THE PERIOD-INDEX PROBLEM IN WC-GROUPS I: ELLIPTIC CURVES

PETE L. CLARK

Abstract. Let E/K be an elliptic curve defined over a number field, and let p be a prime number such that $E(K)$ has full p-torsion. We show that the order of the p-part of the Shafarevich-Tate group of E/L is unbounded as L varies over degree p extensions of K. The proof uses O'Neil's period-index obstruction. We deduce the result from the fact that, under the same hypotheses, there exist infinitely many elements of the Weil-Châtelet group of E/K of period p and index p^2.

1. Introduction

The aim of this paper is to prove the following results (notation is explained at the end of this section):

Theorem 1. *Let p be a prime number, E/K an elliptic curve over a number field with full p-torsion defined over K, and r a positive integer. Then there are infinitely many degree p field extensions L/K such that*

$$\dim_{\mathbb{F}_p} Ш(E/L)[p] \geq r.$$

Recall that for any elliptic curve over a field K of characteristic different from p, all p-torsion points become rational over an extension field of degree dividing $\#GL_2(\mathbb{F}_p) = (p^2-1)(p^2-p)$. Moreover, if $E/\overline{K}$ admits complex multiplication, all p-torsion points become rational over an extension of degree dividing $2(p^2-1)$ or $2(p-1)^2$. This immediately gives the following corollary.

Corollary 2. *If E/K is an elliptic curve over a number field, p a prime and r a positive integer, there exist infinitely many field extensions L/K of degree at most p^5 such that $\dim_{\mathbb{F}_p} Ш(E/L)[p] \geq r$. Moreover, for infinitely many E/K – namely those admitting complex multiplication over $\overline{K}$ – the same result holds for infinitely many field extensions of degree at most $2p^3$.*

In Section 2 we deduce Theorem 1 as a consequence of the following result, which is of independent interest.

Theorem 3. *Let p be a prime, and E/K an elliptic curve over a number field with full p-torsion defined over K. Then there exists an infinite subgroup G of $H^1(K,E)[p]$ such that every nonzero element of G has index p^2 (i.e., p^2 divides the degree of any splitting field extension).*

The proof of Theorem 3 makes essential use of the period-index obstruction map of Catherine O'Neil, which is the subject of Section 3. There is some play in relating two possible definitions, after which we discuss two results concerning this map. The first, Theorem 5, gives a necessary and sufficient condition for the period to equal the index. The second, Theorem 6, is a computation of the period-index obstruction in the case of full level structure, a result which appears in [12] but requires correction.

The proof of Theorem 3 is given in Section 4.

Finally, in Section 5 we discuss some issues raised by the proofs and the possibility of certain generalizations.

Acknowledgements: It is a pleasure to acknowledge helpful conversations with Catherine O'Neil and William Stein, in the course of which many of the ideas of this paper emerged. A motivation for the particular form of the results presented here was the recent preprint [7], which proves – by completely different methods – a result similar to our Corollary 2 but involving simultaneous variation of E and $L/\mathbb{Q}$ among fields of degree $O(p^4)$. Many thanks to the referee for an array of useful suggestions and one invaluable remark. We also thank J.-L. Colliot-Thélène for suggesting various improvements in the exposition.

Notation and terminology: For a field K, we denote by $\overline{K}$ a fixed separable closure of K and by $\mathfrak{g}_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K. If n is a positive integer and G is an abelian group (resp. G/K is a commutative K-group scheme) then $G[n]$ denotes the subgroup (resp. K-subgroup scheme) defined as the kernel of $[n]$, the multiplication by n map. We shall always choose G/K and n such that $G[n]$ is an étale group scheme, which we identify with the $\mathfrak{g}_K$-module $G[n](\overline{K})$. For any $\mathfrak{g}_K$-module M and non-negative integer i, $H^i(K, M) := H^i(\mathfrak{g}_K, M)$, the ith Galois cohomology group. We denote by $\mathrm{Br}(K) = H^2(K, \mathbb{G}_m)$ the Brauer group of K.

