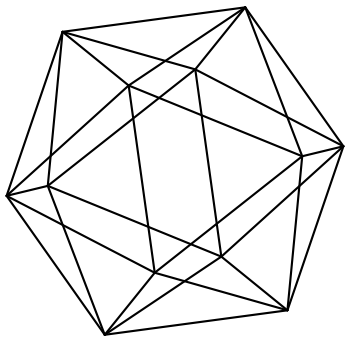
Max-Planck-Institut für Mathematik
Bonn

On uniformity conjectures for abelian varieties and K3 surfaces

by

Martin Orr
Alexei N. Skorobogatov
Yuri G. Zarhin



Max-Planck-Institut für Mathematik
Preprint Series 2018 (52)

On uniformity conjectures for abelian varieties and K3 surfaces

Martin Orr
Alexei N. Skorobogatov
Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Mathematics Institute
University of Warwick
Coventry CV4 7AL
U.K.

Department of Mathematics
South Kensington Campus
Imperial College London
London SW7 2BZ
U.K.

Institute for Information Transmission Problems
Russian Academy of Sciences
19 Bolshoi Karetnyi
Moscow 127994
Russia

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

MPIM 18-52

On uniformity conjectures for abelian varieties and K3 surfaces

Martin Orr, Alexei N. Skorobogatov and Yuri G. Zarhin

Abstract

We discuss logical links among uniformity conjectures concerning K3 surfaces and abelian varieties of bounded dimension defined over number fields of bounded degree. The conjectures concern the endomorphism algebra of an abelian variety, the Néron–Severi lattice of a K3 surface, and the Galois invariant subgroup of the geometric Brauer group.

Contents

[0]The first and second named authors have been supported by the EPSRC grant EP/M020266/1. The third named author is partially supported by Simons Foundation Collaboration grant # 585711. The second and third named authors would like to thank the Max Planck Institut für Mathematik in Bonn for hospitality and support. We are grateful to the organisers of the workshop "Arithmetic of curves" at Baskerville Hall for excellent working conditions that enabled us to complete this project.

1 Introduction

The aim of this paper is to explore logical links among several conjectures about K3 surfaces and abelian varieties defined over number fields. These conjectures state that certain invariants take only finitely many values provided the degree of the field of definition and the dimension (in the case of abelian varieties) are bounded.

Let k be a number field with algebraic closure $\bar{k}$ and let $\Gamma = \mathrm{Gal}(\bar{k}/k)$. For a variety X over k we write $\overline{X} = X \times_k \bar{k}$.

Coleman's conjecture about $\mathrm{End}(\overline{A})$**.** *There are only finitely many rings R, up to isomorphism, for which there exists an abelian variety A of bounded dimension defined over a number field of bounded degree such that* $\mathrm{End}(\overline{A}) \cong R$.

This or a closely related conjecture is attributed to Robert Coleman in [Sha96, Remark 4], see also Conjecture C(e, g) in [BFGR06, p. 384]. There is a version of this conjecture in which $\mathrm{End}(\overline{A})$ is replaced by the ring $\mathrm{End}(A)$ of endomorphisms of A defined over k. It is not too hard to show that Coleman's conjecture about $\mathrm{End}(\overline{A})$ is equivalent to Coleman's conjecture about $\mathrm{End}(A)$, see Theorem 3.4.

In his recent paper Rémond proved that Coleman's conjecture implies the uniform boundedness of torsion $A(k)_{\mathrm{tors}}$ and of the minimal degree of an isogeny between isogenous abelian varieties, see [Rem18, Thm. 1.1]. In this paper we would like to point out several other consequences of Coleman's conjecture.

Shafarevich's conjecture about $\mathrm{NS}\,(\overline{X})$**.** *There are only finitely many lattices L, up to isomorphism, for which there exists a K3 surface X defined over a number field of bounded degree such that* $\mathrm{NS}\,(\overline{X}) \cong L$.

It is in this form that Shafarevich has stated his conjecture in [Sha96]. Since there are only finitely many lattices of bounded rank and discriminant [Cas78, Ch. 9, Thm. 1.1], Shafarevich's conjecture is equivalent to the boundedness of the discriminant of $\mathrm{NS}\,(\overline{X})$. One can also state a variant of Shafarevich's conjecture in which $\mathrm{NS}\,(\overline{X})$ is replaced by its Galois-invariant subgroup $\mathrm{NS}\,(\overline{X})^{\Gamma}$, or, alternatively, by $\mathrm{Pic}(X)$. In Theorem 3.5 we show that all these versions of Shafarevich's conjecture are equivalent.

We denote by $\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$ the (cohomological) Brauer group of a scheme X. When X is a variety over a field k, we use the standard notation $\mathrm{Br}_0(X)$ for the image of the canonical map $\mathrm{Br}(k) \to \mathrm{Br}(X)$. Assume that k is finitely generated over $\mathbb{Q}$, for example, k is a number field. The geometric Brauer group $\mathrm{Br}(\overline{X})$ has a natural structure of a Γ-module. By the main result of [SZ08], if X is an abelian variety or a K3 surface over k, then $\mathrm{Br}(\overline{X})^{\Gamma}$ is finite.

Várilly-Alvarado's conjecture. [VA17, Conj. 4.6] *Let L be a primitive sublattice of the K3 lattice $E_8(-1)^{\oplus 2} \oplus U^{\oplus 3}$. If X is a K3 surface defined over a number field of bounded degree such that* $\mathrm{NS}\,(\overline{X}) \cong L$*, then the cardinality of* $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ *is bounded.*

A stronger form of this conjecture omits the reference to the Néron–Severi lattice. It concerns the uniform boundedness of the Galois invariant subgroup of the geometric Brauer group.

Conjecture Br(K3). *If X is a K3 surface defined over a number field of bounded degree, then the cardinality of* $\mathrm{Br}(\overline{X})^{\Gamma}$ *is bounded.*

A similar conjecture can be stated for abelian varieties of given dimension.

Conjecture Br(AV). *If A is an abelian variety of bounded dimension defined over a number field of bounded degree, then the cardinality of* $\mathrm{Br}(\overline{A})^{\Gamma}$ *is bounded.*

All of the aforementioned conjectures hold for abelian varieties and K3 surfaces with complex multiplication [OS18].

Similarly to Shafarevich's conjecture, Coleman's conjecture can be restated in terms of lattices. Recall that $\mathrm{End}(A)$ is an order in the semisimple $\mathbb{Q}$-algebra $\mathrm{End}(A)_{\mathbb{Q}} = \mathrm{End}(A) \otimes \mathbb{Q}$. Let us define $\mathrm{discr}(A)$ as the discriminant of the integral symmetric bilinear form $\mathrm{tr}(xy)$ on $\mathrm{End}(A)$, where $\mathrm{tr} : \mathrm{End}(A)_{\mathbb{Q}} \to \mathbb{Q}$ is the reduced trace. An equivalent form of Coleman's conjecture says that $\mathrm{discr}(A)$ is uniformly bounded for abelian varieties A of bounded dimension defined over number fields of bounded degree. Thus all of the above conjectures state that a certain integer attached to an abelian variety or a K3 surface is uniformly bounded.

The main results of this paper are summarised in the following diagram:

$$\left.\begin{array}{ccc} \text{Coleman's conjecture} & \Longrightarrow & \text{Shafarevich's conjecture} \\ \Downarrow & & \\ \mathrm{Br(AV)} & \Longrightarrow & \text{Várilly-Alvarado's conjecture} \end{array}\right\} \Longrightarrow \mathrm{Br(K3)}$$

Here is an outline of the paper. After discussing some preliminary results in Section 2, we establish the equivalence of various forms of Coleman's conjecture and also those of Shafarevich's conjecture in Section 3.

Section 4 is devoted to proving that Coleman's conjecture implies Br(AV). We give two different proofs that uniformly large primes do not divide $|\mathrm{Br}(\overline{A})^{\Gamma}|$. In Section 4.1 we give a shorter proof based on the aforementioned result of Rémond [Rem18, Thm. 1.1] and the methods of [Zar77, Zar85]. In Section 4.2 we give a proof that does not use [Rem18, Thm. 1.1]; this approach has the advantage of being more general as it applies also to finitely generated fields. Here the key role is played by the image $\Lambda_\ell(A)$ of the ℓ-adic group algebra of the Galois group in the endomorphism ring of the ℓ-adic Tate module $T_\ell(A)$. A crucial observation (Theorem 4.6) is that a matrix algebra over the opposite algebra of $\Lambda_\ell(A)$ is isomorphic to $\mathrm{End}(B) \otimes \mathbb{Z}_\ell$, where B is an abelian variety isogenous to an abelian subvariety of a bounded power of A. Hence $\mathrm{discr}(\Lambda_\ell(A))$ divides $\mathrm{discr}(B)$, so under Coleman's conjecture we obtain an upper bound for $\mathrm{discr}(\Lambda_\ell(A))$. The relevance of this to Br(AV) is that a prime $\ell > 4\dim(A)$ dividing $|\mathrm{Br}(\overline{A})^{\Gamma}|$ must also divide $\mathrm{discr}(\Lambda_\ell(A \times A^\vee))$, where $A^\vee$ is the

dual abelian variety of A. To complete the proof that Coleman's conjecture implies Br(AV) one needs to show the uniform boundedness of the ℓ-primary torsion of $\mathrm{Br}(\overline{A})^\Gamma$ for a fixed ℓ; this proof can be found in Section 4.3. In Section 4.4, we prove some partial converses to Theorem 4.1: bounds for Brauer groups of abelian varieties imply information about their endomorphisms.

In Section 5 we use the K3 surfaces version of Zarhin's trick from [OS18] to produce a uniform Kuga–Satake construction that does not depend on the degree of polarisation. The Hodge-theoretic aspect of this construction allows us to show that Coleman's conjecture implies Shafarevich's conjecture. In Section 6 we use the compatibility with Galois action to prove that Br(AV) implies Várilly–Alvarado's conjecture. By the finiteness of the isomorphism classes of lattices of the same rank and discriminant, it is clear that the conjectures of Shafarevich and Várilly–Alvarado together imply Conjecture Br(K3).

2 Preliminaries

2.1 Lattices

In this paper we refer to a free abelian group L of finite positive rank with a non-degenerate integral symmetric bilinear form $(x.y)$ as a *lattice*. Write $L^* = \mathrm{Hom}(L, \mathbb{Z})$ and $L_{\mathbb{Q}} = L \otimes_{\mathbb{Z}} \mathbb{Q}$. The *discriminant group* of a lattice L is defined as the cokernel of the map $L \to L^*$ sending $x \in L$ to the linear form $(x.y)$. The *discriminant* $\mathrm{discr}(L)$ of L is the determinant of the matrix $(e_i.e_j)$, where $e_1, \ldots, e_n$ is a $\mathbb{Z}$-basis of L. This is independent of the choice of basis $e_1, \ldots, e_n$. We have $|\mathrm{discr}(L)| = |L^*/L|$.

Let ℓ be a prime. We define the *discriminant* $\mathrm{discr}(L)$ of a free $\mathbb{Z}_\ell$-module L of finite positive rank equipped with a symmetric $\mathbb{Z}_\ell$-valued bilinear form in the same way. However, in this case there is an ambiguity coming from the choice of $\mathbb{Z}_\ell$-basis for L: $\mathrm{discr}(L)$ is well-defined up to multiplication by a square in $\mathbb{Z}_\ell^\times$. In practice, every use we make of the discriminant of a $\mathbb{Z}_\ell$-module L will only depend on the ℓ-adic valuation of $\mathrm{discr}(L)$, which is well-defined.

Lemma 2.1 *Let L be a lattice with discriminant d. Let G be a finite group that acts on L preserving the bilinear form $(x.y)$. If $L^G \neq 0$, then the restriction of $(x.y)$ makes L^G a lattice of discriminant dividing $(d|G|)^r$, where $r = \mathrm{rk}(L^G)$.*

Proof. The G-module $L_{\mathbb{Q}}$ is semisimple, hence is a direct sum of G-modules $L_{\mathbb{Q}}^G \oplus V$, where V is a vector space over $\mathbb{Q}$ such that $V^G = 0$. If $x \in L_{\mathbb{Q}}^G$ and $y \in V$, then $(x.y) = (x.gy)$ for any $g \in G$. Since $\sum_{g \in G} gy \in V^G = 0$, we have $(x.y) = 0$. Thus $L_{\mathbb{Q}} = L_{\mathbb{Q}}^G \oplus V$ is an orthogonal direct sum. It follows that the discriminant of the restriction of the bilinear form on L to L^G is non-zero, so L^G is indeed a lattice. It is clear that the finite abelian group $(L^G)^*/L^G$ is generated by at most r elements. Thus it is enough to show that $(L^G)^*/L^G$ is annihilated by $d|G|$.

The map $L^G \to (L^G)^*$ is the composition of the natural maps

$$L^G \hookrightarrow L \longrightarrow L^* \longrightarrow (L^G)^*.$$

Since L^G is a primitive sublattice of L, the last map here is surjective. Thus any $a \in (L^G)^*$ is in the image of L^*, hence da is in the image of L. Since $|G|a = \sum_{g\in G} ga$, we see that $(d|G|)a$ is in the image of L^G. $\square$

Lemma 2.2 *Let ℓ be a prime. Let M be a free $\mathbb{Z}_\ell$-module of finite positive rank equipped with a symmetric $\mathbb{Z}_\ell$-valued bilinear form $(x.y)$. Let Γ be a group that acts on M preserving the form $(x.y)$. If $L \subset M$ is a $\mathbb{Z}_\ell[\Gamma]$-submodule such that the restriction of $(x.y)$ to L has discriminant $d \neq 0$, then $d \cdot (M/L)^\Gamma$ belongs to the image of the natural map $M^\Gamma \to (M/L)^\Gamma$.*

For any positive integer n the image of the natural map $(M/\ell^n)^\Gamma \to ((M/L)/\ell^n)^\Gamma$ contains $d \cdot ((M/L)/\ell^n)^\Gamma$.

Proof. Let $L^\perp \subset M$ be the orthogonal complement to L with respect to $(x.y)$. We have $L \cap L^\perp = 0$ because $d \neq 0$. Hence the natural map $L \oplus L^\perp \to M$ is injective.

Let $x \in M$. For $y \in L$ the map $y \mapsto (x.y)$ is an element of $\mathrm{Hom}_{\mathbb{Z}_\ell}(L, \mathbb{Z}_\ell)$. Thus we get a map of $\mathbb{Z}_\ell$-modules $M \to \mathrm{Hom}_{\mathbb{Z}_\ell}(L, \mathbb{Z}_\ell)$. Since $d \neq 0$, the restriction of this map to L is injective and has cokernel annihilated by d. Hence there is a $z \in L$ such that $d(x.y) = (z.y)$ for all $y \in L$. Thus $dx - z \in L^\perp$, proving that $dM \subset L \oplus L^\perp$. We summarise this in the following commutative diagram:

$$\begin{array}{ccccc} dM & \hookrightarrow & L \oplus L^\perp & \hookrightarrow & M \\ \downarrow & & \downarrow & & \downarrow \\ d(M/L) & \hookrightarrow & L^\perp & \hookrightarrow & M/L \end{array}$$

The group Γ preserves L and $(x.y)$, hence Γ also preserves $L^\perp$; thus all the arrows in the diagram are maps of Γ-modules. Since the homomorphism $L \oplus L^\perp \to L^\perp$ has a section, the first claim of the lemma follows.

