

# Anabelian geometry and descent obstructions on moduli spaces

Stefan Patrikis, José Felipe Voloch, Yuri G. Zarhin

May 27, 2016

**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. This is done by relating the problem to a local-global principle for Galois representations. For the latter, we show how the sufficiency of the finite descent obstruction implies the same for all hyperbolic curves.

## 1 Introduction

Anabelian geometry is a program proposed by Grothendieck ([17, 18]) 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 ([31]). Grothendieck suggested that moduli spaces of curves and abelian varieties (the latter perhaps less emphatically) should be anabelian. Already Ihara and Nakamura [24] have shown that moduli spaces of abelian varieties should not be anabelian

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

as one cannot recover their automorphism group from the fundamental group and we will further show that other anabelian properties fail in this case.

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, for hyperbolic curves (Stoll, [49] in the projective case and Harari and Voloch [21] in the affine case) to equal that closure. It's not unreasonable to conjecture the same for all anabelian varieties. The relationship between the finite descent obstruction and the section conjecture in anabelian geometry has been discussed by Harari and Stix [20], Stix [48], Section 11 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 section conjecture and finite descent obstruction hold for a general class of adelic points, assuming many established conjectures in arithmetic geometry (specifically, we assume the Hodge, Tate, Fontaine-Mazur and Grothendieck-Serre conjectures, in the precise forms stated in section 3). This is done by converting the question into one about Galois representations.

The section conjecture predicts that sections of the fundamental exact sequence (Section 3, eq. 1) of an anabelian variety over a number field correspond to rational points. In this paper, we look at the sections of the fundamental exact sequence of the moduli spaces of principally polarized abelian varieties that, locally at every place of the ground field come from a point rational over the completion, which moreover is integral for all but finitely many places. This set is denoted  $S_0(K, \mathcal{A}_g)$  and defined precisely at the end of Section 2. We explain, in section 3, how sections of the fundamental exact sequence of the moduli spaces of principally polarized abelian varieties correspond to Galois representations and prove, Theorem 3.7, the following result.

**Theorem 1.1** *Assume the Hodge, Tate, Fontaine-Mazur, and Grothendieck-Serre conjectures. Let  $K$  be a number field. Suppose  $s \in S_0(K, \mathcal{A}_g)$  gives rise to a system of  $\ell$ -adic Galois representations one of which is absolutely irreducible. Then there exists, up to isomorphism, a unique principally polarized abelian variety which, viewed as point of  $\mathcal{A}_g(K)$ , induces (up to conjugation)*

the section  $s$ .

We also give examples (see Theorems 4.4 and 4.5) showing that weaker versions of the above result do not hold. Specifically, the local conditions cannot be weakened to hold almost everywhere, for instance.

For the moduli of curves, we show how combining some of our results and assuming 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  $\pi_1(\cdot)$  the algebraic fundamental group functor on (geometrically pointed) schemes and we omit base-points from the notation. We have the fundamental exact sequence

$$1 \rightarrow \pi_1(\bar{X}) \rightarrow \pi_1(X) \rightarrow G_K \rightarrow 1. \quad (1)$$

The map  $p_X : \pi_1(X) \rightarrow G_K$  from the above sequence is obtained by functoriality from the structural morphism  $X \rightarrow \text{Spec}K$ . 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  $\mathbb{Q}$ . 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 [31] 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 a subfield of a finitely generated extension of  $\mathbb{Q}_p$ . 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  $G_K \rightarrow \pi_1(X)$  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  $G_K \rightarrow \pi_1(X)$  modulo conjugation by  $\pi_1(\bar{X})$  and we denote by  $\sigma_{X/K} : X(K) \rightarrow H(K, X)$  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 [48], Section 18. 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  $s_0 : G_K \rightarrow \pi_1(X)$  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  $s : G_K \rightarrow \pi_1(X)$  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  $H^1(G_K, \pi_1(\bar{X})) \rightarrow H(K, X)$ . 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, in which case there is no natural choice of action of  $G_K$  on  $\pi_1(\bar{X})$  in order to define  $H^1(G_K, \pi_1(\bar{X}))$  which would be non-empty in any case, if defined.

Let  $X/K$  be 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  $\bar{K} \subset \bar{K}_v$  induces a map  $\alpha_v : G_{K_v} \rightarrow G_K$  and a map  $\beta_v : \pi_1(X_v) \rightarrow \pi_1(X)$ , 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  $s \circ \alpha_v = \beta_v \circ \sigma_{X_v/K_v}(P_v)$ . Note that if  $v$  is complex, then the condition at  $v$  is vacuous and that if  $v$  is real,  $\sigma_{X_v/K_v}$  factors through  $X(K_v)_\bullet$ , the set of connected components of  $X(K_v)$ , equipped with the quotient topology (see [32, 40]). In the non-archimedean case,  $X(K_v)$  is totally disconnected so  $X(K_v) = X(K_v)_\bullet$  and we have the following diagram:

$$\begin{array}{ccc}
X(K) & \longrightarrow & \prod X(K_v)_\bullet & \supset X^f \\
\sigma_{X/K} \downarrow & & \downarrow \prod \sigma_{X_v/K_v} & \\
S(K, X) \subset H(K, X) & \xrightarrow{\alpha} & \prod H(K_v, X_v) & 
\end{array}$$

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  $s \circ \alpha_v = \beta_v \circ \sigma_{X_v/K_v}(P_v)$  for all places  $v$ . Also, it is clear that the image of  $X(K)$  is contained in  $X^f$ . At least when  $X$  is proper,  $X^f$  is closed (this follows from the compactness of  $H(K, X)$ , [48], Cor. 45). In that case, one may consider whether 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  $\sigma_{X/K} : X(K) \rightarrow H(K, X)$ . As a specific instance of this relation, we record the following easy fact:

**Proposition 2.2** *We have that  $X^f = \emptyset$  if and only if  $S(K, X) = \emptyset$ .*

**Proof.** If  $X^f \neq \emptyset$  and  $(P_v) \in X^f$ , then there exists  $s \in S(K, X)$  with  $s \circ \alpha_v = \beta_v \circ \sigma_{X_v/K_v}(P_v)$  for all places  $v$ , so  $S(K, X) \neq \emptyset$ .

If  $s \in S(K, X)$ , there exists  $(P_v)$  with  $s \circ \alpha_v = \beta_v \circ \sigma_{X_v/K_v}(P_v)$  for all places  $v$ . So  $(P_v) \in X^f$ .  $\square$

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. We note that  $S_0(K, X)$  is independent of the choice of the model  $\mathcal{X}$ .

We recall here some basic notions about the Tate module of abelian varieties which will be used in the next two sections, in order to set notation. If  $A$  is an abelian variety over the field  $K$  then we write  $\text{End}(A)$  for its ring of all  $K$ -endomorphisms and  $\text{End}^0(A)$  for the corresponding (finite-dimensional semisimple)  $\mathbb{Q}$ -algebra  $\text{End}(A) \otimes \mathbb{Q}$ . If  $n \geq 3$  is an integer that is not divisible by  $\text{char}(K)$  and all points of order  $n$  on  $A$  are defined over  $K$  then, by a theorem of Silverberg [44], all  $\bar{K}$ -endomorphisms of  $A$  are defined over  $K$ , i.e., lie in  $\text{End}(A)$ .

If  $\ell$  is a prime different from  $\text{char}(K)$  then we write  $T_\ell(A)$  for the  $\mathbb{Z}_\ell$ -Tate module of  $A$  which is a free  $\mathbb{Z}_\ell$ -module of rank  $2\dim(A)$  provided with the

natural continuous homomorphism

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

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

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

The image of  $\text{End}(A) \otimes \mathbb{Z}_\ell$  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  $\ell$ -adic representation

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

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

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

which we still denote by  $e_\ell$ . Further we will identify  $\text{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$  with its image in  $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ .

This provides  $V_\ell(A)$  with the natural structure of  $G_K$ -module; in addition,  $\text{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$  is a  $\mathbb{Q}_\ell$ -(sub)algebra of endomorphisms of the Galois module  $V_\ell(A)$ . In other words,

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

### 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 [57]. For a discussion of the case of  $\mathcal{A}_g$ , see

[19]. We can also get what we need from [24] (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  $\mathbb{Q}$ , 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  $\mathbb{Q}$  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  $Sp_{2g}(\mathbb{Z})$  and the algebraic fundamental group is its profinite completion. When  $g > 1$  (which we henceforth assume)  $Sp_{2g}(\mathbb{Z})$  has the congruence subgroup property ([2],[30]) and therefore its profinite completion is  $Sp_{2g}(\hat{\mathbb{Z}})$ .

The group  $\pi_1(\mathcal{A}_g)$  is essentially described by the exact sequences (3.2) and (3.3) of [24] and it follows that the set  $H(K, \mathcal{A}_g)$  consists of  $\hat{\mathbb{Z}}$  representations of  $G_K$  of rank  $2g$  preserving the symplectic form up to a multiplier given by 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 [24].

In the following we denote the cyclotomic character by  $\chi : G_K \rightarrow \hat{\mathbb{Z}}^*$ .

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \pi_1(\bar{\mathcal{A}}_g) & \longrightarrow & \pi_1(\mathcal{A}_g) & \longrightarrow & G_K \longrightarrow 1 \\
 & & \downarrow \cong & & \downarrow & & \chi \downarrow \\
 1 & \longrightarrow & Sp_{2g}(\hat{\mathbb{Z}}) & \longrightarrow & GSp_{2g}(\hat{\mathbb{Z}}) & \longrightarrow & \hat{\mathbb{Z}}^* \longrightarrow 1.
 \end{array}$$

The coverings of  $\bar{\mathcal{A}}_g$  corresponding to the congruence subgroups of  $Sp_{2g}(\hat{\mathbb{Z}})$  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 ([10]). The finiteness of isogeny classes of polarized abelian varieties over  $K$  [10] (see also [55]) implies that for any given  $K$  and  $g$  every fiber of  $\sigma_{\mathcal{A}_g/K}$  is finite. On the other hand,  $\sigma_{\mathcal{A}_g/K}$  is not necessarily injective to  $S_0(K, \mathcal{A}_g)$ , see Sect. 5. For example, for each  $g$  there exists  $K$  with non-injective  $\sigma_{\mathcal{A}_g/K}$ . 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 theorem 3.7 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  $\ell$ -adic cohomology of smooth projective varieties, and the Tate and Hodge con-

tures. 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 [29].

