alpha\alpha' & & & & & & & \\ & \delta_B & & & & & & \\ & & \alpha\alpha' & & & & & \\ & & & \delta_B & & & & \\ & & & & \alpha\alpha' & & & \\ & & & & & \delta_B & & \\ & & & & & & \alpha\alpha' & \\ & & & & & & & \delta_B \end{pmatrix}.$$

From $\rho'_{(U\times B+A\times W)}\rho = \delta'_{\rho^{-1}(U\times B+A\times W)} = \alpha$, we get

$$M_l((\rho'_z)^{(4)}(\rho)^{(4)}) + M_l(\xi')M_l(\xi),$$
$$M_l((\rho'_Z)^{(4)}) = M_l(\xi')M_l(\xi)M_l((\rho)^{(4)})^{-1},$$

where $Z + U\times B + A\times W$. Since

$$\begin{aligned} M_l(\lambda'_{\alpha^{-1}(U)}\lambda) &= E_l(\theta)^{-1}M_l(\lambda)E_l(\alpha^{-1}(U))M_l(\lambda) \\ &= E_l(\theta)^{-1}{}^tM_l(\alpha)E_l(U)M_l(\alpha)M_l(\lambda) \\ &= M_l(\lambda'_U)M_l(\alpha')M_l(\lambda)M_l(\lambda) = M_l(\lambda'_U\alpha'\alpha\lambda), \end{aligned}$$

we have

$$\rho'_{(\alpha^{-1}(U)\times B+A\times W)}\rho = \rho'_Z\begin{pmatrix} \alpha'\alpha & \\ & \delta_B \end{pmatrix}\rho.$$

Put $Z_\alpha = \alpha^{-1}(U)\times B + A\times W$.

Then

$$\begin{aligned} M_l((\rho'_{Z_\alpha}\rho)^{(4)}) &= M_l((\rho'_Z)^{(4)}\begin{pmatrix} \alpha'\alpha & \\ & \delta_B \end{pmatrix}^{(4)}(\rho)^{(4)}) \\ &= M_l(\xi')M_l(\xi)M_l((\rho)^{(4)})M_l\left(\begin{pmatrix} \alpha'\alpha & \\ & \delta_B \end{pmatrix}^{(4)}\right)M_l(\rho)^{(4)})) \end{aligned}$$

$$\begin{aligned} M_l(\xi')^{-1}M_l((\rho'_{Z_\alpha}\rho)^{(4)})M_l(\xi) \\ = M_l(\xi)M_l((\rho)^{(4)})M_l\left(\begin{pmatrix} \alpha'\alpha & \\ & \delta_B \end{pmatrix}^{(4)}\right)M_l((\rho)^{(4)})M_l(\xi)^{-1}, \end{aligned}$$

$$M(\xi'^{-1}(\rho'_{Z_\alpha}\rho)^{(4)}\xi^{-1}) = M_l((\rho)^{4}\xi^{-1})^{-1}M_l\left(\begin{pmatrix} \alpha'\alpha & \\ & \delta_B \end{pmatrix}^{(4)}\right)M_l((\rho)^{(4)}\xi^{-1}).$$

Since

$$\rho^{-1}(Z_\alpha) = \rho^{-1}(\alpha^{-1}(U)\times B + A\times W) \succ 0,$$

by virtue of Proposition 3, § 2, the characteristic roots of $M_l(\xi'^{-1}(\rho_{Z_a}\rho)^{(4)}\xi^{-1})$ are non-negative real numbers. Since $M_l\left(\begin{pmatrix}\alpha'\alpha & \\ & \delta_B\end{pmatrix}^{(4)}\right)$ has the same characteristic roots as the characteristic equation of $M_l(\xi'^{-1}(\rho_{Z_\alpha}\rho)^{(4)}\xi^{-1})$, this shows that the characteristic equation of $M_l(\alpha'\alpha)$ has non-negative real roots only. Therefore $\sigma(\alpha'\alpha)+s_p M_l(\alpha'\alpha)>0$ for $\alpha \neq 0$.

