Almost isomorphic abelian varieties

Yuri G. Zarhin

November 3, 2016

Abstract. We study abelian varieties over finitely generated fields K of characteristic zero, whose ℓ-adic Tate modules are isomorphic as Galois modules for all primes ℓ.

1 Introduction

Let K be a field, $\bar{K}$ its separable algebraic closure, $G_K = \mathrm{Aut}(\bar{K}/K)$ the absolute Galois group of K. If A is an abelian variety over a field K then we write $\mathrm{End}(A)$ for its ring of all K-endomorphisms and $\mathrm{End}^0(A)$ for the corresponding (finite-dimensional semisimple) $\mathbb{Q}$-algebra $\mathrm{End}(A) \otimes \mathbb{Q}$.

If ℓ is a prime different from $\mathrm{char}(K)$ then we write $T_\ell(A)$ for the $\mathbb{Z}_\ell$-Tate module of A [7, 9], which is a free $\mathbb{Z}_\ell$-module of rank $2\dim(A)$ provided with the natural continuous group homomorphism

$$\rho_{\ell,A} : G_K \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A))$$

and the $\mathbb{Z}_\ell$-ring embedding

$$e_l : \mathrm{End}(A) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)).$$

The image of $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ commutes with $\rho_{\ell,A}(G_K)$. Tensoring by $\mathbb{Q}_\ell$ (over $\mathbb{Z}_\ell$), we obtain the $\mathbb{Q}_\ell$-Tate module of A

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

which is a $2\dim(A)$-dimensional $\mathbb{Q}_\ell$-vector space containing

$$T_\ell(A) = T_\ell(A) \otimes 1$$

as a $\mathbb{Z}_\ell$-lattice. We may view $\rho_{\ell,A}$ as an ℓ-adic representation [11]

$$\rho_{\ell,A} : G_K \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$$

and extend e_ℓ by $\mathbb{Q}_\ell$-linearity to the embedding of $\mathbb{Q}_\ell$-algebras

$$\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}(A) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)),$$

which we still denote by e_ℓ. Further we will identify $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ with its image in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. This provides $V_\ell(A)$ with the natural structure of G_K-module; in addition, $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a $\mathbb{Q}_\ell$-(sub)algebra of endomorphisms of the Galois module $V_\ell(A)$. In other words,

$$\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \subset \mathrm{End}_{G_K}(V_\ell(A)).$$

Let K be a field of characteristic zero that is finitely generated over $\mathbb{Q}$. Suppose we are given an abelian variety A of positive dimension over K. Let B be an abelian variety over K such that the $\mathbb{Z}_\ell$-Tate modules of A and B are isomorphic as Galois modules for all ℓ. (We call such A and B *almost isomorphic*.) In this paper we discuss the structure of the corresponding right $\mathrm{End}(A)$-module $\mathrm{Hom}(A, B)$. Using a theorem of Faltings [4, 5] (conjectured by Tate [12]), we prove that $\mathrm{Hom}(A, B)$ is a locally free module of rank 1. In addition, using a special case of Serre's tensor construction ([2, Sect. 7], [3, Sect. 1.7.4]), we prove that there is a natural bijection between isomorphism classes of locally free modules of rank 1 over $\mathrm{End}(A)$ and isomorphism classes of abelian varieties B over K, whose Tate modules are isomorphic to ones of A.

The paper is organized as follows. Section 2 deals with isogenies of abelian varieties and corresponding homomorphisms of their Tate modules. In Section 3 we discuss locally free modules of rank 1 over orders in semisimple $\mathbb{Q}$-algebras. In Section 4 we apply results of Section 3 to a construction of almost isomorphic abelian varieties.

2 Isogenies

If ℓ is a prime then we write $\mathbb{Z}_{(\ell)}$ for the subring in $\mathbb{Q}$ that consists of all the rational numbers, whose denominators are prime to ℓ. We have

$$\mathbb{Z} \subset \mathbb{Z}_{(\ell)} = \mathbb{Z}_\ell \bigcap \mathbb{Q} \subset \mathbb{Z}_\ell.$$

(Here the intersection is taken in $\mathbb{Q}_\ell$.) In addition, if m is a positive integer that is prime to ℓ then

$$\mathbb{Z} \subset \mathbb{Z}[1/m] \subset \mathbb{Z}_{(\ell)} \subset \mathbb{Q}.$$

The intersection of all $\mathbb{Z}_{(\ell)}$'s (in $\mathbb{Q}$) coincides with $\mathbb{Z}$.

Let K be an arbitrary field. If $\ell \ne \mathrm{char}(K)$ and X is an abelian variety over K then we write $X[\ell]$ for the kernel of multiplication by ℓ in $X(\bar{K})$. It is well known that $X[\ell]$ is a finite G_K-submodule in $X(\bar{K})$ of order $\ell^{2\dim(X)}$ and there is a natural isomomorphism of G_K-modules $X[\ell] \cong T_\ell(X)/\ell T_\ell(X)$.

Lemma 2.1 *Let A and B be abelian varieties of positive dimension over K.*

(a) If A and B are isogenous over K then the right $\mathrm{End}(A)\otimes\mathbb{Q}$-module $\mathrm{Hom}(A,B)\otimes\mathbb{Q}$ is free of rank 1. In addition, one may choose as a generator of $\mathrm{Hom}(A,B)\otimes\mathbb{Q}$ any isogeny $\phi : A \to B$.

(b) The following conditions are equivalent.

(i) The right $\mathrm{End}(A)\otimes\mathbb{Q}$-module $\mathrm{Hom}(A,B)\otimes\mathbb{Q}$ is free of rank 1.

