Homomorphisms of abelian varieties over finite fields

Yuri G. Zarhin

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, Russia

e-mail: zarhin@math.psu.edu

Abstract. We give a proof of Tate's theorems on homomorphisms of abelian varieties over finite fields and the corresponding ℓ-divisible groups.

The aim of this note is to give a proof of Tate's theorems on homomorphisms of abelian varieties over finite fields and the corresponding ℓ-divisible groups [27,12], using ideas of [32,33]. We give a unified treatment for both $\ell \neq p$ and $\ell = p$ cases. In fact, we prove a slightly stronger version of those theorems with "finite coefficients". We use neither the existence (and properties) of the Frobenius endomorphism (for $\ell \neq p$) nor Dieudonne modules (for $\ell = p$).

The paper is organized as follows. (A rather long) Section 1 contains auxiliary results about finite commutative group schemes and abelian varieties with special reference to isogenies and polarizations. We discuss ℓ-divisible groups (aka Barsotti–Tate groups) in Section 2. Section 3 contains useful results that play a crucial role in the proof of main results that are stated in Section 4.

The next five Sections contain proofs of results that were stated in Section 3. In Section 5 we discuss abelian subvarieties of a given abelian variety. Section 6 deals with the finiteness of the set of abelian varieties of given dimension and "bounded degree" over a finite field. In Section 7 we present a so called *quaternion trick*. In Section 8 we prove a crucial result about arbitrary finite group subschemes of abelian varieties over finite fields. In Section 9 we try to divide endomorphisms of a given abelian variety modulo n.

The main results of this paper are proven in Section 10. Their variants for Tate modules are discussed in Section 11. An example of non-isomorphic elliptic curves over a finite field with isomorphic ℓ-divisible groups (for all primes ℓ) is discussed in Section 12.

I am grateful to Frans Oort and Bill Waterhouse for useful discussions and to the referee, whose comments helped to improve the exposition. My special thanks go to Dr. Boris Veytsman for his help with TEXnical problems.

1. Definitions and statements

Throughout this paper K is a field and $\bar{K}$ its algebraic closure. If X (resp. W) is an algebraic variety (resp. group scheme) over K then we write $\bar{X}$ (resp. $\bar{W}$) for the corresponding algebraic variety $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K})$ (resp. group scheme $W \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K})$) over $\bar{K}$. If $f : X \to Y$ is a a regular map of algebraic varieties over K then we write $\bar{f}$ for the corresponding map $\bar{X} \to \bar{Y}$.

1.1. Finite commutative group schemes over fields. We refer the reader to the books of Oort [17], Waterhouse [31] and Demazure–Gabriel [3] for basic properties of commutative group schemes; see also [25,21].

Recall that a group scheme V over K is called finite if the structure morphism $V \to \mathrm{Spec}(K)$ is finite. Since $\mathrm{Spec}(K)$ is a one-point set, it follows from the definition of finite morphism [7, Ch. II, Sect. 3] that V is an affine scheme and $\Gamma(V, \mathcal{O}_V)$ is a finite-dimensional commutative K-algebra. The K-dimension of the $\Gamma(V, \mathcal{O}_V)$ is called the *order* of V and denoted by $\#(V)$. An analogue of Lagrange theorem [19] asserts that multiplication by $\#(V)$ kills commutative V.

Let V and W be finite commutative group schemes over K and let $u : V \to W$ be a morphism of group K-schemes. Both V and W are affine schemes, $A = \Gamma(V, \mathcal{O}_V)$ and $B = \Gamma(W, \mathcal{O}_W)$ are finite-dimensional (commutative) K-algebras (with 1), $V = \mathrm{Spec}(A), W = \mathrm{Spec}(B)$ and u is induced by a certain K-algebra homomorphism

$$u^* : B \to A.$$

Since V and W are commutative group schemes, A and B are cocommutative Hopf K-algebras. Since u is a morphism of group schemes, u^* is a morphism of Hopf algebras. It follows that $C := u^*(B)$ is a K-subalgebra and also a Hopf subalgebra in A. It follows that $U := \mathrm{Spec}(C)$ carries the natural structure of a finite group scheme over K such that the natural scheme morphism $U \to V$ induced by $u^* : B \twoheadrightarrow u^*(B) = C$ is a morphism of group schemes. In addition, the inclusion $C \subset A$ induces the morphism of schemes $V \to U$, which is also a morphism of group schemes. The latter morphism is an epimorphism in the category of finite commutative group schemes over K, because the corresponding map

$$C = \Gamma(U, \mathcal{O}_U) \to \Gamma(V, \mathcal{O}_V) = A$$

is nothing else but the inclusion map $C \subset A$ and therefore is injective [18] (see also [5]).

On the other hand, the surjection $B \twoheadrightarrow C$ provides us with a canonical isomorphism $U \cong \mathrm{Spec}(B/\ker(u^*))$; in addition, we observe that $\mathrm{Spec}(B/\ker(u^*))$ is a (closed) group subscheme of $\mathrm{Spec}(B) = W$. We denote $\mathrm{Spec}(B/\ker(u^*))$ by $u(V)$ and call it the image of u or the image of V with respect to u and denote by $u(V)$. Notice that the set theoretic image of u is closed and our definition of the image of u coincides with the one given in [4, Sect. 5.1.1].

One may easily check that the closed embedding $j : u(V) \hookrightarrow V$ induced by $B \twoheadrightarrow B/\ker(u^*)$ is an image in the category of (affine) schemes over K. This means that if $\alpha, \beta : W \to S$ are two morphisms of schemes over K such that their *restrictions* to $u(V)$ do coincide, i.e., $\alpha j = \beta j$ (as morphisms from $u(V)$ to S) then $\alpha u = \beta u$ (as morphisms from U to S). It follows that j is also an image in the category of finite commutative group schemes. group [21, Sect. 10].

Theorem 1.2 (Theorem of Gabriel [18,5]). *The category of finite commutative group schemes over a field is abelian.*

Remark 1.3. Let V be a finite commutative group scheme over K and let W be its finite closed group subscheme. If $V \to U$ is a *surjective* morphism of finite commutative group schemes over K then [5]

$$\#(V) = \#(W) \cdot \#(U).$$

Recall that $\Gamma(W, \mathcal{O}_W)$ is the quotient of $\Gamma(V, \mathcal{O}_V)$. In particular, if the orders of V and W do coincide then $V = W$.

1.4. Abelian varieties over fields. We refer the reader to the books of Mumford [16], Shimura [26] for basic properties of abelian varieties (see also Lang's book [8] and papers of Waterhouse [30], Deligne [2], Milne [13] and Oort [20]). If X is an abelian variety over K then we write $\mathrm{End}(X)$ for the ring of all K-endomorphisms of X. If m is an integer then write m_X for the multiplication by m in X; in particular, 1_X is the identity map. (Sometimes we will use notation m instead of m_X.)

If Y is an abelian variety over K then we write $\mathrm{Hom}(X, Y)$ for the group of all K-endomorphisms $X \to Y$.

Remark 1.5. Warning: sometimes in the literature, including my own papers, the notation $\mathrm{End}(X)$ is used for the ring of $\bar{K}$-endomorphisms.

It is well known [16, Sect. 19, Theorem 3] that $\mathrm{Hom}(X, Y)$ is a free commutative group of finite rank. We write X^t for the dual of X (See [13, Sect. 9–10] for the definition and basic properties of the dual of an abelian variety.) In particular, X^t is also an abelian variety over K that is isogenous to X (over K). If $u \in \mathrm{Hom}(X, Y)$ then we write u^t for its dual in $\mathrm{Hom}(Y, X)$. We have

$$\bar{X}^t = \overline{X^t}.$$

If n is a positive integer then we write X_n for the kernel of n_X; it is a finite commutative (sub)group scheme (of X) over K of rank $2\dim(X)$. By definition, $X_n(\bar{K})$ is the kernel of multiplication by n in $X(\bar{K})$.

If n is not divisible by $\mathrm{char}(K)$ then X_n is an étale group scheme and it is well-known [16, Sect. 4] that $X_n(\bar{K})$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(X)$ and all $\bar{K}$-points of X_n are defined over a finite separable extension of K. In particular, $X_n(\bar{K})$ carries a natural structure of Galois module.

1.6. Isogenies. Let $W \subset X$ be a finite group subscheme over K. It follows from the analogue of Lagrange theorem that $W \subset X_d$ for $d = \#(W)$. The quotient $Y := X/W$ is an abelian variety over K and the canonical isogeny $\pi : X \to X/W = Y$

has kernel W and degree $\#(W)$ ([16, Sect. 12, Corollary 1 to Theorem 1], [3, Sect. 2, pp. 307-314]). In particular, every homomorphism of abelian varieties $u: X \to Z$ over K with $W \subset \ker(u)$ factors through π, i.e., there exists a unique homomorphism of abelian varieties $v: Y \to Z$ over K such that

$$u = v\pi.$$

If m is a positive integer then

$$\pi m_X = m_Y \pi \in \mathrm{Hom}(X, Y).$$

Let us put

$$m^{-1}W := \ker(\pi m_X) = \ker(m_Y \pi) \subset X.$$

For every commutative K-algebra R the group of R-points $m^{-1}W(R)$ is the set of all $x \in X(R)$ with

$$mx \in W(R) \subset X(R).$$

For example, if $W = X_n$ then

$$Y = X, \pi = n_X, m^{-1}X_n = X_{nm}.$$

In general, if $W \subset X_n$ then $m^{-1}W$ is a closed group subscheme in X_nm. E.g., W is always a closed group subscheme of X_{dm} and therefore is a finite group subscheme of X over K. The order

$$\#(m^{-1}W) = \deg(\pi m_X) = \deg(\pi)\deg(m_X) = \#(W) \cdot m^{2\dim(X)}.$$

We have

$$X_m \subset m^{-1}W, \ m_X(m^{-1}W) \subset W$$

and the kernel of $m_X : m^{-1}W \to W$ coincides with X_m.

Lemma 1.7. *The image* $m_X(m^{-1}W) = W$.

Proof. Let us denote the image by G. By Remark 1.3, $\#(G)$ is the ratio

$$\#(m^{-1}W)/\#(X_m) = \dim(W),$$

i.e., the orders of G and W do coincide. Since $G \subset W$, we have (by the same Remark) $G = W$. □

Example 1.8. If $W = X_n$ then $m^{-1}X_n = X_{nm}$ and therefore $m(X_{nm}) = X_n$.

