Journal of Pure and Applied Algebra 90 (1993) 23–37
North-Holland

Isogenies of abelian varieties

A. Silverberg
Department of Mathematics, Ohio State University, Columbus, OH 43210, USA

Yu.G. Zarhin
Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, 142292, Russia, Russian Federation

Communicated by F. Oort
Received 8 October 1991
Revised 30 November 1992

Abstract

Silverberg, A and Yu.G. Zarhin, Isogenies of abelian varieties, Journal of Pure and Applied Algebra 90 (1993) 23–37.

We discuss the question of when two polarized abelian varieties with partial level structure, which are isogenous and are defined over a given field F, are F-isogenous as abelian varieties without structure.

1. Introduction

If X and Y are abelian varieties defined over a field F, and isogenous over some extension of F, then X and Y are not necessarily isogenous over F itself, although they are necessarily isogenous over $F(X_n, Y_n)$, whenever $n \geq 3$ and n is not divisible by the characteristic $\mathrm{char}(F)$ of F (see Theorem 2.4 of [7]). In particular, if Q_1 and Q_2 are abelian varieties with full level n structure, defined over a field F, $n \geq 3$, and n is not divisible by $\mathrm{char}(F)$, then every homomorphism from Q_1 to Q_2 must be defined over F.

In this paper we examine the situation of polarized abelian varieties with partial level n structure, corresponding to maximal isotropic subgroups of X_n and Y_n with respect to the e_n-pairings induced by the polarizations. The question is under what conditions isogenous polarized abelian varieties with partial level structure will be isogenous (at least as abelian varieties) over the ground field. The general setting in which we work is given in the following definition.

Correspondence to: A Silverberg, Department of Mathematics, Ohio State University, 231 West 18 Avenue, Columbus, OH 43210-1174, USA, Email: silver@math.ohio-state.edu.

Definition 1.1. The condition $I(n)$ will mean that the following situation (a)–(h) holds:

(a) X and Y are abelian varieties defined over a field F,
(b) n is a positive integer not divisible by $\mathrm{char}(F)$,
(c) $f: X \to Y$ is an isogeny of degree prime to n,
(d) μ is a polarization on Y,
(e) $\tilde{Y}_n$ is a subgroup of Y_n, defined over F, and containing a maximal isotropic subgroup of Y_n with respect to the e_n-pairing induced by μ,
(f) $\tilde{X}_n$ is a subgroup of X_n, defined over F, such that the restriction of f to $\tilde{X}_n$ is an isomorphism from $\tilde{X}_n$ onto $\tilde{Y}_n$ defined over F,
(g) L is a finite Galois extension of F over which f is defined,
(h) λ is the polarization on X defined by $\lambda = {}^t f \mu f$.

In Theorems 1.2, 1.3, and 1.6 we give conditions under which the abelian varieties of $I(n)$ will be isogenous over the ground field, or under which the initial isogeny f of $I(n)$ will be defined over the ground field (see also Theorem 5.2, Proposition 1.9, and Remarks 5.4, 7.1, 7.2, and 7.3). We prove these results in Sections 5, 6, and 7.

Our major auxiliary results which enter into the proofs of Theorems 1.2 and 1.3 are Theorems 4.1 and 4.2. These results can be viewed as variations on Serre's Lemma (which states that automorphisms of abelian varieties which have finite order and are congruent to the identity modulo an integer greater than or equal to 3, must be the identity). In Section 3 we give generalizations of Serre's Lemma and of Minkowski's Theorem on integral matrices; we use results and ideas from Section 3 in Section 4.

Theorem 1.2. *Suppose we have $I(n)$ for some $n \geq 5$, $\mathrm{End}_L(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$ is commutative, and the degree of the polarization μ is relatively prime to n. Then X and Y are isogenous over F. Further, the isogeny f is defined over every extension of F over which all elements of $\mathrm{End}_L(Y)$ are defined.*

Theorem 1.3. *Suppose we have $I(n)$ for some $n \geq 5$, the polarization μ is defined over L, $\mathrm{End}_L(Y) = \mathrm{End}_F(Y)$, and the Rosati involution induced on $\mathrm{End}_L(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ by the polarization λ is defined over F. Then f is defined over F.*

Remark 1.4. If (X, λ) is a polarized abelian variety defined over a field F, then the Rosati involution on $\mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ induced by λ is defined over F.

Remark 1.5. Suppose X is an abelian variety defined over a field F, and L is a Galois extension of F. If $\mathrm{End}_L(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ either is commutative or is a totally definite division quaternion algebra over a totally real number field, then it has a unique positive involution, and therefore the Rosati involution is always defined over F in these cases.

Theorem 1.6. *Suppose we have $I(n)$ for some n not dividing $[L:F]^2$, and suppose the polarizations λ and μ are defined over the field F. Then X and Y are isogenous over F. In*

particular, the homomorphism $\sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma(f)$ *is an* F*-isogeny from* X *onto* Y*, whose restriction to* $X_t \cap \tilde{X}_n$ *is an isomorphism onto* $Y_t \cap \tilde{Y}_n$*, where* t *is the largest divisor of* n *relatively prime to* $[L:F]$.

Remark 1.7. Propositions 5.4, 5.5, and 5.6 of [7] show how to construct (CM) elliptic curves with points of finite order, defined over a number field F, which have isogenies onto themselves that are not defined over F. These give examples which satisfy the hypotheses of Theorems 1.2 and 1.6, but such that the isogenies f are not themselves defined over F.

Remark 1.8. If we impose additional hypotheses, we can obtain results for $n = 3$ or 4. For example, with the assumptions $I(n)$, $n \geq 3$, $\tilde{Y}_n = Y_n$, and $\mathrm{End}_L(Y)$ commutative, our proof of Theorem 1.3 shows that X and Y are isogenous over F.

Proposition 1.9 (proved in Section 8) gives a result valid for $n \geq 4$. Write ρ_μ for the Rosati involution on $\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$ induced by the polarization μ.

