G. Shimura
Nagoya Math. J.
Vol. 45 (1971), 167–178

ON THE FIELD OF RATIONALITY FOR AN ABELIAN VARIETY

GORO SHIMURA

The purpose of this paper is to prove the following two facts:

(I) *Every generic polarized abelian variety of odd dimension has a model rational over its field of moduli.*

(II) *No generic principally polarized abelian variety of even dimension has a model rational over its field of moduli.*

In both statements and throughout the paper, we assume that the universal domain is of characteristic 0. We call a polarized abelian variety *generic* if its field of moduli has the maximum transcendence degree (i.e., $n(n+1)/2$ if the variety is of dimension n) over the rational number field.

It is well-known that an elliptic curve has a model rational over its field of moduli. However, no general result, not even a counter-example, seems to have been obtained in the higher-dimensional case. In a previous paper [5], we have shown that a polarized abelian variety with sufficiently many complex multiplications, under a certain condition, has a model rational over its field of moduli. We discuss here the other extreme case in which varieties are generic. A negative answer similar to (II) will be given also for abelian varieties with a certain type of polarization which is not necessarily principal, and for hyperelliptic curves of even genera.

It is still an open question to obtain a criterion under which an arbitrarily given polarized abelian variety has a model rational over its field of moduli. The above two statements combined together seem to indicate a rather complicated nature of the problem, which almost defies conjecture. A new viewpoint is certainly necessary to understand the whole situation.

Since the proofs are not so long, we do not try to explain the main ideas at this point, except the following two general remarks.

Received June 17, 1971.

(A) The parity of dimensionality intervenes in the problem in the following way. If ω is a holomorphic n-form on an abelian variety of dimension n, then the automorphism -1 sends ω to $(-1)^n \cdot \omega$. Our proof of (I) relies heavily on this fact. It is not clear, however, whether or not this connection of differential forms with the problem is essential.

(B) The existence of a model is closely connected with the problem of extending a given Galois extension to a larger Galois extension with a preassigned Galois group. But our proof is rather implicit in this respect. Actually we could make it more explicit at the cost of lengthening the paper. It may be interesting to investigate this point in full generality.

1. Preliminaries

Since our treatment is restricted to the case of characteristic 0, we may assume, without losing generality, that the universal domain is the complex number field $\boldsymbol{C}$. Let $P = (A, W)$ be a polarized abelian variety, i.e., a structure formed by an abelian variety A and a polarization W of A. Consider a structure

$$Q = (A, W, t_1, \cdots, t_m)$$

with points $t_1, \cdots, t_m$ of A of finite order. Then we can define, in a natural manner, the notion of an isomorphism of Q onto another structure of the same type, and also the transform Q^σ of Q by an isomorphism σ of a field of rationality for Q into $\boldsymbol{C}$. For details, see [1], [2, II, 1.1]. By *the field of moduli of* Q, we mean the subfield k of $\boldsymbol{C}$ which is characterized by the following property:

For every automorphism σ of $\boldsymbol{C}$, Q^σ is isomorphic to Q if and only if σ is the identity map on k.

Such a field k always exists and is unique for Q (see [1, § 2], [2, II, 1.4]). Obviously the field of moduli depends only on the isomorphism-class of Q, and is contained in any field of rationality for Q. We identify (A, W) with $(A, W, 0)$, and define *the field of moduli of* (A, W) to be that of $(A, W, 0)$. We call any structure isomorphic to Q a *model* of Q. Our construction of a model over a desired field is based on the following proposition which follows immediately from the result of Weil [8].

PROPOSITION 1. *Let Q be rational over a finite Galois extension K of a field*

F. Suppose there is, for each $\sigma \in \mathrm{Gal}(K/F)$, *an isomorphism* λ_σ *of* Q *onto* Q^σ, *satisfying* $\lambda_{\sigma\tau} = \lambda_\sigma^\tau \circ \lambda_\tau$ *for all* $\sigma, \tau \in \mathrm{Gal}(K/F)$. *Then there is a structure* Q' *rational over* F *and an isomorphism* μ *of* Q' *onto* Q *rational over* K *such that* $\mu^\sigma = \lambda_\sigma \circ \mu$ *for all* $\sigma \in \mathrm{Gal}(K/F)$.