Lemma 1.9. *If r is a positive integer then $r(X_n) = X_{n_1}$ where $n_1 = n/(n, r)$.*

Proof. We have $r = (n,r) \cdot r_1$ where r_1 is a positive integer such that n_1 and r_1 are relatively prime. This implies that $r_1(X_{n_1}) = X_{n_1}$. By Lemma 1.9, $(n,r)(X_n) = X_{n_1}$. This implies that

$$r(X_n) = r_1(n,r)(X_n) = r_1((n,r)(X_n)) = r_1(X_{n_1}) = X_{n_1}.$$

□

Lemma 1.10. *Let X and Y be abelian varieties over a field K. Let $u : X \to Y$ be a K-homomorphism of abelian varieties. Let $n > 1$ be an integer and $u_n : X_n \to Y_n$ the morphism of commutative group schemes over K induced by u.*

- *(i) Suppose that u is an isogeny and $\deg(u)$ and n are relatively prime. Then $u_n : X_n \to Y_n$ is an isomorphism.*
- *(ii) Suppose that $u_n : X_n \to Y_n$ is an isomorphism. Then u is an isogeny and $\deg(u)$ and n are relatively prime.*

Proof. Let u be an isogeny such that $m := \deg(u)$ and n are relatively prime. Then $\ker(u) \subset X_m$. It follows that there exists a K-isogeny $v : Y \to X$ such that

$$vu = m_X, uv = m_Y.$$

(i). Since multiplication by m is an automorphism of both X_n and Y_m, we conclude that $u_n : X_n \to Y_n$ and $v_n : Y_n \to X_n$ are isomorphisms.

(ii). Suppose that u_n is an isomorphism. This implies that the orders of X_n and Y_n coincide and therefore $\dim(X) = \dim(Y)$. We need to prove that u is isogeny and $\deg(u)$ and n are relatively prime. In order to do that, we may assume that K is algebraically closed (replacing K, X, Y, u by $\bar{K}, \bar{X}, \bar{Y}, \bar{u}$ respectively). Let us put $Z := u(Y) \subset X$: clearly, Z is a (closed) abelian subvariety of Y and therefore $\dim(Z) \le \dim(Y)$. It is also clear that $u : X \to Y$ coincides with the composition of the natural surjection $X \to u(X) = Z$ and the inclusion map $j : Z \hookrightarrow X$. This implies that $u_n(X_n)$ is a (closed) group subscheme of $j_n(Z_n) \subset Y_n$. It follows that

$$\#(u_n(X_n)) \le \#(j_n(Z_n)) \le \#(Z_n) = n^{2\dim(Z)}.$$

Since u_n is an isomorphism, $u_n(X_n) = Y_n$ and therefore

$$\#(u_n(X_n)) = \#(Y_n) = n^{2\dim(Y)}.$$

It follows that

$$n^{2\dim(Y)} \le n^{2\dim(Z)}$$

and therefore $\dim(Y) \le \dim(Z)$. (Here we use that $n > 1$.) Since Z is a closed subvariety in Y, we conclude that $\dim(Z) = \dim(Y)$ and $Y = Z$. In other words, u is surjective. Taking into account that $\dim(X) = \dim(Y)$, we conclude that u ia an isogeny.

Now let $m = dr$ where d is the largest common divisor of n and m. Then r and n are relatively prime; in particular, multiplication by r is an automorphism of X_n. Let us denote $\ker(u)$ by W: it is a finite commutative group scheme over K of order m and therefore

$$W \subset X_m.$$

This implies that for every commutative K-algebra R we have

$$m \cdot W(R) = \{0\}.$$

On the other hand, since u_n is an isomorphism, the kernel of $W(R) \xrightarrow{n} W(R)$ is $\{0\}$. Since $d \mid n$, the kernel of $W(R) \xrightarrow{d} W(R)$ is also $\{0\}$. This implies that $r \cdot W(R) = \{0\}$ for all R. Hence $W \subset X_r$. It follows that $\deg(u) = \#(W)$ divides $\#(X_r) = r^{2\dim(X)}$ and therefore is coprime to n. □

The next statement will be used only in Section 12.

Proposition 1.11. *Let X and Y be abelian varieties over a field K. Suppose that for every prime ℓ there exists an isogeny $X \to Y$, whose degree is not divisible by ℓ. Then for every positive integer n there exists an isogeny $X \to Y$, whose degree is coprime to n. In particular, $X_n \cong Y_n$.*

Proof. Recall that the additive group $\mathrm{Hom}(X, Y)$ is isomorphic to $\mathbb{Z}^\rho$ for some nonnegative integer ρ. In our case, X and Y are isogenous over K and therefore $\rho > 0$.

Let n be a positive integer and let $P(n)$ be the (finite) set of its prime divisors. For each $\ell \in P(n)$ pick an isogeny $v^{(\ell)} : X \to Y$, whose degree is not divisible by ℓ. By Lemma 1.10(i), $v^{(\ell)}$ induces an isomorphism $X_\ell \cong Y_\ell$. Now, by the Chinese Remainder Theorem, there exists $u \in \mathrm{Hom}(X, Y) \cong \mathbb{Z}^\rho$ such that

$$u - v^{(\ell)} \in \ell \cdot \mathrm{Hom}(X, Y) \ \forall\ \ell \in P.$$

This implies that for each $\ell \in P$ the homomorphisms u and $v^{(\ell)}$ induce the same morphism $X_\ell \cong Y_\ell$, which, as we know, is an isomorphism. It follows from Lemma By Lemma 1.10(ii) that u is an isogeny, whose degree is not divisible by ℓ. Hence $\deg(u)$ and n are coprime. Applying again Lemma 1.10(i), we conclude that u induces an isomorphism $X_n \cong Y_n$. □

1.12. Polarizations. A homomorphism $\lambda : X \to X^t$ is a *polarization* if there exists an ample invertible sheaf $\mathcal{L}$ on $\bar{X}$ such that $\bar{\lambda}$ coincides with

$$\Lambda_{\mathcal{L}} : \bar{X}^t \to \bar{X}^t,\ z \mapsto \mathrm{cl}(T_z^* L \otimes L^{-1})$$

where $T_z : \bar{X} \to \bar{X}$ is the translation map

$$x \mapsto x + z$$

and cl stands for the isomorphism class of an invertible sheaf. Recall [16, Sect, 6, Proposition 1; Sect. 8, Theorem 1; Sect. 13, Corollary 5] that a polarization is an *isogeny.* If λ is an isomorphism, i.e., $\deg(\lambda)=1$, we call λ a *principal polarization* and the pair (X,λ) is called a principally polarized abelian variety (over K).

If $n:=\deg(\lambda)=\#(\ker(\lambda))$ then $\ker(\lambda)$ is killed by multiplication by n, i.e., $\ker(\lambda)\subset X_n$. For every positive integer m we write λ^n for the polarization

$$X^m\to (X^m)^t=(X^t)^m,\ (x_1,\dots,x_m)\mapsto(\lambda(x_1),\dots,\lambda(x_m))$$

that corresponds to the ample invertible sheaf $\otimes_{i=1}^m \mathrm{pr}_i^*\mathcal{L}$ where $\mathrm{pr}_i: X^m\to X$ is the ith projection map. We have

$$\dim(X^m)=m\cdot\dim(X),\ \deg(\lambda^m)=\deg(\lambda)^m$$

and $\ker(\lambda^m)=\ker(\lambda)^m\subset (X^m)_n$ if $\ker(\lambda)\subset X_n$.

There exists a *Riemann form* - a skew-symmetric pairing of group schemes over $\bar{K}$ [16, Sect. 23]

$$e_\lambda:\ker(\bar{\lambda})\times\ker(\bar{\lambda})\to\mathbf{G}_{\mathrm{m}}$$

where $\mathbf{G}_{\mathrm{m}}$ is the multiplicative group scheme over $\bar{K}$.

If

$$e_{\lambda^m}:\ker(\bar{\lambda}^m)\times\ker(\bar{\lambda}^m)\to\mathbf{G}_{\mathrm{m}}$$

is the Riemann form for λ^m then in obvious notation

$$e_{\lambda^m}(x,y)=\prod_{i=1}^m e_\lambda(x_i,y_i)$$

where

$$x=(x_1,\dots,x_m),\ y=(y_1,\dots,y_m)\in\ker(\bar{\lambda})^m=\ker(\bar{\lambda}^m).$$

We have

$$\mathrm{Mat}_m(\mathbb{Z})\subset\mathrm{Mat}_m(\mathrm{End}(\bar{X}))=\mathrm{End}(X^m).$$

One may easily check that every $u\in\mathrm{Mat}_m(\mathbb{Z})$ leaves the group subscheme $\ker(\bar{\lambda}^m)$ invariant and

$$e_{\lambda^m}(ux,y)=e_{\lambda^m}(x,u^*y)$$

where u^* is the transpose of the matrix u. Notice that u^* viewed as an element of

$$\mathrm{Mat}_m(\mathbb{Z})\subset\mathrm{Mat}_m(\mathrm{End}(X^t))=\mathrm{End}((X^t)^m)$$

coincides with $u^t\in\mathrm{End}((X^m)^t)$.

1.13. Polarizations and isogenies. Let $W \subset \ker(\lambda)$ be a finite group subscheme over K. Recall that $Y := X/W$ is an abelian variety over K and the canonical isogeny $\pi : X \to X/W = Y$ has kernel W and degree $\#(W)$.