Proposition 1.9. *Suppose we have* $I(n)$ *for some* n*, the polarizations* μ *and* λ *are defined over* F*, and every* $\alpha \in \mathrm{End}_L(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\deg(f)]$ *such that* $\rho_\mu(\alpha)\alpha = 1$ *is defined over* F*. Then* f *is defined over* F *if, in addition, either*

(a) $n \geq 5$, *or*

(b) $n \geq 4$ *and* $\tilde{Y}_n \cong (\mathbb{Z}/n\mathbb{Z})^b$ *for some* b.

2. Preliminaries

Standard notation. If F is a field, then F^s denotes a separable closure and $\bar{F}$ denotes an algebraic closure. We have $F \subseteq F^s \subseteq \bar{F}$. A set C or a map g which is defined over F^s will be defined over F if and only if it is $\mathrm{Gal}(F^s/F)$-invariant (see [9, pp. 76 and 186]). If Y is an abelian variety, write Y_n for the kernel of multiplication by n in $Y(\bar{F})$, write $\mathrm{End}(Y)$ for the ring of endomorphisms of Y, and let

$$\mathrm{End}^0(Y) = \mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

If n is not divisible by $\mathrm{char}(F)$, then Y_n is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(Y)$, and $Y_n \subseteq Y(F^s)$. If Y is defined over a field L, write $\mathrm{End}_L(Y)$ for the ring of endomorphisms defined over L, and let

$$\mathrm{End}_L^0(Y) = \mathrm{End}_L(Y) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Further, if X is also an abelian variety, let

$$\mathrm{Hom}^0(X, Y) = \mathrm{Hom}(X, Y) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

If α is a homomorphism between abelian varieties which are defined over a field F, then α is defined over a finite separable extension of F (see [1, p. 258, Corollary 1]). If $\alpha \in \mathrm{Hom}(X, Y)$ is an isogeny, then α^{-1} denotes the unique element α' of $\mathrm{Hom}^0(Y, X)$ such that $\alpha\alpha' = 1$ and $\alpha'\alpha = 1$. If X^* and Y^* are the Picard varieties of abelian varieties X and Y, and $\alpha \in \mathrm{Hom}^0(X, Y)$, then ${}^t\alpha \in \mathrm{Hom}^0(Y^*, X^*)$ denotes the transpose of α (see [2, p. 124] or [6, p. 3]). If $\alpha \in \mathrm{Hom}(X, Y)$, then ${}^t\alpha \in \mathrm{Hom}(Y^*, X^*)$ satisfies ${}^t\alpha(\mathrm{Cl}(D)) = \mathrm{Cl}(\alpha^{-1}(D))$ whenever D is a divisor on Y, algebraically equivalent to zero, and such that $\alpha^{-1}(D)$ is defined, where Cl denotes the divisor class in the Picard variety. Polarizations on Y will be viewed as isogenies from Y onto Y^*.

If Y is an abelian variety defined over a field F, μ is a polarization on Y, n is a positive integer not divisible by $\mathrm{char}(F)$, and $\boldsymbol{\mu}_n$ is the $\mathrm{Gal}(F^s/F)$-module of nth roots of unity in F^s, then the *e_n-pairing induced by the polarization μ*,

$$e_{\mu,n} : Y_n \times Y_n \to \boldsymbol{\mu}_n$$

(see [8, Paragraphe 75]), is a skew-symmetric bilinear map which satisfies:

(1) $\sigma(e_{\mu,n}(y_1, y_2)) = e_{\sigma(\mu),n}(\sigma(y_1), \sigma(y_2))$ for every $\sigma \in \mathrm{Gal}(F^s/F)$ and $y_1, y_2 \in Y_n$,

(2) if $f : X \to Y$ is a homomorphism of abelian varieties, λ and μ are polarizations on X and Y, respectively, and $\lambda = {}^t f \mu f$, then

$$e_{\mu,n}(f(x_1), f(x_2)) = e_{\lambda,n}(x_1, x_2)$$

for every $x_1, x_2 \in X_n$,

(3) if n is relatively prime to the degree of μ, then the pairing $e_{\mu,n}$ is non-degenerate.

Additional details may be found in [2], [4], [6], and [8].

Additional notation. If X and Y are abelian varieties defined over a field F, $f : X \to Y$ is an isogeny, L is a Galois extension of F over which f is defined, and $\sigma \in \mathrm{Gal}(L/F)$, let

$$f_\sigma = f\sigma(f)^{-1} \in \mathrm{End}_L^0(Y).$$

Remark 2.1. Suppose we have $I(n)$ for some n. Since n is relatively prime to the degree of f, for $\sigma \in \mathrm{Gal}(L/F)$ we can view f and $\sigma(f)$ as isomorphisms from X_n onto Y_n. Further, by 1.1(f) we can view f_σ as an automorphism of Y_n which induces the identity on $\tilde{Y}_n$.

Write $Z_L(Y)$ for the center of the semi-simple $\mathbb{Q}$-algebra $\mathrm{End}_L^0(Y)$.

If μ is a polarization on Y, write ρ_μ for the Rosati involution on $\mathrm{End}^0(Y)$ induced by μ, i.e., for $\alpha \in \mathrm{End}^0(Y)$,

$$\rho_\mu(\alpha) = \mu^{-1}\,{}^t\alpha\mu.$$

Lemma 2.2. *Suppose we have $I(n)$ for some n, and λ and μ are defined over the field F. Then:*

(a) *for every $\sigma \in \mathrm{Gal}(L/F)$ and $x_1, x_2 \in X_n$, we have*

$$e_{\mu,n}(\sigma(f)(x_1), \sigma(f)(x_2)) = e_{\mu,n}(f(x_1), f(x_2)),$$

(b) *for every $\sigma \in \mathrm{Gal}(L/F)$ and $y_1, y_2 \in Y_n$, we have*

$$e_{\mu,n}(f_\sigma^{-1}(y_1), y_2) = e_{\mu,n}(y_1, f_\sigma(y_2)),$$

(c) *for every $\sigma \in \mathrm{Gal}(L/F)$, we have*

$$(f_\sigma^{-1} - 1)\, Y_n \subseteq \tilde{Y}_n, \quad (f_\sigma - 1)\, Y_n \subseteq \tilde{Y}_n, \quad \text{and} \quad (f_\sigma - 1)^2\, Y_n = 0,$$

(d) *for every $\sigma \in \mathrm{Gal}(L/F)$, we have $\rho_\mu(f_\sigma) f_\sigma = 1$.*