For $n \geq 1$ we obtain a commutative diagram of $\mathbb{Z}_\ell[\Gamma]$-modules

$$\begin{array}{ccccc} dM/\ell^n & \longrightarrow & L/\ell^n \oplus L^\perp/\ell^n & \longrightarrow & M/\ell^n \\ \downarrow & & \downarrow & & \downarrow \\ d(M/L)/\ell^n & \longrightarrow & L^\perp/\ell^n & \longrightarrow & (M/L)/\ell^n \end{array} \tag{1}$$

If $\alpha \in ((M/L)/\ell^n)^\Gamma$, then $d\alpha$ comes from $(L^\perp/\ell^n)^\Gamma$. Similarly to the previous case, the map $L^\perp/\ell^n \to (M/L)/\ell^n$ factors through $M/\ell^n \to (M/L)/\ell^n$. This proves the lemma. $\square$

Let ℓ be a prime and let N be a free $\mathbb{Z}_\ell$-module of finite positive rank. The free $\mathbb{Z}_\ell$-module $\mathrm{End}_{\mathbb{Z}_\ell}(N)$ has a symmetric $\mathbb{Z}_\ell$-valued bilinear form $\mathrm{Tr}(xy)$, where Tr is the usual matrix trace.

Let $\Lambda \subset \mathrm{End}_{\mathbb{Z}_\ell}(N)$ be a $\mathbb{Z}_\ell$-subalgebra. We write $\mathrm{End}_\Lambda(N)$ for the centraliser of Λ in $\mathrm{End}_{\mathbb{Z}_\ell}(N)$, that is, the set of $x \in \mathrm{End}_{\mathbb{Z}_\ell}(N)$ such that $x\lambda = \lambda x$ for all $\lambda \in \Lambda$.

Lemma 2.3 *If the restriction of the bilinear form* $\mathrm{Tr}(xy)$ *to* $\mathrm{End}_\Lambda(N)$ *has discriminant* $d \neq 0$*, then there is an integer* $r \geq 0$ *such that for all* $n \geq 1$ *we have*

$$\ell^r \cdot \mathrm{End}_\Lambda(N/\ell^n) \subset \mathrm{End}_\Lambda(N)/\ell^n \subset \mathrm{End}_\Lambda(N/\ell^n).$$

Proof. Write $M = \mathrm{End}_{\mathbb{Z}_\ell}(N)$, $L = \mathrm{End}_\Lambda(N)$, and let $L^\perp$ be the orthogonal complement to L in M. Since $d \neq 0$ we have $L \cap L^\perp = 0$. In particular, the only element of $L^\perp$ commuting with Λ is 0.

It is clear that L and $L^\perp$ are saturated, free $\mathbb{Z}_\ell$-submodules of M. Thus for all $n \geq 1$ we have $L/\ell^n \subset M/\ell^n$ and $L^\perp/\ell^n \subset M/\ell^n$. Let ℓ^a be the highest power of ℓ dividing d in $\mathbb{Z}_\ell$. We are in the situation of Lemma 2.2, so we have commutative diagram (1). The first row of (1) implies

$$\ell^a \cdot (M/\ell^n) \subset L/\ell^n + L^\perp/\ell^n \subset M/\ell^n.$$

By retaining only the elements commuting with Λ we obtain

$$\ell^a \cdot \mathrm{End}_\Lambda(N/\ell^n) \subset \mathrm{End}_\Lambda(N)/\ell^n + (L^\perp/\ell^n) \cap \mathrm{End}_\Lambda(N/\ell^n) \subset \mathrm{End}_\Lambda(N/\ell^n). \qquad (2)$$

We claim that there exists a positive integer b such that for all $n > b$ we have

$$(L^\perp/\ell^n) \cap \mathrm{End}_\Lambda(N/\ell^n) \subset \ell \cdot (L^\perp/\ell^n). \qquad (3)$$

Indeed, let S_n be the subset of the left hand side consisting of the elements that are not contained in $\ell \cdot (L^\perp/\ell^n)$. Reduction mod ℓ^n maps S_{n+1} to S_{n-1} for each $n \geq 1$. If all the finite sets S_n are non-empty, then $\varprojlim S_n \neq \emptyset$. Any $x \in \varprojlim S_n$ is an element of $L^\perp \setminus \ell L^\perp$, hence $x \neq 0$. But $x \in \mathrm{End}_\Lambda(N) = L$, contradicting $L \cap L^\perp = 0$.

From (3), in view of a canonical isomorphism $\ell \cdot (L^\perp/\ell^n) \xrightarrow{\sim} L^\perp/\ell^{n-1}$, for each $n > b$ we obtain an injection

$$(L^\perp/\ell^n) \cap \mathrm{End}_\Lambda(N/\ell^n) \hookrightarrow (L^\perp/\ell^{n-1}) \cap \mathrm{End}_\Lambda(N/\ell^{n-1}). \qquad (4)$$

This implies

$$\ell^b \cdot ((L^\perp/\ell^n) \cap \mathrm{End}_\Lambda(N/\ell^n)) = 0, \qquad n \geq 1. \qquad (5)$$

Combining (2) with (5) proves the lemma with $r = a + b$. $\square$

2.2 Algebras

Let B be a separable semisimple algebra over a field k. Then B is the product of matrix algebras $B_i = \mathrm{Mat}_{r_i}(D_i)$, where D_i is a division k-algebra, for $i = 1, \ldots, m$. Let K_i be the centre of D_i and let $d_i^2 = \dim_{K_i}(D_i)$. Here K_i is a finite separable field extension of k. We call the *intrinsic trace* of $x \in B$ the trace $\mathrm{Tr}_B(x)$ of the linear transformation of B defined by the left multiplication by x. Write $x = x_1 + \ldots + x_m$, where $x_i \in B_i$. The *relative reduced trace* $\mathrm{tr}_{B/k} : B \to k$ is defined as the sum of compositions of the usual reduced trace $\mathrm{tr}_{B_i/K_i} : B_i \to K_i$ of the central simple K_i-algebra B_i with the trace of the finite separable field extension $\mathrm{Tr}_{K_i/k} : K_i \to k$, for $i = 1, \ldots, m$, see [Rei03, Def. 9.13]. Thus

$$\mathrm{tr}_{B/k}(x) = \sum_{i=1}^{m} \mathrm{tr}_{B_i/k}(x_i) = \sum_{i=1}^{m} \mathrm{Tr}_{K_i/k}\mathrm{tr}_{B_i/K_i}(x_i).$$

These two natural notions of trace are related as follows, see [Rei03], formula (9.22):

$$\mathrm{Tr}_B(x) = \sum_{i=1}^{m} d_i r_i \, \mathrm{tr}_{B_i/k}(x_i). \tag{6}$$

The two notions of trace give rise to two symmetric bilinear forms on B with values in k:

(1) The form $\mathrm{tr}_{B/k}(xy)$. This form is non-degenerate, see [Rei03, Thm. 9.26].

(2) The *intrinsic* bilinear form $\mathrm{Tr}_B(xy)$.

Now let $k = \mathbb{Q}$. Let Λ be an order in the semisimple $\mathbb{Q}$-algebra B. In other words, Λ is a subring of B such that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q} = B$. The restriction of $\mathrm{tr}_{B/\mathbb{Q}}$ to Λ takes values in $\mathbb{Z}$ (see [Rei03, Thm. 10.1]), so the bilinear form $\mathrm{tr}_{B/\mathbb{Q}}(xy)$ is integral on Λ. We define the discriminant $\mathrm{discr}(\Lambda)$ to be the discriminant of the lattice Λ, equipped with this bilinear form.

If $k = \mathbb{Q}_\ell$, we similarly define the discriminant of an order in a semisimple $\mathbb{Q}_\ell$-algebra (well-defined up to multiplication by a square in $\mathbb{Z}_\ell^\times$).

The following two statements are undoubtedly well known. For example, the implication "$\ell \nmid \mathrm{discr}(\Lambda) \Rightarrow \Lambda/\ell$ is semisimple" of Corollary 2.5 is essentially [MW95, Lemma 2.3] (except that in [MW95], the discriminant is defined using the intrinsic trace Tr_B, while we use the reduced trace $\mathrm{tr}_{B/\mathbb{Q}}$). Nevertheless we give a detailed proof as we could not find the full statement of this proposition in the literature.

Proposition 2.4 *Let ℓ be a prime and let Λ be an order in a semisimple $\mathbb{Q}_\ell$-algebra. Then the following conditions are equivalent.*

(i) *ℓ does not divide* $\mathrm{discr}(\Lambda)$.

(ii) *for some positive integers $n_1, \ldots, n_r$ we have $\Lambda \cong \oplus_{i=1}^{r} \mathrm{Mat}_{n_i}(O_{k_i})$, where O_{k_i} is the ring of integers of an unramified finite field extension $k_i/\mathbb{Q}_\ell$ for $i = 1, \ldots, r$.*

(iii) *the $\mathbb{F}_\ell$-algebra Λ/ℓ is semisimple.*

Proof. By assumption Λ is an order in the semisimple $\mathbb{Q}_\ell$-algebra $B = \Lambda \otimes \mathbb{Q}_\ell$.

Let us first assume that this order is maximal. Any maximal order $M \subset B$ is a direct sum of maximal orders of the simple components of B, see [Rei03, Thm. 10.5 (i)]. This direct sum is an orthogonal direct sum for the bilinear form $\mathrm{tr}_{B/\mathbb{Q}_\ell}(xy)$, so it is enough to consider a maximal order $M \subset \mathrm{Mat}_r(D)$, where D is a division $\mathbb{Q}_\ell$-algebra. By [Rei03, Thm. 12.8] there is a unique maximal order $O \subset D$; it is the integral closure of $\mathbb{Z}_\ell$ in D. By [Rei03, Thm. 17.3] any maximal order in $\mathrm{Mat}_r(D)$ is conjugate to $\mathrm{Mat}_r(O)$ by an element of $\mathrm{GL}_r(D)$, so we have an isomorphism of rings $M \cong \mathrm{Mat}_r(O)$. From this we get an $\mathbb{F}_\ell$-algebra isomorphism $M/\ell \cong \mathrm{Mat}_r(O/\ell)$.

It is well known that $\mathrm{rad}(O/\ell) = 0$ if and only if D is an unramified *field* extension of $\mathbb{Q}_\ell$. Then O/ℓ is a field extension of $\mathbb{F}_\ell$, hence $\mathrm{Mat}_r(O/\ell)$ is a semisimple $\mathbb{F}_\ell$-algebra. This shows the equivalence of (ii) and (iii).

If K is the centre of D, and R is the integral closure of $\mathbb{Z}_\ell$ in K, then we have (cf. Exercise 1 on p. 223 of [Rei03])

$$\mathrm{discr}(\mathrm{Mat}_r(O)) = \mathrm{N}_{K/\mathbb{Q}_\ell}(\mathrm{discr}(\mathrm{Mat}_r(O)/R)) \cdot \mathrm{discr}(R/\mathbb{Z}_\ell)^{r^2 \dim_K(D)}. \qquad (7)$$

This element of $\mathbb{Z}_\ell$ is not divisible by ℓ if and only if $D = K$ is an unramified field extension of $\mathbb{Q}_\ell$, see [Rei03, Cor. 25.10]. This proves the equivalence of (i) and (ii).

Now suppose that Λ is not a maximal order. Let us show that in this case each of (i), (ii), (iii) is false. By [Rei03, Cor. 10.4] there is a maximal order $M \subset B$ that contains Λ. Since the index $[M : \Lambda]$ equals ℓ^a for an integer $a \geq 1$ and $\mathrm{discr}(\Lambda) = [M : \Lambda]^2 \,\mathrm{discr}(M)$, we see that ℓ divides $\mathrm{discr}(\Lambda)$, so (i) does not hold.

To show that (iii) does not hold we need to show that $\mathrm{rad}(\Lambda/\ell) \neq 0$, for which it is enough to exhibit a non-zero two-sided nilpotent ideal in Λ/ℓ. Let $N = \Lambda \cap \ell M$. This is a two-sided ideal in Λ, hence $N/\ell\Lambda$ is a two-sided ideal in Λ/ℓ. By Nakayama's lemma we have $M/(\Lambda + \ell M) \neq 0$. Since $\dim_{\mathbb{F}_\ell}(M/\ell) = \dim_{\mathbb{F}_\ell}(\Lambda/\ell)$, the cardinalities of the kernel and the cokernel of the natural homomorphism $\Lambda/\ell \to M/\ell$ are equal, so $N/\ell\Lambda \neq 0$. This ideal of Λ/ℓ is nilpotent. Indeed, take any $x \in N/\ell\Lambda$ and lift it to $\tilde{x} \in N \subset \ell M$. Then $\tilde{x}^{a+1} \in \ell^{a+1} M \subset \ell\Lambda$, hence $x^{a+1} = 0$.

This also implies that (ii) does not hold. Indeed, otherwise Λ/ℓ would be a semisimple $\mathbb{F}_\ell$-algebra, which it is not. □

Corollary 2.5 *Let Λ be an order in a semisimple $\mathbb{Q}$-algebra. A prime ℓ does not divide* $\mathrm{discr}(\Lambda)$ *if and only if the $\mathbb{F}_\ell$-algebra Λ/ℓ is semisimple.*

Proof. Apply Proposition 2.4 to the order $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ in the semisimple $\mathbb{Q}_\ell$-algebra $\Lambda \otimes \mathbb{Q}_\ell$. □

2.3 Abelian varieties

Let k be a field with a separable closure $\bar{k}$ and Galois group $\Gamma_k = \mathrm{Gal}(\bar{k}/k)$. Let A be an abelian variety over k and let ℓ be a prime different from $\mathrm{char}(k)$. For each

positive integer n the Kummer sequence gives rise to an exact sequence of Γ-modules

$$0 \longrightarrow \mathrm{NS}\,(\overline{A})/\ell^n \xrightarrow{c_1} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \longrightarrow \mathrm{Br}(\overline{A})[\ell^n] \longrightarrow 0 \tag{8}$$

Let $A^\vee$ be the dual abelian variety, and let $e_{\ell^n,A} : A[\ell^n] \times A^\vee[\ell^n] \to \mu_{\ell^n}$ be the Weil pairing. We have canonical isomorphisms of Γ-modules

$$\mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \cong \wedge^2 \mathrm{H}^1_{\text{ét}}(\overline{A}, \mu_{\ell^n})(-1) \cong (\wedge^2 A^\vee[\ell]^n)(-1) \cong \mathrm{Hom}(\wedge^2 A[\ell^n], \mu_{\ell^n}) \tag{9}$$

and an injective map of Γ-modules, cf. [SZ08, Section 3.3]:

$$\mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \cong \mathrm{Hom}(\wedge^2 A[\ell^n], \mu_{\ell^n}) \hookrightarrow \mathrm{Hom}(A[\ell^n], A^\vee[\ell^n]). \tag{10}$$

Here the image consists of those $u : A[\ell^n] \to A^\vee[\ell^n]$ such that $e_{\ell^n,A}(x, ux) = 0$ for all $x \in A[\ell^n]$, that is, the form $e_{\ell^n,A}(x, uy)$ is alternating.

Let $\mathrm{Hom}(A[\ell^n], A^\vee[\ell^n])_{\mathrm{sym}}$ be the subgroup of *symmetric* (or self-dual) homomorphisms $u : A[\ell^n] \to A^\vee[\ell^n]$. It is shown in [SZ08, Remark 3.2] that u in $\mathrm{Hom}(A[\ell^n], A^\vee[\ell^n])$ is symmetric if and only if $e_{\ell^n,A}(x, uy) = -e_{\ell^n,A}(y, ux)$, that is, the form $e_{\ell^n,A}(x, uy)$ is skew-symmetric. All alternating forms are skew-symmetric, so we get an injective map

$$\mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \hookrightarrow \mathrm{Hom}(A[\ell^n], A^\vee[\ell^n])_{\mathrm{sym}}. \tag{11}$$

For $\ell \neq 2$ all skew-symmetric forms are alternating, so that (11) is an isomorphism.