(ii) $\dim(A) \le \dim(B)$ and there exists a $\dim(A)$-dimensional abelian K-subvariety $B_0 \subset B$ such that A and B_0 are isogenous over K and

$$\mathrm{Hom}(A,B) = \mathrm{Hom}(A,B_0).$$

In particular, the image of every K-homomorphism of abelian varieties $A \to B$ lies in B_0.

(c) If the equivalent conditions (i) and (ii) hold and $\dim(B) \le \dim(A)$ then $\dim(A) = \dim(B)$, $B = B_0$, and A and B are isogenous over K.

Proof. (a) is obvious.

Suppose (bii) is true. Let us pick an *isogeny* $\phi : A \to B_0$. It follows that $\mathrm{Hom}(A,B_0)\otimes\mathbb{Q} = \phi\,\mathrm{End}^0(A)$ is a free right $\mathrm{End}^0(A)$-module of rank 1 generated by ϕ. Now (bi) follows from the equality

$$\mathrm{Hom}(A,B)\otimes\mathbb{Q} = \mathrm{Hom}(A,B_0)\otimes\mathbb{Q}.$$

Suppose that (bi) is true. We may choose a homomorphism of abelian varieties $\phi : A \to B$ as a generator (basis) of the free right $\mathrm{End}(A)\otimes\mathbb{Q}$-module $\mathrm{Hom}(A,B)\otimes\mathbb{Q}$. In other words, for every homomorphism of abelian varieties $\psi : A \to B$ there are $u \in \mathrm{End}(A)$ and a *nonzero* integer n such that $n\psi = \phi u$. In addition, for each *nonzero* $u \in \mathrm{End}(A)$ the composition ϕu is a *nonzero* element of $\mathrm{Hom}(A, B)$. Clearly, $B_0 := \phi(A) \subset B$ is an abelian K-subvariety of B with $\dim(B_0) \le \dim(A)$. We have

$$n\psi(A) = \phi u(A) \subset \psi(A) \subset B_0.$$

It follows that the identity component of $\psi(A)$ lies in B_0. Since $\psi(A)$ is a (connected) abelian K-subvariety of B, we have $\psi(A) \subset B_0$. This proves that $\mathrm{Hom}(A, B) = \mathrm{Hom}(A, B_0)$. On the other hand, if $\dim(B_0) = \dim(A)$ then $\phi : A \to B_0$ is an *isogeny* and we get (bii) under our additional assumption. If $\dim(B_0) < \dim(A)$ then $\ker(\phi)$ has positive dimension that is strictly less than $\dim(A)$. By the Poincaré complete reducibility theorem [7], there is an endomorphism $u_0 \in \mathrm{End}(A)$ such that the image $u_0(A)$ coincides with the identity component of $\ker(\phi)$; in particular, $u_0 \neq 0$, $u_0(A) \subset \ker(\phi)$. This implies that $\phi u_0 = 0$ in $\mathrm{Hom}(A, B)$ and we get a contradiction, which proves (bii).

(c) follows readily from (bii). □

Lemma 2.2 *Suppose that A, B, C are abelian varieties over K of positive dimension that are mutually isogenous over K. We view* $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$ *and* $\mathrm{Hom}(A, C) \otimes \mathbb{Q}$ *as right* $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$*-modules. Then the natural map*

$$m_{B,C} : \mathrm{Hom}(B, C) \otimes \mathbb{Q} \to \mathrm{Hom}_{\mathrm{End}^0(A)}(\mathrm{Hom}(A, B) \otimes \mathbb{Q}, \mathrm{Hom}(A, C) \otimes \mathbb{Q})$$

that associates to $\tau : B \to C$ a homomorphism of right $\mathrm{End}(A) \otimes \mathbb{Q}$*-modules*

$$m_{B,C}(\tau) : \mathrm{Hom}(A, B) \otimes \mathbb{Q} \to \mathrm{Hom}(A, C) \otimes \mathbb{Q}, \psi \mapsto \tau\psi$$

is a group isomorphism.

Proof. Clearly, $m_{B,C}$ is injective. In order to check the surjectiveness, notice that the statement is clearly *invariant by isogeny*, so we can assume that $B = A$ and $C = A$, in which case it is obvious. □

Now till the end of this paper we assume that K is a field of characteristic zero that is finitely generated over $\mathbb{Q}$, and A and B are abelian varieties of positive dimension over K. By a theorem of Faltings [4, 5],

$$\mathrm{Hom}_{G_K}(T_\ell(A), T_\ell(B)) = \mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell. \qquad (*)$$

Lemma 2.3 *Let ℓ be a prime. Then the following conditions are equivalent.*

(i) There is an isogeny $\phi_\ell : A \to B$, whose degree is prime to ℓ.

(ii) The Tate modules $T_\ell(A)$ and $T_\ell(B)$ are isomorphic as $\mathbb{Z}_\ell[G_K]$-Galois modules.

If the equivalent conditions (i) and (ii) hold then the right $\mathrm{End}(A) \otimes \mathbb{Z}_{(\ell)}$-*module* $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_{(\ell)}$ *is free of rank* 1 *and the right* $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$-*module* $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$ *is free of rank* 1

Proof. (i) implies (ii). Indeed, let $\phi_\ell : A \to B$ be an isogeny such that its degree $d := \deg(\phi_\ell)$ is prime to ℓ. Then there exists an isogeny $\varphi_\ell : B \to A$ such that $\phi_\ell\varphi_\ell$ is multiplication by d in B and $\varphi_\ell\phi_\ell$ is multiplication by d in A. This implies that ϕ_ℓ induces an G_K-equivariant isomorphism of the $\mathbb{Z}_\ell$-Tate modules of A and B.