PROPOSITION 2. *Let* Q *be as above, and* λ *an isomorphism of* Q *onto another structure* Q'. *Suppose that* Q *has no automorphisms other than the identity map. Then* λ *is rational over any field of rationality for* Q *and* Q'.

Proof. Let σ be an automorphism of $\boldsymbol{C}$ over a field of rationality for Q and Q'. Then $\lambda^{-1} \circ \lambda^\sigma$ is an automorphism of Q, hence $\lambda^{-1} \circ \lambda^\sigma = 1$, so that $\lambda^\sigma = \lambda$, q.e.d.

PROPOSITION 3. *If the identity map is the only automorphism of* Q, *then* Q *has a model rational over its field of moduli.*

For the proof, see [2, II, 1.5].

Let us now fix $P = (A, W)$, and put, for a positive integer r,

$$T_r = \{t \in A \mid rt = 0\}. \tag{1}$$

Let $\{t_1, \cdots, t_m\}$ be a set of generators of the module T_r, and let K_r denote the field of moduli of $Q_r = (A, W, t_1, \cdots, t_m)$. Then K_r depends only on P and r; it is independent of the choice of $t_1, \cdots, t_m$. Moreover, K_r is normal over K_1. Of course K_1 is the field of moduli of P.

PROPOSITION 4. *Suppose that* P *has no automorphisms other than* ± 1. *Then, for every integer* $r > 1$, Q_r *has a model rational over* K_r.

Proof. If $r > 2$, this follows immediately from Prop. 3. To prove the case $r = 2$, we start with a structure $Q_4 = (A, W, t_1, \cdots, t_m)$ rational over K_4. Let G denote the group of all automorphisms α of the module T_4 such that $\alpha(t) = t$ if $2t = 0$. We see easily that $\alpha^2 = 1$ for every $\alpha \in G$. Therefore G is a product of several cyclic groups of order 2. Therefore $G = \{\pm 1\} \cdot H$ with a suitable subgroup H not containing -1. (Of course -1 means the element of G that maps t onto $-t$.) Let $\sigma \in \mathrm{Gal}(K_4/K_2)$. Then there is an isomorphism λ of Q_2 onto Q_2^σ. By Prop. 2, λ is rational over K_4. We observe that $\lambda^{-1}(t^\sigma) = \alpha(t)$ for all $t \in T_4$ with an element α of G. Changing λ for $-\lambda$ if necessary, we may assume that $\alpha \in H$. Under the condition $\alpha \in H$, λ is unique for σ. Putting $\lambda = \lambda_\sigma$, we can easily verify $\lambda_{\sigma\tau} = \lambda_\sigma^\tau \circ \lambda_\tau$ for all $\sigma, \tau \in \mathrm{Gal}(K_4/K_2)$. By Prop. 1. Q_2 has a model rational over K_2.

PROPOSITION 5. *Let P be rational over a field F. Suppose that* (i) *P has no automorphisms other than ± 1;* (ii) *$[F : K_r \cap F]$, with an integer $r > 2$, is odd. Then P has a model rational over $K_r \cap F$.*

Proof. Put $M = K_r \cap F$. Since $K_1 \subset M$, K_r is normal over M, so that K_r and F are linearly disjoint over M. For simplicity, let us hereafter write K for K_r. Consider $Q = (A, W, t_1, \cdots, t_m)$ with (A, W) rational over F and with a set of generators $\{t_1, \cdots, t_m\}$ of T_r. Let S be the smallest field of rationality for Q containing F. Then $K \subset S$. By Prop. 4, Q has a model $Q' = (A', W', t'_1, \cdots, t'_m)$ rational over K. Let λ be an isomorphism of Q onto Q'. By Prop. 2, λ is rational over S. Obviously S is normal over F. Put $L = F \cdot K$. If $\sigma \in \mathrm{Gal}(S/L)$, there is an isomorphism ε of Q onto Q^σ. Since $P^\sigma = P$, we have $\varepsilon = \pm 1$. It follows that $[S : L] \leqq 2$. Now we divide our discussion into two cases according to $[S : L]$.

