LOCALLY TRIVIAL TORSORS THAT ARE NOT WEIL-CHÂTELET DIVISIBLE

BRENDAN CREUTZ

Abstract. For every prime p we give infinitely many examples of torsors under abelian varieties over $\mathbb{Q}$ that are locally trivial but not divisible by p in the Weil-Châtelet group. We also give an example of a locally trivial torsor under an elliptic curve over $\mathbb{Q}$ which is not divisible by 4 in the Weil-Châtelet group. This gives a negative answer to a question of Cassels.

1. Introduction

Let A be an abelian variety over a number field k with algebraic closure $\overline{k}$. A k-torsor under A is a variety T/k together with a simply transitive algebraic group action of A on T which is defined over k. The isomorphism classes of such torsors are parameterized by the Galois cohomology group $\mathrm{H}^1(A) := \mathrm{H}^1(k, A(\overline{k}))$, commonly known as the *Weil-Châtelet group*. The subgroup $Ш(A) \subset \mathrm{H}^1(A)$ consisting of classes which become trivial over every completion of k is known as the *Tate-Shafarevich group*. A torsor is trivial precisely when it possesses a rational point, so the classes in $Ш(A)$ are precisely those represented by torsors which have points everywhere locally.

It is conjectured that $Ш(A)$ is finite, and this is known for some modular abelian varieties including all elliptic curves over $\mathbb{Q}$ of analytic rank at most one. For principally polarized abelian varieties it is known that the order of $Ш(A)$, if finite, is either a square or 2 times a square [20]. This follows from the existence of a canonical antisymmetric pairing on $Ш(A)$ whose kernel is the maximal divisible subgroup. The pairing was first defined by Cassels [6] in the case of elliptic curves. While doing so he raised the question of whether the elements of $Ш(A)$ are infinitely divisible in the larger group $\mathrm{H}^1(A)$ [6, Problem 1.3], noting that an affirmative answer would allow him to show that the kernel of the pairing is the maximal divisible subgroup. He was subsequently able to use the weaker result, furnished by Tate, that $Ш(A) \subset p\,\mathrm{H}^1(A)$ when A is an elliptic curve and p is prime to obtain his result on the pairing [7]. He notes, however, that the question of divisibility remained open [7, Problem (b)].

The issue was then taken up by Bashmakov [1, 2] who showed that for certain CM abelian varieties the elements of $Ш(A)$ are infinitely p-divisible in $\mathrm{H}^1(A)$ whenever p is sufficiently large (depending on A). This would also hold, of course, if $Ш(A)$ were finite. Bashmakov's method makes use of results of Serre on the representation of Galois in the Tate module [22]. These have subsequently been extended and improved by Bogomolov and by Serre [3, 23], in effect extending Bashmakov's result to arbitrary abelian varieties. Recently Çiperiani and Stix [9] have given a more refined analysis and, consequently, explicit bounds on p. In particular, they have shown that for elliptic curves over $\mathbb{Q}$, p-divisibility holds for all $p > 7$ [9, Theorem

A]. Moreover, for a fixed elliptic curve over $\mathbb{Q}$, they show that p-divisibility can fail for at most one odd prime, and then for at most two quadratic twists of the given curve.

The main result of this paper is that, despite the mounting evidence, the answer to Cassels' question is in general no.

Theorem 1. *There exists an elliptic curve $A/\mathbb{Q}$ such that $Ш(A) \not\subset 4\,\mathrm{H}^1(A)$.*

Theorem 2. *For every prime p there exist infinitely many non-isomorphic abelian varieties $A/\mathbb{Q}$ such that $Ш(A) \not\subset p\,\mathrm{H}^1(A)$.*

The key to these examples is the characterization of when $Ш(A) \subset n\,\mathrm{H}^1(A)$ given in Theorem 3 below. One consequence of this is an algorithm that, at least in principle, can determine whether $Ш(A)[n] \subset n\,\mathrm{H}^1(A)$ for any n. The example (see Theorem 5) we give to prove Theorem 1 is the curve of smallest conductor (it is 1025) with this property. It was originally found using a crude implementation of the algorithm in `Magma` [4], though the verification we give here is different. The examples for Theorem 2 are constructed using a slightly different approach. They come from Jacobians of cyclic covers of the projective line of genus $(p^3 - 3p + 2)/2$ defined over the p-th cyclotomic field. We obtain examples over $\mathbb{Q}$ (of dimension larger by a factor of $(p-1)$) using restriction of scalars.

