COHOMOLOGY OF VARIETIES OVER THE MAXIMAL KUMMER EXTENSION OF A NUMBER FIELD

DAVIDE LOMBARDO AND TAMÁS SZAMUELY

Abstract. Let X be a smooth projective geometrically connected variety defined over a number field K. We prove that the geometric étale cohomology of X with $\mathbf{Q}/\mathbf{Z}$-coefficients has finitely many classes invariant under the Galois group of the maximal Kummer extension of K in odd degrees. In particular, every abelian variety has finite torsion over the maximal Kummer extension. This improves results by Rössler and the second author as well as Murotani and Ozeki. We also show that finiteness of torsion of a given abelian variety over non-abelian solvable extensions of K is not controlled by the Galois group of the extension.

1. Introduction

Let K be a number field with fixed algebraic closure $\overline{K}$, and let X be a smooth projective geometrically connected variety over K. We denote by $\overline{X}$ the base change of X to $\overline{K}$, and for an intermediate field M with $\overline{K} \supset M \supset K$ we write $G_M := \mathrm{Gal}(\overline{K}|M)$. In this note we shall study the question of finiteness of the subgroup of G_M-invariants of the étale cohomology groups $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))$ over certain infinite extensions $M|K$. Note that when $X = A$ is an abelian variety with dual abelian variety A^*, the group $H^1_{\text{ét}}(\overline{A^*}, \mathbf{Q}/\mathbf{Z}(1))$ identifies with the torsion subgroup of $A(\overline{K})$ as a G_K-module (see, for instance, the introduction of [15]), so in this case G_M-invariants on cohomology correspond to M-rational torsion points of A.

In the paper just mentioned, Rössler and the second author considered the case when M is obtained by adjoining all roots of unity to K and proved finiteness of $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_M}$ for **odd** i. The method of proof generalized that of a much earlier theorem of Ribet [14] who proved finiteness of the torsion subgroup of M-points of an abelian variety for M as above.

But there are other infinite extensions $M|K$ over which finiteness of $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_M}$ holds for odd i. Indeed, recently Murotani and Ozeki [11] proved this for a large class of infinite Kummer extensions M of K. Here we extend their statement to all Kummer extensions.

Theorem 1.1. *Let K^{Kum} be the maximal Kummer extension of K, obtained by adjoining all roots of elements of K. The group $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_{K^{\mathrm{Kum}}}}$ is finite for all odd i and arbitrary j. In particular, the torsion subgroup of K^{Kum}-points of an abelian variety over K is finite.*

As already pointed out in [15, Remark 3.6], for even i the group $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_{K^{\mathrm{Kum}}}}$ is infinite because cycle classes on $X_{K^{\mathrm{Kum}}}$ generate an infinite subgroup. It is an interesting open question whether the quotient modulo cycle classes is finite. On the other hand, finiteness may fail already over infinite abelian extensions: for an abelian variety of CM type over K all torsion points are defined over the maximal abelian extension.

The Galois group of the field K^{Kum} over K is nilpotent of class 2. The proof of Theorem 1.1 will proceed by a general reduction to abelian extensions from solvable extensions of finite class:

Theorem 1.2. *Let K and X be as before, and let $M|K$ be a (possibly infinite) Galois extension contained in $\overline{K}$ such that* $\mathrm{Gal}(M|K)$ *is solvable of finite class. Fix integers $i \geq 0$ and j. Assume that for all finite extensions $K'|K$ contained in $\overline{K}$ and all subextensions $K' \subset F \subset K'M$ with $F|K'$ abelian the following conditions hold:*

(1) For all primes p we have $\left(H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{\text{ss}}\right)^{G_F} = 0$.

(2) For all but finitely many primes p we have $\left(H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{\text{ss}}\right)^{G_F} = 0$.

Then $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_M}$ is finite.

Here $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{\text{ss}}$ (resp. $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{\text{ss}}$) denotes the semisimplication of the module $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))$ (resp. $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))$) with respect to the action of $\mathrm{Gal}(\overline{K}|K)$. It is part of the Tate conjecture (at least with $\mathbf{Q}_p$-coefficients) that these actions are semisimple and thus the superscripts 'ss' can be omitted. If we assume semisimplicity, then in view of well-known arguments about abelian groups (see ([15, Lemma 2.1]) conditions (1) and (2) above can be replaced by the simpler condition that the group $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_F}$ is finite.

Remarks 1.3.

(1) In fact, we prove a slightly stronger statement: there exists a finite extension $K'|K$, depending only on i, j and X, such that if M is as in the theorem and all abelian extensions $F|K'$ contained in $K'M$ satisfy conditions (1) and (2), then $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_M}$ is finite. On the other hand, there may exist $K''|K$ finite (often we may take $K'' = K$; see Remark 3.4 (1)) such that (1) and (2) hold for all abelian $F|K''$ contained in $K''M$ but nevertheless finiteness of $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_M}$ fails.

(2) The semisimplicity conjecture with finite coefficients is perhaps less widely known. However, it is part of general motivic expectations and Corollary 1.3.4 (4) of [3] provides strong evidence for it: Cadoret, Hui and Tamagawa prove that over a finitely generated field of positive characteristic semisimplicity of cohomology with $\mathbf{Q}_p$-coefficients for p large enough (prime to the characteristic) implies semisimplicity with $\mathbf{Z}/p\mathbf{Z}$-coefficients for p large enough. The characteristic 0 analogue of this result would suffice for our purposes. Note also that by an observation of Moonen [10] semisimplicity in characteristic 0 with $\mathbf{Q}_p$-coefficients follows from the usual Tate conjecture on the image of the cycle map.

For an abelian variety A over K semisimplicity of the Galois action on the rational Tate module $V_p(A)$ and on p-torsion points (for p large enough) is known by classical work of Faltings and Zarhin (see e.g. Chapter IV by Schappacher in [5]). So in this case finiteness of torsion points of A over the maximal abelian extension $(K')^{\text{ab}}$ of every finite extension $K'|K$ implies finiteness over solvable extensions of finite class. In particular, plugging in a well-known result of Zarhin ([18], Corollary of Theorem 1) we obtain:

Corollary 1.4. *Let A be an abelian variety over K having no simple isogeny factor of CM type over the algebraic closure $\overline{K}$. Then A has finitely many torsion points over Galois extensions $M|K$ such that* $\mathrm{Gal}(M|K)$ *is solvable of finite class.*

This statement was also obtained using arguments similar to ours in very recent work of Huryn [6]. Huryn's preprint appeared while we were writing up the present note and we took the opportunity to borrow one of his arguments to simplify the proof of one of our lemmas (Lemma 3.2 below).