Proof. Since λ and μ are defined over F, we have for every $\sigma \in \mathrm{Gal}(F^s/F)$,

$$\begin{aligned} e_{\mu,n}(f(x_1), f(x_2)) &= e_{\lambda,n}(x_1, x_2) = \sigma(e_{\lambda,n}(\sigma^{-1}x_1, \sigma^{-1}x_2)) \\ &= \sigma(e_{\mu,n}(f(\sigma^{-1}x_1), f(\sigma^{-1}x_2))) \\ &= e_{\mu,n}(\sigma(f)(x_1), \sigma(f)(x_2)), \end{aligned}$$

and this proves (a). From (a), (b) immediately follows. If $y \in Y_n$ and $\tilde{y} \in \tilde{Y}_n$, then by (b),

$$e_{\mu,n}((f_\sigma^{-1} - 1)y, \tilde{y}) = e_{\mu,n}(y, (f_\sigma - 1)\tilde{y}) = e_{\mu,n}(y, 0) = 1.$$

Since $\tilde{Y}_n$ contains a maximal isotropic subgroup of Y_n, we have $(f_\sigma^{-1} - 1)\, Y_n \subseteq \tilde{Y}_n$. Since $(f_\sigma^{-1} - 1)\, \tilde{Y}_n = 0$, we similarly obtain $(f_\sigma - 1)\, Y_n \subseteq \tilde{Y}_n$. The final statement of (c) now follows since $(f_\sigma - 1)\, \tilde{Y}_n = 0$. The proof of (a) and (b) shows that if l is a prime dividing n, then for all positive integers r and all $y_1, y_2 \in Y_{l^r}$, we have

$$e_{\mu,l^r}(f_\sigma^{-1}(y_1), y_2) = e_{\mu,l^r}(y_1, f_\sigma(y_2)).$$

Since the Rosati involution is the adjoint with respect to the non-degenerate induced pairing on the Tate modules

$$e_{\mu,l^\infty} : T_l(Y) \times T_l(Y) \to \mathbb{Z}_l(1) = \varprojlim \boldsymbol{\mu}_{l^r},$$

we have $\rho_\mu(f_\sigma) = f_\sigma^{-1}$, proving (d). □

Remark 2.3. Suppose we have $I(n)$ for some $n > 2d(\deg(f))^{2d}$, where $d = \dim(Y)$, suppose the polarizations λ and μ are defined over F, and suppose $\tilde{Y}_n \cong (\mathbb{Z}/n\mathbb{Z})^b$ for some b. Then f is defined over F. The idea of the proof is given in Section 3.4.4 of [10], and runs as follows. Since λ and μ are defined over F, we have $\mu = {}^t f_\sigma \mu f_\sigma$ for every $\sigma \in \mathrm{Gal}(L/F)$. Letting $g = \deg(f) f_\sigma \in \mathrm{End}_L(Y)$, then $\rho_\mu(g) g = (\deg(f))^2$. The characteristic polynomial of g is uniquely determined by the traces $\mathrm{Tr}(g^i)$ for $1 \leq i \leq 2d$. By the Proposition on p. 203 of [4], g is semisimple and all its eigenvalues have absolute value equal to $\deg(f)$. Therefore,

$$|\mathrm{Tr}(g^i)| \leq 2d(\deg(f))^i. \tag{1}$$

By Lemma 2.2(c) we have $(f_\sigma - 1) Y_n \subseteq \tilde{Y}_n$. Since $\tilde{Y}_n \cong (\mathbb{Z}/n\mathbb{Z})^b$ and $(f_\sigma - 1)\tilde{Y}_n = 0$, we have $\mathrm{Tr}(f_\sigma^i - 1) \in n\mathbb{Z}[1/\deg(f)]$ for $i = 1, \ldots, 2d$, and therefore

$$\mathrm{Tr}(g^i) \equiv 2d(\deg(f))^i \pmod{n}. \tag{2}$$

If $n > 2d(\deg(f))^{2d}$, then by (1) and (2) we must have $\mathrm{Tr}(g^i) = 2d(\deg(f))^i = \mathrm{Tr}((\deg(f))^i)$. Therefore $g = \deg(f)$, so $f_\sigma = 1$ for all σ, and f is defined over F.

3. Generalizations of Serre's Lemma and Minkowski's Theorem

Recall that Serre's Lemma [5, pp. 17–19, Theorem] says that if Y is an abelian variety, α is an element of $\mathrm{End}(Y)$ of finite order, $3 \leq n \in \mathbb{Z}$, and $\alpha - 1 \in n\,\mathrm{End}(Y)$, then $\alpha = 1$. In Theorem 3.1 we give a generalization of Serre's Lemma (one obtains Serre's Lemma by taking $k = r = i(1) = 1$ in Theorem 3.1 below). Let

$$N(k) = \{\text{prime powers } l^m \mid 0 \leq m(l-1) \leq k\}.$$

For example, $N(1) = \{1, 2\}$, $N(2) = \{1, 2, 3, 4\}$, and $N(3) = \{1, 2, 3, 4, 8\}$.

Theorem 3.1. *If Y is an abelian variety, n, k, r, and M are positive integers such that $n \notin N(k)$ and $(r, n) = 1$, α is an element of $\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r]$ such that $\alpha^M = 1$, $i(1), \ldots, i(k)$ are integers relatively prime to M, and*

$$\prod_{j=1}^{k} (\alpha^{i(j)} - 1) \in n(\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r]),$$

then $\alpha = 1$.

Since α has finite order, $\mathbb{Q}[\alpha]$ is a semisimple commutative subalgebra of $\mathrm{End}^0(Y)$ and therefore is a direct sum of number fields. To prove Theorem 3.1 it suffices to prove the following lemma (see also [4, p. 207]).

Lemma 3.2. *If ζ is an Mth root of unity in $\mathbb{C}$, n, k, and r are positive integers such that $n \notin N(k)$ and $(r, n) = 1$, $\mathcal{O}$ is the ring of all algebraic integers in $\mathbb{C}$, $i(1), \ldots, i(k)$ are integers relatively prime to M, and*

$$\prod_{j=1}^{k} (\zeta^{i(j)} - 1) \in n(\mathcal{O}[1/r]),$$

then $\zeta = 1$.