Suppose that (ii) holds. Since the rank of the free $\mathbb{Z}_\ell$-module $T_\ell(A)$ (resp. $T_\ell(B)$) is $2\dim(A)$ (resp. $2\dim(B)$), we conclude that $2\dim(A) = 2\dim(B)$, i.e. $\dim(A) = \dim(B)$. By the theorem of Faltings (*), there is an isomorphism of the $\mathbb{Z}_\ell$-Tate modules of A and B that lies in $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$. Since $\mathrm{Hom}(A, B)$ is dense in $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$ in the ℓ-adic topology, and the set of isomorphisms $T_\ell(A) \cong T_\ell(B)$ is open in $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$, there is $\phi_\ell \in \mathrm{Hom}(A, B)$ that induces an isomorphism $T_\ell(A) \cong T_\ell(B)$. Clearly, $\ker(\phi_\ell)$ does not contain points of order ℓ and therefore is finite. This implies that ϕ_ℓ is an isogeny, whose degree is prime to ℓ. This proves (i).

In order to prove the last assertion of Lemma 2.3, one has only to observe that $\phi_\ell \in \mathrm{Hom}(A, B) \subset \mathrm{Hom}(A, B) \otimes \mathbb{Z}_{(\ell)} \subset \mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$ is a generator of the (obviously) free right $\mathbb{Z}_{(\ell)}$-module $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_{(\ell)}$ and of the free right $\mathbb{Z}_\ell$-module $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$. □

We say that A and B are *almost isomorphic* if for *all primes* ℓ the equivalent conditions (i) and (ii) of Lemma 2.3 hold. Clearly, if A and B are isomorphic over K then they are almost isomorphic. It is also clear that if A and B are almost isomorphic then they are isogenous over K. Obviously, the property of being almost isomorphic is an equivalence relation on the set of (nonzero) abelian varieties over K.

Corollary 2.4 *Suppose that A and B are almost isomorphic. Then A and B are isomorphic over K if and only if* $\mathrm{Hom}(A, B)$ *is a free* $\mathrm{End}(A)$-*modules of rank* 1. *In particular, if* $\mathrm{End}(A)$ *is a principal ideal domain (for example,* $\mathrm{End}(A) = \mathbb{Z}$*) then every abelian variety over K, which is almost isomorphic to A, is actually isomorphic to A.*

Proof. Suppose $\mathrm{Hom}(A, B)$ is a free $\mathrm{End}(A)$-module, i.e., there is a homomorphism of abelian varieties $\phi : A \to B$ such that $\mathrm{Hom}(A, B) = \phi\,\mathrm{End}(A)$. We know that for any prime ℓ there is an isogeny $\phi_\ell : A \to B$ of degree prime to ℓ. (In particular, $\dim(A) = \dim(B)$.) Therefore there is $u_\ell \in \mathrm{End}(A)$ with $\phi_\ell = \phi u_\ell$. In particular, $\phi_\ell(A) \subset \phi(A)$ and $\deg(\phi_\ell)$ is divisible by $\deg(\phi)$. Since $\phi_\ell(A) = B$ and $\deg(\phi_\ell)$ is prime to ℓ, we conclude that $\phi(A) = B$ (i.e., ϕ is an isogeny) and $\deg(\phi)$ is prime to ℓ. Since the latter is true for all primes ℓ, we conclude that $\deg(\phi) = 1$, i.e., ϕ is an isomorphism.

Conversely, if $A \cong B$ then $\mathrm{Hom}(A, B)$ is obviously a free $\mathrm{End}(A)$-module generated by an isomorphism between A and B.

The last assertion of Corollary follows from the well-known fact that every finitely generated module without torsion over a principal ideal domain is free. □

Remark The special case of Corollary 2.4 when $\mathrm{End}(A) = \mathbb{Z}$ was actually done in [10, second paragraph of p. 1205].

The next statement is a generalization of Corollary 2.4.

Corollary 2.5 *Suppose that A, B, C are abelian varieties of positive dimension over K that are almost isomorphic to each other.*

Then B and C are isomorphic over K if and only if the right $\mathrm{End}(A)$*-modules* $\mathrm{Hom}(A, B)$ *and* $\mathrm{Hom}(A, C)$ *are isomorphic.*

Proof. We know that all A, B, C are mutually isogenous over K. Let us choose an isogeny $\phi : B \to C$. We are given an isomorphism $\delta : \mathrm{Hom}(A, B) \cong \mathrm{Hom}(A, C)$ of right $\mathrm{End}(A)$-modules that obviously extends by $\mathbb{Q}$-linearity to the isomorphism $\mathrm{Hom}(A, B) \otimes \mathbb{Q} \to \mathrm{Hom}(A, C) \otimes \mathbb{Q}$ of right $\mathrm{End}(A) \otimes \mathbb{Q}$-modules, which we continue to denote by δ. By Lemma 2.2, there exists $\tau_0 \in \mathrm{Hom}(B, C) \otimes \mathbb{Q}$ such that $\delta = m_{B,C}(\tau_0)$, i.e.,

$$\delta(\psi) = \tau_0 \psi \ \forall \psi \in \mathrm{Hom}(A, B) \otimes \mathbb{Q}.$$

