Weil–Châtelet divisible elements in Tate–Shafarevich groups I: The Bashmakov problem for elliptic curves over $\mathbb{Q}$

Mirela Çiperiani and Jakob Stix

Abstract

For an abelian variety A over a number field k we discuss the maximal divisibile subgroup of $\mathrm{H}^1(k, A)$ and its intersection with the subgroup $Ш(A/k)$. The results are most complete for elliptic curves over $\mathbb{Q}$.

1. Introduction

1.1 The Bashmakov problem

Let A/k be an abelian variety over an algebraic number field k with algebraic closure k^{alg}. Bashmakov [Ba64, Ba72], studied the question of whether elements of the Tate–Shafarevich group

$$Ш(A/k)$$

become divisible in the Weil–Châtelet group $\mathrm{H}^1(k, A) = \mathrm{H}^1(k, A(k^{\mathrm{alg}}))$, i.e., lie in the subgroup

$$\mathrm{div}(\mathrm{H}^1(k, A))$$

of divisible elements. This question was initially asked by Cassels in the case of elliptic curves (see [Ca62] Problem 1.3) because an affirmative answer would prove that the kernel of the Cassels' pairing equals the maximal divisible subgroup of the Tate-Shafarevich group.

Bashmakov [Ba64] also investigates whether $Ш(A/k)$ can meet the maximal divisible subgroup of $\mathrm{H}^1(k, A)$,

$$\mathrm{Div}(\mathrm{H}^1(k, A)),$$

in a nontrivial way, see also [HS09] §4. Bashmakov's results are recalled in Section §4. In other words, the Cassels–Bashmakov problem considers the filtration

$$\mathrm{H}^1(k, A) \supseteq \mathrm{div}(\mathrm{H}^1(k, A)) \supseteq \mathrm{Div}(\mathrm{H}^1(k, A)) \supseteq 0 \tag{1.1}$$

and intersects it with $Ш(A/k)$. Observe that $\mathrm{div}(\mathrm{H}^1(k, A))$ is generally strictly larger than the maximal divisible subgroup $\mathrm{Div}(\mathrm{H}^1(k, A))$, see Section §1.4.2 and Section §8.

In this article we focus on Bashmakov's question on the intersection of the Tate-Shafarevich group and the maximal divisible subgroup of the Weil-Châtelet group. We address Cassels' original question in a separate article [ÇS12].

2010 Mathematics Subject Classification 11G05, 11G10.
Keywords: Elliptic Curve, Abelian Variety, Selmer Group, Weil-Châtelet Group, Tate-Shafarevich Group.
The authors acknowledge the hospitality and support provided by MATCH and the Newton Institute.
The first author was partially supported by an NSF and an NSA grant during the preparation of this manuscript.

Our motivation for studying the Cassels–Bashmakov problem is twofold. The group $Ш(A/k)$ conjecturally has no divisible elements, and this is known for elliptic curves over $\mathbb{Q}$ of analytic rank $\leqslant 1$. The study of $Ш(A/k)$ in the bigger group $\mathrm{H}^1(k, A)$ may shed some light on the structure of $Ш(A/k)$ itself in the general case.

Secondly, the Bashmakov problem arises naturally in anabelian geometry when one wants to get hold on the index of a hyperbolic curve and therefore passes to the abelianization in form of the universal Albanese torsor. The connection[1] more precisely is as follows. Let W be a principal homogeneous space of A over k, with a geometric point $\bar{w}$ of the base change $\overline{W} = W \times_k k^{\mathrm{alg}}$. Let $\mathrm{Gal}_k = \mathrm{Gal}(k^{\mathrm{alg}}/k)$ be the absolute Galois group k. A section of the fundamental exact sequence

$$1 \to \pi_1(\overline{W}, \bar{w}) \to \pi_1(W, \bar{w}) \to \mathrm{Gal}_k \to 1,$$

yields that the corresponding class $[W] \in \mathrm{H}^1(k, A)$ lies in the maximal divisible subgroup, see [HS09] and also [Sx12] Remark 176(3). If, in addition, local points exist on W, then $[W]$ belongs to $Ш(A/k)$ and the existence of a global k-rational point follows from a negative answer to the Bashmakov problem for A/k, see again [HS09] §4 and also [Sx12] §13.

1.2 Summary of results

In view of the conjectured finiteness of $Ш(A/k)$ the triviality of the p-primary part of

$$\mathrm{Div}(\mathrm{H}^1(k, A)) \cap Ш(A/k).$$

should be guaranteed for large primes p depending on A/k. Our aim therefore is to identify conditions on a prime number p which imply the triviality of the p-primary part of the intersection of the Tate-Shafarevich group with the maximal divisible subgroup of the Weil-Châtelet group without relying on the triviality of $Ш(A/k)_p$.

When we can answer the Bashmakov problem in the negative, i.e., when we can prove that $\mathrm{Div}(\mathrm{H}^1(k, A))$ intersects $Ш(A/k)$ trivially, our method actually shows more. In order to present the results, we define the **locally divisible** H^1 as the kernel

$$\mathrm{H}^1_{\mathrm{div}}(k, A) = \ker\Big(\mathrm{H}^1(k, A) \to \bigoplus_v \mathrm{H}^1(k_v, A)/\operatorname{div}\big(\mathrm{H}^1(k_v, A)\big)\Big).$$

Since $\mathrm{div}(-)$ is a functor, we find

$$\mathrm{div}(\mathrm{H}^1(k, A)) \subseteq \mathrm{H}^1_{\mathrm{div}}(k, A).$$

Focusing on the p-part and using local Tate duality $\mathrm{H}^1(k_v, A) = \mathrm{Hom}(A^t(k_v), \mathbb{Q}/\mathbb{Z})$ we find for $v \nmid p$ that $\mathrm{div}(\mathrm{H}^1(k_v, A)_{p^\infty}) = 0$ and therefore an exact sequence

$$0 \to Ш(A/k)_{p^\infty} \to \mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty} \to \bigoplus_{v|p} \operatorname{div}\big(\mathrm{H}^1(k_v, A)_{p^\infty}\big) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\dim(A)\cdot[k:\mathbb{Q}]}. \tag{1.2}$$

Concerning the relative position of $Ш(A/k)$ and $\mathrm{Div}(\mathrm{H}^1(k, A))$ our main result is for an elliptic curve $E/\mathbb{Q}$ under the assumption of trivial analytic rank (see Sect. §7.2). The following theorem is a summary of the results in this direction (part (4) follows essentially from [HS09] Cor 4.2.).

Theorem A. *Let $E/\mathbb{Q}$ be an elliptic curve.*

(1) *If $E/\mathbb{Q}$ has trivial algebraic rank, then $\mathrm{Div}(\mathrm{H}^1(\mathbb{Q}, E))$ contains a copy of $\mathbb{Q}/\mathbb{Z}$.*

[1] The authors acknowledge the influence of work of Harari and Szamuely for bringing the results of Bashmakov to their attention and for informing the first author about their value from the point of view of anabelian geometry.

(2) *If $E/\mathbb{Q}$ has trivial analytic rank, then* $\mathrm{Div}(\mathrm{H}^1(\mathbb{Q},E)) = \mathbb{Q}/\mathbb{Z}$ *and, for odd primes p of good reduction such that the* $\mathrm{Gal}_{\mathbb{Q}}$*-representation on the p-torsion E_p is irreducible, we find*

$$Ш(E/\mathbb{Q})_{p^\infty} \oplus \mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q},E)\right)_{p^\infty} = \mathrm{H}^1_{\mathrm{div}}(\mathbb{Q},E)_{p^\infty}.$$

(3) *If $E/\mathbb{Q}$ has positive algebraic rank, then* $\mathrm{Div}(\mathrm{H}^1(\mathbb{Q},E)) = \mathrm{Div}(Ш(E/\mathbb{Q}))$.

(4) *If $E/\mathbb{Q}$ has analytic rank* 1*, then* $\mathrm{Div}(\mathrm{H}^1(\mathbb{Q},E)) = 0$.

Remark 1. Observe that the $\mathrm{Gal}_{\mathbb{Q}}$-representation on E_p is irreducible for all

$$p \neq 2,3,5,7,11,13,17,19,37,43,67,163$$

and for all $p > 7$ if E is semistable (see [Ma78]).

With respect to the filtration (1.1) we deduce that even if $\mathrm{Div}(\mathrm{H}^1(\mathbb{Q},E))$ is non-trivial, it can be strictly smaller than $\mathrm{div}(\mathrm{H}^1(\mathbb{Q},E))$. Moreover, it turns out that an old example of Selmer provides an example where the Tate–Shafarevich group intersects the maximal divisible group nontrivially, see Section §8 for the following.

Theorem B. *The Tate-Shafarevich group* $Ш(E/\mathbb{Q})$ *can intersect* $\mathrm{Div}(\mathrm{H}^1(\mathbb{Q},E))$ *non-trivially for an elliptic curve $E/\mathbb{Q}$ of trivial analytic rank. In particular, the Selmer curve*

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

represents a nontrivial class in

$$Ш(E/\mathbb{Q}) \cap \mathrm{Div}(\mathrm{H}^1(\mathbb{Q},E))$$

with E the Jacobian of the Selmer curve.

1.3 Plan of the paper

In Section §2 and Section §3 we discuss background from Galois cohomology and étale cohomology. The material of Section §3 is only used in Section §4, where we discuss Bashmakov's work, and in Section §8, where we prove Theorem B. Theorem A is proven in Section §7 based on the computation of a generalized Selmer group done in Section §6 which in turn depends on some group theory in $\mathrm{GL}_2(\mathbb{F}_\ell)$ that is discussed in Section 5.

Acknowledgements

The authors would like to thank Dorian Goldfeld, David Harari, Ken Ribet and Tamás Szamuely for several useful discussions. The first author is also grateful to her advisor, Andrew Wiles, for introducing her to this method of thinking about the p-divisibility of the Tate-Shafarevich group. Finally, we would also like to thank the referees for several helpful suggestions.

1.4 Notation

We fix some notation which will be in use throughout the text.

1.4.1 *On number fields* In the sequel, we let k be an algebraic number field, i.e., a finite extension of $\mathbb{Q}$. The completion of k at a place v is k_v. For a finite Gal_k-module M the field extension $k(M)/k$ is the fixed field of k^{alg} under $\ker(\mathrm{Gal}_k \to \mathrm{Aut}(M))$.

We set $X = \mathrm{Spec}(\mathfrak{o}_k)$ with the ring of integers $\mathfrak{o}_k$ in k. The finite places of k will be identified with the closed points of X. An abelian variety A/k with good reduction over a nonempty open

$U \subset X$ extends to an abelian scheme over U that we denote by A/U by abuse of notation.

1.4.2 *On abelian groups* Let M be an abelian group. The n-torsion subgroup is denoted by by M_n, and M_{p^∞} denotes the p-primary torsion $\bigcup_n M_{p^n}$. The subgroup

$$\operatorname{div}(M) = \bigcap_{n \geqslant 1} nM$$

of divisible elements of M contains the maximal divisible subgroup

$$\operatorname{Div}(M)$$

of M, which equals $\bigcup \operatorname{im}(\varphi)$ for all $\varphi : \mathbb{Q} \to M$. For matters of clarity we will distinguish between **"a is divisible by p"**, meaning there is a' with $a = pa'$, and **"a is p-divisible"**, which means that for every $n \geqslant 1$ there is a' with $a = p^n a'$. For a discussion of $\operatorname{div}(M)$ and $\operatorname{Div}(M)$ see Jannsen [Ja88] §4. In particular note that in general $\operatorname{div}(M)$ is strictly larger than $\operatorname{Div}(M)$, as in the following example:

$$M = \big(\bigoplus_n \frac{1}{2n}\mathbb{Z}/\mathbb{Z}\big)/\ker\big(\text{sum} : \bigoplus_n \frac{1}{2}\mathbb{Z}/\mathbb{Z} \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}\big)$$

where $\operatorname{div}(M) = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ and $\operatorname{Div}(M) = 0$.

2. Preliminaries and reminder on global Galois cohomology

2.1 Tate–Shafarevich and Selmer groups

Let k be an algebraic number field. For a discrete Gal_k-module M we set

$$Ш^i(k, M) = \ker\Big(\mathrm{H}^i(k, M) \xrightarrow{\mathrm{res}_v} \prod_v \mathrm{H}^i(k_v, M)\Big)$$

with the restriction maps res_v induced by the embedding $k \hookrightarrow k_v$, and the product ranges over all places v of k. The Tate–Shafarevich group $Ш(A/k)$ for an abelian variety A over k is defined[2] as $Ш^1(k, A) = Ш^1(k, A(k^{\mathrm{alg}}))$, and in particular it is a torsion group. This implies that the Bashmakov problem can be considered one prime at a time. We will now concentrate on the p-primary part of the Bashmakov problem, i.e., analyzing the intersection of $Ш(A/k)_{p^\infty}$ and the maximal divisible subgroup of the Weil-Châtelet group.