Suppose that $\bar{W}$ is isotropic with respect to e_λ, i.e., the restriction of e_λ to $\bar{W} \times \bar{W}$ is trivial. Then there exists an ample invertible sheaf $\mathcal{M}$ on $\bar{Y}$ such that $\mathcal{L} \cong \bar{\pi}^* \bar{\mathcal{M}}$ [16, Sect. 23, Corollary to Theorem 2, p. 231] and the $\bar{K}$-polarization $\Lambda_{\bar{\mathcal{M}}} : \bar{Y} \to \bar{Y}^t$ satisfies

$$\bar{\lambda} = \overline{\pi^t} \Lambda_{\bar{\mathcal{M}}} \bar{\pi}.$$

Since $\bar{\pi^t}$ and $\bar{\pi}$ are isogenies that are defined over K, the polarization $\Lambda_{\bar{\mathcal{M}}}$ is also defined over K, i.e., there exists a K-isogeny $\mu : Y \to Y^t$ such that $\Lambda_{\bar{\mathcal{M}}} = \bar{\mu}$ and

$$\lambda = \pi^t \mu \pi.$$

It follows that

$$\deg(\lambda) = \deg(\pi) \deg(\mu) \deg(\pi^t) = \deg(\pi)^2 \deg(\mu) = (\#(W))^2 \deg(\mu).$$

Therefore μ is a principal polarization (i.e., $\deg(\mu) = 1$) if and only if

$$\deg(\lambda) = (\#(W))^2.$$

2. ℓ-divisible groups, abelian varieties and Tate modules

Let h be a non-negative integer and ℓ a prime. The following notion was introduced by Tate [28,25].

Definition 2.1. An ℓ-divisible group G over K of height h is a sequence $\{G_\nu, i_\nu\}_{\nu=1}^\infty$ in which:

- G_ν is a finite commutative group scheme over K of order $\ell^{h\nu}$.
- i_ν is a closed embedding $G_\nu \hookrightarrow G_{\nu+1}$ that is a morphism of group schemes. In addition, $i_\nu(G_\nu)$ is the kernel of multiplication by ℓ^ν in $G_{\nu+1}$.

Example 2.2. Let X be an abelian variety over K of dimension d. Then it is known [28,25] that the sequence $\{X_{\ell^\nu}\}_{\nu=1}^\infty$ is an ℓ-divisible group over K of height $2d$. Here i_ν is the *inclusion map* $X_{\ell^\nu} \hookrightarrow X_{\ell^{\nu+1}}$. We denote this ℓ-divisible group by $X(\ell)$.

2.3. Homomorphisms of ℓ-divisible groups and abelian varieties. If $H = \{H_\nu, j_\nu\}_{\nu=1}^\infty$ is an ℓ-divisible group over K then a morphism $u : G \to H$ is a sequence $\{u_{(\nu)}\}_{\nu=1}^\infty$ of morphisms of group schemes over K

$$u_{(\nu)} : G_\nu \to H_\nu$$

such that the composition

$$u_{(\nu+1)}i_\nu : G_\nu \hookrightarrow G_{\nu+1} \to H_{\nu+1}$$

coincides with

$$j_\nu u_{(\nu)} : G_\nu \to H_\nu \hookrightarrow H_{\nu+1},$$

i.e., the diagram

$$\begin{array}{ccc} G_\nu & \xrightarrow{u_{(\nu)}} & H_\nu \\ {\scriptstyle i_\nu}\downarrow & & \downarrow{\scriptstyle j_\nu} \\ G_{\nu+1} & \xrightarrow{u_{(\nu+1)}} & H_{\nu+1} \end{array}$$

is commutative.

Remark 2.4. A morphism u is an isomorphism of ℓ-divisible groups if and only if all $u_{(\nu)}$ are isomorphisms of the corresponding finite group schemes.

The group $\mathrm{Hom}(G, H)$ of morphisms from G to H carries a natural structure of $\mathbb{Z}_\ell$-module induced by the natural structures of $\mathbb{Z}/\ell^v = \mathbb{Z}_\ell/\ell^\nu$-module on $\mathrm{Hom}(G_\nu, H_\nu)$. Namely, if $u = \{u_{(\nu)}\}_{\nu=1}^{\infty} \in \mathrm{Hom}(G, H)$ and $a \in \mathbb{Z}_\ell$ then $au = \{(au)_{(\nu)}\}_{\nu=1}^{\infty}$ may be defined as follows. For each ν pick $a_\nu \in \mathbb{Z}$ with $a - a_\nu \in \ell^\nu \mathbb{Z}_\ell$ and put

$$(au)_{(\nu)} := a_\nu u_{(\nu)} : G_\nu \to H_\nu.$$

Since multiplication by ℓ^ν kills G_ν, the definition of $(au)_{(\nu)}$ does not depend on the choice of a_ν.

Let X and Y be abelian varieties over K. There is a natural homomorphism of commutative groups $\mathrm{Hom}(X, Y) \to \mathrm{Hom}(X(\ell), Y(\ell))$. Namely, if $u \in \mathrm{Hom}(X, Y)$ then $u(X_{\ell^\nu})$ lies in the kernel of multiplication by ℓ^ν, i.e. $u(X_{\ell^\nu}) \subset Y_{\ell^\nu}$. In fact, we get the natural homomorphism

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}/\ell^\nu \to \mathrm{Hom}(X_{\ell^\nu}, Y_{\ell^\nu}),$$

which is known to be an embedding. (See also Lemma 9.1 below.)

Since $\mathrm{Hom}(X(\ell), Y(\ell))$ is a Z_ℓ-module, we get the natural homomorphism of $\mathbb{Z}_\ell$-modules

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(X(\ell), Y(\ell)).$$

Explicitly, if $u \in \mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell$ then for each ν we may pick

$$w(\nu) \in \mathrm{Hom}(X, Y) = \mathrm{Hom}(X, Y) \otimes 1 \subset \mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell$$

such that

$$u - w(\nu) \in \ell^\nu \cdot \{\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell\} = \{\ell^\nu \cdot \mathrm{Hom}(X,Y)\} \otimes \mathbb{Z}_\ell = \mathrm{Hom}(X,Y) \otimes \ell^\nu \mathbb{Z}_\ell.$$

Then the corresponding morphism of group schemes $u_{(\nu)} := w(\nu) : X_{\ell^\nu} \to Y$ does not depend on the choice of $w(\nu)$ and defines the corresponding morphism of ℓ-divisible groups

$$u_{(\nu)} : X_{\ell^\nu} \to Y_{\ell^\nu};\ \nu = 1, 2, \dots .$$

Remark 2.5. Since $\mathrm{Hom}(X,Y)$ is a free commutative group of finite rank, the $\mathbb{Z}_\ell$-module $\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell$ is a free module of finite rank.

The following assertion seems to be well known (at least, when $\ell \neq \mathrm{char}(K)$).

Lemma 2.6. *The natural homomorphism of $\mathbb{Z}_\ell$-modules*

$$\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(X(\ell), Y(\ell))$$

is injective.

Proof. If it is not injective and u lies in the kernel then $u_{(\nu)} \in \ell^\nu \cdot \mathrm{Hom}(X,Y)$ for all ν. Since $u - u_{(\nu)} \in \ell^\nu \cdot \{\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell\}$, we conclude that $u \in \ell^\nu \cdot \{\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell\}$ for all ν. Since $\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell$ is a free $\mathbb{Z}_\ell$-module of finite rank, it follows that $u = 0$. □

Corollary 2.7. *The following conditions are equivalent:*

- *(i) There exists an isogeny $u : X \to Y$, whose degree is not divisible by ℓ.*
- *(ii) There exists $w \in \mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell$ that induces an isomorphism of ℓ-divisible groups $X(\ell) \to Y(\ell)$.*

Proof. Let $u : X \to Y$ be an isogeny, whose degree is not divisible by ℓ. Applying Lemma 1.10(i) to all $n = \ell^\nu$, we conclude that u induces an isomorphism $X(\ell) \cong Y(\ell)$.

Now suppose that $w \in \mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell$ that induces an isomorphism of ℓ-divisible groups $X(\ell) \to Y(\ell)$. In particular, w induces an isomorphism of finite group schemes $w_{(1)} : X_\ell \cong Y_\ell$. On the other hand, there exists $u \in \mathrm{Hom}(X,Y)$ such that

$$w - u \in \ell \cdot \{\mathrm{Hom}(X,Y) \otimes \mathbb{Z}_\ell\} = \mathrm{Hom}(X,Y) \otimes \ell\mathbb{Z}_\ell.$$

This implies that u and w induce the same morphism of finite group schemes $X_\ell \to Y_\ell$. It follows that the morphism

$$u_\ell = u_{(1)} : X_\ell \to Y_\ell$$

induced by u coincides with $w_{(1)}$ and therefore is an isomorphism. Now Lemma 1.10(ii) implies that u is an isogeny, whose degree is not divisible by ℓ. □

2.8. Tate modules. In this subsection we assume that ℓ is a prime different from $\mathrm{char}(K)$. If $n = \ell^\nu$ then X_n is an étale finite group scheme of order $n^{2\dim(X)}$ and we will identify its with the Galois module of its $\bar{K}$-points. (Actually, all points of X_n are defined over a separable algebraic extension of K). The Tate ℓ-module $T_\ell(X)$ is defined as the projective limit of Galois modules X_{ℓ^ν} where the transition map $X_{\ell^{\nu+1}} \to X_{\ell^\nu}$ is multiplication by ℓ. The Tate module carries a natural structure of free $\mathbb{Z}_\ell$-module of rank $2\dim(X)$; it is also provided with a natural structure of Galois module in such a way that natural homomorphisms $T_\ell(X) \to X_{\ell^\nu}$ induce isomorphisms of Galois modules

$$T_\ell(X) \otimes \mathbb{Z}/\ell^\nu \cong X_{\ell^\nu}.$$

Explicitly, $T_\ell(X)$ is the set of all collections $x = \{x_\nu\}_{\nu=1}^\infty$ with

$$x_\nu \in X_{\ell^\nu}, \quad x_{\nu+1} = \ell x_\nu \ \forall \nu.$$

The map $x \mapsto x_\nu$ defines the surjective homomorphism of Galois modules $T_\ell(X) \to X_{\ell^\nu}$, whose kernel coincides with $\ell^\nu \cdot T_\ell(X)$ and therefore induces the isomorphism of Galois modules $T_\ell(X)/\ell^\nu \cong X_{\ell^\nu}$ mentioned above.

If Y is an abelian variety over K then we write $\mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y))$ for the $\mathbb{Z}_\ell$-module of all homomorphisms of $\mathbb{Z}_\ell$-modules $T_\ell(X) \to T_\ell(Y)$ that commute with the Galois action(s), i.e., are also homomorphisms of Galois modules.