There exists a positive integer n such that $\tau = n\tau_0 \in \mathrm{Hom}(B, C)$ and τ is *not* divisible in $\mathrm{Hom}(B, C)$. This implies that

$$n \cdot \mathrm{Hom}(A, C) = n\delta(\mathrm{Hom}(A, B)) = n\tau_0 \mathrm{Hom}(A, B) = \tau \mathrm{Hom}(A, B).$$

Since B and C are almost isomorphic, for each ℓ there is an isogeny $\phi_\ell : B \to C$ of degree prime to ℓ. Since $n\phi_\ell \in \tau\mathrm{Hom}(A, B)$, we conclude that τ is an isogeny and $\deg(\tau)$ is prime to ℓ if ℓ does *not* divide n. We need to prove that τ is an isomorphism. Suppose it is not, then there is a prime ℓ that divides $\deg(\tau)$ and therefore divides n. We need to arrive to a contradiction. Since A and B are almost isomorphic, there is an isogeny $\psi_\ell : A \to B$ of degree prime to ℓ. We have $\tau\psi_\ell \in n \cdot \mathrm{Hom}(A, C) \subset \ell \cdot \mathrm{Hom}(A, C)$. This implies that τ kills *all* points of order ℓ on B and therefore is divisible by ℓ in $\mathrm{Hom}(B, C)$, which is not the case. This gives us the desired contradiction. □

Remark Let $\mathcal{Z}(A)$ (resp. $\mathcal{Z}(B)$) be the the center of $\mathrm{End}(A)$ (resp. $\mathrm{End}(B)$). Then $\mathcal{Z}(A)_{\mathbb{Q}} := \mathcal{Z}(A) \otimes \mathbb{Q}$ (resp. $\mathcal{Z}(B)_{\mathbb{Q}} := \mathcal{Z}(B) \otimes \mathbb{Q}$) is the center of $\mathrm{End}(A) \otimes \mathbb{Q}$ (resp. $\mathrm{End}(B) \otimes \mathbb{Q}$) and for all primes ℓ the $\mathbb{Z}_{(\ell)}$-subalgebra

$$\mathcal{Z}(A)_{(\ell)} := \mathcal{Z}(A) \otimes \mathbb{Z}_{(\ell)} \subset \mathcal{Z}(A)_{\mathbb{Q}} \subset \mathrm{End}(A) \otimes \mathbb{Q}$$

(resp. the $\mathbb{Z}_{(\ell)}$-subalgebra

$$\mathcal{Z}(B)_{(\ell)} := \mathcal{Z}(B) \otimes \mathbb{Z}_{(\ell)} \subset \mathcal{Z}(B)_{\mathbb{Q}} \subset \mathrm{End}(B) \otimes \mathbb{Q})$$

is the center of $\mathrm{End}(A) \otimes \mathbb{Z}_{(\ell)}$ (resp. of $\mathrm{End}(B) \otimes \mathbb{Z}_{(\ell)}$). Every K-isogeny $\phi : A \to B$ gives rise to an isomorphism of $\mathbb{Q}$-algebras

$$i_\phi : \mathrm{End}(A) \otimes \mathbb{Q} \cong \mathrm{End}(B) \otimes \mathbb{Q}, \ u \mapsto \phi u \phi^{-1},$$

such that $i_\phi(\mathcal{Z}(A)_{\mathbb{Q}}) = \mathcal{Z}(B)_{\mathbb{Q}}$ and the restriction $i_{\mathcal{Z}} : \mathcal{Z}(A)_{\mathbb{Q}} \cong \mathcal{Z}(B)_{\mathbb{Q}}$ of i_ϕ to the center(s) does *not* depend on a choice of ϕ [14]. If $\phi_\ell : A \to B$ is a K-isogeny of degree prime to ℓ then $i_{\phi_\ell}(\mathrm{End}(A) \otimes \mathbb{Z}_{(\ell)}) = \mathrm{End}(B) \otimes \mathbb{Z}_{(\ell)}$ and therefore $i_{\mathcal{Z}}(\mathcal{Z}(A)_{(\ell)})) = \mathcal{Z}(B)_{(\ell)}$. This implies that if A and B are *almost isomorphic* then $i_{\mathcal{Z}}(\mathcal{Z}(A))$ coincides with $\mathcal{Z}(B)$ and therefore $i_{\mathcal{Z}}$ defines a canonical isomorphism of commutative rings $\mathcal{Z}(A) \cong \mathcal{Z}(B)$. In particular, if $\mathrm{End}(A)$ is commutative then $\mathrm{End}(B)$ is also commutative (because $\mathrm{End}(A) \otimes \mathbb{Q}$ and $\mathrm{End}(B) \otimes \mathbb{Q}$ are isomorphic) and there is a canonical ring isomorphisms $\mathrm{End}(A) \cong \mathrm{End}(B)$.

3 Locally free modules of rank 1

Throughout this section, Λ is a ring with 1 that, viewed as an additive group, is a free $\mathbb{Z}$-module of finite positive rank. In addition, we assume that the finite-dimensional $\mathbb{Q}$-algebra $\Lambda_{\mathbb{Q}} := \Lambda \otimes \mathbb{Q}$ is *semisimple*. We write Λ_ℓ (resp. $\Lambda_{(\ell)}$) for the $\mathbb{Z}_\ell$-algebra $\Lambda \otimes \mathbb{Z}_\ell$ (resp. for the $\mathbb{Z}_{(\ell)}$-algebra $\Lambda \otimes \mathbb{Z}_{(\ell)}$). We have

$$\Lambda = \Lambda \otimes 1 \subset \Lambda_{(\ell)} \subset \Lambda_{\mathbb{Q}} \subset \Lambda \otimes \mathbb{Q}_\ell,$$

$$\Lambda \subset \Lambda_{(\ell)} \subset \Lambda_\ell \subset \Lambda \otimes \mathbb{Q}_\ell.$$

In addition, the intersection of Λ_ℓ and $\Lambda_{\mathbb{Q}}$ (in $\Lambda \otimes \mathbb{Q}_\ell$) coincides with $\Lambda_{(\ell)}$.