Observe that the conditions on the extensions of K appearing in Theorem 1.2 are purely Galois-theoretic. This prompts the question whether for fixed X, i and j there exists a Galois-theoretic criterion on extensions $M|K$ that ensures the finiteness of $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_M}$. Unfortunately, this is not the case:

Proposition 1.5. *There exist two infinite Galois extensions M, M' of $\mathbf{Q}$ with $\mathrm{Gal}(M|\mathbf{Q}) \cong \mathrm{Gal}(M'|\mathbf{Q})$ solvable of class 2 such that all abelian varieties defined over subfields of M have finite torsion subgroup over M but some abelian varieties defined over $\mathbf{Q}$ have infinite torsion over M'.*

After some preliminaries, Theorem 1.2 will be proven in Section 3. Theorem 1.1 will be deduced from Theorem 1.2 in Section 5 by means of an adjustment of arguments from [15]. The last section contains the proof of Proposition 1.5.

2. On a theorem of Serre and Wintenberger

During the proof of Theorem 1.2 we shall need a slight variation on a theorem contained in Wintenberger's paper [17] that has its origin in results explained by Serre in courses given at Collège de France in 1985/86. We begin by a list of conditions coming from Section 3.3 of [17].

Definition 2.1. Let K be a number field, p a prime, M_p a finite-dimensional $\mathbf{F}_p$-vector space, and $\rho_p : \mathrm{Gal}(\overline{K}|K) \to \mathrm{GL}(M_p)$ a Galois representation. Fix natural numbers d_0, b. We say that ρ_p is an *SW representation of type* (d_0, b) if the following hold:

1. The $\mathbf{F}_p$-dimension of M_p is at most d_0.
2. The representation ρ_p is semisimple.
3. Every inertia subgroup at a place of K not lying above p acts on M_p via a pro-p-quotient.
4. The weights of the action of the tame inertia subgroup at every place lying above p on M_p lie in the interval $[0, b]$.

Theorem 2.2. *Fix a number field K and natural numbers d_0 and b. There exists a finite extension $K'|K$ such that for all but finitely many primes p the derived subgroup of $\rho_p\big(\mathrm{Gal}(\overline{K}|K')\big)$ is a perfect group for every SW representation $\rho_p : \mathrm{Gal}(\overline{K}|K) \to \mathrm{GL}(M_p)$ of type (d_0, b).*

For the proof we need some auxiliary statements about algebraic groups over finite fields.

Lemma 2.3 (Borel-Tits)**.** *Let p be a prime number and N be a (connected) semisimple algebraic group over $\mathbf{F}_p$. Let $f : \widetilde{N} \to N$ be the universal cover of N and denote by $N(\mathbf{F}_p)_u$ the image of $\widetilde{N}(\mathbf{F}_p) \xrightarrow{f} N(\mathbf{F}_p)$. If $p > 3$, the group $N(\mathbf{F}_p)_u$ is perfect and coincides with the derived subgroup of $N(\mathbf{F}_p)$.*

Proof. See [2, 6.5 and 6.6] and [17, §1.2]. □

Proposition 2.4. *Let G be a connected reductive group over a finite prime field $\mathbf{F}_p$, and let $N = G'$ be its connected derived subgroup. If $p > 3$, we have an equality of groups of $\mathbf{F}_p$-points*

$$G(\mathbf{F}_p)' = N(\mathbf{F}_p)'.$$

Proof. It suffices to prove the containment $G(\mathbf{F}_p)' \subseteq N(\mathbf{F}_p)'$, the other one being obvious. By the lemma above we may replace $N(\mathbf{F}_p)'$ by $N(\mathbf{F}_p)_u = f\big(\widetilde{N}(\mathbf{F}_p)\big)$.

Write Z_G for the (scheme-theoretic) center of G and $G^{\mathrm{ad}} := G/Z_G$ for the adjoint quotient. The commutator morphism

$$c : G \times G \longrightarrow G, \qquad (g,h) \longmapsto [g,h] := g^{-1}h^{-1}gh$$

takes values in N (by definition of the derived subgroup) and is invariant under translation by $Z_G \times Z_G$ on the source. Hence c factors uniquely through the quotient

$$G \times G \longrightarrow (G/Z_G) \times (G/Z_G) = G^{\mathrm{ad}} \times G^{\mathrm{ad}},$$

yielding a morphism of $\mathbf{F}_p$-schemes $\alpha : G^{\mathrm{ad}} \times G^{\mathrm{ad}} \to N$ with $c = \alpha \circ \pi$, where $\pi : G \times G \to G^{\mathrm{ad}} \times G^{\mathrm{ad}}$ is the natural map.

Now note that G and $\tilde{N}$ have the same adjoint simple quotient, since both are given by $G/Z_G \cong N/(Z_G \cap N) \cong \widetilde{N}/Z_{\widetilde{N}}$, where $Z_{\widetilde{N}}$ denotes the center of $\widetilde{N}$. Moreover, since $\widetilde{N}$ is semisimple, it agrees with its own derived subgroup. Thus, the same construction as above, applied to $\widetilde{N}$, produces a morphism

$$\beta : \widetilde{N}^{\mathrm{ad}} \times \widetilde{N}^{\mathrm{ad}} = G^{\mathrm{ad}} \times G^{\mathrm{ad}} \longrightarrow \widetilde{N}$$

such that $f \circ \beta = \alpha$. Therefore, at the level of $\mathbf{F}_p$-points we obtain a map

$$\beta_p : G(\mathbf{F}_p) \times G(\mathbf{F}_p) \longrightarrow \widetilde{N}(\mathbf{F}_p)$$

such that for $g, h \in G(\mathbf{F}_p)$ we have

$$[g,h] = f\left(\beta_p(g,h)\right) \in f\big(\widetilde{N}(\mathbf{F}_p)\big),$$

which concludes the proof. □

Proof of Theorem 2.2. Given an SW representation ρ_p as above, Serre and Wintenberger construct algebraic subgroups G_p^{alg} and N_p of $\mathrm{GL}(M_p)$ and prove the existence of a finite extension $K'|K$ such that for all but finitely many p the following hold (see [17, §3.3, Théorème 4]):

(1) G_p^{alg} is a reductive group and N_p is its derived subgroup.
(2) We have the containments

$$N_p(\mathbf{F}_p)' \subset \rho_p(\mathrm{Gal}(\overline{K}|K'))) \subset G_p^{\mathrm{alg}}(\mathbf{F}_p).$$

(Note that Wintenberger states this with the subgroup $N_p(\mathbf{F}_p)_u$ instead of $N_p(\mathbf{F}_p)'$ but, as remarked above, the two are the same for $p > 3$.)

