Anabelian geometry and descent obstructions on moduli spaces

Stefan Patrikis, José Felipe Voloch, Yuri G. Zarhin

July 5, 2015

Abstract. We study the section conjecture of anabelian geometry and the sufficiency of the finite descent obstruction to the Hasse principle for the moduli spaces of principally polarized abelian varieties and of curves over number fields. For the former we show that the section conjecture fails and the finite descent obstruction holds for a general class of adelic points, assuming several well-known conjectures. For the latter, we prove some partial results that indicate that the finite descent obstruction suffices. We also show how this sufficiency implies the same for all hyperbolic curves.

1 Introduction

Anabelian geometry is a program proposed by Grothendieck ([8, 9]) which suggests that for a certain class of varieties (called anabelian but, as yet, undefined) over a number field, one can recover the varieties from their étale fundamental group together with the Galois action of the absolute Galois group of the number field. Precise conjectures exist only for curves and some of them have been proved, notably by Mochizuki ([19]). Grothendieck suggested that moduli spaces of curves and abelian varieties (the latter perhaps less emphatically) should be anabelian. Already Ihara and Nakamura [14] have shown that moduli spaces of abelian varieties should not be anabelian as one cannot recover their automorphism group from the fundamental group

Keywords: Anabelian geometry, moduli spaces, abelian varieties, descent obstruction.
Mathematical subject classification: Primary 11G35; Secondary:14G05,14G35

and we will further show that other anabelian properties fail in this case. In the case of moduli of curves, we will provide further evidence that they should indeed be considered anabelian.

The finite descent obstruction is a construction that describes a subset of the adelic points of a variety over a number field containing the closure of the rational (or integral) points and is conjectured to sometimes (e.g. for curves, perhaps for anabelian varieties) to equal that closure. The relationship between the finite descent obstruction and the section conjecture in anabelian geometry has been discussed by Harari and Stix [11, 34] and others. We will review the relevant definitions below, although our point of view will be slightly different.

The purpose of this paper is to study the section conjecture of anabelian geometry and the finite descent obstruction for the moduli spaces of principally polarized abelian varieties and of curves over number fields. For the moduli of abelian varieties we show that the section conjecture fails in general and that both the the section conjecture and finite descent obstruction hold for a general class of adelic points, assuming some established conjectures in arithmetic geometry. We also give examples showing that weaker versions of the finite descent obstruction do not hold. For the moduli of curves, we prove some partial results that indicate that the finite descent obstruction suffices. We also show how combining some of our result with the conjectured sufficiency of finite descent obstruction for the moduli of curves, we deduce the sufficiency of finite descent obstruction for all hyperbolic curves.

In the next section we give more precise definitions of the objects we use and in the following two sections we give the applications mentioned above.

2 Preliminaries

Let X/K be a smooth geometrically connected variety over a field K. Let G_K be the absolute Galois group of K and $\bar{X}$ the base-change of X to an algebraic closure of K. We denote by $\pi_1(.)$ the algebraic fundamental group functor on schemes and we omit base-points from the notation. We have the fundamental exact sequence

$$1 \to \pi_1(\bar{X}) \to \pi_1(X) \to G_K \to 1. \tag{1}$$

The map $p_X : \pi_1(X) \to G_K$ from the above sequence is obtained by functoriality from the structural morphism $X \to \mathrm{Spec} K$. Grothendieck's anabelian program is to specify a class of varieties, termed anabelian, for which the varieties and morphisms between them can be recovered from the corresponding fundamental groups together with the corresponding maps p_X when the ground field is finitely generated over its prime field. As this is very vague, we single out here two special cases with precise statements. The first is a (special case of a) theorem of Mochizuki [19] which implies part of Grothendieck's conjectures for curves but also extends it by considering p-adic fields.

Theorem 2.1 *(Mochizuki) Let X, Y be smooth projective curves of genus bigger than one over a field K which is finitely generated over $\mathbf{Q}_p$. If there is an isomorphism from $\pi_1(X)$ to $\pi_1(Y)$ inducing the identity on G_K via p_X, p_Y, then X is isomorphic to Y.*

A point $P \in X(K)$ gives, by functoriality, a section $G_K \to \pi_1(X)$ of the fundamental exact sequence (1) well-defined up to conjugation by an element of $\pi_1(\bar{X})$ (the indeterminacy is because of base points).

We denote by $H(K, X)$ the set of sections $G_K \to \pi_1(X)$ modulo conjugation by $\pi_1(\bar{X})$ and we denote by $\sigma_{X/K} : X(K) \to H(K, X)$ the map that associates to a point the class of its corresponding section, as above, and we call it the section map. As part of the anabelian program, it is expected that $\sigma_{X/K}$ is a bijection if X is projective, anabelian and K is finitely generated over its prime field. This is widely believed in the case of hyperbolic curves over number fields and is usually referred as the section conjecture. For a similar statement in the non-projective case, one needs to consider the so-called cuspidal sections, see [34]. Although we will discuss non-projective varieties in what follows, we will not need to specify the notion of cuspidal sections. The reason for this is that we will be considering sections that locally come from points (the Selmer set defined below) and these will not be cuspidal.

We remark that the choice of a particular section $s_0 : G_K \to \pi_1(X)$ induces an action of G_K on $\pi_1(\bar{X}), x \mapsto s_0(\gamma) x s_0(\gamma)^{-1}$. For an arbitrary section $s : G_K \to \pi_1(X)$ the map $\gamma \mapsto s(\gamma) s_0(\gamma)^{-1}$ is a 1-cocycle for the above action of G_K on $\pi_1(\bar{X})$ and this induces a bijection $H^1(G_K, \pi_1(\bar{X})) \to H(K, X)$. We stress that this only holds when $H(K, X)$ is non-empty and a choice of s_0 can be made. It is possible for $H(K, X)$ to be empty, whereas $H^1(G_K, \pi_1(\bar{X}))$ is never empty.

Let X/K as above, where K is now a number field. If v is a place of K, we have the completion K_v and a fixed inclusion $\overline{K} \subset \overline{K}_v$ induces a map $\alpha_v : G_{K_v} \to G_K$ and a map $\beta_v : \pi_1(X_v) \to \pi_1(X)$, where X_v is the base-change of X to K_v. We define the Selmer set of X/K as the set $S(K,X) \subset H(K,X)$ consisting of the equivalence classes of sections s such that for all places v, there exists $P_v \in X(K_v)$ with $s \circ \alpha_v = \beta_v \circ \sigma_{X/K_v}(P_v)$. Note that if v is complex, then the condition at v is vacuous and that if v is real, σ_{X/K_v} is constant on $X(K_v)_\bullet$, the set of connected components of $X(K_v)$, equipped with the quotient topology (see [27]). So we have the following diagram:

$$\begin{tikzcd}
 & X(K) \arrow[r] \arrow[d, "\sigma_{X/K}"'] & \prod X(K_v)_\bullet \arrow[d, "\prod \sigma_{X/K_v}"] & \supset X^f \\
S(K,X) \subset & H(K,X) \arrow[r, "\alpha"] & \prod H(K_v,X).
\end{tikzcd}$$

We define the set X^f (the finite descent obstruction) as the set of points $(P_v)_v \in \prod_v X(K_v)_\bullet$ for which there exists $s \in H(K,X)$ (which is then necessarily an element of $S(K,X)$) satisfying $s \circ \alpha_v = \beta_v \circ \sigma_{X/K_v}(P_v)$ for all places v. Also, it is clear that the image of $X(K)$ is contained in X^f and also that X^f is closed (this follows from the compactness of G_K). One says that the finite descent obstruction is the only obstruction to strong approximation if the closure of the image of $X(K)$ in $\prod X(K_v)_\bullet$ equals X^f. A related statement is the equality $\sigma_{X/K}(X(K)) = S(K,X)$, which is implied by the "section conjecture", i.e., the bijectivity of $\sigma_{X/K} : X(K) \to H(K,X)$. More explicitly,

Proposition 2.2 *We have that $X^f = \emptyset$ if and only if $S(K,X) = \emptyset$. If, moreover, σ_{X/K_v} induces an injective map on $X(K_v)_\bullet$ for all places v of K then $\sigma_{X/K}(X(K)) = S(K,X)$ if and only if X^f is the image of $X(K)$.*

Proof. If $X^f \neq \emptyset$ and $(P_v) \in X^f$, then there exists $s \in S(K,X)$ with $s \circ \alpha_v = \beta_v \circ \sigma_{X/K_v}(P_v)$ for all places v, so $S(K,X) \neq \emptyset$. If we also have $\sigma_{X/K}(X(K)) = S(K,X)$, then $s = \sigma_{X/K}(P), P \in X(K)$. It follows from the injectivity of σ_{X/K_v} on $X(K_v)_\bullet$ that the image of P in $X(K_v)_\bullet$ coincides with the image of P_v in $X(K_v)_\bullet$ for all v, so X^f is the image of $X(K)$.

If $s \in S(K,X)$, there exists (P_v) with $s \circ \alpha_v = \beta_v \circ \sigma_{X/K_v}(P_v)$ for all places v. So $(P_v) \in X^f$. If X^f is the image of $X(K)$, then (P_v) is the image of $P \in X(K)$. It follows that $s = \sigma_{X/K}(P)$. □

If X is not projective, then one has to take into account questions of integrality. We choose an integral model $\mathcal{X}/\mathcal{O}_{S,K}$, where S is a finite set of places of K and $\mathcal{O}_{S,K}$ is the ring of S-integers of K. The image of $X(K)$ in X^f actually lands in the adelic points which are the points that satisfy $P_v \in \mathcal{X}(\mathcal{O}_v)$ for all but finitely many v, where $\mathcal{O}_v$ is the local ring at v. Similarly, the image of $\sigma_{X/K}$ belongs to the subset of $S(K,X)$ where the corresponding local points P_v also belong to $\mathcal{X}(\mathcal{O}_v)$ for all but finitely many v. We denote this subset of $S(K,X)$ by $S_0(K,X)$ and call it the integral Selmer set.

3 Moduli of abelian varieties

The moduli space of principally polarized abelian varieties of dimension g is denoted by $\mathcal{A}_g$. It is actually a Deligne-Mumford stack or orbifold and we will consider its fundamental group as such. For a general definition of fundamental groups of stacks including a proof of the fundamental exact sequence in this generality, see [41]. For a discussion of the case of $\mathcal{A}_g$, see [10]. We can also get what we need from [14] (see below) or by working with a level structure which bring us back to the case of smooth varieties.

As $\mathcal{A}_g$ is defined over $\mathbf{Q}$, we can consider it over an arbitrary number field K. As per our earlier conventions, $\bar{\mathcal{A}}_g$ is the base change of $\mathcal{A}_g$ to an algebraic closure of $\mathbf{Q}$ and not a compactification. In fact, we will not consider a compactification at all here. The topological fundamental group of $\bar{\mathcal{A}}_g$ is the symplectic group $Sp_{2g}(\mathbf{Z})$ and the algebraic fundamental group is its profinite completion. When $g > 1$ (which we henceforth assume) $Sp_{2g}(\mathbf{Z})$ has the congruence subgroup property ([1],[17]) and therefore its profinite completion is $Sp_{2g}(\hat{\mathbf{Z}})$.