Let M be an *arbitrary* free commutative group of finite positive rank that is provided with a structure of a right Λ-module. We write $M_{\mathbb{Q}}$ for the right $\Lambda_{\mathbb{Q}}$-module $M \otimes \mathbb{Q}$, M_ℓ for the right Λ_ℓ-module $M \otimes \mathbb{Z}_\ell$ and $M_{(\ell)}$ for the right $\Lambda_{(\ell)}$-module $M \otimes \mathbb{Z}_{(\ell)}$. We have

$$M = M \otimes 1 \subset M_{(\ell)} \subset M_{\mathbb{Q}} \subset M \otimes \mathbb{Q}_\ell,$$

$$M \subset M_{(\ell)} \subset M_\ell \subset M \otimes \mathbb{Q}_\ell.$$

In addition, the intersection of M_ℓ and $M_{\mathbb{Q}}$ (in $M \otimes \mathbb{Q}_\ell$) coincides with $M_{(\ell)}$.

Definition. We say that M is a *locally free right* Λ*-module of rank* 1 if for all primes ℓ the right Λ_ℓ-module M_ℓ is free of rank 1. (See [6].)

Theorem 3.1 *Let M be a locally free right Λ-module of rank* 1*. Then it enjoys the following properties.*

(i) M is a projective Λ-module. More precisely, M is isomorphic to a direct summand of a free right Λ-module of rank 2*.*

(ii) The right $\Lambda_{\mathbb{Q}}$-module $M_{\mathbb{Q}}$ is free of rank 1*.*

(iii) The right $\Lambda_{(\ell)}$-module $M_{(\ell)}$ is free of rank 1 *for all primes ℓ.*

Proof. Let $J(\Lambda_{\mathbb{Q}})$ be the (multiplicative) *idele group* of $\Lambda_{\mathbb{Q}}$, i.e., the group of invertible elements of the *adele ring* of $\Lambda_{\mathbb{Q}}$ [6, p. 114]. (In the notation of [6, Sect. 2], $\mathfrak{o} = \mathbb{Z}$, $K = \mathbb{Q}, A = \Lambda_{\mathbb{Q}}$, $\mathfrak{U} = \Lambda$.) To each $\alpha \in J(\Lambda_{\mathbb{Q}})$ corresponds a certain right Λ-submodule $\alpha\Lambda \subset \Lambda_{\mathbb{Q}}$ that is a locally free Λ-module of rank 1 and a $\mathbb{Z}$-lattice of maximal rank in the $\mathbb{Q}$-vector space $\Lambda_{\mathbb{Q}}$, i.e., the natural homomorphism of $\mathbb{Q}$-vector spaces $\alpha\Lambda \otimes \mathbb{Q} \to \Lambda_{\mathbb{Q}}$ is an isomorphism [6, p. 114]. This implies that $(\alpha\Lambda)_{\mathbb{Q}}$ is a free $\Lambda_{\mathbb{Q}}$-module of rank 1. In addition, the direct sum $\alpha\Lambda \oplus \alpha^{-1}\Lambda$ is a free right Λ-module of rank 2 [6, Th. 1 on pp. 114–115]. This implies that $\alpha\Lambda$ is isomorphic to a direct summand of a rank 2 free module; in particular, it is projective. By the same Theorem 1 of

[6], every right locally free Λ-module M of rank 1 is isomorphic to $\alpha\Lambda$ for a suitable α. This proves (i) and (ii).

Let f_0 be a generator of the free $\Lambda_{\mathbb{Q}}$-module $M_{\mathbb{Q}}$ of rank 1. Multiplying f_0 by a sufficiently divisible positive integer, we may and will assume that $f_0 \in M = M \otimes 1 \subset M_{\mathbb{Q}}$. Clearly, the right $\Lambda \otimes \mathbb{Q}_\ell$-module

$$M \otimes \mathbb{Q}_\ell = M_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = M_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

is free of rank 1 for all primes ℓ and f_0 is also a generator of $M \otimes \mathbb{Q}_\ell$. It is also clear that every generator f_ℓ of the Λ_ℓ-module M_ℓ is a generator of the $\Lambda \otimes \mathbb{Q}_\ell$-module $M \otimes \mathbb{Q}_\ell$. We claim that there is a generator f_ℓ that lies in M. Indeed, with respect to the ℓ-adic topology, the subset

$$M = M \otimes 1 \subset M \otimes \mathbb{Z}_\ell = M_\ell$$

is dense in M_ℓ while the set of generators of the free Λ_ℓ-module M_ℓ is open, because the group of units $(\Lambda_\ell)^*$ is open in Λ_ℓ. This implies that there exists a (nonzero) generator $f_\ell \in M \subset M_\ell$ of the Λ_ℓ-module M_ℓ. Recall that f_ℓ is also a generator of the free $\Lambda \otimes \mathbb{Q}_\ell$-module $M \otimes \mathbb{Q}_\ell$. This implies that there exists $\mu_0 \in (\Lambda \otimes \mathbb{Q}_\ell)^*$ such that $f_\ell = f_0\mu_0 \in M \otimes \mathbb{Q}_\ell$. On the other hand, since f_ℓ lies in the free rank 1 $\Lambda_{\mathbb{Q}}$-module $M_{\mathbb{Q}} = f_0\Lambda_{\mathbb{Q}}$, we have $\mu_0 \in \Lambda_{\mathbb{Q}}$. This implies that μ_0 is *not* a zero divisor in the finite-dimensional $\mathbb{Q}$-algebra $\Lambda_{\mathbb{Q}}$ (because it is invertible in $\Lambda \otimes \mathbb{Q}_\ell$) and therefore lies in $\Lambda_{\mathbb{Q}}^*$. It follows that f_ℓ is also a generator of the free $\Lambda_{\mathbb{Q}}$-module $M_{\mathbb{Q}}$ of rank 1.