It is well known that $\mathrm{NS}\,(\overline{A})$ is canonically isomorphic to the subgroup of self-dual elements $\mathrm{Hom}(\overline{A}, \overline{A}^\vee)_{\mathrm{sym}} \subset \mathrm{Hom}(\overline{A}, \overline{A}^\vee)$. This allows one to rewrite the cycle map as a map of Γ-modules

$$\mathrm{Hom}(\overline{A}, \overline{A}^\vee)_{\mathrm{sym}}/\ell^n \longrightarrow \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}). \tag{12}$$

Lemma 2.6 *Let k be a field of characteristic 0. The composition of maps* (12) *and* (11) *is the negative of the natural map* $\mathrm{Hom}(\overline{A}, \overline{A}^\vee)_{\mathrm{sym}} \to \mathrm{Hom}(A[\ell^n], A^\vee[\ell^n])_{\mathrm{sym}}$ *given by the action of endomorphisms of $\overline{A}$ on ℓ^n-torsion points.*

Proof. The claim is that the following diagram commutes:

$$\begin{array}{ccccc}
\mathrm{NS}\,(\overline{A})/\ell^n & \xrightarrow{\quad c_1 \quad} & \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) & \xrightarrow{\quad \cong \quad} & \mathrm{Hom}(\wedge^2 A[\ell^n], \mu_{\ell^n}) \\
\downarrow \cong & & & & \downarrow \\
\mathrm{Hom}(\overline{A}, \overline{A}^\vee)_{\mathrm{sym}}/\ell^n & \longrightarrow & \mathrm{Hom}(A[\ell^n], A^\vee[\ell^n])_{\mathrm{sym}} & \xrightarrow{[-1]} & \mathrm{Hom}(A[\ell^n], A^\vee[\ell^n])_{\mathrm{sym}}.
\end{array}$$

The vertical arrow on the left is induced by the map $\mathrm{NS}\,(\overline{A}) \to \mathrm{Hom}(\overline{A}, \overline{A}^\vee)$ that sends $\mathcal{L}$ to $\phi_{\mathcal{L}}$, where $\phi_{\mathcal{L}}$ is the morphism $\overline{A} \to \overline{A}^\vee$ defined in [Mum74, Ch. 6, Cor. 4]. The vertical arrow on the right sends the Weil pairing $e^{\mathcal{L}}_{\ell^n}$, which is defined by

$$e^{\mathcal{L}}_{\ell^n}(x, y) = e_{\ell^n,A}(x, \phi_{\mathcal{L}}(y)),$$

to the restriction of $\phi_{\mathcal{L}}$ to ℓ^n-torsion subgroups. Thus it suffices to prove that going along the top of the diagram sends $\mathcal{L}$ to $-e^{\mathcal{L}}_{\ell^n}$.

For the proof we can assume that k is finitely generated over $\mathbb{Q}$. Choose an embedding $\bar{k} \hookrightarrow \mathbb{C}$ and extend the ground field from $\bar{k}$ to $\mathbb{C}$. Let $A(\mathbb{C}) = V/\Lambda$, where $V \cong \mathbb{C}^g$ is the tangent space to A at 0, and Λ is a lattice in V.

According to the Appell–Humbert theorem [Mum74, p. 20], any line bundle $\mathcal{L}_{\mathbb{C}}$ on $A(\mathbb{C})$ can be written in the form $\mathcal{L}(H, \alpha)$ for some Hermitian form H on V such that $E = \operatorname{Im} H$ takes integer values on $\Lambda \times \Lambda$ (and some additional data α which are not relevant to us here). The first Chern class of $\mathcal{L}$ is given by $E \in \operatorname{Hom}(\wedge^2\Lambda, \mathbb{Z}) \cong \mathrm{H}^2(A(\mathbb{C}), \mathbb{Z})$. Thus the top line of the above diagram takes $\mathcal{L}$ mod ℓ^n to $\exp(2\pi i \ell^n E) \in \operatorname{Hom}(\wedge^2(\ell^{-n}\Lambda/\Lambda), \mu_{\ell^n})$.

As explained on [Mum74, Ch. 24, p. 237], if $x, y \in A(\mathbb{C})[\ell^n]$ lift to $\tilde{x}, \tilde{y} \in \ell^{-n}\Lambda$, then

$$\exp(-2\pi i \ell^n E(\tilde{x}, \tilde{y})) = e^{\mathcal{L}}_{\ell^n}(x, y).$$

This completes the proof. □

For any abelian variety A, let E_A and H_A be the Γ-modules which make the following sequences exact:

$$0 \longrightarrow \operatorname{End}(\overline{A} \times \overline{A}^{\vee}) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{End}_{\mathbb{Z}_\ell}(T_\ell(A) \oplus T_\ell(A^{\vee})) \longrightarrow E_A \longrightarrow 0, \tag{13}$$

$$0 \longrightarrow \operatorname{Hom}(\overline{A}, \overline{A}^{\vee}) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{Hom}(T_\ell(A), T_\ell(A^{\vee})) \longrightarrow H_A \longrightarrow 0. \tag{14}$$

Note that the exact sequence (14) is a direct summand of (13).

Using (8), (10) and Lemma 2.6, we have a commutative diagram of Γ-modules with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{NS}\,(\overline{A})/\ell^n & \longrightarrow & \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) & \longrightarrow & \operatorname{Br}(\overline{A})[\ell^n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \operatorname{Hom}(\overline{A}, \overline{A}^{\vee})/\ell^n & \xrightarrow{[-1]} & \operatorname{Hom}(A[\ell^n], A^{\vee}[\ell^n]) & \longrightarrow & H_A/\ell^n & \longrightarrow & 0 \end{array} \tag{15}$$

Lemma 2.7 *Let k be a field of characteristic 0. The kernel of the homomorphism $\operatorname{Br}(\overline{A})[\ell^n] \to H_A/\ell^n$ at the right of (15) has exponent dividing 2.*

Proof. Let C_1 and C_2 denote the cokernels of the left and central vertical arrows of (15) respectively. Since the central vertical arrow is injective, the snake lemma implies that $\ker(\operatorname{Br}(\overline{A})[\ell^n] \to H_A/\ell^n)$ injects into $\ker(C_1 \to C_2)$.

If $\rho \in \operatorname{Hom}(\overline{A}, \overline{A}^{\vee})/\ell^n$ maps to 0 in C_2, then the image of ρ in $\operatorname{Hom}(A[\ell^n], A^{\vee}[\ell^n])$ lies in the image of $\mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})$ and hence is in $\operatorname{Hom}(A[\ell^n], A^{\vee}[\ell^n])_{\mathrm{sym}}$ by (11). Choose any $\tilde{\rho} \in \operatorname{Hom}(\overline{A}, \overline{A}^{\vee})$ lifting ρ. Then $\tilde{\rho} + \tilde{\rho}^{\vee}$ is a symmetric lift of 2ρ. Since $\mathrm{NS}\,(\overline{A})/\ell^n \to \operatorname{Hom}(\overline{A}, \overline{A}^{\vee})_{\mathrm{sym}}/\ell^n$ is an isomorphism, we conclude that 2ρ maps to 0 in C_1. This shows that $2 \cdot \ker(C_1 \to C_2) = 0$, which proves the lemma. □

3 Equivalence of variants of conjectures of Coleman and Shafarevich

Let A be an abelian variety of dimension $g \geq 1$ over a field k. Then $\mathrm{End}(A)$ is a free abelian group of positive rank at most equal to $4g^2$; as a ring, it is an order in the finite-dimensional semisimple algebra $\mathrm{End}(A)_{\mathbb{Q}}$, see [Mum74, Ch. 19, Corollaries 1 and 3]. In Section 2 we defined two integral symmetric bilinear forms on any order in $\mathrm{End}(A)_{\mathbb{Q}}$, in particular, on $\mathrm{End}(A)$. The action of $\mathrm{End}(A)$ on A by endomorphisms gives rise to a third bilinear form. To fix notation we review all these forms here.

- The bilinear form $\mathrm{tr}(xy)$ on $\mathrm{End}(A)$, where $\mathrm{tr} : \mathrm{End}(A)_{\mathbb{Q}} \to \mathbb{Q}$ is the *reduced trace*. We call the discriminant of this form $\mathrm{discr}(A)$.

- The *intrinsic* integral symmetric bilinear form on $\mathrm{End}(A)$ is $\mathrm{Tr}_{\mathrm{End}(A)}(xy)$, where $\mathrm{Tr}_{\mathrm{End}(A)}(x)$ is the trace of the linear map $\mathrm{End}(A) \to \mathrm{End}(A)$ sending z to xz. We call the discriminant of this form Δ_A.

- For any $a \in \mathrm{End}(A)$ and $n \in \mathbb{Z}$ the degree of the endomorphism $[n] - a$ of A is a monic polynomial in n with integer coefficients [Mum74, Ch. 19, Thm. 4]. Let $\mathrm{Tr}_A(a) \in \mathbb{Z}$ be the negative of the coefficient of n^{2g-1} in this polynomial. For any prime ℓ not equal to $\mathrm{char}(k)$, we have that $\mathrm{Tr}_A(a)$ is equal to the trace of the $\mathbb{Z}_\ell$-linear transformation of the ℓ-adic Tate module of A defined by a. We call the discriminant of this form δ_A.

Lemma 3.1 *Let g be a positive integer. We have $\Delta_A \neq 0$, $\delta_A \neq 0$. There exist positive real constants c_g and C_g, depending only on g, such that for any abelian variety A of dimension g over a field k we have*

$$c_g \leq |\Delta_A|/|\mathrm{discr}(A)| \leq C_g, \quad c_g \leq |\delta_A|/|\mathrm{discr}(A)| \leq C_g.$$

Proof. If A is a simple abelian variety, then $\mathrm{End}(A)_{\mathbb{Q}}$ is a division algebra over $\mathbb{Q}$. Let K be the centre of $\mathrm{End}(A)_{\mathbb{Q}}$. Write $e = [K : \mathbb{Q}]$ and $d^2 = \dim_K \mathrm{End}(A)_{\mathbb{Q}}$.

Let m be a positive integer. By the proof of [Mum74, Ch. 19, Lemma], any $\Gamma_{\mathbb{Q}}$-invariant linear map $\phi : \mathrm{End}(A^m) \otimes \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ satisfying $\phi(xy) = \phi(yx)$ for all x and y is a rational multiple of the reduced trace. This implies that each of $\mathrm{Tr}_{\mathrm{End}(A^m)}$ and Tr_{A^m} is a non-zero rational multiple of the reduced trace tr on $\mathrm{End}(A^m)_{\mathbb{Q}}$. In particular, each form is non-degenerate. By evaluating at the identity element of $\mathrm{End}(A^m)$ we obtain

$$\frac{\mathrm{Tr}_{\mathrm{End}(A^m)}(x)}{ed^2m^2} = \frac{\mathrm{Tr}_{A^m}(x)}{2gm} = \frac{\mathrm{tr}(x)}{edm}.$$

Since ed divides $2g$ by [Mum74, Ch. 19, Cor., p. 182], we see that each of $\mathrm{Tr}_{\mathrm{End}(A^m)}(x)$ and $\mathrm{Tr}_{A^m}(x)$ is an integral multiple of the reduced trace.

Now let $A_1, \ldots, A_n$ be simple, pairwise non-isogenous abelian varieties over k, of dimension $\dim(A_i) = g_i$. Let $B = \prod_{i=1}^n A_i^{m_i}$ for some positive integers $m_1, \ldots, m_n$. Then $\mathrm{End}(B)$ is the product of rings $\mathrm{End}(A_i^{m_i})$, hence the matrix of each of the three forms on $\mathrm{End}(B)$ is the direct sum of n diagonal blocks. We deduce that

$$\Delta_B = \mathrm{discr}(B) \cdot \prod_{i=1}^n (d_i m_i)^{e_i d_i^2 m_i^2}, \quad \delta_B = \mathrm{discr}(B) \cdot \prod_{i=1}^n \left(\frac{2g_i}{e_i d_i}\right)^{e_i d_i^2 m_i^2}$$

This proves the lemma for B.

Finally, an arbitrary abelian variety A over k is isogenous to some $B = \prod_{i=1}^n A_i^{m_i}$, where $A_1, \ldots, A_n$ are simple and pairwise non-isogenous abelian varieties over k. Then $\mathrm{End}(A)$ and $\mathrm{End}(B)$ are orders in $\mathrm{End}(A)_{\mathbb{Q}} \cong \mathrm{End}(B)_{\mathbb{Q}}$. In each of the three cases, the bilinear forms on $\mathrm{End}(A)_{\mathbb{Q}}$ and $\mathrm{End}(B)_{\mathbb{Q}}$ are compatible under this isomorphism. We have

$$[\mathrm{End}(A) : \mathrm{End}(A) \cap \mathrm{End}(B)]^2 \cdot \mathrm{discr}(A) = [\mathrm{End}(B) : \mathrm{End}(A) \cap \mathrm{End}(B)]^2 \cdot \mathrm{discr}(B).$$

The same formula holds for the discriminants of the two other forms. Hence $\Delta_A/\Delta_B = \delta_A/\delta_B = \mathrm{discr}(A)/\mathrm{discr}(B)$, which proves the statement for A. □

Proposition 3.2 *The following statements are equivalent:*

(i) *Coleman's conjecture about* $\mathrm{End}(A)$*;*

(ii) $\mathrm{discr}(A)$ *is uniformly bounded for all abelian varieties A of bounded dimension defined over a number field of bounded degree;*

(iii) *same as* (ii)*, with* $\mathrm{discr}(A)$ *replaced by* δ_A*;*

(iv) *same as* (ii)*, with* $\mathrm{discr}(A)$ *replaced by* Δ_A*.*

Proof. The equivalence of (ii), (iii) and (iv) was established in Lemma 3.1. It is clear that (i) implies (iv). It remains to show that (ii) implies (i).

The ring $\mathrm{End}(A)$ is an order in the semisimple $\mathbb{Q}$-algebra $\mathrm{End}(A)_{\mathbb{Q}}$, which has dimension at most $4g^2$. Since $\mathrm{discr}(A)$ is bounded, only finitely many semisimple $\mathbb{Q}$-algebras, up to isomorphism, can be realised as $\mathrm{End}(A)_{\mathbb{Q}}$. Indeed, let B be a semisimple $\mathbb{Q}$-algebra, with simple components B_i for $i = 1, \ldots, n$, such that $\dim_{\mathbb{Q}}(B)$ is bounded and B contains an order of bounded discriminant. Then each B_i is a matrix algebra over a division algebra D_i with centre K_i such that $\dim_{\mathbb{Q}}(B_i)$ is bounded. Using Proposition 2.4 and formula (7), we see that the discriminants of the fields K_i are bounded, hence these fields belong to a fixed finite set of number fields. By the same proposition, the division K_i-algebra D_i has bounded rank and ramification, so there are only finitely many isomorphism classes of such algebras.

By the structure theorem for maximal orders over Dedekind domains [Rei03, Thm. 21.6] and the Jordan–Zassenhaus theorem [Rei03, Thm. 26.4], we know that there are only finitely many maximal orders in B, up to conjugation by an element

of $B^\times$, see [Rei03, Section 26, Exercise 8]. Hence there are only finitely many isomorphism classes of maximal orders in B. It follows that there are only finitely many isomorphism classes of orders of bounded discriminant, so only finitely many rings can be realised as $\mathrm{End}(A)$. $\square$

Definition 3.3 *Let p be 0 or a prime number. Define $d_p(g) = |\mathrm{GL}(2g, \mathbb{F}_3)|$ if $p \neq 3$, and $d_p(g) = |\mathrm{GL}(2g, \mathbb{Z}/4)|$ if $p = 3$. Let us write $d(g) = d_0(g)$.*

Theorem 3.4 *Coleman's conjecture about $\mathrm{End}(A)$ is equivalent to Coleman's conjecture about $\mathrm{End}(\overline{A})$.*

Proof. Proposition 3.2 can be applied over the ground field k as well as over $\bar{k}$. Thus to prove the theorem it is enough to show that the uniform boundedness of δ_A is equivalent to the uniform boundedness of $\delta_{\overline{A}}$. It is clear from the definition of Tr_A that for any $a \in \mathrm{End}(A)$ we have $\mathrm{Tr}_A(a) = \mathrm{Tr}_{\overline{A}}(a)$. We note that $\mathrm{End}(A) = \mathrm{End}(\overline{A})^\Gamma$. By a result of Silverberg [Sil92, Thm. 2.4], the cardinality of the image G of Γ in the automorphism group of $\mathrm{End}(\overline{A})$ is bounded by $d(g)$. Thus assuming the boundedness of $\delta_{\overline{A}}$, the boundedness of δ_A follows from Lemma 2.1.