We now show that $N_p(\mathbf{F}_p)'$ equals the derived subgroup of $\rho_p(\mathrm{Gal}(\overline{K}|K'))$. This will prove the theorem as the group $N_p(\mathbf{F}_p)'$ is perfect by Lemma 2.3. Using the second containment in (2) we obtain

$$\left[\rho_p(\mathrm{Gal}(\overline{K}|K')),\ \rho_p(\mathrm{Gal}(\overline{K}|K'))\right] \subseteq \left[G_p^{\mathrm{alg}}(\mathbf{F}_p), G_p^{\mathrm{alg}}(\mathbf{F}_p)\right] = N_p(\mathbf{F}_p)'$$

where the last equality holds by Proposition 2.4. On the other hand, using the first containment in (2) we have

$$N_p(\mathbf{F}_p)' = \left[N_p(\mathbf{F}_p)',\ N_p(\mathbf{F}_p)'\right] \subseteq \left[\rho_p(\mathrm{Gal}(\overline{K}|K')),\ \rho_p(\mathrm{Gal}(\overline{K}|K'))\right],$$

where the first equality uses that $N_p(\mathbf{F}_p)'$ is perfect. Combining the above inclusions we deduce that the derived subgroup of $\rho_p(\mathrm{Gal}(\overline{K}|K'))$ is the perfect group $N_p(\mathbf{F}_p)'$, as desired. □

3. Proof of Theorem 1.2

We begin the proof of Theorem 1.2. As already noted in the introduction, the finiteness of $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_M}$ is equivalent to the vanishing of $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{G_M}$ for all primes p and of $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{G_M}$ for all but finitely many p (see [15], Lemma 2.1). Hence we first prove two auxiliary results, one with $\mathbf{Q}_p$-coefficients and one with $\mathbf{Z}/p\mathbf{Z}$-coefficients.

We formulate these for arbitrary finite-dimensional p-adic G_K-representations V_p stabilizing a $\mathbf{Z}_p$-lattice $T_p \subset V_p$. As before, V_p^{ss} denotes the semisimplification of V_p.

Proposition 3.1. *Assume that G_K has connected image in the automorphism group of V_p^{ss}. Let $M|K$ be a subextension of $\overline{K}|K$ with solvable Galois group of finite class. If for all abelian subextensions $F|K$ of $M|K$ we have $\left(V_p^{\text{ss}}\right)^{G_F} = 0$, then $V_p^{G_M} = 0$.*

The proof uses a group-theoretic lemma.

Lemma 3.2. *Let $G \subset \mathrm{GL}_n(\mathbf{Q}_p)$ be a connected reductive algebraic subgroup and $H \subset G(\mathbf{Q}_p)$ be an abstract subgroup, dense in the Zariski topology. Suppose that H is solvable of finite class as an abstract group. Then G is a torus.*

Proof. The following proof is inspired by [6, Proof of Theorem 1.1(a')]. Let $n \geq 1$ be such that H is n-step solvable. Consider the n-fold commutator map

$$D_n : G^{\times 2^n} \to G',$$

where G' denotes the derived subgroup of G. We claim that this map is surjective (in the algebraic sense). Indeed, the semisimple group G' coincides with its derived subgroup, which in particular gives surjectivity of $D_1 : G' \times G' \to G'$. Iterating this observation implies that $D_n : (G')^{\times 2^n} \to G'$ is surjective, and hence so is $D_n : G^{\times 2^n} \to G'$. By assumption, $H^{\times 2^n}$ is Zariski-dense in $G^{\times 2^n}$, and D_n is trivial on $H^{\times 2^n}$ since H is n-step solvable. This implies that D_n is the trivial map. Since it is also surjective, G' is the trivial group. A reductive group with trivial derived subgroup is a torus. □

Proof of Proposition 3.1. Assume $V_p^{G_M} \neq 0$, and hence also $W := (V_p^{\text{ss}})^{G_M} \neq 0$. As G_M is normal in G_K, the $\mathbf{Q}_p$-submodule $W \subset V_p^{\text{ss}}$ is G_K-stable, and the induced representation $\rho_W \colon G_K \longrightarrow \mathrm{Aut}_{\mathbf{Q}_p}(W)$ factors through $\mathrm{Gal}(M|K)$. In particular, $\rho_W(G_K)$ is a solvable group of finite class.

Denote by G_W the Zariski closure of $\rho_W(G_K)$ seen as an algebraic group over $\mathbf{Q}_p$. It is connected by assumption, and by construction it is a reductive group whose $\mathbf{Q}_p$-points contain $\rho_W(G_K)$ as a Zariski dense subgroup. Lemma 3.2 then shows that G_W is commutative. The fixed field F of $\ker(G_K \to G_W(\mathbf{Q}_p))$ is an abelian extension of K with $W \subset \left(V_p^{\text{ss}}\right)^{G_F}$ by construction. This proves $\left(V_p^{\text{ss}}\right)^{G_F} \neq 0$. □

Proposition 3.3. *Assume that the image of G_K in the automorphism group of $(T_p/pT_p)^{\text{ss}}$ has perfect derived subgroup. Let $M|K$ be a pro-solvable subextension of $\overline{K}|K$. If for all abelian subextensions $F|K$ of $M|K$ we have $((T_p/pT_p)^{\text{ss}})^{G_F} = 0$, then $(T_p/pT_p)^{G_M} = 0$.*

Proof. Assume $(T_p/pT_p)^{G_M} \neq 0$, and hence also $W_p := ((T_p/pT_p)^{\text{ss}})^{G_M} \neq 0$. As in the previous proof, the subspace W_p is G_K-stable and the induced representation $\rho_{W_p} \colon G_K \longrightarrow \mathrm{Aut}_{\mathbf{F}_p}(W_p)$ factors through $G = \mathrm{Gal}(M|K)$. Thus $\rho_{W_p}(G_K)$ is a finite solvable group.

Let $\rho_p\colon G_K \to \mathrm{Aut}_{\mathbf{F}_p}((T_p/pT_p)^{\mathrm{ss}})$ be the full mod p representation on $(T_p/pT_p)^{\mathrm{ss}}$, and let $e_{W_p}\colon \mathrm{Aut}_{G_K}((T_p/pT_p)^{\mathrm{ss}}) \to \mathrm{Aut}_{G_K}(W_p)$ be the natural projection. Then

$$\rho_{W_p}(G_K) = e_{W_p}\big(\rho_p(G_K)\big) \supseteq e_{W_p}\big(\rho_p(G_K)'\big).$$

By assumption $\rho_p(G_K)'$ is a perfect group, hence so is $e_{W_p}\big(\rho_p(G_K)'\big)$. As the latter group is contained in the solvable group $\rho_{W_p}(G_K)$, it must be trivial. Since applying e_{W_p} commutes with taking the derived subgroup, we get triviality of $e_{W_p}\big(\rho_p(G_K)\big)'$, which means that $\rho_{W_p}(G_K) = e_{W_p}\big(\rho_p(G_K)\big)$ is abelian. The fixed field F of $\ker(\rho_{W_p})$ is then an abelian extension of K contained in M such that $W_p \subset ((T_p/pT_p)^{\mathrm{ss}})^{G_F}$. It follows that $((T_p/pT_p)^{\mathrm{ss}})^{G_F} \neq 0$. □

Proof of Theorem 1.2. We take up the notation of the theorem. Recall from the beginning of this section that we have to prove $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{G_M} = 0$ for all primes p and $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{G_M} = 0$ for all but finitely many p. Set $V_p := H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))$ and let T_p be $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}_p(j))$ modulo its torsion subgroup. By a theorem of Larsen and Pink (see [8] or [7, Proposition 6.14]) there exists a finite extension $K'|K$ such that the image of $G_{K'}$ in $\mathrm{Aut}(V_p^{\mathrm{ss}})$ is connected. Hence condition (1) of the theorem implies the assumptions of Proposition 3.1 with K' in place of K, so that $V_p^{G_{K'M}} = 0$ and hence also $V_p^{G_M} = 0$.