Proof. If l is a prime dividing M, then

$$(\zeta^{M/l})^j - 1 = (\zeta^j - 1)(1 + \zeta^j + \zeta^{2j} + \cdots + \zeta^{j(M/l\ \ 1)}),$$

and therefore, replacing ζ by $\zeta^{M/l}$, we can assume the exact order of ζ is a prime number l. We know that the prime ideal above l in the ring of integers of $\mathbb{Q}(\zeta)$ is generated by any one of the $\zeta^a - 1$, for $a = 1, \ldots, l-1$. Therefore,

$$\prod_{a=1}^{l-1} (\zeta^a - 1)^k \in n^{l-1}(\mathcal{O}[1/r]).$$

If Φ_l is the lth cyclotomic polynomial, then

$$l = \Phi_l(1) = \prod_{a=1}^{l-1} (\zeta^a - 1).$$

Therefore, $l^k \in n^{l-1}(\mathcal{O}[1/r])$. Since $(r, n) = 1$, this gives that n^{l-1} divides l^k. Therefore, n is a prime power of the form l^m with $m(l-1) \leq k$. □

Corollary 3.3. *Suppose Y is an abelian variety, n and r are relatively prime integers, and α is an element of $\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r]$ of finite multiplicative order. Then:*

(a) *if k is a positive integer, $n \notin N(k)$, and $(\alpha - 1)^k \in n(\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r])$, then $\alpha = 1$,*

(b) *if $n \geq 5$ and $(\alpha - 1)^2 \in n(\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r])$, then $\alpha = 1$,*

(c) *if $n \geq 5$ and $(\alpha - 1)(\alpha^{-1} - 1) \in n(\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r])$, then $\alpha = 1$.*

Proof. Case (a) is Theorem 3.1 with $i(1) = \cdots = i(k) = 1$. Case (b) is case (a) with $k = 2$. Case (c) is Theorem 3.1 with $k = 2$, $i(1) = 1$, and $i(2) = -1$. Note that case (c) also follows from case (b), since $\alpha^{-1} - 1 = -(\alpha - 1)\alpha^{-1}$. □

A similar result to Lemma 3.2 holds with $\mathcal{O}[1/r]$ replaced by $M_g(\mathbb{Z}[1/r])$ and ζ replaced by a matrix in $\mathrm{GL}_g(\mathbb{Z}[1/r])$ of order dividing M. Such a result can be viewed as a generalization of Minkowski's Theorem [3] which says that an integral

matrix of finite order, which is congruent to the identity matrix modulo an integer $n \geq 3$, must be the identity matrix. In Section 4 we will make use of the following related lemma, which follows from simple divisibility arguments. Write I_g for the $g \times g$ identity matrix, and $\mathbb{Z}_2$ for the ring of 2-adic integers.

Lemma 3.4. *If $A \in \mathrm{Gl}_g(\mathbb{Z}_2)$ is a matrix of finite order, $0 \leq b \leq g$, and β is a $b \times (g-b)$ matrix over $\mathbb{Z}_2$ such that*

$$A - \begin{pmatrix} I_b & \beta \\ 0 & I_{g-b} \end{pmatrix} \in 4M_g(\mathbb{Z}_2),$$

then $A = I_g$. □

4. Variations on Serre's Lemma

Theorem 4.1. *Suppose Y is an abelian variety, n and r are relatively prime positive integers, and n is not divisible by the characteristic of a field of definition for Y. Suppose α is an element of $\mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r]$ (and therefore α induces an endomorphism of Y_n), α has finite multiplicative order, and $\tilde{Y}_n$ is a subgroup of Y_n on which α induces the identity map. Then $\alpha = 1$, provided that one of the following conditions* (a), (b), (c), *or* (d) *holds*:

(a) *$n \geq 5$, μ is a polarization on Y, α commutes with $\rho_\mu(\alpha)$ in $\mathrm{End}^0(Y)$, and $\tilde{Y}_n$ contains a maximal isotropic subgroup of Y_n with respect to $e_{\mu,n}$,*

(b) *$n \geq 5$ and $(\alpha - 1) Y_n \subseteq \tilde{Y}_n$,*

(c) *$n \geq 4$, $\tilde{Y}_n$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^b$ for some b, and $(\alpha - 1) Y_n \subseteq \tilde{Y}_n$,*

(d) *$n \geq 3$ and $\tilde{Y}_n = Y_n$.*

Proof. With assumptions as in case (a), let E be $\mathbb{Q}[\alpha, \rho_\mu(\alpha)]$, a commutative $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(Y)$ stable under the action of ρ_μ. Then E is semisimple (since it has a positive involution, ρ_μ), E is a direct sum of totally real number fields and CM-fields, and ρ_μ acts on E by complex conjugation (i.e., as the identity on the totally real fields and by complex conjugation on the CM-fields). (See also [4, p. 204].) Now we have $\rho_\mu(\alpha)\alpha = 1$, since $\rho_\mu(\alpha)\alpha$ is positive and of finite order. Since α has finite order, we have $\alpha^{-1} \in \mathrm{End}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[1/r]$, so α^{-1} induces an endomorphism on Y_n. For $y \in Y_n$ and $\tilde{y} \in \tilde{Y}_n$ we have

$$\begin{aligned} e_{\mu,n}((\alpha^{-1} - 1)y, \tilde{y}) &= e_{\mu,n}((\rho_\mu(\alpha) - 1)y, \tilde{y}) = e_{\mu,n}(y, (\alpha - 1)\tilde{y}) \\ &= e_{\mu,n}(y, 0) = 1. \end{aligned}$$

Since $\tilde{Y}_n$ contains a maximal isotropic subgroup of Y_n, we have $(\alpha^{-1} - 1) Y_n \subseteq \tilde{Y}_n$. Therefore we have $(\alpha - 1)(\alpha^{-1} - 1) Y_n = 0$, and case (a) follows by applying Corollary 3.3(c). Case (b) follows from Corollary 3.3(b). For case (c), it suffices to treat the

case $n = 4$. Case (c) then follows from Lemma 3.4, by viewing α as a matrix of finite order in $\mathrm{GL}_{2d}(\mathbb{Z}_2)$, where $d = \dim(Y)$. Case (d) is Serre's Lemma. □

Suppose Y is an abelian variety, μ is a polarization on Y, and E is a commutative $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(Y)$ stable under the action of ρ_μ. Then E is a direct sum of totally real number fields and CM-fields, and we define a *minimal idempotent* of E to be an idempotent p of E such that pE is a field. Let $\mathscr{M}$ be the set of minimal idempotents of E. Then $E = \bigoplus_{p\in\mathscr{M}} pE$. Let pY be the abelian variety which is RpY for every positive integer R such that $Rp \in \mathrm{End}(Y)$. Then $Y(\bar{F}) = \sum_{p\in\mathscr{M}} pY(\bar{F})$.