Let p be a prime number. The p^n-torsion Selmer group of A is defined as

$$\mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n}) = \ker\Big(\mathrm{H}^1(k, A_{p^n}) \to \prod_v \mathrm{H}^1(k_v, A)\Big)$$

with v ranging over all places of k. A quick diagram chase with the cohomology sequence of the Kummer sequence

$$0 \to A_{p^n} \to A \xrightarrow{p^n \cdot} A \to 0$$

over k and all the localisations k_v yields the fundamental short exact sequence

$$0 \to A(k)/p^n A(k) \xrightarrow{\delta_{\mathrm{kum}}} \mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n}) \to Ш(A/k)_{p^n} \to 0. \tag{2.1}$$

[2]The traditional definition of $Ш(A/k)$ is indeed equivalent due to the subtle equality

$$\mathrm{H}^1(k_v, A) = \mathrm{H}^1(k_v, A(k_v^{\mathrm{alg}})) = \mathrm{H}^1(k_v, A(k^{\mathrm{alg}})).$$

It is known that $\mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n})$ is a finite group.

2.2 Generalized Selmer groups

The Selmer group $\mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n})$ is a global H^1 with local Selmer-conditions at every place. A **generalized Selmer group** $\mathrm{H}^1_{\mathbb{L}}(k, M)$ for a discrete finitely generated Gal_k-module M occurs by imposing **local conditions** $\mathbb{L}_v \subset \mathrm{H}^1(k_v, M)$ as follows

$$\mathrm{H}^1_{\mathbb{L}}(k, M) = \ker\Big(\mathrm{H}^1(k, M) \to \prod_v \mathrm{H}^1(k_v, M)/\mathbb{L}_v\Big),$$

such that the local conditions $\mathbb{L}_v$ agree for almost all v with the **unramified local cohomology**

$$\mathrm{H}^1_{\mathrm{nr}}(k_v, M) = \inf\big(\mathrm{H}^1(\kappa(v), M^{\mathrm{I}_v})\big) = \ker\big(\mathrm{H}^1(k_v, M) \to \mathrm{H}^1(\mathrm{I}_v, M)\big).$$

Here $\kappa(v)$ is the residue field at v and $\mathrm{I}_v \subset \mathrm{Gal}_{k_v}$ is the inertia subgroup. We do not bother to define $\mathrm{H}^1_{\mathrm{nr}}$ for infinite places v since there are only finitely many of them. For a textbook reference we refer to [NSW08] (8.7.8).

Observe that in the case when $M = A_{p^n}$, it is known that the image of the boundary map δ_{kum} of the Kummer sequence

$$\mathrm{Sel}_v = \delta_{\mathrm{kum}}\big(A(k_v)/p^n A(k_v)\big) \subset \mathrm{H}^1(k_v, A_{p^n})$$

coincides with $\mathrm{H}^1_{\mathrm{nr}}(k_v, A_{p^n})$ at places of good reduction with residue characteristic distinct from p (see [Mi86] Theorem 2.6). Hence for $M = A_{p^n}$ with $\mathbb{L}_v = \mathrm{Sel}_v$ we find back our original definition of the Selmer group.

Let $\mathbb{L} = (\mathbb{L}_v)$ be local conditions for the Gal_k-module M, and let Q be a finite set of places of k. Then we set $\mathbb{L}_Q$ (resp. $\mathbb{L}^Q$) for the local conditions $\mathbb{L}$ **but free at** Q (resp. $\mathbb{L}$ **but trivial at** Q) which agree with $\mathbb{L}$ at all places $v \notin Q$ and with $\mathbb{L}_{Q,v} = \mathrm{H}^1(k_v, M)$ (resp. $\mathbb{L}^Q_v = 0$) for all $v \in Q$. We shall mainly be working with the following generalized Selmer groups. Let Q be a finite set of finite places. The **Selmer group free at** Q is defined as

$$\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n}) = \ker\Big(\mathrm{H}^1(k, A_{p^n}) \to \prod_{v \notin Q} \mathrm{H}^1(k_v, A_{p^n})/\mathrm{Sel}_v\Big)$$

and the **Selmer group trivial at** Q is defined as

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n}) = \ker\Big(\mathrm{H}^1(k, A_{p^n}) \to \prod_{v \notin Q} \mathrm{H}^1(k_v, A_{p^n})/\mathrm{Sel}_v \times \prod_{v \in Q} \mathrm{H}^1(k_v, A_{p^n})\Big).$$

In the case when Q is the set of primes of k dividing p, we use $\mathrm{H}^1_{\mathrm{Sel}^p}(k, A_{p^n})$ (resp. $\mathrm{H}^1_{\mathrm{Sel}_p}(k, A_{p^n})$) to denote the Selmer groups $\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n})$ (resp. $\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n})$). Obviously we have inclusions

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}}(k, A_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n}).$$

2.3 Dual conditions and Euler characteristic formula

Let $\mathbb{L} = (\mathbb{L}_v)$ be a collection of local conditions for a discrete finitely generated Gal_k-module M. The dual local conditions $\mathbb{L}^* = (\mathbb{L}^*_v)$ are defined as the orthogonal complements $\mathbb{L}^*_v = \mathbb{L}_v^{\perp}$ with respect to the local Tate-duality pairing. Hence $\mathbb{L}^*$ is a collection of local conditions for the dual Gal_k-module

$$M^D = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z}(1)).$$

We know that

$$\mathrm{H}^1_{\mathrm{nr}}(k_v, M) = \mathrm{H}^1_{\mathrm{nr}}(k_v, M^D)^\perp$$

for almost all v, see [Mi86] Theorem 2.6, and consequently, if $\mathrm{H}^1_{\mathbb{L}}(k, M)$ is a generalized Selmer group then so is $\mathrm{H}^1_{\mathbb{L}^*}(k, M^D)$. If $M = A_{p^n}$ for an abelian variety A/k, so that $M^D = A^t_{p^n}$, where A^t is the dual abelian variety, then the Selmer condition is self-dual: $\mathrm{Sel}^* = \mathrm{Sel}$.

In order to relate sizes of these generalized Selmer groups, one adapts the Tate–Poitou exact sequence as in the proof of [NSW08] Theorem (8.7.9). We denote by $(-)^\vee$ the Pontrjagin dual $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ and get the exact sequence

$$0 \to \frac{\mathrm{H}^2(k_S/k, M^D)^\vee}{\prod_{v\in S} \mathrm{H}^0(k_v, M)} \to \mathrm{H}^1_{\mathbb{L}}(k, M) \to \prod_{v\in S} \mathbb{L}_v \to \mathrm{H}^1(k_S/k, M^D)^\vee \to \mathrm{H}^1_{\mathbb{L}^*}(k, M^D)^\vee \to 0 \qquad (2.2)$$

where S is a finite set of primes of k which includes all the archimedean primes, all primes that ramify in the extension $k(M)/k$, all the primes for which $\mathbb{L}_v \neq \mathrm{H}^1_{\mathrm{nr}}(k_v, M)$, as well as all the primes dividing the order of M. Here, as usual, the field k_S is the maximal extension of k unramified outside S.

For two sets of local conditions $\mathbb{L}_0 \subseteq \mathbb{L}$, meaning $\mathbb{L}_{0,v} \subseteq \mathbb{L}_v$ for all v, we use the natural map of (2.2) for $\mathbb{L}_0$ to the sequence for $\mathbb{L}$ with the same set S adapted to both local conditions,

$$\begin{array}{ccccccccc}
0 \to & \frac{\mathrm{H}^2(k_S/k,M^D)^\vee}{\prod_{v\in S}\mathrm{H}^0(k_v,M)} & \to & \mathrm{H}^1_{\mathbb{L}_0}(k,M) & \to & \prod_{v\in S}\mathbb{L}_{0,v} & \to & \mathrm{H}^1(k_S/k,M^D)^\vee & \to & \mathrm{H}^1_{\mathbb{L}_0^*}(k,M^D)^\vee \to 0 \\
& \| & & \downarrow & & \downarrow & & \| & & \downarrow \\
0 \to & \frac{\mathrm{H}^2(k_S/k,M^D)^\vee}{\prod_{v\in S}\mathrm{H}^0(k_v,M)} & \to & \mathrm{H}^1_{\mathbb{L}}(k,M) & \to & \prod_{v\in S}\mathbb{L}_v & \to & \mathrm{H}^1(k_S/k,M^D)^\vee & \to & \mathrm{H}^1_{\mathbb{L}^*}(k,M^D)^\vee \to 0.
\end{array}$$

A diagram chase leads to

$$\begin{array}{ccccccccc}
0 & \to & \frac{\mathrm{H}^1_{\mathbb{L}_0}(k,M)}{\mathrm{H}^2(k_S/k,M^D)^\vee} & \to & \prod_{v\in S}\mathbb{L}_{0,v} & \to & \ker\left(\mathrm{H}^1(k_S/k,M^D)^\vee \to \mathrm{H}^1_{\mathbb{L}_0^*}(k,M^D)^\vee\right) & \to & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \frac{\mathrm{H}^1_{\mathbb{L}}(k,M)}{\mathrm{H}^2(k_S/k,M^D)^\vee} & \to & \prod_{v\in S}\mathbb{L}_v & \to & \ker\left(\mathrm{H}^1(k_S/k,M^D)^\vee \to \mathrm{H}^1_{\mathbb{L}^*}(k,M^D)^\vee\right) & \to & 0.
\end{array}$$

Applying the snake lemma twice we find thus a short exact sequence

$$0 \to \frac{\mathrm{H}^1_{\mathbb{L}}(k, M)}{\mathrm{H}^1_{\mathbb{L}_0}(k, M)} \to \prod_v \mathbb{L}_v/\mathbb{L}_{0,v} \to \left(\frac{\mathrm{H}^1_{\mathbb{L}_0^*}(k, M^D)}{\mathrm{H}^1_{\mathbb{L}^*}(k, M^D)}\right)^\vee \to 0 \qquad (2.3)$$

where we can afford to take the product over all places v since $\mathbb{L}_{0,v} = \mathbb{L}_v$ for $v \notin S$ by assumption. We will apply (2.3) in the following special case which will help estimating sizes of generalized Selmer groups later.

Proposition 2. *Let M be a finite self-dual Gal_k-module and let $\mathbb{L} = \mathbb{L}^*$ be a system of local conditions for M that is self dual with respect to the identification $M \cong M^D$. Let Q be a finite set of places. Then we have the numerical Euler-Poincaré characteristic formula*

$$\frac{|\,\mathrm{H}^1_{\mathbb{L}_Q}(k, M)|}{|\,\mathrm{H}^1_{\mathbb{L}^Q}(k, M)|} = \prod_{v\in Q} |\mathbb{L}_v|.$$

Proof. We count for $\mathbb{L} \subseteq \mathbb{L}_Q$ by $\mathrm{H}^1_{\mathbb{L}}(k, M) = \mathrm{H}^1_{\mathbb{L}^*}(k, M^D)$ and by (2.3)

$$\frac{|\,\mathrm{H}^1_{\mathbb{L}_Q}(k, M)|}{|\,\mathrm{H}^1_{\mathbb{L}_Q}(k, M)|} = \frac{|\,\mathrm{H}^1_{\mathbb{L}_Q}(k, M)|}{|\,\mathrm{H}^1_{\mathbb{L}}(k, M)|} \cdot \frac{|\,\mathrm{H}^1_{\mathbb{L}^*}(k, M^D)|}{|\,\mathrm{H}^1_{\mathbb{L}^*_Q}(k, M^D)|} = \prod_{v \in Q} |\,\mathrm{H}^1(k_v, M)/\mathbb{L}_v| = \prod_{v \in Q} |\mathbb{L}_v|,$$

where the last equality is due to

$$|\,\mathrm{H}^1(k_v, M)/\mathbb{L}_v| = |\,\mathrm{Hom}(\mathbb{L}_v^*, \mathbb{Q}/\mathbb{Z})| = |\mathbb{L}_v^*| = |\mathbb{L}_v|$$

because of the self duality of $\mathbb{L}$. □

3. Translation between Galois cohomology and étale cohomology

3.1 Compactly supported étale cohomology

In this section we shall not be concerned with the effect of real places by assuming there are none, or that we deal with $p \neq 2$. Otherwise, there are expositions of the necessary modifications after Artin–Verdier by introducing the Woods-Hole site, see for example [Zi78].

Set $X = \mathrm{Spec}(\mathfrak{o}_k)$ for the ring of integers $\mathfrak{o}_k$ of an algebraic number field k. Let $j : U \subset X$ be a dense Zariski open. Then compactly supported cohomology of a constructible torsion sheaf $\mathscr{F}$ on the small étale site $U_{\text{ét}}$ is defined as

$$\mathrm{H}^i_{\mathrm{c}}(U, \mathscr{F}) = \mathrm{H}^i(X, j_!\mathscr{F}).$$

Restriction induces the natural "forget support" map $\mathrm{H}^i_{\mathrm{c}}(U, \mathscr{F}) \to \mathrm{H}^i(U, \mathscr{F})$.