The other half of the proof amounts to verifying that there exist a finite extension $K'|K$ as well as integers d_0 and b, all independent of p, so that $M_p := (T_p/pT_p)^{\mathrm{ss}}$ is an SW representation of $G_{K'}$ of type (d_0, b) as in Definition 2.1 for all but finitely many p. Then, after replacing K' by another finite extension, Theorem 2.2 gives that condition (2) of the theorem implies the assumptions of Proposition 3.3 with K' in place of K, so that $(T_p/pT_p)^{G_{K'M}} = (T_p/pT_p)^{G_M} = 0$ for all but finitely many p. Note that by comparison with singular cohomology over $\mathbf{C}$ one knows that $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}_p(j))$ is torsion free for p large enough, in which case $T_p/pT_p \cong H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))$. The same comparison shows that condition (1) of SW representations is satisfied for M_p for p large enough, with d_0 the i-th Betti number of $X(\mathbf{C})$; in fact, the $\mathbf{F}_p$-dimension of M_p equals this d_0 for p large enough. Condition (2) being automatic, we pass to (3). As explained in ([15], Lemma 3.3 (b)), a strong form of Grothendieck's local monodromy theorem implies that there is a finite extension $K'|K$ independent of p so that all inertia subgroups in $G_{K'}$ at places not lying above p act unipotently on V_p. It follows that these inertia subgroups act on T_p/pT_p with eigenvalues congruent to 1 mod p, and hence they act on M_p via a p-group. Finally, condition (4) is a consequence of Serre's tame inertia conjecture as proven by Caruso [4]. □

Remarks 3.4.

(1) One may ask whether Theorem 1.2 holds with $K' = K$, i.e. whether it is sufficient to check finiteness over abelian subextensions of $M|K$. The answer is negative, even when $i = j = 1$ and X is an abelian variety, as the following example shows.

Recall from the introduction that this case amounts to understanding the torsion subgroups of abelian varieties. Consider the elliptic curve E with Weierstrass equation $y^2 = x^3 + x$, with complex multiplication by $\mathbb{Z}[i]$ over $\mathbf{Q}(i)$. By the theory of complex multiplication the field M obtained by adjoining all torsion points of E to $\mathbf{Q}(i)$ is the maximal abelian extension of $\mathbf{Q}(i)$ (it is easy to show that $M|\mathbf{Q}(i)$ is abelian, and this is all we need). This implies that $M|\mathbf{Q}$ is a solvable extension, because both $M|\mathbf{Q}(i)$ and $\mathbf{Q}(i)|\mathbf{Q}$ are abelian. By construction, the torsion subgroup $E(M)_{\mathrm{tors}} \subset E(M)$ is infinite. On the other hand, since $\mathbf{Q}^{\mathrm{ab}} = \mathbf{Q}^{\mathrm{cyc}}$ by the Kronecker–Weber theorem, Ribet's result [14] shows that $E(\mathbf{Q}^{\mathrm{ab}})$ is finite, hence there is no abelian subextension F of $M|\mathbf{Q}$ such that $E(F)_{\mathrm{tors}}$ is infinite.

(2) Note that Proposition 3.3 holds for *pro*-solvable Galois groups and not just for solvable groups of finite class. Therefore the part of Theorem 1.2 concerning the triviality of $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{G_M}$ for all but finitely many p holds for $\mathrm{Gal}(M|K)$ prosolvable. In the case of the p-adic Tate module of an abelian variety, combining this more general form with Zarhin's theorem as in the proof of Corollary 1.4, one recovers [6, Theorem 1.1(b)]. We thank Jake Huryn for drawing our attention to this point.

4. Some lemmas from Galois theory

In this section we collect some statements about Galois extensions of number fields that will be used in the proof of Theorem 1.1.

Proposition 4.1. *Let K be a number field and denote by K^{Kum}, K^{ab}, and K^{cyc} its maximal Kummer, abelian and cyclotomic extensions, respectively (inside a fixed algebraic closure). We have*

$$K^{\mathrm{Kum}} \cap K^{\mathrm{ab}} = LK^{\mathrm{cyc}},$$

where $L \subset K^{\mathrm{ab}}$ is an abelian extension of K of finite exponent, linearly disjoint from K^{cyc} over K.

Proof. Writing $G := \mathrm{Gal}(K^{\mathrm{Kum}}|K)$, $\Gamma := \mathrm{Gal}(K^{\mathrm{cyc}}|K)$ and $A := \mathrm{Gal}(K^{\mathrm{Kum}}|K^{\mathrm{cyc}})$ we have a short exact sequence of profinite groups

$$1 \longrightarrow A \longrightarrow G \longrightarrow \Gamma \longrightarrow 1.$$

The groups A and Γ are abelian, and the conjugation action of G on A induces a Γ-action on A which we shall write additively. The maximal abelian quotient of G is given by

$$G^{\mathrm{ab}} \cong A_\Gamma \times \Gamma,$$

where $A_\Gamma := A/\langle(\gamma-1)A : \gamma \in \Gamma\rangle$ are the coinvariants of Γ on A.

The group G^{ab} is exactly the Galois group of $K^{\mathrm{Kum}} \cap K^{\mathrm{ab}}$ over K. Therefore $K^{\mathrm{Kum}} \cap K^{\mathrm{ab}}$ is the compositum of two linearly disjoint subextensions: the fixed field of A_Γ which is none other than K^{cyc}, and that of Γ which we denote by L. To finish the proof, we show that $A_\Gamma = \mathrm{Gal}(L|K)$ is of finite exponent. By definition, Γ is an open subgroup in $\widehat{\mathbf{Z}}^\times$, so it contains $\widehat{\mathbf{Z}}^{\times n}$ for some $n > 0$. In particular, Γ contains (say) the element $\gamma_0 := (3^n, 2^n, 2^n, \ldots) \in \prod_p \mathbf{Z}_p^\times \subset \widehat{\mathbf{Z}}$, and A_Γ is a quotient of $A/(\gamma_0 - 1)A$. Note that the subgroup topologically generated by $\gamma_0 - 1$ in $\widehat{\mathbf{Z}}$ contains $N\widehat{\mathbf{Z}}$, where $N := (2^n-1)(3^n-1)$. Therefore A_Γ is a quotient of A/NA, and as such it is of finite exponent dividing N. □

Remark 4.2. The extension $L|K$ is nontrivial in general. Indeed, if K contains the m-th roots of unity, then $K^{\mathrm{Kum}} \cap K^{\mathrm{ab}}$ contains $K(\sqrt[m]{K^\times})$, which is in general not contained in K^{cyc}. In the context of the above proof, if $\mu_m \subset K$, then $\gamma \equiv 1 \pmod{m}$ for all $\gamma \in \Gamma$, hence A_Γ surjects onto A/mA.