The proof of Theorem 4.2 combines elements of the proofs of Theorem 4.1 and Lemma 3.2.

Theorem 4.2. *Suppose Y is an abelian variety, μ is a polarization on Y, $5 \le n \in \mathbb{Z}$, n is not divisible by the characteristic of a field of definition for Y and is relatively prime to the degree of the polarization μ, E is a commutative $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(Y)$ stable under the action of ρ_μ, and $\mathscr{M}$ is the set of minimal idempotents of E. Suppose $\alpha \in E \cap (\mathrm{End}(Y) \otimes \mathbb{Z}[1/r])$ for some integer r relatively prime to n, $\tilde{Y}_n$ is a subgroup of Y_n which contains a maximal isotropic subgroup of Y_n with respect to the pairing $e_{\mu,n}$, and α induces the identity map on $\tilde{Y}_n$. Suppose $p \in \mathscr{M}$ and $p\alpha$ is an element of finite order in the number field pE. Then $p\alpha = p$ (i.e., $p\alpha = 1$ in the field pE).*

Proof. If $p\alpha \neq 1$ in pE, then, replacing α by a power of α if necessary, we can assume $p\alpha$ has prime order, say q, in pE. Let l be a prime dividing n, and let

$$T(l) = pV_l(Y) \cap T_l(Y).$$

Let $\mathscr{O}_l = \mathbb{Z}_l[p\alpha] = \mathbb{Z}_l[\zeta]$, where ζ is a primitive qth root of unity. Since p is an idempotent, $p\alpha$ acts on $pV_l(Y)$ as α does. Since r and n are relatively prime, α acts on $T_l(Y)$. Therefore, $p\alpha T(l) = \alpha T(l) = T(l)$, and $T(l)$ is a free $\mathscr{O}_l$-module of positive rank. Let

$$Y(n) = T(l)/nT(l).$$

We can view $Y(n)$ as a subgroup of Y_n. Since n is relatively prime to the degree of μ, we can view $\rho_\mu(\alpha)$ as an endomorphism of Y_n. For $y \in Y_n$ and $\tilde{y} \in \tilde{Y}_n$ we have

$$e_{\mu,n}((\rho_\mu(\alpha) - 1)y, \tilde{y}) = e_{\mu,n}(y, (\alpha - 1)\tilde{y}) = e_{\mu,n}(y, 0) = 1.$$

Since $\tilde{Y}_n$ contains a maximal isotropic subgroup of Y_n, we have

$$(\rho_\mu(\alpha) - 1)\, Y(n) \subseteq (\rho_\mu(\alpha) - 1)\, Y_n \subseteq \tilde{Y}_n.$$

Therefore,

$$(\alpha - 1)(\rho_\mu(\alpha) - 1)\, Y(n) \subseteq (\alpha - 1)\, \tilde{Y}_n = 0,$$

and thus

$$(\alpha - 1)(\rho_\mu(\alpha) - 1)\, T(l) \subseteq nT(l).$$

Now α acts on $T(l)$ as ζ does, and $\rho_\mu(\alpha)$ acts on $T(l)$ as ζ^{-1} does. Therefore,

$$(\zeta - 1)(\zeta^{-1} - 1)\, T(l) \subseteq nT(l). \tag{3}$$

The proof now proceeds in a similar way to the proof of Lemma 3.2. If $q \neq l$, then the left side of (3) is $T(l)$, and the right side is contained in $lT(l)$, giving a contradiction. Therefore, $q = l$ for all primes l dividing n. We can therefore write $q = l$ and $n = l^i$. Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Q}(\zeta) = \mathbb{Q}(p\alpha)$ above l. Then

$$(l) = \mathfrak{P}^{l-1} \quad \text{and} \quad \mathfrak{P} = (\zeta^j - 1) \text{ for } j = 1, \ldots, l-1.$$

By (3) we now have

$$\mathfrak{P}^2 T(l) \subseteq nT(l) = l^i T(l) = \mathfrak{P}^{i(l-1)} T(l).$$

Therefore $i(l-1) \leq 2$, and so $n = l^i \leq 4$, contradicting our assumption on n. □

5. Proof of Theorem 1.2

Recall that $Z_L(Y)$ denotes the center of $\mathrm{End}_L^0(Y)$, and that for $f: X \to Y$ an isogeny of F-abelian varieties, and L a Galois extension of F over which f is defined, we write $f_\sigma = f\sigma(f)^{-1} \in \mathrm{End}_L^0(Y)$, if $\sigma \in \mathrm{Gal}(L/F)$. Further, let $\varphi_{f,L}$ denote the isomorphism

$$\varphi_{f,L}: \mathrm{End}_L^0(Y) \xrightarrow{\sim} \mathrm{End}_L^0(X)$$

defined by $\varphi_{f,L}(u) = f^{-1}uf$.

Lemma 5.1. *Suppose X and Y are abelian varieties defined over a field F, $f: X \to Y$ is an isogeny, and L is a Galois extension of F over which f is defined. Then $\varphi_{f,L}$ is defined over F if and only if $f_\sigma \in Z_L(Y)$ for every $\sigma \in \mathrm{Gal}(L/F)$.*

Proof. The isomorphism $\varphi_{f,L}$ is defined over L. It is defined over F if and only if

$$\varphi_{f,L}(u) = \sigma(\varphi_{f,L}(\sigma^{-1}(u))) \tag{4}$$

for every $\sigma \in \mathrm{Gal}(L/F)$ and $u \in \mathrm{End}_L^0(Y)$. Now (4) is equivalent to $f_\sigma^{-1} u f_\sigma = u$, and the result follows. □

By Lemma 5.1, Theorem 1.2 will be proved once we know the following result.