The group $\pi_1(\mathcal{A}_g)$ is essentially described by the exact sequences (3.2) and (3.3) of [14] and it follows that the set $H(K,\mathcal{A}_g)$ consists of $\hat{\mathbf{Z}}$ representations of G_K of rank $2g$ preserving the symplectic form up to scalar and having as determinant the cyclotomic character. Indeed, it is clear that every section gives such a representation and the converse follows formally from the diagram below, which is a consequence of (3.2) and (3.3) of [14].

Here $\chi : G_K \to \hat{\mathbf{Z}}^*$, the cyclotomic character.

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(\bar{\mathcal{A}}_g) \arrow[r] \arrow[d, "\cong"] & \pi_1(\mathcal{A}_g) \arrow[r] \arrow[d] & G_K \arrow[r] \arrow[d, "\chi"'] & 1 \\
1 \arrow[r] & Sp_{2g}(\hat{\mathbf{Z}}) \arrow[r] & GSp_{2g}(\hat{\mathbf{Z}}) \arrow[r] & \hat{\mathbf{Z}}^* \arrow[r] & 1.
\end{tikzcd}$$

The coverings of $\bar{\mathcal{A}}_g$ corresponding to the congruence subgroups of $Sp_{2g}(\hat{\mathbf{Z}})$ are those obtained by adding level structures. In particular, for an abelian variety A, $\sigma_{\mathcal{A}_g/K}(A) = \prod T_\ell(A)$, the product of its Tate modules considered, as usual, as a G_K-module. If K is a number field, whenever two abelian varieties are mapped to the same point by $\sigma_{\mathcal{A}_g/K}$, then they are isogenous, by Faltings ([4]). Whether $\sigma_{\mathcal{A}_g/K}$ is injective to $S_0(K, \mathcal{A}_g)$ or not does depend on K and g, see Sect. 4. For example, if $g = 1$ and K admits an embedding into the field $\mathbf{R}$ of real numbers then $\sigma_{\mathcal{A}_1/K}$ is injective. On the other hand, for each g there exists K with non-injective $\sigma_{\mathcal{A}_g/K}$. However, for any K and g every fiber of $\sigma_{\mathcal{A}_g/K}$ is finite.

Note also that the hypotheses of proposition 2.2 do not hold for $\mathcal{A}_g$ as the ℓ-adic representation is locally constant in the v-adic topology for non-archimedian v, so for those places $\sigma_{\mathcal{A}_g/K_v}$ is not injective. Regarding surjectivity, we will prove that those elements of $S_0(K, \mathcal{A}_g)$ for which the corresponding Galois representation is absolutely irreducible (see below for the precise hypothesis and corollary 3.6 for a precise statement) are in the image of $\sigma_{\mathcal{A}_g/K}$, assuming the Fontaine-Mazur conjecture, the Grothendieck-Serre conjecture on semi-simplicity of ℓ-adic cohomology of smooth projective varieties, and the Tate and Hodge conjectures. The integral Selmer set $S_0(K, \mathcal{A}_g)$, defined in the previous section, corresponds to the set of Galois representations that are almost everywhere unramified and, locally, come from abelian varieties (which thus are of good reduction for almost all places of K) and we will also consider a few variants of the question of surjectivity of $\sigma_{\mathcal{A}_g/K}$ to $S_0(K, \mathcal{A}_g)$ by different local hypotheses and discuss what we can and cannot prove. A version of this kind of question has also been considered by B. Mazur [16].

Here is the setting. Let K be a number field, with $G_K = \mathrm{Gal}(\overline{K}/K)$. Fix a finite set of rational primes S, and suppose we are given a weakly compatible system of almost everywhere unramified ℓ-adic representations

$$\{\rho_\ell \colon G_K \to \mathrm{GL}_N(\mathbb{Q}_\ell)\}_{\ell \notin S},$$

satisfying the following two properties:

1. For some prime $\ell_1 \notin S$, ρ_{ℓ_1} is absolutely irreducible.
2. For some prime $\ell_2 \notin S$, and at least one place $v|\ell_2$ of K, $\rho_{\ell_2}|_{G_{K_v}}$ is de Rham with Hodge-Tate weights $-1, 0$, each with multiplicity $\frac{N}{2}$. (Note that this condition holds if there exists an abelian variety A_v/K_v such that $\rho_{\ell_2}|_{G_{K_v}} \cong V_{\ell_2}(A_v)$, the latter denoting the rational Tate module of A_v.)

Our aim is to prove the following:

Theorem 3.1 *Assume the Hodge, Tate, Fontaine-Mazur, and Grothendieck-Serre conjectures, and suppose that the set S is empty. Then there exists an abelian variety A over K such that $\rho_\ell \cong V_\ell(A)$ for all ℓ.*

We begin by making somewhat more precise the combined implications of the Grothendieck-Serre, Tate, and Fontaine-Mazur conjectures (the Hodge conjecture will only be used later, in the proof of Lemma 3.4). For any field k and characteristic zero field E, let $\mathcal{M}_{k,E}$ denote the category of pure homological motives over k with coefficients in E (omitting E from the notation will mean $E = \mathbf{Q}$); since we assume the Tate conjecture (when k is finitely-generated), the Standard Conjectures hold over k (even when k is not finitely-generated, e.g. $k = \mathbf{C}$), so we have a motivic Galois formalism: $\mathcal{M}_{k,E}$ is equivalent to $\mathrm{Rep}(\mathcal{G}_{k,E})$ for some pro-reductive group $\mathcal{G}_{k,E}$ over E, the equivalence depending on the choice of an E-linear fiber functor. Our k will always have characteristic zero, so such a fiber functor is obtained by embedding k into $\mathbf{C}$ and taking Betti cohomology; this will be left implicit in all that follows. For an extensions of fields k'/k, we denote the base-change of motives by

$$(\cdot)|_{k'} \colon \mathcal{M}_{k,E} \to \mathcal{M}_{k',E}.$$

This is not to be confused with the change of coefficients. Fix an embedding $\iota \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$, so that when E is a subfield of $\overline{\mathbb{Q}}$ we can speak of the ℓ-adic realization

$$H_\iota \colon \mathcal{M}_{k,E} \to \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G_k)$$

associated to ι.

Lemma 3.2 *Let $r_\ell \colon G_K \to \mathrm{GL}_N(\mathbb{Q}_\ell)$ be an irreducible geometric Galois representation. Then there exists an object M of $\mathcal{M}_{K,\overline{\mathbb{Q}}}$ such that*

$$r_\ell \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \cong H_\iota(M).$$

Proof. The Fontaine-Mazur conjecture asserts that for some smooth projective variety X/k, r_ℓ is a sub-quotient of $H^i(X_{\overline{K}}, \mathbb{Q}_\ell)(j)$ for some integers i and j, and the Grothendieck-Serre conjecture implies this sub-quotient is in fact a direct summand. We denote by $H^i(X)(j)$ the object of $\mathcal{M}_K$ whose existence is ensured by the Künneth Standard Conjecture. The Tate conjecture then says that

$$H_\iota \colon \operatorname{End}_{\mathcal{M}_K}\left(H^i(X)(j)\right) \otimes_{\mathbf{Q}} \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \operatorname{End}_{\overline{\mathbb{Q}}_\ell[G_K]}\left(H^i(X_{\overline{K}}, \mathbb{Q}_\ell)(j)\right) \qquad (2)$$

is an isomorphism.

Now, there is a projector (of $\overline{\mathbb{Q}}_\ell[G_K]$-modules) $H^i(X_{\overline{K}}, \overline{\mathbb{Q}}_\ell)(j) \twoheadrightarrow r_\ell$, which combined with Equation (2) yields a projector in $\operatorname{End}_{\mathcal{M}_K}(H^i(X)(j)) \otimes_{\mathbf{Q}} \overline{\mathbb{Q}}_\ell$ whose image has ℓ-adic realization r_ℓ. But $\operatorname{End}_{\mathcal{M}_K}(H^i(X)(j))$ is a semisimple algebra over $\mathbf{Q}$, which certainly splits over $\overline{\mathbb{Q}}$, so the decomposition of $H^i(X)(j)$ into simple objects of $\mathcal{M}_{K,\overline{\mathbb{Q}}_\ell}$ is already realized in $\mathcal{M}_{K,\overline{\mathbb{Q}}}$.[1] □

Returning to our particular setting, fix any $\ell_0 \notin S$ and an embedding $\iota_0 \colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{\ell_0}$, so that Lemma 3.2 provides us with a number field $E \subset \overline{\mathbb{Q}}$ (which we may assume Galois over $\mathbf{Q}$) and a motivic Galois representation $\rho \colon \mathcal{G}_{K,E} \to \mathrm{GL}_{N,E}$ such that $H_{\iota_0}(\rho) \cong \rho_{\ell_0} \otimes \overline{\mathbf{Q}}_{\ell_0}$. Let us denote by λ_0 the place of E induced by $E \subset \overline{\mathbb{Q}} \xrightarrow{\iota_0} \overline{\mathbb{Q}}_\ell$. Then for all finite places λ of E (say $\lambda | \ell$), and for almost all places v of K, compatibility gives us the following equality of rational numbers (note that ρ_λ denotes the λ-adic realization of the motivic Galois representation ρ, while ρ_ℓ denotes the original ℓ-adic representation in our compatible system):

$$\operatorname{tr}(\rho_\lambda(fr_v)) = \operatorname{tr}(\rho_{\lambda_0}(fr_v)) = \operatorname{tr}(\rho_{\ell_0}(fr_v)) = \operatorname{tr}(\rho_\ell(fr_v)).$$

Here we use the fact that the collection of ℓ-adic realizations of a motive form a (weakly) compatible system; this follows from the Lefschetz trace formula. We deduce as usual (Brauer-Nesbitt and Chebotarev) that $\rho_\ell \otimes_{\mathbb{Q}_\ell} E_\lambda \cong \rho_\lambda$; this holds for all λ for which ρ_ℓ makes sense, i.e. for all λ above $\ell \notin S$.

The next question is whether having each (or almost all) ρ_λ in fact definable over $\mathbb{Q}_\ell$ forces ρ to be definable over $\mathbf{Q}$. Recall that for some $\ell_1 \notin S$, we have assumed ρ_{ℓ_1} is absolutely irreducible. *A fortiori*, ρ is absolutely irreducible, and then by the Tate conjecture all ρ_ℓ ($\ell \notin S$) are absolutely irreducible. Since the ρ_λ descend to $\mathbb{Q}_\ell$, the Tate conjecture implies that

[1] In fact, it is realized over the maximal CM subfield of $\overline{\mathbb{Q}}$: see e.g. [28, Lemma 4.1.22].

for all $\sigma \in \mathrm{Gal}(E/\mathbf{Q})$, ${}^{\sigma}\rho \cong \rho$; and since $\mathrm{End}(\rho)$ is E, the obstruction to descending ρ to a $\mathbf{Q}$-rational representation of $\mathcal{G}_K$ is an element obs_ρ of $H^1(\mathrm{Gal}(E/\mathbf{Q}), \mathrm{PGL}_N(E))$.

Lemma 3.3 *With the notation above,* obs_ρ *in fact belongs to*

$$\ker\left(H^1(\mathrm{Gal}(E/\mathbf{Q}), \mathrm{PGL}_N(E)) \to \prod_{\ell \notin S} H^1(\mathrm{Gal}(E_\lambda/\mathbf{Q}_\ell), \mathrm{PGL}_N(E_\lambda))\right).$$

In particular, if S is empty, then ρ can be defined over $\mathbf{Q}$.