Acknowledgments. The author would like to thank Mirela Çiperiani and Jakob Stix for their comments, encouragement and useful discussions.

2. Characterizing divisibility by n

Let $\mathfrak{g}_k$ denote the absolute Galois group of the number field k. For a $\mathfrak{g}_k$-module M and a nonnegative integer i, we use $\mathrm{H}^i(k, M)$ to denote Galois cohomology groups, and let $Ш^i(M)$ denote the kernel of the map $\mathrm{H}^i(k, M) \to \prod \mathrm{H}^i(k_v, M)$, the product running over all completions k_v of k. When the base field is clear we will write $\mathrm{H}^1(M)$ in place of $\mathrm{H}^1(k, M)$. For a morphism $\phi : M \to M'$ of $\mathfrak{g}_k$-modules we will use $M[\phi]$, $\mathrm{H}^i(M)[\phi]$ and $Ш^i(M)[\phi]$ to denote the subgroups killed by ϕ.

Cassels' pairing on the Shafarevich-Tate group of an elliptic curve was generalized by Tate to a pairing $Ш(A) \times Ш(\hat{A}) \to \mathbb{Q}/\mathbb{Z}$, where $\hat{A}$ denotes the dual abelian variety [25]. Tate showed that the left and right kernels are the divisible subgroups. This was derived as an easy consequence of (and motivation for) his global arithmetic duality theorems, also developed independently by Poitou. The same tools allow one to characterize the divisibility of $Ш(A)$ by n in $\mathrm{H}^1(A)$.

Theorem 3. *Let A be an abelian variety over a number field and n an integer. In order that $Ш(A) \subset n\,\mathrm{H}^1(A)$ it is necessary and sufficient that the image of the natural map $Ш^1(\hat{A}[n]) \to Ш(\hat{A})$ is contained in the maximal divisible subgroup of $Ш(\hat{A})$.*

Since the maximal divisible subgroup of $Ш(\hat{A})$ is the (right) kernel of the pairing Theorem 3 is a consequence of the following.

Theorem 4. *Suppose $\phi : B \to A$ is an isogeny of abelian varieties over a number field with dual isogeny $\hat{\phi} : \hat{A} \to \hat{B}$, and let $T \in Ш(A)$. There exists $T' \in \mathrm{H}^1(B)$ such that $\phi T' = T$ if and only if T is orthogonal to the image of the map $Ш^1(\hat{A}[\hat{\phi}]) \to Ш(\hat{A})$ induced by the inclusion $\hat{A}[\hat{\phi}] \subset \hat{A}$.*

Proof. Let $T \in Ш(A)$ and let $\delta : \mathrm{H}^1(A) \to \mathrm{H}^2(B[\phi])$ be the connecting homomorphism arising from the exact sequence $0 \to B[\phi] \to B \xrightarrow{\phi} A \to 0$. There exists a lift of T as in the statement of the theorem if and only if $\delta(T) = 0$. We want to show that this is the case if and only if the character

$$Ш^1(\hat{A}[\hat{\phi}]) \xrightarrow{i} Ш(\hat{A}) \xrightarrow{\langle T, \bullet \rangle_{CT}} \mathbb{Q}/\mathbb{Z}\,, \tag{1}$$

induced by the inclusion $i : \hat{A}[\hat{\phi}] \subset \hat{A}$ and the Cassels-Tate pairing $\langle\ ,\ \rangle_{CT}$ is trivial.

The kernels of ϕ and $\hat{\phi}$ are dual (as $\mathfrak{g}_k$-modules), so Poitou-Tate duality [25, Theorem 3.1] gives an isomorphism $Ш^2(B[\phi]) \cong Ш^1(\hat{A}[\hat{\phi}])^*$, where for an abelian group G, $G^* = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. On the other hand, the Cassels–Tate pairing gives a map $Ш(A) \to Ш(\hat{A})^*$, and δ maps $Ш(A)$ to $Ш^2(B[\phi])$. These maps form a diagram:

$$\begin{array}{ccc} Ш(A) & \xrightarrow{\delta} & Ш^2(B[\phi]) \\ \downarrow & & \downarrow \cong \\ Ш(\hat{A})^* & \xrightarrow{i^*} & Ш^1(\hat{A}[\hat{\phi}])^* \end{array} \tag{2}$$

If the diagram commutes, then the image of $\delta(T)$ under the vertical map on the right is the character (1), in which case the proof is complete since the vertical map on the right is an isomorphism. So it only remains to prove that (2) commutes.