Definition 4.3. We shall say that an algebraic extension $L|\mathbf{Q}$ has *bounded local degrees* if there exists a constant $B \geq 1$ such that for every rational prime p and every place $w \mid p$ of L the completion L_w satisfies $[L_w : \mathbf{Q}_p] \leq B$.

Note that a finite extension $K|\mathbf{Q}$ has bounded local degrees (tautologically), and so does any abelian extension $L|K$ of finite exponent, by local class field theory and the structure of the multiplicative group of a p-adic field.

Lemma 4.4. *Let $L|\mathbf{Q}$ be an algebraic extension with bounded local degrees. Let $L^{\rm cyc}$ be its maximal cyclotomic extension, and let $L' \subset L^{\rm cyc}$ be the maximal subextension of $L^{\rm cyc}|L$ which is unramified at all finite places of L. Then L' has bounded local degrees.*

Proof. We may identify the Galois group $\Gamma := \mathrm{Gal}(L^{\rm cyc}|L)$ with a closed subgroup of $\hat{\mathbf{Z}}^\times$ via the adelic cyclotomic character. Consider a prime number p and a place w of L dividing p. As we have $[L_w : \mathbf{Q}_p] \le B$ (with B as in the definition above) and w is totally ramified in p-cyclotomic extensions of L_w, the inertia subgroup $I_w \subset \Gamma$ maps onto an open subgroup $I_p \subset \mathbf{Z}_p^\times$ of index $\le B$ via the p-adic cyclotomic character $\Gamma \to \mathbf{Z}_p^\times$. In any case, the index of I_p in $\mathbf{Z}_p^\times$ divides $B!$.

Set $I := \prod_p I_p \le \prod_p \mathbf{Z}_p^\times \simeq \widehat{\mathbf{Z}}^\times$. Since $\mathrm{Gal}(L^{\rm cyc}|L')$ is the closed subgroup of Γ generated by the inertia subgroups at all finite places of L, the group $\mathrm{Gal}(L'|L)$ identifies with a closed subgroup of $\widehat{\mathbf{Z}}^\times/I \cong \prod_p(\mathbf{Z}_p^\times/I_p)$ and as such has exponent dividing $B!$ by the arguments above. Since moreover $L'|L$ is an unramified extension, all decomposition subgroups in $\mathrm{Gal}(L'|L)$ above places of L are cyclic and hence must be of order dividing $B!$. This shows the boundedness of the local degrees of L' relative to L, from which the lemma follows. □

Corollary 4.5. *With notation as in the lemma, the largest subextension $L_p|L$ of $L^{\rm cyc}|L$ unramified outside the primes dividing p and ∞ is $L'(\mu_{p^\infty})$, the extension obtained by adjoining all p-power order roots of unity to L'. In particular, L_p is a p-cyclotomic extension of a field having bounded local degrees.*

Proof. The proof is identical to that of [14, Lemma on p. 316], except that Ribet works with a finite extension $k|\mathbf{Q}$ and takes the maximal subextension $k'|k$ of $k^{\rm cyc}|k$ unramified at the finite places, whereas we start with our L which may be an infinite extension of $\mathbf{Q}$ but has bounded local degrees. □

5. Proof of Theorem 1.1

We now return to the situation of the introduction. In particular, X is a smooth proper geometrically integral variety over a number field K with base change $\overline{X}$ to the algebraic closure $\overline{K}$. We take an abelian extension $L|K$ with bounded local degrees and maximal cyclotomic extension $L^{\rm cyc}$. As before, we write $G_{L^{\rm cyc}}$ for $\mathrm{Gal}(\overline{K}|L^{\rm cyc})$.

The remainder of the proof of Theorem 1.1 is a mild generalization of arguments from [15]. We state the two key propositions separately.

Proposition 5.1. *If i is odd, then $\left(H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{\rm ss}\right)^{G_{L^{\rm cyc}}} = 0$ for all primes p.*

Proof. The proof of [15, Proposition 3.1] goes through verbatim with Corollary 4.5 replacing Ribet's Galois-theoretic lemma cited above. We briefly review the argument. Pick a simple nonzero G_L-submodule $W \subset \left(H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{\rm ss}\right)^{G_{L^{\rm cyc}}}$. Note that G_L acts on W via $G_L/G_{L^{\rm cyc}}$ which is abelian, and that W is semisimple for this action. Using Grothendieck's local monodromy theorem one then shows that after taking a suitable finite extension of L the action of G_L on W is unramified outside p; thus by Corollary 4.5 it factors through $G_p := \mathrm{Gal}(L(\mu_{p^\infty})|L)$. For a place $w \mid p$ of L the extension $L_w|\mathbf{Q}_p$ is finite by our assumption on L and the local extension $L_w(\mu_{p^\infty})|L_w$ is totally ramified, hence the local Galois group of L_w surjects onto G_p. As in the original proof, after taking a further finite field extension the existence of the Hodge–Tate decomposition and the Weil conjectures (Deligne's theorem) force a Frobenius at a place of good reduction $w \nmid p$ to have eigenvalues that are both integral powers of Nw and of absolute value $(Nw)^{i/2-j}$, which is impossible for odd i. □

Proposition 5.2. *If i is odd, then $\big(H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{\text{ss}}\big)^{G_{L^{\text{cyc}}}} = 0$ for all but finitely many primes p.*

Proof. Here we adapt the proof of [15, Proposition 3.4]; note some similarities with the proof of Theorem 1.2.

We may replace L by a finite extension at any point of the proof. Assume for contradiction that there are infinitely many primes p for which $\big(H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{\text{ss}}\big)^{G_{L^{\text{cyc}}}} \neq 0$. For such a p pick a simple nonzero G_L-submodule $W_p \subset \big(H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{\text{ss}}\big)^{G_{L^{\text{cyc}}}}$. As in the proof of [15, Proposition 3.4], using Corollary 4.5 and a refined form of the local monodromy theorem that results from de Jong's alteration method one may ensure that, after extending L if necessary and taking p large enough, the action of G_L on W_p factors through $\text{Gal}(L(\mu_p)|L)$ which is nontrivial for large p by our assumption on L. Thus W_p is one-dimensional over $\mathbf{Z}/p\mathbf{Z}$ and G_L acts via a power $\bar{\chi}_p^{n(p)}$ of the mod p cyclotomic character $\bar{\chi}_p$.