Here is the setting. Let  $K$  be a number field, with  $G_K = \text{Gal}(\overline{K}/K)$ . Fix a finite set of rational primes  $S$ , and consider a collection of continuous  $\ell$ -adic representations

$$\{\rho_\ell: G_K \rightarrow \text{GL}_N(\mathbb{Q}_\ell)\}_{\ell \notin S}.$$

We will say that the collection  $\{\rho_\ell\}_{\ell \notin S}$  is *weakly compatible* if there exists a finite set of places  $\Sigma$  of  $K$  such that

- I. for all  $\ell \notin S$ ,  $\rho_\ell$  is unramified outside the union of  $\Sigma$  and the places  $\Sigma_\ell$  of  $K$  dividing  $\ell$ ; and
- II. for all  $v \notin \Sigma \cup \Sigma_\ell$ , denoting by  $fr_v$  a (geometric) Frobenius element at  $v$ , the characteristic polynomial of  $\rho_\ell(fr_v)$  has rational coefficients and is independent of  $\ell \notin S$ .<sup>1</sup>

We will assume  $\{\rho_\ell\}_{\ell \notin S}$  is weakly compatible in this sense and moreover satisfies the following three conditions:

1. For some prime  $\ell_0 \notin S$ ,  $\rho_{\ell_0}$  is de Rham at all places of  $K$  above  $\ell_0$ .
2. For some prime  $\ell_1 \notin S$ ,  $\rho_{\ell_1}$  is absolutely irreducible.
3. 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  $\rho_{\ell_2}|_{G_{K_v}} \cong V_{\ell_2}(A_v)$ ).

We note that the  $\ell_i$  need not be distinct, and in fact in the anabelian application (Theorem 3.7) they can all be taken to be equal; we have phrased things this way to have hypotheses that most clearly match the form of the argument.

Our aim is to prove the following:

<sup>1</sup>These systems were introduced by Serre [43], who called them *strictly compatible*.



**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  $\ell$ .*

We begin by making 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 3.5). 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  $E = \mathbb{Q}$ ).

**Lemma 3.2** *Assume the Tate conjecture for all finitely-generated extensions  $k$  of  $\mathbb{Q}$ . Then:*

1. *The Lefschetz Standard Conjecture holds for all fields of characteristic zero.*
2. *All of the Standard Conjectures (namely, the Künneth and Hodge Standard Conjectures, and the agreement of numerical and homological equivalence) hold for all fields of characteristic zero.*
3. *For any field  $k$  that can be embedded in  $\mathbb{C}$ , the category  $\mathcal{M}_k$  is a semi-simple neutral Tannakian category over  $\mathbb{Q}$ .*
4. *For any finitely-generated  $k/\mathbb{Q}$ , the étale  $\ell$ -adic realization functor*

$$\mathcal{M}_{k,\mathbb{Q}_\ell} \rightarrow \text{Rep}_{\mathbb{Q}_\ell}(G_k),$$

*valued in the category of continuous  $\ell$ -adic representations of  $G_k$ , is fully faithful.*

**Proof.** For the first assertion, see, eg, [1, 7.3.1.3]); for the second, see [1, 5.4.2.2]. The third part is the basic motivating consequence of the Standard Conjectures (a fiber functor over  $\mathbb{Q}$  is given by Betti cohomology, after fixing an embedding  $k \hookrightarrow \mathbb{C}$ ): see [25, Corollary 2], especially for the semi-simplicity claim. Finally, for the last part, fullness is the Tate conjecture; and faithfulness follows from the agreement of numerical and homological equivalence and [50, Lemma 2.5] (note that faithfulness on  $\mathcal{M}_k$  is simply by definition of homological equivalence: it is only with  $\mathbb{Q}_\ell$ -coefficients that some argument is needed).  $\square$

For the rest of this section, we assume the Tate conjecture for all finitely-generated  $k$  of characteristic zero. Thus, we have a motivic Galois formalism:  $\mathcal{M}_{k,E}$  is equivalent to  $\text{Rep}(\mathcal{G}_{k,E})$  for some pro-reductive group  $\mathcal{G}_{k,E}$  over  $E$ ,

the equivalence depending on the choice of an  $E$ -linear fiber functor. We will implicitly fix an embedding  $k \hookrightarrow \mathbb{C}$  and use the associated Betti realization as our fiber functor. Before proceeding, we introduce two pieces of notation. For an extensions of fields  $k'/k$ , we denote the base-change of motives by

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

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

$$H_\iota: \mathcal{M}_{k,E} \rightarrow \text{Rep}_{\overline{\mathbb{Q}}_\ell}(G_k)$$

associated to  $\iota$ .

Now we turn to the case of number fields, i.e.  $k = K$ . The Tate conjecture alone does not suffice to link Galois representations with motives: it yields full faithfulness of the  $\ell$ -adic realization (as in Lemma 3.2), but does not characterize the essential image. This is done via the combination of the Fontaine-Mazur and Grothendieck-Serre semi-simplicity conjectures, which we now recall. Recall that a semi-simple representation  $r_\ell: G_K \rightarrow \text{GL}_N(\mathbb{Q}_\ell)$  is said to be *geometric* (in the sense of Fontaine-Mazur: [13]) if it is unramified outside a finite set of places of  $K$ , and if for all  $v|\ell$  of  $K$ , the restriction  $r_\ell|_{G_{K_v}}$  is de Rham (equivalently, potentially semi-stable, as in the original formulation). See [14, 4] for the definition and basic properties of deRham representations. Fontaine and Mazur have conjectured that any irreducible geometric  $r_\ell$  is isomorphic to a sub-quotient of  $H^i(X_{\overline{K}}, \mathbb{Q}_\ell)(j)$  for some smooth projective variety  $X/K$  and some integers  $i$  and  $j$ ; that the converse assertion holds is a consequence of the base-change theorems of étale cohomology ([7]) and Faltings'  $p$ -adic de Rham comparison isomorphism ([12]). Grothendieck and Serre have moreover conjectured that for any smooth projective  $X/K$ , and any integer  $i$ ,  $H^i(X_{\overline{K}}, \mathbb{Q}_\ell)$  is a semi-simple representation of  $G_K$ . Putting all of these conjectures together, we can characterize the essential image of  $H_\iota$ :

**Lemma 3.3** *Assume the Tate, Fontaine-Mazur, and Grothendieck-Serre conjectures. Let  $r_\ell: G_K \rightarrow \text{GL}_N(\mathbb{Q}_\ell)$  be an irreducible geometric Galois representation. Then there exists an object  $M$  of  $\mathcal{M}_{K,\overline{\mathbb{Q}}}$  such that*

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

*More generally, the essential image of  $H_\iota$  consists of all semi-simple geometric representations (with coefficients in  $\overline{\mathbb{Q}}_\ell$ ) of  $G_K$ .*

**Proof.** The Fontaine-Mazur conjecture asserts that for some smooth projective variety  $X/k$ ,  $r_\ell$  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. Under the Künneth Standard Conjecture (a consequence of our hypotheses by Lemma 3.2),  $\mathcal{M}_K$  has a canonical (weight) grading, and we denote by  $H^i(X)$  the weight  $i$  component of the motive of  $X$ . The Tate conjecture then implies (Lemma 3.2) that

$$H_\iota: \text{End}_{\mathcal{M}_K}(H^i(X)(j)) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \xrightarrow{\sim} \text{End}_{\overline{\mathbb{Q}}_\ell[G_K]}(H^i(X_{\overline{K}}, \overline{\mathbb{Q}}_\ell)(j)) \quad (2)$$

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  $\text{End}_{\mathcal{M}_K}(H^i(X)(j)) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$  whose image has  $\ell$ -adic realization  $r_\ell$ . But  $\text{End}_{\mathcal{M}_K}(H^i(X)(j))$  is a semi-simple algebra over  $\mathbb{Q}$  (Lemma 3.2), which certainly splits over  $\overline{\mathbb{Q}}$ , so the decomposition of  $H^i(X)(j)$  into simple objects of  $\mathcal{M}_{K, \overline{\mathbb{Q}}}$  is already realized in  $\mathcal{M}_{K, \overline{\mathbb{Q}}}$ .<sup>2</sup>

For the final claim about the essential image (which we do not use in what follows), it suffices to show an irreducible  $r_\iota: G_K \rightarrow \text{GL}_N(\overline{\mathbb{Q}}_\ell)$  lies in the essential image. Such an  $r_\iota$  is defined over a finite extension of  $\mathbb{Q}_\ell$  and can thus be regarded as a higher-dimensional geometric representation  $r_\ell$  with  $\overline{\mathbb{Q}}_\ell$ -coefficients, necessarily semi-simple. By the first part of the lemma,  $r_\ell \otimes_{\overline{\mathbb{Q}}_\ell} \overline{\mathbb{Q}}_\ell$  is isomorphic to  $H_\iota(M)$  for some  $M \in \mathcal{M}_{K, \overline{\mathbb{Q}}}$ , and by the Tate conjecture there is a projector in  $\text{End}(M) \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}_\ell$  inducing the canonical (adjunction) projector  $r_\ell \otimes_{\overline{\mathbb{Q}}_\ell} \overline{\mathbb{Q}}_\ell \twoheadrightarrow r_\iota$ . Arguing as before (a simple object of  $\mathcal{M}_{K, \overline{\mathbb{Q}}}$  arises by scalar-extension from one of  $\mathcal{M}_{K, \overline{\mathbb{Q}}}$ ), we see that  $r_\iota$  is in the essential image of  $H_\iota$ .  $\square$

Returning to our particular setting, fix any  $\ell_0 \notin S$  as in our first condition on the compatible system  $\{\rho_\ell\}_{\ell \notin S}$ , and also fix an embedding  $\iota_0: \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{\ell_0}$ , so that Lemma 3.3 provides us with a number field (the linear combinations of correspondences needed to cut out a given object of  $\mathcal{M}_{K, \overline{\mathbb{Q}}}$  have coefficients in a finite extension of  $\mathbb{Q}$ )  $E \subset \overline{\mathbb{Q}}$  (which we may assume Galois over  $\mathbb{Q}$ ) and a motivic Galois representation  $\rho: \mathcal{G}_{K, E} \rightarrow \text{GL}_{N, E}$  such that  $H_{\iota_0}(\rho) \cong \rho_{\ell_0} \otimes \overline{\mathbb{Q}}_{\ell_0}$ . Let us denote by  $\lambda_0$  the place of  $E$  induced by  $E \subset \overline{\mathbb{Q}} \xrightarrow{\iota_0} \overline{\mathbb{Q}}_{\ell_0}$ . Then for all finite places  $\lambda$  of  $E$  (say  $\lambda|\ell$ ), and for almost all places  $v$  of  $K$ , compatibility gives us the following equality of rational numbers (note that  $\rho_\lambda$  denotes the

<sup>2</sup>In fact, it is realized over the maximal CM subfield of  $\overline{\mathbb{Q}}$ : see e.g. [41, Lemma 4.1.22].

$\lambda$ -adic realization of the motivic Galois representation  $\rho$ , while  $\rho_\ell$  denotes the original  $\ell$ -adic representation in our compatible system):

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

Here we use the fact that the collection of  $\ell$ -adic realizations of a motive form a (weakly) compatible system; this follows from the Lefschetz trace formula, in its ‘formal’ version for correspondences (see for instance [1, 3.3.3, 7.1.4]). We deduce as usual (Brauer-Nesbitt and Chebotarev) that  $\rho_\ell^{\mathrm{ss}} \otimes_{\mathbb{Q}_\ell} E_\lambda \cong \rho_\lambda$ ; this holds for all  $\lambda$  for which  $\rho_\ell$  makes sense, i.e. for all  $\lambda$  above  $\ell \notin S$ .

Recall that for some  $\ell_1 \notin S$ , we have assumed  $\rho_{\ell_1}$  is absolutely irreducible; hence for any place  $\lambda_1$  of  $E$  above  $\ell_1$ , the previous paragraph shows that  $\rho_{\lambda_1} \cong \rho_{\ell_1} \otimes E_{\lambda_1}$  is absolutely irreducible. *A fortiori*,  $\rho$  is absolutely irreducible, and then by the Tate conjecture all  $\rho_\lambda$  are absolutely irreducible, so we can upgrade the conclusion of the previous paragraph to an isomorphism of absolutely irreducible representations  $\rho_\ell \otimes_{\mathbb{Q}_\ell} E_\lambda \cong \rho_\lambda$ , for all  $\ell \notin S$ .

The next question is whether having each (or almost all)  $\rho_\lambda$  in fact definable over  $\mathbb{Q}_\ell$  forces  $\rho$  to be definable over  $\mathbb{Q}$ . Since the  $\rho_\lambda$  descend to  $\mathbb{Q}_\ell$ , the Tate conjecture implies that for all  $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ ,  ${}^\sigma \rho \cong \rho$ ; and since  $\mathrm{End}(\rho)$  is  $E$ , the obstruction to descending  $\rho$  to a  $\mathbb{Q}$ -rational representation of  $\mathcal{G}_K$  is an element  $\mathrm{obs}_\rho$  of  $H^1(\mathrm{Gal}(E/\mathbb{Q}), \mathrm{PGL}_N(E))$ .

**Lemma 3.4** *With the notation above,  $\mathrm{obs}_\rho$  in fact belongs to*

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

*In particular, if  $S$  is empty, then  $\rho$  can be defined over  $\mathbb{Q}$ .*

**Proof.** We know that each of the  $\lambda$ -adic realizations  $\rho_\lambda$  (for  $\lambda | \ell \notin S$ ) can be defined over  $\mathbb{Q}_\ell$ ; to prove the lemma, we need to verify that the canonical localizations of  $\mathrm{obs}_\rho$  (which arise by extending scalars on the motivic Galois representation) are in fact given by the corresponding obstruction classes for the  $\lambda$ -adic realizations. Thus, we have to recall how these realizations are constructed from  $\rho$  itself. The surjection  $\mathcal{G}_K \twoheadrightarrow G_K$  admits a continuous section on  $\mathbb{Q}_\ell$ -points,  $s_\ell: G_K \rightarrow \mathcal{G}_K(\mathbb{Q}_\ell)$ ; composition with  $\rho \otimes_E E_\lambda$  yields  $\rho_\lambda$ :

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

$\rho_\lambda$

By construction of the respective obstruction classes, the canonical map from endomorphisms of  $\rho \otimes_E E_\lambda$  to those of  $\rho_\lambda$  realizes the obstruction class for  $\rho_\lambda$  as the localization of  $\text{obs}_\rho$  at  $\text{Gal}(E_\lambda/\mathbb{Q}_\ell)$ . But we have seen that  $\rho_\lambda$  can be defined over  $\mathbb{Q}_\ell$ , so we conclude that  $\text{obs}_\rho$  has trivial restriction to each  $\text{Gal}(E_\lambda/\mathbb{Q}_\ell)$ , as desired.

For the final claim, note that by Hilbert 90 we can regard  $\text{obs}_\rho$  as an element of

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

If  $S$  is empty, then the structure of the Brauer group of  $\mathbb{Q}$  (which has only one infinite place!) then forces  $\text{obs}_\rho$  to be trivial.  $\square$

**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

$$\rho: \mathcal{G}_K \rightarrow \text{GL}_{N, \mathbb{Q}}.$$

Let  $M$  be the rank  $N$  object of  $\mathcal{M}_K$  corresponding to  $\rho$  via the Tannakian equivalence. Recall that we are given a prime  $\ell_2$  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 ‘ $\ell_2$ -adic Hodge theory’: denoting Fontaine’s period ring over  $K_v$  by  $B_{\text{dR}, K_v}$ , and the de Rham realization functor by  $H_{\text{dR}}: \mathcal{M}_K \rightarrow \text{Fil}_K$  (the category of filtered  $K$ -vector spaces), we have the comparison (respecting filtration and  $G_{K_v}$ -action)

$$H_{\text{dR}}(M) \otimes_K B_{\text{dR}, K_v} \xrightarrow{\sim} H_{\ell_2}(M) \otimes_{\mathbb{Q}_{\ell_2}} B_{\text{dR}, K_v},$$

hence

$$H_{\text{dR}}(M) \otimes_K K_v \cong D_{\text{dR}, K_v}(H_{\ell_2}(M)).$$

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

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

and  $\text{gr}^i(H_{\text{dR}}(M)) = 0$  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  $K \hookrightarrow \mathbb{C}$ ; we regard  $K$  as a subfield of  $\mathbb{C}$  via this embedding. Then we also have the analytic Betti-de Rham comparison isomorphism

$$H_{\text{dR}}(M) \otimes_K \mathbb{C} \xrightarrow{\sim} H_{\text{B}}(M|_{\mathbb{C}}) \otimes_{\mathbb{Q}} \mathbb{C}. \quad (4)$$

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

**Lemma 3.5** *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  $H_{\text{B}}(M|_{\mathbb{C}})$  is a polarizable rational Hodge structure of type  $\{(0, -1), (-1, 0)\}$ . It follows from Riemann's theorem that there is an abelian variety  $A/\mathbb{C}$  and an isomorphism of  $\mathbb{Q}$ -Hodge structures  $H_1(A(\mathbb{C}), \mathbb{Q}) \cong H_{\text{B}}(M|_{\mathbb{C}})$ . The Hodge conjecture implies that this isomorphism comes from an isomorphism  $H_1(A) \xrightarrow{\sim} M|_{\mathbb{C}}$  in  $\mathcal{M}_{\mathbb{C}}$ .

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

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

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

It follows from Lemma 3.6 that  $A$  has a model  $A_{\overline{\mathbb{Q}}}$  over  $\overline{\mathbb{Q}}$ . The morphism

$$\text{Hom}_{\mathcal{M}_{\overline{\mathbb{Q}}}}(H_1(A_{\overline{\mathbb{Q}}}), M|_{\overline{\mathbb{Q}}}) \rightarrow \text{Hom}_{\mathcal{M}_{\mathbb{C}}}(H_1(A), M|_{\mathbb{C}})$$

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  $\text{Res}_{L/K}(A_L)$ ; under the *fully faithful* embedding

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

we can think of  $H_1(\text{Res}_{L/K}(A_L))$  as  $\text{Ind}_L^K(H_1(A_L))$ , where the induction is taken in the sense of motivic Galois representations (note that the quotient  $\mathcal{G}_K/\mathcal{G}_L$  is canonically  $\text{Gal}(L/K)$ , so this is just the usual induction from a finite-index subgroup). Frobenius reciprocity then implies the existence of a non-zero map  $M \rightarrow \text{Ind}_L^K(H_1(A_L))$  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  $\text{AV}_K^0$  as well. That is, there is an endomorphism of  $\text{Res}_{L/K}(A_L)$  whose image is an abelian variety  $A$  over  $K$  with  $H_1(A) \cong M$ .  $\square$

**Proof of Lemma 3.6.** We may assume that  $g \geq 1$ . 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  $\mathcal{Y}$  consists of a countable set of (complex) abelian varieties (up to an isomorphism), we conclude that the set  $\text{Aut}(\mathbb{C}/\mathcal{K})(\mathcal{Y})$  of isomorphism classes of complex abelian varieties of the form  $\{\sigma\mathcal{Y} \mid \sigma \in \text{Aut}(\mathbb{C}/\mathcal{K})\}$  is either finite or countable.

Our plan is as follows. Let us consider a *fine* moduli space  $\mathcal{A}_{g,?}$  over  $\bar{\mathbb{Q}}$  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  $\mathcal{Y}$  (there should be only finitely many choices) and let  $P \in \mathcal{A}_{g,?}(\mathbb{C})$  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  $\text{Aut}(\mathbb{C}/\mathcal{K})(P)$  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  $\text{Aut}(\mathbb{C}/\mathcal{K})$ -orbit of this coordinate coincides with uncountable  $\mathbb{C} \setminus \mathcal{K}$  and therefore the  $\text{Aut}(\mathbb{C}/\mathcal{K})$ -orbit  $\text{Aut}(\mathbb{C}/\mathcal{K})(P)$  of  $P$  is uncountable in  $\mathcal{A}_{g,?}(\mathbb{C})$ . However, for each  $\sigma \in \text{Aut}(\mathbb{C}/\mathcal{K})$  the point  $\sigma(P)$  corresponds to  $\sigma\mathcal{Y}$  with some additional structures

and there are only finitely many choices for these structures. Since we know that the orbit  $\text{Aut}(\mathbb{C}/\mathcal{K})(\mathcal{Y})$  of  $\mathcal{Y}$ , is, at most, countable, we conclude that the orbit  $\text{Aut}(\mathbb{C}/\mathcal{K})(P)$  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  $\delta$  that was introduced and studied by D. Mumford [34]. In order to choose (define) a suitable  $\delta$ , let us pick a totally symmetric ample invertible sheaf  $\mathcal{L}_0$  on  $\mathcal{Y}$  [34, Sect. 2] and consider its 8th power  $\mathcal{L} := \mathcal{L}_0^8$  in  $\text{Pic}(\mathcal{Y})$ . Then  $\mathcal{L}$  is a very ample invertible sheaf that defines a polarization  $\Lambda(\mathcal{L})$  on  $\mathcal{Y}$  [34, Part I, Sect. 1] that is an isogeny from  $\mathcal{Y}$  to its dual; the kernel  $H(\mathcal{L})$  of  $\Lambda(\mathcal{L})$  is a finite commutative subgroup of  $\mathcal{Y}(\mathbb{C})$  (that contains all points of order 8). The order of  $H(\mathcal{L})$  is the degree of the polarization. The type  $\delta$  is essentially the isomorphism class of the group  $H(\mathcal{L})$  [34, Part I, Sect. 1, p. 294]. The resulting moduli space  $\mathcal{A}_{g,?} := M_\delta$  [34, Part II, Sect. 6] enjoys all the properties that we used in the course of the proof.  $\square$

Here is the anabelian application already mentioned in the introduction:

**Theorem 3.7** *Assume the Hodge, Tate, Fontaine-Mazur, and Grothendieck-Serre conjectures. Suppose  $s \in S_0(K, \mathcal{A}_g)$  gives rise to a system of  $\ell$ -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  $s_\ell$  for the  $\ell$ -adic representation associated to  $s$ ; thus  $s_\ell$  is a representation of  $G_K$  on a free  $\mathbb{Z}_\ell$ -module of rank  $2g$ . The hypotheses of Theorem 3.1 apply to the compatible system associated to  $s$  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  $s_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$  (for all  $\ell$ ). Moreover, the hypotheses also imply that the endomorphism ring of  $A$  is  $\mathbb{Z}$ . 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  $s_\ell$  (as  $\mathbb{Z}_\ell$ -representations), i.e. such that  $\sigma_{\mathcal{A}_g/K}(B) = s$ . For this, we first observe that by [8, Proposition 3.3] (which readily generalizes to abelian varieties of any dimension), it suffices to show that for almost all  $\ell$ , there is an isomorphism  $T_\ell(A) \cong s_\ell$ . Since  $\text{End}(A) = \mathbb{Z}$ , [55, Corollary 5.4.5] implies that  $A[\ell]$  is absolutely simple for almost all  $\ell$ , and hence that for almost all  $\ell$ , 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  $s_\ell$  for almost all  $\ell$ . Thus there exists an abelian variety  $B$  in the isogeny class of  $A$  such that  $\sigma_{\mathcal{A}_g/K}(B) = s$ . In order to prove the uniqueness of such a  $B$  up to an isomorphism, first, notice that  $\text{End}(B) = \mathbb{Z}$ . Second, let  $C$  be an abelian variety over  $K$  such that the  $\mathbb{Z}_\ell[G_K]$ -modules  $T_\ell(B)$  and  $T_\ell(C)$  are isomorphic for all primes  $\ell$ . This implies that the  $\mathbb{Z}_\ell$ -ranks of  $T_\ell(B)$  and  $T_\ell(C)$  coincide and therefore

$$\dim(B) = \dim(C).$$

By a theorem of Faltings [10],

$$\text{Hom}(B, C) = \text{Hom}_{G_K}(T_\ell(B), T_\ell(C)).$$

Since  $\text{Hom}(B, C)$  is dense in  $\text{Hom}(B, C) \otimes \mathbb{Z}_\ell$  in the  $\ell$ -adic topology, and the set of isomorphisms  $T_\ell(B) \cong T_\ell(C)$  is open in  $\text{Hom}(B, C) \otimes \mathbb{Z}_\ell$ , there is a homomorphism  $\phi_\ell \in \text{Hom}(B, C)$  that induces an isomorphism of Tate modules  $T_\ell(B) \cong T_\ell(C)$ . Clearly,  $\ker(\phi_\ell)$  does *not* contain points of order  $\ell$  and therefore is finite. Since  $\dim(B) = \dim(C)$ , we obtain that  $\phi_\ell$  is an isogeny, whose degree is prime to  $\ell$ . In particular,  $B$  and  $C$  are isogenous. On the other hand, since  $\text{End}(B) = \mathbb{Z}$ , the group  $\text{Hom}(B, C)$  is a free  $\mathbb{Z}$ -module of rank 1. Let us choose  $\psi : B \rightarrow C$  that is a generator of  $\text{Hom}(B, C)$ . Clearly,  $\psi$  is an isogeny. Since for *all* primes  $\ell$

$$\phi_\ell \in \text{Hom}(B, C) = \mathbb{Z} \cdot \psi,$$

$\deg(\psi)$  is *not* divisible by  $\ell$  and therefore  $\deg(\psi) = 1$ , i.e.,  $\psi$  is an isomorphism of abelian varieties  $B$  and  $C$ . □

Results in the same vein as this corollary have been obtained for elliptic curves over  $\mathbb{Q}$  in [22] and for elliptic curves over function fields in [53].

## 4 Counterexamples

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.

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  $\ell$  is a prime then we have

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

This implies that if  $\ell \neq p$  then  $D \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$  is either (isomorphic to) the *simple* matrix algebra (of size 2) over a quadratic extension of  $\mathbb{Q}_{\ell}$  or a direct sum of two copies of the *simple* matrix algebra (of size 2) over  $\mathbb{Q}_{\ell}$ . (In both cases,  $D \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$  is isomorphic to the matrix algebra  $\mathbb{M}_2(k \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell})$  of size 2 over  $k \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$ .)

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

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

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

that sends 1 to 1. This gives us the embedding

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

Recall that if  $\ell \neq p$  then  $D \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$  is isomorphic to the matrix algebra of size 2 over  $k \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$ . This implies that there are two isomorphic  $\mathbb{Q}_{\ell}[G_L]$ -submodules  $W_{1,\ell}(Y)$  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  $\mathbb{Q}_{\ell}[G_L]$ -module  $W_{1,\ell}$  then we get an isomorphism of  $\mathbb{Q}_{\ell}[G_L]$ -modules

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

This implies that the centralizer  $\text{End}_{G_L}(V_{\ell}(Y))$  coincides with the matrix algebra  $\mathbb{M}_2(\text{End}_{G_L}(W_{\ell}(Y)))$  of size 2 over the centralizer  $\text{End}_{G_L}(W_{\ell}(Y))$ .

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

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

of its certain nonzero  $\mathbb{Q}_p[G_L]$ -submodules  $W_{1,p}(Y)$  and  $W_{2,p}(Y)$ . (Actually,

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

because  $V_p(Y)$  is a free  $k \otimes_{\mathbb{Q}} \mathbb{Q}_p$ -module of rank  $2\dim(Y)/[k : \mathbb{Q}] = \dim(Y)$  [42, Th. 2.1.1 on p. 768].)

**Remark** Let  $L$  be a finitely generated field of characteristic 0. Suppose that  $D = \text{End}^0(Y)$ . By Faltings' results about the Galois action on Tate modules of abelian varieties [10, 11], the  $G_L$ -module  $V_\ell(Y)$  is semisimple and

$$\text{End}_{G_L}(V_\ell(Y)) = D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

This implies that if  $\ell \neq p$  then (the submodule)  $W_\ell(Y)$  is also semisimple and

$$\mathbb{M}_2(\text{End}_{G_L}(W_\ell(Y))) \cong \mathbb{M}_2(k \otimes_{\mathbb{Q}} \mathbb{Q}_\ell).$$

It follows that

$$\text{End}_{G_L}(W_\ell(Y)) \cong k \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

On the other hand, the  $G_L$ -modules  $W_{1,p}(Y)$  and  $W_{2,p}(Y)$  are non-isomorphic.

According to Shimura ([46], see also the case of Type II( $e_0 = 2$ ) with  $m = 1$  in [36, Table 8.1 on p. 498] and [39, Table on p. 23]) there exists a complex abelian fourfold  $X$ , whose endomorphism algebra  $\text{End}^0(X)$  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 of all  $\bar{K}$ -endomorphisms of  $A$  is also isomorphic to  $D$  (see [35, Cor. 1.5 on p. 165]). Enlarging  $K$ , we may assume that all points of order 12 on  $A$  are defined over  $K$  and therefore, by the theorem of Silverberg, all  $\bar{K}$ -endomorphisms of  $A$  are defined over  $K$ . Now Raynaud's criterion ([16], see also [45]) implies that  $A$  has everywhere semistable reduction. On the other hand,

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

By [36, 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  $\text{char}(\kappa(v)) \neq 2$  then all points of order 4 on  $A(v)$  are defined over  $\kappa(v)$ ; if  $\text{char}(\kappa(v)) \neq 3$  then all points of order 3 on  $A(v)$  are defined over  $\kappa(v)$ . It follows from the

theorem of Silverberg that all  $\overline{\kappa(v)}$ -endomorphisms of  $A(v)$  are defined over  $\kappa(v)$ . For each  $v$  we get an embedding of  $\mathbb{Q}$ -algebras

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

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

**Theorem 4.1** *If  $\ell := \text{char}(\kappa(v)) \neq p$  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  $\ell$ .

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  $\pi$  be a *Weil  $q_v$ -number* that corresponds to the  $\kappa(v)$ -isogeny class of  $A(v)$  [51, 52]. In particular,  $\pi$  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  $\pi$ .

Let  $E = \mathbb{Q}(\pi)$  be the number field generated by  $\pi$  and let  $\mathcal{O}_E$  be the ring of integers in  $E$ . Then  $E$  contains  $\bar{\pi}$  and is isomorphic to the center of  $\text{End}^0(A(v))$  [51, 52]; one may view  $\text{End}^0(A(v))$  as a *central* division algebra over  $E$ . It is known that  $E$  is either  $\mathbb{Q}$ ,  $\mathbb{Q}(\sqrt{\ell})$  or a (purely imaginary) CM field [52, 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  $[E : \mathbb{Q}]$  divides  $2\dim(A(v))$ , we have  $[E : \mathbb{Q}] = 2, 4$  or 8. By [52, p. 96, Th. 1(ii), formula (2)]<sup>3</sup>,

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

Since  $\text{End}^0(A(v))$  is *noncommutative*, it follows that  $E$  is either an imaginary quadratic field and  $\text{End}^0(A(v))$  is a 16-dimensional division algebra over  $E$  or  $E$  is a CM field of degree 4 and  $\text{End}^0(A(v))$  is a 4-dimensional (i.e., quaternion) division algebra over  $E$ . In both cases  $\text{End}^0(A(v))$  is unramified at all places of  $E$  except some places of residual characteristic  $\ell$  [52, p. 96, Th. 1(ii)]. It follows from the Hasse–Brauer–Noether theorem that  $\text{End}^0(A(v))$

<sup>3</sup>In [52] our  $E$  is denoted by  $F$  while our  $\text{End}^0(A(v))$  is denoted by  $E$ .

is ramified at, at least, two places of  $E$  with residual characteristic  $\ell$ . This implies that  $\mathcal{O}_E$  contains, at least, two maximal ideals that lie above  $\ell$ .

Clearly,

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

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

First assume that  $E$  has degree 4 and  $\text{End}^0(A(v))$  is a quaternion algebra. Then (thanks to the theorem of Hasse–Brauer–Noether) there exists a place  $w$  of  $E$  with residual characteristic  $\ell$  and such that the localization  $\text{End}^0(A(v)) \otimes_E E_w$  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)  $\mathbb{Q}_\ell$ -algebra homomorphism

$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \rightarrow \text{End}^0(A(v)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \rightarrow \text{End}^0(A(v)) \otimes_E E_w.$$

This implies that  $\text{End}^0(A(v)) \otimes_E E_w$  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

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

In particular, the order of the class of  $\text{End}^0(A(v))$  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  $\ell$ . 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

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

Let

$$\text{ord}_{w_i} : E^* \rightarrow \mathbb{Z}$$

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

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

By [52, page 96, Th. 1(ii), formula (1)], the local invariant of  $\text{End}^0(A(v))$  at  $w_i$  is

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

In addition, the sum in  $\mathbb{Q}/\mathbb{Z}$  of local invariants of  $\text{End}^0(A(v))$  at  $w_1$  and  $w_2$  is zero [52, 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  $\text{End}^0(A(v))$  in the Brauer group of  $E$  is either 2 or 4, we conclude that the local invariants of  $\text{End}^0(A(v))$  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  $\text{End}^0(A(v))$  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  $\text{End}^0(A(v))$  that

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

and therefore  $\bar{\pi}/\pi$  is a  $w_i$ -adic unit for both  $w_1$  and  $w_2$ . Therefore  $\bar{\pi}/\pi$  is an  $\ell$ -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

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

and therefore  $\mathbb{Q}(\pi^m) = \mathbb{Q}$ . Let  $\kappa(v)_m$  be the finite degree  $m$  field extension of  $\kappa(v)$ , which consists of  $q_v^m$  elements. Then  $\pi^m$  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  $\mathbb{Q}(\pi^m) = \mathbb{Q}$ , 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  $\text{End}^0(A(v)) \otimes_E E_{w_1}$  in the Brauer group of the  $E_{w_1} \cong \mathbb{Q}_\ell$  is 4. This implies that  $\text{End}^0(A(v)) \otimes_E E_{w_1}$  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  $\text{End}^0(A(v)) \otimes_E E_{w_1}$  is a *division algebra* over  $E_{w_1}$ . However, there is again a nonzero (because it sends 1 to 1)  $\mathbb{Q}_\ell$ -algebra homomorphism

$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \rightarrow \text{End}^0(A(v)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \rightarrow \text{End}^0(A(v)) \otimes_E E_{w_1}.$$

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

**Theorem 4.2** *If  $\ell := \text{char}(\kappa(v)) \neq p$  then there exists an abelian surface  $B(v)$  over  $\kappa(v)$  such that  $A(v)$  is  $\kappa(v)$ -isogenous to the square  $B(v)^2$  of  $B(v)$ .*

**Proof.** We know that  $A(v)$  is *not* simple and that all  $\overline{\kappa(v)}$ -endomorphisms of  $A(v)$  are defined over  $k(v)$ . Now let us split  $A(v)$  up to a  $\kappa(v)$ -isogeny into a product of its  $\kappa(v)$ -isotypic components, using Poincaré Complete Reducibility Theorem [26, Th. 6 on p. 28 and Th. 7 on p. 30]. In other words, there is a  $\kappa(v)$ -isogeny

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

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

$$\text{End}^0(A(v)) \cong \text{End}^0\left(\prod_{i \in I} A_i\right) = \bigoplus_{i \in I} \text{End}^0(A_i).$$

This gives us nonzero  $\mathbb{Q}$ -algebra homomorphisms

$$D \rightarrow \text{End}^0(A_i)$$

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

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

Since all  $\overline{\kappa(v)}$ -endomorphisms of  $A(v)$  are defined over  $k(v)$ , all  $\overline{\kappa(v)}$ -endomorphisms of  $A_i$  are also defined over  $\kappa(v)$ ; in addition, if  $i$  and  $j$  are distinct elements of  $I$  then every  $\overline{\kappa(v)}$ -homomorphism between  $A_i$  and  $A_j$  is 0.

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 [54, Remark 4.1 on p. 2088]. However, in both (ordinary and almost ordinary) cases the endomorphism algebra of a simple abelian variety is commutative [38, Lemma 2.3 on p. 136]. 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. It follows that if  $\ell = \text{char}(\kappa(v)) \neq p$  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  $A(v)$ .  $\square$

Let  $B(v)$  be as in Theorem 4.2. One may lift the abelian surface  $B(v)$  over  $\kappa(v)$  to an abelian surface  $B^v$  over  $K_v$ , whose reduction is  $B(v)$  (see [37, Prop. 11.1 on p. 177]). Now if one restricts the action of  $G_K$  on the  $\mathbb{Q}_r$ -Tate module (here  $r$  is any prime different from  $\text{char}(\kappa(v))$ )

$$V_r(A) = T_r(A) \otimes_{\mathbb{Z}_r} \mathbb{Q}_r$$

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 4.3** *If  $r \neq p$  and  $\text{char}(\kappa(v)) \neq r$  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  $V_r(A)$ . Since the Frobenius endomorphism of  $A(v)$  acts on  $V_r(A)$  as a semisimple linear operator (by a theorem of A. Weil), the



$G_{K_v}$ -module  $V_r(A)$  is semisimple. This implies that the  $G_{K_v}$ -modules  $V_r(B^v)$  and  $W_r(A)$  are isomorphic.  $\square$

For primes  $\ell \neq p$ , the algebra  $D \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$  splits and correspondingly, the representation  $V_{\ell}(A)$  splits as  $W_{\ell} \oplus W_{\ell}$ . Locally, at a place  $v \nmid \ell$ , we have  $W_{\ell} \cong V_{\ell}(B^v)$ . However, *globally*, the representation  $W_{\ell}$  does *not* come from an abelian variety over  $K$ . Indeed, if the  $G_K$ -module  $W_{\ell}$  is isomorphic to  $V_{\ell}(B)$  for an abelian variety  $B$  over  $K$  then  $\dim(B) = 2$  and the theorem of Faltings implies that there is a *nonzero* homomorphism of abelian varieties  $B \rightarrow A$  over  $K$ , which is not the case, since the fourfold  $A$  is simple. On the other hand, if  $v \mid \ell$  then  $V_{\ell}(A)$  is a *deRham representation* of  $G_{K_v}$  with weights 0 and  $-1$ , both of multiplicity  $\dim(A) = 4$ . Since a subrepresentation of a deRham representation is also deRham, we conclude that  $W_{\ell}$  is deRham. It is also clear that  $W_{\ell}$  has the same Hodge-Tate weights as

$$V_{\ell}(A) = W_{\ell} \oplus W_{\ell}$$

but the multiplicities should be divided by 2, i.e., the Hodge-Tate weights of  $W_{\ell}$  are 0 and  $-1$ , both of multiplicity 2.

We thus obtain:

**Theorem 4.4** *The system of representations  $\{W_{\ell}\}_{\ell \neq p}$  constructed above does not come globally from an abelian variety defined over the field  $K$  but for all  $v \nmid \ell$  the representation  $W_{\ell}$  locally comes from an abelian variety  $B^v/K_v$ . In particular,  $\{W_{\ell}\}_{\ell \neq p}$  is a weakly compatible system of 4-dimensional  $\ell$ -adic representations of  $G_K$ .*

*If  $v \mid \ell$  then  $W_{\ell}$  is locally a deRham representation with Hodge-Tate weights 0 and  $-1$ , both of multiplicity 2.*

**Remark** By a theorem of Faltings [10], the  $G_K$ -module  $V_{\ell}(A)$  is semisimple and therefore its submodule  $W_{\ell}$  is also semisimple. On the other hand, we know that the centralizer

$$\text{End}_{G_K}(W_{\ell}) = k \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell} \neq \mathbb{Q}_{\ell};$$

in particular, none of  $W_{\ell}$  is absolutely irreducible. In what follows we construct an example of a weakly compatible system (for all  $\ell \neq p$ ) of absolutely irreducible deRham representations that does not come globally from an abelian variety over a number field. However, we do not know whether it comes *locally* from abelian varieties.

Let  $p$  be a prime and  $H$  be a *definite* quaternion algebra over  $\mathbb{Q}$  that is unramified exactly at  $p$  and  $\infty$ . In particular, for each prime  $\ell \neq p$  the  $\mathbb{Q}_\ell$ -algebra

$$H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathbb{M}_2(\mathbb{Q}_\ell).$$

Let  $g \geq 4$  be an even integer. According to Shimura ([46], see also the case of Type III( $e_0 = 1$ ) with  $m = g/2$  in [36, Table 8.1 on p. 498] and [39, Table on p. 23]) there exists a complex  $g$ -dimensional abelian variety  $X$ , whose endomorphism algebra  $\text{End}^0(X)$  is isomorphic to  $H$ . The same arguments as above (related to  $D$ ) prove that there exists a  $g$ -dimensional abelian variety  $B$  over a certain number field  $K$  such that all endomorphisms of  $B$  are defined over  $K$  and  $\text{End}^0(B) \cong H$ . In particular,  $B$  is absolutely simple. By the theorem of Faltings, if  $\ell$  is a prime then the  $G_K$ -module  $V_\ell(B)$  is semisimple and

$$\text{End}_{G_K}(V_\ell(B)) = H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

In particular, if  $\ell \neq p$  then  $\text{End}_{G_K}(V_\ell(B)) \cong \mathbb{M}_2(\mathbb{Q}_\ell)$  and therefore there are two isomorphic  $\mathbb{Q}_\ell[G_K]$ -submodules  $U_{1,\ell}(B)$  and  $U_{2,\ell}(B)$  in  $V_\ell(B)$  such that

$$V_\ell(B) = U_{1,\ell}(B) \oplus U_{2,\ell}(B) \cong U_{1,\ell}(B) \oplus U_{1,\ell}(B) \cong U_{2,\ell}(B) \oplus U_{2,\ell}(B).$$

If we denote by  $U_\ell$  the  $\mathbb{Q}_\ell[G_K]$ -module  $U_{1,\ell}(B)$  then  $\dim_{\mathbb{Q}_\ell}(U_\ell) = g$  and we get an isomorphism of  $\mathbb{Q}_\ell[G_K]$ -modules

$$V_\ell(B) \cong U_\ell \oplus U_\ell.$$

Clearly, the submodule  $U_\ell$  is semisimple and

$$\mathbb{M}_2(\mathbb{Q}_\ell) = H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \text{End}_{G_K}(V_\ell(B)) = \mathbb{M}_2(\text{End}_{G_K}(U_\ell)).$$

This implies that  $\text{End}_{G_K}(U_\ell) = \mathbb{Q}_\ell$ , i.e., the  $\ell$ -adic (sub)representation

$$G_K \rightarrow \text{Aut}_{\mathbb{Q}_\ell}(U_\ell) \cong \text{GL}_g(\mathbb{Q}_\ell)$$

is *absolutely irreducible*. Clearly, for each  $\sigma \in G_K$  its characteristic polynomial with respect to the action on  $V_\ell(B)$  is the square of its characteristic polynomial with respect to the action on  $U_\ell$ . This implies that if  $v$  is a nonarchimedean place  $v$  of  $K$  where  $B$  has good reduction then for all primes  $\ell \neq p$  such that  $v \nmid \ell$  the characteristic polynomial of the frobenius element at  $v$  with respect to its action on  $U_\ell$  has rational coefficients and does not

depend on  $\ell$ . In other words,  $U_\ell$  is a weakly compatible system of (absolutely irreducible)  $\ell$ -adic representations. As above, locally for each  $v \mid \ell$  the  $G_{K_v}$ -module  $V_\ell(B)$  is deRham with Hodge weights 0 and  $-1$  with weights  $g$ , which implies that  $U_\ell$  is also deRham with the same Hodge-Tate weights, whose multiplicities are  $g/2$ .

**Theorem 4.5** *The weakly compatible system of  $g$ -dimensional absolutely irreducible representations  $\{U_\ell\}_{\ell \neq p}$  constructed above does not come globally from an abelian variety defined over the field  $K$ .*

*If  $v \mid \ell$  then  $U_\ell$  is locally a deRham representation with Hodge-Tate weights 0 and  $-1$ , both of multiplicity  $g/2$ .*

**Proof.** We claim that none of  $U_\ell$  comes out from an abelian variety over  $K$ . Indeed, if there is an abelian variety  $C$  over  $K$  such that the  $G_K$ -modules  $V_\ell(C)$  and  $U_\ell$  are isomorphic then  $\dim(C) = g/2$  and the theorem of Faltings implies the existence of a *nonzero* homomorphism  $C \rightarrow B$ , which contradicts the simplicity of  $g$ -dimensional  $B$ .  $\square$

## 5 Almost isomorphic abelian varieties

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

In this section we discuss the structure of the right  $\text{End}(A)$ -module  $\text{Hom}(A, B)$  when the  $\mathbb{Z}_\ell$ -Tate modules of  $A$  and  $B$  are isomorphic as Galois modules for all  $\ell$  and  $K$  is finitely generated over  $\mathbb{Q}$ . If  $\ell \neq \text{char}(K)$  and  $X$  is an abelian variety over  $K$  then we write  $X[\ell]$  for the kernel of multiplication by  $\ell$  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 isomorphism of  $G_K$ -modules  $X[\ell] \cong T_\ell(X)/\ell T_\ell(X)$ .

**Lemma 5.1** *Let  $A$  and  $B$  be abelian varieties of positive dimension over  $K$ .*

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

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

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

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

- (c) *If the equivalent conditions (i) and (ii) hold and  $\dim(B) \leq \dim(A)$  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  $\phi : A \rightarrow B_0$ . It follows that  $\text{Hom}(A, B_0) \otimes \mathbb{Q} = \phi \text{End}^0(A)$  is a free right  $\text{End}^0(A)$ -module of rank 1 generated by  $\phi$ . Now (bi) follows from the equality

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

Suppose that (bi) is true. We may choose a homomorphism of abelian varieties  $\phi : A \rightarrow B$  as a generator (basis) of the free right  $\text{End}(A) \otimes \mathbb{Q}$ -module  $\text{Hom}(A, B) \otimes \mathbb{Q}$ . In other words, for every homomorphism of abelian varieties  $\psi : A \rightarrow B$  there are  $u \in \text{End}(A)$  and a nonzero integer  $n$  such that  $n\psi = \phi u$ . In addition, for each nonzero  $u \in \text{End}(A)$  the composition  $\phi u$  is a nonzero element of  $\text{Hom}(A, B)$ . Clearly,  $B_0 := \phi(A) \subset B$  is an abelian  $K$ -subvariety of  $B$  with  $\dim(B_0) \leq \dim(A)$ . 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  $\text{Hom}(A, B) = \text{Hom}(A, B_0)$ . On the other hand, if  $\dim(B_0) = \dim(A)$  then  $\phi : A \rightarrow B_0$  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 there is an endomorphism  $u_0 \in \text{End}(A)$  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  $\text{Hom}(A, B)$  and we get a contradiction, which proves (bii).

(c) follows readily from (bii). □

**Lemma 5.2** *Suppose that  $A, B, C$  are abelian varieties over  $K$  of positive dimension that are mutually isogenous over  $K$ . We view  $\text{Hom}(A, B) \otimes \mathbb{Q}$  and  $\text{Hom}(A, C) \otimes \mathbb{Q}$  as right  $\text{End}^0(A) = \text{End}(A) \otimes \mathbb{Q}$ -modules. Then the natural map*

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

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

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

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 section 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 [10, 11],

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

**Lemma 5.3** *Let  $\ell$  be a prime. Then the following conditions are equivalent.*

- (i) *There is an isogeny  $\phi_\ell : A \rightarrow B$ , whose degree is prime to  $\ell$ .*
- (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  $\text{End}(A) \otimes \mathbb{Z}_{(\ell)}$ -module  $\text{Hom}(A, B) \otimes \mathbb{Z}_{(\ell)}$  is free of rank 1 and the right  $\text{End}(A) \otimes \mathbb{Z}_\ell$ -module  $\text{Hom}(A, B) \otimes \mathbb{Z}_\ell$  is free of rank 1*

**Proof.** (i) implies (ii). Indeed, let  $\phi_\ell : A \rightarrow B$  be an isogeny such that its degree  $d := \deg(\phi_\ell)$  is prime to  $\ell$ . Then there exists an isogeny  $\varphi_\ell : B \rightarrow A$  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  $\phi_\ell$  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  $\text{Hom}(A, B) \otimes \mathbb{Z}_\ell$ . Since  $\text{Hom}(A, B)$  is dense in  $\text{Hom}(A, B) \otimes \mathbb{Z}_\ell$  in the  $\ell$ -adic topology, and the set of isomorphisms  $T_\ell(A) \cong T_\ell(B)$  is open in  $\text{Hom}(A, B) \otimes \mathbb{Z}_\ell$ , there is  $\phi_\ell \in \text{Hom}(A, B)$  that induces an isomorphism  $T_\ell(A) \cong T_\ell(B)$ . Clearly,  $\ker(\phi_\ell)$  does not contain points of order  $\ell$  and therefore is finite. This implies that  $\phi_\ell$  is an isogeny, whose degree is prime to  $\ell$ . This proves (i).

In order to prove the last assertion of Lemma 5.3, one has only to observe that  $\phi_\ell \in \text{Hom}(A, B) \subset \text{Hom}(A, B) \otimes \mathbb{Z}_{(\ell)} \subset \text{Hom}(A, B) \otimes \mathbb{Z}_\ell$  is a generator of the (obviously) free right  $\mathbb{Z}_{(\ell)}$ -module  $\text{Hom}(A, B) \otimes \mathbb{Z}_{(\ell)}$  and of the free right  $\mathbb{Z}_\ell$ -module  $\text{Hom}(A, B) \otimes \mathbb{Z}_\ell$ .  $\square$

We say that  $A$  and  $B$  are *almost isomorphic* if for *all primes*  $\ell$  the equivalent conditions (i) and (ii) of Lemma 5.3 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 5.4** *Suppose that  $A$  and  $B$  are almost isomorphic. Then  $A$  and  $B$  are isomorphic over  $K$  if and only if  $\text{Hom}(A, B)$  is a free  $\text{End}(A)$ -module of rank 1. In particular, if  $\text{End}(A)$  is a principal ideal domain (for example,  $\text{End}(A) = \mathbb{Z}$ ) then every abelian variety over  $K$ , which is almost isomorphic to  $A$ , is actually isomorphic to  $A$ .*

**Proof.** Suppose  $\text{Hom}(A, B)$  is a free  $\text{End}(A)$ -module, i.e., there is a homomorphism of abelian varieties  $\phi : A \rightarrow B$  such that  $\text{Hom}(A, B) = \phi \text{End}(A)$ . We know that for any prime  $\ell$  there is an isogeny  $\phi_\ell : A \rightarrow B$  of degree prime to  $\ell$ . (In particular,  $\dim(A) = \dim(B)$ .) Therefore there is  $u_\ell \in \text{End}(A)$  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  $\ell$ , we conclude that  $\phi(A) = B$  (i.e.,

$\phi$  is an isogeny) and  $\deg(\phi)$  is prime to  $\ell$ . Since the latter is true for all primes  $\ell$ , we conclude that  $\deg(\phi) = 1$ , i.e.,  $\phi$  is an isomorphism.

Conversely, if  $A \cong B$  then  $\text{Hom}(A, B)$  is obviously a free  $\text{End}(A)$ -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.  $\square$

The next statement is a generalization of Corollary 5.4.

**Corollary 5.5** *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  $\text{End}(A)$ -modules  $\text{Hom}(A, B)$  and  $\text{Hom}(A, C)$  are isomorphic.*

**Proof.** We know that all  $A, B, C$  are mutually isogenous over  $K$ . Let us choose an isogeny  $\phi : B \rightarrow C$ . We are given an isomorphism  $\delta : \text{Hom}(A, B) \cong \text{Hom}(A, C)$  of right  $\text{End}(A)$ -modules that obviously extends by  $\mathbb{Q}$ -linearity to the isomorphism  $\text{Hom}(A, B) \otimes \mathbb{Q} \rightarrow \text{Hom}(A, C) \otimes \mathbb{Q}$  of right  $\text{End}(A) \otimes \mathbb{Q}$ -modules, which we continue to denote by  $\delta$ . By Lemma 5.2, there exists  $\tau_0 \in \text{Hom}(B, C) \otimes \mathbb{Q}$  such that  $\delta = m_{B,C}(\tau_0)$ , i.e.,

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

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

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

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

**Remark** Let  $\mathcal{Z}(A)$  (resp.  $\mathcal{Z}(B)$ ) be the the center of  $\text{End}(A)$  (resp.  $\text{End}(B)$ ). 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  $\text{End}(A) \otimes \mathbb{Q}$  (resp.  $\text{End}(B) \otimes \mathbb{Q}$ ) and for all primes  $\ell$  the  $\mathbb{Z}_{(\ell)}$ -subalgebra

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

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

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

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

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

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  $i_{\phi}$  to the center(s) does *not* depend on a choice of  $\phi$  [56]. If  $\phi_{\ell} : A \rightarrow B$  is a  $K$ -isogeny of degree prime to  $\ell$  then  $i_{\phi_{\ell}}(\text{End}(A) \otimes \mathbb{Z}_{(\ell)}) = \text{End}(B) \otimes \mathbb{Z}_{(\ell)}$  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  $\text{End}(A)$  is commutative then  $\text{End}(B)$  is also commutative (because  $\text{End}(A) \otimes \mathbb{Q}$  and  $\text{End}(B) \otimes \mathbb{Q}$  are isomorphic) and there is a canonical ring isomorphism  $\text{End}(A) \cong \text{End}(B)$ .

Until the end of this section,  $\Lambda$  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  $\Lambda_{\ell}$  (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

$$\begin{aligned} \Lambda &= \Lambda \otimes 1 \subset \Lambda_{(\ell)} \subset \Lambda_{\mathbb{Q}} \subset \Lambda \otimes \mathbb{Q}_{\ell}, \\ \Lambda &\subset \Lambda_{(\ell)} \subset \Lambda_{\ell} \subset \Lambda \otimes \mathbb{Q}_{\ell}. \end{aligned}$$

In addition, the intersection of  $\Lambda_{\ell}$  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  $\Lambda$ -module. We write  $M_{\mathbb{Q}}$  for the right  $\Lambda_{\mathbb{Q}}$ -module  $M \otimes \mathbb{Q}$ ,  $M_{\ell}$  for the right  $\Lambda_{\ell}$ -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  $M_\ell$  and  $M_\mathbb{Q}$  (in  $M \otimes \mathbb{Q}_\ell$ ) coincides with  $M_{(\ell)}$ .

**Definition.** We say that  $M$  is a *locally free right  $\Lambda$ -module of rank 1* if for all primes  $\ell$  the right  $\Lambda_\ell$ -module  $M_\ell$  is free of rank 1. (See [15].)

**Theorem 5.6** *Let  $M$  be a locally free right  $\Lambda$ -module of rank 1. Then it enjoys the following properties.*

- (i)  *$M$  is a projective  $\Lambda$ -module. More precisely,  $M$  is isomorphic to a direct summand of a free right  $\Lambda$ -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  $\ell$ .*

**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  $\Lambda_\mathbb{Q}$  [15, p. 114]. (In the notation of [15, 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  $\Lambda$ -submodule  $\alpha\Lambda \subset \Lambda_\mathbb{Q}$  that is a locally free  $\Lambda$ -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  $\alpha\Lambda \otimes \mathbb{Q} \rightarrow \Lambda_\mathbb{Q}$  is an isomorphism [15, 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  $\Lambda$ -module of rank 2 [15, 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 [15], every right locally free  $\Lambda$ -module  $M$  of rank 1 is isomorphic to  $\alpha\Lambda$  for a suitable  $\alpha$ . 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  $\ell$  and  $f_0$  is also a generator of  $M \otimes \mathbb{Q}_\ell$ . It is also clear that every generator  $f_\ell$  of the  $\Lambda_\ell$ -module  $M_\ell$  is a generator of the  $\Lambda \otimes \mathbb{Q}_\ell$ -module  $M \otimes \mathbb{Q}_\ell$ . We claim that there is a generator  $f_\ell$  that lies in  $M$ . Indeed, with respect to the  $\ell$ -adic topology, the subset

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

is dense in  $M_\ell$  while the set of generators of the free  $\Lambda_\ell$ -module  $M_\ell$  is open, because the group of units  $(\Lambda_\ell)^*$  is open in  $\Lambda_\ell$ . This implies that there exists a (nonzero) generator  $f_\ell \in M \subset M_\ell$  of the  $\Lambda_\ell$ -module  $M_\ell$ . Recall that  $f_\ell$  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  $f_\ell$  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  $\mu_0$  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  $f_\ell$  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  $f_\ell$ .) 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  $f_\ell$  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  $f\mu_0 = x = f\lambda$  in  $M \otimes \mathbb{Q}_\ell$ .

Since  $f_\ell$  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  $\Lambda_\ell$  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).  $\square$

**Corollary 5.7** *Let  $M$  be a free commutative group of finite positive rank that is provided with a structure of a right  $\Lambda$ -module. Then  $M$  is a locally free  $\Lambda$ -module of rank 1 if and only if the right  $\Lambda_{(\ell)}$ -module  $M_{(\ell)}$  is free of rank 1 for all primes  $\ell$ .*

**Proof.** Clearly, if  $M_{(\ell)}$  is a free right  $\Lambda_{(\ell)}$ -module of rank 1 then the right  $\Lambda_\ell$ -module  $M_\ell$  is free of rank 1. The converse follows from Theorem 5.6(iii).  $\square$

**Remark** Suppose that  $\Lambda$  is an *order* in a number field  $E$ , i.e.,  $\Lambda$  is a finitely generated over  $\mathbb{Z}$  a subring (with 1) of  $E$  such that  $\Lambda_\mathbb{Q} = E$ . Let  $M$  be a  $\Lambda$ -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  $\Lambda$  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* [27, 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 5.7,  $M$  is locally free of rank 1.

- (ii) Suppose that  $E$  is a quadratic field. We don't impose any restrictions on  $\Lambda$  but instead assume that  $\text{End}_{\Lambda}(M) = \Lambda$ . Then it is known [3, Lemma 2 on p. 55] that for each prime  $\ell$  there is a nonzero ideal  $\mathfrak{J} \subset \Lambda$  such that the order of the finite quotient  $\Lambda/\mathfrak{J}$  is prime to  $\ell$  and the  $\Lambda$ -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 5.7,  $M$  is locally free of rank 1.

Now we are going to use Theorem 5.6, 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* ([5, Sect. 7], [6, Sect. 1.7.4]).

Suppose we are given a free commutative group  $M$  of finite (positive) rank that is provided with a structure of a right locally free  $\Lambda = \text{End}(A)$ -module of rank 1. Let  $F_2$  be a free right  $\Lambda$ -module of rank 2. It follows from Theorem 5.6(i) that there is an endomorphism  $\gamma : F_2 \rightarrow F_2$  of the right  $\Lambda$ -module  $F_2$  such that  $\gamma^2 = \gamma$  and whose image  $M' = \gamma(F_2)$  is isomorphic to  $M$ . Notice that  $\text{End}_{\Lambda}(F_2)$  is the matrix algebra  $\mathbb{M}_2(\Lambda)$  of size 2 over  $\Lambda$ . So, the idempotent

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

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  $B \times C \rightarrow A^2$ ,  $(x, y) \mapsto x + y$  of abelian varieties over  $K$  is an isomorphism, i.e.,  $A^2 = B \times C$ . This implies that the right  $\text{End}(A)$ -module  $\text{Hom}(A, B)$  coincides with

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

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

$$\gamma(A^2[\ell]) = B[\ell]. \tag{**}$$

**Theorem 5.8** *Let us consider the abelian variety  $B = A \otimes M$  over  $K$ . Then:*

- (i)  *$A$  and  $B$  are isogenous over  $K$ .*
- (ii) *The right  $\text{End}(A)$ -module  $\text{Hom}(A, B)$  is isomorphic to  $M$ .*
- (iii)  *$A$  and  $B$  are almost isomorphic.*

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

Since the right  $\text{End}(A) \otimes \mathbb{Q}$ -module  $M \otimes \mathbb{Q}$  is free of rank 1, the same is true for the right  $\text{End}(A) \otimes \mathbb{Q}$ -module  $\text{Hom}(A, B)$ . By Lemma 5.1,  $\dim(A) \leq \dim(B)$  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

$$\text{Hom}(A, B) = \text{Hom}(A, B_0). \quad (***)$$

We claim that  $B = B_0$ . Indeed, if  $B_0 \neq B$  then, by the Poincaré Complete Reducibility theorem [26, Th. 6 on p. 28], there is an “almost complementary” abelian  $K$ -subvariety  $B_1 \subset B$  of positive dimension  $\dim(B) - \dim(B_0)$  such that the intersection  $B_0 \cap B_1$  is finite and  $B_0 + B_1 = B$ . It follows from (\*\*\*) that  $\text{Hom}(A, B_1) = \{0\}$ . However,  $B_1 \subset B \subset A^2$  is an abelian  $K$ -subvariety of  $A^2$  and therefore there is a surjective homomorphism  $A^2 \rightarrow B$  and therefore there exists a nonzero homomorphism  $A \rightarrow B$ . This is a contradiction, which proves that  $B = B_0$ , the right  $\text{End}(A)$ -module  $\text{Hom}(A, B)$  is isomorphic to  $M$ , and  $A$  and  $B$  are isogenous over  $K$ . In particular,  $\dim(A) = \dim(B)$ . This proves (i).

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

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

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

$$\phi_1 = \phi u_1, \quad \phi_2 = \phi u_2$$

in  $\text{Hom}(A, B) \otimes \mathbb{Z}_\ell$ . 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  $\phi$  induces a surjective homomorphism  $A[\ell] \rightarrow B[\ell]$ . Since finite groups  $A[\ell]$  and  $B[\ell]$  have the same order,  $\phi$  induces an isomorphism  $A[\ell] \rightarrow B[\ell]$ . This implies that  $\ker(\phi)$  does not contain points of order  $\ell$  and therefore is an isogeny of degree prime to  $\ell$ . This proves (iii).  $\square$

**Corollary 5.9** *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  $\text{End}(A)$ -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  $\text{End}(A)$ -modules  $M_1$  and  $M_2$  are isomorphic.*

**Proof.** By Theorem 5.8(ii), the right  $\text{End}(A)$ -module  $\text{Hom}(A, B_i)$  is isomorphic to  $M_i$ . Now the result follows from Theorem 5.8(iii) combined with Corollary 5.5.  $\square$

**Corollary 5.10** *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  $\ell$ . Then abelian varieties  $B$  and  $C := A \otimes \text{Hom}(A, B)$  are isomorphic over  $K$ .*

**Proof.** By Theorem 5.8(ii), the right  $\text{End}(A)$ -module  $\text{Hom}(A, C)$  is isomorphic to  $\text{Hom}(A, B)$ . Now the result follows from Theorem 5.8(iii) combined with Corollary 5.5.  $\square$

**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  $\text{Hom}(A_1, A_2) = \{0\}$ . Then  $\text{End}(A) = \text{End}(A_1) \oplus \text{End}(A_2)$ . 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  $\text{End}(A_i)$ -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  $\text{End}(A_1) \oplus \text{End}(A_2) = \text{End}(A)$ . 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, suppose  $A_1$  is principally polarized,  $\text{End}(A_1) = \mathbb{Z}$  and all  $\bar{K}$ -endomorphisms of  $A$  are defined over  $K$ ; in particular,  $A$  is absolutely simple. Let us take  $M_1 = \mathbb{Z}$ . Let  $A_2$  be an elliptic curve such that  $\text{End}(A_2)$  is the ring of integers in an imaginary quadratic field with class number  $> 1$ . Clearly,  $\text{Hom}(A_1, A_2) = \{0\}$ . Actually, every  $\bar{K}$ -homomorphism between  $A_1$

and  $A_2$  is 0. Let  $M_2$  be a *non-principal* ideal in  $\text{End}(A_2)$ . 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  $\bar{K}$ . On the other hand, 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.

