HOMOMORPHISMS OF ABELIAN VARIETIES OVER GEOMETRIC FIELDS OF FINITE CHARACTERISTIC

YURI G. ZARHIN

Abstract. We study analogues of Tate's conjecture on homomorphisms for abelian varieties when the ground field is finitely generated over an algebraic closure of a finite field. Our results cover the case of abelian varieties without nontrivial endomorphisms.

1. Introduction

Let K be a field, $\bar{K}$ its algebraic closure, $\bar{K}_s \subset K$ the separable algebraic closure of K, $\mathrm{Gal}(K)=\mathrm{Gal}(\bar{K}_s/K)=\mathrm{Aut}(\bar{K}_s/K)$ the absolute Galois group of K. Let X be an abelian variety over K. Then we write $\mathrm{End}_K(X)$ for its ring of K-endomorphisms and put $\mathrm{End}_K^0(X):=\mathrm{End}_K(X)\otimes\mathbf{Q}$. We write $\mathrm{End}(X)$ for the endomorphism ring of $X\times\bar{K}$ and write $\mathrm{End}^0(X)$ for the corresponding finite-dimensional semisimple $\mathbf{Q}$-algebra $\mathrm{End}(X)\otimes\mathbf{Q}$. If n is a positive integer that is not divisible by $\mathrm{char}(K)$ then we write X_n for the kernel of multiplication by n in $X(\bar{K})$; it is well known that X_n is free $\mathbf{Z}/n\mathbf{Z}$-module of rank $2\mathrm{dim}(X)$ [8], which is a Galois submodule of $X(\bar{K}_s)$. We write $\bar{\rho}_{n,X}$ for the corresponding (continuous) structure homomorphism

$$\bar{\rho}_{n,X}:\mathrm{Gal}(K)\to\mathrm{Aut}_{\mathbf{Z}/n\mathbf{Z}}(X_n)\cong\mathrm{GL}(2\mathrm{dim}(X),\mathbf{Z}/n\mathbf{Z}).$$

In particular, if $n=\ell$ is a prime then X_ℓ is a $2\mathrm{dim}(X)$-dimensional $\mathbf{F}_\ell$-vector space provided with

$$\bar{\rho}_{\ell,X}:\mathrm{Gal}(K)\to\mathrm{Aut}_{\mathbf{F}_\ell}(X_\ell)\cong\mathrm{GL}(2\mathrm{dim}(X),\mathbf{F}_\ell).$$

If ℓ is a prime that is different from $\mathrm{char}(K)$ then we write $T_\ell(X)$ for the $\mathbf{Z}_\ell$-Tate module of X and $V_\ell(X)$ for the corresponding $\mathbf{Q}_\ell$-vector space

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

provided with the natural continuous Galois action [11]

$$\rho_{\ell,X}:\mathrm{Gal}(K)\to\mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X))\subset\mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(X)).$$

Recall [8] that $T_\ell(X)$ is a free $\mathbf{Z}_\ell$-module of rank $2\mathrm{dim}(X)$ and $V_\ell(X)$ is a $\mathbf{Q}_\ell$-vector space of dimension $2\mathrm{dim}(X)$. Notice that there are canonical isomorphisms of $\mathrm{Gal}(K)$-modules

$$X_\ell=T_\ell(X)/\ell T_\ell(X) \qquad (0).$$

There are natural algebra injections

$$\mathrm{End}(X)\otimes\mathbf{Z}/n\hookrightarrow\mathrm{End}_{\mathrm{Gal}K}(X_n) \qquad (1),$$

$$\mathrm{End}(X)\otimes\mathbf{Z}_\ell\hookrightarrow\mathrm{End}_{\mathrm{Gal}K}(T_\ell(X)) \qquad (2),$$

$$\mathrm{End}(X)\otimes\mathbf{Q}_\ell\hookrightarrow\mathrm{End}_{\mathrm{Gal}K}(V_\ell(X)) \qquad (3).$$

It is known [13, Sect. 1] that for given ℓ, K, X, Y the map in (2) is bijective if and only if the map in (3) is bijective.

The Tate conjecture on homomorphisms of abelian varieties [13] asserts that if K is finitely generated over its prime subfield then the last two injections are bijective. This conjecture was proven by J. Tate himself over finite fields [13], the author when $\mathrm{char}(K) > 2$ [14, 15], G. Faltings when $\mathrm{char}(K) = 0$ [4, 5] and by S. Mori when $\mathrm{char}(K) = 2$ [7]. They also proved (in the corresponding characteristics) that the Galois module $V_\ell(X)$ is semisimple. (In the case of finite fields the semisimplicity result is due to A. Weil. See also [19].) Let us state explicitly the following two well known corollaries of the Tate conjecture. (Here we assume that K is finitely generated over its prime subfield.)