Now consider a place $v \mid p$ of L where X has good reduction. By Caruso's proof of Serre's tame inertia conjecture [4, Theorem 1.2], the tame inertia weights on $H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{\text{ss}}$ are bounded *uniformly* in p by a constant depending only on i and the absolute ramification index $e(v)$. Since $k|\mathbf{Q}$ has bounded local degrees, we have $e(v) \leq [k_v : \mathbf{Q}_p] \leq B$, hence there exists an N independent of p such that $n(p) \leq N$ for all p under consideration. (Here we use that, upon restriction to the inertia at v, the mod-p cyclotomic character $\bar{\chi}_p$ is a power of the fundamental inertia character of level 1 with exponent bounded by $e(v)$, so the boundedness of the inertia weights implies the boundedness of the possible exponents of $\bar{\chi}_p$.)

From this point on, the proof concludes as that of [15, Proposition 3.4]. One deduces from the above boundedness statement using elementary mod p reduction arguments that for p as above large enough, at a place $w \nmid p$ of good reduction of L the Frobenius F_w acts on a simple G_L-submodule of $\big(H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{\text{ss}}\big)^{G_{L^{\text{cyc}}}}$ as multiplication by an integral power of Nw, contradicting the Weil conjectures when i is odd. □

Finally, we arrive at:

Proof of Theorem 1.1. Suppose by contradiction that $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}/\mathbf{Z}(j))^{G_{K^{\text{Kum}}}}$ is infinite. By Theorem 1.2, there exist a finite extension $K'|K$ and an abelian subextension F of $K'K^{\text{Kum}}|K'$ such that at least one of the following holds:

(1) $\big(H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{\text{ss}}\big)^{G_F} \neq (0)$ for some prime p;
(2) $\big(H^i_{\text{ét}}(\overline{X}, \mathbf{Z}/p\mathbf{Z}(j))^{\text{ss}}\big)^{G_F} \neq (0)$ for infinitely many primes p.

Replacing K with K' (which is again a number field), we have an abelian extension $F|K$ contained in K^{Kum} for which (1) or (2) above holds. Applying Proposition 4.1, we find that F is the compositum of K^{cyc} and an abelian extension $L|K$ with bounded local degrees. Further replacing K with L, we obtain an extension $F|L$, where F is contained in L^{cyc} and (1) or (2) above holds. The two cases contradict Proposition 5.1 and Proposition 5.2, respectively. □

Remark 5.3. The finiteness of $H^i_{\text{ét}}(\overline{X}, \mathbf{Q}_p(j))^{G_{K^{\text{Kum}}}}$ for odd i was also obtained in ([11], Theorem 2.11) using results from [15].

6. Proof of Proposition 1.5

In this section we describe the example announced in Proposition 1.5. We begin with the construction of particular infinite solvable extensions of $\mathbf{Q}$.

Proposition 6.1. *Let K be a real quadratic field of odd conductor and class number 1. There exists an infinite sequence of rational primes $p_1 < p_2 < \dots$, each split in $\mathbb{Q}(i)$, and a totally real Galois extension $M|K$ with $\mathrm{Gal}(M|K) \cong H$, where*

$$H := \prod_{i \geq 1} H_i$$

with

$$H_i := (\mathbf{Z}/p_i\mathbf{Z})^\times \times (\mathbf{Z}/p_i\mathbf{Z})^\times,$$

such that moreover the group extension

$$1 \to H \to \mathrm{Gal}(M|\mathbf{Q}) \to \mathbf{Z}/2\mathbf{Z} \to 1$$

corresponding to the tower of fields $M|K|\mathbf{Q}$ splits as a semidirect product

$$\mathrm{Gal}(M|\mathbf{Q}) \cong H \rtimes \mathbf{Z}/2\mathbf{Z},$$

with the nontrivial element of $\mathbf{Z}/2\mathbf{Z}$ acting on H by swapping the $(\mathbf{Z}/p_i\mathbf{Z})^\times$-factors of each H_i.

The proof will use an easy lemma from group cohomology.

Lemma 6.2. *Let A be an abelian group, and make $\mathbf{Z}/2\mathbf{Z}$ act on $A \times A$ via swapping the factors. With the resulting $\mathbf{Z}/2\mathbf{Z}$-module structure we have $H^2(\mathbf{Z}/2\mathbf{Z}, A \times A) = 0$.*

Proof. In order not to confuse notation, denote by σ the nontrivial element of $\mathbf{Z}/2\mathbf{Z}$. By the description of the cohomology of cyclic groups we have $H^2(\mathbf{Z}/2\mathbf{Z}, A\times A) \cong (A\times A)^\sigma / N(A\times A)$, where $(A \times A)^\sigma$ is the subgroup of invariants and $N : A \times A \to A \times A$ is the norm map $(a_1, a_2) \mapsto (a_1, a_2) + (a_2, a_1)$. Since $(A \times A)^\sigma$ is the diagonal image of A in $A \times A$, it suffices to notice that for all $a \in A$ one has $(a, a) = (a, 0) + (0, a) = N(a, 0)$. □

Proof. We will obtain M as the increasing union of certain abelian extensions $L^{(n)}$ that satisfy

$$\mathrm{Gal}(L^{(n)}|K) \cong \prod_{i=1}^n H_i,$$

with $\mathbf{Z}/2\mathbf{Z}$ acting on $\prod_{i=1}^n H_i$ as in the statement. In turn, the extension $L^{(n)}$ will be constructed as the compositum of extensions $L_{p_1}, \dots, L_{p_n}$, so we start by describing the construction of a single L_p.

Let c be the conductor of K. We will choose our primes to be congruent to 1 modulo c and to 5 (mod 8). These conditions ensure that

1. p splits in $\mathcal{O}_K$ (the condition $p \equiv 1 \pmod{c}$ implies that p splits in $\mathbf{Q}(\zeta_c) \supseteq K$);
2. $4 \mid p-1$ but $8 \nmid p-1$. In particular, we will have $p \equiv 1 \pmod 4$, so that p splits in $\mathbb{Q}(i)$.

Since c is odd by assumption, the conditions are compatible and hence Dirichlet's theorem implies that there there exist infinitely many such primes. Fix one such p and write $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$. By the Grunwald–Wang theorem (see [1, Chapter X, Theorem 5] or [13, Theorem 9.2.8]) there is a cyclic extension $M_p|K$ with group $(\mathbf{Z}/p\mathbf{Z})^\times$ such that:

- there is only one prime in $\mathcal{O}_{M_p}$ above $\mathfrak{p}$ and the corresponding local extension is cyclic with group $(\mathbf{Z}/p\mathbf{Z})^\times$ (so the decomposition group at $\mathfrak{p}$ is all of $\mathrm{Gal}(M_p|K)$);
- $\mathfrak{p}'$ splits completely in M_p (so the corresponding local extensions are all trivial);
- M_p is a totally real number field (i.e., the infinite places of K split in M_p).