The $\mathbb{Z}_\ell$-module $\mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y))$ is the set of collections $w = \{w_\nu\}_{\nu=1}^\infty$ of homomorphisms of Galois modules

$$w_\nu : T_\ell(X)/\ell^\nu = X_{\ell^\nu} \to Y_{\ell^\nu} = T_\ell(Y)/\ell^\nu$$

such that

$$w_\nu(x_\nu) = \ell \cdot u w_{\nu+1}(x_{\nu+1}) \quad \forall x = \{x_\nu\}_{\nu=1}^\infty \in T_\ell(X).$$

Now if $z \in X_{\ell^\nu}$ then there exists $x \in T_\ell(X)$ with $x_\nu = z$. We have $\ell x_{\nu+1} = x_\nu = z$ and

$$w_\nu(z) = w_\nu(x_\nu) = \ell \cdot w_{\nu+1}(x_{\nu+1}) = w_{\nu+1}(\ell x_{\nu+1}) = w_{\nu+1}(x_\nu) = w_{\nu+1}(z),$$

i.e., the restriction of $w_{\nu+1}$ to X_{ℓ^ν} coincides with w_ν. This means that the collection $\{w_\nu\}_{\nu=1}^\infty$ defines a morphism of ℓ-divisible groups over K

$$X(\ell) \to Y(\ell).$$

Conversely, if $u = \{u_{(\nu)}\}_{\nu=1}^\infty$ is a morphism $X(\ell) \to Y(\ell)$ over K then

$$u_{(\nu)} : X_{\ell^\nu} \to Y_{\ell^\nu}$$

is a homomorphism of Galois modules; in addition, the restriction of $u_{(\nu+1)}$ to X_{ℓ^ν} coincides with $u_{(\nu)}$. This implies that for each $\{x_\nu\}_{\nu=1}^\infty \in T_\ell(X)$

$$u_{(\nu)}(x_\nu) = u_{(\nu+1)}(x_\nu) = u_{(\nu+1)}(\ell x_{\nu+1}) = \ell u_{(\nu+1)}(x_{\nu+1})$$

for all ν. This means that the collection $\{u_{(\nu)}\}_{\nu=1}^{\infty}$ defines a homomorphism of Galois modules $T_\ell(X) \to T_\ell(Y)$. Those observations give us the natural isomorphism of $\mathbb{Z}_\ell$-modules

$$\mathrm{Hom}(X(\ell), Y(\ell)) = \mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y)).$$

3. Useful results

Theorem 3.1 ([32,34,14]). *Let X be an abelian variety of positive dimension over a field K and X^t its dual. Then $(X \times X^t)^4$ admits a principal K-polarization.*

We prove Theorem 3.1 in Section 7.

Theorem 3.2 ([11]). *Let X be an abelian variety over K. The set of abelian K-subvarieties of X is finite, up to the action of the group $\mathrm{Aut}(X)$ of K-automorphisms of X.*

We sketch the proof of Theorem 3.2 in Section 5.

Lemma 3.3 (Tate ([27], Sect. 2, p. 136)). *Let K be a finite field, and let g and d be positive integers. The set of K-isomorphism classes of g-dimensional abelian varieties over K that admit a K-polarization of degree d is finite.*

Lemma 3.3 will be proven in Section 6.

Theorem 3.4 ([32], Th. 4.1). *Let K be a finite field, g a positive integer. Then the set of K-isomorphism classes of g-dimensional abelian varieties over K is finite.*

Proof of Theorem 3.4 (modulo Theorem 3.1 and Lemma 3.3). Suppose that X is a g-dimensional abelian variety over K. By Lemma 3.3, the set of $4g$-dimensional abelian varieties over K of the form $(X \times X^t)^4$ is finite, up to K-isomorphism. The abelian variety X is isomorphic over K to an abelian subvariety of $(X \times X^t)^4$. In order to finish the proof, one has only to recall that thanks to Theorem 3.2, the set of abelian subvarieties of a given abelian variety is finite, up to a K-isomorphism. □

We need Theorem 1.2 in order to state the following assertion.

Corollary 3.5 (Corollary to Theorem 3.4). *Let X be an abelian variety of positive dimension over a finite field K. There exists a positive integer $r = r(X, K)$ that enjoys the following properties:*

(i) If Y is an abelian variety over K that is K-isogenous to X then there exists a K-isogeny $\beta : X \to Y$ such that $\ker(\beta) \subset X_r$.
(ii) If n is a positive integer and $W \subset X_n$ is a group subscheme over K then there exists an endomorphism $u \in \mathrm{End}(X)$ such that

$$rW \subset uX_n \subset W.$$

Remark 3.6. The assertion 3.5(i) follows readily from Theorem 3.4.

We prove Corollary 3.5(ii) in Section 8.

4. Main results

Theorem 4.1. *Let X be an abelian variety of positive dimension over a finite field K. There exists a positive integer $r_1 = r_1(X, K)$ that enjoys the following properties:*

Let n be a positive integer and $u_n \in \operatorname{End}(X_n)$. Let us put $m = n/(n, r_1)$. Then there exists $u \in \operatorname{End}(X)$ such that the images of u and u_n in $\operatorname{End}(X_m)$ do coincide.

We prove Theorem 4.1 in Section 10.

Applying Theorem 4.1 to a product $X = A \times B$ of abelian varieties A and B, we obtain the following statement.

Theorem 4.2. *Let A, B be abelian varieties of positive dimension over a finite field K. There exists a positive integer $r_2 = r_2(A, B)$ that enjoys the following properties:*

Suppose that n is a positive integer and $u_n : A_n \to B_n$ is a morphism of group schemes over K. Let us put $m = n/(n, r_2)$. Then there exists a homomorphism $u : A \to B$ of abelian varieties over K such that the images of u and u_n in $\operatorname{Hom}(A_m, B_m)$ do coincide.

The following assertions follow readily from Theorem 4.2.

Corollary 4.3 (First Corollary to Theorem 4.2)**.** *If n and r_2 are relatively prime (e.g., n is a prime that does not divide r_2) then the natural injection*

$$\operatorname{Hom}(A, B) \otimes \mathbb{Z}/n \hookrightarrow \operatorname{Hom}(A_n, B_n)$$

is bijective.

Corollary 4.4 (Second Corollary to Theorem 4.2)**.** *Let ℓ be a prime and $\ell^{r(\ell)}$ is the exact power of ℓ dividing r_2. Then for each positive integer i the image of*

$$\operatorname{Hom}(A_{\ell^{i+r(\ell)}}, B_{\ell^{i+r(\ell)}}) \to \operatorname{Hom}(A_{\ell^i}, B_{\ell^i})$$

coincides with the image of

$$\operatorname{Hom}(A, B) \otimes \mathbb{Z}/\ell^i \hookrightarrow \operatorname{Hom}(A_{\ell^i}, B_{\ell^i}).$$

5. Abelian subvarieties

We follow the exposition in [11].

The next statement is a corollary of a finiteness result of Borel and Harish-Chandra [1, Theorem 6.9]; it may also be deduced from the Jordan–Zassenhaus theorem [23, Theorem 26.4].

Proposition 5.1 ([11], p. 514). *Let F be a finite-dimensional semisimple $\mathbb{Q}$-algebra, M a finitely generated right F-module, L a $\mathbb{Z}$-lattice in M. Let G be the group of those automorphisms σ of the F-module M for which $\sigma(L) = L$. Then the number of G-orbits of the set of F-submodules of M is finite.*

Now let X be an abelian variety over K. We are going to apply Proposition 5.1 to

$$F = \mathrm{End}(X) \otimes \mathbb{Q}, \ M = \mathrm{End}(X) \otimes \mathbb{Q}, \ L = \mathrm{End}(X).$$

One may identify G with the group $\mathrm{Aut}(X) = \mathrm{End}(X)^*$ of automorphisms of X: here elements of $\mathrm{End}(X)^*$ act as left multiplications on $\mathrm{End}(X) \otimes \mathbb{Q} = M$.

On the other hand, to each abelian K-subvariety $Y \subset X$ corresponds the right ideal

$$I(Y) = \{u \in \mathrm{End}(X) \mid u(X) \subset Y\}$$

and the F-submodule

$$I(Y)_{\mathbb{Q}} = I(Y) \otimes \mathbb{Q} \subset \mathrm{End}(X) \otimes \mathbb{Q} = M.$$

Using the theorem of Poincaré–Weil [13, Proposition 12.1], one may prove ([11, p. 515] that $I(Y)_{\mathbb{Q}}$ uniquely determines Y. Even better, if Y' is an abelian K-subvariety of X and

$$uI(Y)_{\mathbb{Q}} = I(Y')_{\mathbb{Q}}$$

for $u \in \mathrm{Aut}(X) = \mathrm{End}(X)^*$ then $Y' = u(Y)$. Now Proposition 5.1 implies the finiteness of the number of orbits of the set of abelian K-subvarieties of X under the natural action of $\mathrm{Aut}(X)$. This proves Theorem 3.2. (See [10] for variants and complements.)

6. Polarized abelian varieties

Lemma 6.1 (Mumford's lemma [15]). *Let X be an abelian variety of positive dimension over a field K. If $\lambda : X \to X^t$ is a polarization then there exists an ample invertible sheaf $\mathcal{L}$ on X such that*

$$\Lambda_{\bar{\mathcal{L}}} = 2\bar{\lambda}$$

where $\bar{\mathcal{L}}$ is the invertible sheaf on $\bar{X}$ induced by $\mathcal{L}$.