(I) $S = L$. In this case, $\mathrm{Gal}(S/F)$ can be identified with $\mathrm{Gal}(K/M)$. Put $P' = (A', W')$ and $\mu_\sigma = \lambda^\sigma \circ \lambda^{-1}$ for every $\sigma \in \mathrm{Gal}(S/F)$. Then μ_σ is an isomorphism of P' onto P'^σ. By Prop. 2, μ_σ is rational over K. Since $\mu_{\sigma\tau} = \mu_\sigma^\tau \circ \mu_\tau$ for $\sigma, \tau \in \mathrm{Gal}(K/M)$, we obtain, by Prop. 1, a model rational over M.

(II) $[S : L] = 2$. Let $G = \mathrm{Gal}(S/F)$, and let π be the generator of $\mathrm{Gal}(S/L)$. Then $G/\{1, \pi\}$ can be identified with $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(K/M)$. Take an element v of S so that $S = L(v)$, $v^2 \in L$. Put $x_\sigma = v^\sigma / v$ for every $\sigma \in G$. Then $x_\pi = -1$, $x_\sigma \in L$, and $x_{\sigma\tau} = x_\sigma^\tau x_\tau$. Put $y_\sigma = N_{L/K}(x_\sigma)$, and $z = N_{L/K}(v^2)$. Then $y_\sigma^2 = z^\sigma / z$ and $y_{\sigma\tau} = y_\sigma^\tau y_\tau$. Since $[L : K]$ is odd, $y_\pi = -1$. Let w be a square root of z. We discuss two cases $w \in K$ and $w \notin K$ separately.

(II$_a$) Suppose $w \in K$. Put $f(\sigma) = y_\sigma w / w^\sigma$. Since $y_\sigma^2 = (w^\sigma / w)^2$, we have $f(\sigma) = \pm 1$. Therefore f is a cocycle with values ± 1, so that it must be a character of G. Furthermore f is non-trivial, since $f(\pi) = -1$. Let H be the kernel of f. Then $G = H \cdot \{1, \pi\}$, and H can be identified with $\mathrm{Gal}(K/M)$. For every $\sigma \in H$, put $\mu_\sigma = \lambda^\sigma \circ \lambda^{-1}$. We see again that μ_σ is an isomorphism of P' onto P'^σ rational over K, and $\mu_{\sigma\tau} = \mu_\sigma^\tau \circ \mu_\tau$. Therefore P' has a model rational over M.

(II$_b$) Suppose $w \notin K$. Extend an element of $\mathrm{Gal}(K/M)$ to an automorphism α of $\boldsymbol{C}$. If an element ξ of G coincides with α on K, then $(w^\alpha)^2 = z^\xi = y_\xi^2 w^2$, so that $w^\alpha = \pm y_\xi w \in K(w)$. Therefore $K(w)$ is normal over M. Now,

for every $\sigma \in G$, we can define an element $[\sigma]$ of $\mathrm{Gal}(K(w)/M)$ by $w^{[\sigma]} = y_\sigma w$, and $[\sigma] = \sigma$ on K. Then we see easily that $\sigma \longmapsto [\sigma]$ is an isomorphism of G onto $\mathrm{Gal}(K(w)/M)$. Put $\mu_{[\sigma]} = \lambda^\sigma \circ \lambda^{-1}$ for every $\sigma \in G$. Then $\mu_{[\sigma]}$ is an isomorphism of P' onto P'^σ, rational over K, and

$$\mu_{[\sigma][\tau]} = \lambda^{\sigma\tau} \circ \lambda^{-1} = (\lambda^\sigma \circ \lambda^{-1})^\tau \circ (\lambda^\tau \circ \lambda^{-1}) = \mu_{[\sigma]}^{[\tau]} \circ \mu_{[\tau]}.$$

Therefore, by Prop. 1, we obtain a model rational over M.

2. The odd dimensional case

Let $P = (A, W)$ and $P' = (A', W')$ be two polarized abelian varieties of dimension n, rational over a field K, and λ an isomorphism of P onto P', not necessarily rational over K. Take non-zero holomorphic differential n-forms ω on A and ω' on A', rational over K. Denote by $\omega' \circ \lambda$ the transform of ω' by λ. Then $\omega' \circ \lambda = c \cdot \omega$ with a constant c. If τ is an automorphism of $\boldsymbol{C}$ over K, we have $\omega' \circ \lambda^\tau = c^\tau \cdot \omega$, hence $\omega' \circ \lambda^\tau \circ \lambda^{-1} = c^\tau c^{-1} \omega'$. Now we impose the following two conditions on P:

(2) *P has no automorphisms other than* ± 1.