Proof. We know that each of the λ-adic realizations ρ_λ (for $\lambda|\ell \notin S$) can be defined over $\mathbb{Q}_\ell$; to prove the lemma, we have to recall how these are constructed from ρ itself. The surjection $\mathcal{G}_K \twoheadrightarrow G_K$ admits a continuous section on $\mathbb{Q}_\ell$-points, $s_\ell \colon G_K \to \mathcal{G}_K(\mathbb{Q}_\ell)$; composition with $\rho \otimes_E E_\lambda$ yields ρ_λ. We have seen that ρ_λ can be defined over $\mathbb{Q}_\ell$, so that after $\mathrm{GL}_N(E_\lambda)$-conjugation we can assume that the composite

$$G_K \xrightarrow{s_\ell} \mathcal{G}_K(\mathbb{Q}_\ell) \subset \mathcal{G}_{K,E}(E_\lambda) \xrightarrow{\rho \otimes_E E_\lambda} \mathrm{GL}_N(E_\lambda)$$

has values in $\mathrm{GL}_N(\mathbb{Q}_\ell)$. The Tate and Grothendieck-Serre conjectures imply that $s_\ell(G_K)$ is Zariski-dense in $\mathcal{G}_{K,E_\lambda}$, by applying, for instance, [3, I, Proposition 3.1]. Thus $\rho \otimes_E E_\lambda$ must be definable over $\mathbb{Q}_\ell$, since composing with any element of $\mathrm{Gal}(E_\lambda/\mathbb{Q}_\ell)$ the result agrees with $\rho \otimes E_\lambda$ on $s_\ell(G_K)$, hence must equal $\rho \otimes E_\lambda$. It follows that obs_ρ has trivial restriction to each $\mathrm{Gal}(E_\lambda/\mathbb{Q}_\ell)$, as desired.

For the final claim, note that by Hilbert 90 we can regard obs_ρ as an element of

$$\ker\left(H^2(\mathrm{Gal}(E/\mathbf{Q}), E^\times) \to \prod_{\ell \notin S} H^2(\mathrm{Gal}(E_\lambda/\mathbb{Q}_\ell), E_\lambda^\times)\right).$$

If S is empty, then the structure of the Brauer group of $\mathbf{Q}$ (which has only one infinite place!) then forces obs_ρ to be trivial. □

Proof. [Proof of Theorem 3.1] From now on we assume $S = \emptyset$, so that our compatible system $\{\rho_\ell\}_\ell$ arises from a rational representation

$$\rho \colon \mathcal{G}_K \to \mathrm{GL}_{N,\mathbf{Q}}.$$

Let M be the rank N object of $\mathcal{M}_K$ corresponding to ρ via the Tannakian equivalence. Recall that we are given a prime ℓ_2 and a place $v|\ell_2$ of K for which we are given that $\rho_{\ell_2}|_{G_{K_v}}$ is de Rham with Hodge numbers equal to those of an abelian variety of dimension $\frac{N}{2}$. All objects of $\mathcal{M}_K$ enjoy the de Rham comparison theorem of 'ℓ_2-adic Hodge theory': denoting Fontaine's period ring over K_v by $\mathrm{B}_{\mathrm{dR},K_v}$, and the de Rham realization functor by $H_{\mathrm{dR}}\colon \mathcal{M}_K \to \mathrm{Fil}_K$ (the category of filtered K-vector spaces), we have the comparison (respecting filtration and G_{K_v}-action)

$$H_{\mathrm{dR}}(M) \otimes_K \mathrm{B}_{\mathrm{dR},K_v} \xrightarrow{\sim} H_{\ell_2}(M) \otimes_{\mathbf{Q}_{\ell_2}} \mathrm{B}_{\mathrm{dR},K_v},$$

hence

$$H_{\mathrm{dR}}(M) \otimes_K K_v \cong \mathrm{D}_{\mathrm{dR},K_v}(H_{\ell_2}(M)).$$

The Hodge filtration on $H_{\mathrm{dR}}(M)$ therefore satisfies

$$\dim_K \mathrm{gr}^0\,(H_{\mathrm{dR}}(M)) = \dim_K \mathrm{gr}^{-1}\,(H_{\mathrm{dR}}(M)) = \frac{N}{2} \tag{3}$$

and $\mathrm{gr}^i\,(H_{\mathrm{dR}}(M)) = 0$ for $i \neq 0, -1$.

Now we turn to the Betti picture. Recall that to define the fiber functor on $\mathcal{M}_K$ we had to fix an embedding $K \hookrightarrow \mathbf{C}$; we regard K as a subfield of $\mathbf{C}$ via this embedding. Then we also have the analytic Betti-de Rham comparison isomorphism

$$H_{\mathrm{dR}}(M) \otimes_K \mathbf{C} \xrightarrow{\sim} H_{\mathrm{B}}(M|_{\mathbf{C}}) \otimes_{\mathbf{Q}} \mathbf{C}. \tag{4}$$

We collect our findings in the following lemma, which relies on an application of the Hodge conjecture:

Lemma 3.4 *There is an abelian variety A over K, and an isomorphism of motives $H_1(A) \cong M$.*

Proof. We see from Equations (3) and (4) that $H_{\mathrm{B}}(M|_{\mathbf{C}})$ is a polarizable rational Hodge structure of type $\{(0,-1),(-1,0)\}$. It follows from Riemann's theorem that there is an abelian variety $A/\mathbf{C}$ and an isomorphism of $\mathbf{Q}$-Hodge structures $H_1(A(\mathbf{C}),\mathbf{Q}) \cong H_{\mathrm{B}}(M|_{\mathbf{C}})$. The Hodge conjecture implies that this isomorphism comes from an isomorphism $H_1(A) \xrightarrow{\sim} M|_{\mathbf{C}}$ in $\mathcal{M}_{\mathbf{C}}$.

For any $\sigma \in \mathrm{Aut}(\mathbf{C}/\overline{\mathbb{Q}})$, we deduce an isomorphism

$${}^{\sigma}H_1(A) \xrightarrow{\sim} {}^{\sigma}M|_{\mathbf{C}} = M|_{\mathbf{C}} \xleftarrow{\sim} H_1(A),$$

and again from Riemann's theorem we see that ${}^{\sigma}A$ and A are isogenous.

The following statement will be proven later in this paper.

Lemma 3.5 *Let $\mathcal{K}$ be a countable subfield of the field $\mathbf{C}$ and $\bar{\mathcal{K}}$ the algebraic closure of $\mathcal{K}$ in $\mathbf{C}$. Let $\mathcal{A}$ be a complex abelian variety of positive dimension g such that for each field automorphism $\sigma \in \mathrm{Aut}(\mathbf{C}/\mathcal{K})$ the complex abelian varieties $\mathcal{A}$ and its "conjugate" ${}^{\sigma}\mathcal{A} = \mathcal{A} \times_{\mathbf{C},\sigma} \mathbf{C}$ are isogenous. Then there exists an abelian variety $\mathcal{A}_0$ over $\bar{\mathcal{K}}$ such that $\mathcal{A}_0 \times_{\bar{\mathcal{K}}} \mathbf{C}$ is isomorphic to $\mathcal{A}$.*

It follows from Lemma 3.5 that A has a model $A_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$. The morphism

$$\mathrm{Hom}_{\mathcal{M}_{\overline{\mathbb{Q}}}}(H_1(A_{\overline{\mathbb{Q}}}), M|_{\overline{\mathbb{Q}}}) \to \mathrm{Hom}_{\mathcal{M}_{\mathbf{C}}}(H_1(A), M|_{\mathbf{C}})$$

is an isomorphism, and then by general principles we deduce the existence of some finite extension L/K inside $\overline{\mathbb{Q}}$ over which A descends to an abelian variety A_L, and where we have an isomorphism $H_1(A_L) \xrightarrow{\sim} M|_L$ in $\mathcal{M}_L$.

Finally, we treat the descent to K itself. We form the restriction of scalars abelian variety $\mathrm{Res}_{L/K}(A_L)$; under the *fully faithful* embedding

$$\begin{aligned} \mathrm{AV}_K^0 &\subset \mathcal{M}_K \\ B &\mapsto H_1(B), \end{aligned}$$

we can think of $H_1(\mathrm{Res}_{L/K}(A_L))$ as $\mathrm{Ind}_L^K(H_1(A_L))$, where the induction is taken in the sense of motivic Galois representations (note that the quotient $\mathcal{G}_K/\mathcal{G}_L$ is canonically $\mathrm{Gal}(L/K)$, so this is just the usual induction from a finite-index subgroup). Frobenius reciprocity then implies the existence of a non-zero map $M \to \mathrm{Ind}_L^K(H_1(A_L))$ in $\mathcal{M}_K$. Since M is a simple motive, this map realizes it as a direct summand in $\mathcal{M}_K$, and consequently (full-faithfulness) in AV_K^0 as well. That is, there is an endomorphism of $\mathrm{Res}_{L/K}(A_L)$ whose image is an abelian variety A over K with $H_1(A) \cong M$. □

Proof of Lemma 3.5. Since $\bar{\mathcal{K}}$ is also countable, we may replace $\mathcal{K}$ by $\bar{\mathcal{K}}$, i.e., assume that $\mathcal{K}$ is algebraically closed. Since the isogeny class of $\mathcal{A}$ consists of a countable set of (complex) abelian varieties (up to an isomorphism), we conclude that the set $\mathrm{Aut}(\mathbf{C}/\mathcal{K})(\mathcal{A})$ of isomorphism classes of complex abelian varieties of the form $\{{}^{\sigma}\mathcal{A} \mid \sigma \in \mathrm{Aut}(\mathbf{C}/\mathcal{K})\}$ is either finite or countable.

Our plan is as follows. Let us consider a *fine* moduli space $\mathcal{A}_{g,?}$ over $\overline{\mathbb{Q}}$ of g-dimensional abelian varieties (schemes) with certain additional structures (there should be only finitely many choices of these structures for any given abelian variety) such that it is a quasiprojective subvariety in some projective space $\mathbf{P}^N$. Choose these additional structures for $\mathcal{A}$ (there should be only finitely many choices) and let $P \in \mathcal{A}_{g,?}(\mathbf{C})$ be the corresponding point of our moduli space. We need to prove that

$$P \in \mathcal{A}_{g,?}(\mathcal{K}).$$

Suppose that it is not true. Then the orbit $\mathrm{Aut}(\mathbf{C}/\mathcal{K})(P)$ of P is *uncountable*. Indeed, P lies in one of the $(N+1)$ affine charts/spaces $\mathbf{A}^N$ that do cover $\mathbf{P}^N$. This implies that P does *not* belong to $\mathbf{A}^N(\mathcal{K})$ and therefore (at least) one of its coordinates is transcendental over $\mathcal{K}$. But the $\mathrm{Aut}(\mathbf{C}/\mathcal{K})$-orbit of this coordinate coincides with uncountable $\mathbf{C} \setminus \mathcal{K}$ and therefore the $\mathrm{Aut}(\mathbf{C}/\mathcal{K})$-orbit $\mathrm{Aut}(\mathbf{C}/\mathcal{K})(P)$ of P is uncountable in $\mathcal{A}_{g,?}(\mathbf{C})$. However, for each $\sigma \in \mathrm{Aut}(\mathbf{C}/\mathcal{K})$ the point $\sigma(P)$ corresponds to ${}^{\sigma}\mathcal{A}$ with some additional structures and there are only finitely many choices for these structures. Since we know that the orbit $\mathrm{Aut}(\mathbf{C}/\mathcal{K})(\mathcal{A})$ of $\mathcal{A}$, is, at most, countable, we conclude that the orbit $\mathrm{Aut}(\mathbf{C}/\mathcal{K})(P)$ of P is also, at most, countable, which is not the case. This gives us a desired contradiction.