To that end let $\eta \in Ш^1(\hat{A}[\hat{\phi}])$. We must show that $\langle \delta(T), \eta \rangle_{PT} = \langle T, i(\eta) \rangle_{CT}$, where $i(\eta)$ is the image of η in $Ш(\hat{A})$ and $\langle\ ,\ \rangle_{PT}$ denotes the pairing coming from Poitou–Tate duality. This will be achieved by comparing the *Weil pairing definition* for the Cassels–Tate pairing with an explicit description of the Poitou–Tate pairing. We use C^i and Z^i for the functors taking a Galois module to the corresponding group of continuous i-cochains and i-cocycles (respectively), and use $d : C^i \to Z^{i+1} \subset C^{i+1}$ for the differential operator.

We begin by computing $\langle T, i(\eta) \rangle_{CT}$ using the *Weil pairing definition* in [20, Section 12]. As $Ш(A)$ is torsion we can choose an integer m such that $mT = 0$. Let $\tau \in Z^1(k, A[m])$ represent a lift of T under the surjective map $\mathrm{H}^1(k, A[m]) \to \mathrm{H}^1(k, A)[m]$, and let $\tau' \in Z^1(k, \hat{A}[\hat{\phi}])$ be a representative for η (note τ' is a representative for a lift of $i(\eta)$ to $\mathrm{H}^1(k, \hat{A}[\hat{\phi}])$). Choose $\sigma \in C^1(k, B[m\phi])$ such that $\phi\sigma = \tau$. Note that $d\sigma$ lies in $Z^2(k, B[\phi])$ and (by definition of the connecting homomorphism) represents $\delta(T) \in Ш^1(B[\phi])$. Since $\mathrm{H}^3(k, \bar{k}^\times) = 0$, there exists $\bar{\epsilon} \in C^2(k, \bar{k}^\times)$ such that $d\bar{\epsilon} = d\sigma \cup \tau'$.

Since T is locally trivial, for each v we can choose $\beta_v \in A(\bar{k}_v) = Z^0(k_v, A)$ such that the image of τ in $Z^1(k_v, A)$ is equal to $d\beta_v$. Now choose $Q_v \in A(\bar{k}_v)$ such that $\phi Q_v = \beta_v$, and set $\rho_v = dQ_v$. For each v, $((\mathrm{res}_v(\sigma) - \rho_v) \cup \mathrm{res}_v(\tau') - \bar{\epsilon}_v)$ is a 2-cocycle representing a class c_v in $\mathrm{H}^2(k_v, \bar{k}_v^\times)$. In [20, Section 12] it is shown that the Cassels-Tate pairing is the sum of the local invariants of these classes:

$$\langle T, i(\eta) \rangle_{CT} = \sum_v \mathrm{inv}(c_v)\,.$$

Now we will compute $\langle \delta(T), \eta \rangle_{PT}$ using Tate's definition in [25, Section 3]. One must choose a cocycle $f \in Z^2(B[\phi])$ representing $\delta(T)$ and, for each prime v, a cochain $g_v \in C^1(G_v, B[\phi])$ such that $dg_v = \mathrm{res}_v(f)$. The definition also involves $h \in C^2(k, \bar{k}^\times)$ such that $dh = f \cup \tau'$ (which exists since $\mathrm{H}^3(k, \bar{k}^\times) = 0$). The pairing

is defined as the sum over all v of the invariants $(g_v \cup \mathrm{res}_v(\eta)) - \mathrm{res}_v(h) \in Z(k_v, \bar{k}_v^\times)$. In the notation above we may take $f = d\sigma$ and $g_v = (\mathrm{res}_v(\sigma) - \rho_v)$ and $h = \bar{\epsilon}$. Then c_v is represented by $(g_v \cup \mathrm{res}_v(\eta)) - \mathrm{res}_v(h)$, and so