3.2 Étale cohomology and the relation to generalized Selmer groups

Let $\mathscr{M}$ be a locally constant constructible sheaf on $U_{\text{ét}}$ with generic fiber the finite Gal_k-module M. Part of the localisation sequence for an open $V \subset U$ reads

$$\bigoplus_{v \in U \setminus V} \mathrm{H}^1_v(U, \mathscr{M}) \to \mathrm{H}^1(U, \mathscr{M}) \to \mathrm{H}^1(V, \mathscr{M}) \to \bigoplus_{v \in U \setminus V} \mathrm{H}^2_v(U, \mathscr{M}). \tag{3.1}$$

As $\mathrm{H}^1_v(U, \mathscr{M}) = 0$ for locally constant sheaves $\mathscr{M}$, we find that

$$\mathrm{H}^1(U, \mathscr{M}) \hookrightarrow \mathrm{H}^1(k, M) = \varinjlim_V \mathrm{H}^1(V, \mathscr{M})$$

is injective. Let $\mathbb{L} = (\mathbb{L}_v)$ be a collection of local conditions for M. We define the étale cohomology with local conditions as

$$\mathrm{H}^1_{\mathbb{L}}(U, \mathscr{M}) = \ker\Big(\mathrm{H}^1(U, \mathscr{M}) \to \prod_v \mathrm{H}^1(k_v, M)/\mathbb{L}_v\Big), \tag{3.2}$$

which agrees with $\mathrm{H}^1(U, \mathscr{M}) \cap \mathrm{H}^1_{\mathbb{L}}(k, M)$ inside $\mathrm{H}^1(k, M)$. In particular, we have étale cohomology $\mathrm{H}^1_{\mathrm{Sel}}(U, A_{p^n})$ with Selmer condition for a Zariski open $U \subset X$ with good reduction of A over U and a prime number p invertible on U.

Proposition 3. *If $\mathbb{L}_v = \mathrm{H}^1_{\mathrm{nr}}(k_v, M)$ for all $v \in U$ then*

$$\mathrm{H}^1_{\mathbb{L}}(U, \mathscr{M}) = \mathrm{H}^1_{\mathbb{L}}(k, M). \tag{3.3}$$

If in addition $\mathbb{L}_v = \mathrm{H}^1(k_v, M)$ for all $v \notin U$, then

$$\mathrm{H}^1(U, \mathscr{M}) = \mathrm{H}^1_{\mathbb{L}}(k, M),$$

whereas if in addition $\mathbb{L}_v = 0$ for all $v \notin U$, then

$$\operatorname{im}\big(\mathrm{H}^1_{\mathrm{c}}(U, \mathscr{M}) \to \mathrm{H}^1(U, \mathscr{M})\big) = \mathrm{H}^1_{\mathbb{L}}(k, M).$$

Proof. By definition of $\mathrm{H}^1_{\mathbb{L}}(U, \mathscr{M})$ it suffices to show that $\mathrm{H}^1_{\mathbb{L}}(k, M) \subset \mathrm{H}^1(U, \mathscr{M})$. Any class $\alpha \in \mathrm{H}^1(k, M)$ lies in $\mathrm{H}^1(V, \mathscr{M})$ for small enough open $V \subset U$. The claim follows from (3.1) because the image of an $\alpha \in \mathrm{H}^1_{\mathbb{L}}(k, M)$ vanishes in

$$\mathrm{H}^2_v(U, \mathscr{M}) = \mathrm{H}^1(k_v, M)/\mathrm{H}^1_{\mathrm{nr}}(k_v, M).$$

The additional claims follow from (3.3), the definition (3.2), and the exact sequence

$$\bigoplus_{v \in X \setminus U} \mathrm{H}^{i-1}(k_v, M) \to \mathrm{H}^i_{\mathrm{c}}(U, \mathscr{M}) \to \mathrm{H}^i(U, \mathscr{M}) \xrightarrow{\mathrm{res}_v} \bigoplus_{v \in X \setminus U} \mathrm{H}^i(k_v, M) \tag{3.4}$$

for $i \geqslant 0$. These exact sequences arise from the localisation sequence for $U \subset X$ and the sheaf $j_!\mathscr{M}$ because by excision $\mathrm{H}^{i+1}_v(X, j_!\mathscr{M}) = \mathrm{H}^i(k_v, M)$. □

Corollary 4. *Let A/k be an abelian variety with good reduction over U and let p be a rational prime invertible on U. With Q equal to the set of finite places $v \notin U$ we have*

$$\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n}) = \mathrm{H}^1(U, A_{p^n}) \tag{3.5}$$

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^n}) = \operatorname{im}\big(\mathrm{H}^1_{\mathrm{c}}(U, A_{p^n}) \to \mathrm{H}^1(U, A_{p^n})\big) \tag{3.6}$$

Proof. By assumption for $v \in U$ we have $\mathrm{Sel}_v = \mathrm{H}^1_{\mathrm{nr}}(k_v, A_{p^n})$, so the corollary follows from Proposition 3. □

Corollary 5. *Let $U \subset X$ be a Zariski open where the abelian variety A/k has good reduction and p is invertible. By abuse of notation we also denote by $A \to U$ the smooth model of A/k. Then for an open $V \subset U$ the restriction map $\mathrm{H}^1(U, A) \to \mathrm{H}^1(V, A)$ is injective and*

$$Ш(A/k)_{p^\infty} \subseteq \mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty} \subseteq \mathrm{H}^1(U, A) \subseteq \mathrm{H}^1(k, A) = \varinjlim_{V \subset U} \mathrm{H}^1(V, A).$$

Proof. An element of $\mathrm{H}^1(U, A)$ is represented by a principal homogeneous space W under A over U, which is trivial if and only $W(U)$ is nonempty. The valuative criterion of properness yields $W(U) = W(V)$ which proves the claim on injectivity.

Now $\mathrm{H}^1_{\mathrm{div}}(k, A)_{p^n}$ consists of classes that are trivial outside all $v \mid p$, see (1.2), hence is contained in the image of

$$\mathrm{H}^1_{\mathrm{Sel}_p}(U, A_{p^n}) = \mathrm{H}^1_{\mathrm{Sel}_p}(k, A_{p^n}) \to \mathrm{H}^1(k, A)$$

which maps to $\mathrm{H}^1(U, A)$. □

4. Review of Bashmakov's results: when the pro-p fundamental group is free

In [Ba64] Bashmakov proves that

$$Ш(A/k)_{p^\infty} \subseteq \mathrm{Div}(\mathrm{H}^1(k, A))$$

for abelian varieties A/k with very special properties. First, the number field k is required to satisfy the following conditions:

(i) k contains the pth roots of unity ζ_p,

(ii) there is a unique $\mathfrak{p} \mid (p)$ in $k/\mathbb{Q}$,

(iii) and the class number of k is prime to p.

It is a well known result of Shafarevich [Sh63], that conditions (i)–(iii) imply that the complement

$$V = \mathrm{Spec}(\mathfrak{o}_k) \setminus \{\mathfrak{p}\}$$

has a free pro-p group as its maximal pro-p quotient $\pi_1(V)^{\mathrm{pro}-p}$ of its fundamental group, see [NSW08] Cor 10.7.14. Moreover, the abelian variety A/k has to satisfy:

(iv) A/k has good reduction above V,

(v) the action of Gal_k on A_p factors over a p-group.

In [Ba64], Bashmakov does not require condition (v), although his argument at the very end does depend on it. Namely, under these assumptions we compute by [Zi78] Proposition 3.3.1

$$\mathrm{H}^2(V, A_{p^n}) = \mathrm{H}^2(\pi_1(V), A_{p^n}).$$

Due to (v) and a theorem of Neumann [Ne75], see [NSW08] Cor 10.4.8, we find that

$$\mathrm{H}^2(\pi_1(V), A_{p^n}) = \mathrm{H}^2(\pi_1(V)^{\mathrm{pro}-p}, A_{p^n}) = 0 \tag{4.1}$$

which vanishes in view of the freeness of $\pi_1(V)^{\mathrm{pro}-p}$ recalled above.

Proposition 6. *Let p be a regular prime number. Let k be a subfield of $\mathbb{Q}(\zeta_p)$ and let A/k be an abelian variety with good reduction away from the prime above p. If $\mathrm{Gal}_{\mathbb{Q}(\zeta_p)}$ acts via a p-group on A_p, then $\mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty}$ agrees with the p-part of $\mathrm{Div}(\mathrm{H}^1(k, A))$.*

Proof. We set $U = \mathrm{Spec}(\mathfrak{o}_k[1/p])$ and write by abuse of notation A/U for the smooth model of A/k over U. By Corollary 5 we have the second and third inclusion in

$$\mathrm{Div}(\mathrm{H}^1(k, A))_{p^\infty} \subseteq \mathrm{H}^1_{\mathrm{div}}(k, A)_{p^\infty} \subseteq \mathrm{H}^1(U, A)_{p^\infty} \subseteq \mathrm{H}^1(k, A)_{p^\infty}.$$

Thus, and since $\mathrm{H}^1(U, A)_{p^\infty}$ is a finitely cogenerated abelian torsion group, we find

$$\mathrm{Div}(\mathrm{H}^1(k, A))_{p^\infty} = \mathrm{Div}(\mathrm{H}^1(U, A)_{p^\infty}) = \mathrm{div}(\mathrm{H}^1(U, A)_{p^\infty}).$$

It therefore suffices to show that every element of $\mathrm{H}^1(U, A)_{p^\infty}$ is p-divisible in $\mathrm{H}^1(U, A)_{p^\infty}$. The Kummer exact sequence

$$0 \to A_{p^r} \to A \xrightarrow{p^r \cdot} A \to 0$$

on $U_{\text{ét}}$ yields a short exact sequence

$$\mathrm{H}^1(U, A) \xrightarrow{p^r \cdot} \mathrm{H}^1(U, A) \xrightarrow{\delta_r} \mathrm{H}^2(U, A_{p^r})$$

and the task left is showing $\delta_r = 0$. Since $\mathbb{Q}(\zeta_p)/k$ is of order prime to p, restriction via the finite étale

$$V = \mathrm{Spec}(\mathbb{Z}[\zeta_p, 1/p]) \to U$$

is injective by the corestriction argument and we have by (4.1)

$$\mathrm{H}^2(U, A_{p^n}) \hookrightarrow \mathrm{H}^2(V, A_{p^n}) = \mathrm{H}^2(\pi_1(V)^{\mathrm{pro}-p}, A_{p^n}) = 0,$$

completing the proof. □

Example 7. Examples of abelian varieties above $k = \mathbb{Q}(\zeta_p)$ with respect to a regular prime p and which satisfy the constraints imposed by Bashmakov (including condition (v)) are given by the Jacobian of the Fermat curve $X^p + Y^p = 1$, see for example [AI82].

However, the natural second family of examples to consider, namely the Jacobian of the modular curve $X_0(p)$ for $p = 11$ or $p \geqslant 17$, fail condition (v). Indeed[3], no prime $\mathfrak{m}$ of the Hecke algebra $\mathbb{T}$ above p is Eisenstein (those divide $p-1$) and the corresponding representation $\rho_{\mathfrak{m}} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}/\mathfrak{m})$ is irreducible by Mazur [Ma78]. Thus $\rho_{\mathfrak{m}}$ is surjective due to [Ri97].

5. Finite subgroups of GL_2

The purpose of this section is to provide the necessary statements from finite group theory.

Lemma 8. *Let W be a finite dimensional $\mathbb{F}_p$-vector space, and let $G \subset \mathrm{GL}(W)$ be a subgroup which intersects the center $\mathbb{F}_p^* \cong Z \subset \mathrm{GL}(W)$ nontrivially. Then the following holds.*

(1) *W and the adjoint representation $\mathrm{End}(W)$ have no common irreducible factor.*
(2) $\mathrm{H}^1(G, W) = 0$.

Proof. (1) The group $H = G \cap Z$ of homotheties in G acts trivially on every irreducible factor of $\mathrm{End}(W)$ and faithfully on every irreducible factor of W. Hence none of them can occur in both W and $\mathrm{End}(W)$.

(2) The inflation/restriction sequence for $H \trianglelefteq G$ reads

$$0 \to \mathrm{H}^1(G/H, W^H) \to \mathrm{H}^1(G, W) \to \mathrm{H}^1(H, W)^{G/H}.$$

Since H was assumed nontrivial and is necessarily of order prime to p, both W^H and $\mathrm{H}^1(H, W)$ vanish, and consequently also $\mathrm{H}^1(G, W) = 0$. □

In the 2-dimensional case we have a further criterion.