We want to prove that $M_{(\ell)} = f_\ell[\Lambda \otimes \mathbb{Z}_{(\ell)}]$. (This would prove that $M_{(\ell)}$ is a free right $\Lambda_{(\ell)}$-module of rank 1 with the generator f_ℓ.) For each $x \in M_{(\ell)}$ there exists a unique $\lambda \in \Lambda_\ell$ with $x = f\lambda$. We need to prove that $\lambda \in \Lambda_{(\ell)}$. Notice that $x \in M_{(\ell)} \subset M_{\mathbb{Q}}$. Since f_ℓ is a generator of the free $\Lambda_{\mathbb{Q}}$-module $M_{\mathbb{Q}}$, there exists exactly one $\mu_0 \in \Lambda_{\mathbb{Q}}$ such that $x = f\mu_0$. We get the equalities $f\mu_0 = x = f\mu$ in $M \otimes \mathbb{Q}_\ell$.

Since f_ℓ is a generator of the free $\Lambda \otimes \mathbb{Q}_\ell$-module $M \otimes \mathbb{Q}_\ell$, we get $\mu = \mu_0$. Since $\Lambda_{(\ell)}$ coincides with intersection of Λ_ℓ and $\Lambda_{\mathbb{Q}}$ in $\Lambda \otimes \mathbb{Q}_\ell$, we conclude that $\mu = \mu_0 \in \Lambda_{(\ell)}$ and therefore $x \in f[\Lambda \otimes \mathbb{Z}_{(\ell)}]$. This implies that $M_{(\ell)}$ is a free right $\Lambda_{(\ell)}$ module of rank 1, which proves (iii). □

Corollary 3.2 *Let M be a free commutative group of finite positive rank that is provided with a structure of a right Λ-module. Then M is a locally free Λ-module of rank 1 if and only if the right $\Lambda_{(\ell)}$-module $M_{(\ell)}$ is free of rank 1 for all primes ℓ.*

Proof. Clearly, if $M_{(\ell)}$ is a free right $\Lambda_{(\ell)}$-module of rank 1 then the right Λ_ℓ-module M_ℓ is free of rank 1. The converse follows from Theorem 3.1(iii). $\square$

Remark Suppose that Λ is an *order* in a number field E, i.e., Λ is a finitely generated over $\mathbb{Z}$ a subring (with 1) of E such that $\Lambda_{\mathbb{Q}} = E$. Let M be a Λ-module in E, i.e., a free commutative additive (sub)group of finite rank in E such that $M \cdot \Lambda = M$. In particular, $M_{\mathbb{Q}} = E$ is a free $E = \Lambda_{\mathbb{Q}}$-module of rank 1.

(i) If Λ is the ring of all integers in E then it is a Dedekind ring and each of its *localizations* $\Lambda_{(\ell)}$ is a Dedekind ring with finitely many maximal ideals and therefore is a *principal ideal domain* [8, Ch. III, Prop. 2.12 on p.93]. This implies that $M_{(\ell)}$ is a free $\Lambda_{(\ell)}$-module, whose rank is obviously 1. By Corollary 3.2, M is locally free of rank 1.

(ii) Suppose that E is a quadratic field. We don't impose any restrictions on Λ but instead assume that $\mathrm{End}_\Lambda(M) = \Lambda$. Then it is known [1, Lemma 2 on p. 55] that for each prime ℓ there is a nonzero ideal $\mathfrak{J} \subset \Lambda$ such that the order of the finite quotient $\Lambda/\mathfrak{J}$ is prime to ℓ and the Λ-modules M and $\mathfrak{J}$ are isomorphic. This implies that the $\Lambda_{(\ell)}$-module $J_{(\ell)} = \Lambda_{(\ell)}$ is free and therefore the $\Lambda_{(\ell)}$-module $M_{(\ell)}$ is also free and its rank is obviously 1. By Corollary 3.2, M is locally free of rank 1.

4 Tensor products

Now we are going to use Theorem 3.1, in order to construct abelian varieties $A \otimes M$ over K that are *almost isomorphic* to a given A. Notice that our $A \otimes M$ are a rather special *naive* case of powerful *Serre's tensor construction* ([2, Sect. 7], [3, Sect. 1.7.4]).