Proof. See [15, Ch. 6, Sect. 2, pp. 120–121] where a much more general case of abelian schemes is considered. (In notation of [15], S is the spectrum of K.) Let me just recall an explicit construction of $\mathcal{L}$. Let $\mathbb{P}$ be the universal Poincaré invertible sheaf on $X \times X^t$ [13, Sect. 9]. Then $\mathcal{L} := (1_X, \lambda)^*\mathbb{P}$ where $(1_X, \lambda) : X \to X \times X^t$ is defined by the formula

$$x \mapsto (x, \lambda(x)).$$

□

Proof of Lemma 3.3. So, let X be a g-dimensional abelian variety over a finite field K and let $\lambda : X \to X^t$ be a polarization of degree d. We follow the exposition in [22, p. 243]. By Lemma 6.1, there exists an invertible ample sheaf $\mathcal{L}$ on X such that the self-intersection index of $\bar{\mathcal{L}}$ equals $2^g dg!$ [16, Sect. 16]. The invertible sheaf $\bar{\mathcal{L}}^3$ is very ample, its space of global section has dimension $6^g d$; the self-intersection index of $\mathcal{L}$ equals $6^g dg!$ [16, Sect. 16]. This implies that $\mathcal{L}^3$ is also very ample and gives us an embedding (over K) of X into the $6^g d-1$-dimensional projective space as a closed K-subvariety of degree $6^g dg!$. All those subvarieties are uniquely determined by their Chow forms ([29, Ch. 1, Sect. 6.5], [6, Lecture 21, pp. 268–273]), whose coefficients are elements of K. Since K is finite and the number of coefficients depends only on the degree and dimension, we get the desired finiteness result. □

7. Quaternion trick

Let X be an abelian variety of positive dimension over a field K and $\lambda : X \to X^t$ a K-polarization. Pick a positive integer n such that

$$\ker(\lambda) \subset X_n.$$

Lemma 7.1. *Suppose that there exists an integer a such that a^2+1 is divisible by n. Then $X \times X^t$ admits a principal polarization that is defined over K.*

Proof. Let

$$V \subset \ker(\lambda) \times \ker(\lambda) \subset X_n \times X_n \subset X \times X$$

be the graph of multiplication by a in $\ker(\lambda)$. Clearly, V is a finite group subscheme over K that is isomorphic to $\ker(\lambda)$ and therefore its order is equal to $\deg(\lambda)$. Notice that $\deg(\lambda)$ is the square root of $\deg(\lambda^2)$.

For each commutative $\bar{K}$-algebra R the group $\bar{V}(R)$ of R-points coincides with the set of all the pairs (x, ax) with $x \in \ker(\bar{\lambda}) \subset \bar{X}_n$. This implies that for all $(x, ax), (y, ay) \in \bar{V}(R)$ we have

$$e_{\lambda^2}((x, ax), (y, ay)) = e_\lambda(x, y) \cdot e_\lambda(ax, ay) = e_\lambda(x, y) \cdot e_\lambda(a^2 x, y) =$$

$$e_\lambda(x, y) \cdot e_\lambda(-x, y) = e_\lambda(x, y)/e_\lambda(x, y) = 1.$$

In other words, $\bar{V}$ is isotropic with respect to e_{λ^2}; in addition,

$$\#(\bar{V})^2 = \deg(\lambda)^2 = \deg(\lambda^2).$$

This implies that X^2/V is a principally polarized abelian variety over K. On the other hand, we have an isomorphism of abelian varieties over K

$$f : X \times X \to X \times X = X^2,\ (x, y) \mapsto (x, ax) + (0, y) = (x, ax + y)$$

and

$$V = f(\ker \lambda \times \{0\}) \subset f(X \times \{0\}).$$

Thus, we obtain K-isomorphisms

$$X^2/V \cong X/\ker(\lambda) \times X = X^t \times X = X \times X^t.$$

In particular, $X \times X^t$ admits a principal K-polarization and we are done. □

Proof of Theorem 3.1. Choose a quadruple of integers a, b, c, d such that

$$0 \neq s := a^2 + b^2 + c^2 + d^2$$

is congruent to -1 modulo n. We denote by $\mathcal{I}$ the "quaternion"

$$\mathcal{I} = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix} \in \mathrm{Mat}_4(\mathbb{Z}) \subset \mathrm{Mat}_4(\mathrm{End}(X) = \mathrm{End}(X*^4)).$$

We have

$$\mathcal{I}^*\mathcal{I} = a^2 + b^2 + c^2 + d^2 = s \in \mathbb{Z} \subset \mathrm{Mat}_4(\mathbb{Z}) \subset \mathrm{Mat}_4(\mathrm{End}(X) = \mathrm{End}(X^4).$$

Let

$$V \subset \ker(\lambda^4) \times \ker(\lambda^4) \subset (X^4)_n \times (X^4)_n \subset X^4 \times X^4 = X^8$$

be the graph of

$$\mathcal{I} : \ker(\lambda^4) \to \ker(\lambda^4).$$

Clearly, V is a finite group subscheme over K and its order is equal to $\deg(\lambda^4)$. Notice that $\deg(\lambda^4)$ is the square root of $\deg(\lambda^8)$.

For each commutative $\bar{K}$-algebra R the group $\bar{V}(R)$ of R-points consists of all the pairs $(x, \mathcal{I}x)$ with $x \in \ker(\bar{\lambda}^4) \subset (\bar{X^4})_n$. This implies that for all $(x, \mathcal{I}x), (y, \mathcal{I}y) \in \bar{V}(R)$ we have

$$e_{\lambda^4}((x, \mathcal{I}x), (y, \mathcal{I}y)) = e_{\lambda^4}(x, y) \cdot e_{\lambda^4}(\mathcal{I}x, \mathcal{I}y) = e_{\lambda^4}(x, y) \cdot e_{\lambda}(x, \mathcal{I}^t\mathcal{I}y) =$$

$$e_{\lambda}(x, y) \cdot e_{\lambda}(x, sy) = e_{\lambda}(x, y) \cdot e_{\lambda}(x, -y) = e_{\lambda}(x, y)/e_{\lambda}(x, y) = 1.$$

In other words, $\bar{V}$ is isotropic with respect to e_{λ^4}; in addition,

$$\#(\bar{V})^2 = \deg(\lambda^4)^2 = \deg(\lambda^8).$$

This implies that X^8/V is a principally polarized abelian variety over K. On the other hand, we have an isomorphism of abelian varieties over K

$$f : X^4 \times X^4 \to X^4 \times X^4 = X^8,\ (x,y) \mapsto (x, \mathcal{I}x) + (0,y) = (x, \mathcal{I}x + y)$$

and

$$V = f(\ker(\lambda^4) \times \{0\}) \subset f(X^4 \times \{0\}).$$

Thus, we obtain K-isomorphisms

$$X^4/V \cong X^4/\ker \lambda^4 \times X^4 = (X^4)^t \times X^4 = (X \times X^t)^4.$$

In particular, $(X \times X^t)^4$ admits a principal K-polarization and we are done. □

Remark 7.2. We followed the exposition in [32, Lemma 2.5], [34, Sect. 5]. See [14, Ch. IX, Sect. 1] where Deligne's proof is given.

8. Finite group subschemes of abelian varieties

Proof of Corollary 3.5(ii). Let r be as in 3.5(i). Let us consider the abelian variety $Y := X/W$ and the canonical K-isogeny $\pi : X \to X/W = Y$. Clearly,

$$W = \ker(\pi).$$

Since $W \subset X_n$, there exists a K-isogeny $v : Y \to X/X_n = X$ such that the composition $v\pi$ coincides with multiplication by n in X; in addition,

$$\pi n_X = n_Y \pi : X \to Y$$

is a K-isogeny, whose degree is $\#(W) \times n^{2\dim(X)}$. Here n_X (resp. n_Y) stands for multiplication by n in X (resp. in Y). Let us put

$$U = \ker(\pi n_X) = \ker(n_Y \pi) \subset X;$$

it is a finite commutative group K-(sub)scheme and

$$\#(U) = \#(W) \times n^{2\dim(X)}.$$

Then

$$X_n \subset U,\ W \subset U;\ \pi(U) \subset Y_n,\ n_X(U) \subset W.$$

The order arguments imply that the natural morphisms of group K-schemes

$$\pi : U \to Y_n,\ n_X : U \to W$$

are surjective, i.e.,

$$\pi(U) = Y_n,\ nU = W.$$

We have

$$v(Y_n) = v(\pi(U)) = v\pi(U) = nU = W,$$

i.e.,

$$v(Y_n) = W.$$

By 3.5(i), there exists a K-isogeny $\beta : X \to Y$ with $\ker(\beta) \subset X_r$. Then there exists a K-isogeny $\gamma : Y \to X$ such that $\gamma\beta = r_X$. This implies that

$$\gamma r_Y = r_X\gamma = \gamma\beta\gamma = \gamma(\beta\gamma),$$

i.e.,

$$\gamma r_Y = \gamma(\beta\gamma).$$

It follows that $r_Y = \beta\gamma$, because $\ker(\gamma)$ is finite while $(r_Y - \beta\gamma)Y$ is an abelian subvariety. This implies that

$$\beta(X_n) \supset \beta(\gamma(Y_n)) = \beta\gamma(Y_n) = rY_n.$$

Let us put

$$u = v\beta \in \mathrm{End}(X).$$

We have

$$Y_n \supset \beta(X_n) \supset rY_n.$$

This implies that

$$W = v(Y_n) \supset v(\beta)(X_n) = u(X_n),$$

$$u(X_n) = v(\beta(X_n)) \supset v(rY_n) = r(W)$$

and therefore

$$W \supset u(X_n) \supset r(W).$$

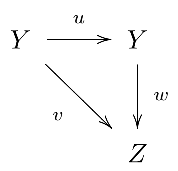
□

9. Dividing homomorphisms of abelian varieties

Results of this Section will be used in the proof of Theorem 4.1 in Section 10.

Throughout this Section, Y is an abelian variety over a field K. The following statement is well known.

Lemma 9.1. *let $u : Y \to Y$ be a K-isogeny. Suppose that Z is an abelian variety over K. Let $v \in \mathrm{Hom}(Y, Z)$ and $\ker(u) \subset \ker(v)$ (as a group subscheme in Y). Then there exists exactly one $w \in \mathrm{Hom}(Y, T)$ such that $v = wu$, i.e., the diagram*



is commutative. In addition, w is an isogeny if and only if v is an isogeny.

Proof. We have $Y \cong Y/\ker(u)$. Now the result follows from the universality property of quotient maps.

□

Let n be a positive integer and u an endomorphism of Y. Let us consider the homomorphism of abelian varieties over K

$$(n_Y, u) : Y \to Y \times Y, \quad y \mapsto (ny, uy).$$

Then

$$\ker((n_Y, u)) = \ker(Y_n \xrightarrow{u} Y_n) \subset Y_n \subset Y.$$

Slightly abusing notation, we denote the finite commutative group K-(sub)scheme $\ker((n_Y, u))$ by $\{\ker(u) \bigcap Y_n\}$.