Note that condition (2) implies that we are not in the so-called *special case* of the Grunwald–Wang theorem, because in the notation of [1, Chapter X, Theorems 1 and 5] we have $m = 2^2 m'$ with m' odd and the inequality $2 > s \geq 2$ is not satisfied. So the theorem indeed applies and gives an extension $M_p|K$ with the local behaviour described above.

The extension $M_p|K$ is defined by a character χ of $\mathrm{Gal}(K^{\mathrm{ab}}|K)$. The conjugation action of the nontrivial element $\sigma \in \mathrm{Gal}(K|\mathbf{Q})$ on $\mathrm{Gal}(K^{\mathrm{ab}}|K)$ coming from the extension

$$1 \to \mathrm{Gal}(K^{\mathrm{ab}}|K) \to \mathrm{Gal}(K^{\mathrm{ab}}|\mathbf{Q}) \to \mathrm{Gal}(K|\mathbf{Q}) \to 1$$

defines another character χ^σ whose kernel fixes a Galois extension $M_p^\sigma|K$ with group $(\mathbf{Z}/p\mathbf{Z})^\times$. Its local behaviour at the primes above p is obtained by swapping $\mathfrak{p}$ and $\mathfrak{p}'$: the prime $\mathfrak{p}'$ is totally inert in $M_p|K$ and $\mathfrak{p}$ is completely split. Therefore the cyclic extensions M_p and M_p^σ are linearly disjoint over K as $\mathfrak{p}$ is totally inert in the first and splits completely in the second. Let $L_p := M_p M_p^\sigma$ be their compositum (it is also the Galois closure of M_p over $\mathbf{Q}$). We have $\mathrm{Gal}(L_p|K) \cong (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/p\mathbf{Z})^\times$; moreover, σ acts on $\mathrm{Gal}(L_p|K)$ by swapping the factors. Finally, applying Lemma 6.2 with $A = (\mathbf{Z}/p\mathbf{Z})^\times$ gives that $\mathrm{Gal}(L_p|\mathbf{Q})$ is a split extension of $\mathrm{Gal}(K|\mathbf{Q})$ by $\mathrm{Gal}(L_p|K)$, i.e. a semi-direct product $((\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/p\mathbf{Z})^\times) \rtimes \mathbf{Z}/2\mathbf{Z}$.

We now proceed inductively. Assume $L_{p_1}, \ldots, L_{p_n}$ have been constructed, and let p_{n+1} be a prime strictly larger than $p_1, \ldots, p_n$, congruent to 1 modulo c and to 5 modulo 8, and unramified in each of the fields $L_{p_1}, \ldots, L_{p_n}$. As noted above, there are infinitely many primes that satisfy the congruence conditions, and the unramifiedness condition excludes only finitely many of them. So such a p_{n+1} indeed exists. We carry out the above construction to obtain a field $L_{p_{n+1}}|K$ with

$$\mathrm{Gal}(L_{p_{n+1}}|K) \cong H_{n+1} = (\mathbf{Z}/p_{n+1}\mathbf{Z})^\times \times (\mathbf{Z}/p_{n+1}\mathbf{Z})^\times.$$

When we apply the Grunwald–Wang theorem as explained above, we further impose that the extension $L_{p_{n+1}}|K$ be locally trivial (hence in particular unramified) at all the finitely many primes above any of the rational primes that ramify in $L_{p_1}, \ldots, L_{p_n}$. It follows that the fields L_{p_i} for $1 \leq i \leq n+1$ are linearly disjoint over K. Indeed, the above ramification condition implies that the intersection of one of them with the compositum of the others is an everywhere unramified abelian extension of K. Since K has class number 1, this implies that the intersection must be K itself. Setting $L^{(n+1)} := L_{p_1} \cdots L_{p_{n+1}}$, we then have

$$\mathrm{Gal}(L^{(n+1)}|K) \;\cong\; \prod_{i=1}^{n+1} \mathrm{Gal}(L_{p_i}|K) \;\cong\; \prod_{i=1}^{n+1} H_i.$$

By construction we have $\mathrm{Gal}(L_{p_i}|\mathbf{Q}) \cong H_i \rtimes \mathbf{Z}/2\mathbf{Z}$ with the desired action of σ on H_i for each i, and moreover $L^{(n+1)}$ is stable by the action of $\mathbf{Z}/2\mathbf{Z}$. Hence $L^{(n+1)}$ is a Galois extension of $\mathbf{Q}$ which is moreover totally real as so are the L_{p_i}.

Finally, as already noted at the beginning of the proof, to complete the construction it suffices to take $M = \bigcup_n L^{(n)}$. □

Remark 6.3. Related results on the existence of Galois extensions of $\mathbf{Q}$ with solvable Galois group and prescribed local conditions are proven, for example, in [12, Theorem 6.6]. However, it seems that Neukirch's statements do not immediately apply in the context of our inductive construction.

We now construct the other field extension required by Proposition 1.5.

Proposition 6.4. *Let E be an elliptic curve E defined over $\mathbf{Q}$ that has CM by $\mathbf{Z}[i]$, and let $p_1 < p_2 < \dots$ be a sequence of primes of good reduction for E that split completely in $\mathbf{Q}(i)$. There exists a Galois extension $M'|\mathbf{Q}$ containing $\mathbf{Q}(i)$ such that E has infinite torsion over M' and moreover $\mathrm{Gal}(M'|\mathbf{Q}) \cong H \rtimes \mathbf{Z}/2\mathbf{Z}$, where $H = \prod_i (\mathbf{Z}/p_i\mathbf{Z})^\times \times (\mathbf{Z}/p_i\mathbf{Z})^\times)$ and $\mathbf{Z}/2\mathbf{Z}$ acts by swapping the $(\mathbf{Z}/p_i\mathbf{Z})^\times$-factors.*

Proof. Let first p be any prime of good reduction for E that splits in $\mathbf{Q}(i)$, and consider the representation $\rho_p : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(i)) \to \mathrm{End}_{\mathbf{F}_p}(E[p])$ on the p-torsion points of an elliptic curve E as above. Since E has CM by $\mathbf{Z}[i]$, Corollary 2 to Theorem 5 of [16] implies that ρ_p factors through an injection $(\mathbf{F}_p^2)^\times \hookrightarrow \mathrm{End}_{\mathbf{F}_p}(E[p])$, yielding a map $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(i))^{\mathrm{ab}} \to (\mathbf{F}_p^2)^\times$. On the other hand, since $\mathbf{Q}(i)$ has class number 1, class field theory gives a surjection $r : \prod_{v\in\Omega_{\mathbf{Q}(i)}} \mathcal{O}^\times_{\mathbf{Q}(i),v} \to \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(i))^{\mathrm{ab}}$ where $\Omega_{\mathbf{Q}(i)}$ denotes the set of finite places of $\mathbf{Q}(i)$. Composing the two we obtain a map $\prod_{v\in\Omega_{\mathbf{Q}(i)}} \mathcal{O}^\times_{\mathbf{Q}(i),v} \to (\mathbf{F}_p^2)^\times$. By the results of [16] summarized in [9, Theorem 5.1], this map sends $(a_v)_{v\in\Omega_{\mathbf{Q}(i)}}$ to $(a_{\mathfrak{p}}^{-1}, a_{\mathfrak{p}'}^{-1}) \bmod p$. (Indeed, note that in the formula of *loc. cit.* the maps N_{K_ℓ/E_ℓ^*}, $\Phi_{E,S}$ and ε are all trivial in our case, the first two because we are dealing with a CM elliptic curve over $\mathbf{Q}(i)$ and the last one because $\mathfrak{p}$, $\mathfrak{p}'$ are primes of good reduction for E.) In particular, this map is the sum of two surjective characters with values in $(\mathbf{Z}/p\mathbf{Z})^\times$.