Suppose we are given a a free commutative group M of finite (positive) rank that is provided with a structure of a right locally free $\Lambda = \mathrm{End}(A)$-module of rank 1. Let F_2 be a free right Λ-module of rank 2. It follows from Theorem 3.1(i) that there is an endomorphism $\gamma : F_2 \to F_2$ of the right Λ-module F_2 such that $\gamma^2 = \gamma$ and whose image $M' = \gamma(F_2)$ is isomorphic to M. Notice that $\mathrm{End}_\Lambda(F_2)$ is the matrix algebra $\mathbb{M}_2(\Lambda)$ of size 2 over Λ. So, the idempotent

$$\gamma \in \mathrm{End}_\Lambda(F_2) = \mathbb{M}_2(\Lambda) = \mathbb{M}_2(\mathrm{End}(A)) = \mathrm{End}(A^2)$$

where $A^2 = A \times A$. Let us define the K-abelian (sub)variety

$$B = A \otimes M := \gamma(A^2) \subset A^2.$$

Clearly, B is a direct factor of A^2. More precisely, if we consider the K-abelian (sub)variety $C = (1-\gamma)(A^2) \subset A^2$ then the natural homomorphism $B \times C \to A^2$, $(x,y) \mapsto x+y$ of abelian varieties over K is an isomorphism, i.e., $A^2 = B \times C$. This implies that the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A,B)$ coincides with

$$\gamma \mathrm{Hom}(A, A^2) \subset \mathrm{Hom}(A, A^2) = \mathrm{End}(A) \oplus \mathrm{End}(A) = F_2$$

and therefore the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A,B)$ is canonically isomorphic to $\gamma(F_2) = M' \cong M$. It also follows that for every prime ℓ

$$\gamma(A^2[\ell]) = B[\ell]. \qquad (**)$$

Theorem 4.1 *Let us consider the abelian variety $B = A \otimes M$ over K. Then:*

(i) A and B are isogenous over K.

(ii) The right $\mathrm{End}(A)$*-module* $\mathrm{Hom}(A,B)$ *is isomorphic to M.*

(iii) A and B are almost isomorphic.

Proof. We have already seen that $\mathrm{Hom}(A,B) \cong M$, which proves (ii).

Since the right $\mathrm{End}(A) \otimes \mathbb{Q}$-module $M \otimes \mathbb{Q}$ is free of rank 1, the same is true for the right $\mathrm{End}(A) \otimes \mathbb{Q}$-module $\mathrm{Hom}(A,B)$. By Lemma 2.1, $\dim(A) \le \dim(B)$ and there exists a $\dim(A)$-dimensional abelian K-subvariety $B_0 \subset B$ such that A and B_0 are isogenous over K and

$$\mathrm{Hom}(A,B) = \mathrm{Hom}(A,B_0). \qquad (***)$$

We claim that $B = B_0$. Indeed, if $B_0 \ne B$ then, by the Poincaré Complete Reducibility theorem [7, Th. 6 on p. 28], there is an "almost complimentary" abelian K-subvariety $B_1 \subset B$ of positive dimension $\dim(B) - \dim(B_0)$ such that the intersection $B_0 \bigcap B_1$ is finite and $B_0 + B_1 = B$. It follows from (***) that $\mathrm{Hom}(A, B_1) = \{0\}$. However, $B_1 \subset B \subset A^2$ is an abelian K-subvariety of A^2 and therefore there is a surjective homomorphism $A^2 \to B$ and therefore there exists a nonzero homomorphism $A \to B$. This is a contradiction, which proves that $B = B_0$, the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A,B)$ is isomorphic to

M, and A and B are isogenous over K. In particular, $\dim(A) = \dim(B)$. This proves (i).

Let ℓ be a prime. Since $M \otimes \mathbb{Z}_\ell$ is a free right $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$-module of rank 1, $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$ is a free right $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$-module of rank 1. Let us choose a generator $\phi \in \mathrm{Hom}(A, B)$ of the module $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$. The *surjection* $\gamma : A^2 \to B \subset A^2$ is defined by a certain pair of homomorphisms $\phi_1, \phi_2 : A \to B$, i.e.,

$$\gamma(x_1, x_2) = \phi_1(x_1) + \phi_2(x_2) \ \forall (x_1, x_2) \in A^2.$$

Since ϕ is the generator, there are $u_1, u_2 \in \mathrm{End}(A) \otimes \mathbb{Z}_\ell$ such that

$$\phi_1 = \phi u_1, \ \phi_1 = \phi u_1$$

in $\mathrm{Hom}(A, B) \otimes \mathbb{Z}_\ell$. It follows that

$$\gamma(A^2[\ell]) = \phi_1(A[\ell]) + \phi_2(A[\ell]) = \phi u_1(A[\ell]) + \phi u_2(A[\ell]) \subset \phi(A[\ell]) \subset B[\ell].$$

By (**), $\gamma(A^2[\ell]) = B[\ell]$. This implies that ϕ induces a surjective homomorphism $A[\ell] \to B[\ell]$. Since finite groups $A[\ell]$ and $B[\ell]$ have the same order, ϕ induces an isomorphism $A[\ell] \to B[\ell]$. This implies that $\ker(\phi)$ does not contain points of order ℓ and therefore is an *isogeny* of degree prime to ℓ. This proves (iii). □

Corollary 4.2 *Suppose that for each $i = 1, 2$ we are given a commutative free group M_i of finite positive rank provided with the structure of a right locally free* $\mathrm{End}(A)$*-module of rank* 1*. Then abelian varieties $B_1 = A \otimes M_1$ and $B_2 = A \otimes M_2$ are isomorphic over K if and only if the* $\mathrm{End}(A)$*-modules M_1 and M_2 are isomorphic.*

Proof. By Theorem 4.1(ii), the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A, B_i)$ is isomorphic to M_i. Now the result follows from Theorem 4.1(iii) combined with Corollary 2.5. □

Corollary 4.3 *Let A and B be abelian varieties over K of positive dimension. Suppose that the Galois modules $T_\ell(A)$ and $T_\ell(B)$ are isomorphic for all primes ℓ. Then abelian varieties B and $C := A \otimes \mathrm{Hom}(A, B)$ are isomorphic over K.*

Proof. By Theorem 4.1(ii), the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A, C)$ is isomorphic to $\mathrm{Hom}(A, B)$. Now the result follows from Theorem 4.1(iii) combined with Corollary 2.5. □

Remark Let $g \ge 2$ be an integer and a g-dimensional abelian variety A is a product $A_1 \times A_2$ where A_1 and A_2 are abelian varieties of positive dimension over K with $\mathrm{Hom}(A_1, A_2) = \{0\}$. Then $\mathrm{End}(A) = \mathrm{End}(A_1) \oplus \mathrm{End}(A_2)$. Suppose that for each $i = 1, 2$ we are given a commutative free group M_i of finite positive rank provided with the structure of a right locally free $\mathrm{End}(A_i)$-module of rank 1.