Theorem 5.2. *Suppose we have $I(n)$ for some $n \geq 5$, the map $\varphi_{f,L}$ is defined over F, and the degree of μ is relatively prime to n. Then X and Y are isogenous over F. Further, the isogeny f is defined over every extension of F over which all elements of $Z_L(Y)$ are defined.*

The remainder of this section is devoted to the proof of Theorem 5.2.

Assume $I(n)$ for some $n \geq 5$, and suppose $\varphi_{f,L}$ is defined over F and the degree of μ is relatively prime to n. We will apply Theorem 4.2 with $E = Z_L(Y)$. By Lemma 5.1, we know $f_\sigma \in Z_L(Y)$ for every $\sigma \in \mathrm{Gal}(L/F)$. If $p \in \mathscr{M}$, let E_p be the field $pZ_L(Y) = pE \subset Z_L(Y)$, and let

$$G_p = \{\sigma \in \mathrm{Gal}(L/F) \mid \sigma(p) = p\}.$$

If $\sigma \in G_p$, then $\sigma(E_p) = E_p$; so G_p acts on E_p. Let

$$G_p^0 = \ker(G_p \to \mathrm{Aut}(E_p)).$$

Clearly, G_p/G_p^0 acts faithfully on E_p. Let $F(p)$ be the subfield of L fixed by G_p.

Lemma 5.3. *If $p \in \mathscr{M}$, then there exists an element $v \in E_p^\times \cap \mathrm{End}_L(Y)$ such that the homomorphism vf is defined over the field $F(p)$.*

Proof. The map $g_p: G_p \to E_p^\times$ defined by $g_p(\sigma) = pf_\sigma$ defines a cocycle, and therefore a cohomology class in $H^1(G_p, E_p^\times)$, since $f_\sigma \in Z_L(Y) = E$. Consider the inflation–restriction exact sequence:

$$1 \to H^1(G_p/G_p^0, (E_p^\times)^{G_p^0}) \to H^1(G_p, E_p^\times) \to H^1(G_p^0, E_p^\times). \tag{5}$$

The left term is trivial by Hilbert's Theorem 90. The last term is $\mathrm{Hom}(G_p^0, E_p^\times)$. Therefore $g_p(\sigma)$ is an element of finite order in $E_p^\times$, if σ is in the finite group G_p^0. Applying Theorem 4.2 with $\alpha = f_\sigma$ for each $\sigma \in G_p^0$, we see that g_p is trivial on G_p^0. By (5), g_p is now a coboundary, so there exists an element $v \in E_p^\times$ such that for every

$\sigma \in G_p$, $g_p(\sigma) = v^{-1}\sigma(v)$. After multiplying if necessary by a positive integer, we can assume that $v \in E_p^\times \cap \mathrm{End}_L(Y)$. Now for $\sigma \in G_p$,

$$v^{-1}\sigma(v) = g_p(\sigma) = pf_\sigma = pf\sigma(f)^{-1}.$$

Therefore, viewing v as an element of $\mathrm{End}_L(Y)$, we have $\sigma(vf) = vpf$. Since $v \in E_p$, we have $vp = v$. Therefore, $\sigma(vf) = vf$ for all $\sigma \in G_p$, and so vf is defined over $F(p)$. □

Remark 5.4. If we have $I(n)$ for some $n \geq 5$, and $\mathrm{End}_L^0(Y)$ is a field, then X and Y are isogenous over F, even without assuming $(\deg(\mu), n) = 1$. This is true because when $\mathrm{End}_L^0(Y)$ is a field we can apply Theorem 4.1 rather than Theorem 4.2 in the proof of Lemma 5.3, and Lemma 5.3 then gives an element $v \in \mathrm{End}_L(Y)$ such that vf is an F-isogeny from X onto Y.

Let S be the set of $\mathrm{Gal}(L/F)$-orbits in $\mathscr{M}$. Choose one representative from each orbit $j \in S$, to obtain a finite set $\{p_j \mid j \in S\}$ of minimal idempotents such that

$$\mathscr{M} = \{\sigma(p_j) \mid j \in S \text{ and } \sigma \in \mathrm{Gal}(L/F)\}.$$

By Lemma 5.3, for each $j \in S$ there is an element $v_j \in E_{p_j}^\times \cap \mathrm{End}_L(Y)$ such that $v_j f$ is defined over $F(p_j)$. After multiplying v_j by a positive integer if necessary, we can assume that for every $\sigma \in \mathrm{Gal}(L/F)$ we have $\sigma(v_j)f_\sigma^{-1} \in \mathrm{End}_L(Y)$. Fix one such v_j for each $j \in S$. If $\sigma \in \mathrm{Gal}(L/F)$ and $p = \sigma(p_j) \in \mathscr{M}$, let $h_p = \sigma(v_j f)$.

Then h_p is well-defined, since for $\sigma(p_j) = \tau(p_j)$ with $\sigma, \tau \in \mathrm{Gal}(L/F)$, we then have $\tau^{-1}\sigma \in G_{p_j}$. Since $v_j f$ is defined over $F(p_j)$, and $F(p_j)$ is the fixed field of G_{p_j}, we have $\tau^{-1}\sigma(v_j f) = v_j f$, so $\sigma(v_j f) = \tau(v_j f)$.

Further, $h_{\tau(p)} = \tau(h_p)$, for $\tau \in \mathrm{Gal}(L/F)$ and $p \in \mathscr{M}$. Let $h = \sum_{p \in \mathscr{M}} h_p$. Then h is defined over F, since $\sum_{p \in j} h_p$ is $\mathrm{Gal}(L/F)$-invariant and $h = \sum_{j \in S}(\sum_{p \in j} h_p)$. We will show that h is an isogeny from X onto Y.

For $p \in \mathscr{M}$, let $u_p = h_p f^{-1} \in \mathrm{End}_L^0(Y)$.