Conversely, let A be an abelian variety of dimension g defined over a number field of degree at most e. By Silverberg's result, the boundedness of $\mathrm{discr}(A)$, where A is considered over a number field of degree at most $e \cdot d(g)$, implies the boundedness of $\mathrm{discr}(\overline{A})$. $\square$

Theorem 3.5 *The following conjectures are equivalent:*

(i) *Shafarevich's conjecture about $\mathrm{NS}(\overline{X})$;*

(ii) *Shafarevich's conjecture about $\mathrm{NS}(\overline{X})^\Gamma$;*

(iii) *Shafarevich's conjecture about $\mathrm{Pic}(X)$.*

Proof. Let $\mathrm{discr}(\mathrm{NS}(\overline{X}))$ be the discriminant of the bilinear form on $\mathrm{NS}(\overline{X})$ given by the intersection pairing. Define $\mathrm{discr}(\mathrm{NS}(\overline{X})^\Gamma)$ and $\mathrm{discr}(\mathrm{Pic}(X))$ similarly. The ground field k being of characteristic 0, the ranks of these lattices do not exceed 20. By [Cas78, Ch. 9, Thm. 1.1], (i) is equivalent to the boundedness of $\mathrm{discr}(\mathrm{NS}(\overline{X}))$ for K3 surfaces defined over number fields of bounded degree, and similarly for (ii) and (iii). It remains to prove the equivalence of these three boundedness conditions.

The boundedness of $\mathrm{discr}(\mathrm{NS}(\overline{X}))$ is equivalent to that of $\mathrm{discr}(\mathrm{NS}(\overline{X})^\Gamma)$ in view of Lemma 2.1 and the classical Minkowski's lemma that gives a bound on the size of finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$ in terms of n. To complete the proof it is enough to show that $\mathrm{Pic}(X)$ is a subgroup of $\mathrm{NS}(\overline{X})^\Gamma$ of bounded index. The spectral sequence $\mathrm{H}^p(k, \mathrm{H}^q(\overline{X}, \mathbb{G}_m)) \Rightarrow \mathrm{H}^{p+q}(X, \mathbb{G}_m)$ gives rise to the well known exact sequence of low degree terms

$$0 \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{Pic}(\overline{X})^\Gamma \longrightarrow \mathrm{Br}(k) \to \mathrm{Br}(X).$$

Every K3 surface has a 0-cycle of degree 24, namely the second Chern class of the tangent bundle. This implies that there are finite field extensions $k_1, \ldots, k_n$ of k such that X has a k_i-point for each i, and g.c.d.$([k_1 : k], \ldots, [k_n : k])$ divides 24. If K is a finite extension of k such that X has a K-point, then the natural map $\mathrm{Br}(K) \to \mathrm{Br}(X_K)$ has a section and so is injective. Now a restriction-corestriction argument shows that the kernel of $\mathrm{Br}(k) \to \mathrm{Br}(X)$ is annihilated by 24. It follows that $\mathrm{Pic}(X)$ is a subgroup of $\mathrm{Pic}(\overline{X})^\Gamma = \mathrm{NS}\,(\overline{X})^\Gamma$ of index dividing 24. $\square$

4 Coleman implies Br(AV)

4.1 Abelian varieties at large primes, I

We now show that Coleman's conjecture implies $\mathrm{Br}(\overline{A})[\ell]^\Gamma = 0$ for abelian varieties A of dimension g defined over a number field of degree d, for all ℓ greater than some constant depending only on d and g.

Theorem 4.1 *Suppose that for all pairs of positive integers (d, g) there is a constant $c = c(d, g)$ such that $|\mathrm{discr}(A)| < c$ for any abelian variety A of dimension g defined over a number field of degree d. Then there is a constant $C = C(d, g)$ such that for any prime $\ell > C$ and any abelian variety A of dimension g defined over a number field of degree d we have the following statements.*

(a) *the $\mathbb{F}_\ell$-algebra $\mathrm{End}(A)/\ell$ is semisimple;*

(b) *the Γ-module $A[\ell]$ is semisimple;*

(c) $\mathrm{End}(A)/\ell = \mathrm{End}(A[\ell])^\Gamma$*;*

(d) $\mathrm{Br}(\overline{A})[\ell]^\Gamma = 0$.

We give two proofs of Theorem 4.1. In this section we prove it via a shortcut provided by a recent theorem of Rémond [Rem18, Thm. 1.1]. In Section 4.2 we prove a slightly stronger statement, which is valid over finitely generated fields of characteristic zero rather than just number fields, without using Rémond's theorem.

Parts (a), (b) and (c) of Theorem 4.1 can be proved by combining results of Masser and Wüstholz [MW95] with [Rem18, Thm. 1.1]. The methods of Masser and Wüstholz are similar to the proof given in this section. See [MW95, Lemma 2.3] for part (a), [MW95, p. 222] for part (b) and [MW95, Lemma 3.2] for part (c).

The result of Rémond is used via the following lemma.

Lemma 4.2 *Suppose that for all pairs of positive integers (d, g) there is a constant $c = c(d, g)$ such that $|\mathrm{discr}(A)| < c$ for any abelian variety A of dimension g defined over a number field of degree d. Then for all pairs of positive integers (d, g) there is a positive integer $r = r(d, g)$ such that for any abelian variety A of dimension g defined over a number field of degree d, for any positive integer n and any Γ-submodule $W \subset A[n]$ there is an isogeny $u : A \to A$ such that $rW \subset uA[n] \subset W$.*

Proof. Let A be an abelian variety over a number field k such that $[k:\mathbb{Q}] = d$ and $\dim(A) = g$. Under our assumptions, by [Rem18, Thm. 1.1] for any abelian variety B defined over k and k-isogenous to A there is a k-isogeny $A \to B$ of degree bounded in terms of d and g. One deduces the existence of a positive integer $r = r(d,g)$ such that, for every pair of isogenous abelian varieties A and B of dimension g defined over a number field k of degree d, $[r] : A \to A$ factors through some k-isogeny $A \to B$. The rest of proof is identical to the proof of [Zar85, Cor. 5.4.1]. $\square$

Proof of Theorem 4.1. (a) For ℓ not dividing $\mathrm{discr}(A)$, the semisimplicity of the $\mathbb{F}_\ell$-algebra $\mathrm{End}(A)/\ell$ follows from Corollary 2.5.

(b) We follow the proof of [Zar85, Cor. 5.4.3]. Assume that ℓ does not divide $r(d,g)\mathrm{discr}(A)$, where $r(d,g)$ is as in Lemma 4.2. To prove that $A[\ell]$ is a semisimple Γ-module it is enough to show that for any Γ-submodule $W \subset A[\ell]$ there is an idempotent $\pi \in \mathrm{End}(A)/\ell$ such that $W = \pi A[\ell]$. We apply Lemma 4.2 with $n = \ell$ to obtain an isogeny $u : A \to A$ such that $W = uA[\ell]$, where we used that ℓ and r are coprime. Since $\mathrm{End}(A)/\ell$ is semisimple by (a), we can write $u(\mathrm{End}(A)/\ell) = \pi(\mathrm{End}(A)/\ell)$ for some idempotent $\pi \in \mathrm{End}(A)/\ell$. Then $W = \pi A[\ell]$.

(c) We follow the proof of [Zar85, Cor. 5.4.5] which refers to [Zar77, 3.4]. Assume that ℓ does not divide any of the integers $\mathrm{discr}(A)$, $r(d,g)$, $r(d,2g)$.

Let D be the centraliser of $\mathrm{End}(A)/\ell$ in $\mathrm{End}(A[\ell]) \cong \mathrm{Mat}_{2g}(\mathbb{F}_\ell)$. Since $\mathrm{End}(A)/\ell$ is a semisimple $\mathbb{F}_\ell$-algebra by (a), the $\mathrm{End}(A)/\ell$-module $A[\ell]$ is semisimple, hence D is a semisimple $\mathbb{F}_\ell$-algebra. By the double centraliser theorem, the centraliser of D in $\mathrm{End}(A[\ell])$ is $\mathrm{End}(A)/\ell$.

Take any $\varphi \in \mathrm{End}(A[\ell])^\Gamma$. To prove that $\varphi \in \mathrm{End}(A)/\ell$ we need to show that φ commutes with D. Applying Lemma 4.2 to the graph of φ in $A[\ell]^{\oplus 2}$ and using that ℓ does not divide $r(d,2g)$, we write the graph of φ as $uA[\ell]^{\oplus 2}$ for some $u \in \mathrm{Mat}_2(\mathrm{End}(A)/\ell)$. Let $p_i : A[\ell]^{\oplus 2} \to A[\ell]$ be the projector to the i-th summand, for $i = 1, 2$. Since $p_1 u$ is surjective, for each $x \in A[\ell]$ we can write $x = p_1 u(y)$ for some $y \in A[\ell]^{\oplus 2}$. Then since $p_1 u, p_2 u : A[\ell]^{\oplus 2} \to A[\ell]$ are maps of D-modules and $\varphi p_1 u = p_2 u$, we have for all $d \in D$:

$$\varphi(dx) = \varphi p_1 u(dy) = p_2 u(dy) = d.p_2 u(y) = d\varphi(x).$$

This proves (c).

(d) This follows from (b), (c) applied to $A \times A^\vee$ and the following lemma.

Lemma 4.3 *Let k be a field of characteristic 0. Let A be an abelian variety over k of dimension $g \geq 1$. If $\ell > 4g$, the Γ-module $A[\ell]$ is semisimple, and*

$$\mathrm{End}(A \times A^\vee)/\ell = \mathrm{End}_\Gamma(A[\ell] \oplus A^\vee[\ell]),$$

then $\mathrm{Br}(\overline{A})[\ell]^\Gamma = 0$.

Proof. Since the Γ-module $A[\ell]$ is semisimple, so is $A^\vee[\ell] \cong \mathrm{Hom}(A[\ell], \mu_\ell)$. Hence by Serre's theorem [Ser94] and the fact that $\ell > 4g$, we deduce that $\mathrm{End}(A[\ell] \oplus A^\vee[\ell])$ is a semisimple Γ-module.

Let E_A and H_A be the Γ-modules from the exact sequences (13) and (14). The assumption $\mathrm{End}(A \times A^\vee)/\ell = \mathrm{End}_\Gamma(A[\ell] \oplus A^\vee[\ell])$, together with the semisimplicity of $\mathrm{End}(A[\ell] \oplus A^\vee[\ell])$, implies that $(E_A/\ell)^\Gamma = 0$. Since the sequence (14) is a direct summand of (13), we deduce that $(H_A/\ell)^\Gamma = 0$. Because ℓ is odd, combining this with Lemma 2.7 implies that $\mathrm{Br}(\overline{A})[\ell]^\Gamma = 0$. $\square$

This finishes the proof of Theorem 4.1. $\square$

Remark The statement of Lemma 4.3 remains true in positive characteristic. For the proof one has to replace the reference to Lemma 2.7 by a counting argument similar to the one used in [SZ08, Lemma 3.5].

4.2 Abelian varieties at large primes, II

The aim of this section is to prove a somewhat stronger version of Theorem 4.1, see Corollaries 4.7 and 4.8.

Let A be an abelian variety over a field k. For a prime $\ell \neq \mathrm{char}(k)$ let $T_\ell(A)$ be the ℓ-adic Tate module of A, and let $\rho_{\ell,A} : \Gamma \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A))$ be the attached ℓ-adic Galois representation. We denote by $\Lambda_\ell(A)$ the $\mathbb{Z}_\ell$-subalgebra of $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$ generated by $\rho_{\ell,A}(\Gamma)$. Write $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and define

$$D_\ell(A) = \Lambda_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

Thus $\Lambda_\ell(A)$ is an order in the $\mathbb{Q}_\ell$-algebra $D_\ell(A)$. Define

$$E(A) = \mathrm{End}(A) \otimes \mathbb{Q}, \quad E_\ell(A) = \mathrm{End}(A) \otimes \mathbb{Q}_\ell \subset \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

It is well known that $E(A)$ is a semisimple $\mathbb{Q}$-algebra [Mum74], so that $E_\ell(A)$ is a semisimple $\mathbb{Q}_\ell$-algebra. The $\mathbb{Z}$-algebra $\mathrm{End}(A)$ is an order in $E(A)$, hence the $\mathbb{Z}_\ell$-algebra $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ is an order in $E_\ell(A)$. It is clear that $\Lambda_\ell(A)$ and $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ are commuting subalgebras of $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$, and $D_\ell(A)$ and $E_\ell(A)$ are commuting subalgebras of $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. By the work of Weil, Tate, Zarhin, Faltings, Mori on the Tate conjecture [Zar75, Zar76, Fal83, Fal84, Mor85] it is known that if k is finitely generated over its prime subfield, then $D_\ell(A)$ is a semisimple $\mathbb{Q}_\ell$-algebra and

$$\mathrm{End}_\Gamma(T_\ell(A)) = \mathrm{End}_{\Lambda_\ell(A)}(T_\ell(A)) = \mathrm{End}(A) \otimes \mathbb{Z}_\ell.$$

This implies

$$E_\ell(A) = \mathrm{End}_{D_\ell(A)}(V_\ell(A)), \quad D_\ell(A) = \mathrm{End}_{E_\ell(A)}(V_\ell(A)), \tag{16}$$

where the second identity follows from the first by the double centraliser theorem.

Proposition 4.4 *Let k be a field finitely generated over $\mathbb{Q}$. Let A be an abelian variety over k of dimension $g \geq 1$. If ℓ is a prime not dividing* $\mathrm{discr}(\Lambda_\ell(A))$*, then the Γ-module $A[\ell]$ is semisimple,* $\mathrm{End}(A)/\ell$ *is a semisimple $\mathbb{F}_\ell$-algebra, and*

$$\mathrm{End}_\Gamma(A[\ell]) = \mathrm{End}(A)/\ell.$$

Proof. Because k is finitely generated over $\mathbb{Q}$, $\Lambda_\ell(A)$ is an order in the *semisimple* $\mathbb{Q}_\ell$-algebra $D_\ell(A)$. By Proposition 2.4 the $\mathbb{F}_\ell$-algebra $\Lambda_\ell(A)/\ell$ is semisimple, thus $A[\ell]$ is a semisimple $\Lambda_\ell(A)/\ell$-module, hence also a semisimple Γ-module.

Also by Proposition 2.4 we have an isomorphism $\Lambda_\ell(A) \cong \oplus_{i=1}^r \mathrm{Mat}_{n_i}(O_{k_i})$, where O_{k_i} is the ring of integers of an unramified field extension $k_i/\mathbb{Q}_\ell$ and n_i is a positive integer, for $i = 1, \ldots, r$. Write $\mathbb{F}_i = O_{k_i}/\ell$ for the residue field of O_{k_i}.

Using the fact that $\mathrm{Mat}_{n_i}(O_{k_i})$ is Morita-equivalent to O_{k_i}, we obtain that for each $i = 1, \ldots, r$ there exists a free O_{k_i}-module T_i of finite rank such that $T_\ell(A) \cong \oplus_{i=1}^r T_i^{\oplus n_i}$, where the action of $\Lambda_\ell(A)$ on $T_i^{\oplus n_i} = T_i \otimes_{O_{k_i}} O_{k_i}^{\oplus n_i}$ is induced by the natural action of $\mathrm{Mat}_{n_i}(O_{k_i})$ on $O_{k_i}^{\oplus n_i}$. Hence $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$, being the centraliser of $\Lambda_\ell(A)$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$, is equal to $\oplus_{i=1}^r \mathrm{End}_{O_{k_i}}(T_i)$. Thus $\mathrm{End}(A)/\ell = \oplus_{i=1}^r \mathrm{End}_{\mathbb{F}_i}(T_i/\ell)$ is a semisimple $\mathbb{F}_\ell$-algebra. On the other hand, the centraliser of $\Lambda_\ell(A)/\ell = \oplus_{i=1}^r \mathrm{Mat}_{n_i}(\mathbb{F}_i)$ in $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell]) = \mathrm{End}_{\mathbb{F}_\ell}(\oplus_{i=1}^r (T_i/\ell)^{\oplus n_i})$ is also equal to $\oplus_{i=1}^r \mathrm{End}_{\mathbb{F}_i}(T_i/\ell)$. This finishes the proof. □

Proposition 4.5 *Let k be a field finitely generated over $\mathbb{Q}$. Let A be an abelian variety over k of dimension $g \geq 1$. If $\ell > 4g$ is a prime that does not divide* $\mathrm{discr}(\Lambda_\ell(A \times A^\vee))$*, then* $\mathrm{Br}(\overline{A})[\ell]^\Gamma = 0$.