$$\langle \delta(T), \eta \rangle_{PT} = \sum_v \mathrm{inv}(c_v)\,,$$

exactly as above. Thus (2) commutes. □

2.1. **Remarks.** In regard to Theorem 4, it is well known that the stronger requirement that T' lie in $Ш(B)$ can be met if and only if T is orthogonal to $Ш(\hat{A})[\hat{\phi}_*]$ (see e.g. [7, Lemma 4.1], [8, Corollary to Theorem 1.2], [11, Lemma 2.5] or [14, Lemma I.6.17]). In regard to Theorem 3, the fact that the vanishing of $Ш^1(\hat{A}[n])$ implies that the elements of $Ш(A)$ are divisible by n in $\mathrm{H}^1(A)$ has been applied many times over. The results of Bashmakov, Çiperiani-Stix and Tate's result that $Ш(E) \subset p\,\mathrm{H}^1(E)$ all reduce to establishing that $Ш^1(\hat{A}[n])$ is trivial under suitable circumstances.

From the Kummer sequence,

$$0 \to \hat{A}(k)/n\hat{A}(k) \to \mathrm{H}^1(\hat{A}[n]) \to \mathrm{H}^1(\hat{A})[n] \to 0\,,$$

it is clear that the vanishing of $Ш^1(\hat{A}[n])$ implies a local-global principle for divisibility by n in $\hat{A}(k)$. This has been studied by Dvornicich-Zannier [12] and later by Paladino-Ranieri-Viada [18]. Their positive results are also established by showing that $Ш^1(\hat{A}[n])$ vanishes under suitable hypothesis. Dvornicich-Zannier [13] and Paladino [16, 17] provide examples where the local-global principle for divisibility by n in $A(k)$ fails (and hence for which $Ш^1(\hat{A}[n]) \neq 0$) in the case of elliptic curves over $\mathbb{Q}$ with $n = 4$, as well as inferring the existence of such examples for larger prime powers over higher degree number fields.

If one is willing to assume that $Ш(\hat{A})$ contains no nontrivial divisible elements, then Theorem 3 may be interpreted as saying that a nontrivial elements of $Ш^1(\hat{A}[n])$ always poses a nontrivial obstruction to the local-global principle for divisibility by n, either in $\hat{A}(k)$ or in $\mathrm{H}^1(A)$.

3. The Example for Theorem 1

Theorem 5. *Let E be the elliptic curve over $\mathbb{Q}$ with Weierstrass equation*

$$E : y^2 = x(x + 80)(x + 205)\,.$$

Then $Ш(E) \not\subset 4\,\mathrm{H}^1(E)$.

Remark 6. *This is the smallest elliptic curve over $\mathbb{Q}$ (ordered by conductor) with this property. It is labelled* `1025b2` *in Cremona's Database* [10].

Proof. Since $E[2] \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$ as a $\mathfrak{g}_\mathbb{Q}$-module, Kummer theory gives an isomorphism $\mathrm{H}^1(K, E[2]) \simeq \left(K^\times/K^{\times 2}\right)^2$. The composition of this isomorphism with the connecting homomorphism $\delta : E(K) \to \mathrm{H}^1(K, E[2])$ is given explicitly by [24, Proposition X.1.4]. Namely, using the basis $P_1 = (0, 0)$, $P_2 = (-80, 0)$ for $E[2]$ the

composition is given by

$$P = (x, y) \longmapsto \begin{cases} (x, x + 80) & \text{if } P \neq P_1, P_2 \\ (41, 5) & \text{if } P = P_1 \\ (-5, -1) & \text{if } P = P_2 \\ (1, 1) & \text{if } P = 0 \end{cases}$$

Let us consider the class $\xi \in \mathrm{H}^1(\mathbb{Q}, E[2])$ represented by $(1, 5)$. We claim that for every prime p, the image of ξ in $\mathrm{H}^1(\mathbb{Q}_p, E[2])$ lies in the image of $E[2]$ under the local connecting homomorphism $E(\mathbb{Q}_p) \to \mathrm{H}^1(\mathbb{Q}_p, E[2])$. Assuming this we can complete the proof as follows. For any $K/\mathbb{Q}$ the exact sequence

$$0 \to E[2] \to E[4] \to E[2] \to 0$$

induces an exact sequence

$$E[2] \xrightarrow{\delta} \mathrm{H}^1(K, E[2]) \to \mathrm{H}^1(K, E[4])\,.$$

Thus our claim implies that the image of ξ in $\mathrm{H}^1(\mathbb{Q}, E[4])$ lies in $Ш^1(E[4])$. On the other hand, E has analytic rank 0. This implies that $Ш(E)$ is finite and, in particular, that it contains no nontrivial divisible elements. Also since $E(\mathbb{Q}) = E[2]$ and ξ is clearly not contained in $\delta(E[2])$, the image of ξ in $Ш(E)$ is nontrivial. The result then follows from Theorem 3.