We choose as $\mathcal{A}_{g,?}$ the moduli space of (polarized) abelian schemes of relative dimension g with theta structures of type δ that was introduced and studied by D. Mumford [21]. In order to choose (define) a suitable δ, let us pick a totally symmetric ample invertible sheaf $\mathcal{L}_0$ on $\mathcal{A}$ [21, Sect. 2] and consider its 8th power $\mathcal{L} := \mathcal{L}_0^8$ in $\mathrm{Pic}(\mathcal{A})$. Then $\mathcal{L}$ is a very ample invertible sheaf that defines a polarization $\Lambda(\mathcal{L})$ on $\mathcal{A}$ [21, Part I, Sect. 1] that is a canonical isogeny from $\mathcal{A}$ to its dual; the kernel $H(\mathcal{L})$ of $\Lambda(\mathcal{L})$ is a finite commutative subgroup of $\mathcal{A}(\mathbf{C})$ (that contains all points of order 8). The order of $H(\mathcal{L})$ is the degree of the polarization. The type δ is essentially the isomorphism class of the group $H(\mathcal{L})$ [21, Part I, Sect. 1, p. 294]. The resulting moduli space M_δ [21, Part II, Sect. 6] enjoys all the properties that we used in the course of the proof. □

Here is the anabelian application:

Corollary 3.6 *Suppose $s \in S_0(K, \mathcal{A}_g)$ gives rise to a system of ℓ-adic Galois representations one of which is absolutely irreducible. Then there exists up to isomorphism a unique abelian variety B/K with $\sigma_{\mathcal{A}_g/K}(B) = s$.*

Proof. Let us write s_ℓ for the ℓ-adic representation associated to s; thus s_ℓ is a representation of G_K on a free $\mathbf{Z}_\ell$-module of rank $2g$, automatically satisfying Hypothesis 2 of Theorem 3.1 since s belongs to $S_0(K, \mathcal{A}_g)$. Hypothesis 1 of Theorem 3.1 is satisfied by assumption, so we obtain an abelian variety A/K (well-defined up to isogeny) whose rational Tate modules $V_\ell(A)$ are isomorphic to the given $s_\ell \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ (for all ℓ). Moreover Hypothesis 1 implies that the endomorphism ring of A is $\mathbf{Z}$. It remains to see that within the isogeny class of A there is an abelian variety B over K whose integral Tate modules $T_\ell(B)$ are isomorphic to the s_ℓ (as $\mathbf{Z}_\ell$-representations), i.e. such that $\sigma_{\mathcal{A}_g/K}(B) = s$. For this, we first observe that by [2, Proposition 3.3] (which readily generalizes to abelian varieties of any dimension), it suffices to show that for almost all ℓ, there is an isomorphism $T_\ell(A) \cong s_\ell$. Since $\mathrm{End}(A) = \mathbf{Z}$, [40, Corollary 5.4.5] implies that $A[\ell]$ is absolutely simple for almost all ℓ, and hence that for almost all ℓ, all Galois-stable lattices in $V_\ell(A)$ are of the form $\ell^m T_\ell(A)$ for some integer m; we conclude that $T_\ell(A)$ is isomorphic to s_ℓ for almost all ℓ. Thus there exists B in the isogeny class of A such that $\sigma_{\mathcal{A}_g/K}(B) = s$. This B is moreover unique up to isomorphism since $\mathrm{End}(B) = \mathbf{Z}$ does not have locally trivial, non-trivial rank one modules. □

Results in the same vein as this corollary have been obtained for elliptic curves over $\mathbf{Q}$ in [12] and [34] and for elliptic curves over function fields in [38].

Now we will construct an example of Galois representation that will provide us with examples that show that some of the hypotheses of the above results are indispensable.

Recall that if L is a field then we write $\bar{L}$ for its algebraic closure and G_L for its absolute Galois group $\mathrm{Aut}(\bar{L}/L)$. If Y is an abelian variety over a field L then we write $\mathrm{End}(Y)$ for its ring of all $\bar{L}$-endomorphisms and $\mathrm{End}^0(Y)$ for the corresponding (finite-dimensional semisimple) $\mathbf{Q}$-algebra $\mathrm{End}(Y) \otimes \mathbf{Q}$. If ℓ is a prime different from $\mathrm{char}(L)$ then we write $T_\ell(Y)$ for the $\mathbf{Z}_\ell$-Tate module of Y that is a free $\mathbf{Z}_\ell$-module of rank $2\dim(Y)$ provided with the natural continuous homomorphism

$$\rho_{\ell,Y} : G_L \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(Y))$$

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

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

If all endomorphisms of Y are defined over L then the image of $\mathrm{End}(Y) \otimes \mathbf{Z}_\ell$ commutes with $\rho_{\ell,Y}(G_L)$. Tensoring by $\mathbf{Q}_\ell$ (over $\mathbf{Z}_\ell$), we obtain the $\mathbf{Q}_\ell$-Tate module of Y

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

which is a 2dim (Y)-dimensional $\mathbf{Q}_\ell$-vector space containing $T_\ell(Y) = T_\ell(Y) \otimes 1$ as a $\mathbf{Z}_\ell$-lattice. We may view $\rho_{\ell,Y}$ as an ℓ-adic representation

$$\rho_{\ell,Y} : G_L \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(Y)) \subset \mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(Y))$$

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

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

which we still denote by e_ℓ. Further we will identify $\mathrm{End}^0(Y) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ with its image in

This provides $V_\ell(Y)$ with the natural structure of G_L-module; in addition, if all endomorphisms of Y are defined over L then $\mathrm{End}^0(Y) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is a $\mathbf{Q}_\ell$-(sub)algebra of endomorphisms of the Galois module $V_\ell(Y)$. In other words,

$$\mathrm{End}^0(Y) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \subset \mathrm{End}_{G_L}(V_\ell(Y)).$$

Let k be a real quadratic field. Let us choose a prime p that splits in k. Now let D be the indefinite quaternion k-algebra that splits everywhere outside (two) prime divisors of p and is ramified at these divisors. If a prime $\ell \ne p$ then we have

$$D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell = [D \otimes_k k] \otimes_{\mathbf{Q}} \mathbf{Q}_\ell = D \otimes_k [k \otimes_{\mathbf{Q}} \mathbf{Q}_\ell].$$

This implies that if $\ell \ne p$ is a prime then $D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is either (isomorphic to) the *simple* matrix algebra (of size 2) over a quadratic extension of $\mathbf{Q}_\ell$ or a direct sum of two copies of of the *simple* matrix algebra (of size 2) over $\mathbf{Q}_\ell$. (In both cases, $D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is isomorphic to the matrix algebra of size 2 over $k \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$.

In particular, the image of $D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ under each nonzero $\mathbf{Q}_\ell$-algebra homomorphism contains *zero divisors*.

Let Y be an abelian variety over field L. Suppose that all endomorphisms of Y are defined over L and there is a $\mathbf{Q}$-algebra embedding

$$D \hookrightarrow \mathrm{End}^0(Y)$$

that sends 1 to 1. This gives us the embedding

$$D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \subset \mathrm{End}^0(Y) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \subset \mathrm{End}_{G_L}(V_\ell(Y)).$$

Recall that if $\ell \neq p$ then $D\otimes_{\mathbf{Q}}\mathbf{Q}_\ell$ is isomorphic to the matrix algebra of size 2 over $k\otimes_{\mathbf{Q}}\mathbf{Q}_\ell$. This implies that there are two isomorphic $\mathbf{Q}_\ell[G_L]$-submodule $W_{1,\ell}(Y)$ and $W_{2,\ell}(Y)$ in $V_\ell(Y)$ such that

$$V_\ell(Y) = W_{1,\ell}(Y) \oplus W_{2,\ell}(Y) \cong W_{1,\ell}(Y) \oplus W_{1,\ell}(Y) \cong W_{2,\ell}(Y) \oplus W_{2,\ell}(Y).$$

If we denote by $W_\ell(Y)$ the $\mathbf{Q}_\ell[G_L]$-module $W_{1,\ell}$ then we get an isomorphism of $\mathbf{Q}_\ell[G_L]$-modules

$$V_\ell(Y) \cong W_\ell(Y) \oplus W_\ell(Y).$$

If $\ell = p$ then $D\otimes_{\mathbf{Q}}\mathbf{Q}_p$ splits into a direct sum of two (mutually isomorphic) quaternion algebras over $\mathbf{Q}_p$. This also gives us a splitting of the Galois module $V_\ell(Y)$ into a direct sum

$$V_\ell(Y) = W_{1,p}(Y) \oplus W_{2,p}(Y).$$

of its certain nonzero $\mathbf{Q}_p[G_L]$-submodules $W_{1,p}(Y)$ and $W_{2,p}(Y)$. (In fact, one may check that

$$\dim_{\mathbf{Q}_p} W_{1,p} = \dim_{\mathbf{Q}_p} W_{2,p} = \dim(Y).)$$

Remark. Suppose that $D = \mathrm{End}^0(Y)$. Then it follows from Faltings' results about the Galois action on Tate modules of abelian varieties [4] that if $\ell \neq p$ then

$$\mathrm{End}_{G_L} W_\ell(Y) = k \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$$

while the G_L-module $W_{1,p}(Y)$ and $W_{2,p}(Y)$ are non-isomorphic.

According to Shimura ([32], see also the case of Type II($e_0 = 2$) with $m = 1$ in [23, Table 8.1 on p. 498] and [26, Table on p. 23]) there exists a complex abelian fourfold X, whose endomorphism algebra $\mathrm{End}^0(X)$ is isomorphic to D. Clearly, X is defined over a finitely generated field of characteristic zero. It follows from Serre's variant of Hilbert's irreducibility theorem for infinite Galois extensions combined with results of Faltings that there exists a number field K and an abelian fourfold A over K such that the endomorphism algebra $\mathrm{End}^0(A)$ of all $\bar{K}$-endomorphisms of A is also isomorphic to D (see [22, Cor. 1.5 on p. 165]). Enlarging K, we may assume that all points of order 12 on A are defined over K. Now Raynaud's criterion ([7], see also [30]) implies that A has everywhere semistable reduction. On the other hand,

$$\dim_{\mathbf{Q}} \mathrm{End}^0(A) = \dim_{\mathbf{Q}} D = 8 > 4 = \dim(A).$$

By [23, Lemma 3.9 on p. 484], A has everywhere potential good reduction. This implies that A has good reduction everywhere. If v is a nonarchimedean place of K with finite residue field $\kappa(v)$ then we write $A(v)$ for the reduction of A at v; clearly, $A(v)$ is an abelian fourfold over $\kappa(v)$. If $\mathrm{char}(\kappa(v)) \ne 2$ then all points of order 4 on $A(v)$ are defined over $\kappa(v)$; if $\mathrm{char}(\kappa(v)) \ne 3$ then all points of order 3 on $A(v)$ are defined over $\kappa(v)$. It follows from a theorem of Silverberg [29] that all $\overline{\kappa(v)}$-endomorphisms of $A(v)$ are defined over $\kappa(v)$. (The same result implies that all $\bar{K}$-endomorphisms of A are defined over K.) For each v we get an embedding of $\mathbf{Q}$-algebras

$$D \cong \mathrm{End}^0(A) \hookrightarrow \mathrm{End}^0(A(v)).$$

In particular, $\mathrm{End}^0(A(v))$ is a *noncommutative* $\mathbf{Q}$-algebra, whose $\mathbf{Q}$-dimension is divisible by 8.