Proof. This follows from Proposition 4.4 applied to $A \times A^\vee$ and Lemma 4.3. □

For positive integers g, let $n(g) = [2ge^{2g/e}]$, where e is the base of the natural logarithm. The significance of this quantity will appear in the proof of Theorem 4.6.

The following theorem is the main result of this section.

Theorem 4.6 *Let k be a field finitely generated over $\mathbb{Q}$. Let A be an abelian variety over k of dimension $g \geq 1$. There exists an abelian variety B over k which is k-isogenous to an abelian subvariety of $A^{n(g)}$ such that* $\mathrm{End}(B) \otimes \mathbb{Z}_\ell$ *is isomorphic to a matrix algebra over $\Lambda_\ell(A)^{\mathrm{op}}$. In particular,* $\mathrm{discr}(\Lambda_\ell(A))$ *divides* $\mathrm{discr}(B)$.

Proof. Let us first prove the statement in the isotypic case, i.e. when A is a power of a simple abelian variety. Then $E(A)$ is a simple $\mathbb{Q}$-algebra.

Let us fix an embedding $\bar{k} \hookrightarrow \mathbb{C}$. The natural action of $E(A)$ on $\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q})$ gives rise to an embedding $E(A) \subset \mathrm{End}_{\mathbb{Q}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q}))$, so that $E(A)$ is a simple $\mathbb{Q}$-subalgebra of the matrix algebra $\mathrm{End}_{\mathbb{Q}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q}))$ containing its centre $\mathbb{Q}\,\mathrm{Id}$. By

[Her68, Thm. 4.3.2] the centraliser $D(A) = \mathrm{End}_{E(A)}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q}))$ is also a simple $\mathbb{Q}$-subalgebra of $\mathrm{End}_{\mathbb{Q}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q}))$. Moreover, by [Her68, p. 105] we have

$$\dim_{\mathbb{Q}}(D(A)) \cdot \dim_{\mathbb{Q}}(E(A)) = \dim_{\mathbb{Q}}(\mathrm{End}_{\mathbb{Q}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q}))) = 4g^2.$$

Next, $D(A)$ is isomorphic to a matrix algebra over a division $\mathbb{Q}$-algebra F, say $D(A) \cong \mathrm{Mat}_m(F)$. Comparing dimensions over $\mathbb{Q}$ we see that m divides $2g$.

Let $M \cong F^{\oplus m}$ be a simple left $D(A)$-module (unique up to isomorphism). Any left $D(A)$-module that has finite dimension over F is isomorphic to a direct sum of finitely many copies of M; in particular, the left $D(A)$-module $D(A)$ is isomorphic to $M^{\oplus m}$ and the $D(A)$-module $\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q})$ is isomorphic to $M^{\oplus r}$, where r divides $2g$. We obtain an isomorphism of left $D(A)$-modules

$$\mathrm{H}_1(A^m_{\mathbb{C}}, \mathbb{Q}) = \mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q})^{\oplus m} \cong M^{\oplus mr} \cong D(A)^{\oplus r}. \tag{17}$$

The Tate module $T_\ell(A)$ is isomorphic to $\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{Z}_\ell$ as an $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$-module. Hence $V_\ell(A) \cong \mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Q}) \otimes \mathbb{Q}_\ell$ as an $E_\ell(A)$-module. But $T_\ell(A)$ is naturally a Galois module; in fact, we know that $V_\ell(A)$ is a $D_\ell(A)$-module satisfying (16). From this and the definition of $D(A)$ it follows that $D_\ell(A) = D(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Now (17) gives rise to isomorphisms of left $D_\ell(A)$-modules (hence also of Γ-modules)

$$V_\ell(A^m) = V_\ell(A)^{\oplus m} \cong D_\ell(A)^{\oplus r}. \tag{18}$$

Recall that $\Lambda_\ell(A)$ is an order, hence a lattice in $D_\ell(A)$. Let S be the lattice in $V_\ell(A^m)$ obtained from the lattice $\Lambda_\ell(A)^{\oplus r} \subset D_\ell(A)^{\oplus r}$ via the isomorphism (18). It is clear that S is stable under the action of the Galois group Γ. We note that $T_\ell(A^m)$ is also a Γ-stable lattice in $V_\ell(A^m)$. Hence for some positive integer N we have $\ell^N S \subset T_\ell(A^m)$. There exists an abelian variety B over k such that $S \cong T_\ell(B)$ as Γ-modules together with a k-isogeny $\alpha : B \to A^m$ of degree $|T_\ell(A^m)/\ell^N S|$ such that $\alpha_*(T_\ell(B)) = \ell^N S$. From the construction of S we have

$$\mathrm{End}(B) \otimes \mathbb{Z}_\ell = \mathrm{End}_\Gamma(T_\ell(B)) = \mathrm{End}_\Gamma(\Lambda_\ell(A)^{\oplus r}) = \mathrm{End}_{\Lambda_\ell(A)}(\Lambda_\ell(A)^{\oplus r}) = \mathrm{Mat}_r(\Lambda_\ell(A)^{\mathrm{op}}).$$

Since m divides $2g$, this finishes the proof in the isotypic case.

In the general case A is isogenous to $\prod_{i=1}^s A_i$, where each A_i is a power of a simple abelian variety and $\mathrm{Hom}(A_i, A_j) = 0$ for $i \neq j$. Fixing such an isogeny we obtain an isomorphism of Γ-modules $V_\ell(A) \cong \oplus_{i=1}^s V_\ell(A_i)$ and an isomorphism of $\mathbb{Q}_\ell$-algebras $D_\ell(A) \cong \oplus_{i=1}^s D_\ell(A_i)$. For each $i = 1, \ldots, s$ we construct an isomorphism of Γ-modules $V_\ell(A_i^{m_i}) \cong D_\ell(A_i)^{\oplus r_i}$ as in (18), where both m_i and r_i divide $2\dim(A_i)$. Write $r = \prod_{i=1}^s r_i$. Then we have isomorphisms of Γ-modules $V_\ell(A_i^{m_i r/r_i}) \cong D_\ell(A_i)^{\oplus r}$, which add up to an isomorphism of Γ-modules

$$V_\ell(A') \cong D_\ell(A)^{\oplus r}, \quad \text{where} \quad A' = \prod_{i=1}^s A_i^{m_i r/r_i}. \tag{19}$$

For any $x > 0$ we have $\log(x) \leq x/e$, whence we obtain $r \leq e^{\sum_{i=1}^{s} r_i/e} \leq e^{2g/e}$. Thus A' is an abelian subvariety of $A^{n(g)}$.

Let S be the lattice in $V_\ell(A')$ obtained from the lattice $\Lambda_\ell(A)^{\oplus r} \subset D_\ell(A)^{\oplus r}$ via isomorphism (19). As above, there is an abelian variety B over k such that $S \cong T_\ell(B)$ as Γ-modules together with a k-isogeny $B \to A'$, for which there is an isomorphism $\mathrm{End}(B) \otimes \mathbb{Z}_\ell \cong \mathrm{Mat}_r(\Lambda_\ell(A)^{\mathrm{op}})$. This proves the theorem. □

Remark By the Poincaré reducibility theorem there are only finitely many abelian subvarieties of a given abelian variety considered up to k-isogeny. (In fact, the same is true up to k-isomorphism, see [LOZ96].) When k is finitely generated over $\mathbb{Q}$ each isogeny class of abelian varieties over k consists of finitely many k-isomorphism classes. (The case of number fields was treated in [Zar85, Prop. 3.1]. For the case of arbitrary finitely generated fields see [Fal84, Thm. 2 and its proof on pp. 214–215].) Thus the abelian variety B in Theorem 4.6 belongs to a finite set of k-isomorphism classes determined by A.

Corollary 4.7 *Consider a family $\mathcal{F}$ of abelian varieties such that each $A \in \mathcal{F}$ is defined over a field k_A finitely generated over $\mathbb{Q}$. Suppose that there is a constant c such that for every $A \in \mathcal{F}$ and every abelian variety B over k_A which is k_A-isogenous to an abelian subvariety of $A^{n(\dim(A))}$, we have $\mathrm{discr}(B) < c$. Then for every prime $\ell > c$ and every $A \in \mathcal{F}$, the Γ-module $A[\ell]$ is semisimple, $\mathrm{End}(A)/\ell$ is a semisimple $\mathbb{F}_\ell$-algebra, and $\mathrm{End}_\Gamma(A[\ell]) = \mathrm{End}(A)/\ell$.*

Proof. Combine Theorem 4.6 with Proposition 4.4. □

Corollary 4.8 *Consider a family $\mathcal{F}$ of abelian varieties such that each $A \in \mathcal{F}$ is defined over a field k_A finitely generated over $\mathbb{Q}$. Suppose that there is a constant c such that for every $A \in \mathcal{F}$ and every abelian variety B over k_A which is k_A-isogenous to an abelian subvariety of $A^{n(2\dim(A))}$, we have $\mathrm{discr}(B) < c$. Then for every prime $\ell > \max(c, 4\dim(A))$ and every $A \in \mathcal{F}$ we have $\mathrm{Br}(\overline{A})[\ell]^\Gamma = 0$.*

Proof. Combine Theorem 4.6 with Proposition 4.5. □

4.3 Abelian varieties at a fixed prime

The following proposition develops [Zar85, Remark 5.4.7]. For abelian varieties over number fields, this proposition can also be proved by combining [MW95, Lemma 4.1] with [Rem18, Thm. 1.1].

Proposition 4.9 *Let ℓ be a prime and let g be a positive integer. Consider a family $\mathcal{F}$ of abelian varieties such that each $A \in \mathcal{F}$ has dimension at most g and is defined over a field k_A finitely generated over $\mathbb{Q}$. Suppose that there is a constant c such that for every $A \in \mathcal{F}$ and every abelian variety B over k_A which is k_A-isogenous to an abelian subvariety of $A^{n(\dim(A))}$, we have $\mathrm{discr}(B) < c$.*

Then there exists a positive integer $a = a(\mathcal{F})$ such that for every abelian variety $A \in \mathcal{F}$ and every $n \geq 1$, the subgroup $[\ell^a] \cdot \mathrm{End}_\Gamma(A[\ell^{n+a}])$ of $\mathrm{End}_\Gamma(A[\ell^n])$ is contained in the image of $\mathrm{End}(A)/\ell^n$.

Proof. We can apply Lemma 2.3 to the Tate module $N = T_\ell(A)$, where $\Lambda = \Lambda_\ell(A)$ is the $\mathbb{Z}_\ell$-subalgebra of $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$ generated by $\rho_{\ell,A}(\Gamma)$. Indeed, by Faltings [Fal84] we have $\mathrm{End}_\Lambda(N) = \mathrm{End}_\Gamma(T_\ell(A)) = \mathrm{End}(A) \otimes \mathbb{Z}_\ell$, whereas the restriction of $(x.y) = \mathrm{Tr}(xy)$ to $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ is non-degenerate by Lemma 3.1.

Lemma 2.3 now gives a positive integer a such that $\ell^a \cdot \mathrm{End}_\Gamma(A[\ell^{n+a}])$ is contained in the image of $\mathrm{End}(A)$ for every $n \geq 1$. However a may depend on the subalgebra Λ of $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$ and on the structure of $T_\ell(A)$ as a Λ-module.

As recalled in Section 4.2, Λ is an order in an semisimple $\mathbb{Q}_\ell$-algebra of dimension at most $16g^2$. By Theorem 4.6, $\mathrm{discr}(\Lambda)$ is bounded by c. By a similar argument to that used in the proof of Proposition 2.3, there are only finitely many isomorphism classes of $\mathbb{Z}_\ell$-orders of given discriminant in semisimple $\mathbb{Q}_\ell$-algebras of given dimension. Thus there are finitely many possibilities for Λ.

Furthermore, for each $\mathbb{Z}_\ell$-algebra Λ, there are only finitely many isomorphism classes of Λ-modules of given finite $\mathbb{Z}_\ell$-rank. This implies that our constant a can be chosen to depend only on $\mathcal{F}$. $\square$

The main result of this section is the following theorem.

Theorem 4.10 *Let ℓ be a prime and let g be a positive integer. Consider a family $\mathcal{F}$ of abelian varieties such that each $A \in \mathcal{F}$ has dimension at most g and is defined over a field k_A finitely generated over $\mathbb{Q}$. Suppose that there is a constant c such that for every $A \in \mathcal{F}$ and every abelian variety B over k_A which is k_A-isogenous to an abelian subvariety of $A^{n(2\dim(A))}$, we have $\mathrm{discr}(B) < c$.*

Then there exists a positive integer r such that for every abelian variety $A \in \mathcal{F}$ the group $\mathrm{Br}(\overline{A})\{\ell\}^\Gamma$ is annihilated by ℓ^r, and so is a finite abelian group of cardinality dividing $\ell^{r(g(2g-1)-1)}$.

Proof. Recall the definitions of E_A and H_A from the exact sequences (13) and (14).

By Lemma 2.7, it suffices to prove that there is an integer s depending only on $\mathcal{F}$ such that, for every $n \geq 1$, we have $[\ell^s] \cdot (H_A/\ell^n)^\Gamma = 0$.

We equip $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A) \oplus T_\ell(A^\vee))$ with the unimodular symmetric bilinear form $\mathrm{Tr}(xy)$, where Tr is the usual matrix trace. By Lemma 3.1 and our hypothesis on $\mathcal{F}$, the restriction of this form to $\mathrm{End}(\overline{A} \times \overline{A}^\vee) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ has bounded, non-zero discriminant. By Lemma 2.2 this gives a positive integer b such that $[\ell^b] \cdot (E_A/\ell^n)^\Gamma$ is contained in the image of

$$(\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A) \oplus T_\ell(A^\vee))/\ell^n)^\Gamma = \mathrm{End}_\Gamma(A[\ell^n] \oplus A^\vee[\ell^n]),$$

for every $n \geq 1$.

By Proposition 4.9, this implies that $[\ell^{a+b}] \cdot (E_A/\ell^n)^\Gamma$ is contained in the image of $\mathrm{End}(A \times A^\vee)/\ell^n$. But by the exact sequence (13), the image of $\mathrm{End}(A \times A^\vee)/\ell^n$ in E_A/ℓ^n is 0. Thus $[\ell^{a+b}] \cdot (E_A/\ell^n)^\Gamma = 0$. Since the exact sequence (14) is a direct summand of (13), it follows that $[\ell^{a+b}] \cdot (H_A/\ell^n)^\Gamma = 0$, as required.

To deduce the bound on the cardinality of $\mathrm{Br}(\overline{A})\{\ell\}^\Gamma$, observe that $\mathrm{Br}(\overline{A})[\ell]$ is a quotient of a free $\mathbb{Z}_\ell$-module $\mathrm{H}^2(\overline{A}, \mathbb{Z}_\ell(1))/(\mathrm{NS}\,(\overline{A}) \otimes \mathbb{Z}_\ell)$ of rank

$$\mathrm{rk}(\mathrm{H}^2(\overline{A}, \mathbb{Z}_\ell)) - \mathrm{rk}(\mathrm{NS}\,(\overline{A})) \leq g(2g-1) - 1. \ \square$$

4.4 Converse results

Let p be 0 or a prime number. The function $d_p(g)$ was introduced in Definition 3.3.

For an abelian group B and a prime p, define $B(p')$ to be the subgroup of B_{tors} consisting of the elements whose order is not divisible by p. For $p = 0$, we write $B(p') = B_{\mathrm{tors}}$.