(3) *n is odd.*

Then $\lambda^\tau \circ \lambda^{-1} = \pm 1$, and $\omega' \circ (-1) = (-1)^n \omega' = -\omega'$. Therefore $c^\tau = \pm c$, and $\lambda^\tau = (c^\tau/c) \cdot \lambda$. It follows that $K(c)$ is the smallest field of rationality for λ containing K, $c^2 \in K$, and $[K(c) : K] \leqq 2$. After this preliminary consideration, we now prove

PROPOSITION 6. *Suppose that $P = (A, W)$ satisfies (2) and (3). Let K be a field of rationality for P, and σ an automorphism of K of order 2 such that P^σ is isomorphic to P. Then P has a model rational over the fixed subfield of K by σ.*

Proof. Let $F = \{x \in K \mid x^\sigma = x\}$, and let λ be an isomorphism of P onto P^σ. Take a non-zero holomorphic n-form ω on A rational over K, and put $\omega^\sigma \circ \lambda = c \cdot \omega$ with a constant c. Extend σ to an automorphism of $\boldsymbol{C}$, and denote it again by σ. Then $\omega \circ \lambda^\sigma = c^\sigma \cdot \omega^\sigma$, and $\omega \circ \lambda^\sigma \circ \lambda = c^\sigma c \cdot \omega$. Since $\lambda^\sigma \circ \lambda$ is an automorphism of P, we have $\lambda^\sigma \circ \lambda = \pm 1$, and $c^\sigma c = \pm 1$. By the above consideration, λ is rational over $K(c)$, and $c^2 \in K$. Now $N_{K/F}(c^2) = 1$, so that $c^2 = b/b^\sigma$ with an element b of K. Let d be a square root of b. Suppose $d \in K$. Then $c^2 = (d/d^\sigma)^2$, so that $c = \pm d/d^\sigma \in K$, hence $c^\sigma c = 1$. Therefore λ is rational over K, and $\lambda^\sigma \circ \lambda = 1$. By Prop. 1, P has a model rational over F. Next suppose $d \notin K$. Then we can find a polarized abelian variety P'

$= (A', W')$ rational over K and an isomorphism μ of P to P' rational over $K(d)$ such that $\mu^\alpha = -\mu$ if α is the generator of $\mathrm{Gal}(K(d)/K)$. (This is another application of Prop. 1.) Let ω' be a non-zero holomorphic n-form on A' rational over K. Then $\omega' \circ \mu = e \cdot \omega$ with a constant e such that $K(e) = K(d)$ and $e^\alpha = -e$. Then $d/e \in K$. Changing ω' for $(d/e) \cdot \omega'$, we may assume that $\omega' \circ \mu = d \cdot \omega$. Put $\lambda' = \mu^\sigma \circ \lambda \circ \mu^{-1}$. Then λ' is an isomorphism of P' onto P'^σ, and $\omega'^\sigma \circ \lambda' = \omega'^\sigma \circ \mu^\sigma \circ \lambda \circ \mu^{-1} = (d^\sigma c/d) \cdot \omega'$. Now $(d^\sigma c/d)^2 = c^2 b^\sigma / b = 1$, hence $d^\sigma c/d = \pm 1$. Therefore λ' is rational over K, and $\omega' \circ (\lambda'^\sigma \circ \lambda') = \omega'$, hence $\lambda'^\sigma \circ \lambda' = 1$. By Prop. 1, P' has a model rational over F. This completes the proof.

PROPOSITION 7. *Suppose that P satisfies (2) and (3). Let K_r be defined for P as in § 1. Let r be a positive integer > 2, and F a finite normal extension of K_1 over which P has a model. Then P has a model rational over $K_r \cap F$.*

Proof. Let H be a 2-Sylow subgroup of $\mathrm{Gal}(F/K_1)$, and M the subfield of F corresponding to H. The field F can be obtained from M by successive quadratic extensions. Therefore, by Prop. 6, P has a model rational over M. Now $K_1 \subset M \cap K_r \subset M$, and $[M : K_1]$ is odd. By Prop. 5, P has a model rational over $K_r \cap M$, hence over $K_r \cap F$, q.e.d.