Theorem 3.7 *If $\ell := \mathrm{char}(\kappa(v)) \ne p$ then $A(v)$ is not simple over $\kappa(v)$.*

Proof. We write q_v for the cardinality of $\kappa(v)$. Clearly, q_v is a power of ℓ.

Suppose that $A(v)$ is simple over $\kappa(v)$. Since all endomorphisms of $A(v)$ are defined over $\kappa(v)$, the abelian variety $A(v)$ is *absolutely simple*.

Let π be a *Weil q_v-number* that corresponds to the $\kappa(v)$-isogeny class of $A(v)$ [36, 37]. In particular, π is an algebraic integer (complex number), all whose Galois conjugates have (complex) absolute value $\sqrt{q_v}$. In particular, the product

$$\pi\bar{\pi} = q_v,$$

where $\bar{\pi}$ is the complex conjugate of π.

Let $E = \mathbf{Q}(\pi)$ be the number field generated by π and let $\mathcal{O}_E$ be the ring of integers in E. Then E contains $\bar{\pi}$ and is isomorphic to the center of $\mathrm{End}^0(A(v))$ [36, 37]; one may view $\mathrm{End}^0(A(v))$ as a *central* division algebra over E. It is known that E is either $\mathbf{Q}$, $\mathbf{Q}(\sqrt{\ell})$ or a (purely imaginary) CM field [37, p. 97]. It is known (ibid) that in the first two (totally real) cases simple $A(v)$ has dimension 1 or 2, which is not the case. So, E is a CM field; Since $\dim(A(v)) = 4$ and $[E : \mathbf{Q}]$ divides $2\dim(A(v))$, we have $[E : \mathbf{Q}] = 2, 4$ or 8. By [37, p. 96, Th. 1(ii), formula (2)] [2],

$$8 = 2 \cdot 4 = 2\dim(A(v))) = \sqrt{\dim_E(\mathrm{End}^0(A(v))} \cdot [E : \mathbf{Q}].$$

[2] In [37] our E is denoted by F while our $\mathrm{End}^0(A(v))$ is denoted by E.

Since $\mathrm{End}^0(A(v))$ is *noncommutative*, it follows that E is either an imaginary quadratic field and $\mathrm{End}^0(A(v))$ is a 16-dimensional division algebra over E or E is a CM field of degree 4 and $\mathrm{End}^0(A(v))$ is a 4-dimensional (i.e., quaternion) division algebra over E. In both cases $\mathrm{End}^0(A(v))$ is unramified at all places of E except some places of residual characteristic ℓ [37, p. 96, Th. 1(ii)]. It follows from the Hasse–Brauer-Noether theorem that $\mathrm{End}^0(A(v))$ is unramified at, at least, two places of E with residual characteristic ℓ. This implies that $\mathcal{O}_E$ contains, at least, two maximal ideals that lie above ℓ.

Clearly,

$$\pi, \bar{\pi} \in \mathcal{O}_E.$$

Recall that $\pi\bar{\pi} = q_v$ is a power of ℓ. This implies that for every prime $r \neq \ell$ both π and $\bar{\pi}$ are r-adic units in E.

First assume that E has degree 4 and $\mathrm{End}^0(A(v))$ is a quaternion algebra. Then (thanks to the theorem of Hasse–Brauer–Noether) there exists a place w of E with residual characteristic ℓ and such that the localization $\mathrm{End}^0(A(v)) \otimes_E E_w$ is a quaternion division algebra over the w-adic field E_w. On the other hand, there is a nonzero (because it sends 1 to 1) $\mathbf{Q}_\ell$-algebra homomorphism

$$D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \to \mathrm{End}^0(A(v)) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \twoheadrightarrow \mathrm{End}^0(A(v)) \otimes_E E_w.$$

This implies that $\mathrm{End}^0(A(v)) \otimes_E E_w$ contains zero divisors, which is not the case and we get a contradiction.

So, now we assume that E is an *imaginary quadratic* field and

$$\dim_E(\mathrm{End}^0(A(v))) = 16 = 4^2.$$

In particular, the order of the class of $\mathrm{End}^0(A(v))$ in the Brauer group of E divides 4 and therefore is either 2 or 4.

We have already seen that there exist, at least, two maximal ideals in $\mathcal{O}_E$ that lie above ℓ. Since E is an imaginary quadratic field, the ideal $\ell\mathcal{O}_L$ of $\mathcal{O}_L$ splits into a product of two distinct complex-conjugate maximal ideals w_1 and w_2 and therefore

$$E_{w_1} = \mathbf{Q}_\ell,\ E_{w_2} = \mathbf{Q}_\ell;\ [E_{w_1} : \mathbf{Q}_\ell] = [E_{w_2} : \mathbf{Q}_\ell] = 1.$$

Let

$$\mathrm{ord}_{w_i} : E^* \twoheadrightarrow \mathbf{Z}$$

be the discrete valuation map that corresponds to w_i. Recall that q_v is a power of ℓ, i.e., $q_v = \ell^N$ for a certain positive integer N. Clearly

$$\mathrm{ord}_{w_i}(\ell) = 1, \ \mathrm{ord}_{w_i}(\pi) + \mathrm{ord}_{w_i}(\bar{\pi}) = \mathrm{ord}_{w_i}(q_v) = N.$$

By [37, page 96, Th. 1(ii), formula (1)], the local invariant of $\mathrm{End}^0(A(v))$ at w_i is

$$\frac{\mathrm{ord}_{w_i}(\pi)}{\mathrm{ord}_{w_i}(q_v)} \cdot [E_{w_1} : \mathbf{Q}_\ell](\mathrm{mod} 1) = \frac{\mathrm{ord}_{w_i}(\pi)}{N}(\mathrm{mod} 1).$$

In addition, the sum in $\mathbf{Q}/\mathbf{Z}$ of local invariants of $\mathrm{End}^0(A(v))$ at w_1 and w_2 is zero [37, Sect. 1, Theorem 1 and Example b)]; we have already seen that its local invariants at all other places of E do vanish. Using the Hasse–Brauer-Noether theorem and taking into account that the order of the class of $\mathrm{End}^0(A(v))$ in the Brauer group of E is either 2 or 4, we conclude that the local invariants of $\mathrm{End}^0(A(v))$ at $\{w_1, w_2\}$ are either $\{1/4 \bmod 1, 3/4 \bmod 1\}$ or $\{3/4 \bmod 1, 1/4 \bmod 1\}$ (and in both cases the order of $\mathrm{End}^0(A(v))$ in the Brauer group of E is 4) or $\{1/2 \bmod 1, 1/2 \bmod 1\}$. In the latter case it follows from the formula for the w_i-adic invariant of $\mathrm{End}^0(A(v))$ that

$$\mathrm{ord}_{w_i}(\pi) = \frac{N}{2} = \mathrm{ord}_{w_i}(\bar{\pi})$$

and therefore $\bar{\pi}/\pi$ is a w_i-adic unit for both w_1 and w_2. Therefore $\bar{\pi}/\pi$ is an ℓ-adic unit. This implies that $\bar{\pi}/\pi$ is a unit in imaginary quadratic E and therefore is a root of unity. It follows that

$$\frac{\pi^2}{q_v} = \frac{\pi^2}{\pi\bar{\pi}} = \frac{\pi}{\bar{\pi}}$$

is a root of unity. This implies that there is a positive (even) integer m such that

$$\pi^m = q_v^{m/2} \in \mathbf{Q}$$

and therefore $\mathbf{Q}(\pi^m) = \mathbf{Q}$. Let $\kappa(v)_m$ be the finite degree m field extension of $\kappa(v)$, which consists of q_v^m elements. Then π^m is the Weil q_v^m-number that corresponds to the simple 4-dimensional abelian variety $A(v) \times \kappa(v)_m$ over $\kappa(v)_m$. Since $\mathbf{Q}(\pi^m) = \mathbf{Q}$, we conclude (as above) that $A(v) \times \kappa(v)_m$ has dimension 1 or 2, which is not the case.

In both remaining cases the order of the algebra $\mathrm{End}^0(A(v)) \otimes_E E_{w_1}$ in the Brauer group of the $E_{w_1} \cong \mathbf{Q}_\ell$ is 4. This implies that $\mathrm{End}^0(A(v)) \otimes_E E_{w_1}$

is neither the matrix algebra of size 4 over E_{w_1} nor the matrix algebra of size two over a quaternion algebra over E_{w_1}. The only remaining possibility is that $\mathrm{End}^0(A(v)) \otimes_E E_{w_1}$ is a *division algebra* over E_{w_1}. However, there is again a nonzero (because it sends 1 to 1) $\mathbf{Q}_\ell$-algebra homomorphism

$$D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \to \mathrm{End}^0(A(v)) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \twoheadrightarrow \mathrm{End}^0(A(v)) \otimes_E E_{w_1}.$$

This implies that $\mathrm{End}^0(A(v)) \otimes_E E_{w_1}$ contains zero divisors, which is not the case and we get a contradiction. □

Now let us split $A(v)$ up to a $\kappa(v)$-isogeny into a product of its $\kappa(v)$-isotypic components (see, e.g., [31, Sect. 3]). In other words, there is a $\kappa(v)$-isogeny

$$S : \prod_{i \in I} A_i \to A(v)$$

where each A_i is a nonzero abelian $\kappa(v)$-subvariety in A such that $\mathrm{End}^0(A_i)$ is a *simple* $\mathbf{Q}$-algebra and S induces an isomorphism iof $\mathbf{Q}$-algebras

$$\mathrm{End}^0(A(v)) \cong \mathrm{End}^0(\prod_{i \in I} A_i) = \oplus_{i \in I} \mathrm{End}^0(A_i).$$

This gives us a nonzero $\mathbf{Q}$-algebra isomorphisms

$$D \to \mathrm{End}^0(A_i)$$

that must be injective, since D is a *simple* $\mathbf{Q}$-algebra. This implies that each $\mathrm{End}^0(A_i)$ is a noncommutative simple $\mathbf{Q}$-algebra, whose $\mathbf{Q}$-dimension is divisible by 8. In particular, all $\dim(A_i) \geq 2$ and therefore I consists of, at most, 2 elements, since

$$\sum_{i \in I} \dim(A_i) = \dim(A(v)) = 4.$$

If we have $\dim(A_i) = 2$ for some i then either A_i is isogenous to a square of a supersingular elliptic curve or A_i is an absolutely simple abelian surface. However, each absolutely simple abelian surface over a finite field is either *ordinary* (i.e., the slopes of its Newton polygon are 0 and 1, both of length 2) or *almost ordinary* (i.e., the slopes of its Newton polygon are 0 and 1, both of length 1, and 1/2 with length 2): this assertion is well known and follows easily from [39, Remark 4.1 on p. 2088]. However, in both (ordinary and almost ordinary) cases the endomorphism algebra of a simple abelian variety is commutative [25]. This implies that if $\dim(A_i) = 2$ then A_i is $\kappa(v)$-isogenous to a square of a supersingular elliptic curve. However, if I consists of two elements say, i and j then it follows that both A_i and A_j are 2-dimensional and therefore both isogenous to a square of a supersingular elliptic curve. This implies that A_i and A_j are isotypic and therefore A itself is isotypic and we get a contradiction, i.e., none of A_i has dimension 2. It is also clear that if $\dim(A_i) = 3$ then $\dim(A_j) = 1$, which could not be the case. This implies that $A(v)$ itself is isotypic. This implies that if $\ell = \mathrm{char}(\kappa(v)) \neq p$ then $A(v)$ is $\kappa(v)$-isogenous either to a 4th power of an elliptic curve or to a square of an abelian surface over $\kappa(v)$ (recall that $A(v)$ is not simple!). In both cases there exists an abelian surface $B(v)$ over $\kappa(v)$, whose square $B(v)^2$ is $\kappa(v)$-isogenous to $A(v)$. Now one may lift $B(v)$ to an abelian surface B^v over K_v, whose reduction is $B(v)$ (see [24, Prop. 11.1 on p. 177]). Now if one restricts the action of G_K on the $\mathbf{Q}_r$-Tate module (here r is any prime different from $\mathrm{char}(\kappa(v))$

$$V_r(A) = T_r(A) \otimes \mathbf{Q}_r$$

to the decomposition group $D(v) = G_{K_v}$ then the corresponding G_{K_v}-module $V_r(A)$ is *unramified* (i.e., the inertia group acts trivially) and isomorphic to

$$V_r(B^v) \oplus V_r(B^v).$$

Theorem 3.8 *If $r \neq p$ and $\mathrm{char}(\kappa(v)) \neq r$ then the G_{K_v}-modules $V_r(B^v)$ and $W_r(A)$ are isomorphic. In particular, the G_{K_v}-modules*

$$V_r(A) = W_r(A) \oplus W_r(A)$$

and

$$V_r(B^v) \oplus V_r(B^v) = V_r((B^v)^2)$$

are isomorphic.

Proof. We know that the G_{K_v}-modules $W_r(A) \oplus W_r(A)$ and $V_r(B^v) \oplus V_r(B^v)$ are both isomorphic to $V_\ell(A)$. Since the Frobenius endomorphism of $A(v)$ acts on $V_\ell(A)$ as a semisimple linear operator (by a theorem of A. Weil), the G_{K_v}-module $V_\ell(A)$ is semisimple. This implies that the G_{K_v}-modules $V_r(B^v)$ and $W_r(A)$ are isomorphic. □

For primes $\ell \neq p$, the algebra $D \otimes \mathbf{Q}_\ell$ splits and correspondingly, the representation $V_\ell(A)$ splits as $W_\ell \oplus W_\ell$. Locally, at a place $v \nmid \ell$, we have $W_\ell \cong V_\ell(B^v)$ but the representation W_ℓ does not come from an abelian variety, as A is simple. However, locally at $v \nmid \ell$, W_ℓ comes from the abelian variety B^v. The system of representations $\{W_\ell\}_{\ell \neq p}$ provides an example showing that the previous result would be false under weaker requirements on the sets of ℓ and v for which the representation locally comes from an abelian variety.

4 Abelian varieties with isomorphic Tate modules

Throughout this section, K is a field. A and B are abelian varieties of positive dimension over K. Recall that $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbf{Q}$. If ℓ is a positive integer then we write $\mathbf{Z}_{(\ell)}$ for the subring in $\mathbf{Q}$ that consists of all the rational numbers, whose denominators are powers of ℓ. We have

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

In this section we discuss the structure of the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A, B)$ when the $\mathbf{Z}_\ell$-Tate modules of A and B are isomorphic as Galois modules for all ℓ and K is finitely generated over $\mathbf{Q}$. If $\ell \neq \mathrm{char}(K)$ 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 homomorphism of G_K-modules $X[\ell] \cong T_\ell(X)/\ell T_\ell(X)$.

Lemma 4.1 *Let A and B be abelian varieties of positive dimension over K.*

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

(b) *The following conditions are equivalent.*

(i) *The right $\mathrm{End}(A) \otimes \mathbf{Q}$-module $\mathrm{Hom}(A, B) \otimes \mathbf{Q}$ 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 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 $\mathrm{Hom}(A, B_0) \otimes \mathbf{Q} = \phi\,\mathrm{End}^0(A)$ is a free right $\mathrm{End}^0(A)$-module of rank 1 generated by ϕ. Now (bi) follows from the equality

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

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 $\mathrm{End}(A) \otimes \mathbf{Q}$-module $\mathrm{Hom}(A, B) \otimes \mathbf{Q}$. 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

Poincaré reducibility theorem there is $u_0 \in \mathrm{End}(A)$ 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 4.2 *Suppose that A, B, C are abelian varieties over K of positive dimension that are mutually isogenous over K. We view* $\mathrm{Hom}(A, B)$ *and* $\mathrm{Hom}(A, C)$ *as right* $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbf{Q}$*-modules. Then the natural map*

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

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

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

is a group isomorphism.

Proof. Clearly, $m_{B,C}$ is injective. In order to check the surjectiveness, recall that $\mathrm{Hom}(A, B) \otimes \mathbf{Q}$ is a free right $\mathrm{End}^0(A)$-module of rank 1 and one may choose as its generator an isogeny $\phi : A \to B$. Then every homomorphism $\delta : \mathrm{Hom}(A, B) \otimes \mathbf{Q} \to \mathrm{Hom}(A, C) \otimes \mathbf{Q}$ is uniquely determined by the image $\delta(\phi) \in \mathrm{Hom}(A, C) \otimes \mathbf{Q}$. We have $\phi^{-1} \in \mathrm{Hom}(B, A) \otimes \mathbf{Q}$. Now if we put

$$\tau := \delta(\phi)\phi^{-1} \in \mathrm{Hom}(B, C) \otimes \mathbf{Q}$$

then

$$m_{B,C}(\tau)(\phi) = \delta(\phi)\phi^{-1}\phi = \delta(\phi)$$

and therefore $\delta = m_{B,C}(\tau)$. □

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

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

Lemma 4.3 *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 $\mathbf{Z}_\ell[G_K]$-Galois modules.

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

Suppose that (ii) holds. Since the rank of the free $\mathbf{Z}_\ell$-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 $\mathbf{Z}_\ell$-Tate modules of A and B that lies in $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$. Since $\mathrm{Hom}(A, B)$ is dense in $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$ in the ℓ-adic topology, and the set of isomorphisms $T_\ell(A) \cong T_\ell(B)$ is open in $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$, 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 4.3, one has only to observe that

$$\phi_\ell \in \mathrm{Hom}(A, B) \subset \mathrm{Hom}(A, B) \otimes \mathbf{Z}_{(\ell)} \subset \mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$$

is a generator of the (obviously) free right $\mathbf{Z}_{(\ell)}$-module $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_{(\ell)}$ and of the free right $\mathbf{Z}_\ell$-module $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$. □

We say that A and B are *almost isomorphic* if for *all primes* ℓ the equivalent conditions (i) and (ii) of Lemma 4.3 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 4.4 *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.

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 next statement is a generalization of Corollary 4.4.

Corollary 4.5 *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 $\mathbf{Q}$-linearity to the isomorphism $\mathrm{Hom}(A,B)\otimes\mathbf{Q} \to \mathrm{Hom}(A,C)\otimes\mathbf{Q}$ of right $\mathrm{End}(A)\otimes\mathbf{Q}$-modules, which we continue to denote by δ. By Lemma 4.2, there exists $\tau_0 \in \mathrm{Hom}(B,C)\otimes\mathbf{Q}$ such that $\delta = m_{B,C}(\tau_0)$, i.e.,

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

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. □

Theorem 4.6 (Theorem-Construction) *Let Λ be a a ring with 1 that, viewed as an additive group, is a free $\mathbf{Z}$-module of finite positive rank. Let M be an arbitrary free commutative group of finite positive rank that is provided with a structure of a right Λ-module. Suppose that M enjoys the following properties.*

(i) The right $\Lambda \otimes \mathbf{Q}$-module $M \otimes \mathbf{Q}$ is free of rank 1;

(ii) For all primes ℓ the right $\Lambda \otimes \mathbf{Z}_\ell$-module $M \otimes \mathbf{Z}_\ell$ is free of rank 1.

Then M also enjoys the following properties.

(iii) Let n be a positive integer. Then there is a positive integer m that is relatively prime to n and such that the right $\Lambda \otimes \mathbf{Z}[1/m]$-module $M \otimes \mathbf{Z}[1/m]$ is free of rank 1.

(iv) Let $r > 1$ be a positive integer that is relatively prime to m and such that the right $\Lambda \otimes \mathbf{Z}[1/r]$-module $M \otimes \mathbf{Z}[1/r]$ is free of rank 1. (The existence of such an r follows from (iii).) Let us choose a generator (basis)

$$e_m \in M = M \otimes 1 \subset M \otimes \mathbf{Z}[1/m]$$

of the free $\mathbf{Z}[1/m]$-module $M \otimes \mathbf{Z}[1/m]$ and a generator (basis)

$$e_r \in M = M \otimes 1 \subset M \otimes \mathbf{Z}[1/r]$$

of the free $\mathbf{Z}[1/r]$-module $M \otimes \mathbf{Z}[1/r]$. Let

$$F_2 = \Lambda \oplus \Lambda = f_1\Lambda \oplus f_2\Lambda$$

be a rank 2 free right Λ-module with basis $\{f_1, f_2\}$. Then the homomorphism of right Λ-modules

$$\beta : F_2 \to M,\ \ f_1a_1 + f_2a_2 \mapsto e_1a_1 + e_2a_2$$

is surjective.

(v) *There exists a homomorphism of right Λ-modules*

$$\alpha : M \to F_2$$

that is a section of β. In particular, M is (isomorphic to) a direct summand $M' = \alpha(M)$ of F_2 and therefore is a projective Λ-module. In addition,

$$\gamma = \alpha\beta \in \mathrm{End}_{\Lambda}(F_2)$$

is an idempotent with $\gamma(F_2) = M' \cong M$.

Proof. Let us prove (iii). If $n = 1$ then we pick an element $\phi \in M$ that is a generator of $M \otimes \mathbf{Q}$. Then $\phi\dot{\Lambda} \subset M$ is a $\mathbf{Z}$-lattice in the finite-dimensional $\mathbf{Q}$-vector space $M \otimes \mathbf{Q}$. This implies that the ranks of (free) commutative groups $\phi\dot{\Lambda}$ and M do coincide and therefore $\phi\dot{\Lambda}$ is a subgroup of finite index in M. Now one has take as m this index.

If $n > 1$ then for each prime ℓ dividing n choose a generator ϕ_ℓ of $M \otimes \mathbf{Z}_\ell$. Since the group of units in $\Lambda \otimes \mathbf{Z}_\ell$ is open in ℓ-adic topology, the set of generators in $M \otimes \mathbf{Z}_\ell$ is also open in ℓ-adic topology. Since M is dense in $\prod_{\ell \mid n} M \otimes \mathbf{Z}_\ell$ with respect to the product topology (the ℓth factor is provided by ℓ-adic topology, there exists $\phi \in M$ that is a generator of $M \otimes \mathbf{Z}_\ell$ for all ℓ dividing n. Let $\phi_0 \subset M \otimes \mathbf{Q}$ be a generator of $M \otimes \mathbf{Q}$. Multiplying ϕ_0 by a sufficiently divisible nonzero integer, we may and will assume that $\phi_0 \in M$. Then there is $a \in \Lambda \otimes \mathbf{Q}$ such that $\phi = \phi_0 a$. If ℓ is a prime dividing n then we know that for all nonzero $b \in \Lambda \otimes \mathbf{Z}_\ell$

$$0 \neq \phi b = (\phi_0 a) b = \phi_0 (ab) \in M \otimes \mathbf{Z}_\ell,$$

because ϕ is a generator of the free right $\Lambda \otimes \mathbf{Z}_\ell$-module $M \otimes \mathbf{Z}_\ell$ of rank 1. This means that $ab \neq 0$. It follows that for each nonzero $b \in \Lambda$ the product $ab \neq 0$; obviously, the inequality remains true for all nonzero $b \in \Lambda \otimes \mathbf{Q}$. Since $\Lambda \otimes \mathbf{Q}$ is a finite-dimensional $\mathbf{Q}$-algebra, the $\mathbf{Q}$-subspace $[\Lambda \otimes \mathbf{Q}] \cdot a$ has the same $\mathbf{Q}$-dimension as $\Lambda \otimes \mathbf{Q}$ and therefore coincides with $\Lambda \otimes \mathbf{Q}$. Since Λ (and therefore $\Lambda \otimes \mathbf{Q}$) contains 1, there is $b \in \Lambda \otimes \mathbf{Q}$ such that $ba = 1$ and therefore a is invertible in $\Lambda \otimes \mathbf{Q}$, which implies that ϕ is also a generator of the $\Lambda \otimes \mathbf{Q}$-module $M \otimes \mathbf{Q}$. As above, this implies that $\phi \cdot \Lambda$ is a subgroup of finite index in M and we take as m this index. If d is the rank of the free $\mathbf{Z}$-module M, there is a basis $\{y_1, \dots, y_d\}$ of M and positive integers $\{m_1, \dots, m_d\}$ such that

$$\phi \cdot \Lambda = \oplus_{i=1}^{d} m_i \mathbf{Z} \cdot y_i \subset \oplus_{i=1}^{d} \mathbf{Z} \cdot y_i = M.$$

The index m coincides with the product $\prod_{i=1}^{d} m_i$. The completion of $\phi \cdot \Lambda$ (with respect to ℓ-adic topology) in

$$M \otimes \mathbf{Z}_\ell = \oplus_{i=1}^{d} \mathbf{Z}_\ell \cdot y_i$$

is $\oplus_{i=1}^{d} m_i \mathbf{Z}_\ell \cdot y_i$, which coincides with $M \otimes \mathbf{Z}_\ell$ if and only if *all* m_i are *not* divisible by ℓ, i.e., if and only if m is *not* divisible by ℓ. However, since ϕ is a generator of $M \otimes \mathbf{Z}_\ell$ (when $\ell \mid n$) and Λ is dense in $\Lambda \otimes \mathbf{Z}_\ell$ (with respect to ℓ-adic topology) the subgroup $\phi \cdot \Lambda$ is dense in

$$\phi \cdot [\Lambda \otimes \mathbf{Z}_\ell] = M \otimes \mathbf{Z}_\ell.$$

This implies that m is *not* divisible by ℓ for all ℓ dividing n. This means that n and m are relatively prime. This ends the proof of (iii).

Proof of (iv). Clearly, $M/(e_m \cdot \Lambda)$ is a commutative periodic group, all whose elements have orders dividing a power of m and $M/(e_r \cdot \Lambda)$ is a commutative periodic group, all whose elements have orders dividing a power of r. Since M is a finitely generated $\mathbf{Z}$-module, both quotients are finite commutative groups, whose orders divide certain powers of m and r respectively. This implies that $M/(e_m \cdot \Lambda e_m + e_r \cdot \Lambda)$ is a finite commutative group, whose order divides a certain power of m and a certain power of r. Since m and r are relatively prime, the order of $M/(e_m \cdot \Lambda e_m + e_r \cdot \Lambda)$ is 1, i.e., $M = e_m \cdot \Lambda + e_r \cdot \Lambda$. Now $\beta : F_2 \to M$ is surjective, because by the very definition of β,

$$e_m \cdot \Lambda + e_r \cdot \Lambda = \beta(\mathbf{F}_2).$$

Proof of (v). Since $M \otimes \mathbf{Z}[1/m]$ and $M \otimes \mathbf{Z}[1/r]$ are free modules over $\Lambda[1/m]$ and $\Lambda[1/r]$ respectively, there exist *sections*

$$u_m : M \otimes \mathbf{Z}[1/m] \hookrightarrow F_2 \otimes \mathbf{Z}[1/m], \ u_m : M \otimes \mathbf{Z}[1/r] \hookrightarrow F_2 \otimes \mathbf{Z}[1/r]$$

of

$$\beta \otimes \mathbf{Z}[1/m] : F_2 \to M \otimes \mathbf{Z}[1/m]$$

and

$$\beta \otimes \mathbf{Z}[1/r] : F_2 \to M \otimes \mathbf{Z}[1/r]$$

respectively. Since M is finitely generated $\mathbf{Z}$-module, there exist nonnegative integers i and j such that

$$m^i u_m(M) \subset F_2, \ r^j u_r(M) \subset M.$$

We have

$$\beta(m^i u_m(z)) = m^i z, \ \beta(r^j u_r(z)) = r^j z \ \forall z \in M.$$

Since m and r are relatively prime, there exist integers c and d such that $cm^i + dr^j = 1$. This implies that the homomorphism of right Λ-modules

$$\alpha := c \cdot m^i u_m + d \cdot r^j u_r : M \to F_2$$

is a *section* of β. In particular, M is (isomorphic to) a direct summand $M' = \alpha(M)$ of F_2 and therefore is a projective Λ-module. In addition,

$$\gamma = \alpha\beta \in \mathrm{End}_\Lambda(F_2)$$

is an idempotent with $\gamma(F_2) = M' \cong M$. □

Remark Actually, the property (i) in the statement of Theorem 4.6 follows from (ii). Indeed, suppose that there is a prime ℓ such that $M \otimes \mathbf{Z}_\ell$ is a free right $\Lambda \otimes \mathbf{Z}_\ell$-module of rank 1. This implies that the free commutative (additive) groups M and Λ have the same rank say, d, which also coincides with the dimension of the $\mathbf{Q}$-vector space $M \otimes \mathbf{Q}$. Let us choose a generator $x \in M$ of the free module $M \otimes \mathbf{Z}_\ell$. Then for each *nonzero* $a \in \Lambda \subset \Lambda \otimes \mathbf{Z}_\ell$ the product

$$x \cdot a \in M \subset M \otimes \mathbf{Z}_\ell$$

is not zero in $M \otimes \mathbf{Z}_\ell$ and therefore is not zero in M. This implies that $x \cdot \Lambda \subset M$ is a free commutative subgroup of rank d, i.e., of the same rank as $\mathcal{M}$. It follows that $x \cdot \Lambda$ is a subgroup of finite index in M and therefore $x \cdot [\Lambda \otimes \mathbf{Q}] = M \otimes \mathbf{Q}$. This means that the homomorphism of right $\Lambda \otimes \mathbf{Q}$-modules

$$\Lambda \otimes \mathbf{Q} \to M \otimes \mathbf{Q}, \ a \mapsto x \cdot a$$

is surjective and therefore is also injective, because both modules have the same (finite) $\mathbf{Q}$-dimension d. This implies that the right $\Lambda \otimes \mathbf{Q}$-module $M \otimes \mathbf{Q}$ is free of rank one.

Now we are going to use Theorem 4.6, in order to construct abelian varieties over K that are almost isomorphic to a given A. Suppose we are given a a free commutative group M of finite (positive) rank that is provided with a structure of a right $\Lambda = \mathrm{End}(A)$-module in such a way that the conditions (i) and (ii) hold of Theorem 4.6. It follows from this Theorem that the conditions (iii)-(v) also hold. In particular, there is an *idempotent*

$\gamma : F_2 \to F_2$, 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 of abelian varieties over K

$$B \times C \to A^2, \ (x, y) \mapsto x + y$$

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

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

for every prime ℓ.

Theorem 4.7 *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 $\mathrm{End}(A) \otimes \mathbf{Q}$-module $M \otimes \mathbf{Q}$ is free of rank 1, the same is true for the right $\mathrm{End}(A) \otimes \mathbf{Q}$-module $\mathrm{Hom}(A, B)$. By Lemma 4.1, $\dim(A) \leq \dim(B)$ 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 $B_0 \neq B$ then, by Poincaré reducibility theorem, 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 $\mathrm{Hom}(A, B_0) = \{0\}$. However, $B_0 \subset B \subset A^2$ 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 $M \otimes \mathbf{Z}_\ell$ is a free right $\mathrm{End}(A) \otimes \mathbf{Z}_\ell$-module of rank 1, $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$ is a free right $\mathrm{End}(A) \otimes \mathbf{Z}_\ell$-module of rank 1. Let us choose a generator $\phi \in \mathrm{Hom}(A, B)$ of the module $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$. 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 $u_1, u_2 \in \mathrm{End}(A) \otimes \mathbf{Z}_\ell$ such that

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

in $\mathrm{Hom}(A, B) \otimes \mathbf{Z}_\ell$. 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 4.8 *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 right* $\mathrm{End}(A)$*-module in such a way that $M_i \otimes \mathbf{Q}$ is a free* $\mathrm{End}(A) \otimes \mathbf{Q}$ *of rank* 1 *and for all primes ℓ the right* $\mathrm{End}(A) \otimes \mathbf{Z}_\ell$*-module $M_i \otimes \mathbf{Z}_\ell$ is free 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 4.7(ii), the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A, B_i)$ is isomorphic to M_i. Now the result follows from Theorem 4.7(iii) combined with Corollary 4.5. □

Corollary 4.9 *Let A and B be abelian varieties over K of positive dimension. Suppose that $\mathrm{Hom}(A, B) \otimes \mathbf{Q}$ is a free $\mathrm{End}(A) \otimes \mathbf{Q}$-module of rank 1 and for all primes ℓ the $\mathbf{Z}_\ell$-Tate modules of A and B are isomorphic as Galois modules. Then the abelian varieties B and $C = A \otimes \mathrm{Hom}(A, B)$ are isomorphic over K.*

Proof. By Theorem 4.7(ii), the right $\mathrm{End}(A)$-module $\mathrm{Hom}(A, C)$ is isomorphic to $\mathrm{Hom}(A, B)$. Now Now the result follows from Theorem 4.7(iii) combined with Corollary 4.5. □

Remark Suppose that A is the 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 right $\mathrm{End}(A_i)$-module such that $M_i \otimes \mathbf{Q}$ is a free $\mathrm{End}(A_i) \otimes \mathbf{Q}$ of rank 1 and for all primes ℓ the right $\mathrm{End}(A_i) \otimes \mathbf{Z}_\ell$-module $M_i \otimes \mathbf{Z}_\ell$ is free of rank 1. Then $M = M_1 \oplus M_2$ becomes a right $\mathrm{End}(A_1) \oplus \mathrm{End}(A_2) = \mathrm{End}(A)$-module such that $M \otimes \mathbf{Q}$ is a free $\mathrm{End}(A) \otimes \mathbf{Q}$ of rank 1 and for all primes ℓ the right $\mathrm{End}(A) \otimes \mathbf{Z}_\ell$-module $M \otimes \mathbf{Z}_\ell$ is free of rank 1. One may easily check that there is a canonical isomorphism between abelian varieties $A \otimes M$ and $(A_1 \otimes M_1) \times (A_2 \otimes M_2)$ over K.

5 Moduli of curves

The moduli space of smooth projective curves of genus g is denoted by $\mathcal{M}_g$. It is also an orbifold and we will consider its fundamental group as such. For definitions see [10]. It is defined over $\mathbf{Q}$ and thus we can consider it over an arbitrary number field K. As per our earlier conventions, $\bar{\mathcal{M}}_g$ is the base change of $\mathcal{M}_g$ to an algebraic closure of $\mathbf{Q}$ and not a compactification.

Let X be a curve of genus g defined over K. There is a map (an arithmetic analogue of the Dehn-Nielsen-Baer theorem, see [15]) $\rho : \pi_1(\mathcal{M}_g) \to Out(\pi_1(X))$. This follows by considering the universal curve $\mathcal{C}_g$ of genus g

together with the map $\mathcal{C}_g \to \mathcal{M}_g$, so X can be viewed as a fiber of this map. This gives rise to the fibration exact sequence

$$1 \to \pi_1(X) \to \pi_1(\mathcal{C}_g) \to \pi_1(\mathcal{M}_g) \to 1$$

and the action of $\pi_1(\mathcal{C}_g)$ on $\pi_1(X)$ gives ρ. Now, X, viewed as a point on $\mathcal{M}_g(K)$, gives a map $\sigma_{\mathcal{M}_g/K}(X) : G_K \to \pi_1(\mathcal{M}_g)$. As pointed out in [15], $\rho \circ \sigma_{\mathcal{M}_g/K}(X)$ induces a map $G_K \to Out(\pi_1(\bar{X}))$ which is none other than the map obtained from the exact sequence (1) by letting $\pi_1(X)$ act on $\pi_1(\bar{X})$ by conjugation. Combining this with Mochizuki's theorem 2.1 gives:

Theorem 5.1 *For any field K contained in a finite extension of a p-adic field, the section map $\sigma_{\mathcal{M}_g/K}$ is injective.*

The following result confirms a conjecture of Stoll [35] if we assume that $\sigma_{\mathcal{M}_g/K}$ surjects onto $S_0(K, \mathcal{M}_g)$.

Theorem 5.2 *Assume that $\sigma_{\mathcal{M}_g/K}(\mathcal{M}_g(K)) = S_0(K, \mathcal{M}_g)$ for all $g > 1$ and all number fields K. Then $\sigma_{X/K}(X(K)) = S(K, X)$ for all smooth projective curves of genus at least two and all number fields K.*

Proof. For any algebraic curve X/K there is a non-constant map $X \to \mathcal{M}_g$ with image Y, say, for some g, defined over an extension L of K, given by the Kodaira-Parshin construction. This gives a map, over L $\gamma : \pi_1(X) \to \pi_1(\mathcal{M}_g)$. Let $s \in S(K, X)$, then $\gamma(s) \in S_0(L, \mathcal{M}_g)$ and the assumption of the theorem yields that $\gamma(s) = \sigma_{\mathcal{M}_g/L}(P), P \in \mathcal{M}_g(L)$. We can combine this with the injectivity of $\sigma_{\mathcal{M}_g/K_v}$ (Mochizuki's theorem) to deduce that in fact $P \in Y(L_v) \cap \mathcal{M}_g(L) = Y(L)$. We can consider the pullback to X of the Galois orbit of P, which gives us a zero dimensional scheme in X having points locally everywhere and, moreover, being unobstructed by every abelian cover coming from an abelian cover of X. By the work of Stoll [35] we conclude that X has a rational point corresponding to s. □

Acknowledgements. The second author would like to thank D. Harari, E. Ozman, T. Schlank, and J. Starr for comments and information. He would also like to thank the Simons Foundation (grant #234591) and the Centre Bernoulli at EPFL for financial support.

The third author (Y.Z.) is grateful to Frans Oort for helpful discussions 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 he was visiting Department of Mathematics of the Weizmann Institute of Science (Rehovot, Israel), whose hospitality is gratefully acknowledged.

We would also like to thank W. Sawin for comments.

References

[1] H. Bass, M. Lazard, J.-P. Serre, *Sous-groupes d'indice fini dans SL(n,Z)* Bull. Amer. Math. Soc. 70 (1964) 385–392.

[2] P. Deligne, *Formes modulaires et représentations l-adiques.* Séminaire Bourbaki. Vol. 1968/69: Exposés 347363, Exp. No. 355, 139–172, Lecture Notes in Mathematics, vol. 175, Springer-Verlag, Berlin, 1971.

[3] P. Deligne, J. S. Milne, A. Ogus, and K. Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982.

[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] J.-M. Fontaine, B. Mazur, *Geometric Galois representations*, in Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, (1995), pp 41–78.

[7] A. Grothendieck, *Modéles de Néron et monodromie*. In: Groupes de monodromie en géométrie algébrique (SGA7 I), Exp. IX, pp. 313–523, Lecture Notes in Mathematics **288** (1972), Berlin.

[8] A. Grothendieck, *Letter to Faltings* 1983. Reprinted with English translation in pp 285–293 *Geometric Galois actions* London Math. Soc. Lecture Note Ser., 242, 1, 49–58, Cambridge Univ. Press, Cambridge, 1997.

[9] A. Grothendieck, *Esquisse d'un Programme* 1984. Reprinted with English translation in pp 243–283 *Geometric Galois actions* London Math.

Soc. Lecture Note Ser., 242, 1, 5–48, Cambridge Univ. Press, Cambridge, 1997.

[10] R. Hain, *Rational points of universal curves.* J. Amer. Math. Soc. 24 (2011), 709–769.

[11] D. Harari, J. Stix, *Descent obstruction and fundamental exact sequence* in: J. Stix (editor): The Arithmetic of Fundamental Groups - PIA 2010 Contributions in Mathematical and Computational Sciences, Vol. 2, Springer-Verlag Berlin Heidelberg, 2012.

[12] D. Helm, J. F. Voloch, *Finite descent obstruction on curves and modularity*, Bull. LMS, 43 (2011) 805-810.

[13] E. Howe, *Kernels of polarizations of abelian varieties over finite fields.* J. Algebraic Geom. 5 (1996), no. 3, 583–608.

[14] I. Ihara, H. Nakamura, *Some illustrative examples for anabelian geometry in high dimensions.* in *Geometric Galois actions* London Math. Soc. Lecture Note Ser., 242, 1, 127–138, Cambridge Univ. Press, Cambridge, 1997.

[15] M. Matsumoto, A. Tamagawa, *Mapping-class-group action versus Galois action on profinite fundamental groups.* Amer. J. Math. 122 (2000), 1017–1026.

[16] B. Mazur, *Open problems: Descending cohomology, geometrically.* Notices of the International Congress of Chinese Mathematicians, Volume 2, Number 1 (July 2014), 37–40; available at http://www.math.harvard.edu/ mazur/ .

[17] J. L. Mennicke, *Finite factor groups of the unimodular group* Ann. of Math. 81 (1965) 31–37.

[18] J. S. Milne, *Algebraic geometry* (v5.22), 2012, Available at www.jmilne.org/math/, p. 260.

[19] S. Mochizuki, *The profinite Grothendieck conjecture for closed hyperbolic curves over number fields.* J. Math. Sci. Univ. Tokyo 3 (1996), no. 3, 571–627.

[20] Y. Morita, *On potential good reduction of abelian varieties* J. Fac. Sci. Univ. Tokyo Sect. I A Math. 22 (1975) 437–447.

[21] D. Mumford, *On the Equations Defining Abelian Varieties* I, II. Invent. Math. **1** (1966), 287–384; **3** (1967), 75–135.

[22] R. Noot, *Abelian varieties - Galois representations and properties of ordinary reduction* . Compositio Math. **97** (1995), 161–171.

[23] F. Oort, *Endomorphism algebras of abelian varieties.* In: Algebraic Geometry and Commutative Algebra, Vol. II (in Honor of M. Nagata). Kinokuniya Company Ltd., Tokyo, pp. 469–502 (1988).

[24] F. Oort, *Lifting algebraic curves, and their endomorphisms to characteristic zero.* In: Proc. Symp. Pure Math. **46** (1987), 165–195.

[25] F. Oort, CM-liftings of abelian varieties. J. Algebraic Geometry **1** (1992), 131–146.

[26] F. Oort, Yu.G. Zarhin, *Endomorphism Algebras of Complex Tori.* Math. Ann. **303** (1995), 11–29.

[27] A. Pal, *The real section conjecture and Smith's fixed point theorem for pro-spaces* J. Lond. Math. Soc. 83 (2011) 353–367.

[28] S. T. Patrikis, *Variations on a theorem of Tate*, ArXiv e-prints 1207.6724v4 (2012).

[29] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties.* J. Pure and Applied Algebra **77** (1992) 253–262.

[30] A. Silverberg, Yu. G. Zarhin, *Semistable reduction and torsion subgroups of abelian varieties*, Ann. Inst. Fourier **45** (1995) 403–420.

[31] A. Silverberg, Yu. G. Zarhin, *Isogenies of abelian varieties over finite fields.* arXiv:1409.0592 [math.NT]. Designs, Codes and Cryptography, DOI 10.1007/s10623-015-0078-2.

[32] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions.* Ann. Math. **78** (1963), 149–192.

[33] A. Skorobogatov, *Torsors and rational points*, Cambridge University Press, Cambridge 2001.

[34] J. Stix, *Birational Galois sections over* $\mathbf{Q}$*, families of elliptic curves and modularity*, preprint.

[35] M. Stoll, *Finite descent and rational points on curves*, Algebra and Number Theory **2** (2008), no 5, 595–611.

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

[37] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki, no. **352** (1968), pp. 95–110. Lecture Notes in Mathematics **179**, Springer-Verlag, Berlin, 1971.

[38] J. F. Voloch, *Finite descent obstruction for curves over function fields*, Bol. Soc. Brasil. Math. 43 (2012) 1-6.

[39] Yu. G. Zarhin, *Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension*. J. Pure and Applied Algebra **219** (2015), 2076–2098.

[40] 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.

[41] V. Zoonekynd, *The fundamental group of an algebraic stack*, arxiv.org math.AG/0111071

Department of Mathematics, University of Utah
Salt Lake City, UT 84103, USA
e-mail: patrikis@math.utah.edu
Department of Mathematics, University of Texas
Austin, TX 78712, USA
e-mail: voloch@math.utexas.edu
Department of Mathematics, Pennsylvania State University,
University Park, PA 16802, USA
e-mail: zarhin@math.psu.edu