(i) **The isogeny theorem**. If for some $\ell \neq \mathrm{char}(K)$ the $\mathrm{Gal}(K)$-modules $V_\ell(X)$ and $V_\ell(Y)$ are isomorphic then X and Y are isogenous over K. (See [13, Sect. 3, Th. 1(b) and its proof] and [9, Proof of Cor. 1.3 on p. 118].)

(ii) If $\mathrm{End}_K(X) = \mathbf{Z}$ then the $\mathrm{Gal}(K)$-module $V_\ell(X)$ is absolutely simple.

In addition, if K is finitely generated over its prime subfield and $\mathrm{char}(K) \neq 2$ then for all but finitely many primes ℓ the $\mathrm{Gal}(K)$-module X_ℓ is semisimple and the injection

$$\mathrm{Hom}(X, Y) \otimes \mathbf{Z}/\ell \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(K)}(X_\ell, Y_\ell)$$

in (1) is bijective ([16, Th. 1.1],[18, Cor. 5.4.3 and Cor. 5.4.5], [12, Prop. 3.4], [23, Th.4.4]). (See [22, Cor. 10.1] for a discussion of the case of finite fields.) It follows immediately that if $\mathrm{End}_K(X) = \mathbf{Z}$ then for all but finitely many primes ℓ the Galois module X_ℓ is absolutely simple. We discuss an analogue of the isogeny theorem with "finite coefficients" in Section 2.

Let p be a prime, $\mathbf{F}$ a finite field of characteristic p and $\bar{\mathbf{F}}$ an algebraic closure of $\mathbf{F}$. The aim of this note is to discuss the situation when the ground field L is a field of characteristic p that contains $\bar{\mathbf{F}}$ and is finitely generated over it. We call such a field a *geometric field* of characteristic p. Geometric fields are precisely the fields of rational functions of irreducible algebraic varieties over $\bar{\mathbf{F}}$.

Our main results are the following three theorems.

Theorem 1.1. *Let $p > 2$ be a prime, L a geometric field of characteristic p and X an abelian variety of positive dimension over L. Suppose that $\mathrm{End}_L(X) = \mathbf{Z}$. Then:*

(i) *For all primes $\ell \neq \mathrm{char}(L)$ the Galois module $V_\ell(X)$ is absolutely simple.*

(ii) *For all but finitely many primes ℓ the Galois module X_ℓ is absolutely simple.*

Remark 1.2. In the case of $\mathrm{End}(X) = \mathbf{Z}$ the assertion (i) of Theorem 1.1 follows from [17, Cor. 1.4].

Remark 1.3. Theorem 1.1 gives a positive answer to a question of W. Gajda that was asked in connection with [1].

Theorem 1.4. *Let p be a prime, L a geometric field of characteristic p and X and Y are abelian varieties of positive dimension over L. Suppose that $\mathrm{End}_L(X) = \mathbf{Z}$ and one of the following two conditions holds:*

(i) *There exists a prime ℓ such that the $\mathrm{Gal}(L)$-modules $V_\ell(X)$ and $V_\ell(Y)$ are isomorphic.*

(ii) *The $\mathrm{Gal}(L)$-modules X_ℓ and Y_ℓ are isomorphic for infinitely many primes ℓ.*

Then X and Y are isogenous over L.

Remark 1.5. There are plenty of explicit examples in characteristic $p > 2$ of abelian varieties X with $\mathrm{End}(X) = \mathbf{Z}$ [20, 21].

Theorem 1.6. *Let $p > 2$ be a prime, L a geometric field of characteristic p and X an abelian variety of positive dimension over L. Let $\mathcal{Z}$ be the center of $\mathrm{End}_L(X)$. Then:*

(i) *For all primes $\ell \neq \mathrm{char}(L)$ the center $\mathcal{Z}_{\ell,X}$ of $\mathrm{End}_{\mathrm{Gal}(L)}(V_\ell(X))$ lies in*
$$\mathcal{Z} \otimes \mathbf{Q}_\ell \subset \mathrm{End}_L(X) \otimes \mathbf{Q}_\ell.$$

(ii) *For all but finitely many primes ℓ the center $\bar{\mathcal{Z}}_{\ell,X}$ of $\mathrm{End}_{\mathrm{Gal}(L)}(X_\ell)$ lies in*
$$\mathcal{Z}/\ell \subset \mathrm{End}_L(X) \otimes \mathbf{Z}/\ell.$$