Lemma 5.5. *For every $p \in \mathscr{M}$, we have $u_p \in E_p^\times \cap \mathrm{End}_L(Y) \subset Z_L(Y)$.*

Proof. Writing $p = \sigma(p_j)$ with $j \in S$ and $\sigma \in \mathrm{Gal}(L/F)$, then $u_p = \sigma(v_j f)f^{-1} = \sigma(v_j)f_\sigma^{-1}$. Therefore, by the choice of v_j, we have $u_p \in \mathrm{End}_L(Y)$. We know $v_j \in E_{p_j}^\times = (p_j E)^\times$ and $f_\sigma \in E^\times$. Therefore, $u_p = \sigma(v_j)f_\sigma^{-1} \in \sigma(p_j E)^\times E^\times = (pE)^\times E^\times = E_p^\times$. □

Let $v = \sum_{p \in \mathscr{M}} u_p \in \bigoplus_{p \in \mathscr{M}} E_p^\times = E^\times = Z_L(Y)^\times$. Then $h = vf$ is an F-isogeny from X onto Y. Therefore f is defined over every extension of F over which v is defined, and we have Theorem 5.2. □

6. Proof of Theorem 1.3

Lemma 6.1. *Suppose Y is an abelian variety defined over a field F, μ is a polarization on Y, L is a field extension of F over which μ is defined, and* $\mathrm{End}_L(Y) = \mathrm{End}_F(Y)$. *Then μ is defined over F.*

Proof. By [6, p. 27, Proposition 11], Y has a polarization φ defined over F. Then $\mu^{-1}\varphi \in \mathrm{End}_L^0(Y) = \mathrm{End}_F^0(Y)$, and therefore μ is defined over F. □

Lemma 6.2. *If X is an abelian variety defined over a field L, and λ_1 and λ_2 are polarizations on X defined over L whose induced Rosati involutions coincide on* $\mathrm{End}_L^0(X)$, *then $\lambda_2^{-1}\lambda_1 \in Z_L(X)$.*

Proof. Let $\alpha = \lambda_2^{-1}\lambda_1 \in \mathrm{End}_L^0(X)$. Take any $\gamma \in \mathrm{End}_L^0(X)$. The transpose map gives a natural isomorphism $\psi : \mathrm{End}_L^0(X) \xrightarrow{\sim} \mathrm{End}_L^0(X^*)$, where X^* is the Picard variety of X. Let $\beta = \psi^{-1}(\lambda_2 \gamma \lambda_2^{-1}) \in \mathrm{End}_L^0(X)$. By the equality of the Rosati involutions ρ_1 and ρ_2 corresponding to λ_1 and λ_2, we have

$$\begin{aligned}\gamma &= \lambda_2^{-1}\psi(\beta)\lambda_2 = \rho_2(\beta) = \rho_1(\beta)\\ &= \lambda_1^{-1}\psi(\beta)\lambda_1 = \alpha^{-1}\lambda_2^{-1}\psi(\beta)\lambda_2\alpha = \alpha^{-1}\gamma\alpha,\end{aligned}$$

i.e., $\gamma = \alpha^{-1}\gamma\alpha$ for every $\gamma \in \mathrm{End}_L^0(X)$. Therefore, $\alpha \in Z_L(X)$. □

Lemma 6.3. *Suppose X is an abelian variety defined over a field F, λ is a polarization on X, and L is a Galois extension of F over which λ is defined. Let ρ be the restriction to* $\mathrm{End}_L^0(X)$ *of the Rosati involution induced by λ. If ρ is defined over F, then $\sigma(\lambda)^{-1}\lambda \in Z_L(X)$ for every $\sigma \in \mathrm{Gal}(L/F)$.*

Proof. Direct computation shows that if ρ is defined over F, then $\rho_{\sigma(\lambda)} = \rho_\lambda$ on $\mathrm{End}_L^0(X)$. By Lemma 6.2, we have $\sigma(\lambda)^{-1}\lambda \in Z_L(X)$. □

We will now prove Theorem 1.3. Suppose we have $I(n)$ for some $n \geq 5$, L is a finite Galois extension of F over which f and μ are defined, $\mathrm{End}_L(Y) = \mathrm{End}_F(Y)$, and the Rosati involution on $\mathrm{End}_L^0(X)$ induced by the polarization λ is defined over F. We will show f is defined over F. By Lemma 6.1, the polarization μ is defined over F, and therefore a direct computation gives that $\rho_\mu(f_\sigma) f_\sigma = \sigma(f)\sigma(\lambda)^{-1}\lambda\sigma(f)^{-1}$. By Lemma 6.3, we have $\sigma(\lambda)^{-1}\lambda \in Z_L(X)$. Therefore, $\rho_\mu(f_\sigma) f_\sigma \in Z_L(Y)$, so f_σ and $\rho_\mu(f_\sigma)$ commute in $\mathrm{End}_L^0(Y)$. Since $\mathrm{End}_L(Y) = \mathrm{End}_F(Y)$, the map $\sigma \mapsto f_\sigma$ is an element of $\mathrm{Hom}(\mathrm{Gal}(L/F), (\mathrm{End}_L^0(Y))^\times)$. Since $\mathrm{Gal}(L/F)$ is a finite group, f_σ has finite multiplicative order in $\mathrm{End}_L^0(Y) = \mathrm{End}_F^0(Y)$, for every $\sigma \in \mathrm{Gal}(L/F)$. By Theorem 4.1, we have $f_\sigma = 1$. Therefore, $f = \sigma(f)$ for every $\sigma \in \mathrm{Gal}(L/F)$, so f is defined over F. □

Remark 6.4. By Lemma 6.1, Remark 1.4, and Theorem 1.3, if we have $I(n)$ for some $n \geq 5$, the polarizations λ and μ are defined over L, $\mathrm{End}_L(Y) = \mathrm{End}_F(Y)$, and $\mathrm{End}_L(X) = \mathrm{End}_F(X)$, then f, λ, and μ are defined over F.

7. Proof of Theorem 1.6

In this section we will show that if we have $I(n)$, with n arbitrary, and the given polarizations λ and μ are defined over the ground field F, then the lack of an F-isogeny would imply that $[L:F]^2$ is divisible by n. With assumptions as in Theorem 1.6, let $h = \sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma(f)$. Then h is a homomorphism from X to Y defined over F, and we will show h is an isogeny.