Theorem 9. *Let V be a vector space over $\mathbb{F}_p$ of dimension 2 with $p \geqslant 3$, and let $G \subseteq \mathrm{GL}(V)$ be a subgroup such that the G-module V is irreducible. Then the following holds:*

(1) $\mathrm{H}^1(G, V) = 0$,

and if, moroeover, G is not conjugate to a subgroup of $S_3 \subseteq \mathrm{GL}(V)$ with respect to a 2-dimensional irreducible representation of S_3, then:

(2) *V and $\mathrm{End}(V)$ have no common irreducible factor as G-modules.*

Proof. We first recall the classification of subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, see §2 of [Se72]. Let $\overline{G}$ be the image of G under the natural map $\mathrm{GL}_2(\mathbb{F}_p) \to \mathrm{PGL}_2(\mathbb{F}_p)$. Then one of the following holds.

(a) $p \mid \#G$ and G is contained in a Borel $B \subset \mathrm{GL}_2(\mathbb{F}_p)$.
(b) $p \mid \#G$ and G contains $\mathrm{SL}_2(\mathbb{F}_p)$.
(c) $p \nmid \#G$ and G is contained in a normalizer of a split torus.
(d) $p \nmid \#G$ and G is contained in a normalizer of a non-split torus.
(e) $p \nmid \#G$ and $\overline{G}$ is isomorphic to A_4, S_4, or A_5.

The case $p \mid \#G$. As by assumption G is not contained in a Borel, we conclude by the above list that G contains $\mathrm{SL}(V)$. Now since $p \geqslant 3$, the group G necessarily meets the center of $\mathrm{GL}(V)$ nontrivially, so that we conclude by Lemma 8.

[3]We thank K. Ribet for information on the Galois representation of the modular Jacobian.

The case $p \nmid \#G$. In this case $\mathrm{H}^1(G, V) = 0$ holds trivially, so we are done with assertion (1). If G belongs to case (e) of the above list, then Lemma 10 below shows that the intersection with the center of $\mathrm{GL}(V)$ is nontrivial and we conclude by Lemma 8.

It remains to discuss the case that $p \nmid \#G$ and G is contained in the normalizer $N = C \rtimes \mathbb{Z}/2\mathbb{Z}$ of a torus $C \subset \mathrm{GL}(V)$ such that V is an irreducible G-module. In order to understand the G-action on $\mathrm{End}(V)$ we identify $V = \mathbb{F}_p[\alpha]$ with a separable quadratic $\mathbb{F}_p$-algebra with $\mathrm{Aut}(\mathbb{F}_p[\alpha]/\mathbb{F}_p) = \mathbb{Z}/2\mathbb{Z}$ generated by $F \in \mathrm{End}(V)$ such that

$$N = \mathbb{F}_p[\alpha]^* \rtimes \langle F \rangle \subset \mathrm{GL}(V).$$

We find an isomorphism

$$\mathbb{F}_p[\alpha] \oplus \mathbb{F}_p[\alpha] \cdot F \xrightarrow{\sim} \mathrm{End}(V)$$

$$a + b \cdot F \mapsto x \mapsto ax + bF(x)$$

as N-modules, where N acts on the first summand $V_1 = \mathbb{F}_p[\alpha]$ through the quotient

$$\mathbb{F}_p[\alpha]^* \rtimes \langle F \rangle \twoheadrightarrow \langle F \rangle = \mathrm{Aut}(\mathbb{F}_p[\alpha]/\mathbb{F}_p) \subset \mathrm{GL}(V),$$

and, by a straight forward calculation left to the reader, on $V_2 = \mathbb{F}_p[\alpha] \cdot F$ through the endomorphism

$$\mathbb{F}_p[\alpha]^* \rtimes \langle F \rangle \to \mathbb{F}_p[\alpha]^* \rtimes \langle F \rangle$$

which maps F to F and $\lambda \in \mathbb{F}_p[\alpha]^*$ to $\lambda/F(\lambda)$, followed by the tautological action on $V = \mathbb{F}_p[\alpha]$ identified with $\mathbb{F}_p[\alpha] \cdot F$ by formally multiplying with F. As $p \nmid \#G$ the representation theory of G in $\mathbb{F}_p$-vector spaces is semissimple and assertion (2) can only fail if V is isomorphic to V_1 or V_2.

Let $H = G \cap C$ be the intersection with the torus, hence a subgroup in G of index $\leqslant 2$. Because V is not a reducible G-module and $p \geqslant 3$ we have $\#G \geqslant 3$ and therefore $H \neq 1$. As H acts trivial on V_1 we have $V \ncong V_1$ as G-modules. It remains to exclude $V \cong V_2$ as G-modules.

The representation $V \otimes \mathbb{F}_{p^2}$ regarded as an H-module decomposes as a sum of characters $\chi_1 \oplus \chi_2$ of H. The representation $V \cdot F \subset \mathrm{End}(V)$ decomposes after scalar extension to $\mathbb{F}_{p^2}$ as H-module as $\chi_1\chi_2^{-1} \oplus \chi_2\chi_1^{-1}$. Comparing the two, we find either $\chi_1 = \mathbf{1} = \chi_2$, whence $H = 1$ contradicting the irreduciblity of V as a G-module. Or, $\chi_1 = \chi_2^2 \neq 1$ and $\chi_2 = \chi_1^2 \neq 1$ which means χ_1 and χ_2 are of order 3 and determine each other. In this case $H \cong \mathbb{Z}/3\mathbb{Z}$ and acts on V noncentrally and without a common fixed vector. In any case, split or non-split, the subgroup $H \subset C$ is normal but not central in N. Hence either $H = G$ and G can be embedded in a subgroup $S_3 \subseteq \mathrm{GL}(V)$, or $H \trianglelefteq G$ of index 2 and $G \cong S_3$ itself. In any case, these subgroups G are excluded by assumption. This completes the proof of Theorem 9. □

Lemma 10. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ such that $p \nmid \#G$ and in the notation above $\overline{G}$ is isomorphic to A_4, S_4, or A_5, i.e., in case (e) of the above list. Then G meets the center Z of $\mathrm{GL}_2(\mathbb{F}_p)$ nontrivially.*

Proof. It suffices to discuss $\overline{G} = A_4$. If $G \cap Z = 1$, then we have a copy $A_4 \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ and $p > 2$. The 2-Sylow subgroup $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of A_4 has a completely reducible representation theory already rationally over $\mathbb{F}_p$ as we may produce enough projectors already over $\mathbb{F}_p$. Hence V_4 is contained in a split torus $C = \mathbb{F}_p^* \times \mathbb{F}_p^*$ and must agree with the 2-torsion of C. Thus V_4 already contains the central element -1, a contradiction. □

6. By induction to the structure of generalized Selmer groups

6.1 The Selmer splitting field

Let A/k be an abelian variety. We set

$$\mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p)$$

for the intersection of $\mathrm{H}^1(k(A_p)/k, A_p)$ under inflation with $\mathrm{H}^1_{\mathrm{Sel}}(k, A_p)$ in $\mathrm{H}^1(k, A_p)$. Then we have the following commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p) & \xrightarrow{\inf} & \mathrm{H}^1_{\mathrm{Sel}}(k, A_p) & \xrightarrow{\mathrm{res}} & \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p, A_p) \\
 & & \cap\mathrel{|} & & \cap\mathrel{|} & & \| \\
0 & \longrightarrow & \mathrm{H}^1(k(A_p)/k, A_p) & \xrightarrow{\inf} & \mathrm{H}^1(k, A_p) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(k(A_p), A_p)^{\mathrm{Gal}(k(A_p)/k)}
\end{array}$$

The exactness of the top row follows from the exactness of the bottom row. The restriction map defines a canonical continuous Gal_k-equivariant pairing

$$\mathrm{H}^1_{\mathrm{Sel}}(k, A_p) \times \left(\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p \right) \to A_p.$$

Let $\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p \twoheadrightarrow M$ be the continuous finite quotient by the right kernel of the pairing. Then the restriction map factors as

$$\mathrm{H}^1_{\mathrm{Sel}}(k, A_p) \to \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(M, A_p) \subset \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(\mathrm{Gal}^{\mathrm{ab}}_{k(A_p)} \otimes \mathbb{F}_p, A_p).$$

The quotient M corresponds to a finite Galois extension $L/k(A_p)$, the **Selmer splitting field** of A with respect to the prime p, more precisely $M = \mathrm{Gal}(L/k(A_p))$. Since M is a quotient as $\mathrm{Gal}(k(A_p)/k)$-module, the field L is in fact Galois over k and $\mathrm{Gal}(k(A_p)/k)$ acts on M by conjugation after lifting under the quotient map $\mathrm{Gal}(L/k) \twoheadrightarrow \mathrm{Gal}(k(A_p)/k)$.

Lemma 11. *Let A/k be an abelian variety, and let L be the Selmer splitting field with respect to p. Then the following holds.*

(1) *The following sequence is exact:*

$$0 \to \mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p) \to \mathrm{H}^1_{\mathrm{Sel}}(k, A_p) \to \mathrm{Hom}_{\mathrm{Gal}(k(A_p)/k)}(\mathrm{Gal}(L/k(A_p)), A_p) \tag{6.1}$$

(2) *Every irreducible $\mathrm{Gal}(k(A_p)/k)$-module subquotient of $\mathrm{Gal}(L/k(A_p))$ is isomorphic to an irreducible subquotient of A_p.*

Proof. (1) is obvious by the definition of L. For (2) we note that the defining pairing yields an injective map

$$\mathrm{Gal}(L/k(A_p)) = M \hookrightarrow \mathrm{Hom}(\mathrm{H}^1_{\mathrm{Sel}}(k, A_p), A_p) \cong A_p \oplus \ldots \oplus A_p \tag{6.2}$$

of $\mathrm{Gal}(k(A_p)/k)$-modules, where $\mathrm{H}^1_{\mathrm{Sel}}(k, A_p)$ carries trivial action. □

6.2 The structure of some generalized Selmer groups

The following theorem will be ultimately applied to elliptic curves that are automatically principally polarized.

Theorem 12. *Let A/k be a principally polarized abelian variety, and let p be a prime number, such that*

(i) $A_p(k) = 0$,

(ii) $\mathrm{H}^1(k(A_p)/k, A_p) = 0$.

Let Q be a finite set of finite primes of k not dividing p, and fix $n \in \mathbb{N}$ such that

(iii) *A has good reduction at v for all $v \in Q$;*

(iv) *the set of Frobenius elements $\mathrm{Frob}_w \in \mathrm{Gal}(L/k(A_p))$ where L is the Selmer splitting field of A/k with respect to p and w denotes a prime of $k(A_p)$ dividing v, when v ranges over Q, generates $\mathrm{Gal}(L/k(A_p))$ as a $\mathrm{Gal}(k(A_p)/k)$-module;*

(v) *$A_{p^n}(k_v)$ is a free $\mathbb{Z}/p^n\mathbb{Z}$-module for all $v \in Q$.*

Then for all $m \leqslant n$ we have that

(1) $\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^m}) = 0$,

(2) $\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^m}) \cong \prod_{v\in Q} A_{p^m}(k_v)$ *under a non-canonical group isomorphism.*

Proof. Step 1: We first treat (1) for $m = 1$. We set $k_1 = k(A_p)$, and $k_{1,w}$ for the completion of $k(A_p)$ in w. Localization at v respectively w yields a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^1_{\mathrm{Sel}}(k, A_p) & \xrightarrow{\mathrm{res}_{k_1/k}} & \mathrm{Hom}_{\mathrm{Gal}(k_1/k)}(\mathrm{Gal}(L/k_1), A_p) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{ev}_w} \\ \mathrm{H}^1_{\mathrm{nr}}(k_v, A_p) & \xrightarrow{\mathrm{res}_{k_{1,w}/k_v}} & \mathrm{H}^1_{\mathrm{nr}}(k_{1,w}, A_p) = A_p \end{array}$$

with the evaluation map ev_w mapping a morphism $\varphi : \mathrm{Gal}(L/k_1) \to A_p$ to its value $\varphi(\mathrm{Frob}_w)$ at the Frobenius element of w. Assumption (iv), the sequence (6.1), and assumption (ii) imply

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_p) \subseteq \mathrm{H}^1_{\mathrm{Sel}}(k(A_p)/k, A_p) \subseteq \mathrm{H}^1(k(A_p)/k, A_p) = 0.$$

Step 2: We now show (1) by induction on m terminating in n. As an abbreviation we set

$$\mathbb{L}_{m,v} = \mathrm{Sel}_v^Q \subseteq \mathrm{H}^1(k_v, A_{p^m})$$

for the Selmer condition trivial at Q for A_{p^m}-coefficients. Then the following diagram is commutative and the rows are exact

$$\begin{array}{ccccccccc} & & \mathbb{L}_{m-1,v} & \longrightarrow & \mathbb{L}_{m,v} & \longrightarrow & \mathbb{L}_{1,v} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^1(k_v, A_{p^{m-1}})/\delta_{\mathrm{kum}}\big(A_p(k_v)\big) & \longrightarrow & \mathrm{H}^1(k_v, A_{p^m}) & \xrightarrow{p^{m-1}\cdot} & \mathrm{H}^1(k_v, A_p) & & \end{array} \tag{6.3}$$