Now let $p_1 < p_2 < \dots$ be the sequence of completely split primes of good reduction as in the assumption. With this choice of primes consider the product representation

$$\prod_i \rho_{p_i} : \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(i)) \to \prod_i \mathrm{End}_{\mathbf{F}_{p_i}}(E[p_i]).$$

Factoring through the $(\mathbf{F}_{p_i}^2)^\times$ and composing with r as above we obtain a surjection

$$\prod_i \left(\mathcal{O}^\times_{\mathbf{Q}(i),\mathfrak{p}_i} \times \mathcal{O}^\times_{\mathbf{Q}(i),\mathfrak{p}'_i}\right) \twoheadrightarrow \prod_i ((\mathbf{Z}/p_i\mathbf{Z})^\times \times (\mathbf{Z}/p_i\mathbf{Z})^\times) = H.$$

Thus H arises as a quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(i))$, corresponding to a field extension $M'|\mathbf{Q}(i)$. Since the action of $\mathrm{Gal}(\mathbf{Q}(i)|\mathbf{Q})$ exchanges the primes $\mathfrak{p}_i$ and $\mathfrak{p}'_i$, its action on $\mathrm{Gal}(M'|\mathbf{Q}(i))$ exchanges the $(\mathbf{Z}/p_i\mathbf{Z})^\times$-factors in H. Thus, again using Lemma 6.2, we obtain that $\mathrm{Gal}(M'|\mathbf{Q})$ is a semidirect product $H \rtimes \mathbf{Z}/2\mathbf{Z}$ as in the statement.

Finally, note that by construction $\mathrm{Gal}(\overline{\mathbf{Q}}|M')$ fixes the p_i-torsion points of E for all i, so that E has infinite torsion over M'. □

Proof of Proposition 1.5. Take an elliptic curve E as in Proposition 6.4 and choose a sequence of primes $p_1 < p_2 < \cdots$ as in Proposition 6.1. Leaving out finitely many of the p_i we may assume they are all of good reduction for E. Construct the extensions M and M' of Propositions 6.1 and 6.4 with this sequence of primes. They have isomorphic Galois groups over $\mathbf{Q}$ that are solvable of class 2, and we also know that E has infinite torsion over M'. On the other hand, note that every abelian variety defined over the totally real field M is defined over some totally real subfield $\widetilde{M} \subset M$ finite over $\mathbf{Q}$ and in particular cannot have CM defined over $\widetilde{M}$. Therefore by the result of Zarhin already cited in the introduction ([18], Corollary of Theorem 1) it has finite torsion over every abelian extension of $\widetilde{M}$, and in particular over M. □

Remark 6.5. To be somewhat more concrete, in Proposition 6.4 we can work with the elliptic curve E of Weierstrass equation $y^2 = x^3 + x$ that has CM by $\mathbf{Z}[i]$ and 2 as its only prime of bad reduction. Then in Proposition 6.1 we may take $K = \mathbf{Q}(\sqrt{5})$ that has class number 1 and conductor 5. For the sequence of primes $p_1 < p_2 < \cdots$ we can take any sequence provided by Proposition 6.1 provided that $p_1 \neq 2$.

References

[1] Emil Artin and John Tate. *Class field theory.* AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[2] Armand Borel and Jacques Tits. Homomorphismes “abstraits” de groupes algébriques simples. *Ann. of Math. (2)*, 97:499–571, 1973.

[3] Anna Cadoret, Chun Yin Hui, and Akio Tamagawa. $\mathbb{Q}_\ell$- versus $\mathbb{F}_\ell$-coefficients in the Grothendieck-Serre/Tate conjectures. *Isr. J. Math.*, 257(1):71–101, 2023.

[4] Xavier Caruso. Conjecture de l’inertie modérée de Serre. *Invent. Math.*, 171(3):629–699, 2008.

[5] Gerd Faltings and Gisbert Wüstholz, editors. *Rational points. Seminar Bonn/Wuppertal 1983/84. 2nd ed*, volume E6 of *Aspects Math.* Springer, Wiesbaden, 1986.

[6] Jake Huryn. Torsion of abelian varieties over solvable extensions of number fields, preprint, 2025. Available at `https://arxiv.org/abs/2510.24588`.

[7] Michael Larsen and Richard Pink. On l-independence of algebraic monodromy groups in compatible systems of representations. *Invent. Math.*, 107(3):603–636, 1992.

[8] Michael Larsen and Richard Pink. A connectedness criterion for ℓ-adic galois representations. *Israel J. Math.*, 97:1–10, 1997.

[9] Davide Lombardo. Galois representations attached to abelian varieties of CM type. *Bull. Soc. Math. France*, 145(3):469–501, 2017.

[10] Ben Moonen. A remark on the Tate conjecture. *J. Algebr. Geom.*, 28(3):599–603, 2019.

[11] Takahiro Murotani and Yoshiyasu Ozeki. Some Kummer extensions over maximal cyclotomic fields, a finiteness theorem of Ribet and TKND-AVKF fields. *Int. Math. Res. Not.*, 2025(14):20, 2025. Id/No rnaf209.

[12] Jürgen Neukirch. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.*, 21:59–116, 1973.

[13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren Math. Wiss.* Berlin: Springer, 2nd ed. edition, 2008.

[14] Kenneth A. Ribet. Torsion points of abelian varieties in cyclotomic extensions, appendix to N. M. Katz and S. Lang, Finiteness theorems in geometric class field theory. *L’Enseignement Mathématique*, 27(1–2):315–319, 1981.

[15] Damian Rössler and Tamás Szamuely. Cohomology and torsion cycles over the maximal cyclotomic extension. *J. reine angew. Math.*, 752:211–227, 2019.

[16] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. Math. (2)*, 88:492–517, 1968.

[17] Jean-Pierre Wintenberger. Démonstration d’une conjecture de Lang dans des cas particuliers. *J. reine angew. Math.*, 553:1–16, 2002.

[18] Yuri G. Zarhin. Endomorphisms and torsion of abelian varieties. *Duke Math. J.*, 54(1):131–145, 1987.

Università degli studi di Pisa, Pisa, Italy
Email address: `davide.lombardo@unipi.it`
Email address: `tamas.szamuely@unipi.it`