Lemma 9.2. *Let Y be an abelian variety of positive dimension over a field K. Then there exists a positive integer $h = h(Y, K)$ that enjoys the following properties:*

If n is a positive integer, $u, v \in \mathrm{End}(Y)$ are endomorphisms such that

$$\{\ker(u) \bigcap Y_n\} \subset \{\ker(v) \bigcap Y_n\}$$

then there exists a K-isogeny $w : Y \to Y$ such that

$$hv - wu \in n \cdot \mathrm{End}(Y).$$

In particular, the images of hv and wu in $\mathrm{End}(Y_n)$ do coincide.

Proof. Since $\mathcal{O} := \mathrm{End}(Y)$ is an order in the semisimple finite-dimensional $\mathbb{Q}$-algebra $\mathrm{End}(Y) \otimes \mathbb{Q}$, the Jordan–Zassenhaus theorem [23, Th. 26.4] implies that there exists a positive integer M that enjoys the following properties:

if I is a left ideal in $\mathcal{O}$ that is also a subgroup of finite index then there exists $a_I \in \mathcal{O}$ such that the principal left ideal $a \cdot \mathcal{O}$ is a subgroup in I of finite index dividing M; in particular,

$$M \cdot I \subset a_I \cdot \mathcal{O} \subset I.$$

Clearly, such a_I is invertible in $\mathrm{End}(Y) \otimes \mathbb{Q}$ and therefore is an isogeny. Let us put

$$h := M^3.$$

Let us consider the left ideals

$$I = n\mathcal{O} + u\mathcal{O}, \ J = n\mathcal{O} + v\mathcal{O}$$

in $\mathcal{O}$. Then both I and J are subgroups of finite index in $\mathcal{O}$. So, there exist K-isogenies

$$a_I : Y \to Y, \ a_J : Y \to Y$$

such that

$$M \cdot I \subset a_I \cdot \mathcal{O} \subset I, \ M \cdot I \subset a_J \cdot \mathcal{O} \subset J.$$

In particular, there exist $b, c \in \mathcal{O}$ such that

$$Ma_I - bu \in n \cdot \mathcal{O}, \ Mv = ca_J.$$

In obvious notation

$$\{\ker(v) \bigcap Y_n\} \subset \ker(a_J) \subset \{\ker(Mv) \bigcap Y_{Mn}\} = M^{-1}\{\ker(v) \bigcap Y_n\} \subset Y,$$

$$\{\ker(u) \bigcap Y_n\} \subset \ker(a_I) \subset \{\ker(Mu) \bigcap Y_{Mn}\} = M^{-1}\{\ker(u) \bigcap Y_n\} \subset Y.$$

This implies that

$$\ker(a_I) \subset M^{-1}\{\ker(u) \bigcap Y_n\} \subset M^{-1}\{\ker(v) \bigcap Y_n\} \subset M^{-1} \ker(a_J) = \ker(Ma_J)$$

and therefore

$$\ker(a_I) \subset \ker(Ma_J).$$

By Lemma 9.1, there exists a K-isogeny $z : Y \to Y$ such that $Ma_J = za_I$ and therefore $M^2 a_J = Mza_I$. This implies that

$$M^3v = M^2ca_J = Mc(Ma_J) = Mc(za_I) = cz(Ma_I) =$$

$$cz[bu + (Ma_I - bu)] = (czb)u + cz(Ma_I - bu).$$

Since $h = M^3$ and $bu - Ma_I$ is divisible by n in $\mathcal{O} = \mathrm{End}(Y)$,

$$hv - (czb)u \in n \cdot \mathrm{End}(Y).$$

So, we may put $w = czb$. $\square$

10. Endomorphisms of group schemes

Proof of Theorem 4.1. Let X be an abelian variety of positive dimension over a finite field K. Let us put $Y := X \times X$. Let $h = h(Y)$ be as in Lemma 9.2 and $r = r(Y, K)$ be as in Corollary 3.5. Let us put

$$r_1 = r_1(X, K) := r(Y, K)h(Y, K).$$

Let n be a positive integer and $u_n \in \mathrm{End}(X_n)$. Let W be the graph of u_n in $X_n \times X_n = (X \times X)_n = Y_n$, i.e., the image of

$$(\mathbf{1}_n, u_n) : X_n \hookrightarrow X_n \times X_n = (X \times X)_n = Y_n.$$

Here $\mathbf{1}_n$ is the identity automorphism of X_n.

By Corollary 3.5, there exists $v \in \mathrm{End}(Y)$ such that

$$rW \subset u(Y_n) \subset W.$$

Let $\mathrm{pr}_1, \mathrm{pr}_2 : Y = X \times X \to X$ be the projection maps and

$$q_1 : X = X \times \{0\} \subset X \times X = Y,\ q_2 : X = \{0\} \times X \subset X \times X = Y$$

be the inclusion maps. Let us consider the homomorphisms

$$\mathrm{pr}_1 v, \mathrm{pr}_2 v : Y \to X$$

and the endomorphisms

$$v_1 = q_1 \mathrm{pr}_1 v,\ v_2 = q_1 \mathrm{pr}_2 v \in \mathrm{End}(X \times X) = \mathrm{End}(Y).$$

Clearly,

$$v : Y \to Y = X \times X$$

is "defined" by pair

$$(\mathrm{pr}_1 v, \mathrm{pr}_2 v) : Y \to X \times X = Y.$$

Since W is a graph,

$$\mathrm{pr}_1(W) = X_n,\ v(Y_n) \subset W$$

and

$$\{\ker(\mathrm{pr}_1 v) \bigcap Y_n\} \subset \{\ker(\mathrm{pr}_2 v) \bigcap Y_n\}.$$

Since q_1 and q_2 are embeddings,

$$\{\ker(v_1) \bigcap Y_n\} \subset \{\ker(v_2) \bigcap Y_n\}.$$

By Lemma 9.2, there exists a K-isogeny $w : Y \to Y$ such that the restrictions of hv_2 and wv_1 to Y_n do coincide. Taking into account that

$$v_1(X \times X) \subset X \times \{0\},\ v_2(X \times X) \subset \{0\} \times X,$$

we conclude that if we put

$$w_{12} = \mathrm{pr}_2 w q_1 \in \mathrm{End}(X)$$

then the images of $h\ \mathrm{pr}_2 v$ and $w_{12}\mathrm{pr}_1 v$ in $\mathrm{Hom}(Y_n, X_n) = \mathrm{Hom}(X_n \times X_n, X_n)$ do coincide.

Since W is the graph of u_n and $u(Y_n) \subset W$,

$$\mathrm{pr}_2 v = u_n \mathrm{pr}_1 v \in \mathrm{Hom}(Y_n, X_n);$$

here both sides are viewed as morphisms of group schemes $Y_n \to X_n$. This implies that in $\mathrm{Hom}(Y_n, X_n)$ we have

$$w_{12}\mathrm{pr}_1 v = h\ \mathrm{pr}_2 v = h\ u_n \mathrm{pr}_1 v.$$

This implies that $w_{12} = h\ u_n$ on

$$\mathrm{pr}_1 v(Y_n) \subset X_n.$$

We have

$$\mathrm{pr}_1 v(Y_n) \supset r\ \mathrm{pr}_1(r(W)) = r(X_n)$$

and therefore $w_{12} = h\ u_n$ on $r(X_n)$. By Lemma 1.8,

$$r(X_n) = X_{n_1},$$

where $n_1 = n/(n,r)$. So, $w_{12} = h\ u_n$ on X_{n_1}. Let us put $d := (n_1, h)$. Clearly, $X_d \subset X_{n_1}$ and $w_{12} = hu_n$ kills X_d, because d divides h. This implies that there exists $u \in \mathrm{End}(X)$ such that $w_{12} = d\ u$. If we put $m = n_1/d$ then h/d is a positive integer relatively prime to m and $(h/d)\ u\ d = (h/d)\ u_n\ d$ on X_{n_1} and therefore $(h/d)\ u = (h/d)\ u_n$ on $d(X_{n_1}) = X_m$. Since multiplication by (h/d) is an automorphism of X_m, we conclude that $u = u_n$ on X_m.

□

Corollary 10.1. *Let K be a finite field, X and Y abelian varieties over K. Let S be the set of positive integers n such that the finite commutative group K-schemes X_n and Y_n are isomorphic. If S is infinite then X and Y are isogenous over K. In addition, if S is the set of powers of a prime ℓ then there exists a K-isogeny $X \to Y$, whose degree is not divisible by ℓ.*

Proof. Pick $n \in S$ such that $n > r_2 := r_2(X, Y)$ where r_2 is as in Theorem 4.2. Then $m := n/(n, r_2)$ is strictly greater than 1. (In addition, if n is a power of ℓ then m is also a power of ℓ.(Fix an isomorphism $w_n : X_n \cong Y_n$. By Theorem 4.2, there exists $u \in \mathrm{Hom}(X, Y)$ such that the induced morphism $u_m : X_m \to Y_m$ coincides with the restriction (image) of w_n to (in) $\mathrm{Hom}(X_m, Y_m)$. But this restriction is an isomorphism, since w_n is an isomorphism. It follows that u_m is an isomorphism. Now the desired result follows from Lemma 1.10(ii).

□

Theorem 10.2 (Tate's theorem on homomorphisms)**.** *Let K be a finite field, ℓ an arbitrary prime, X and Y abelian varieties over K of positive dimension. Let $X(\ell)$ and $Y(\ell)$ be the ℓ-divisible groups attached to X and Y respectively. Then the natural embedding*

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}(X(\ell), Y(\ell))$$

is bijective.

Remark 10.3. Our proof will work for both cases $\ell \neq \mathrm{char}(K)$ and $\ell = \mathrm{char}(K)$.