The snake lemma applied to (6.3) yields that in the commutative diagram

$$\begin{array}{ccccccc} A_p(k) & \xrightarrow{\delta_{\mathrm{kum}}} & \mathrm{H}^1(k, A_{p^{m-1}}) & \longrightarrow & \mathrm{H}^1(k, A_{p^m}) & \longrightarrow & \mathrm{H}^1(k, A_p) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \prod_v A_p(k_v) & \xrightarrow{\delta_{\mathrm{kum}}} & \prod_v \frac{\mathrm{H}^1(k_v, A_{p^{m-1}})}{\mathbb{L}_{m-1,v}} & \longrightarrow & \prod_v \frac{\mathrm{H}^1(k_v, A_{p^m})}{\mathbb{L}_{m,v}} & \longrightarrow & \prod_v \frac{\mathrm{H}^1(k_v, A_p)}{\mathbb{L}_{1,v}} \end{array} \tag{6.4}$$

the bottom row is exact. The map δ_{kum} in the bottom row is the zero map: by assumption (v) when $v \in Q$, then $A_{p^m}(k_v)/A_{p^{m-1}}(k_v) \to A_p(k_v)$ is surjective for $m \leqslant n$, or, in general for $v \notin Q$,

by comparing the boundary maps for the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{p^{m-1}} & \longrightarrow & A_{p^m} & \xrightarrow{p^{m-1}\cdot} & A_p & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_{p^{m-1}} & \longrightarrow & A & \xrightarrow{p^{m-1}\cdot} & A & \longrightarrow & 0 \end{array}$$

(It is the limitation of assumption (v) that forces the induction terminate at n). Again the snake lemma applied to (6.4) yields exactness of

$$\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^{m-1}}) \to \mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^m}) \to \mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_p)$$

so that with Step 1 we deduce (1) by induction on m.

Step 3: By (i) we have

$$\mathrm{H}^1(k, A_{p^m}) = \mathrm{H}^1(k, A_{p^n})_{p^m},$$

and it follows then from the definition that

$$\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^m}) = \mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n})_{p^m}.$$

is also the exact p^m-torsion.

Step 4: Since A is principally polarized, the coefficients A_{p^m} are self dual and the Selmer condition is self dual with respect to the identification $A_{p^m} = A^D_{p^m}$.

With the Euler-Poincaré characteristic formula of Proposition 2 and (1) we compute

$$|\,\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^m})| = \frac{|\,\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^m})|}{|\,\mathrm{H}^1_{\mathrm{Sel}^Q}(k, A_{p^m})|} = \prod_{v\in Q} |A(k_v)/p^m A(k_v)| = \prod_{v\in Q} |A_{p^m}(k_v)|.$$

The last equation $|A(k_v)/p^m A(k_v)| = |A_{p^m}(k_v)|$ follows because by Mattuck–Tate the p-primary part of $A(k_v)$ is finite since $v \nmid p$ for all $v \in Q$.

Step 5: In order to show (2) it suffices to treat the case of $\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n})$. By Steps 3 and 4 we conclude that $\mathrm{H}^1_{\mathrm{Sel}_Q}(k, A_{p^n})$ has the same number of p^m-torsion elements for every $m \leqslant n$ as

$$\prod_{v\in Q} A_{p^n}(k_v),$$

so that both groups are noncanonically isomorphic. This proves (2). □

6.3 The case of elliptic curves

Based on the group theory of GL_2 in Section 5 we can show existence for auxiliary sets of primes Q in Theorem 12 in the special case of elliptic curves.

Proposition 13. *Let E/k be an elliptic curve and let p be an odd prime number such that E_p is an irreducible Gal_k-module and $\mathrm{Gal}(k(E_p)/k) \subseteq \mathrm{GL}(E_p)$ is not contained in a conjugate of $S_3 \subseteq \mathrm{GL}(E_p)$. Fix an $n \in \mathbb{N}$. Then*

(1) *$E_p(k) = 0$,*
(2) *and $\mathrm{H}^1(k(E_p)/k, E_p) = 0$.*

Moreover, we can find a finite set of primes Q not dividing p such that

(3) *E has good reduction at v for all $v \in Q$;*

(4) *the primes $v \in Q$ are completely split in $k(E_{p^n})/k$;*

(5) *the set of $\mathrm{Frob}_w \in \mathrm{Gal}(L/k(E_p))$ where L is the Selmer splitting field of E/k with respect to p and w denotes a prime of $k(E_p)$ dividing v as v varies though Q, generates $\mathrm{Gal}(L/k(E_p))$ as a $\mathrm{Gal}(k(E_p)/k)$-module.*

In particular, for all $m \leqslant n$ we have

(6) $\mathrm{H}^1_{\mathrm{Sel}_Q}(k, E_{p^m}) \cong (\mathbb{Z}/p^m\mathbb{Z})^{2\cdot \# Q}$.

Proof. The subgroup $E_p(k) \subseteq E_p(k^{\mathrm{alg}})$ is a Gal_k-submodule and thus in view of the irreducibility assumption either all or nothing. In case of trivial Gal_k-action, the module E_p is not irreducible, so that we conclude (1). Assertion (2) follows from Theorem 9 (1).

We will now construct the set Q of auxiliary primes. First we prove that L and $k(E_{p^n})$ are linearly disjoint over $k(E_p)$. Indeed, let $K = L \cap k(E_{p^n})$ be their intersection and set $\overline{M} = \mathrm{Gal}(K/k(E_p))$ for the abelian Galois group over $k(E_p)$. Then, since K/k is Galois, the projection

$$\mathrm{Gal}(L/k(E_p)) \twoheadrightarrow \overline{M}$$

is a surjection of $\mathrm{Gal}(k(E_p)/k)$-modules. It follows from Lemma 11 that $\overline{M}$ has a composition series as $\mathrm{Gal}(k(E_p)/k)$-module consisting of irreducible subquotients of E_p. On the other hand, the group $\mathrm{Gal}(k(E_{p^n})/k(E_p))$ is a subgroup of

$$N = \ker\big(\mathrm{GL}(E_{p^n}) \to \mathrm{GL}(E_p)\big).$$

The group N is solvable with abelian subquotients

$$N_m = \ker\big(\mathrm{GL}(E_{p^m}) \to \mathrm{GL}(E_{p^{m-1}})\big)$$

that are canonically $\mathrm{Gal}(k(E_p)/k)$-modules by conjugation with lifts and as such isomorphic to the adjoint representation of $\mathrm{Gal}(k(E_p)/k)$ on $\mathrm{End}(E_p)$. Since, by Theorem 9 (2), E_p and $\mathrm{End}(E_p)$ have no common irreducible $\mathrm{Gal}(k(E_p)/k)$-subquotient, we deduce that $\overline{M} = 0$ and $K = k(E_p)$, which means that L and $k(E_{p^n})$ are linearly disjoint over $k(E_p)$.

The Chebotarev density theorem enables us to choose a finite set Q of finite places $v \nmid p$ in the locus of good reduction of E/k, so that the Frobenius elements Frob_v for $v \in Q$ satisfy

(i) the image of Frob_v in $\mathrm{Gal}(k(E_{p^n})/k)$ is trivial,

(ii) the images of Frob_v for $v \in Q$ generate $\mathrm{Gal}(L/k(E_p))$.

The linear disjointness of L and $k(E_{p^n})$ over $k(E_p)$ implies that (i) and (ii) do not contradict each other. This shows (3)–(5).

In order to prove (6) we apply Theorem 12 with the set Q constructed above. Indeed, elliptic curves are principally polarized and (4) implies that $E_{p^n}(k_v) \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$. □

7. Intersection with the maximal divisible subgroup

We are ultimately interested in understanding the intersection of $Ш(A/k)$ with the maximal divisible subgroup of the Weil–Châtelet group $\mathrm{Div}\big(\mathrm{H}^1(k, A)\big)$. We proceed by analyzing one prime at a time.

7.1 Using the Euler characteristic formula

Recall from (1.2) that $\mathrm{Div}\big(\mathrm{H}^1(k, A)_{p^\infty}\big)$ is locally trivial at all primes v which do not divide p. This implies that the image of $\mathrm{H}^1_{\mathrm{Sel}_p}(k, A_{p^\infty})$ in $\mathrm{H}^1(k, A)$ contains $\mathrm{Div}\big(\mathrm{H}^1(k, A)_{p^\infty}\big)$, and together

with the analysis in Section §2.3 gives us a way of exploring the intersection of $Ш(A/k)_{p^\infty}$ with $\mathrm{Div}\left(\mathrm{H}^1(k,A)_{p^\infty}\right)$. We will follow this path first for a general abelian variety and then in the case of elliptic curves.

Lemma 14. *Let A/k be an abelian variety, and let p be a rational prime. If $\mathrm{H}^1_{\mathrm{Sel}}(k,A^t_{p^n})$ equals $\mathrm{H}^1_{\mathrm{Sel}^p}(k,A^t_{p^n})$ for almost all n then $\mathrm{Div}\left(\mathrm{H}^1(k,A)_{p^\infty}\right) \neq 0$ but its intersection with $Ш(A/k)_{p^\infty}$ agrees with $\mathrm{Div}\left(Ш(A/k)_{p^\infty}\right)$.*

Remark 15. The assumption $\mathrm{H}^1_{\mathrm{Sel}}(k,A^t_{p^n}) = \mathrm{H}^1_{\mathrm{Sel}^p}(k,A^t_{p^n})$ for almost all n implies by (2.1) that

$$A^t(k) \subseteq \bigcap_{n\geqslant 1} p^n A^t(k_v)$$

where $v \mid p$ is a place of k. Therefore A^t and, being isogenous, also A have trivial algebraic rank.

Proof of Lemma 14. Consider the sequence (2.3) for $M = A_{p^n}$, $\mathbb{L} = \mathrm{Sel}_p$ and $\mathbb{L}_0 = \mathrm{Sel}$. Then, since $\mathbb{L}^* = \mathrm{Sel}^p$, our assumption $\mathrm{H}^1_{\mathrm{Sel}}(k,A^t_{p^n}) = \mathrm{H}^1_{\mathrm{Sel}^p}(k,A^t_{p^n})$ for $n \gg 0$ leads to the exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{Sel}}(k,A_{p^n}) \to \mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^n}) \to \prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^n} \to 0. \tag{7.1}$$

Local Tate duality implies that we have the following group isomorphism

$$\prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^n} \simeq (\mathbb{Z}/p^n\mathbb{Z})^d \oplus \prod_{\mathfrak{p}\mid p} A(k_\mathfrak{p})_{p^\infty}/p^n \tag{7.2}$$

where $d = [k:\mathbb{Q}]\cdot\dim(A)$ and the order of $\prod_{\mathfrak{p}\mid p} A(k_\mathfrak{p})_{p^\infty}/p^n$ is independent of n for $n \gg 0$. In the limit for $n \to \infty$ the exact sequence (7.1) becomes the exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{Sel}}(k,A_{p^\infty}) \to \mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty}) \to \prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^\infty} \to 0, \tag{7.3}$$

and local Tate duality implies an isomorphism

$$\prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^\infty} = \prod_{\mathfrak{p}\mid p} \mathrm{Hom}\left(A(k_\mathfrak{p}),\mathbb{Q}_p/\mathbb{Z}_p\right) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^d \oplus \prod_{\mathfrak{p}\mid p} A(k_\mathfrak{p})_{p^\infty}$$

Let $D_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^d$ be the intersection of the maximal divisible subgroup

$$D = \mathrm{Div}\Big(\prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^\infty}\Big) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^d$$

with the p^n-torsion subgroup $\prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^n}$. Since (7.1) is an exact sequence of finite length $\mathbb{Z}/p^n\mathbb{Z}$-modules, the set S_n of partial splittings $s_n : D_n \to \mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty})$ is finite and non-empty. Restriction defines a map $S_{n+1} \to S_n$, and a well-known compactness argument shows that $\varprojlim_n S_n$ is non-empty. An element s of the projective limit is nothing but a partial splitting $s : D \to \mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty})$ of (7.3). We conclude that the sequence

$$0 \to \mathrm{Div}\left(\mathrm{H}^1_{\mathrm{Sel}}(k,A_{p^\infty})\right) \to \mathrm{Div}\left(\mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty})\right) \to \mathrm{Div}\Big(\prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^\infty}\Big) \to 0. \tag{7.4}$$

is split exact. Moreover, if we map to $\mathrm{H}^1(k,A)_{p^\infty}$, in view of the discussion at the beginning of this section we find an exact sequence

$$0 \to Ш(A/k)_{p^\infty} \to \mathrm{im}\left(\mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty}) \to \mathrm{H}^1(k,A)_{p^\infty}\right) \to \prod_{\mathfrak{p}\mid p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^\infty} \to 0,$$

and again exploiting the partial splitting s we find that

$$0 \to \mathrm{Div}\left(Ш(A/k)_{p^\infty}\right) \to \mathrm{Div}\left(\mathrm{H}^1(k,A)_{p^\infty}\right) \to \mathrm{Div}\left(\prod_{\mathfrak{p}|p} \mathrm{H}^1(k_\mathfrak{p},A)_{p^\infty}\right) \to 0$$

is also split exact. It follows that $\mathrm{Div}\left(\mathrm{H}^1(k,A)_{p^\infty}\right)$ is nontrivial of corank at least

$$d = [k:\mathbb{Q}]\cdot \dim(A)$$

and that indeed the intersection of $Ш(A/k)_{p^\infty} \cap \mathrm{Div}\left(\mathrm{H}^1(k,A)_{p^\infty}\right)$ lies in $\mathrm{Div}\left(Ш(A/k)\right)$. □

The **corank** of a p-primary torsion group $M = (\mathbb{Q}_p/\mathbb{Z}_p)^n \times M_0$ with finite M_0, is the well-defined number $n = \mathrm{corank}_{\mathbb{Z}_p}(M)$.