Then the direct sum $M = M_1 \oplus M_2$ becomes a right locally free module of rank 1 over the ring $\mathrm{End}(A_1) \oplus \mathrm{End}(A_2) = \mathrm{End}(A)$.

There is an obvious canonical isomorphism between abelian varieties $A \otimes M$ and $(A_1 \otimes M_1) \times (A_2 \otimes M_2)$ over K.

For example, we may take as A_2 (for a suitable number field K) an elliptic curve such that $\mathrm{End}(A_2)$ is the ring of integers in an imaginary quadratic field with class number > 1 while A_1 is a $(g-1)$-dimensional principally polarized with

$$\mathrm{End}(A_1 \times \bar{K}) = \mathrm{End}(A_1) = \mathbb{Z}.$$

(If $g > 2$ then one may take as A_1 the $(g-1)$-dimensional jacobian of the hyperelliptic curve $y^2 = x^{2g-1} - x - 1$, see [13].) Clearly, all $\bar{K}$-endomorphisms of A are defined over K; in particular, A_1 is absolutely simple. Let us take $M_1 = \mathbb{Z}$. Clearly, $\mathrm{Hom}(A_1, A_2) = \{0\}$. Actually, every $\bar{K}$-homomorphism between A_1 and A_2 is 0. Let M_2 be a *non-principal* ideal in $\mathrm{End}(A_2)$. Then elliptic curves A_2 and $A_2 \otimes M$ are almost isomorphic but are *not isomorphic* over K and even over $\bar{K}$. This implies that $A \otimes M = A_1 \times (A_2 \otimes M_2)$ is almost isomorphic over K but is *not* isomorphic to $A = A_1 \times A_2$ over $\bar{K}$. Notice that both A and $A \otimes M$ are principally polarized, since A_1 is principally polarized while both A_2 and $A_2 \otimes M_2$ are elliptic curves.

Remark See last section of [15] for examples of almost isomorphic but not isomorphic elliptic curves over finite fields.

Acknowledgements. I am grateful to Jiangwei Xue for useful discussions, to Stefan Patrikis and Felipe Voloch for their interest in this paper and to the Simons Foundation for financial and moral support (via grant #246625 to Yuri Zarkhin). Part of this work was done in May–June 2015 when I was visiting Department of Mathematics of the Weizmann Institute of Science (Rehovot, Israel) and in May-June 2016 when I was a visitor at the Max-Planck-Institut für Mathematik (Bonn, Germany). The hospitality and support of both Institutes are gratefully acknowledged.

References

[1] Z.I. Borevich, D.K. Faddeev, Integral representations of quadratic rings. Vestnik Leningrad. Univ. **15** (1960), no. 19, 52–64. (Russian) MR0153707 (27 #3668).

[2] B. Conrad, *Gross-Zagier revisited.* With an appendix by W. R. Mann. In: Math. Sci. Res. Inst. Publ., **49**, Heegner points and Rankin L-series, 67–163, Cambridge Univ. Press, Cambridge, 2004.

[3] C.-L. Chai, B. Conrad, F. Oort, Complex multiplication and lifting problems. Mathematical Surveys and Monographs **195**, American Mathematical Society, Providence, RI, 2014.

[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

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

[6] A. Frölich, *Locally free modules over arithmetic orders.* J. Reine Angew. Math. **274/275** (1975), 112–124.

[7] S. Lang, Abelian Varieties, 2nd edition. Springer-Verlag, New York Berlin Heidelberg Tokyo, 1983.

[8] D. Lorenzini, An invitation to Arithmetic Geometry. Graduate Studies in Mathematics **9**, American Mathematical Society, Providence, RI, 1996.

[9] D. Mumford, Abelian varieties, 2nd edition. Oxford University Press, 1974.

[10] S. Patrikis, F. Voloch, Yu. G. Zarhin, *Anabelian geometry and descent obstructions on moduli spaces*. Algebra and Number Theory **10:6** (2016), 1191–1219.

[11] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves, 2nd edition. Addison-Wesley Publishing Company, Redwood, CA, 1989.

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

[13] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Research Letters **7** (2000), no. 1, 123–132.

[14] Yu. G. Zarhin, *Homomorphisms of abelian varieties*. In: Arithmetic, Geometry and Coding Theory (AGCT 2003) (Y. Aubry, G. Lachaud, eds.), Sémin. Congr. **11**, Soc. Math. France, Paris, 2005, 189–215.

[15] Yu. G. Zarhin, *Homomorphisms of abelian varieties over finite fields*, pp. 315–344. In: Higher-dimensional geometry over finite fields (D. Kaledin, Yu. Tschinkel, eds.). IOS Press, Amsterdam, 2008.

Department of Mathematics, Pennsylvania State University,
University Park, PA 16802, USA
e-mail: `zarhin@math.psu.edu`