The following statement will be used in Section 6.

Proposition 4.11 *Let k be a field of characteristic p. Let A be an abelian variety over k of dimension $g \geq 1$. If $\mathrm{Br}(\overline{A} \times \overline{A}^\vee)(p')^\Gamma$ is annihilated by a positive integer M, then for any positive integer n not divisible by p, we have*

$$d_p(g)M \cdot \mathrm{End}_\Gamma(A[n]) \subset \mathrm{End}(A)/n \subset \mathrm{End}_\Gamma(A[n]).$$

In particular, if ℓ is a prime not dividing $d_p(g)M$ and not equal to p, then

$$\mathrm{End}_\Gamma(A[\ell]) = \mathrm{End}(A)/\ell.$$

Proof. In [SZ14] the last two authors used the Kummer sequence and the Künneth formula to obtain an expression for the Brauer group of a product of varieties, see [SZ14, formula (20), p. 761]. Applied to the abelian variety $A \times A^\vee$ it gives a canonical isomorphism of Γ-modules

$$\mathrm{Br}(\overline{A} \times \overline{A}^\vee)[n] \cong \mathrm{Br}(\overline{A})[n] \oplus \mathrm{Br}(\overline{A}^\vee)[n] \oplus \mathrm{End}_{\mathbb{Z}/n}(A[n])/\big(\mathrm{End}(\overline{A})/n\big).$$

Thus $\big(\mathrm{End}_{\mathbb{Z}/n}(A[n])/\big(\mathrm{End}(\overline{A})/n\big)\big)^\Gamma$ is a subgroup of $\mathrm{Br}(\overline{A} \times \overline{A}^\vee)[n]^\Gamma$, and so is annihilated by M. In view of the exact sequence of Γ-modules

$$0 \longrightarrow \mathrm{End}(\overline{A})/n \longrightarrow \mathrm{End}_{\mathbb{Z}/n}(A[n]) \longrightarrow \mathrm{End}_{\mathbb{Z}/n}(A[n])/\big(\mathrm{End}(\overline{A})/n\big) \longrightarrow 0$$

we conclude that $M \cdot \mathrm{End}_\Gamma(A[n]) \subset (\mathrm{End}(\overline{A})/n)^\Gamma$.

Let G be the image of Γ in $\mathrm{Aut}(\mathrm{End}(\overline{A}))$ via its natural action on $\mathrm{End}(\overline{A})$. By a result of Silverberg [Sil92, Thm. 2.4], G is a finite group of order dividing $d_p(g)$. The exact sequence of Γ-modules

$$0 \longrightarrow \mathrm{End}(\overline{A}) \xrightarrow{[n]} \mathrm{End}(\overline{A}) \longrightarrow \mathrm{End}(\overline{A})/n \longrightarrow 0$$

comes from the same sequence considered as an exact sequence of G-modules. It gives rise to the exact sequence of abelian groups

$$0 \longrightarrow \mathrm{End}(A)/n \longrightarrow (\mathrm{End}(\overline{A})/n)^{\Gamma} \longrightarrow \mathrm{H}^1(G, \mathrm{End}(\overline{A})),$$

where we took into account that $\mathrm{End}(\overline{A})^G = \mathrm{End}(\overline{A})^{\Gamma} = \mathrm{End}(A)$. Since $\mathrm{H}^1(G, \mathrm{End}(\overline{A}))$ is annihilated by $d_p(g)$, we obtain $d_p(g) \cdot (\mathrm{End}(\overline{A})/n)^{\Gamma} \subset \mathrm{End}(A)/n$, and thus $d_p(g)M \cdot (\mathrm{End}_{\Gamma}(A[n]) \subset \mathrm{End}(A)/n$. □

We point out the following partial converse to Theorem 4.1.

Corollary 4.12 *Let ℓ be a prime and let k be a field of characteristic $p \neq \ell$. Let A be an abelian variety over k of dimension $g \geq 1$. If ℓ does not divide $d_p(g)$, the Γ-module $A[\ell]$ is semisimple and $\mathrm{Br}(\overline{A} \times \overline{A}^{\vee})[\ell]^{\Gamma} = 0$, then the following hold:*

(a) *the $\mathbb{F}_\ell$-algebra $\mathrm{End}(A)/\ell$ is semisimple;*

(b) *ℓ does not divide $\mathrm{discr}(A)$.*

Proof. (a) Since the Γ-module $A[\ell]$ is semisimple, the $\mathbb{F}_\ell$-algebra $\mathrm{End}_{\Gamma}(A[\ell])$ is semisimple. By the second part of Proposition 4.11 it coincides with $\mathrm{End}(A)/\ell$.

(b) This follows from (a) and Corollary 2.5. □

5 Coleman implies Shafarevich

In this section, we show that Coleman's conjecture implies Shafarevich's conjecture. We use the Kuga–Satake construction to relate Hodge structures associated with K3 surfaces to abelian varieties. In order to obtain a result which is independent of the degree of polarisation of the K3 surface, we use a K3 surfaces version of Zarhin's trick from [OS18] and [She], which is described in terms of orthogonal Shimura varieties.

We first recall how one constructs an orthogonal Shimura variety from a lattice L with signature $(2, n)$, $n \geq 1$. Let $\mathbf{SO}(L)$ be the group scheme over $\mathbb{Z}$ whose functor of points associates to a ring R the group $\mathrm{SO}(L \otimes_{\mathbb{Z}} R)$. Let $\mathbb{S} = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)$ denote the Deligne torus and let Ω_L be the set of $h \in \mathrm{Hom}(\mathbb{S}, \mathbf{SO}(L)_{\mathbb{R}})$ such that the associated $\mathbb{Z}$-Hodge structure on L is of K3 type, that is, the following properties are satisfied:

1. $\dim((L \otimes_{\mathbb{Z}} \mathbb{C})_h^{(1,-1)}) = \dim((L \otimes_{\mathbb{Z}} \mathbb{C})_h^{(-1,1)}) = 1$ and $\dim((L \otimes_{\mathbb{Z}} \mathbb{C})_h^{(0,0)}) = n$;
2. for every non-zero $v \in (L \otimes_{\mathbb{Z}} \mathbb{C})_h^{(1,-1)}$ we have $(v, v) = 0$ and $(v, \bar{v}) > 0$;
3. $((L \otimes_{\mathbb{Z}} \mathbb{C})_h^{(1,-1)}, (L \otimes_{\mathbb{Z}} \mathbb{C})_h^{(0,0)}) = 0$.

Sending h to $(L \otimes_{\mathbb{Z}} \mathbb{C})_h^{(1,-1)}$ identifies Ω_L with $\{[x] \in \mathbb{P}(L \otimes_{\mathbb{Z}} \mathbb{C}) \mid (x^2) = 0,\ (x, \bar{x}) > 0\}$, which is a homogeneous space of $\mathrm{SO}(L \otimes_{\mathbb{Z}} \mathbb{R})$.

Let $\mathbb{K} \subset \mathbf{SO}(L)(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ be a compact open subgroup. The canonical model of the associated Shimura variety $\mathrm{Sh}_{\mathbb{K}}(L) := \mathrm{Sh}_{\mathbb{K}}(\mathbf{SO}(L)_{\mathbb{Q}}, \Omega_L)$ is a quasi-projective variety over $\mathbb{Q}$. By construction, the $\mathbb{C}$-points of $\mathrm{Sh}_{\mathbb{K}}(L)$ parameterise $\mathbb{Z}$-Hodge structures on L satisfying properties 1, 2, 3 above.

Suppose that $\mathbb{K}$ is torsion-free. (Every compact open subgroup of $\mathbf{SO}(L)(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ contains a torsion-free subgroup of finite index.) Then for each prime ℓ there is a lisse $\mathbb{Z}_\ell$-sheaf L_ℓ on $\mathrm{Sh}_{\mathbb{K}}(L)$ defined by the inverse system of finite étale covers $\mathrm{Sh}_{\mathbb{K}(\ell^m)}(L) \to \mathrm{Sh}_{\mathbb{K}}(L)$, where $\mathbb{K}(\ell^m)$ is the largest subgroup of $\mathbb{K}$ that acts trivially on L/ℓ^m. Thus, to a k-point x of $\mathrm{Sh}_{\mathbb{K}}(L)$ there corresponds a representation $\mathrm{Gal}(\overline{k}/k) \to \mathrm{SO}(L \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$. Putting together these representations for all ℓ gives a representation

$$\phi_x : \mathrm{Gal}(\overline{k}/k) \to \mathrm{SO}(L \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}). \tag{20}$$

This construction was also described in [CM, 3.1] or [UY13, 2.2].

From a lattice L with signature $(2, n)$, $n \geq 1$, one can also construct a spin Shimura variety, see [MP16, Section 3]. Let $C(L)$ be the Clifford algebra of L, and let $C^+(L) \subset C(L)$ be the even Clifford algebra. Let $\mathbf{GSpin}(L)$ be the group $\mathbb{Z}$-scheme whose functor of points associates to a ring R the group of invertible elements g of $C^+(L \otimes_{\mathbb{Z}} R)$ such that $g(L \otimes_{\mathbb{Z}} R)g^{-1} = L \otimes_{\mathbb{Z}} R$. If $\tilde{\mathbb{K}} \subset \mathbf{GSpin}(L)(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ is a compact open subgroup, we write $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L)$ for the Shimura variety $\mathrm{Sh}_{\tilde{\mathbb{K}}}(\mathbf{GSpin}(L)_{\mathbb{Q}}, \Omega_L)$. Let $\mathbb{K}$ be the image of $\tilde{\mathbb{K}}$ in $\mathbf{SO}(L)(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$. By [And96, 4.4] this subgroup of $\mathbf{SO}(L)(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ is compact and open. The natural group homomorphism $\mathbf{GSpin}(L)_{\mathbb{Q}} \to \mathbf{SO}(L)_{\mathbb{Q}}$ induces a morphism $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L) \to \mathrm{Sh}_{\mathbb{K}}(L)$. This morphism is finite and surjective by [Orr13, Thm. 2.4], and defined over $\mathbb{Q}$ because the Shimura datum $(\mathbf{GSpin}(L)_{\mathbb{Q}}, \Omega_L)$ has reflex field $\mathbb{Q}$ [And96, App. 1].

Let $\tilde{\mathbb{K}}_N \subset \mathbf{GSpin}(L)(\hat{\mathbb{Z}})$ be the set of elements congruent to 1 modulo N in $C^+(L \otimes_{\mathbb{Z}} \hat{\mathbb{Z}})$. If $\tilde{\mathbb{K}} \subset \tilde{\mathbb{K}}_N$ for $N \geq 3$, then $\tilde{\mathbb{K}}$ and $\mathbb{K}$ are torsion-free and the morphism $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L) \to \mathrm{Sh}_{\mathbb{K}}(L)$ is étale. Rizov shows in [Riz10, Section 5.5, (32)] that this morphism restricts to an isomorphism on each geometric connected component. Thus $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L) \to \mathrm{Sh}_{\mathbb{K}}(L)$ has a section defined over a number field E which only depends on L and $\tilde{\mathbb{K}}$.

There is a finite morphism of Shimura varieties from $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L)$ to a moduli space of abelian varieties, defined over $\mathbb{Q}$. In order to construct this, we find a skew-symmetric form on $C(L)$ following [Huy16, Ch. 4, 2.2]. Indeed, we choose orthogonal elements $f_1, f_2 \in L$ satisfying $(f_1^2), (f_2^2) > 0$. Then we can define a skew-symmetric form on $C(L)$ by $\pm\mathrm{Tr}_{C(L)}(f_1 f_2 v^* w)$, where $\mathrm{Tr}_{C(L)}$ is the intrinsic trace. The action of $\mathbf{GSpin}(L)$ on this form is multiplication by the spinor norm (see [Huy16, Ch. 4, Prop. 2.5] for proofs of these facts, as well as the correct choice of sign). The group $\mathbf{GSpin}(L)$ injects into the group of symplectic similitudes $\mathbf{GSp}(C(L))$ of this form.

If $\tilde{\mathbb{K}} \subset \tilde{\mathbb{K}}_N$, then we have a morphism from $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L)$ to the Shimura variety $\mathrm{Sh}_{\Gamma_N}(\mathbf{GSp}(C(L))_{\mathbb{Q}}, \mathcal{H}^{\pm})$, where Γ_N is the subgroup of $\mathbf{GSp}(C(L))(\hat{\mathbb{Z}})$ consisting of

the elements that are congruent to 1 modulo N. The latter Shimura variety is identified with the moduli variety $\mathcal{A}_{g,\delta,N}$ parameterising abelian varieties of dimension $g = 2^{n+1}$, polarisation type δ (explicitly computable in terms of L and f_1, f_2) and level structure of level N. If $N \geq 3$, then $\mathcal{A}_{g,\delta,N}$ is a fine moduli space, so we can define the *Kuga–Satake abelian scheme* $f : A \to \mathrm{Sh}_{\mathbb{K}}(L)_E$ as the pullback of the universal family of abelian varieties on $\mathcal{A}_{g,\delta,N}$ to $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L)$, and then, after extending the ground field from $\mathbb{Q}$ to E, to $\mathrm{Sh}_{\mathbb{K}}(L)_E$. (As above, E is a number field over which there exists a section of $\mathrm{Sh}^{\mathrm{spin}}_{\tilde{\mathbb{K}}}(L)_E \to \mathrm{Sh}_{\mathbb{K}}(L)_E$. The Kuga–Satake scheme depends on the choice of such a section.)

The left multiplication of $L \subset C(L)$ on $C(L)$ gives a homomorphism $L \hookrightarrow \mathrm{End}_{\mathbb{Z}}(C(L))$ whose cokernel is torsion-free. Since $C(L) = R^1 f_{\mathrm{an},*}\mathbb{Z}$ as sheaves on $\mathrm{Sh}_{\mathbb{K}}(L)_{\mathbb{C}}$, this gives rise to a morphism of variations of $\mathbb{Z}$-Hodge structures

$$L \to C(L) \to \mathrm{End}_{\mathbb{Z}}(R^1 f_{\mathrm{an},*}\mathbb{Z}).$$

Via the comparison theorems we get a morphism of $\mathbb{Z}_\ell$-sheaves $L_\ell \to \mathrm{End}_{\mathbb{Z}_\ell}(R^1 f_* \mathbb{Z}_\ell)$.

Proposition 5.1 *Let L be a unimodular lattice of signature $(2, n)$, $n \geq 1$. Let $\tilde{\mathbb{K}} \subset \tilde{\mathbb{K}}_3 \subset \mathbf{GSpin}(L)(\hat{\mathbb{Z}})$ be a compact open subgroup and let $\mathbb{K}$ be the image of $\tilde{\mathbb{K}}$ in $\mathbf{SO}(L)(\hat{\mathbb{Z}})$. For a $\mathbb{C}$-point s of $\mathrm{Sh}_{\mathbb{K}}(L)$, write L_s for the $\mathbb{Z}$-Hodge structure on L parameterised by s. Define T_s to be the smallest primitive sub-$\mathbb{Z}$-Hodge structure of L_s whose complexification contains $L_s^{(1,-1)}$.*

If Coleman's conjecture about $\mathrm{End}(\overline{A})$ holds for abelian varieties of dimension 2^{n+1}, then the discriminant of the restriction of the bilinear form on L to T_s is bounded by a constant that depends only on n and d, provided that s is defined over a number field of degree d.

Proof. Define $N_s = L \cap (L_s \otimes_{\mathbb{Z}} \mathbb{C})^{(0,0)}$. Then T_s is the orthogonal complement to N_s in L. Since L is unimodular, we have $|\mathrm{discr}(N_s)| = |\mathrm{discr}(T_s)|$, so it is enough to prove that $|\mathrm{discr}(N_s)|$ is bounded.