By this lemma most results on divisors obtained for Jacobian varieties are also true for special abelian varieties.

THEOREM 5. *Let A be a special abelian variety and X be a positive non-degenerate divisor of A. Let $\chi_1, \chi_2, \ldots, \chi_{2n}$ be the roots of the characteristic polynomial of $M_l(\delta'_X)$ and let $c_1=c_1(Q(\chi_1))$, $c_2=c_2(Q(\chi_2)), \ldots, c_{2n}=c(Q(\chi_{2n}))$ be Siegel's constants of $Q(\chi_1), Q(\chi_2), \ldots, Q(\chi_{2n})$ respectively (where Q is the rational number field). If $\nu(\lambda)$ and $c=\prod_{i=1}^{2n} c_i$ are not divisible by p, then $l(X) = \sqrt{\nu(\delta'_X)}$.*

Proof. Similarly as the case of Jacobian varieties $\chi_1, \chi_2, \ldots, \chi_{2n}$ are non-negative real numbers. From Lemma 4 there exists an endomorphism λ of $A^{(4)} + A\times A\times A\times A$ such that

$$\begin{pmatrix} c^2\delta'_X & & & \\ & c^2\delta'_X & & \\ & & c^2\delta'_X & \\ & & & c^2\delta'_X \end{pmatrix} = \lambda'\lambda = \delta'_{\lambda^{-1}(U^{(4)})}$$

with a natural number c, where $\delta'_{\lambda^{-1}(U^{(4)})}$ is the endomorphism such that $\lambda^{-1}(U_t^{(4)} - U^{(4)}) \sim U^{(4)}_{\delta'_{\lambda^{-1}(U^{(4)})}t} - U^{(4)}$ and $U^{(4)} = U\times A\times A\times A + A\times U\times A\times A + A\times A\times U\times A + A\times A\times A\times U$. From Theorem 3

$$l(\lambda^{-1}(U^{(4)})) = \nu(\lambda)\, l(U^{(4)}), \quad l(c^2X^{(4)}) = l((c\delta_{A^{(4)}})^{-1}(X^{(4)})) = \nu(c\delta_{A^{(4)}})\, l(X^{(4)}),$$

where $X^{(4)} = X\times A\times A\times A + A\times X\times A\times A + A\times A\times X\times A + A\times A\times A\times X$.

$$\begin{aligned} E_l(\lambda^{-1}(U^{(4)})) &= {}^tM_l(\lambda)\, E_l(U^{(4)})\, M_l(\lambda) = E_l(U^{(4)})^{-1} M_l(\lambda'\lambda) \\ &= E_l(U^{(4)})^{-1} E_l(U^{(4)})\, M_l\begin{pmatrix} c^2\delta'_X & & \\ & \ddots & \\ & & \cdot \end{pmatrix} = E_l(c^2X^{(4)}). \end{aligned}$$

Hence $E_l(\lambda^{-1}(U^{(4)})) = E_l(c^2X^{(4)})$. This shows $c^2X^{(4)} \equiv \lambda^{-1}(U^{(4)})$. By virtue of Proposition 1,

$$\begin{aligned} l(c^2X^{(4)}) &= l(c^2X)^4 = \nu(c\delta_A)^4 l(X)^{(4)} = l(\lambda^{-1}(U^{(4)})) \\ &= \nu(\lambda)\, l(U^{(4)}) = \nu(\lambda)\, l(U)^{(4)} = \nu(\lambda) \\ &= \sqrt{\nu(\lambda')\,\nu(\lambda)} = \sqrt{\nu\begin{pmatrix} c^2\delta'_X & & \\ & \ddots & \\ & & \cdot \end{pmatrix}} = \nu(c^2\delta'_X)^2 = \nu(c\delta_A)^4\,\nu(\delta'_X)^2. \end{aligned}$$

Therefore $l(X)=\sqrt{\nu(\delta'_X)}$.