## 6 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 [19]. It is defined over  $\mathbb{Q}$  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  $\mathbb{Q}$  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 [28], in particular, lemma 2.1)  $\rho : \pi_1(\mathcal{M}_g) \rightarrow \text{Out}(\pi_1(\bar{X}))$ . This follows by considering the universal curve  $\mathcal{C}_g$  of genus  $g$  together with the map  $\mathcal{C}_g \rightarrow \mathcal{M}_g$ , so  $X$  can be viewed as a fiber of this map. This gives rise to the fibration exact sequence

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

and the action of  $\pi_1(\mathcal{C}_g)$  on  $\pi_1(\bar{X})$  gives  $\rho$ . Now,  $X$ , viewed as a point on  $\mathcal{M}_g(K)$ , gives a map  $\sigma_{\mathcal{M}_g/K}(X) : G_K \rightarrow \pi_1(\mathcal{M}_g)$ . As pointed out in [28],  $\rho \circ \sigma_{\mathcal{M}_g/K}(X)$  induces a map  $G_K \rightarrow \text{Out}(\pi_1(\bar{X}))$  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 6.1** *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 [49] if we assume that  $\sigma_{\mathcal{M}_g/K}$  surjects onto  $S_0(K, \mathcal{M}_g)$ .

**Theorem 6.2** *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  $X \rightarrow \mathcal{M}_g$  with image  $Y$ , say, for some  $g$ , defined over an extension  $L$  of  $K$ , given by the Kodaira-Parshin construction. This gives a map  $\gamma : \pi_1(X \otimes L) \rightarrow \pi_1(\mathcal{M}_g \otimes L)$ , over  $L$ . Let  $s \in S(K, X)$ , then  $\gamma \circ (s|_{G_L}) \in S_0(L, \mathcal{M}_g)$  and the assumption of the theorem yields that  $\gamma \circ (s|_{G_L}) = \sigma_{\mathcal{M}_g/L}(P)$ ,  $P \in \mathcal{M}_g(L)$ . 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 [49], Proposition 5.2, we conclude that  $X$  has a rational point corresponding to  $s$ .  $\square$

**Acknowledgements.** The second author would like to thank J. Achter, D. Harari, E. Ozman, T. Schläpke, 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, Ching-Li Chai and Jiangwei Xue 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). The final version of this paper was prepared in May–June 2016 when he was a visitor at the Max-Planck-Institut für Mathematik (Bonn, Germany). The hospitality and support of both Institutes are gratefully acknowledged.

We are very grateful to the anonymous referees, whose careful readings and comments have greatly improved the readability of this paper. We would also like to thank W. Sawin for comments.

## References

- [1] Y. André, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*. Panoramas et Synthèses **17**, Société Mathématique de France, Paris, 2004.
- [2] H. Bass, M. Lazard, J.-P. Serre, *Sous-groupes d'indice fini dans  $SL(n, \mathbb{Z})$* . Bull. Amer. Math. Soc. **70** (1964) 385–392.

- [3] Z.I. Borevich, D.K. Faddeev, Integral representations of quadratic rings. (Russian) Vestnik Leningrad. Univ. **15** (1960), no. 19, 52–64. MR0153707 (27 #3668).
- [4] O. Brinon, B. Conrad, *CMI Summer School Notes on  $p$ -adic Hodge Theory (preliminary version)*. <http://www.claymath.org/galois-representations> .
- [5] 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.
- [6] C.-L. Chai, B. Conrad, F. Oort, Complex multiplication and lifting problems, *Mathematical Surveys and Monographs* **195**, American Mathematical Society, Providence, RI, 2014.
- [7] P. Deligne, *Cohomologie étale*. Lecture Notes in Mathematics, vol. **569**, Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 $\frac{1}{2}$ , avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier, Springer-Verlag, Berlin-NewYork (1977).
- [8] P. Deligne, *Formes modulaires et représentations  $l$ -adiques*. Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Exp. No. 355, 139–172, Lecture Notes in Mathematics, vol. **175**, Springer-Verlag, Berlin, 1971.
- [9] 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.
- [10] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.
- [11] 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.
- [12] G. Faltings, *Crystalline cohomology and  $p$ -adic Galois representations*. In: Algebraic analysis, geometry, and number theory. Johns Hopkins Univ. Press, Baltimore (1989), pp 25-80.



- [13] 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.
- [14] J.-M. Fontaine, Y. Ouyang, Theory of  $p$ -adic representations. Springer, to appear; <http://www.math.upsud.fr/~fontaine/recherche.html> .
- [15] A. Frölich, *Locally free modules over arithmetic orders*. J. Reine Angew. Math. **274/275** (1975), 112–124.
- [16] A. Grothendieck, *Modèles de Néron et monodromie*. In: Groupes de monodromie en géométrie algébrique (SGA7 I), Exp. IX, , Lecture Notes in Mathematics **288** (1972), pp. 313–523; Springer-Verlag, Berlin, Heidelberg.
- [17] 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.
- [18] 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.
- [19] R. Hain, *Rational points of universal curves*. J. Amer. Math. Soc. **24** (2011), 709–769.
- [20] 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.
- [21] D. Harari, J. F. Voloch, *The Brauer-Manin obstruction for integral points on curves*, Math. Proc. Cam. Phil. Soc, **149** (2010), 413-421.
- [22] D. Helm, J. F. Voloch, *Finite descent obstruction on curves and modularity*, Bull. LMS, **43** (2011) 805-810.
- [23] E. Howe, *Kernels of polarizations of abelian varieties over finite fields*. J. Algebraic Geom. **5** (1996), no. 3, 583–608.

- [24] 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.
- [25] U. Jannsen, *Motives, numerical equivalence, and semi-simplicity*. Invent. Math. **107** (1992), 447–452.
- [26] S. Lang, *Abelian Varieties*, 2nd edition. Springer-Verlag, New York Berlin Heidelberg Tokyo, 1983.
- [27] D. Lorenzini, *An invitation to Arithmetic Geometry*. Graduate Studies in Mathematics **9**, American Mathematical Society, Providence, RI, 1996.
- [28] M. Matsumoto, A. Tamagawa, *Mapping-class-group action versus Galois action on profinite fundamental groups*. Amer. J. Math. **122** (2000), 1017–1026.
- [29] 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/> .
- [30] J. L. Mennicke, *Finite factor groups of the unimodular group*. Ann. of Math. **81** (1965), 31–37.
- [31] S. Mochizuki, *The profinite Grothendieck conjecture for closed hyperbolic curves over number fields*. J. Math. Sci. Univ. Tokyo **3** (1996), no. 3, 571–627.
- [32] S. Mochizuki, *Topics surrounding the anabelian geometry of hyperbolic curves*. in *Galois groups and fundamental groups*, Math. Sci. Res. Inst. Publ., vol 41, Cambridge Univ. Press, Cambridge, 2003. pp 119–165.
- [33] Y. Morita, *On potential good reduction of abelian varieties* J. Fac. Sci. Univ. Tokyo Sect. I A Math. **22** (1975) 437–447.
- [34] D. Mumford, *On the Equations Defining Abelian Varieties I, II*. Invent. Math. **1** (1966), 287–384; **3** (1967), 75–135.

- [35] R. Noot, *Abelian varieties - Galois representations and properties of ordinary reduction*. Compositio Math. **97** (1995), 161–171.
- [36] 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).
- [37] F. Oort, *Lifting algebraic curves, and their endomorphisms to characteristic zero*. In: Proc. Symp. Pure Math. **46** (1987), 165–195.
- [38] F. Oort, *CM-liftings of abelian varieties*. J. Algebraic Geometry **1** (1992), 131–146.
- [39] F. Oort, Yu.G. Zarhin, *Endomorphism Algebras of Complex Tori*. Math. Ann. **303** (1995), 11–29.
- [40] A. Pál, *The real section conjecture and Smith’s fixed point theorem for pro-spaces* J. Lond. Math. Soc. **83** (2011) 353–367.
- [41] S. T. Patrikis, *Variations on a theorem of Tate*, ArXiv e-prints 1207.6724v4 (2012).
- [42] K.A. Ribet, *Galois Action on Division Points of Abelian Varieties with Real Multiplications*. Amer. J. Math. **98** (1976), 751–804.
- [43] J.-P. Serre, *Abelian  $\ell$ -adic representations and elliptic curves*, 2nd edition. Addison-Wesley Publishing Company, Redwood, CA, 1989.
- [44] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*. J. Pure Applied Algebra **77** (1992) 253–262.
- [45] A. Silverberg, Yu. G. Zarhin, *Semistable reduction and torsion subgroups of abelian varieties*, Ann. Inst. Fourier **45** (1995) 403–420.
- [46] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*. Ann. Math. **78** (1963), 149–192.
- [47] A. Skorobogatov, *Torsors and rational points*, Cambridge University Press, Cambridge 2001.
- [48] J. Stix, *Rational Points and Arithmetic of Fundamental Groups*, Lecture Notes in Mathematics **2054**, Springer-Verlag, Berlin, Heidelberg 2013.

- [49] M. Stoll, *Finite descent and rational points on curves*, Algebra and Number Theory **2** (2008), no 5, 595–611.
- [50] J. Tate, *Conjectures on algebraic cycles in  $\ell$ -adic cohomology*. Proc. Sympos. Pure Math. **55:1** Amer. Math. Soc., Providence, RI (1994) 71-83.
- [51] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.
- [52] 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.
- [53] J. F. Voloch, *Finite descent obstruction for curves over function fields*, Bol. Soc. Brasil. Math. **43** (2012), 1-6.
- [54] Yu. G. Zarhin, *Eigenvalues of Frobenius endomorphisms of abelian varieties of low dimension*. J. Pure Applied Algebra **219** (2015), 2076–2098.
- [55] 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.
- [56] 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.
- [57] 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 and

School of Mathematics and Statistics, University of Canterbury,

Private Bag 4800, Christchurch 8140, New Zealand

e-mail: voloch@math.utexas.edu

Department of Mathematics, Pennsylvania State University,

University Park, PA 16802, USA

e-mail: zarhin@math.psu.edu