Let $u = hf^{-1} \in \mathrm{End}(Y) \otimes \mathbb{Z}[1/\deg(f)]$. Writing $u_\sigma = f_\sigma^{-1} = \sigma(f) f^{-1} \in \mathrm{End}^0(Y)$, then $u = \sum_{\sigma \in \mathrm{Gal}(L/F)} u_\sigma$. Since n is relatively prime to $\deg(f)$, we can view u as an endomorphism of Y_n. If h is not an isogeny, then for every positive integer M not divisible by $\mathrm{char}(F)$ there is a point $x \in X$ of exact order M such that $h(x) = 0$. Considering the case $M = n$, and letting $y = f(x)$, then $y \in Y_n$ is a point of exact order n and $u(y) = 0$.

By Lemma 2.2(c), $(u_\sigma - 1) Y_n \subseteq \tilde{Y}_n$. Therefore, $(u_\sigma - 1)^2 = 0$ on Y_n, and $(u_\sigma - 1)(u_\tau - 1) = 0$ on Y_n, for every $\sigma, \tau \in \mathrm{Gal}(L/F)$. Let $m = [L:F]$. It follows that $(u - m)^2 = 0$ on Y_n. This implies that $(2m - u)u = m^2$ on Y_n. Since n does not divide m^2, we obtain that for every point $y \in Y$ of exact order n,

$$(2m - u)u(y) = m^2 y \neq 0.$$

Therefore $u(y) \neq 0$, and h must be an isogeny. If $x \in \tilde{X}_n$, then $h(x) = mf(x)$. Therefore the restriction of h to $X_t \cap \tilde{X}_n$ has trivial kernel. □

Remark 7.1. Let $L(f)$ be the smallest extension of F over which f is defined, i.e., the subfield of invariants of $\{\sigma \in \mathrm{Gal}(L/F) \mid \sigma(f) = f\}$. Then the result of Theorem 1.6 remains true if we replace $[L:F]$ by $[L(f):F] = \#\{\mathrm{Gal}(L/F)f\}$ and $\sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma(f)$ by $\sum_{g \in \mathrm{Gal}(L/F)f} g$. Note that $L(f)$ is not necessarily Galois over F.

Remark 7.2. Suppose we have $I(n)$ for some $n \geq 5$, and we take the field L of 1.1(g) to be the smallest extension of F over which all the endomorphisms of X and of Y are defined. Then L is a finite Galois extension of F over which f, μ, and λ are defined, by Remark 6.4. Further, $[L:F]$ is not divisible by any primes greater than $2\dim(X) + 1$. For an explicit integer that $[L:F]$ must divide, in terms of $\dim(X) = \dim(Y)$, see [7]. Therefore f is defined over an extension of F whose degree can be bounded in terms of $\dim(X)$. Moreover, we can conclude from Theorem 1.6 that if we have $I(n)$ with n sufficiently large (depending only on $\dim(X)$), and if λ and μ are defined over F, then X and Y are F-isogenous.

Remark 7.3. Suppose X and Y are abelian varieties defined over a field F, $f: X \to Y$ is an isogeny, Y is F-simple, L is a finite Galois extension of F over which f is defined, and $x \in X$ is a point such that the order of $f(x)$ does not divide $[L:F]$ and such that $\sigma(f)(x) = f(x)$ for every $\sigma \in \mathrm{Gal}(L/F)$. Then $\sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma(f)$ is an F-isogeny from X onto Y.

8. Proof of Proposition 1.9

Under the hypotheses in Proposition 1.9, consider

$$g \in H^1(\mathrm{Gal}(L/F), (\mathrm{End}_L^0(Y))^\times)$$

defined by $g(\sigma) = f_\sigma$. By Lemma 2.2(d), we have $\rho_\mu(f_\sigma) f_\sigma = 1$. Our hypotheses now tell us that the $\mathrm{Gal}(L/F)$-action on the images of g is trivial. Therefore, $g \in \mathrm{Hom}(\mathrm{Gal}(L/F), (\mathrm{End}_L^0(Y))^\times)$. Since $\mathrm{Gal}(L/F)$ is a finite group, the element $g(\sigma) = f_\sigma$ has finite order, for every $\sigma \in \mathrm{Gal}(L/F)$. By Theorem 4.1 and Lemma 2.2(c), we have $f_\sigma = 1$, so f is defined over F. □

Acknowledgment

The work was done while the second author was a Visiting Professor at Ohio State University and a Visiting Scholar at Harvard University; he would like to thank both universities for their hospitality. The first author would like to thank the Alfred P. Sloan Foundation, the NSF, and Ohio State University for financial support.

References

[1] W.L. Chow, Abelian varieties over function fields, Trans. Amer. Math. Soc. 78 (1955) 253–275.
[2] S. Lang, Abelian Varieties (Springer, New York, 2nd ed., 1983).
[3] H. Minkowski, Gesammelte Abhandlungen, Band I (Leipzig, 1911) 212–218; Zur Theorie der positiven quadratischen Formen, J. Reine Angew. Math. 101 (1887) 196–202.
[4] D. Mumford, Abelian Varieties, Tata Lecture Notes (Oxford University Press, London, UK, 2nd ed., 1974).
[5] J-P. Serre, Rigidité du foncteur de Jacobi d'echelon $n \geq 3$, Appendix to A. Grothendieck, Techniques de Construction en Géométrie Analytique, X. Construction de l'espace de Teichmüller, Séminaire Henri Cartan, 1960/61, no. 17.
[6] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its application to number theory, Publ. Math. Soc. Japan 6 (1961).
[7] A Silverberg, Fields of definition for homomorphisms of abelian varieties, J. Pure Appl. Algebra 77 (1992) 253–262.
[8] A. Weil, Variétés Abéliennes et Courbes Algébriques (Hermann, Paris, 1948).
[9] A. Weil, Foundations of Algebraic Geometry (American Mathematical Society, Providence, RI, 2nd ed., 1962).
[10] Yu.G. Zarhin, On equations defining moduli of abelian varieties with endomorphisms in a totally real field, Trudy Moskov. Mat. Obshch. 42 (1981) 3–49; translation: Trans. Moscow Math. Soc. (2) (1982) 1–46.