Remark 1.7. Clearly, for all ℓ the commutative $\mathbf{Q}_\ell$-algebra $\mathcal{Z} \otimes \mathbf{Q}_\ell$ coincides with the center of $\mathrm{End}_L(X) \otimes \mathbf{Q}_\ell$. It is also clear that for all but finitely many primes ℓ the commutative $\mathbf{F}_\ell$-algebra $\mathcal{Z}/\ell$ coincides with the center of $\mathrm{End}_L(X) \otimes \mathbf{Z}/\ell\mathbf{Z}$. Notice also that
$$\mathrm{End}_L(X) \otimes \mathbf{Q}_\ell \subset \mathrm{End}_{\mathrm{Gal}(L)}(V_\ell(X)),\ \mathrm{End}_L(X) \otimes \mathbf{Z}/\ell\mathbf{Z} \subset \mathrm{End}_{\mathrm{Gal}(L)}(X_\ell).$$
This implies that for all ℓ
$$\mathcal{Z}_{\ell,X} \bigcap [\mathrm{End}_L(X) \otimes \mathbf{Q}_\ell] \subset \mathcal{Z} \otimes \mathbf{Q}_\ell$$
and for all but finitely many ℓ
$$\bar{\mathcal{Z}}_{\ell,X} \bigcap [\mathrm{End}_L(X) \otimes \mathbf{Z}/\ell] \subset \mathcal{Z}/\ell.$$
It follows that in order to prove Theorem 1.6, it suffices to check that for all ℓ
$$\mathcal{Z}_{\ell,X} \subset \mathrm{End}_L(X) \otimes \mathbf{Q}_\ell$$
and for all but finitely many ℓ
$$\bar{\mathcal{Z}}_{\ell,X} \subset \mathrm{End}_L(X) \otimes \mathbf{Z}/\ell.$$

Remark 1.8. Compare Theorem 1.6 with [3, Cor. 4.2.8(ii)].

The paper is organized as follows. In Section 2 we discuss a variant of the isogeny theorem with finite coefficients. Section 3 contains auxiliary results from representation theory of groups with procyclic quotients. We prove the main results in Section 4.

2. Isogeny theorem with finite coefficients

Theorem 2.1. *Let K be a finitely generated over its prime subfield and $\mathrm{char}(K) \neq 2$. Let X and Y be abelian varieties over K. Suppose that for infinitely many primes ℓ the $\mathrm{Gal}(K)$-modules X_ℓ and Y_ℓ are isomorphic. Then X and Y are isomorphic.*

Proof. We may assume that $\dim(X) > 0$ and $\dim(Y) > 0$. Since for all primes $\ell \neq \mathrm{char}(K)$
$$2\dim(X) = \dim_{\mathbf{F}_\ell}(X_\ell),\ 2\dim(Y) = \dim_{\mathbf{F}_\ell}(Y_\ell),$$
and therefore $\dim(X) = \dim(Y)$. Since for all but finitely many primes ℓ
$$\mathrm{Hom}_K(X,Y) \otimes \mathbf{Z}/\ell\mathbf{Z} = \mathrm{Hom}_{\mathrm{Gal}(K)}(X_\ell, Y_\ell),$$
there exist a prime $\ell \neq \mathrm{char}(K)$ and a K-homomorphism $u : X \to Y$ such that u induces an isomorphism between X_ℓ and Y_ℓ. In particular, $\ker(u)$ does not contain

points of order ℓ on X while the image $u(X)$ contains all points of order ℓ on Y. This implies that $\ker(u)$ has dimension zero while irreducible closed $u(Y)$ has dimension $\dim(Y)$. In other words, $u : X \to Y$ is a surjective homomorphism with finite kernel, i.e., is an isogeny. □

Remark 2.2. It would be interesting to get an analogue of Theorem 2.1 where say, a number field K is replaced by its infinite ℓ-cyclotomic extension $K(\mu_{\ell^\infty})$. Some important special cases of this analogue are done in [6].

3. Representation theory

Throughout this Section, G is a profinite group H a closed normal subgroup of G such that the quotient $\Gamma = G/H$ is a procyclic group. We call G a *procyclic extension* of H.

We write down the group operation in G (and H) multiplicatively and in Γ additively. We write $\pi : G \to \Gamma$ for the natural continuous surjective homomorphism from G to Γ. If n is a positive integer then $n\Gamma$ is the closed subgroup (as the image of compact Γ under $\Gamma \stackrel{n}{\to} \Gamma$) in Γ, whose index divides n; since the index in finite, $n\Gamma$ is open in Γ. Notice that $n\Gamma$ is also a procyclic group.