As an immediate consequence, we obtain

PROPOSITION 8. *Suppose that P satisfies (2) and (3). Let r and s be positive integers such that $r > 2$ and $s > 1$. Then P has a model rational over $K_r \cap K_s$.*

Let us now consider a generic $P = (A, W)$ of even or odd dimension. Define K_r for P as above. The structure of $\mathrm{Gal}(K_r/K_1)$ has been determined in [2] and [4]. To explain the result, take a basic polar divisor X belonging to W, let $T_r = \{t \in A \mid rt = 0\}$, and define the symbol $e_{X,r}(s, t)$ for $(s, t) \in T_r \times T_r$ as in Weil [7, § XI]. Let G denote the group of all automorphisms α of T_r such that

$$e_{X,r}(\alpha(s), \alpha(t)) = e_{X,r}(s, t)^{c(\alpha)}$$

with an integer $c(\alpha)$ prime to r. Further let L denote the algebraic closure of K_1. For every $\sigma \in \mathrm{Gal}(L/K_1)$, take an isomorphism λ of P onto P^σ. Then $t \longmapsto \lambda^{-1}(t^\sigma)$ is an automorphism of T_r, which can be shown to belong to G. Writing it α_σ, we have

$$t^\sigma = \lambda(\alpha_\sigma(t)) \qquad (t \in T_r). \tag{4}$$

The element α_σ of G is uniquely determined for σ by (4), up to the factor -1. Then the map $\sigma \longmapsto \pm\alpha_\sigma$ gives an injection of $\mathrm{Gal}(K_r/K_1)$ into $G/\{\pm 1\}$. This much is true for any P, not necessarily generic, whose automorphisms are ± 1. Suppose that r is prime to the degree of the polarization. (By the *degree* of the polarization W, we understand the degree of the isogeny of A onto its Picard variety associated with X.) Then G is isomorphic to a group $\mathfrak{G}_r$ defined by

$$\mathfrak{G}_r = \{S \in GL_{2n}(\boldsymbol{Z}/r\boldsymbol{Z}) \mid {}^tSJS = c(S)J \text{ with } c(S) \in \boldsymbol{Z}/r\boldsymbol{Z}\},$$

$$J = \begin{bmatrix} 0 & -1_n \\ 1_n & 0 \end{bmatrix}, \quad n = \dim(A).$$

If P is generic, the map of $\mathrm{Gal}(K_r/K_1)$ into $\mathfrak{G}_r/\{\pm 1\}$ is surjective. (For the proof, see [2, II, § 7], where a more general result is given with no restriction on r, nor on the type of polarization. See also [4, 9.5, 9.8].)

PROPOSITION 9. *Suppose P is generic. If r and s are relatively prime, and rs is prime to the degree of the polarization, then $K_r \cap K_s = K_1$.*

Proof. It can easily be seen that $\mathfrak{G}_{rs} = \mathfrak{G}_r \times \mathfrak{G}_s$, and K_r, as a subfield of K_{rs}, corresponds to the subgroup $\{\pm 1\} \times \mathfrak{G}_s$ of $\mathfrak{G}_{rs}$, and K_s to $\mathfrak{G}_r \times \{\pm 1\}$, hence $K_r \cap K_s = K_1$.

(Note that $[K_{rs} : K_r K_s] = 2$ if both r and s are > 2.)