It remains to establish the claim. Equivalently we must show that for every p, the image ξ_p of $(1, 5)$ in $(\mathbb{Q}_p/\mathbb{Q}_p^{\times 2})^2$ is represented by at least one of the pairs $(1, 1), (41, 5), (-5, -1)$, or $(-205, -5)$. If $5 \in \mathbb{Q}_p^{\times 2}$ or if $41 \in \mathbb{Q}_p^{\times 2}$, then ξ_p is clearly represented by the first or by the second pair, respectively. This covers the case when $p \in \{2, 5, 41, \infty\}$. For any other p, all the entries lie in $\mathbb{Z}_p^\times$, which has exactly 2 square classes. If $-5 \in \mathbb{Q}_p^{\times 2}$, then -1 and 5 have the same square class, and we see that ξ_p is represented by the third pair. If none of 5, -5 or 41 is a square in $\mathbb{Q}_p^\times$, then they all have the same square class and $-205 = (-5) \cdot 41 \in \mathbb{Q}_p^{\times 2}$, so ξ_p is represented by the fourth pair. The cases considered are exhaustive, so the claim is proven. □

Remark 7. *In the example $Ш(E) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and it is possible to write down models for the corresponding torsors as double covers of $\mathbb{P}^1$. The torsor corresponding to ξ is given by*

$$T_1 : y^2 = (11x^2 - 67x + 31)(-x^2 - 3x - 1)\,.$$

The other two nontrivial elements are given by

$$T_2 : y^2 = (11x^2 - 34x + 19)(x^2 + 6x + 4)\,, \text{ and}$$
$$T_3 : y^2 = (11x^2 - 89x - 11)(-x^2 - x + 1)\,.$$

Since there are no elements of order 4 in $Ш(E)$, T_1 pairs nontrivially with both T_2 and T_3. So by Theorem 4 we see that $T_2, T_3 \notin 4\,\mathrm{H}^1(E)$. On the other hand, arguing as in the proof it is possible to show that neither T_2 nor T_3 lies in the image of $Ш^1(E[4])$. Thus $T_1 \in 4\,\mathrm{H}^1(E)$.

4. The Examples for Theorem 2

As mentioned in the introduction, our examples are Jacobians of cyclic covers of the projective line. We begin by fixing some notation. Let X be a cyclic cover of $\mathbb{P}^1$ of prime degree p defined over a field k of characteristic prime to p containing the p-th roots of unity. We will assume that the covering is not ramified above $\infty \in \mathbb{P}^1$ (this can always be arranged by a change of the coordinate on $\mathbb{P}^1$ when k is infinite). By Kummer theory, X has a (possibly singular) model of the form $y^p = cf(x)$ where $c \in k^\times$ and $f \in k[x]$ has degree divisible by p (since there is no ramification at ∞) and leading coefficient 1. Let Ω denote the set of ramification points. The 0-cycles of degree 0 supported on Ω generate a subgroup J_ϕ of the the p-torsion subgroup of the Jacobian $J = \mathrm{Jac}(X)$. There is an action of μ_p on $X/\mathbb{P}^1$ given by $\zeta \cdot (x, y) = (x, \zeta y)$, which induces an inclusion of the cyclotomic ring $\mathbb{Z}[\mu_p]$ in $\mathrm{End}(J)$. The subgroup J_ϕ is the kernel of the isogeny $\phi = (1 - \zeta) \in \mathrm{End}(J)$ where ζ is a (hereupon fixed) primitive p-th root of unity (see [21, Proposition 3.2]).

For any $\omega \in \Omega$ the 1-cocycle $\xi : \mathfrak{g}_k \ni \sigma \mapsto (\sigma(\omega) - \omega) \in J_\phi$ represents a class in $\mathrm{H}^1(J_\phi)$, which we will again denote by ξ. The class of this cocycle does not depend on the choice for ω. One can easily determine if it is trivial with the following (see [19, Lemma 11.2]).