Let us put $G_n = \pi^{-1}(n\Gamma)$; clearly, G_n is an open normal subgroup in G, whose index divides n. In addition, each G_n contains H and the quotient G/G_n is canonically isomorphic to $\Gamma/n\Gamma$ while $G_n/H \cong n\Gamma$. In particular, H is closed normal subgroup of G_n and the quotient G_n/H is procyclic, i.e. G_n is also a procyclic extension of H. In particular, for each positive integer m we may define the open normal subgroup $(G_n)_m$ of G_n; clearly,

$$(G_n)_m = G_{mn},$$

because $m(n\Gamma) = (mn)\Gamma$.

Remark 3.1. Let $c : G \to k^*$ be a continuous group homomorphism (character) of G with values in the multiplicative group of a locally compact field k that enjoys the following properties:

(i) c kills H, i.e., c factors through $G/H = \Gamma$.
(i) c^n is the trivial character, i.e., c^n kills the whole G.

Then obviously c kills $\pi^{-1}(n\Gamma) = G_n$, i.e., c factors through the finite cyclic quotient $G/G_n = \Gamma/n\Gamma$.

Let k be a a locally compact field (e.g., k is finite or $\mathbf{Q}_\ell$.) Let d be a positive number and V a d=dimensional k-vector space provided with discrete topology. Let

$$\rho : G \to \mathrm{Aut}_k(V) \cong \mathrm{GL}(d, k)$$

be a continuous semisimple linear representation of G. As usual, $\det(V)$ stands for the one-dimensional G-module $\Lambda_k^d(V)$.

Lemma 3.2. *Suppose that*

$$\mathrm{End}_{G_d}(V) = k.$$

Then the H-module V is absolutely simple. In particular,

$$\mathrm{End}_H(V) = k.$$

Remark 3.3. Lemma 3.2 asserts that if W is an absolutely simple G_d-module then it remains absolutely simple, being viewed as a H-module.

Proof. We have

$$k \subset \mathrm{End}_G(V) \subset \mathrm{End}_{G_d}(V) \subset \mathrm{End}_H(V).$$

Since $\mathrm{End}_{G_d}(V) = k$, we conclude that $k = \mathrm{End}_G(V)$.

By Clifford's Lemma [2, Theorem (49.2)], the H-module V is semisimple. Let us split V into a direct sum $V = \oplus_{i=1}^{r} V_i$ of isotypic H-modules. Clearly G permutes V_i's; the simplicity of the G-module V implies that G acts on $\{V_1, \dots, V_r\}$ transitively. In particular, all V_i's have the same dimension and therefore

$$\dim(V_i) = \frac{\dim(V)}{r} = \frac{d}{r};$$

in particular, $r \mid d$. Clearly, the action of G on $\{V_1, \dots, V_r\}$ factors through G/H. Since this action is transitive and G/H is procyclic, this action factors through finite cyclic G/G_r and therefore through G/G_n, i.e,, each V_i is a G_n-submodule. Since the G_n-module V is (absolutely) simple, $V = V_i$. In other words, the H-nodule V is isotypic.Then the centralizer

$$D = \mathrm{End}_H(V)$$

is a simple k-algebra. Let k' be the center of D: it is an overfield of k. Clearly, V becomes a k'-vector space; in particular, k'/k is a finite algebraic extension and $[k' : k] \mid d$. On the other hand, since H is normal in G,

$$\rho(g) D \rho(g)^{-1} = D \ \forall g \in G.$$

Clearly, the center k' is also stable under the conjugations by elements of $\rho(G)$ and $\{k'\}^G = k$. This gives us a continuous group homomorphism $G/H \to \mathrm{Aut}(k'/k$ such that $\{k'\}^{G/H} = k$. It follows that k'/k is a finite cyclic Galois extension and

$$G/H \to \mathrm{Aut}(k'/k) = \mathrm{Gal}(k'/k)$$

is a surjective homomorphism. Since $\#(\mathrm{Gal}(k'/k)) = [k' : k]$ divides d, the surjection $\mathrm{Gal}(k'/k) \twoheadrightarrow \mathrm{Gal}(k'/k)$ factors through G/G_n and therefore

$$k' \subset \mathrm{End}_{G_n}(V);$$

since $\mathrm{End}_{G_n}(V) = k$, we conclude that $k' \subset k$ and therefore $k' = k$. This means that D is a central simple k-algebra and let $t := \dim_k(D)$. We need to prove that $t = 1$. Suppose that $t > 1$, pick a generator in Γ and denote by g its preimage in G. Then the map

$$u \mapsto \rho(g) u \rho(g)^{-1}$$

is an automorphism of D, whose set of fixed points coincides with k. By Skolem-Noether theorem, there exists an element $z \in A^*$ such that

$$\rho(g) u \rho(g)^{-1} = z u z^{-1} \ \forall u \in D.$$

Clearly, z itself is a fixed point of this automorphism and therefore $z \in k$, which implies that the automorphism is the identity map and therefore its set of fixed points must be the whole D, which is not the case, because $t > 1$. The obtained contradiction proves that $t = 1$, i.e.,

$$\mathrm{End}_H(V) = D = k$$

and we are done. □

Lemma 3.4. *Let $\rho_1 : G \to \mathrm{Aut}_k(W_1)$ be a continuous linear d-dimensional representation of G over k. Let $\rho_2 : G \to \mathrm{Aut}_k(W_2)$ be a linear finite-dimensional continuous representation of G over k. Suppose that $\mathrm{End}_H(W_1) = k$ and the H-modules W_1 and W_2 are isomorphic. Then there exists a continuous character*

$$\chi : G/H = \Gamma \to k^*$$

such that the G-module W_2 is isomorphic to the twist $V_1(\chi)$. In particular, the one-dimensional G-modules $\det(W_2)$ and $[\det(W_1)](\chi^d)$ are isomorphic.

Proof. It is well known that the vector space $\mathrm{Hom}_k(W_1, W_2)$ carries the natural structure of a G-module defined by

$$g, u \mapsto \rho_2(g)u\rho_1(g)^{-1} \ \forall g \in G, \ u \in \mathrm{Hom}_k(W_1, W_2).$$

Since H is normal in G, the subspace $\mathrm{Hom}_H(W_1, W_2)$ of H-invariants is a G-invariant subspace in $\mathrm{Hom}_k(W_1, W_2)$. Our conditions on the H-module W_1 and W_2 imply that the k-vector space $\mathrm{Hom}_H(W_1, W_2)$ is one-dimensional (and its every nonzero element $W_1 \to W_2$ is an isomorphism of H-modules). Therefore the action of G on one-dimensional $\mathrm{Hom}_k(W_1, W_2)$ is defined by a certain continuous character $\chi : G \to k^*$, which obviously kills H, so we may view χ a a continuous character

$$\Gamma = G/H \to k^*.$$

This means thai if $u : W_1 \cong W_2$ is an isomorphism of H-modules then

$$\rho_2(g)u\rho_1(g)^{-1} = \chi(g)u \ \forall g \in G.$$

Multiplying this equality from the right by $\rho_1(g)$, we obtain that

$$\rho_2(g)u = \chi(g)u\rho_1(g) = u[\chi(g)\rho_1(g)] \ \forall g \in G,$$

which means that u is an isomorphism of G-modules $W_1(\chi)$ and W_2. It remains to notice that $\det(W_1(\chi)) = [\det(W_1)](\chi^d)$. □

Corollary 3.5. *We keep the notation and assumptions of Lemma 3.4. If for some positive integer N the G-modules $\det(W_1)^{\otimes N}$ and $\det(W_2)^{\otimes N}$ are isomorphic then the character χ^{Nd} is trivial.*

Theorem 3.6. *Suppose that the G-module V is semisimple. Then there exists a positive integer n that is bounded by a constant depending only on d and such that the center of $\mathrm{End}_H(V)$ lies in $\mathrm{End}_{G_n}(V)$.*

Proof. By a variant of Clifford's Lemma [23, Lemma 3.4], the H-module V is semisimple. In particular, the centralizer $D = \mathrm{End}_H(V)$ is a (finite-dimensional) semisimple k-algebra. Since H is normal in G

$$\rho(g)D\rho(g)^{-1} = D \ \forall g \in G.$$

Let Z be the center of D. Since D is semisimple, Z is isomorphic to a direct sum $\oplus_{i=1}^r k_i$ of finitely many overfields $k_i \supset k$ where each k_i/k is a finite algebraic field extension. Clearly,

$$[k_i : k] \le \dim_k(Z) \le \dim_k(V) = d, \ r \le d$$

and the k-algebra Z has exactly r minimal idempotents (the identity elements e_i's of k_i's. Clearly, group $\mathrm{Aut}_k(Z)$ of k-linear automorphisms of Z permutes e_i's, which gives us the homomorphism from $\mathrm{Aut}_k(Z)$ to the full symmetric group $\mathbf{S}_r$, whose kernel leaves invariant each summand k_i and therefore sits in the product $\prod_{i=1}^r \mathrm{Aut}(k_i/k)$, whose order does not exceed $\prod_{i=1}^r [k_i : k] \le d^d$. It follows that

$\mathrm{Aut}_k(Z)$ is a finite group, whose order n does not exceed $d!d^d$. On the other hand, clearly,

$$\rho(g)Z\rho(g)^{-1} = Z \ \forall g \in G,$$

because every automorphism of D respects its center. This gives us the group homomorphism

$$\phi : G \to \mathrm{Aut}_k(Z), \ \phi(g)(z) = \rho(g)z\rho(g)^{-1} \ \forall z \in Z, \ g \in G,$$

which kills H, because

$$Z \subset D = \mathrm{End}_H(V).$$

Clearly, ϕ kills G_n and we are done. □

4. Proofs of main results

There is a subfield $K \subset L$ such that K is finitely generated over $\mathbf{F}_p$ and the compositum $K\bar{\mathbf{F}} = L$ while given abelian varieties X and Y, their group laws and zeros are defined over K. We also require that

$$\mathrm{End}_K(X) = \mathrm{End}_L(X), \ \mathrm{End}_K(Y) = \mathrm{End}_L(Y) \qquad (4).$$

Let us put

$$G = \mathrm{Gal}(K), H = \mathrm{Gal}(L), \Gamma = \mathrm{Gal}(L/K_).$$

Since $\bar{\mathbf{F}}/\mathbf{F}$ is a Galois extension and $K\bar{\mathbf{F}} = L$, the Galois group $\Gamma = \mathrm{Gal}(L/K)$ is canonically isomorphic to a closed subgroup of $\mathrm{Gal}(\mathbf{F}/\mathbf{F}_p)$; since the latter is procyclic, Γ is also procyclic.

Let n be a positive integer and let us consider the open normal subgroup G_n of G. Since G_n contains H, the subfield $K_n = \bar{K}_s^{G_n}$ of G_n-invariants is a finite (cyclic) Galois extension of K that lies in L. In particular, K_n is finitely generated over $\mathbf{F}_p$ and $\mathrm{Gal}(K_n) = G_n$. Since $K \subset K_n \subset L$, it follows from (4) that

$$\mathrm{End}_{K_n}(X) = \mathrm{End}_L(X), \ \mathrm{End}_{K_n}(Y) = \mathrm{End}_L(Y) \qquad (5).$$

If ℓ is a prime different from p we write

$$\bar{\chi}_\ell : \mathrm{Gal}(K) \to (\mathbf{Z}/\ell\mathbf{Z})^* = \mathbf{F}_\ell^*, \ \chi_\ell : \mathrm{Gal}(K) \to \mathbf{Z}_\ell^* \subset \mathbf{Q}_\ell^*$$

for the cyclotomic characters that define the Galois action on all ℓth roots of unity (resp. all ℓ-power roots of unity). Clearly,

$$\bar{\chi}_\ell = \chi_\ell \bmod \ell \qquad (4).$$

Since K is finitely generated over $\mathbf{F}_p$, the cyclotomic characters enjoy the following properties:

- (i) The character χ_ℓ has infinite multiplicative order.
- (ii) If N is a positive integer then for all but finitely many primes ℓ the character $\bar{\chi}_\ell^N$ is nontrivial.

Since every K_n is finitely generated over $\mathbf{F}_p$, the abelian variety X over K enjoys the following properties.

- (a) For all primes $\ell \neq \mathrm{char}(K)$ the G_n-module $V_\ell(X)$ is semisimple and

  $$\mathrm{End}_{G_n}(V_\ell(X)) = \mathrm{End}_{K_n}(X) \otimes \mathbf{Q}_\ell = \mathrm{End}_L(X) \otimes \mathbf{Q}_\ell.$$

  In particular, if $\mathrm{End}_L(X) = \mathbf{Z}$ then G_n-module $V_\ell(X)$ is absolutely simple.

(b) For all but finitely many primes ℓ the G_n-module X_ℓ is semisimple and

$$\mathrm{End}_{G_n}(X_\ell) = \mathrm{End}_{K_n}(X) \otimes \mathbf{Z}/\ell = \mathrm{End}_L(X) \otimes \mathbf{Z}/\ell.$$

In particular, if $\mathrm{End}_L(X) = \mathbf{Z}$ then G_n-module X_ℓ is absolutely simple for all but finitely many primes ℓ.

Proof of Theorem 1.1. Let $d = \dim(X)$. Let us consider the open normal subgroup G_{2d} of G.

Since $\mathrm{End}_L(X) = \mathbf{Z}$, (a) tells us that the G_{2d}-module $V_\ell(X)$ is absolutely simple for each $\ell \ne p$; in particular,

$$\mathbf{Q}_\ell = \mathrm{End}_{G_{2d}}(V_\ell(X)) = \mathrm{End}_G(V_\ell(X)).$$

On the other hand, (b) tells us that for all but finitely many ℓ the G_{2d}-module X_ℓ is absolutely simple; in particular,

$$\mathbf{F}_\ell = \mathrm{End}_{G_{2d}}(X_\ell) = \mathrm{End}_G(X_\ell).$$

Now, in order to finish the proof of Theorem 1.1(i) it suffices to apply Lemma 3.2 in the following situations (taking into account that $2d = \dim_{\mathbf{Q}_\ell}(V_\ell(X)) = \dim_{\mathbf{F}_\ell}(X_\ell)$).

(i) $k = \mathbf{Q}_\ell,\ V = V_\ell(X)$.
(ii) $k = \mathbf{F}_\ell,\ V = X_\ell$.

□

Proof of Theorem 1.4. Clearly, $d := \dim(X) = \dim(Y)$. It is well known that the existence of Galois-equivariant nondegenerate alternating bilinear (Weil–Riemann) forms on Tate modules [10, Sect. 1.3], [23, Proof of Prop. 2.2] implies that $\det(V_\ell(X))$ and $\det(V_\ell(Y))$ are one-dimensional G-modules defined by the character χ_ℓ^d. Now applying Lemma 3.4, we conclude the G-module $V_\ell(Y)$ is isomorphic to the twist $V_\ell(X)(\chi)$ for a certain continuous character $\chi : G/H = \Gamma \to \mathbf{Q}_\ell^*$. It follows from Corollary to Lemma 3.4 that χ^{2d} is trivial. This implies that χ kills G_{2d} and therefore the G_{2d}-modules $V_\ell(X)$ and $V_\ell(Y)$ are isomorphic. Now the isogeny theorem over K_{2d} implies that X and Y are isogenous over K_{2d} and therefore over L. This proves (i).

Similar arguments work in the case (ii). Clearly, $d := \dim(X) = \dim(Y)$ and the structure of $\mathrm{Gal}(K)$-modules on the rank 1 free $\mathbf{Z}_\ell$-modules $\Lambda^{2d}_{\mathbf{Z}_\ell} T_\ell(X)$ and $\Lambda^{2d}_{\mathbf{Z}_\ell} T_\ell(Y)$ is defined by χ_ℓ^d, because

$$\Lambda^{2d}_{\mathbf{Z}_\ell} T_\ell(X) \subset \Lambda^{2d}_{\mathbf{Q}_\ell} V_\ell(X) = \det(V_\ell(X)),\ \Lambda^{2d}_{\mathbf{Z}_\ell} T_\ell(Y) \subset \Lambda^{2d}_{\mathbf{Q}_\ell} V_\ell(Y) = \det(V_\ell(Y)).$$

It follows from (0) that

$$\det(X_\ell) = \Lambda^{2d}_{\mathbf{Z}_\ell} X_\ell = \Lambda^{2d}_{\mathbf{Z}_\ell}(T_\ell(X)/\ell) = [\Lambda^{2d}_{\mathbf{Z}_\ell}(T_\ell(X)]/\ell$$

and therefore the structure of the Galois module on $\det(X_\ell)$ is defined by the character $\chi_\ell^d \bmod \ell = \bar{\chi}_\ell^d$. By the same token, the structure of the Galois module on the one-dimensional $\det(Y_\ell)$ is also defined by $\bar{\chi}_\ell^d$. Now applying Lemma 3.4, we conclude the G-module Y_ℓ is isomorphic to the twist $Y_\ell(\bar{\chi})$ for a certain continuous character $\bar{\chi} : G/H = \Gamma \to \mathbf{F}_\ell^*$. It follows from Corollary to Lemma 3.4 that $\bar{\chi}^{2d}$ is trivial. As above, this implies that $\bar{\chi}$ kills G_{2d} and therefore the G_{2d}-modules X_ℓ and Y_ℓ are isomorphic for infinitely many ℓ. Now Theorem 2.1 implies that X and Y are isogenous over K_{2d} and therefore over L. This proves (ii). □

Proof of Theorem 1.6. As above, $G = \mathrm{Gal}(K), H = \mathrm{Gal}(L)$.

(i) Let us put $k = \mathbf{Q}_\ell, V = V_\ell(X)$ and apply Theorem 3.6. We obtain that there exists a positive integer n such that the center of $\mathrm{End}_{\mathrm{Gal}(L)}(V_\ell(X))$ lies in $\mathrm{End}_{G_n}(V_\ell(X)) \otimes \mathbf{Q}_\ell$. By (a),

$$\mathrm{End}_{G_n}(V_\ell(X)) = \mathrm{End}_{K_n}(X) \otimes \mathbf{Q}_\ell = \mathrm{End}_L(X) \otimes \mathbf{Q}_\ell$$

and we are done.

(ii) Let us put $k = \mathbf{F}_\ell, V = X_\ell$ and apply Theorem 3.6. We obtain that there exists a universal positive integer n such that for all but finitely many primes ℓ the center of $\mathrm{End}_{\mathrm{Gal}(L)}(X_\ell)$ lies in $\mathrm{End}_{G_n}(X_\ell)$. By (b),

$$\mathrm{End}_{G_n}(X_\ell) = \mathrm{End}_{K_n}(X) \otimes \mathbf{Z}/\ell = \mathrm{End}_L(X) \otimes \mathbf{Z}/\ell$$

and we are done, taking into account Remark 1.7.

□

References

[1] S. Arias-de-Reyna, W. Gajda, S. Petersen, *Abelian varieties over finitely generated fields and the conjecture of Geyer and Jarden on torsion.* arXiv:1010.2444 [math.AG]

[2] Ch. W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras. Interscience Publishers, New York London, 1962.

[3] P. Deligne, Théorie de Hodge.II, Publ. Math. IHES 40 (1971) 5–58.
73 (1983) 337–347.

[4] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zählkorpern, Invent. Math. 73 (1983) 349–366; Erratum 75 (1984) 381.

[5] G. Faltings, 'Complements to Mordell', Chapter VI in: G. Faltings, G. Wustholz et al., Rational points. Aspects of Mathematics, E6. Friedr. Vieweg & Sohn, Braunschweig, 1984.

[6] M. Hindry, N. Ratazzi, *Points de torsion sur les variétés abéliennes de type* GSp. J. Institut Math. Jussieu. Available on CJO 05 Aug 2010 doi:10.1017/S147474801000023X ; arXiv:0911.5505 [math.NT].

[7] L. Moret-Bailly, Pinceaux de variétés abéliennes, Astérisque, vol. 129 (1985).

[8] D. Mumford, Abelian varieties, Second edition, Oxford University Press, London, 1974.

[9] N. Schappacher, *Tate's conjecture on the homomorphisms of abelian varieties.* Chapter IV in: G. Faltings, G. Wustholz et al., Rational points. Aspects of Mathematics, E6. Friedr. Vieweg & Sohn, Braunschweig, 1984.

[10] J.-P. Serre, *Sur les groupes des congruence des variétés abéliennes.* Izv. Akad. Nauk SSSR ser. matem. **28**:1 (1964), 3-18; Œuvres **II**, pp. 230–245. Springer-Verlag, Berlin, 1986.

[11] J-P. Serre, Abelian ℓ-adic representations and elliptic curves. Second edition (Addison-Wesley, New York, 1989).

[12] A.N. Skorobogatov, Yu. G. Zarhin, *A finiteness theorem for Brauer groups of abelian varieties and K3 surfaces.* J. Algebraic Geometry **17** (2008), no. 3, 481–502.

[13] J. Tate, Endomorphisms of Abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.

[14] Yu. G. Zarhin, Endomorphisms of Abelian varieties over fields of finite characteristic,. Izv. Akad. Nauk SSSR ser. matem. 39 (1975) 272–277; Math. USSR Izv. 9 (1975) 255–260.

[15] Yu. G. Zarhin, Abelian varieties in characteristic P, Mat. Zametki 19 (1976) 393–400; Mathematical Notes 19 (1976) 240–244.

[16] 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.

[17] Yu. G. Zarhin, Torsion of abelian varieties in fininite characteristic. Mat. Zametki **22** (1977), 1-11; Mathematical Notes **22** (1978), 493 - 498.

[18] 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.

[19] Yu. G. Zarhin, A. N. Parshin, *Finiteness problems in Diophantine geometry.* Amer. Math. Soc. Transl. (2) 143 (1989) 35–102; arXiv 0912.4325 [math.NT] .

[20] Yu. G. Zarhin, *Hyperelliptic Jacobians without complex multiplication in positive characteristic.* Math. Research Letters **8** (2001), 429–435.

[21] Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians*. Bull. Soc. Math. France **132** (2004), 617–634.

[22] Yu. G. Zarhin, *Homomorphisms of abelian varieties over finite fields*, pp. 315–343. In: Higher-dimensional geometry over finite fields, (D. Kaledin, Yu. Tschinkel, eds.), IOS Press, Amsterdam, 2008.

[23] Yu. G. Zarhin, *Endomorphisms of abelian varieties, cyclotomic extensions and Lie algebras*. Mathematicheskij Sbornik **201**:12 (2010), 93–102; http://mi.mathnet.ru/msb7697 ; arXiv:1001.3424 .

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

E-mail address: zarhin@math.psu.edu