Combining Prop. 9 with Prop. 8, we obtain

THEOREM 1. *Every generic polarized abelian variety of odd dimension has a model rational over its field of moduli.*

3. The even dimensional case

Let $\mathfrak{H}_n$ denote the Siegel upper half space of degree n, i.e., the set of all complex symmetric matrices with positive definite imaginary parts. Let δ be a diagonal matrix of degree n whose diagonal elements are non-zero rational integers with no common divisors other than ± 1. For each $z \in \mathfrak{H}_n$, we consider an $(n \times 2n)$-matrix

$$\Omega(z) = (z \ \delta)$$

and a lattice $L(z)$ in $\boldsymbol{C}^n$ generated by the column vectors of $\Omega(z)$. Then the complex torus $\boldsymbol{C}^n/L(z)$ has a structure of an abelian variety. Moreover, we obtain a Riemann form Φ_z on it by

https://doi.org/10.1017/S0027763000014720 Published online by Cambridge University Press

$$\Phi_z(\Omega(z)x,\ \Omega(z)y) = {}^t x \Delta y \qquad (x,\ y \in \boldsymbol{R}^{2n}),$$

$$\Delta = \begin{bmatrix} 0 & -\delta \\ \delta & 0 \end{bmatrix}.$$

Here we consider the elements of $\boldsymbol{R}^{2n}$ as column vectors. Each point z of $\mathfrak{H}_n$ determines in this way an isomorphism class of polarized abelian varieties over $\boldsymbol{C}$. We take any model in the class, and call it $P_z = (A_z, W_z)$. The degree of W_z coincides with $\det(\Delta)$.

It is well-known that an arbitrary polarized abelian variety P is isomorphic to P_z for some δ and z; the invariant factors of δ are completely determined by P; z is unique for P modulo a certain discontinuous group commensurable with $\mathrm{Sp}(2n, \boldsymbol{Z})$.

Now we assume that n is even, and put $n = 2m$. Furthermore we consider the following condition on the type of polarization.

(5) *Each invariant factor of δ occurs with an even multiplicity. In other words, there exist two elements α and β of $GL_n(\boldsymbol{Z})$ such that $\alpha\delta\beta = \begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix}$ with a diagonal matrix d of size m.*

If this is satisfied, we may assume, by transforming Δ by $\begin{bmatrix} {}^t\alpha & 0 \\ 0 & \beta \end{bmatrix}$, that δ itself is of the form $\begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix}$.

PROPOSITION 10. *Suppose that $\delta = \begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix}$ with a diagonal matrix d of size m. Let $j = \begin{bmatrix} 0 & -1_m \\ 1_m & 0 \end{bmatrix}$, and let $\mathfrak{Y}$ be the set of all $z \in \mathfrak{H}_n$ such that $jz = -z^\rho j$. Then, for every $z \in \mathfrak{Y}$, there is an isomorphism λ of P_z onto P_z^ρ such that $\lambda^\rho \circ \lambda = -1$.*

Here and henceforth, ρ denotes the complex conjugation.

Proof. Let f be a holomorphic map of $\boldsymbol{C}^n$ onto A_z which induces an isomorphism of $\boldsymbol{C}^n/L(z)$ onto A_z. Then we can define a holomorphic map f' of $\boldsymbol{C}^n$ onto A_z^ρ with kernel $L(z)^\rho$ by $f'(u) = f(u^\rho)^\rho$ for $u \in \boldsymbol{C}^n$. Suppose $z \in \mathfrak{Y}$. Then

$$j \cdot \Omega(z) = \Omega(-z^\rho)J', \quad J' = \begin{bmatrix} j & 0 \\ 0 & j \end{bmatrix}.$$

Since $L(z)^\rho = L(-z^\rho)$, the automorphism of $\boldsymbol{C}^n$ obtained from j gives an

https://doi.org/10.1017/S0027763000014720 Published online by Cambridge University Press

isomorphism of $\boldsymbol{C}^n/L(z)$ onto $\boldsymbol{C}^n/L(z)^\rho$. Therefore we can define an isomorphism λ of A_z onto A_z^ρ by $\lambda(f(u)) = f'(ju)$ for $u \in \boldsymbol{C}^n$. Then

$$\lambda^\rho(f'(u)) = \lambda^\rho(f(u^\rho)^\rho) = f'(ju^\rho)^\rho = f(ju),$$

so that $\lambda^\rho(\lambda(f(u))) = \lambda^\rho(f'(ju)) = f(j^2u) = -f(u)$, hence $\lambda^\rho \circ \lambda = -1$. Let X be a polar divisor of A_z corresponding to Φ_z with respect to f. Define the symbol $e_{X,N}(s, t)$ as in Weil [7, § XI] for every positive integer N. By [6, p. 25, (7)], we have

$$e_{X,N}(f(u), f(v)) = \exp[-2\pi i \cdot N \cdot \Phi_z(u, v)] \qquad (u, v \in N^{-1}L(z)).$$