Lemma 8. *ξ is trivial if and only if*

1. *f has a factor of degree prime to p, or*
2. *$p = 2$, $\deg(f) \equiv 2 \mod 4$ and $f(x)$ factors over some quadratic extension K as $f = cg\bar{g}$ where $g, \bar{g} \in K[x]$ are $\mathrm{Gal}(K/k)$ conjugates.*

The image of ξ under the natural map $\mathrm{H}^1(J_\phi) \to \mathrm{H}^1(J)$ is represented by the torsor $\mathbf{Alb}^1_X$ paremeterizing 0-cycles of degree 1 on X. In the global situation, Lemma 8 gives us a way to ensure that $\mathbf{Alb}^1_X$ lies in the image of $Ш^1(J_\phi) \to Ш(J)$. For example, if we choose f so as to have a root in every completion this will be the case. The more involved task of arranging that $\mathbf{Alb}^1_X$ is not divisible in $Ш(J)$ will be achieved with the following.

Lemma 9. *Suppose k is a number field and that X has points everywhere locally. Let L denote the k-algebra $k[x]/f$, and let $N_{L/k} : L \to k$ denote the norm. If $c \notin N_{L/k}(L^\times)k^{\times p}$, then $\mathbf{Alb}^1_X \notin \phi Ш(J)$.*

This follows directly from [11, Theorem 4.6], and the details are to be found there. We simply summarize the principal train of thought. There is an explicit construction which, given $\alpha \in L^\times$ such that $cN(\alpha) \in k^{\times p}$, produces an unramified covering of X. The coverings produced this way are in fact torsors under J_ϕ (whose *type* in the sense of Colliot-Thélène and Sansuc's theory of torsors under groups of multiplicative type is given by $J_\phi \hookrightarrow J(\bar{k}) = \mathrm{Pic}^0(\bar{X}) \subset \mathrm{Pic}(\bar{X})$). One can show that every such torsor with the property (call it **P**) that the pullbacks of the ramification points are linearly equivalent to k-rational divisors arises in this way. Geometric class field theory gives a bijective correspondence between abelian X-torsors and abelian $\mathbf{Alb}^1_X$-torsors. One can show that any $\mathbf{Alb}^1_X$-torsor of type J_ϕ that has points everywhere locally corresponds to an X-torsor of type J_ϕ with property **P** (assuming X has points everywhere locally). On the other hand, a k-torsor T under J can be made into an $\mathbf{Alb}^1_X$-torsor under J_ϕ if and only if

$\phi T = \mathbf{Alb}^1_X$ in $\mathrm{H}^1(J)$. Thus $\mathbf{Alb}^1_X$ lies in $\phi Ш(J)$ if and only there is some $\mathbf{Alb}^1_X$-torsor under J_ϕ that has points everywhere locally. As described above, this would imply that c is a norm modulo p-th powers.

Remark 10. *In the case $p = 2$, Bruin and Stoll asked* [5, Question 7.2] *if it were possible to find X that is everywhere locally solvable for which c is not a norm modulo squares. It was this question that originally motivated our construction of the examples in the following theorem.*

Theorem 11. *Let $k = \mathbb{Q}(\zeta)$ where ζ is a primitive p-th root of unity. Let p and q be rational primes satisfying $q \equiv 1 \mod p^2$ (resp. modulo 8 if $p = 2$). Let*

$$f(x) = (x^p - \zeta)(x^p - q)(x^p - \zeta q) \cdots (x^p - \zeta^{p-1} q)\,.$$

There are infinitely many classes $c \in k^\times / k^{\times p}$ such that the Jacobian J of the cyclic cover of $\mathbb{P}^1_k$ defined by $y^p = cf(x)$ satisfies $Ш(J) \not\subset p\,\mathrm{H}^1(J)$. In particular, there are infinitely many non-isomorphic abelian varieties over k with this property.

Proof. The condition on p and q ensures that the first and second factors of $f(x)$ have a linear factor over $\mathbb{Q}_q$ and over $\mathbb{Q}_p$, respectively. For primes of k not lying above p or q, Hensel's Lemma shows that the factorization of $f(x)$ can be determined by working over the residue field. By the pigeonhole principle at least one of the reductions of $\zeta, q, \zeta q, \ldots, \zeta^{p-1} q$ must be a p-th power. Thus we conclude that $f(x)$ has a linear factor over every completion of k. By Lemma 8 this implies that $\mathbf{Alb}^1_X$ lies in the image of $Ш(J_\phi) \to Ш(J)$ (for any $c \in k^\times$).