LEMMA 9. *Let A be an abelian variety. There exists an isogeneous abelian variety B with a positive divisor Z such that $Z_t-Z\sim 0$ if and only if $t=0$.*

Proof. Let X be a non-degenerate positive divisor of A and let C be the finite subgroup of all points t of A satisfying $X_t-X\sim 0$. Let B be a quotient abelian variety of A by C and let λ be the separable homomorphism from A onto B whose kernel is exactly C. Then $X_t-X\sim 0$ for all points t satisfying $\lambda t=0$. Since λ is separable, by Proposition 33, N° 78, § XI, [V] there exists a positive divisor Z such that $X=\lambda^{-1}(Z)$. This Z is our divisor, for $X_t-X\sim\lambda^{-1}(Z_{\lambda t})-\lambda^{-1}(Z)=\lambda^{-1}(Z_{\lambda t}-Z)\sim 0$ if and only if $\lambda t=0$.

LEMMA 10. *Let A be an abelian variety defined over a field of characteristic zero. Then there exists an isogeneous abelian variety B with a positive divisor U such that $l(U)=1$.*

Proof. Let A be an abelian variety such that $A\times A'$ is isogeneous to a Jacobian variety J. Let B be the abelian variety isogeneous to A on which there exists a positive divisor V such that $V_t-V\sim 0$ if and only if $t=0$, and let B' be the abelian variety isogeneous to A on which there exists a positive divisor W such that $W_s-W\sim 0$ if and only if $s=0$. If λ is a homomorphism from J onto $B\times B'$, $l(\lambda^{-1}(V\times B'+B\times W))=\nu(\lambda)l(V)l(W)$. On the other hand $l(\lambda^{-1}(V\times B'+B\times W))=\sqrt{\nu(\delta'_{\lambda^{-1}(V\times B'+B\times W)})}=\sqrt{|{}^tM_l(\lambda)||E_l(V)||E_l(W)||M_l(\lambda)|}$ $=\nu(\lambda)$. Hence $l(V)l(W)=1$. Since $V, W>0$, $l(V)=l(W)=1$.

LEMMA 11. *Let A be an abelian variety defined over a field of characteristic zero and let V be a divisor of A such that $V_t-V\sim 0$ if and only if $t=0$. Then $l(V)=1$.*

THEOREM 6. (*Frobenius' Theorem*) *Let A be an abelian variety defined over a field of characteristic zero and let X be a positive non-degenerate divisor of A. Then $l(X)=\sqrt{|E(X)|}$, where $|E(X)|=\prod_l l^{e_l}$, $l^{e_l}a=|E_l(X)|$, $l\nmid a$.*

Proof. Let B be a special abelian variety isogeneous to A and let λ be a homomorphism from B onto A. Then from Theorem 4 $l(\lambda^{-1}(X))=\nu(\lambda)l(X)$. On the other hand, $l(\lambda^{-1}(X))=\sqrt{\nu(\delta'_{\lambda^{-1}(X)})}$ by Theorem 5. Since $\nu(\delta'_{\lambda^{-1}(X)})$ $=|E_l(U)^{-1}\,{}^tM_l(\lambda)E_l(X)M_l(\lambda)|=\nu(\lambda)^2|E_l(U)^{-1}||E_l(X)|$ and $E_l(U)$ is an l-adic unit, $\nu(\delta'_{\lambda^{-1}(X)})=\nu(\lambda)^2\prod_l l^{e_l}$ where $|E_l(X)|=l^{e_l}a$, $l\nmid a$. Hence $l(X)=\sqrt{\prod_l l^{e_l}}$ $=\sqrt{|E(X)|}$.