Proposition 16. *Let A/k be an abelian variety with algebraic rank $r < d = \dim(A)\cdot[k:\mathbb{Q}]$. Then $\mathrm{Div}(\mathrm{H}^1(k,A))$ contains a copy of $(\mathbb{Q}/\mathbb{Z})^{d-r}$.*

Proof. We can focus on the p-primary part for a prime number p and have to compute the corank of $\mathrm{Div}(\mathrm{H}^1(k,A)_{p^\infty})$. We set $s_p = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty}))$, $s = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathrm{Sel}}(k,A_{p^\infty}))$, and $s^p = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{H}^1_{\mathrm{Sel}^p}(k,A_{p^\infty}))$. These coranks are constant on isogeny classes, in particular they are the same for the dual A^t. Analyzing the asymptotic cardinality for $n \gg 0$ in (2.3) with $M = A_{p^n}$, $\mathbb{L} = \mathrm{Sel}_p$ and $\mathbb{L}_0 = \mathrm{Sel}$, we obtain

$$s_p - s^p = (s_p - s) + (s - s^p) = d.$$

The exact sequence

$$0 \to A(k)\otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty}) \to \ker\left(\mathrm{H}^1(k,A)_{p^\infty} \to \prod_{v\nmid p} \mathrm{H}^1(k_v,A)\right) \to 0 \tag{7.5}$$

splits since $A(k)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ is a divisible group. Therefore (7.5) remains exact upon applying the functor $\mathrm{Div}(-)$. Using the exact sequence

$$0 \to A(k)\otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Div}\left(\mathrm{H}^1_{\mathrm{Sel}_p}(k,A_{p^\infty})\right) \to \mathrm{Div}\left(\mathrm{H}^1(k,A)_{p^\infty}\right) \to 0$$

we find

$$\mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Div}\left(\mathrm{H}^1(k,A)_{p^\infty}\right)\right) = s_p - r = d + s^p - r \tag{7.6}$$

which is $\geqslant d - r$ and proves the proposition. □

7.2 Results for elliptic curves over $\mathbb{Q}$

Proposition 17. *Let $E/\mathbb{Q}$ be an elliptic curve of trivial algebraic rank. Then we have:*

(1) $\mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q},E)\right)$ *contains a copy of $\mathbb{Q}/\mathbb{Z}$ and in particular is nontrivial.*

(2) *If $Ш(E/\mathbb{Q})$ is finite, then $\mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q},E)\right) \cong \mathbb{Q}/\mathbb{Z}$ and*

$$Ш(E/\mathbb{Q}) + \mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q},E)\right) = \mathrm{H}^1_{\mathrm{div}}(\mathbb{Q},E).$$

Proof. (1) This is a special case of Proposition 16.

(2) Fusing together the exact sequences (1.2) for all p we obtain

$$0 \to Ш(E/\mathbb{Q}) \to \mathrm{H}^1_{\mathrm{div}}(\mathbb{Q},E) \to \mathbb{Q}/\mathbb{Z} \to 0$$

which is exact since $Ш(E/\mathbb{Q})$ was assumed finite and there is a copy of $\mathbb{Q}/\mathbb{Z}$ in $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q},E)$ by (1). The result follows at once. □

Theorem 18. *Let $E/\mathbb{Q}$ be an elliptic curve of trivial analytic rank. Then we have:*

(1) *The intersection $Ш(E/\mathbb{Q})_{p^\infty}$ with $\operatorname{Div}\big(\mathrm{H}^1(\mathbb{Q},E)_{p^\infty}\big)$ is trivial for all odd primes p of good reduction such that the $\mathrm{Gal}_\mathbb{Q}$-representation on E_p is irreducible.*

(2) $\operatorname{Div}\big(\mathrm{H}^1(\mathbb{Q},E)\big) \cong \mathbb{Q}/\mathbb{Z}$ *and the sum*

$$Ш(E/\mathbb{Q})_{p^\infty} \oplus \operatorname{Div}\big(\mathrm{H}^1(\mathbb{Q},E)\big)_{p^\infty} = \mathrm{H}^1_{\mathrm{div}}(\mathbb{Q},E)_{p^\infty}$$

is direct for all p as in (1).

Remark 19. We refer to the example in Section §8 for an elliptic curve $E/\mathbb{Q}$ of trivial analytic rank with non-trivial 3-torsion in $Ш(E/\mathbb{Q}) \cap \operatorname{Div}(\mathrm{H}^1(\mathbb{Q},E))$.

Proof of Theorem 18. Since the analytic rank of $E/\mathbb{Q}$ is trivial we know that $Ш(E/\mathbb{Q})$ is finite (see [Ko90]), and hence (2) follows from (1) and Proposition 17. We now prove (1) in several steps.

Step 1: We choose a quadratic imaginary extension $K = \mathbb{Q}(\sqrt{-d})$ such that

(i) K is distinct from the field of complex multiplication of E in case E has CM,

(ii) $K/\mathbb{Q}$ is linearly disjoint from $\mathbb{Q}(E_p)/\mathbb{Q}$,

(iii) $d \geqslant 5$,

(iv) E/K has analytic rank 1,

(v) all the primes dividing the conductor of $E/\mathbb{Q}$ split,

(vi) p is inert in $K/\mathbb{Q}$.

Friedberg, and Hoffstein have shown that such an extension exists (see [FH95] Theorem B(2)).

Step 2: We fix $n \in \mathbb{N}$ large enough so that

(i) $p^{n-1}Ш(E/K)_{p^\infty} = 0$,

(ii) p^n does not divide the basic Heegner point defined over K.

This is possible since we know that $Ш(E/K)$ is finite, and due to the nontriviality of this Heegner point, since the analytic rank of E/K is 1.

Step 3: Since we have chosen $\mathbb{Q}(E_p)$ and K to be linearly disjoint over $\mathbb{Q}$ the restriction yields an isomorphism

$$G = \mathrm{Gal}(K(E_p)/K) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}).$$

Hence the assumption that E_p is an irreducible $\mathrm{Gal}_\mathbb{Q}$-module, implies that it is also irreducible as a Gal_K-module. Moreover, we have an isomorphism

$$\mathrm{Gal}(K(E_p)/\mathbb{Q}) = G \times \langle\sigma\rangle,$$

where

$$\langle\sigma\rangle = \mathrm{Gal}(K(E_p)/\mathbb{Q}(E_p)) \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}).$$

Step 4: The image $\mathrm{Gal}(K(E_p)/K) \subseteq \mathrm{GL}(E_p)$ is not contained in a subgroup $S_3 \subseteq \mathrm{GL}(E_p)$, because $p = 2$ was excluded, if $p = 3$ then any 2-dimensional S_3-representation is reducible, and for $p \geqslant 5$ we have

$$|\det(\mathrm{Gal}(K(E_p)/K))| = |\det(\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q}))| = [\mathbb{Q}(\mu_p):\mathbb{Q}] = p-1 > 2 = |\det(S_3)|.$$

Step 5: Let L be the Selmer splitting field of E over K with respect to p, see Section 6.1. Because E is defined over $\mathbb{Q}$ and L is characteristic for the base change of E to K, we deduce

that L is Galois over $\mathbb{Q}$. As in the proof of Proposition 13 we conclude from Step 3 and 4 that L and $K(E_{p^n})$ are linearly disjoint over $K(E_p)$. It follows from

$$L \cap \mathbb{Q}(E_{p^n}) = K(E_p) \cap \mathbb{Q}(E_{p^n}) = \mathbb{Q}(E_p)$$

that the natural map to the fibre product

$$\mathrm{Gal}(LK(E_{p^n})/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q}) \times_{\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})} \mathrm{Gal}(\mathbb{Q}(E_{p^n})/\mathbb{Q}) \tag{7.7}$$

is an isomorphism (here $LK(E_{p^n})$ denotes the compositum of L and $K(E_{p^n})$).

Step 6: Let $\tau \in \mathrm{Gal}(LK(E_{p^n})/\mathbb{Q})$ denote a complex conjugation. The restriction of τ in

$$\mathrm{Gal}(K(E_p)/\mathbb{Q}) = G \times \langle\sigma\rangle \subseteq \mathrm{GL}(E_p) \times \langle\sigma\rangle$$

after a suitable choice of basis for E_p reads

$$\begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \cdot \sigma. \tag{7.8}$$

We have to understand $M = \mathrm{Gal}(L/K(E_p))$ as a G-module, more precisely as a $G \times \langle\sigma\rangle$-module. Recall from (6.2) that naturally, and thus even as $G \times \langle\sigma\rangle$-modules, we have an inclusion

$$M \hookrightarrow \mathrm{Hom}(\mathrm{H}^1_{\mathrm{Sel}}(K, E_p), E_p).$$

Here the product acts through projection to $\langle\sigma\rangle$ on $\mathrm{H}^1_{\mathrm{Sel}}(K, E_p)$ and through projection to G on E_p. Let $\chi_{K/\mathbb{Q}}$ be the quadratic character associated to the extension $K/\mathbb{Q}$. It follows (p is odd) that as $G \times \langle\sigma\rangle$-module

$$M \cong (E_p)^a \oplus (E_p \otimes \chi_{K/\mathbb{Q}})^b \tag{7.9}$$

for some $a, b \in \mathbb{N}$, because E_p (and thus $E_p \otimes \chi_{K/\mathbb{Q}}$) is irreducible and a submodule of a direct sum of simple modules is isomorphic to the direct sum over a subset of those summands.

Since p is assumed to be odd, M splits as a direct sum

$$M = M^+ \oplus M^-$$

of its eigenspaces under τ. We claim that M^+ generates M as a G-module. By the decomposition (7.9) it suffices to prove this claim for the $G \times \langle\sigma\rangle$-modules E_p and $E_p \otimes \chi_{K/\mathbb{Q}}$. Due to (7.8) in both cases τ acts via a matrix conjugate to

$$\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$$

and the corressponding $+$-eigenspaces are nontrivial, so that these generate as a G-module by the irreducibility of E_p (and thus $E_p \otimes \chi_{K/\mathbb{Q}}$) as a G-module.

Step 7: Let $S \subseteq M = \mathrm{Gal}(L/K(E_p))$ be a generating set of M. We pick a finite set of rational primes Q of $\mathbb{Q}$ by choosing for every $h \in S$, using the Chebotarev density theorem, a rational prime ℓ unramified in $LK(E_{p^n})/\mathbb{Q}$ and coprime to the conductor of $E/\mathbb{Q}$ such that

(i) $\mathrm{Frob}_\ell = \tau h \in \mathrm{Gal}(L/\mathbb{Q})$, and
(ii) $\mathrm{Frob}_\ell = \tau \in \mathrm{Gal}(\mathbb{Q}(E_{p^n})/\mathbb{Q})$.

These requirements are free of contradictions by the structure assertion (7.7).

This set of auxiliary primes Q satisfies the following properties:

(i) E has good reduction at $\ell \in Q$,

(ii) $\ell \in Q$ is inert in $K/\mathbb{Q}$,

(iii) $|E(K_\lambda)_{p^n}| = p^{2n}$ for every $\ell \in Q$ (with λ the unique prime of K above ℓ by (ii)),

(iv) the set of Frobenius elements $\mathrm{Frob}_w \in \mathrm{Gal}(L/K(E_p))$ where w denotes a prime of $K(E_p)$ dividing ℓ, when ℓ ranges over Q, generates $\mathrm{Gal}(L/K(E_p))$ as a $\mathrm{Gal}(K(E_p)/K)$-module.