If $c \in k^\times$ is not a norm modulo p-th powers from $L = k[x]/f(x)$, then by Lemma 9 the class of $\mathbf{Alb}^1_X$ in $Ш(J)$ is not divisible by ϕ. As the induced pairing on $Ш(J)/\phi Ш(J) \times Ш(J)[\phi]$ is nondegenerate there must exist some $T \in Ш(J)[\phi]$ pairing nontrivially with $\mathbf{Alb}^1_X$. By Theorem 4, T is not divisible by ϕ. This implies that $T \notin pШ(J)$ since ϕ^{p-1} equals p up to a unit in $\mathrm{End}(J)$. Thus the proof will be complete if we can show that there are infinitely many distinct classes in $k^\times / k^{\times p}$ that remain nontrivial in the quotient $k^\times / N_{L/k}(L^\times) k^{\times p}$.

We claim that if $\mathfrak{r}$ is a prime of k lying above a rational prime r distinct from p and q such that $\mathfrak{r}$ splits in the extension defined by $x^p - \zeta^i q$ for some $i \in \{1, \ldots, p-1\}$, and is inert in the extension defined by $x^p - \zeta$, then $r \notin N_{L/k}(L^\times) k^{\times p}$. Clearly the set of such primes has positive density and these r lie in distinct cosets of $k^{\times p}$. Since $[k : \mathbb{Q}] = p - 1$ it will suffice to show that for any such r we have $r \notin N_{L/\mathbb{Q}}(L^\times)\mathbb{Q}^{\times p}$. By way of contradiction, let us suppose r is such a prime and that we can find $\alpha \in L^\times$ and $z \in \mathbb{Q}^\times$ such that $N_{L/\mathbb{Q}}(\alpha) = r z^p$.

Set $K_1 = k(\sqrt[p]{\zeta})$ and $K_2 = k(\sqrt[p]{q})$. For $i = 1, \ldots, p-1$ the extensions of k defined by $x^p - \zeta^i q$ all define the same extension of $\mathbb{Q}$, which we will denote by K_3. For a rational prime s distinct from p and q let $\tau_i(s)$ be the greatest common divisor of the inertia degrees of the primes in K_i above s. Then $\tau_1(s)$ is prime to p if and only if $\zeta \in k_{\mathfrak{s}}^{\times p}$ for every completion of k at a prime $\mathfrak{s}$ above s, and this occurs if and only if s is a p-th power modulo p^2. Similarly $\tau_2(s)$ is prime to p if and only if $q \in k_{\mathfrak{s}}^{\times p}$ for every $\mathfrak{s}$ above s. Finally $\tau_3(s)$ is prime to p if and only if $\zeta q \in k_{\mathfrak{s}}^{\times p}$ for some $\mathfrak{s}$ above s. Thus, when s is not a square modulo p^2, at most one of $\tau_1(s)$, $\tau_2(s)$ and $\tau_3(s)$ can be prime to p.

As a $\mathbb{Q}$-algebra, L splits as $K_1 \times K_2 \times K_3 \times \cdots \times K_3$, and the norm $N_{L/\mathbb{Q}}$ is simply the product of the norms of the individual factors. So without loss of generality we can assume the image of α under the splitting is given by $\alpha = (\alpha_1, \alpha_2, \alpha_3, 1, \ldots, 1)$

with $\alpha_i \in K_i^\times$. The assumption on r implies that $\tau_1(r)$ and $\tau_2(r)$ are divisible by p. So we see that the r-adic valuations of $N_{K_1/\mathbb{Q}}(\alpha_1)$ and $N_{K_2/\mathbb{Q}}(\alpha_2)$ are divisible by p. Thus the r-adic valuation of $N_{K_3/\mathbb{Q}}(\alpha_3)$ must be congruent to 1 modulo p.