We equip the $\mathbb{Z}$-algebra $\mathrm{End}_{\mathbb{Z}}(C(L)) = \mathrm{Mat}_{2^{n+2}}(\mathbb{Z})$ with the unimodular bilinear form $\mathrm{Tr}_{C(L)}(xy)$, where $\mathrm{Tr}_{C(L)}$ is the usual matrix trace (which, by definition, is the same as the reduced trace). This form is compatible with the Hodge structure, because the Hodge parameter $h_{\mathrm{End}} : \mathbb{S} \to \mathrm{GL}(\mathrm{End}_{\mathbb{Z}}(C(L)) \otimes \mathbb{R})$ is given by $h_{\mathrm{End}}(z)(x) = h_{C(L)}(z)\, x\, h_{C(L)}(z)^{-1}$. From the definition of the Clifford algebra we see that the restriction of this form to $L \subset \mathrm{End}_{\mathbb{Z}}(C(L))$ is the original unimodular form on L multiplied by 2^{n+2}. Let $L^\perp$ be the orthogonal complement to L in $\mathrm{End}_{\mathbb{Z}}(C(L))$. By the non-degeneracy of the form on L we have $L \cap L^\perp = 0$. The index of $L \oplus L^\perp$ in $\mathrm{End}_{\mathbb{Z}}(C(L))$ is equal to the discriminant of the restriction to L of the bilinear form on $\mathrm{End}_{\mathbb{Z}}(C(L))$, and so depends only on n.

Suppose s is defined over a number field k. Without loss of generality we can assume that k contains E. Thus we have an abelian variety A_s defined over k

which is the fibre of $f : A \to \mathrm{Sh}_{\mathbb{K}}(L)$ at s. The natural injection $\mathrm{End}(A_{s,\mathbb{C}}) \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{Z}))$ gives an identification

$$\mathrm{End}(A_{s,\mathbb{C}}) = \mathrm{End}_{\mathbb{Z}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{Z})) \cap \mathrm{End}_{\mathbb{C}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{C}))^{(0,0)}.$$

In particular, $\mathrm{End}(A_{s,\mathbb{C}})$ is saturated in $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{Z}))$.

Since L_s is a sub-$\mathbb{Z}$-Hodge structure of $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{Z}))$ and the Hodge structure is compatible with the bilinear form on $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{Z})) \cong \mathrm{End}_{\mathbb{Z}}(C(L))$, we see that $L_s^\perp$ is also a sub-$\mathbb{Z}$-Hodge structure. Write $N_s' = L^\perp \cap (L_s^\perp \otimes_{\mathbb{Z}} \mathbb{C})^{(0,0)}$. In the category of $\mathbb{Q}$-Hodge structures, $\mathrm{End}_{\mathbb{Q}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{Q})) = L_s \otimes_{\mathbb{Z}} \mathbb{Q} \oplus L_s^\perp \otimes_{\mathbb{Z}} \mathbb{Q}$, and so

$$\mathrm{End}(A_{s,\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q} = (N_s \otimes_{\mathbb{Z}} \mathbb{Q}) \oplus (N_s' \otimes_{\mathbb{Z}} \mathbb{Q}).$$

It follows that $N_s \oplus N_s'$ has finite index in $\mathrm{End}(A_{s,\mathbb{C}})$.

We have $\mathrm{End}(A_{s,\mathbb{C}}) \cap L = N_s$ and $\mathrm{End}(A_{s,\mathbb{C}}) \cap L^\perp = N_s'$. If $x \in L$ and $y \in L^\perp$ are such that $(x, y) \in (L \oplus L^\perp) \cap \mathrm{End}(A_{s,\mathbb{C}})$, then both x and y have type $(0, 0)$, hence $x \in N_s$ and $y \in N_s'$. This shows that $(L \oplus L^\perp) \cap \mathrm{End}(A_{s,\mathbb{C}}) = N_s \oplus N_s'$. Using the fact that $\mathrm{End}(A_{s,\mathbb{C}})$ is saturated in $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}^1(A_{s,\mathbb{C}}, \mathbb{Z}))$, we deduce that the index of $N_s \oplus N_s'$ in $\mathrm{End}(A_{s,\mathbb{C}})$ divides the index of $L \oplus L^\perp$ in $\mathrm{End}_{\mathbb{Z}}(C(L))$. Hence $|\mathrm{discr}(N_s)|$ divides the product of $|\mathrm{discr}(\mathrm{End}(A_{s,\mathbb{C}}))|$ and a constant depending only on n. By Proposition 3.2 and Theorem 3.4, Coleman's conjecture implies that $|\mathrm{discr}(\mathrm{End}(A_{s,\mathbb{C}}))|$ is bounded. This finishes the proof. □

The construction of the orthogonal Shimura variety associated to a lattice of signature $(2, n)$ is functorial with respect to primitive embeddings of such lattices $\iota : L \hookrightarrow L'$. Indeed, ι induces an injective group homomorphism of algebraic groups $\mathbf{SO}(L)_{\mathbb{Q}} \to \mathbf{SO}(L')_{\mathbb{Q}}$ and thus an injective homomorphism $r : \mathbf{SO}(L)(\mathbb{A}_{\mathbb{Q},\mathrm{f}}) \to \mathbf{SO}(L')(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$. If $\mathbb{K} \subset \mathbf{SO}(L)(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ and $\mathbb{K}' \subset \mathbf{SO}(L')(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ are compact open subgroups such that $r(\mathbb{K}) \subset \mathbb{K}'$, then this gives rise to a finite morphism of $\mathbb{Q}$-varieties $f : \mathrm{Sh}_{\mathbb{K}}(L) \longrightarrow \mathrm{Sh}_{\mathbb{K}'}(L')$. When $\mathbb{K}'$ is torsion-free, this morphism is compatible with the associated variations of Hodge structures on L and L', as well as with the associated ℓ-adic sheaves. In particular, a $\mathbb{C}$-point x of $\mathrm{Sh}_{\mathbb{K}}(L)$ gives rise to an isometric embedding of associated $\mathbb{Z}$-Hodge structures $L_x \to L'_{f(x)}$.

We apply these considerations to orthogonal Shimura varieties related to moduli spaces of polarised K3 surfaces, giving a version of Zarhin's trick for K3 surfaces as proposed in [OS18] and [She]. For a positive integer d let Λ_{2d} be the lattice $E_8(-1)^{\oplus 2} \oplus U^{\oplus 2} \oplus \langle -2d \rangle$. There exist a positive integer n and a *unimodular* lattice $\Lambda_\#$ of signature $(2, n)$ such that for each $d \geq 1$ there is a primitive embedding $\Lambda_{2d} \to \Lambda_\#$. In the version of [OS18] this lattice has been chosen as the even lattice $E_8(-1)^{\oplus 3} \oplus U^{\oplus 2}$ (so that $n = 26$), using results of Nikulin. Here we follow a simpler version based on Lagrange's four squares theorem as in [She, Lemma 3.3.1] and set $\Lambda_\# = E_8(-1)^{\oplus 2} \oplus U^{\oplus 2} \oplus \langle -1 \rangle^{\oplus 5}$ (so that $n = 23$). For each d we pick a primitive embedding $\iota_d : \Lambda_{2d} \to \Lambda_\#$, inducing $r_d : \mathbf{SO}(\Lambda_{2d})(\mathbb{A}_{\mathbb{Q},\mathrm{f}}) \to \mathbf{SO}(\Lambda_\#)(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$.

If $\mathbb{K} \subset \mathbf{SO}(\Lambda_{2d})(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ and $\mathbb{K}_{\#} \subset \mathbf{SO}(\Lambda_{\#})(\mathbb{A}_{\mathbb{Q},\mathrm{f}})$ are compact open subgroups such that $r_d(\mathbb{K}) \subset \mathbb{K}_{\#}$, then there is a finite morphism of Shimura varieties over $\mathbb{Q}$

$$f_d : \mathrm{Sh}_{\mathbb{K}}(\Lambda_{2d}) \longrightarrow \mathrm{Sh}_{\mathbb{K}_{\#}}(\Lambda_{\#}).$$

Let M_{2d} be the coarse moduli space over $\mathbb{Q}$ of primitively polarised K3 surfaces of degree $2d$; this is a quasi-projective variety defined over $\mathbb{Q}$, see [Huy16, Ch. 5]. Let $\tilde{M}_{2d}$ be the coarse moduli space over $\mathbb{Q}$ of triples (X, λ, u) such that X is a K3 surface over a field of characteristic 0, λ is a primitive polarisation of X of degree $2d$, and u is an isometry

$$\det(P^2(\overline{X}, \mathbb{Z}_2(1))) \longrightarrow \det(\Lambda_{2d} \otimes_{\mathbb{Z}} \mathbb{Z}_2),$$

where $P^2(\overline{X}, \mathbb{Z}_2(1))$ is the orthogonal complement of the image of λ in the 2-adic étale cohomology $\mathrm{H}^2(\overline{X}, \mathbb{Z}_2(1))$. We have a double cover $\tilde{M}_{2d} \to M_{2d}$. By the work of Rizov and Madapusi Pera (based on the Torelli theorem), there is an open immersion $\tilde{M}_{2d} \hookrightarrow \mathrm{Sh}_{\mathbb{K}_d}(\Lambda_{2d})$ defined over $\mathbb{Q}$, where

$$\mathbb{K}_d = \{g \in \mathrm{SO}(\Lambda_{2d} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}) : g \text{ acts trivially on } \Lambda_{2d}^*/\Lambda_{2d}\}.$$

For a proof that this immersion is defined over $\mathbb{Q}$, see [MP15, Cor. 5.4] (see also [Riz10, Thm. 3.9.1] and [Tae]).

Theorem 5.2 *Coleman's conjecture about* $\mathrm{End}(\overline{A})$ *implies Shafarevich's conjecture about* $\mathrm{NS}\,(\overline{X})$.

Proof. Let k be a number field and let X be a K3 surface defined over k. Let d be a positive integer such that X has a polarisation of degree $2d$ over k. Then X gives rise to a k-point on M_{2d}. Replacing k by a quadratic extension, we can assume that this point lifts to a k-point x on $\tilde{M}_{2d} \subset \mathrm{Sh}_{\mathbb{K}_d}(\Lambda_{2d})$.

Let $\mathbb{K}_{\#} \subset \mathbf{SO}(\Lambda_{\#})(\hat{\mathbb{Z}})$ be the image of $\tilde{\mathbb{K}}_3 \subset \mathbf{GSpin}(\Lambda_{\#})(\hat{\mathbb{Z}})$. Define

$$\mathbb{K}'_d = r_d^{-1}(\mathbb{K}_{\#}) \cap \mathbb{K}_d.$$

By [Huy16, Ch. 14, Prop. 2.6], we have $r_d(\mathbb{K}_d) \subset \mathbf{SO}(\Lambda_{\#})(\hat{\mathbb{Z}})$. Hence $[\mathbb{K}_d : \mathbb{K}'_d] \leq [\mathbf{SO}(\Lambda_{\#})(\hat{\mathbb{Z}}) : \mathbb{K}_{\#}]$, that is, the index $[\mathbb{K}_d : \mathbb{K}'_d]$ is uniformly bounded. Thus replacing k by an extension of uniformly bounded degree we can assume that x lifts to a k-point x' on $\mathrm{Sh}_{\mathbb{K}'_d}(\Lambda_{2d})$.

We need to show that $|\mathrm{discr}(\mathrm{NS}\,(\overline{X}))|$ is universally bounded when $[k : \mathbb{Q}]$ is bounded. Choose an embedding $\bar{k} \hookrightarrow \mathbb{C}$. We have $\mathrm{NS}\,(\overline{X}) = \mathrm{NS}\,(X_{\mathbb{C}})$. Let $T(X_{\mathbb{C}}) \subset \mathrm{H}^2(X_{\mathbb{C}}, \mathbb{Z}(1))$ be the transcendental lattice of $X_{\mathbb{C}}$ defined as the orthogonal complement to $\mathrm{NS}\,(X_{\mathbb{C}})$ in $\mathrm{H}^2(X_{\mathbb{C}}, \mathbb{Z}(1))$ with respect to the bilinear form given by the cup-product. Since this form is unimodular, we have $|\mathrm{discr}(\mathrm{NS}\,(X_{\mathbb{C}}))| = |\mathrm{discr}(T(X_{\mathbb{C}}))|$, so it is enough to bound $|\mathrm{discr}(T(X_{\mathbb{C}}))|$.

Let $s = f_d(x') \in \mathrm{Sh}_{\mathbb{K}_{\#}}(\Lambda_{\#})$. The proof of [OS18, Lemma 4.3] shows that $\iota_d : \Lambda_{2d} \to \Lambda_{\#}$ induces an isometry $T(X_{\mathbb{C}}) \tilde{\longrightarrow} T_s$. Finally Proposition 5.1 tells us that $|\mathrm{discr}(T_s)|$ is bounded by a constant that depends only on $[k : \mathbb{Q}]$. □

6 Br(AV) implies Várilly-Alvarado

The main result of this section is that uniform boundedness of $\mathrm{Br}(\overline{A})^\Gamma$, for abelian varieties A of bounded dimension over number fields of bounded degree, implies Várilly-Alvarado's conjecture.

Before proving this main result, we relate two Galois representations attached to a polarised K3 surface (X, λ) defined over a number field k. Choose an isometry $u : \det(P^2(\overline{X}, \mathbb{Z}_2(1))) \to \det(\Lambda_{2d} \otimes_{\mathbb{Z}} \mathbb{Z}_2)$. After replacing k by a quadratic extension we can assume that Γ acts trivially on $\det(P^2(\overline{X}, \mathbb{Z}_2(1)))$. By [Sai12, Cor. 3.3] the quadratic character through which Γ acts on $\det(\mathrm{H}^2(\overline{X}, \mathbb{Q}_\ell(1)))$ does not depend on ℓ. Thus Γ acts trivially on $\det(P^2(\overline{X}, \mathbb{Z}_\ell(1)))$ for all primes ℓ, hence the representation $\rho_X : \Gamma \to \mathrm{O}(P^2(\overline{X}, \hat{\mathbb{Z}}(1)))$ attached to X takes values in $\mathrm{SO}(P^2(\overline{X}, \hat{\mathbb{Z}}(1)))$.

The triple (X, λ, u) defines a k-point x in $\tilde{M}_{2d} \subset \mathrm{Sh}_{\mathbb{K}_d}(\Lambda_{2d})$. Choose a torsion-free compact open subgroup $\mathbb{K}'_d \subset \mathbb{K}_d$ and let x' be a lift of x in $\mathrm{Sh}_{\mathbb{K}'_d}(\Lambda_{2d})$, defined over a finite extension k' of k. Let $\Gamma' = \mathrm{Gal}(\overline{k}/k')$ and let $\phi_{x'} : \Gamma' \to \mathrm{SO}(\Lambda_{2d} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}})$ denote the monodromy representation associated with the point x', as defined at (20).

Lemma 6.1 *The adelic Galois representations $\rho_{X|\Gamma'} : \Gamma' \to \mathrm{SO}(P^2(\overline{X}, \hat{\mathbb{Z}}(1)))$ and $\phi_{x'} : \Gamma' \to \mathrm{SO}(\Lambda_{2d} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}})$ are isometric.*

Proof. This is an immediate consequence of [MP16, Prop. 5.6(1)]. □

Theorem 6.2 *Assume that for every positive integer e, there exists $B = B(e) > 0$ such that every abelian variety A of dimension 2^{25} defined over a number field of degree at most e satisfies $|\mathrm{Br}(\overline{A})^\Gamma| < B$. Then for every pair of positive integers (e, M), there exists a constant $C = C(e, M)$ such that for every K3 surface X defined over a number field of degree e, if $|\mathrm{discr}(\mathrm{NS}\,(\overline{X}))| < M$, then $|\mathrm{Br}(\overline{X})^\Gamma| < C$.*

Proof. Let X be a K3 surface defined over a number field k. Let d be a positive integer such that X has a polarisation of degree $2d$ over k. After an extension of the field k of degree at most 2, X is represented by a k-point x of $\tilde{M}_{2d} \subset \mathrm{Sh}_{\mathbb{K}_d}(\Lambda_{2d})$.