Applying ρ to this relation ,we obtain

$$e_{X^\rho,N}(f'(u), f'(v)) = \exp[2\pi i \cdot N \cdot \Phi_z(u^\rho, v^\rho)] \qquad (u, v \in N^{-1}L(-z^\rho)).$$

Put $S = \begin{bmatrix} -1_n & 0 \\ 0 & 1_n \end{bmatrix}$, $u = \Omega(-z^\rho)x$, $v = \Omega(-z^\rho)y$ with $x, y \in \boldsymbol{R}^{2n}$. Then $u^\rho = \Omega(z)Sx$, $v^\rho = \Omega(z)Sy$, so that

$$\Phi_z(u^\rho, v^\rho) = {}^t x \cdot {}^t S \Delta S y = -{}^t x \Delta y = -\Phi_w(u, v), \quad w = -z^\rho.$$

Therefore

$$e_{X^\rho,N}(f'(u), f'(v)) = \exp[-2\pi i \cdot N \cdot \Phi_w(u, v)].$$

This implies that X^ρ is a divisor of A_z^ρ corresponding to Φ_w with respect to f'. Since $j \cdot \Omega(z) = \Omega(-z^\rho)J'$ and ${}^t J' \Delta J' = \Delta$, we see that λ sends W_z onto W_z^ρ, q.e.d.

PROPOSITION 11. *The set $\mathfrak{Y}$ of Prop. 10 is non-empty. Moreover, let g be a holomorphic function defined on a connected domain D contained in $\mathfrak{H}_n$. If $g = 0$ on a non-empty open subset of $D \cap \mathfrak{Y}$, then g is identically 0 on D.*

Proof. It can easily be verified that every point z of $\mathfrak{Y}$ can be written in the form

$$z = \begin{bmatrix} a & b \\ b^\rho & -a^\rho \end{bmatrix}$$

with complex matrices a and b of size m such that ${}^t a = a$, ${}^t b^\rho = b$. Conversely, such a z, whose imaginary part is positive definite, belongs to $\mathfrak{Y}$. If we put $a = x + iy$ and $b = r + is$ with real matrices x, y, r, s, then the conditions become as follows:

$${}^t x = x, \quad {}^t y = y, \quad {}^t r = r, \quad {}^t s = -s;$$

https://doi.org/10.1017/S0027763000014720 Published online by Cambridge University Press

$$\begin{bmatrix} y & s \\ {}^t s & y \end{bmatrix} \text{ is positive definite.}$$

Therefore $\mathfrak{Y}$ is non-empty. Our second assertion follows from the following well-known facts:

(i) A holomorphic function $h(z)$ in one complex variable z is identically 0, if $h(x) = 0$ for all real x.

(ii) A holomorphic function $h(z, z')$ in two complex variables z and z' is identically 0, if $h(z, z^\rho) = 0$ for all complex z.

Of course the function in each case must be defined on a connected domain for which the condition $h(x) = 0$ or $h(z, z^\rho) = 0$ is meaningful.

PROPOSITION 12. *If P_z, with $z \in \mathfrak{Y}$, has no automorphisms other than ± 1, then P_z has no model rational over its field of moduli.*

Proof. Since P_z is isomorphic to P_z^ρ, the field of moduli of P_z is contained in $\boldsymbol{R}$. Assume that P_z has a model P rational over $\boldsymbol{R}$, and let μ be an isomorphism of P onto P_z. Then $\lambda^{-1} \circ \mu^\rho \circ \mu^{-1}$, with λ as in Prop. 10, is an automorphism of P_z, so that $\lambda^{-1} \circ \mu^\rho \circ \mu^{-1} = \pm 1$, hence $\lambda = \pm \mu^\rho \circ \mu^{-1}$. But this contradicts the equality $\lambda^\rho \circ \lambda = -1$.

THEOREM 2. *Let P be a generic polarized abelian variety of even dimension. If the polarization satisfies the condition* (5), *then P has no model rational over its field of moduli.*

Proof. As mentioned above, there is a discrete subgroup Γ of $\mathrm{Sp}(2n, \boldsymbol{R})$ such that P_z is isomorphic to P_w if and only if $\gamma(z) = w$ for some $\gamma \in \Gamma$. Moreover $\mathfrak{H}_n/\Gamma$ is isomorphic to a Zariski open subset V of a projective variety. Let φ be a holomorphic map of $\mathfrak{H}_n$ onto V which induces an isomorphism of $\mathfrak{H}_n/\Gamma$ onto V. By [3], we can take V and φ so that the following conditions are satisfied:

(i) *V is defined over the rational number field $\boldsymbol{Q}$;*

(ii) *$\boldsymbol{Q}(\varphi(z))$ is the field of moduli of P_z for every $z \in \mathfrak{H}_n$;*

(iii) *For an automorphism σ of $\boldsymbol{C}$, P_z is isomorphic to P_w^σ if and only if $\varphi(z) = \varphi(w)^\sigma$.*

Thus P_z is generic if and only if $\varphi(z)$ is generic on V over $\boldsymbol{Q}$. Therefore if

P_z and P_w are generic, there is an automorphism σ of $\boldsymbol{C}$ such that P_z is isomorphic to P_w^σ. For this reason and by virtue of Prop. 12, to prove our theorem, it is sufficient to find a generic P_z with z in $\mathfrak{Y}$. This can be done as follows. Let S be the set of all homogeneous polynomials with rational coefficients viewed as functions in the projective space in which V is situated. Let S' be the subset of S consisting of all the $f \in S$ such that $f \circ \varphi$ is not identically 0. Put, for each $f \in S'$,

$$X_f = \{z \in \mathfrak{Y} \mid f(\varphi(z)) = 0\}.$$

Then X_f is a closed subset of $\mathfrak{Y}$, which contains no non-empty open subset of $\mathfrak{Y}$ by Prop. 11. Since S' is a countable set, $\mathfrak{Y}$ cannot be covered by the X_f. Therefore $\mathfrak{Y}$ has a point z for which $f(\varphi(z)) \neq 0$ for all $f \in S'$. Then $\varphi(z)$ is generic on V over $\boldsymbol{Q}$, q.e.d.

A counter-example of the same nature can be obtained also for hyperelliptic curves of even genera. In fact consider a hyperelliptic curve U of genus $m-1$ defined by

$$y^2 = a_0 x^m + \sum_{r=1}^{m} (a_r x^{m+r} + (-1)^r a_r^\rho x^{m-r}), \quad a_m = 1,$$

where a_0 is a real number and $a_1, \cdots, a_{m-1}$ are complex numbers. Suppose m is odd. Then we can define a birational map μ of U onto U^ρ by

$$\mu(x, y) = (-x^{-1}, \ i \cdot x^{-m} y).$$

We see that $\mu^\rho \circ \mu$ maps (x, y) onto $(x, -y)$. Take the a_r so that $a_0, a_1, \cdots, a_{m-1}, a_1^\rho, \cdots, a_{m-1}^\rho$ are algebraically independent over $\boldsymbol{Q}$. Then U has no automorphisms other than the obvious two. Therefore, for the same reason as in the proof of Prop. 12, U cannot have a model rational over $\boldsymbol{R}$. Thus wəobtain

THEOREM 3. *No generic hyperelliptic curve of even genus has a model rational over its field of moduli.*

REFERENCES

[1] G. Shimura, On the theory of automorphic functions, Ann. of Math., **70** (1959), 101–144.

[2] G. Shimura, On the field of definition for a field of automorphic functions: I, II, Ann. of Math., **80** (1964), 160–189, **81** (1965), 124–165.

[3] G. Shimura, Moduli and fibre systems of abelian varieties, Ann. of Math., **83** (1966), 294–338.

[4] G. Shimura, Algebraic number fields and symplectic discontinuous groups, Ann. of Math. **86** (1967), 503–592.
[5] G. Shimura, On the zeta-function of an abelian variety with complex multiplication, to appear.
[6] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, No. **6**, 1961.
[7] A. Weil, Variétés abéliennes et courbes algébriques, Hermann, Paris, 1948.
[8] A. Weil, The field of definition of a variety, Amer. J. Math., **78** (1956), 509–524.

Princeton University