The completion of K_3 at the prime above p is the p^2-cyclotomic extension of $\mathbb{Q}_p$ (since $q \in \mathbb{Q}_p^{\times p}$). Using higher ramification theory one gets that $N_{K_3/\mathbb{Q}}(\mathcal{O}_{K_3}) \subset 1+p^2\mathbb{Z}$ (or see [15, Satz V.1.8] for a direct proof). As r is not a p-th power modulo p^2 (and in particular not in $1+p^2\mathbb{Z}$), there must exist some rational prime s distinct from r and not in $1+p^2\mathbb{Z}$ such that the s-adic valuation of $N_{K_3/\mathbb{Q}}(\alpha_3)$ is prime to p. This means that $\tau_3(s)$ is prime to s. Thus $\tau_1(s)$ and $\tau_2(s)$ are divisible by p. But then the s-adic valuation of $N_{L/\mathbb{Q}}(\alpha)$ is prime to p which is a contradiction. This completes the proof □

To complete the proof of Theorem 2 it suffices to note that for a finite extension K/k and an abelian variety A over K, restriction of scalars gives an isomorphism $\mathrm{H}^1(K, A) \cong \mathrm{H}^1(k, R_{K/k}(A))$. Thus the examples in the theorem also give rise to examples over $\mathbb{Q}$. For a concrete example we may take $X : y^2 = 3(x^2+1)(x^2+17)(x^2-17)$. Its Jacobian is an abelian surface $J/\mathbb{Q}$ with $Ш(J) \not\subset 2\,\mathrm{H}^1(J)$.

References

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

[2] M.I. Bašmakov: *The cohomology of abelian varieties over a number field*, (Russian) Uspehi Mat. Nauk **27** (1972), 25–66; (English Translation) Russian Math. Surv. **27** (1972) 25–70.

[3] F. Bogomolov: *Points of finite order on an abelian variety*, Izv. Akad. Nauk SSSR Ser. Mat., **44** (1980) 782–804.

[4] W. Bosma, J. Cannon and C. Playoust: *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) 235–265.

[5] N. Bruin and M. Stoll: *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009) 2347–2370.

[6] J.W.S. Cassels: *Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups*, Proc. London Math. Soc. **12** (1962) 259–296.

[7] J.W.S. Cassels: *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962) 95–112.

[8] J.W.S. Cassels: *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965) 180–189.

[9] M. Çiperiani and J. Stix: *Weil–Châtelet divisible elements in Tate–Shafarevich groups II: On a question of Cassels*, (preprint 2012).

[10] J.E. Cremona: Elliptic curves database, available online at http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data.

[11] B. Creutz: *Explicit descent in the Picard group of a cyclic cover of the projective line*, to appear in ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, `arXiv:1204.5803`.

[12] R. Dvornicich and U. Zannier: *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129** (2001) 317–338.

[13] R. Dvornicich and U. Zannier: *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris **338** (2004) 47–50.

[14] J.S. Milne: *Arithmetic Duality Theorems*, (second edition) Book Surge, LLC, 2006.

[15] J. Neukirch: Algebraische Zahlentheorie, Springer-Verlag Berlin Heidelberg, 1992.

[16] L. Paladino: *Local-global divisibility by* 4 *in elliptic curves over* $\mathbb{Q}$, Ann. Mat. Pura Appl. **189** (2010) 17–23.

[17] L. Paladino: *Elliptic curves with* $\mathbb{Q}(E[3]) = Q(\zeta_3)$ *and counterexamples to local-global divisibility by* 9, J. Théor. Nombres Bordeaux **22** (2010) 139–160.

[18] L. Paladino, G. Ranieri and E. Viada: *On local-global divisibility by* p^n *in elliptic curves*, Bull. London Math. Soc. **44** (2012) 789–802.

[19] B. Poonen and E.F. Schaefer: *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997) 141–188.
[20] B. Poonen and M. Stoll: *The Cassels-Tate pairing for principally polarized abelian varieties*, Ann. of Math. **150** (1999) 1109–1149.
[21] E.F. Schaefer: *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998) 447–471.
[22] J.-P. Serre: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259–331.
[23] J.-P. Serre: *Points rationnels des courbes modulaires $X_0(N)$ [d'après Barry Mazur]*, Séminaire Bourbaki (1977/78), Exp. 511, Lecture Notes in Math. **710** (1979) 89–100.
[24] J.H. Silverman: *The Arithmetic of Elliptic Curves*, Springer GTM **106** 1986.
[25] J. Tate: *Duality theorems in Galois cohomology over number fields*, Proc. Intern. Cong. Math. Stockholm (1967) 288–295.