For an abelian variety onto which there exists a homomorphism from a special abelian variety satisfying $p\nmid\nu(\lambda)$, we can easily prove the same result.

https://doi.org/10.1017/S0027763000017086 Published online by Cambridge University Press

§ 4. Positive divisors

THEOREM 7. *Let A be a special abelian variety. Let α be a symmetic element of $\mathfrak{A}(A)$ satisfying $\sigma(\beta'\alpha\beta)\geqq 0$ for all $\beta\in\mathfrak{A}(A)$, where the involution $'$ is introduced by U as follows: $\alpha^{-1}(U_t-U)\sim U_{\alpha' t}-U$. Then there exist a positive divisor X and a natural number ν such that $p^{\nu}\alpha=\delta'_X$ where $X_t-X\sim U_{\delta'_X t}-U$.*

Proof. By virtue of Lemma 8, § 3, $\sigma(\beta'\alpha\beta)\geqq 0$ for all β implies that there exist a natural number c and an endomorphism of $A^{(4)}=A\times A\times A\times A$ such that

$$\begin{pmatrix} c\alpha & & & \\ & c\alpha & & \\ & & c\alpha & \\ & & & c\alpha \end{pmatrix}=\lambda'\lambda=\delta'_{\lambda^{-1}(U^{(4)})}$$

where $U^{(4)}=U\times A\times A\times A+A\times U\times A\times A+A\times A\times U\times A+A\times A\times A\times U$.

From Lemma 4, § 3 there exists a divisor W such that $\alpha=\delta'_W$ when $p\neq 2$ and $2\alpha=\delta'_W$ when $p=2$. Therefore

$$\begin{pmatrix} \varepsilon c\alpha & & \\ & \cdot & \\ & & \cdot \end{pmatrix}=\begin{pmatrix} \delta'_W & & \\ & \cdot & \\ & & \cdot \end{pmatrix}=\delta'_{W^{(4)}},$$

where $W^{(4)}=W\times A\times A\times A+A\times W\times A\times A+A\times A\times W\times A+A\times A\times A\times W$, and $\varepsilon=1, 2$ according as $p\neq$ or $=2$. Hence $\lambda^{-1}(\varepsilon U^{(4)})=W^{(4)}$. From Lemma 1 of § 1 $\lambda^{-1}(\varepsilon U^{(4)})_t-W^{(4)}=0$ with a suitable t. Put $(f(x_1, x_2, x_3, x_4))=\varepsilon\lambda^{-1}(U^{(4)})_t-W^{(4)}\succ -W^{(4)}$. Let x_2^0, x_3^0, x_4^0 be independent generic points of A over a common field of definition for W, A, U and f. Put $g(x_1)=f(x_1, x_2^0, x_3^0, x_4^0)$. Then $g(x)\succ -W$. Put $Z=(g(x))+W$. Then $Z\succ 0$ and $\delta'_Z=\varepsilon c\alpha=\varepsilon c\delta'_W=\delta'_{\varepsilon cW}$. Let $\varepsilon c=p^r b$, $p\nmid b$. Then $p^r bZ=(p^r b)^2 W\equiv p^{2r}(b\delta)^{-1}(W)$, $bZ=p^r(b\delta)^{-1}(W)$. From Lemma 7, § 1, $(bZ)_t\sim(b\delta)^{-1}(p^r W)$ with a suitable t. Hence $l(bZ)=l((b\delta)^{-1}(p^r Z))=\nu(b\delta)\,l(p^r W)\geqq 1$. Therefore $l(p^r W)\geqq 1$. Let $(\psi(x))\succ -p_r W$ and let $X=(\psi(x))+p^r W$. Then $X\succ 0$, $X\equiv p^r W$ and $\delta'_X=\delta'_{p^r W}=p^r\delta'_W=\varepsilon p^r\alpha$. Therefore $p^r\alpha=\delta'_X$ when $p\neq 2$ and $2^{r+1}\alpha=\delta'_X$ when $p=2$.

COROLLARY 1. *Let A be a special abelian variety defined over a field of characteristic zero. Then for a symmetric element α (by the involution introduced by a basic divisor), $\sigma(\beta'\alpha\beta)\geqq 0$ for dll $\beta\in\mathfrak{A}(A)$ if and only if there exists a positive divisor X such that $\alpha=\delta'_X$.*

Mathematical Institute,
Nagoya University