Indeed, properties (i)–(iii) are obvious and property (iv) holds by Step 6 because the τ-eigenspace M^+ is generated by elements of the form

$$\mathrm{Frob}_w = (\mathrm{Frob}_\ell)^2 = (\tau h)^2 = \tau(h) \cdot h$$

where $h \in S$. Here again, $p \neq 2$ is used.

We can then apply Theorem 12 with the auxiliary set Q by now viewing Q as a set of primes of K (since there is a unique prime λ of K above each $\ell \in Q$). It follows that

$$\mathrm{H}^1_{\mathrm{Sel}_Q}(K, E_{p^n}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{2t}$$

where $t = \#Q$.

Step 8: We now argue as in Theorem 1.1.7 of [ÇW08]. Since by Step 1 (ii) we still have $E_p(K) = 0$ and by Step 1 (iv) $E(K)$ contains a non-torsion Heegner point we have

$$E(K)/p^n E(K) \cong \mathbb{Z}/p^n\mathbb{Z}$$

and the exact sequence

$$0 \to E(K)/p^n E(K) \to \mathrm{H}^1_{\mathrm{Sel}}(K, E_{p^n}) \to Ш(E/K)_{p^n} \to 0$$

splits. By the elementary divisor theorem for $\mathrm{H}^1_{\mathrm{Sel}}(K, E_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}_Q}(K, E_{p^n})$ and Step 7, and by the large enough choice of n in Step 2(i) we find $m_1 \leqslant \ldots \leqslant m_{2t-1} < n$ such that

$$\mathrm{H}^1_{\mathrm{Sel}}(K, E_{p^n}) \cong E(K)/p^n E(K) \oplus \mathbb{Z}/p^{m_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{m_{2t-1}}\mathbb{Z}.$$

Again by the choice of n we know

$$\mathrm{H}^1_{\mathrm{Sel}}(K, E_{p^n}) \supset \mathbb{Z}/p^{m_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{m_{2t-1}}\mathbb{Z} \xrightarrow{\sim} Ш(E/K)_{p^n} = Ш(E/K)_{p^\infty},$$

meaning that we can construct $Ш(E/K)_{p^\infty}$ by constructing $2t-1$ independent ramified classes in $\mathrm{H}^1_{\mathrm{Sel}}(K, E_{p^n}) \subseteq \mathrm{H}^1_{\mathrm{Sel}_Q}(K, E_{p^n})$.

Step 9: Our choice of primes $\ell \in Q$ in Step 7 allows us to construct Kolyvagin classes

$$\{c_{\ell_1}, \ldots, c_{\ell_t}, c_{\ell_1\ell_2}, \ldots, c_{\ell_1\ell_t}\} \subseteq \mathrm{H}^1_{\mathrm{Sel}_Q}(K, E_{p^n}),$$

where $Q = \{\ell_1, \ldots \ell_t\}$. The assumption (ii) of Step 2 allows us to refine our choice of primes Q in Step 7, as in section §1.4 of [ÇW08], so that

- c_{ℓ_1} is ramified at ℓ_1, and
- c_{ℓ_i} and $c_{\ell_1\ell_i}$ are ramified at ℓ_i for every $i \geqslant 2$.

Finally, since the analytic rank of $E/\mathbb{Q}$ is trivial we know that the complex conjugation τ fixes c_{ℓ_i} and $\tau c_{\ell_1\ell_i} = -c_{\ell_1\ell_i}$. This implies that we have constructed $2t-1$ independent ramified classes and that $\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_{p^n})$ is contained in the subgroup of $\mathrm{H}^1(K, E_{p^n})$ generated by $\{c_{\ell_1}, \ldots, c_{\ell_t}\}$. The assumption that p is inert in $K/\mathbb{Q}$ implies that p splits completely in $K[\ell_i]/K$, where $K[\ell_i]$ denotes the ring class field of conductor ℓ_i. Consequently, the classes $\{c_{\ell_1}, \ldots, c_{\ell_t}\}$ are trivial at p and hence

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_{p^n}) \hookrightarrow \mathrm{H}^1_{\mathrm{Sel}^p}(K, E_{p^n}).$$

Since p is odd and $K/\mathbb{Q}$ is a quadratic extension it follows that

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_{p^n}) = \mathrm{H}^1_{\mathrm{Sel}^p}(\mathbb{Q}, E_{p^n}).$$

Then, using Lemma 14, we see that the intersection $Ш(E/\mathbb{Q})_{p^\infty}$ with $\mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q}, E)_{p^\infty}\right)$ is a subgroup of $\mathrm{Div}\left(Ш(E/\mathbb{Q})_{p^\infty}\right)$ which is trivial since $Ш(E/\mathbb{Q})$ is finite. □

Corollary 20. *There are infinitely many elliptic curves $E/\mathbb{Q}$ of trivial analytic rank such that the intersection of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ and $\mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q}, E)\right)$ is a $2\,\mathrm{N}$-power torsion group, where N is the conductor of $E/\mathbb{Q}$*

Proof. Recall that a Serre elliptic curve is an elliptic curve $E/\mathbb{Q}$ such that the image of the product over all p of the p-adic representations associated to the elliptic curve

$$\rho_E : \mathrm{Gal}_{\mathbb{Q}} \to \prod_p \mathrm{GL}(E_{p^\infty}) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$$

has index 2 (the minimal possible index as noticed by Serre, see [Se79] Proposition 22).

Jones [Jo10] and Zywina [Zy10] consider the set of elliptic curves $E_{a,b}$ in the form

$$Y^2 = X^3 + aX + b$$

such that a and b are integers of $\mathbb{Q}$ that lie in the box defined by $h(a, b) < x$ (where h denotes a height on such pairs). They show that the ratio of the cardinality of the subset of Serre elliptic curves by the total number of curves in the box $h(a, b) < x$ approaches 1 as x goes to infinity.

Clearly, for a Serre elliptic curve the $\mathrm{Gal}_{\mathbb{Q}}$-representation E_p is irreducible for all primes p. Hence in this sense for 'most' elliptic curves $E/\mathbb{Q}$, the $\mathrm{Gal}_{\mathbb{Q}}$-representation E_p is irreducible for every prime $p \geqslant 2$.

Friedberg and Hoffstein (see [FH95] Theorem B (1)) show that for every elliptic curve $E/\mathbb{Q}$ there are infinitely many quadratic twists $E'/\mathbb{Q}$ of trivial analytic rank. Observe that if E_p is irreducible then so is E'_p. Hence we have infinitely many elliptic curves E' of trivial analytic rank, irreducible E'_p for every prime p. It then follows that the p-primary part of $Ш(E/\mathbb{Q})$ and $\mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q}, E)\right)$ intersect trivially for every odd prime p of good reduction and the corollary follows. □

Proposition 21. *Let $E/\mathbb{Q}$ be an elliptic curve of non-trivial algebraic rank. Then*

$$\mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q}, E)\right) = \mathrm{Div}\left(Ш(E/\mathbb{Q})\right).$$

Proof. It suffices to argue for the p-primary part for every prime number p. Using (2.3) for $M = E_{p^n}$, $\mathbb{L} = \mathrm{Sel}_p$ and $\mathbb{L}_0 = \mathrm{Sel}$ together with local Tate duality, we see that

$$\frac{|\,\mathrm{H}^1_{\mathrm{Sel}_p}(\mathbb{Q}, E_{p^n})|}{|\,\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_{p^n})|} = |\,\mathrm{H}^1(\mathbb{Q}_p, E)_{p^n}| \cdot \frac{|\,\mathrm{H}^1_{\mathrm{Sel}^p}(\mathbb{Q}, E_{p^n})|}{|\,\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_{p^n})|}$$

$$\leqslant \frac{|E(\mathbb{Q}_p)/p^n E(\mathbb{Q}_p)|}{|\,\mathrm{im}\left(E(\mathbb{Q})/p^n E(\mathbb{Q}) \to E(\mathbb{Q}_p)/p^n E(\mathbb{Q}_p)\right)|} = |E(\mathbb{Q}_p)/(p^n E(\mathbb{Q}_p) + E(\mathbb{Q}))|$$

which is bounded independently of n since the algebraic rank of $E/\mathbb{Q}$ is non-trivial. In view of the discussion at the beginning of this section it then follows that $\mathrm{Div}\left(\mathrm{H}^1(\mathbb{Q}, E)_{p^\infty}\right) \subseteq \mathrm{Div}\left(Ш(E/\mathbb{Q})\right)_{p^\infty}$. The other inclusion is clear. □

Proposition 21 above can also be deduced from [Ba72] Theorem 7 and can essentially be found in [HS09] Corollary 4.2. It has the following consequence.

Corollary 22. *Let $E/\mathbb{Q}$ be an elliptic curve of analytic rank 1. Then* $\operatorname{Div}\big(\mathrm{H}^1(\mathbb{Q}, E)\big)$ *is trivial.*

Proof. Kolyvagin [Ko90] has shown that $Ш(E/\mathbb{Q})$ is finite for all elliptic curves $E/\mathbb{Q}$ of analytic rank 1 and that the algebraic rank is equal to 1 as well. Hence by Proposition 21 we find $\operatorname{Div}\big(\mathrm{H}^1(\mathbb{Q}, E)_{p^\infty}\big) \subseteq \operatorname{Div}\big(Ш(E/k)\big)_{p^\infty} = 0$ for all primes p. □

8. An example: the Jacobian of the Selmer curve

We are now discussing in detail the plane cubic

$$S = \{3X^3 + 4Y^3 + 5Z^3 = 0\}$$

describing Selmer's curve of genus 1 that violates the Hasse principle. Its Jacobian $E = \mathrm{Pic}^0_S$ is an elliptic curve over $\mathbb{Q}$ of analytic rank 0 given by the homogeneous equation

$$X^3 + Y^3 + 60Z^3 = 0 \tag{8.1}$$

with $[1 : -1 : 0]$ as its origin. The curve E has Mordell-Weil group $E(\mathbb{Q}) = 0$, see [Ca91] §18 Lemma 2, and 3-torsion in an exact sequence

$$0 \to \mu_3 \to E_3 \to \mathbb{Z}/3\mathbb{Z} \to 0, \tag{8.2}$$

which splits over a field $k/\mathbb{Q}$ if and only if 60 is a cube in k. Note that (8.2) shows that with respect to the prime $p = 3$ we are in the S_3-case excluded in Proposition 13 (on top of E_3 not being irreducible).

The curve S, as a principal homogeneous space under E describes a nontrivial 3-torsion element of $Ш(E/\mathbb{Q})$, see [Ma93] I §4 and §9. Mazur and Rubin determine

$$Ш(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

unconditionally, see [Ma93] Theorem 1 and §9, and give a list of the isomorphism classes as genus 1 curves of the principal homogeneous spaces[4] under E representing nontrivial elements of $Ш(E/\mathbb{Q})$ as, besides S,

$$\begin{aligned} S' &= \{X^3 + 5Y^3 + 12Z^3 = 0\}, \\ S'' &= \{X^3 + 4Y^3 + 15Z^3 = 0\}, \\ S''' &= \{X^3 + 3Y^3 + 20Z^3 = 0\}. \end{aligned} \tag{8.3}$$

Kummer theory and the vanishing $E(\mathbb{Q}) = 0$ yield isomorphisms

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_3) \xrightarrow{\sim} \mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_{3^n}) \xrightarrow{\sim} Ш(E/\mathbb{Q}).$$

The E_3-torsor associated to an element of $Ш(E/\mathbb{Q})$ is given by the zero set of $XYZ = 0$ in the description given by (8.1) and (8.3). The Selmer group trivial at 3 can now be determined via the defining exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{Sel}^3}(\mathbb{Q}, E_3) \to \mathrm{H}^1_{\mathrm{Sel}}(\mathbb{Q}, E_3) \to \mathrm{H}^1(\mathbb{Q}_3, E_3)$$

since we only need to check whether $XYZ = 0$ on S, S', S'' or S''' has a $\mathbb{Q}_3$-point. This is true for S and false for S', S'', S''' as can be deduced from $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^3 = \langle 2, 3\rangle$ with 10 being a cube in $\mathbb{Q}_3^*$. We conclude that

$$Ш(E/\mathbb{Q}) \supset \langle [S] \rangle = \mathrm{H}^1_{\mathrm{Sel}^3}(\mathbb{Q}, E_3) = \mathrm{H}^1_{\mathrm{Sel}^3}(\mathbb{Q}, E_{3^n}) \cong \mathbb{Z}/3\mathbb{Z}.$$

[4] The element $W \in Ш(E/\mathbb{Q})$ is isomorphic to $-W$ as a curve of genus 1.