Let Λ_{2d}, $\Lambda_\#$ and $\mathbb{K}_\#$, $\mathbb{K}'_d$ be the same as in the proof of Theorem 5.2. This proof shows that replacing k by an extension of uniformly bounded degree we can assume that x lifts to a k-point x' on $\mathrm{Sh}_{\mathbb{K}'_d}(\Lambda_{2d})$. Let $s = f_d(x') \in \mathrm{Sh}_{K_\#}(\Lambda_\#)$.

Write $\Lambda_{2d} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \Lambda_{2d,\ell}$ and $\Lambda_\# \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \Lambda_{\#,\ell}$. The injective homomorphism of $\mathbb{Z}$-modules $\iota_d : \Lambda_{2d} \to \Lambda_\#$ gives rise to an injective homomorphism of $\mathbb{Z}_\ell$-modules $\iota_{d,\ell} : \Lambda_{2d,\ell} \to \Lambda_{\#,\ell}$, which is also a homomorphism of Γ-modules (with respect to the Γ-module structures associated with the points $x' \in \mathrm{Sh}_{K'_d}(\Lambda_{2d})$ and $s \in \mathrm{Sh}_{K_\#}(\Lambda_\#)$ respectively). Using comparison theorems between classical and étale cohomology, and noting that $T(X_{\mathbb{C}}) = \mathrm{NS}\,(X_{\mathbb{C}})^\perp$, we see that $T(X_{\mathbb{C}})_\ell = T(X_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ has a canonical structure of a Γ-module. The proof of [OS18, Lemma 4.3], relying on [Zar83, Thm. 1.4.1], shows that $\iota_d(T(X_{\mathbb{C}})) = T_s$ (where T_s is defined in Proposition 5.1),

hence $\iota_{d,\ell}$ sends $T(X_{\mathbb{C}})_\ell$ isomorphically onto $T_{s,\ell} = T_s \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. By Lemma 6.1, we conclude that $\iota_{d,\ell}$ induces an isomorphism of Γ-modules $T(X_{\mathbb{C}})_\ell \xrightarrow{\sim} T_{s,\ell}$.

The Kummer exact sequence gives rise to short exact sequences of Γ-modules

$$0 \longrightarrow \mathrm{NS}\,(\overline{X})/\ell^n \longrightarrow \mathrm{H}^2(\overline{X}, \mu_{\ell^n}) \longrightarrow \mathrm{Br}(\overline{X})[\ell^n] \longrightarrow 0.$$

Since the intersection pairing on $\mathrm{H}^2(X_{\mathbb{C}}, \mathbb{Z}(1))$ is unimodular, and using again the comparison between Betti and étale cohomology, this implies that $\mathrm{Br}(\overline{X})[\ell^n] \cong \mathrm{Hom}(T(X_{\mathbb{C}})_\ell, \mathbb{Z}/\ell^n)$.

Therefore, it is enough to show that Br(AV) together with boundedness of $[k : \mathbb{Q}]$ and $\mathrm{discr}(\mathrm{NS}\,(\overline{X}))$ imply that

(1) there is a constant C such that $\mathrm{Hom}_\Gamma(T_{s,\ell}, \mathbb{Z}/\ell) = 0$ for any prime $\ell > C$, where s is any k-point of $\mathrm{Sh}_{\mathbb{K}}(\Lambda_\#)$;

(2) for each prime ℓ there is an integer $m \geq 0$ such that $\ell^m \mathrm{Hom}_\Gamma(T_{s,\ell}, \mathbb{Z}/\ell^n) = 0$ for any $n \geq 1$, where s is any k-point of $\mathrm{Sh}_{\mathbb{K}}(\Lambda_\#)$.

We assumed that $|\mathrm{discr}(\mathrm{NS}\,(\overline{X}))| = |\mathrm{discr}(T(X_{\mathbb{C}}))| = |\mathrm{discr}(T_s)| < M$, thus the natural homomorphism of abelian groups $T_s \to \mathrm{Hom}_{\mathbb{Z}}(T_s, \mathbb{Z})$ given by the intersection pairing is injective with cokernel of cardinality less than M. Hence if $\ell \geq M$, the Γ-modules $T_{s,\ell}/\ell$ and $\mathrm{Hom}(T_{s,\ell}, \mathbb{Z}/\ell)$ are canonically isomorphic, so to prove (1) it is enough to prove the following statement:

(1′) there is a constant C such that $(T_{s,\ell}/\ell)^\Gamma = 0$ for any prime $\ell > C$.

For any fixed prime ℓ we have an injective homomorphism of Γ-modules $T_{s,\ell} \to \mathrm{Hom}(T_{s,\ell}, \mathbb{Z}_\ell)$ with bounded cokernel. Thus, to prove (2) it is enough to prove

(2′) for each prime ℓ there is an integer $m \geq 0$ such that $[\ell^m] \cdot (T_{s,\ell}/\ell^n)^\Gamma = 0$ for all $n \geq 1$.

We use the notation of the proof of Proposition 5.1. Recall that $A = A_s$ is an abelian variety over k of fixed dimension $g = 2^{n+1}$ (where $\Lambda_\#$ has signature $(2, n)$ – recall that we can take $n = 23$). We have an injective homomorphism of $\mathbb{Z}$-Hodge structures $T_s \to \Lambda_{\#,s} \to \mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}))$. After tensoring with $\mathbb{Z}_\ell$ it gives rise to an injective homomorphism of Γ-modules $T_{s,\ell} \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$.

We equip $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}))$ with the unimodular symmetric bilinear form $\mathrm{Tr}(xy)$, where Tr is the usual matrix trace. After tensoring with $\mathbb{Z}_\ell$ this gives a Γ-invariant form on $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$ with values in $\mathbb{Z}_\ell$.

Let $T_s^\perp$ be the orthogonal complement to T_s in $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}))$ with respect to $\mathrm{Tr}(xy)$. Clearly $T_s^\perp$ is saturated in $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}))$. In the proof of Proposition 5.1 we observed that the restriction of $\mathrm{Tr}(xy)$ to T_s is the intersection form on T_s multiplied by 2^{n+2}. Since this form is non-degenerate, we have $T_s \cap T_s^\perp = 0$. The discriminant of T_s is bounded by assumption and $\mathrm{Tr}(xy)$ is unimodular, so

$$F = \mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}))/(T_s \oplus T_s^\perp)$$

is a finite abelian group of bounded size. We write $T_{s,\ell}^{\perp} = T_s^{\perp} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. This is the orthogonal complement to $T_{s,\ell}$ in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$, so is naturally a Γ-module. In particular, T_s/ℓ^n and $T_s^{\perp}/\ell^n$ are Γ-submodules of

$$\mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}))/\ell^n = \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))/\ell^n = \mathrm{End}_{\mathbb{F}_\ell}(A[\ell^n])$$

for any prime ℓ and any positive integer n.

The bilinear form $\mathrm{Tr}(xy)$ is compatible with the Hodge structure. Since $T_s \otimes \mathbb{Q}$ is an irreducible $\mathbb{Q}$-Hodge structure and contains elements of type $(1,-1)$, it follows that all elements of $\mathrm{End}_{\mathbb{Z}}(\mathrm{H}_1(A_{\mathbb{C}}, \mathbb{Z}))$ of Hodge type $(0,0)$ are orthogonal to T_s. In particular, $\mathrm{End}(A_{\mathbb{C}}) \subset T_s^{\perp}$. Since $\mathrm{End}(A_{\mathbb{C}})$ is saturated in $T_s^{\perp} \subset \mathrm{End}_{\mathbb{Z}}(H_1(A_{\mathbb{C}}, \mathbb{Z}))$, we also have $\mathrm{End}(A_{\mathbb{C}})/\ell^n \subset T_s^{\perp}/\ell^n$.

We shall first prove $(2')$. Fix an arbitrary prime ℓ and let ℓ^a be the highest power of ℓ dividing the exponent of F. Since $|F|$ is bounded, so is a. Applying the snake lemma to the self-map $[\ell^n]$ of the exact sequence of Γ-modules

$$0 \longrightarrow T_{s,\ell} \oplus T_{s,\ell}^{\perp} \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A)) \longrightarrow F[\ell^\infty] \longrightarrow 0$$

and then applying the left exact functor $-^{\Gamma}$, we get an exact sequence

$$0 \longrightarrow F[\ell^n]^{\Gamma} \longrightarrow (T_{s,\ell}/\ell^n)^{\Gamma} \oplus (T_{s,\ell}^{\perp}/\ell^n)^{\Gamma} \longrightarrow \mathrm{End}_{\Gamma}(A[\ell^n]). \tag{21}$$

By Proposition 4.11 there is a positive integer b that depends only on the upper bound for the cardinality of $\mathrm{Br}(\overline{A} \times \overline{A}^{\vee})^{\Gamma}$ such that $[\ell^b] \cdot \mathrm{End}_{\Gamma}(A[\ell^n])$ is contained in $\mathrm{End}(A)/\ell^n \subset \mathrm{End}_{\Gamma}(A[\ell^n])$. Recall that

$$\mathrm{End}(A)/\ell^n = \mathrm{End}(\overline{A})^{\Gamma}/\ell^n \subset (\mathrm{End}(A_{\mathbb{C}})/\ell^n)^{\Gamma} \subset (T_{s,\ell}^{\perp}/\ell^n)^{\Gamma}.$$

Let $x \in (T_{s,\ell}/\ell^n)^{\Gamma}$. Using (21), we see that there is a $y \in (T_{s,\ell}^{\perp}/\ell^n)^{\Gamma}$ such that $\ell^b x \oplus y$ is in the image of $F[\ell^n]^{\Gamma}$. Therefore, $\ell^a(\ell^b x \oplus y) = 0$ hence $\ell^m x = 0$, where $m = a+b$. This finishes the proof of $(2')$.

To prove $(1')$, note that if ℓ does not divide $|F|$, then $a = 0$ in the above argument. And by the second part of Proposition 4.11, we can take $b = 0$ for all primes ℓ greater than some constant depending only on the upper bound for $\mathrm{Br}(\overline{A} \times \overline{A}^{\vee})^{\Gamma}$. Thus for large enough primes ℓ, the above argument for $(2')$ shows that $(T_{s,\ell}/\ell)^{\Gamma} = 0$. $\square$

References

[And96] Y. André. On the Shafarevich and Tate conjectures for hyperkähler varieties. *Math. Ann.* **305** (1996) 205–248.

[BFGR06] N. Bruin, V.E. Flynn, J. González, and V. Rotger. On finiteness conjectures for endomorphism algebras of abelian surfaces. *Math. Proc. Cambridge Phil. Soc.* **141** (2006) 383–408.

[Cas78] J.W.S. Cassels. *Rational quadratic forms*. London Math. Soc. Monographs **13**, Academic Press, 1978.

[CM] A. Cadoret and B. Moonen. Integral and adelic aspects of the Mumford–Tate conjecture. *J. Inst. Math. Jussieu*, to appear. Preprint, available at `arXiv:1508.06426`.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983) 349366; Erratum **75** (1984) 381.

[Fal84] G. Faltings. Complements to Mordell. In: *Rational Points* (G. Faltings, G. Wüstholz et al.), Vieweg, 1984.

[Her68] I.N. Herstein. *Noncommutative rings*. Mathematical Association of America, 1968.

[Huy16] D. Huybrechts. *Lectures on K3 surfaces*. Cambridge Studies in Advanced Mathematics, Cambridge University Press, 2016.

[LOZ96] H.W. Lenstra, F. Oort, and Yu.G. Zarhin. Abelian subvarieties. *J. Algebra* **180** (1996) 513–536.

[MP15] K. Madapusi Pera. The Tate conjecture for K3 surfaces in odd characteristic. *Invent. Math.* **201** (2015) 625–668.

[MP16] K. Madapusi Pera. Integral canonical models for spin Shimura varieties. *Compos. Math.* **152** (2016) 769–824.

[Mor85] L. Moret-Bailly. Pinceaux de variétés abéliennes. *Astérisque* **129**, 1985.

[Mum74] D. Mumford. *Abelian varieties*. 2nd edition. Oxford University Press, 1974.

[MW95] D. W. Masser and G. Wüstholz. Refinements of the Tate conjecture and abelian varieties. *Abelian varieties* (Egloffstein, 1993), De Gruyter, 1995, pp. 211–223.

[Orr13] M. Orr. La conjecture d'André–Pink : Orbites de Hecke et sous-variétés faiblement spéciales. PhD thesis, Université Paris-Sud, 2013. Available at `http://tel.archives-ouvertes.fr/tel-00879010/`.

[OS18] M. Orr and A.N. Skorobogatov. Finiteness theorems for K3 surfaces and abelian varieties of CM type. *Compositio Math.* **154** (2018) 1571–1592.

[Rei03] I. Reiner. *Maximal orders*. London Mathematical Society Monographs. New Series **28**. The Clarendon Press, Oxford University Press, 2003.

[Rem18] G. Rémond. Conjectures uniformes sur les variétés abéliennes. *Quart. J. Math.* **69** (2018) 459–486.

[Riz10] J. Rizov. Kuga–Satake abelian varieties of K3 surfaces in mixed characteristic. *J. Reine Angew. Math.* **648** (2010) 13–67.

[Sai12] T. Saito. The discriminant and the determinant of a hypersurface of even dimension. *Math. Res. Lett.* **19** (2012) 855–871.

[Ser94] J.-P. Serre. Sur la semisimplicité des produits tensoriels de représentations de groupes. *Invent. Math.* **116** (1994) 513–530.

[Sha96] I.R. Shafarevich. On the arithmetic of singular K3-surfaces. *Algebra and analysis* (Kazan, 1994), De Gruyter, 1996, pp. 103–108.

[She] Y. She. The unpolarized Shafarevich conjecture for K3 surfaces. Preprint, available at `arXiv:1705.09038`.

[Sil92] A. Silverberg. Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra* **77** (1992) 253–262.

[SZ08] A.N. Skorobogatov and Yu.G. Zarhin. A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces. *J. Alg. Geom.* **17** (2008) 481–502.

[SZ14] A.N. Skorobogatov and Yu.G. Zarhin. The Brauer group and the Brauer–Manin set of products of varieties. *J. Eur. Math. Soc.* **16** (2014) 749–769.

[Tae] L. Taelman. Complex multiplication and Shimura stacks. Preprint, available at `arXiv:1707.01236`.

[UY13] E. Ullmo and A. Yafaev. Mumford–Tate and generalised Shafarevich conjectures. *Ann. Math. Québec* **37** (2013) 255–284.

[VA17] A. Várilly-Alvarado. Arithmetic of K3 surfaces. *Geometry over nonclosed fields* (eds. F. Bogomolov, B. Hassett, Y. Tschinkel), Simons Symposia **5**, Springer, 2017, pp. 197–248.

[Zar75] Yu.G. Zarhin. Endomorphisms of abelian varieties over fields of finite characteristic. *Izv. Akad. Nauk SSSR Ser. Matem.* **39** (1975) 272–277. English translation: *Math. USSR Izv.* **9** (1975) 255–260.

[Zar76] Yu.G. Zarhin. Abelian varieties in characteristic P. *Mat. Zametki* **19** (1976) 393–400. English translation: *Math. Notes* **19** (1976) 240–244.

[Zar77] Yu.G. Zarhin. Endomorphisms of abelian varieties and points of finite order in characteristic *p*. *Mat. Zametki* **21** (1977) 737–744. English translation: *Math. Notes* **21** (1977) 415–419.

[Zar83] Yu.G. Zarhin. Hodge groups of K3 surfaces. *J. Reine Angew. Math.* **341** (1983), 193–220.

[Zar85] 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.

Mathematics Institute, University of Warwick, Coventry CV4 7AL England, U.K.

`martin.orr@warwick.ac.uk`

Department of Mathematics, South Kensington Campus, Imperial College London, SW7 2BZ England, U.K. – and – Institute for the Information Transmission Problems, Russian Academy of Sciences, 19 Bolshoi Karetnyi, Moscow 127994 Russia

`a.skorobogatov@imperial.ac.uk`

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

`zarhin@math.psu.edu`