Proof of Theorem 10.2. Any element of $\mathrm{Hom}(X(\ell), Y(\ell))$ is a collection

$$\{w_{(\nu)} \in \mathrm{Hom}(X_{\ell^\nu}, Y_{\ell^\nu})\}_{\nu=1}^{\infty}$$

such that every $w_{(\nu)}$ coincides with the "restriction" of $w_{(\nu+1)}$ to X_{ℓ^ν}. It follows from Corollary 4.4 that there exists $u_\nu \in \mathrm{Hom}(X, Y) \otimes \mathbb{Z}/\ell^\nu$ such that $w_{(\nu)} = u_\nu$. This implies that the image of $u_{\nu+1}$ in $\mathrm{Hom}(X, Y) \otimes \mathbb{Z}/\ell^\nu$ coincides with u_ν for all ν. This means that if u is the projective limit of u_ν in $\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell$ then u induces (for all ν) the morphism from X_{ℓ^ν} to Y_{ℓ^ν} that coincides with u_ν and therefore with $w_{(\nu)}$. □

Corollary 10.4. *Let K be a finite field, ℓ an arbitrary prime, X and Y abelian varieties over K of positive dimension. Then the following conditions are equivalent:*

- *There exists a K-isogeny $X \to Y$, whose degree is not divisible by ℓ.*
- *The ℓ-divisible groups $X(\ell)$ and $Y(\ell)$ are isomorphic.*

Proof. It follows readily from Theorem 10.2 and Corollary 2.7. □

11. Homomorphisms of Tate modules and isogenies

Throughout this Section, K is a finite field and ℓ is a prime $\neq \mathrm{char}(K)$.

Combining Theorem 10.2 with results of Section 2.8, we obtain the following statement.

Theorem 11.1 (Tate [27]). *Let X and Y be abelian varieties over K. Then*

$$\mathrm{Hom}(X,Y)\otimes \mathbb{Z}_\ell = \mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y)).$$

Let X be an abelian variety over K. Let us consider the $\mathbb{Q}_\ell$-vector space

$$V_\ell(X) = T_\ell(X)\otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

provided with the natural structure of Galois module. We have

$$\dim_{\mathbb{Q}_\ell}(V_\ell(X)) = 2\dim(X)$$

and the map

$$T_\ell(X) \hookrightarrow V_\ell(X),\ z \mapsto z\otimes 1$$

identifies $T_\ell(X)$ with a Galois-invariant $\mathbb{Z}_\ell$-lattice. This implies that the natural map

$$\mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y))\otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \to \mathrm{Hom}_{\mathrm{Gal}}(V_\ell(X), V_\ell(Y))$$

is bijective. Here $\mathrm{Hom}_{\mathrm{Gal}}(V_\ell(X), V_\ell(Y))$ is the $\mathbb{Q}_\ell$-vector space of $\mathbb{Q}_\ell$-linear homomorphisms of Galois modules $V_\ell(X)\to V_\ell(Y)$.

Applying Theorem 11.1, we obtain the following statement.

Theorem 11.2 (Tate [27]). *Let X and Y be abelian varieties over K. Then the natural map*

$$\mathrm{Hom}(X,Y)\otimes \mathbb{Q}_\ell = \mathrm{Hom}_{\mathrm{Gal}}(V_\ell(X), V_\ell(Y))$$

is bijective.

The following assertion is very useful.

Corollary 11.3 (Tate's isogeny theorem [27]). *Let X and Y be abelian varieties over K. Then X and Y are isogenous over K if and only if the Galois modules $V_\ell(X)$ and $V_\ell(Y)$ are isomorphic.*

Proof. If X and Y are isogenous over K then there exist a positive integer N and isogenies

$$\alpha : X\to Y,\ \beta : Y\to X$$

such that

$$\beta\alpha = N_X, \ \alpha\beta = N_Y.$$

By functoriality, α and β induce homomorphisms of Galois modules

$$\alpha(\ell): V_\ell(X) \to V_\ell(Y), \ \beta(\ell): V_\ell(Y) \to V_\ell(X)$$

such that the compositions $\beta(\ell)\alpha(\ell)$ and $\alpha(\ell)\beta(\ell)$ coincide with multiplication by N in $V_\ell(X)$ and $V_\ell(Y)$ respectively. It follows that $\alpha(\ell)$ is an isomorphism of Galois modules $V_\ell(X)$ and $V_\ell(Y)$.

Suppose now that the Galois modules $V_\ell(X)$ and $V_\ell(Y)$ are isomorphic. Then their $\mathbb{Q}_\ell$-dimensions coincide and therefore

$$\dim(X) = \dim(Y).$$

Choose an isomorphism

$$w: V_\ell(X) \cong V_\ell(Y)$$

of Galois modules. Replacing (if necessary) w by $\ell^M w$ for sufficiently large positive integer M, we may and will assume that

$$w(T_\ell(X)) \subset T_\ell(Y).$$

The image $w(T_\ell(X))$ is a $\mathbb{Z}_\ell$-lattice in $V_\ell(Y)$. This implies that $w(T_\ell(X))$ is a subgroup of finite index in $T_\ell(Y)$. So, we may view w as an *injective* homomorphism $T_\ell(X) \to T_\ell(Y)$ of Galois modules. There exists a positive integer M such that if

$$w' \in \mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y)), \ w' - w \in \ell^M \cdot \mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y))$$

then

$$w': T_\ell(X) \to T_\ell(Y)$$

is also injective. Since $\mathrm{Hom}(X, Y)$ is everywhere dense with respect to ℓ-adic topology in

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell = \mathrm{Hom}_{\mathrm{Gal}}(T_\ell(X), T_\ell(Y)),$$

there exists $u \in \mathrm{Hom}(X, Y)$ such that the induced (by u) homomorphism of Galois modules

$$u(\ell): T_\ell(X) \to T_\ell(Y)$$

is injective. This implies that

$$\mathrm{rk}_{\mathbb{Z}_\ell}(u(\ell)(T_\ell(X))) = \mathrm{rk}_{\mathbb{Z}_\ell}(T_\ell(X)) = 2\dim(X) = 2\dim(Y).$$

I claim that u is an isogeny. Indeed, let us put $Z := u(X)$: it is a (closed) abelian subvariety of Y that is defined over K. The homomorphism $u: X \to Y$ coincides with the composition of the natural surjection $X \to Z$ and the inclusion map $j: Z \hookrightarrow X$. This implies that $u(\ell)(T_\ell(X))$ is contained in $j(\ell)(T_\ell(Z))$ where

$$j(\ell): T_\ell(Z) \to T_\ell(Y)$$

is the homomorphism of Tate modules induced by j. It follows that

$$2\dim(Z) = \mathrm{rk}(T_\ell(Z)) \geq \mathrm{rk}(j(\ell)(T_\ell(Z))) \geq$$

$$\mathrm{rk}(u(\ell)(T_\ell(X))) = 2\dim(X) = 2\dim(Y)$$

and therefore $\dim(Z) \geq \dim(Y)$. (Hereafter rk stands for the rank of a free $\mathbb{Z}_\ell$-module.)

Since Z is a closed subvariety of Y, we conclude that $\dim(Z) = \dim(Y)$ and therefore $Z = Y$. This implies that $u: X \to Y$ is surjective. Since $\dim(X) = \dim(Y)$, we conclude that u is an isogeny. □

Corollary 11.3 admits the following "refinement".

Corollary 11.4. *Let X and Y be abelian varieties over K. The following assertions are equivalent.*

- *There exists an isogeny $X \to Y$, whose degree is not divisible by ℓ.*
- *The Galois modules $T_\ell(X)$ and $T_\ell(Y)$ are isomorphic.*

Proof. It follows readily from Corollary 10.4 and the last displayed formula in Subsection 2.8. □

12. An example

Corollaries 10.1 and Corollary 10.4 suggest the following question: if X and Y are abelian varieties over a finite field K such that $X_n \cong Y_n$ for all n and $X(\ell) \cong Y(\ell)$ for all ℓ then is it true that X and Y are isomorphic? The aim of this Section is to give a negative answer to this question. Our construction is based on the theory of elliptic curves with complex multiplication [24,9].

We start to work over the field $\mathbb{C}$ of complex numbers. Let $F \subset \mathbb{C}$ be an imaginary quadratic field with the ring of integers $\mathcal{O}_F$. For every non-zero ideal $\mathfrak{b} \subset \mathcal{O}_F$ there exists an elliptic curve $E^{(\mathfrak{b})}$ over $\mathbb{C}$ such that that its group of complex points $E^{(\mathfrak{b})}(\mathbb{C})$ (viewed as a complex Lie group) is $\mathbb{C}/\mathfrak{b}$. There is a natural ring isomorphism $\mathcal{O}_F \cong \mathrm{End}(E^{(\mathfrak{b})})$ where any $a \in \mathcal{O}_F$ acts on $E^{(\mathfrak{b})}(\mathbb{C})$ as

$$z + \mathfrak{b} \mapsto az + \mathfrak{b}.$$

In particular, $E^{(\mathfrak{b})}$ is an elliptic curve with complex multiplication and $\mathrm{j}(E^{(\mathfrak{b})}) \in \mathbb{C}$ is an *algebraic integer*.

Let us put $E := E^{(\mathcal{O}_F)}$. There is a natural bijection of groups

$$\mathfrak{b} \cong \mathrm{Hom}(E, E^{(\mathfrak{b})}),\ c \mapsto u(c),$$

where homomorphism $u(c)$ acts on complex points as

$$u(c) : \mathbb{C}/\mathcal{O}_F \to \mathbb{C}/\mathfrak{b},\ z + \mathcal{O}_F \mapsto cz + \mathfrak{b}.$$

In addition, for every non-zero c the homomorphism $u(c) : E \to E^{(\mathfrak{b})}$ is an isogeny, whose degree is the order of the (finite) quotient $\mathfrak{b}/c\mathcal{O}_F$. In particular, E and $E^{(\mathfrak{b})}$ are isomorphic if and only if $\mathfrak{b}$ is a principal ideal. This implies that if $\mathfrak{b}$ is not principal then

$$\mathrm{j}(E^{(\mathfrak{b})}) \neq \mathrm{j}(E).$$

Lemma 12.1. *For every prime ℓ there exists a non-zero $c \in \mathfrak{b}$ such that the order of $\mathfrak{b}/c\mathcal{O}_F$ is not divisible by ℓ.*