Since $E(\mathbb{Q}_3)$ has no 3-torsion, we find by local Tate duality

$$\mathrm{H}^1(\mathbb{Q}_3, E)_{3^\infty} = \mathrm{Hom}(E(\mathbb{Q}_3), \mathbb{Q}_3/\mathbb{Z}_3) = \mathbb{Q}_3/\mathbb{Z}_3,$$

so that counting in (2.3) for $M = E_{3^n}$, $\mathbb{L} = \mathrm{Sel}_3$ and $\mathbb{L}_0 = \mathrm{Sel}$, leads to

$$|\,\mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^n})| = 3^{n+1}. \tag{8.4}$$

The map $\mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^n}) \to \mathrm{H}^1(\mathbb{Q}, E)$ is injective with image the 3^n-torsion of the subgroup

$$\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)_{3^\infty} = \ker\big(\mathrm{H}^1(\mathbb{Q}, E) \to \prod_{v\neq 3} \mathrm{H}^1(\mathbb{Q}_v, E)\big),$$

and hence

$$\mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^\infty}) = \mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)_{3^\infty} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Q}_3/\mathbb{Z}_3.$$

Here we have used the elementary fact that for a finitely cogenerated torsion group M the knowledge of the orders of n-torsion M_n for all n uniquely determines the structure as an abstract group: the sizes are given by (8.4), while

$$\mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^n}) = \big(\mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^\infty})\big)_{3^n}$$

shows that we have indeed counted the exact 3^n-torsion of a finitely cogenerated torsion group.

It follows that $Ш(E/\mathbb{Q})$ meets the maximal divisible group of $\mathrm{H}^1(\mathbb{Q}, E)$ nontrivially, namely

$$Ш(E/\mathbb{Q}) \cap \mathrm{Div}(\mathrm{H}^1(\mathbb{Q}, E)) = Ш(E/\mathbb{Q}) \cap \mathrm{Div}(\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)) \cong \mathbb{Z}/3\mathbb{Z},$$

which shows the limitation of Theorem 18 towards $p = 3$: the prime $p = 3$ happens to be a prime of additive bad reduction for $E/\mathbb{Q}$ and E_3 is a reducible $\mathrm{Gal}_{\mathbb{Q}}$-module.

We proceed to determine, which of the principal homogeneous spaces S, S', S'' or S''' generates the intersection $Ш(E/\mathbb{Q}) \cap \mathrm{Div}(\mathrm{H}^1(\mathbb{Q}, E))$, thereby preparing the answer to [Sx11] Question 49 given in Remark 25 below and completing the proof of Theorem B of the introduction.

Proposition 23. *The intersection $Ш(E/\mathbb{Q}) \cap \mathrm{Div}(\mathrm{H}^1(\mathbb{Q}, E))$ is generated by the class of the Selmer curve S.*

Proof. The Jacobian E of the Selmer curve has good reduction outside $\{2, 3, 5\}$. We set

$$U = \mathrm{Spec}(\mathbb{Z}[1/30])$$

and consider E by abuse of notation as the relative elliptic curve E/U. Since for $v = 2, 5$ neither a cube root of 60 nor ζ_3 is contained in $\mathbb{Q}_v$, we have $E_3(\mathbb{Q}_v) = 0$ and thus by local Tate-duality

$$\mathrm{H}^1(\mathbb{Q}_v, E_3) = \mathrm{H}^1(\mathbb{Q}_v, E_9) = 0$$

for $v = 2, 5$. We conclude by Corollary 4 and (3.4) that

$$\begin{aligned}
\mathrm{H}^1(U, E_3) &= \mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_3) = Ш(E/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\\
\mathrm{H}^1_{\mathrm{c}}(U, E_3) &= \mathrm{H}^1_{\mathrm{Sel}^3}(\mathbb{Q}, E_3) = \langle [S] \rangle \cong \mathbb{Z}/3\mathbb{Z},\\
\mathrm{H}^1(U, E_9) &= \mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_9) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.
\end{aligned}$$

In order to decide which element of $Ш(E/\mathbb{Q})$ generates the intersection with $\mathrm{Div}(\mathrm{H}^1(\mathbb{Q}, E))$, it suffices to check which classes are divisible by 3 in $\mathrm{H}^1(U, E_9)$ which is the 9-torsion of

$$\mathrm{H}^1(U, E_{3^\infty}) = \mathrm{H}^1_{\mathrm{Sel}_3}(\mathbb{Q}, E_{3^\infty}) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Q}_3/\mathbb{Z}_3.$$

This is controlled by a Bockstein map as we will explain now. The long exact cohomology sequence for

$$0 \to E_3 \to E_9 \to E_3 \to 0 \tag{8.5}$$

reads

$$0 \to \mathrm{H}^1(U, E_3) \to \mathrm{H}^1(U, E_9) \xrightarrow{\text{"3."}} \mathrm{H}^1(U, E_3) \xrightarrow{\beta} \mathrm{H}^2(U, E_3) \to 0$$

where the **Bockstein** map $\beta : \mathrm{H}^1(U, E_3) \to \mathrm{H}^2(U, E_3)$ is surjective by counting and Artin–Verdier duality

$$\mathrm{H}^2(U, E_3) = \mathrm{Hom}(\mathrm{H}^1_{\mathrm{c}}(U, E_3), \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$$

induced by the Weil pairing $e : E_3 \otimes E_3 \to \mu_3$, see [Zi78] Theorem 3.2 and [Zi78] Lemma 3.2.2. We introduce the **Weil–Bockstein** pairing

$$\langle -, - \rangle_{\mathrm{WB}} \ : \ \mathrm{H}^1(U, E_3) \times \mathrm{H}^1_{\mathrm{c}}(U, E_3) \to \mathbb{Z}/3\mathbb{Z}$$

$$\langle a, b \rangle_{\mathrm{WB}} = e_*\big(\beta(a) \cup b\big).$$

With the "forget support map"

$$f^i : \mathrm{H}^i_{\mathrm{c}}(U, E_3) \to \mathrm{H}^i(U, E_3)$$

and the class of the Selmer curve $s \in \mathrm{H}^1_{\mathrm{c}}(U, E_3)$ the claim of the proposition is equivalent to $\beta(f^1(s)) = 0$ which boils down to the vanishing of

$$\langle f^1(s), s \rangle_{\mathrm{WB}}.$$

Applying compactly supported cohomology to (8.5) we find the **compact Bockstein**

$$\beta_{\mathrm{c}} : \mathrm{H}^1_{\mathrm{c}}(U, E_3) \to \mathrm{H}^2_{\mathrm{c}}(U, E_3)$$

which is adjoint to β with respect to Artin–Verdier duality sponsored by the Weil pairing. Moreover, the forget support maps f^1 and f^2 are also adjoints. We can thus compute

$$\langle f^1(s), s \rangle_{\mathrm{WB}} = e_*\big(f^1(s)) \cup \beta_{\mathrm{c}}(s)\big) = e_*\big(s \cup f^2(\beta_{\mathrm{c}}(s))\big) = e_*\big(s \cup \beta(f^1(s))\big) = -\langle f^1(s), s \rangle_{\mathrm{WB}}$$

due to anti-symmetry of the Weil-pairing, so that indeed $\langle f^1(s), s \rangle_{\mathrm{WB}} = 0$. □

Remark 24. The proof of Proposition 23 given above can be used to identify the pairing $\langle -, - \rangle_{\mathrm{WB}}$ with the restriction of the Cassels–Tate pairing on $Ш(E/\mathbb{Q})$ in the form of the "Weil–pairing definition" of Poonen and Stoll [PS99] §12.2.

Remark 25. Proposition 23 answers [Sx11] Question 49. The Selmer curve $S/\mathbb{Q}$ provides an explicit example for a smooth projective curve with no rational point over $\mathbb{Q}$, but rational points everywhere locally, and nevertheless split fundamental group extension

$$1 \to \pi_1(\overline{S}, \bar{s}) \to \pi_1(S, \bar{s}) \to \mathrm{Gal}_k \to 1$$

due to [Sx12] Corollary 177. The splitting obviously does not come from a rational point, see [Sx12] §13 for the context of the section conjecture of anabelian geometry.

Remark 26. We will show in a subsequent paper [ÇS12], when we discuss the divisibility question in the sense of Cassels, that $Ш(E/\mathbb{Q})$, and consequently $\mathrm{H}^1_{\mathrm{div}}(\mathbb{Q}, E)_{3^\infty}$, is contained in $\mathrm{div}(\mathrm{H}^1(\mathbb{Q}, E))$. Therefore the Jacobian of the Selmer curve gives a concrete example where the filtration (1.1) of the introduction has all its steps nontrivial.

References

AI82 Anderson, G., Ihara, Y., Pro-ℓ branched coverings of $\mathbb{P}^1$ and higher circular ℓ-units, *Ann. of Math.* (2) **128** (1988), no. 2, 271–293.

Ba64 Bashmakov, M. I., On the divisibility of principal homogeneous spaces over Abelian varieties, *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 661–664.

Ba72 Bashmakov, M. I., The cohomology of abelian varieties over a number field, (English translation) *Russian Math. Surveys* **27** (1972), no. 6, 25–70.

Ca62 Cassels, J. W. S., Arithmetic on curves of genus 1. III. The Tate-Shafarevic and Selmer groups, *Proc. London Math. Soc.* (3) **12** 1962, 259–296.

Ca91 Cassels, J. W. S., *Lectures on elliptic curves*, London Mathematical Society Student Texts **24**, Cambridge University Press, 1991, vi+137pp.

ÇS12 Çiperiani, M., Stix, J., Weil–Châtelet divisible elements in Tate–Shafarevich groups II: On a question of Cassels, preprint, 2012.

ÇW08 Çiperiani, M., Wiles, A., Solvable points on genus one curves, *Duke Mathematical Journal* **142** (2008), no. 3, 381–464.

FH95 Friedberg, S., Hoffstein, J., Nonvanishing theorems for automorphic L-functions on GL(2), *Ann. of Math.* (2) **142** (1995), no. 2, 385–423.

HS09 Harari, D., Szamuely, T., Galois sections for abelianized fundamental groups, with an Appendix by E. V. Flynn, *Math. Ann.* **344** (2009), no. 4, 779–800.

Ja88 Jannsen, U., Continuous étale cohomology, *Math. Annalen* **280** (1988), 207–245.

Jo10 Jones, N., Almost all elliptic curves are Serre curves, *Trans. Amer. Math. Soc.* **362** (2010), no. 3, 1547–1570.

Ko90 Kolyvagin, V. A., Euler systems, *The Grothendieck Festschrift*, Vol. II, Progr. Math., 87, Birkhauser Boston, Boston, MA, 1990, 435–483.

Ma78 Mazur, B., Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47**, (1978), 33–186.

Ma93 Mazur, B., On the passage from local to global in number theory, *Bull. Amer. Math. Soc.* **29** (1993), no. 1, 14–50.

Mi86 Milne, J.S., *Arithmetic duality theorems*, Perspectives in Mathematics, 1. Academic Press, Inc., Boston, MA, 1986.

Ne75 Neumann, O., p-closed algebraic number fields with bounded ramification, *Izv. Akad. Nauk SSSR Ser. Mat.* **39** (1975), no. 2, 259–271, 471.

NSW08 Neukirch, J., Schmidt, A., Wingberg, K., *Cohomology of number fields*, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, 2008, xvi+825pp.

PS99 Poonen, B., Stoll, M., The Cassels-Tate pairing on polarized abelian varieties, *Ann. of Math. (2)* **150** (1999), no. 3, 1109–1149.

Ri97 Ribet, K., Images of semistable Galois representations, *Pacific J. of Math.* **181** (1997), no. 3, 277–297.

Se72 Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), no. 4, 259–331.

Se79 Serre, J.-P., Points rationnels des courbes modulaires $X_0(N)$ [d'après Barry Mazur], *Séminaire Bourbaki* (1977/78), exposé **511**, Lecture Notes in Math. **710** (1979), 89–100.

Sh63 Shafarevich, I. R., Extensions with given ramification points (russian), *Publ. Math. IHES* **18** (1963), 71–95, translated in *Amer. Math. Soc. Transl.* **59** (1966), 128–149.

Sx11 Stix, J., The Brauer–Manin obstruction for sections of the fundamental group, *Journal of Pure and Applied Algebra* **215** (2011), no. 6, 1371–1397.

Sx12 Stix, J., *Rational Points and Arithmetic of Fundamental Groups: Evidence for the Section Conjecture*, Springer Lecture Notes in Mathematics **2054**, Springer, 2012, xx+247 pp.

Zi78 Zink, Th., Étale cohomology and duality in number fields, Appendix 2 in: Haberland, K., *Galois Cohomology of Algebraic Number Fields*, VEB Deutscher Verlag der Wissenschaften, 1978.

Zy10 Zywina, D., Elliptic curves with maximal Galois action on their torsion points, *Bull. Lond. Math. Soc.* **42** (2010), no. 5, 811–826.

Mirela Çiperiani mirela@math.utexas.edu
Department of Mathematics, the University of Texas at Austin, 1 University Station, C1200 Austin, Texas 78712, USA

Jakob Stix stix@mathi.uni-heidelberg.de
Mathematisches Institut, Universität Heidelberg, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany