J. Inst. Math. Jussieu (2013) **12**(2), 225–236
doi:10.1017/S1474748012000655 


# HOMOMORPHISMS OF ABELIAN VARIETIES OVER GEOMETRIC FIELDS OF FINITE CHARACTERISTIC

YURI G. ZARHIN

*Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA* (zarhin@math.psu.edu)

(Received 23 December 2010; accepted 30 June 2011;
first published online 16 May 2012)

*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 non-trivial endomorphisms.

*Keywords:* Abelian varieties; Tate modules; cyclotomic extensions

AMS 2010 *Mathematics subject classification:* Primary 11G10; 14K15

## 1. Introduction

Let $K$ be a field, $\bar{K}$ its algebraic closure, $\bar{K}_s \subset \bar{K}$ the separable algebraic closure of $K$, and $\mathrm{Gal}(K) = \mathrm{Gal}(\bar{K}_s/K) = \mathrm{Aut}(\bar{K}_s/K)$ 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 ring $\mathrm{End}_{\bar{K}}(X)$ of $\bar{K}$-endomorphisms of $X$ and write $\mathrm{End}^0(X)$ for the corresponding finite-dimensional semisimple $\mathbf{Q}$-algebra $\mathrm{End}(X) \otimes \mathbf{Q}$. If $Y$ is an abelian variety over $K$, then we write $\mathrm{Hom}_K(X, Y)$ for the (free) commutative group of $K$-homomorphisms from $X$ to $Y$.

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 a free $\mathbf{Z}/n\mathbf{Z}$-module of rank $2\dim(X)$ [8], which is a Galois submodule of $X(\bar{K}_s)$. We write $\bar{\rho}_{n,X}$ for the corresponding (continuous) structure homomorphism

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

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

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

If $\ell$ 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 $2\dim(X)$ and that $V_\ell(X)$ is a $\mathbf{Q}_\ell$-vector space of dimension $2\dim(X)$. Notice that there are canonical isomorphisms of $\mathrm{Gal}(K)$-modules

$$X_\ell = T_\ell(X)/\ell T_\ell(X). \tag{0}$$

There are natural algebra injections

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

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

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

It is known [13, § 1] that for given $\ell, K, X, Y$ 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 Tate himself over finite fields [13], by the author for $\mathrm{char}(K) > 2$ [14, 15], by Faltings for $\mathrm{char}(K) = 0$ [4, 5], and by Mori for $\mathrm{char}(K) = 2$ [7]. The author, Faltings and Mori 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 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, § 3, Theorem 1(b) and its proof] and [9, Proof of Corollary 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 $\ell$ the $\mathrm{Gal}(K)$-module $X_\ell$ is semisimple and the injection

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

in (1) is bijective ([16, Theorem 1.1], [18, Corollaries 5.4.3 and 5.4.5], [12, Proposition 3.4], [24, Theorem 4.4]). (See [23, Corollary 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 $\ell$ the Galois module $X_\ell$ is absolutely simple. We discuss an analogue of the isogeny theorem with 'finite coefficients' in § 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 (strictly) 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 (of positive dimension) over $\bar{\mathbf{F}}$.

https://doi.org/10.1017/S1474748012000655 Published online by Cambridge University Press

Our main results are the following four 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 the following hold.*

(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 $\ell$, the Galois module $X_\ell$ is absolutely simple.*

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

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

**Theorem 1.4.** *Let $p > 2$ be a prime, $L$ a geometric field of characteristic $p$, and $X$ and $Y$ abelian varieties of positive dimension over $L$. Suppose that* $\mathrm{End}_L(X) = \mathbf{Z}$ *and that one of the following two conditions holds.*

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

(ii) *The* $\mathrm{Gal}(L)$*-modules $X_\ell$ and $Y_\ell$ are isomorphic for infinitely many primes $\ell$.*

*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 $\mathrm{End}(X) = \mathbf{Z}$ [21, 22].

**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 centre of* $\mathrm{End}_L(X)$. *Then the following hold.*

(i) *For all primes $\ell \neq \mathrm{char}(L)$, the centre $\mathcal{Z}_{\ell,X}$ 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 $\ell$, the centre $\bar{\mathcal{Z}}_{\ell,X}$ 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 $\ell$, the commutative $\mathbf{Q}_\ell$-algebra $\mathcal{Z} \otimes \mathbf{Q}_\ell$ coincides with the centre of $\mathrm{End}_L(X) \otimes \mathbf{Q}_\ell$. It is also clear that for all but finitely many primes $\ell$ the commutative $\mathbf{F}_\ell$-algebra $\mathcal{Z}/\ell$ coincides with the centre of $\mathrm{End}_L(X) \otimes \mathbf{Z}/\ell\mathbf{Z}$. Notice also that

$$\mathrm{End}_L(X) \otimes \mathbf{Q}_\ell \subset \mathrm{End}_{\mathrm{Gal}(L)}(V_\ell(X)), \quad \mathrm{End}_L(X) \otimes \mathbf{Z}/\ell\mathbf{Z} \subset \mathrm{End}_{\mathrm{Gal}(L)}(X_\ell).$$

This implies that, for all $\ell \neq \mathrm{char}(L)$,

$$\mathcal{Z}_{\ell,X} \bigcap [\mathrm{End}_L(X) \otimes \mathbf{Q}_\ell] \subset \mathcal{Z} \otimes \mathbf{Q}_\ell,$$

and, for all but finitely many $\ell$,

$$\bar{\mathcal{Z}}_{\ell,X}\bigcap[\mathrm{End}_L(X)\otimes\mathbf{Z}/\ell]\subset\mathcal{Z}/\ell.$$

It follows that, in order to prove Theorem 1.6, it suffices to check that, for all $\ell\neq\mathrm{char}(L)$,

$$\mathcal{Z}_{\ell,X}\subset\mathrm{End}_L(X)\otimes\mathbf{Q}_\ell,$$

and, for all but finitely many $\ell$,

$$\bar{\mathcal{Z}}_{\ell,X}\subset\mathrm{End}_L(X)\otimes\mathbf{Z}/\ell.$$

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

**Theorem 1.9.** *Let $p>2$ be a prime, $L$ a geometric field of characteristic $p$, and $X$ an abelian variety of positive dimension over $L$. Then the following hold.*

(i) *For all primes $\ell\neq\mathrm{char}(L)$, the $\mathrm{Gal}(L)$-module $V_\ell(X)$ is semisimple.*

(ii) *For all but finitely many primes $\ell$, the $\mathrm{Gal}(L)$-module $X_\ell$ is semisimple.*

**Example 1.10** (counterexample). Let $K$ be a field of characteristic $p>2$ that is finitely generated over a finite field $\mathbf{F}$, and let $L=K\bar{\mathbf{F}}$.

Suppose that $X$ is a *non-supersingular* abelian variety of positive dimension over $K$ that is actually defined with all its endomorphisms over $\mathbf{F}$. (For example, one may take as $X$ an *ordinary* elliptic curve over $\mathbf{F}$.) Then all the torsion points of $X$ are defined over $\bar{\mathbf{F}}\subset L$. It follows that $\mathrm{Gal}(L)$ acts trivially on all $X_n$ and $V_\ell(X)$. In particular,

$$\mathrm{End}_{\mathrm{Gal}(L)}(V_\ell(X))=\mathrm{End}_{\mathbf{Q}_\ell}(V_\ell(X))$$

has $\mathbf{Q}_\ell$-dimension $[2\dim(X)]^2$. However, the $\mathbf{Q}$-dimension of $\mathrm{End}^0(X)$ is strictly less than $[2\dim(X)]^2$ [20, Lemma 3.1], and therefore the centralizer of $\mathrm{Gal}(L)$ in $\mathrm{End}_{\mathbf{Q}_\ell}(V_\ell(X))$ is strictly bigger than

$$\mathrm{End}^0(X)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell=\mathrm{End}(X)\otimes\mathbf{Q}_\ell=\mathrm{End}_L(X)\otimes\mathbf{Q}_\ell.$$

This implies that the analogue of the Tate conjecture does not hold for such $X$ over $L$.

The paper is organized as follows. In § 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 § 4.

## 2. Isogeny theorem with finite coefficients

**Theorem 2.1.** *Let $K$ be a field that is finitely generated over its prime subfield, and let $\mathrm{char}(K)\neq 2$. Let $X$ and $Y$ be abelian varieties over $K$. Suppose that, for infinitely many primes $\ell$, the $\mathrm{Gal}(K)$-modules $X_\ell$ and $Y_\ell$ are isomorphic. Then $X$ and $Y$ are isogenous over $K$.*

**Proof.** We may assume that $\dim(X) > 0$ and $\dim(Y) > 0$. Since, for all primes $\ell \neq \mathrm{char}(K)$,

$$2\dim(X) = \dim_{\mathbf{F}_\ell}(X_\ell), \quad 2\dim(Y) = \dim_{\mathbf{F}_\ell}(Y_\ell),$$

we obtained that $\dim(X) = \dim(Y)$. Since, for all but finitely many primes $\ell$,

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

there exist a prime $\ell \neq \mathrm{char}(K)$ and a $K$-homomorphism $u : X \to Y$ such that $u$ induces an isomorphism between $X_\ell$ and $Y_\ell$. In particular, $\ker(u)$ does not contain points of order $\ell$ on $X$, while the image $u(X)$ contains all points of order $\ell$ 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 in which, say, a number field $K$ is replaced by its infinite $\ell$-cyclotomic extension $K(\mu_{\ell^\infty})$. Some important special cases of this analogue are investigated in [6].

## 3. Representation theory

Throughout this section, $G$ is a profinite group and $H$ is 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 $\Gamma$ additively. We write $\pi : G \to \Gamma$ for the natural continuous surjective homomorphism from $G$ to $\Gamma$. If $n$ is a positive integer, then $n\Gamma$ is the closed subgroup (as the image of compact $\Gamma$ under $\Gamma \stackrel{n}{\to} \Gamma$) in $\Gamma$, whose index divides $n$; since the index is finite, $n\Gamma$ is open in $\Gamma$. 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 a 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 $G/H = \Gamma$.

(ii) $c^n$ 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 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 natural topology induced by the topology on $k$. 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 $V$ 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 and the $G_d$-module $V$ is absolutely simple. Let us split $V$ into a direct sum $V = \oplus_{i=1}^r V_i$ of isotypic $H$-modules. Clearly, $G$ permutes the $V_i$; the simplicity of the $G$-module $V$ implies that $G$ acts on $\{V_1, \ldots, V_r\}$ transitively. In particular, all the $V_i$ have the same dimension, and therefore

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

in particular, $r|d$. Clearly, the action of $G$ on $\{V_1, \ldots, V_r\}$ 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 $G/G_d$; i.e., each $V_i$ is a $G_d$-submodule. Since the $G_d$-module $V$ is (absolutely) simple, $V = V_i$. In other words, the $H$-module $V$ is isotypic. Then the centralizer

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

is a simple $k$-algebra. Let $k'$ be the centre 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 $[k' : k]|d$. On the other hand, since $H$ is normal in $G$,

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

Clearly, the centre $k'$ 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 that

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

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 $G/G_d$, and therefore

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

since $\mathrm{End}_{G_d}(V) = k$, we conclude that $k' \subset k$, and therefore $k' = k$. This means that $D$ is a central simple $k$-algebra. Let $t := \dim_k(D)$. We need to prove that $t = 1$. Suppose that $t > 1$, pick a generator in $\Gamma$, 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 the Skolem–Noether theorem, there exists an element $z \in D^*$ such that

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

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 $W_1(\chi)$. 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

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

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 each of its non-zero elements $W_1 \to W_2$ is an isomorphism of $H$-modules). Therefore the action of $G$ on one-dimensional $\mathrm{Hom}_H(W_1, W_2)$ is defined by a certain continuous character $\chi : G \to k^*$, which obviously kills $H$, so we may view $\chi$ as a continuous character

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

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

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

https://doi.org/10.1017/S1474748012000655 Published online by Cambridge University Press

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

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

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 $\chi^{Nd}$ is trivial.*

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

**Proof.** By a variant of Clifford's lemma [24, 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 $G$,

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

Let $Z$ be the centre 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,

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

and the $k$-algebra $Z$ has exactly $r$ minimal idempotents (the identity elements $e_i$ of the $k_i$. Clearly, group $\mathrm{Aut}_k(Z)$ of $k$-linear automorphisms of $Z$ permutes the $e_i$, 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 $\prod_{i=1}^r [k_i : k] \leqslant d^d$. It follows that $\mathrm{Aut}_k(Z)$ is a finite group, whose order does not exceed $d! \cdot d^d$. This implies that $n := (d! \cdot d^d)!$ is divisible by the order of $\mathrm{Aut}_k(Z)$.

On the other hand, clearly,

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

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

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

which kills $H$, because

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

Clearly, $\phi$ 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 $\mathbf{F} = \mathbf{F}_p$ 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

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

Let us put

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

Since $\bar{\mathbf{F}}/\mathbf{F}_p$ 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 $\mathrm{Gal}(\bar{\mathbf{F}}/\mathbf{F}_p)$; since the latter is procyclic, $\Gamma$ 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

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

If $\ell$ is a prime different from $p$, we write

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

for the cyclotomic characters that define the Galois action on all $\ell$th roots of unity (respectively, all $\ell$-power roots of unity). Clearly,

$$\bar{\chi}_\ell=\chi_\ell \bmod \ell. \tag{6}$$

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

(i) The character $\chi_\ell$ has infinite multiplicative order.

(ii) If $N$ is a positive integer, then, for all but finitely many primes $\ell$, the character $\bar{\chi}_\ell^N$ is non-trivial.

Since every $K_n$ is finitely generated over $\mathbf{F}_p$, the abelian variety $X$ over $K_n$ 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 $\ell$, the $G_n$-module $X_\ell$ 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 $X_\ell$ is absolutely simple for all but finitely many primes $\ell$.

**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 $\ell\neq p$; in particular,

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

https://doi.org/10.1017/S1474748012000655 Published online by Cambridge University Press

On the other hand, (b) tells us that, for all but finitely many $\ell$, the $G_{2d}$-module $X_\ell$ 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, 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, § 1.3], [24, Proof of Proposition 2.2] implies that $\det(V_\ell(X))$ and $\det(V_\ell(Y))$ are one-dimensional $G$-modules defined by the character $\chi_\ell^d$. Now, applying Lemma 3.4, we conclude that 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 the corollary to Lemma 3.4 that $\chi^{2d}$ is trivial. This implies that $\chi$ 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 are also isogenous over $L$. This proves (i).

Similar arguments work in 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 $\chi_\ell^d$, because

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

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 that the $G$-module $Y_\ell$ 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 the 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 $X_\ell$ and $Y_\ell$ are isomorphic for infinitely many $\ell$. 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 centre 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 $n$ that depends only on $2\dim(X)$ such that, for all but finitely many primes $\ell$, the centre 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. □

**Proof of Theorem 1.9.** Recall that $H = \mathrm{Gal}(L)$ is a *normal* subgroup in $G = \mathrm{Gal}(K)$. By the variant of Clifford's lemma [24, Lemma 3.4], the semisimplicity of the $\mathrm{Gal}(K)$-modules $V_\ell(X)$ and $X_\ell$ implies that they are semisimple $\mathrm{Gal}(L)$-modules. □

## References


1. S. Arias-de-Reyna, W. Gajda and 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 and 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.
4. G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zählkorpern, *Invent. Math.* **73** (1983), 349–366 (erratum: *Invent. Math.* **75** (1984), 381).
5. G. Faltings, Complements to Mordell, in *Rational points* (ed. G. Faltings and G. Wüstholz *et al.*), Aspects of Mathematics, Volume E6, Chapter VI (Friedr. Vieweg & Sohn, Braunschweig, 1984).
6. M. Hindry and 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* **129** (1985).
8. D. Mumford, *Abelian varieties*, 2nd edn (Oxford University Press, London, 1974).
9. N. Schappacher, Tate's conjecture on the homomorphisms of abelian varieties, in *Rational points* (ed. G. Faltings and G. Wüstholz *et al.*). Aspects of Mathematics, Volume E6, Chapter IV (Friedr. Vieweg & Sohn, Braunschweig, 1984).
10. J.-P. Serre, Sur les groupes des congruence des variétés abéliennes, *Izv. Akad. Nauk SSSR Ser. Mat.* **28**(1) (1964), 3–18 Oeuvres II, pp. 230–245 (Springer-Verlag, Berlin, 1986).
11. J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 2nd edn (Addison-Wesley, New York, 1989).
12. A. N. Skorobogatov and Y. G. Zarhin, A finiteness theorem for Brauer groups of abelian varieties and K3 surfaces, *J. Algebraic Geom.* **17**(3) (2008), 481–502.
13. J. Tate, Endomorphisms of Abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.
14. Y. G. Zarhin, Endomorphisms of Abelian varieties over fields of finite characteristic, *Izv. Akad. Nauk SSSR Ser. Mat.* **39** (1975) 272–277; *Math. USSR Izv.* **9** (1975) 255–260.
15. Y. G. Zarhin, Abelian varieties in characteristic $P$, *Mat. Zametki* **19** (1976) 393–400; *Math. Notes* **19** (1976) 240–244.
16. Y. G. Zarhin, Endomorphisms of Abelian varieties and points of finite order in characteristic $P$, *Mat. Zametki* **21** (1977) 737–744; *Math. Notes* **21** (1978) 415–419.
17. Y. G. Zarhin, Torsion of abelian varieties in finite characteristic, *Mat. Zametki* **22** (1977), 1–11; *Math. Notes* **22** (1978), 493–498.

18. Y. 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. Y. G. Zarhin and A. N. Parshin, Finiteness problems in diophantine geometry, *Amer. Math. Soc. Transl.* **143**(2) (1989), 35–102 (arXiv:0912.4325 [math.NT]).
20. Y. G. Zarhin, Hyperelliptic Jacobians without complex multiplication, *Math. Res. Lett.* **7** (2000), 123–132.
21. Y. G. Zarhin, Hyperelliptic Jacobians without complex multiplication in positive characteristic, *Math. Res. Lett.* **8** (2001), 429–435.
22. Y. G. Zarhin, Non-supersingular hyperelliptic Jacobians, *Bull. Soc. Math. France* **132** (2004), 617–634.
23. Y. G. Zarhin, Homomorphisms of abelian varieties over finite fields, in *Higher-dimensional geometry over finite fields* (ed. D. Kaledin and Yu. Tschinkel ), pp. 315–343 (IOS Press, Amsterdam, 2008).
24. Y. G. Zarhin, Endomorphisms of abelian varieties, cyclotomic extensions and Lie algebras. *Math. Sb.* **201**(12) (2010), 93–102; *Sb. Math.* **201**(12) (2010), 1801–1810.