Proof. We may assume that $\mathfrak{b}$ is not principal. If $\ell\mathcal{O}_F$ is a prime ideal in $\mathcal{O}_F$, pick any $c \in \mathfrak{b} \setminus \ell\mathfrak{b}$. If $\ell\mathcal{O}_F$ is a square $\mathfrak{L}^2$ of a prime ideal $\mathfrak{L}$, pick any $c \in \mathfrak{b} \setminus \mathfrak{L} \cdot \mathfrak{b}$. If $\ell\mathcal{O}_F$ is a product $\mathfrak{L}_1\mathfrak{L}_2$ of two distinct prime ideals $\mathfrak{L}_1, \mathfrak{L}_2 \subset \mathcal{O}_F$, pick

$$c_1 \in \mathfrak{L}_1 \cdot b \setminus \mathfrak{L}_2 \cdot \mathfrak{b},\ c_2 \in \mathfrak{L}_2 \cdot \mathfrak{b} \setminus \mathfrak{L}_1 \cdot \mathfrak{b}$$

and put $c = c_1 + c_2$; clearly,

$$c \notin \mathfrak{L}_1 \cdot \mathfrak{b},\ c \notin \mathfrak{L}_2 \cdot \mathfrak{b}.$$

In all three cases

$$c\mathcal{O}_F = \mathfrak{M} \cdot \mathfrak{b}$$

where the ideal $\mathfrak{M} = \prod_{\mathfrak{P}} \mathfrak{P}^{m_{\mathfrak{P}}}$ is a (finite) product of powers of (non-zero) prime ideals $\mathfrak{P}$, none of which divides ℓ. It follows that $\mathfrak{b}/c\mathcal{O}_F$ is a (finite) $\mathcal{O}_F/\mathfrak{M}$-module. By the Chinese Remainder Theorem,

$$\mathcal{O}_F/\mathfrak{M} = \oplus_{\mathfrak{P}}\mathcal{O}_F/\mathfrak{P}^{m_{\mathfrak{P}}}.$$

Therefore $\mathfrak{b}/c\mathcal{O}_F$ is a product of finite $\mathcal{O}_F/\mathfrak{P}^{m_{\mathfrak{P}}}$-modules. Since the multiplication by the residual characteristic of $\mathfrak{P}$ kills $\mathcal{O}_F/\mathfrak{P}$, it follows that the $m_{\mathfrak{P}}$th power of this characteristic kills every $\mathcal{O}_F/\mathfrak{P}^{m_{\mathfrak{P}}}$-module. This implies that the order of $\mathfrak{b}/c\mathcal{O}_F$ is a product of powers of residual characteristics of $\mathfrak{P}$'s and therefore is not divisible by ℓ. □

Corollary 12.2. *For every prime ℓ there exists an isogeny $E \to E^{(\mathfrak{b})}$, whose degree is not divisible by ℓ.*

12.3. The construction. Choose an imaginary quadratic field F with class number > 1 and pick a *non*-principal ideal $\mathfrak{b} \subset \mathcal{O}_F$. We have

$$\mathrm{j}(E^{(\mathfrak{b})}) \neq \mathrm{j}(E).$$

There exists an algebraic number field $L \subset \mathbb{C}$ such that:

- L contains F, $\mathrm{j}(E)$ and $\mathrm{j}(E^{(\mathfrak{b})})$.
- The elliptic curves E and $E^{(\mathfrak{b})}$ are defined over L.
- All homomorphisms between E and $E^{(\mathfrak{b})}$ are defined over L.

Let us choose a maximal ideal $\mathfrak{q} \subset \mathcal{O}_F$ such that both E and $E^{(\mathfrak{b})}$ have good reduction at $\mathfrak{q}$ and $j(E) - j(E^{(\mathfrak{b})})$ does *not* lie in $\mathfrak{q}$. (Those conditions are satisfied by all but finitely many $\mathfrak{q}$.) Let K be the (finite) residue field at $\mathfrak{q}$, let $\mathbf{E}$ and $\mathbf{E}^{(b)}$ be the reductions at $\mathfrak{q}$ of E and $E^{(\mathfrak{b})}$ respectively: they are elliptic curves over K. Then $\mathrm{j}(\mathbf{E})$ and $\mathrm{j}(\mathbf{E}^{(b)})$ are the reductions modulo $\mathfrak{q}$ of $\mathrm{j}(E)$ and $\mathrm{j}(E^{(\mathfrak{b})})$ respectively. Our assumptions on $\mathfrak{q}$ imply that

$$\mathrm{j}(\mathbf{E}) \neq \mathrm{j}(\mathbf{E}^{(b)}).$$

Therefore $\mathbf{E}$ and $\mathbf{E}^{(b)}$ are not isomorphic over K and even over $\bar{K}$!

On the other hand, it is known [9, Ch. 9, Sect. 3] that there is a natural embedding

$$\mathrm{Hom}(E, E^{(\mathfrak{b})}) \hookrightarrow \mathrm{Hom}(\mathbf{E}, \mathbf{E}^{(\mathfrak{b})})$$

that respects the degrees of isogenies. It follows from Corollary 12.2 that for every prime ℓ there exists an isogeny $\mathbf{E} \to \mathbf{E}^{(\mathfrak{b})}$, whose degree is not divisible by ℓ. Now Proposition 1.11 implies that $\mathbf{E}_n \cong \mathbf{E}^{(\mathfrak{b})}{}_n$ for all positive integers n. It follows from Corollary 10.4 that the ℓ-divisible groups $\mathbf{E}(\ell)$ and $\mathbf{E}^{(\mathfrak{b})}(\ell)$ are isomorphic for all ℓ, including $\ell = \mathrm{char}(K)$. Since both $\mathbf{E}(\bar{K})$ and $\mathbf{E}^{(\mathfrak{b})}(\bar{K})$ are torsion groups, they are isomorphic as Galois modules. This implies that their subgroups of all Galois invariants are isomorphic, i.e., the finite groups $\mathbf{E}(K)$ and $\mathbf{E}^{(\mathfrak{b})}(K)$ are isomorphic.

References

[1] A. Borel, Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. **75** (1962), 485–535.

[2] P. Deligne, *Variétés abéliennes ordinaire sur un corps fini*, Invent. Math. **8** (1969), 238-243.

[3] M. Demazure, P. Gabriel, Groupes algébriques, Tome I, North Holland, Amsterdam 1970.

[4] D. Eisenbud, J. Harris, The geometry of schemes, GTM **197**, Springer-Verlag, New York 2000.

[5] R. Hoobler and A. Magid, *Finite group schemes over fields*, Proc. Amer. Math. Soc. **33** (1972), 310–312.

[6] J. Harris, Algebraic geometry, Corrected 3rd printing, Springer Verlag New York, 1995.

[7] R. Hartshorne, Algebraic geometry, GTM **52**, Springer Verlag, New York Heidelberg Berlin, 1977.

[8] S. Lang, Abelian varieties, 2nd edition, Springer Verlag, New York, 1983.

[9] S. Lang, Elliptic functions, Addison-Wesley, 1973.
[10] H.W. Lenstra, Jr., F. Oort, Yu. G. Zarhin, *Abelian subvarieties*, University of Utrecht, Department of Mathematics, Preprint 842, March 1994; 19 pp.
[11] H.W. Lenstra, Jr., F. Oort, Yu. G. Zarhin, *Abelian subvarieties*, J. Algebra **80** (1996), 513–516.
[12] J.S. Milne, W. C. Waterhouse, *Abelian varieties over finite fields*, Proc. Symp. Pure Math. 20 (1971), 53-64.
[13] J.S. Milne, *Abelian varieties*, Chapter V in: Arithmetic geometry (G. Cornell, J.H. Silverman, eds.). Springer-Verlag, New York 1986.
[14] L. Moret-Bailly, Pinceaux de variétés abéliennes, Astérisque, vol. 129 (1985).
[15] D. Mumford, J. Fogarty, F. Kirwan, Geometric invariant theory, 3rd enlarged edition, Springer Verlag 1994.
[16] D. Mumford, Abelian varieties, 2nd edition, Oxford University Press, 1974.
[17] F. Oort, Commutative group schemes, Springer Lecture Notes in Math. **15** (1966).
[18] F. Oort and J.R. Strooker, *The category of finite groups over a field*, Indag. Math. **29** (1967), 163–169.
[19] F. Oort and J. Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.
[20] F. Oort, *Abelian varieties over finite fields*, This volume, `www.math.uu.nl/people/oort/`.
[21] R. Pink, *Finite group schemes*, Lecture course in WS 2004/05 ETH Zürich, `www.math.ethz.ch/ pink/ftp/FGS/CompleteNotes.pdf`.
[22] C.P. Ramanujam, *The theorem of Tate*, Appendix I to [16].
[23] I. Reiner, Maximal orders, First edition, Academic Press, London, 1975; Second edition, Clarendon Press, Oxford, 2003.
[24] J.-P. Serre, *Complex multiplication*, Chapter 13 in: Algebraic Number Theory (J. Cassels A. Frölich, eds), Academic Press, London, 1967.
[25] S.S. Shatz, *Group schemes, Formal groups and p-divisible groups*, Chapter III in: Arithmetic Geometry (G. Cornell, J.H. Silverman, eds.). Springer-Verlag, New York 1986.
[26] G. Shimura, Abelian varieties with complex multiplication and modular functions, Princeton University Press, Princeton, 1997.
[27] J.T. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.
[28] J.T. Tate, *p-divisible groups*, In: Proceedings of a Conference on Local Fields, Driebergen, 1966. Springer-Verlag, Berlin Heidelberg New York, 1967, pp. 158–183.
[29] I.R. Shafarevich, Basic algebraic geometry, First edition, Springer Verlag, Berlin Heidelberg New York 1977.
[30] W.C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Écol. Norm. Supér. (4) **2**, (1969), 521-560.
[31] W.C. Waterhouse, Introduction to affine group schemes, Springer-Velag, New York 1979.
[32] Yu. G. Zarhin, *Endomorphisms of abelian varieties and points of finite order in characteristic P*, Mat. Zametki, **21** (1977), 737-744; Mathematical Notes **21** (1978) 415–419.
[33] Yu. G. Zarhin, *Homomorphisms of Abelian varieties and points of finite order over fields of finite characteristic* (in Russian), pp. 146-147, In: Problems in Group Theory and Homological Algebra (A. L. Onishchik, editor), Yaroslavl Gos. Univ., Yaroslavl, 1981; MR0709632 (84m:14051).
[34] Yu. G. Zarhin, *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction*, Invent. Math. **79** (1985), 309–321.