Unless explicit mention is made to the contrary, varieties V/K are assumed to be smooth, projective and geometrically irreducible. We denote by $K(V)$ the field of rational functions on V/K. For a scheme X, $\mathrm{Pic}(X) = H^1(X, \mathbb{G}_m)$ is the usual Picard group, while for a variety V/K, $\mathbf{Pic}(V)$ is the sheafification of the fppf presheaf $S/K \mapsto \mathrm{Pic}(V/S)$ (see [1, §8.1] for a nice discussion). Especially, if L/K is any separable algebraic field extension, $\mathbf{Pic}(V)(L) = \mathrm{Pic}(V/\overline{K})^{\mathfrak{g}_L}$.

If M is any $\mathfrak{g}_K$-module and $\eta \in H^i(K, M)$ for $i > 0$, then the *period* of η is just its order as an element of $H^i(K, M)$ (a torsion group). If L/K is a finite separable field extension such that $\eta|_L = 0$, we say that L/K is a *splitting field* for η. The (separable) *index* of η is the greatest common divisor of all degrees of separable splitting fields L/K for η. In general, the period divides the index and the two quantities have the same prime divisors ([8, Prop. 5] in the case of Weil-Châtelet groups, [6, Prop. 9] for the general case, which is not any harder). If η is an element of the Weil-Châtelet group $H^1(K, E)$ of an elliptic curve E/K, then the index is attained, i.e., the greatest common divisor of all degrees of separable splitting fields is itself the degree of a separable splitting field [8, p. 670]. Moreover, modifying the definition of the index by allowing not necessarily separable splitting fields would not result in a lower value for any principal homogeneous space of an elliptic curve [9, Theorem 4].

2. Theorem 3 implies Theorem 1

Let us first recall important results of Cassels and Lichtenbaum, both of the form "period equals index." Let K be a field, E/K an elliptic curve, and $\eta \in H^1(K,E)$ a class of exact order n. Then η is split by a degree n field extension if i) K is a number field and $\eta \in Ш(E/K)$ is a locally trivial class [2, (IV): Theorem 1.2], or ii) K is a finite extension of $\mathbb{Q}_p$ [9, Theorem 3]. One immediately verifies the analogue of Lichtenbaum's theorem for principal homogeneous spaces of elliptic curves over complete Archimedean fields: since the period and the index of an element of the Weil-Châtelet group have the same prime divisors, and since any Galois cohomology class $\eta \in H^i(\mathbb{R},M)$ with $i > 0$ is killed by restriction to $\mathbb{C}$ hence has index at most 2, the version over $\mathbb{R}$ is almost trivial. Truly trivial, but still perhaps worth mentioning, is the fact that period equals index (equals one!) for any principal homogeneous space of an elliptic curve $E/\mathbb{C}$. In fact Lichtenbaum's theorem continues to hold for locally compact fields of positive characteristic [10].

Now let $S \subset H^1(K,E)[p]$ be an infinite subgroup such that every nonzero element of S has index p^2. For each nonzero $\eta_i \in S$, there is a finite set Σ_i of places v of K such that η_i remains nonzero in the completion K_v; note that Σ_i is nonempty by Cassels' theorem. Moreover, by Lichtenbaum's theorem, every class in $H^1(K_v,E)[p]$ can be split by a degree p extension L_w/K_v. For any given η_i, we can find a degree p global extension L_i/K such that $\eta_i|_{L_i}$ is zero everywhere locally, i.e., represents an element of $Ш(E/L_i)[p]$. Indeed, to deal with the finite places we combine the standard (weak) approximation theorem for valuations with the fact that any polynomial $P \in K[x]$ whose coefficients are sufficiently v-adically close to an irreducible polynomial $P_0 \in K_v[X]$ with corresponding extension L_w will, over K_v, also be irreducible with corresponding extension L_w (Krasner's Lemma). Moreover, weak approximation implies that we may require that L_i be totally imaginary at every real Archimedean place $v \in \Sigma_i$ (such places can exist only if $p = 2$). Because the index of η_i is p^2 and we have made a field extension L_i/K of degree only p, the element $\eta_i \in Ш(E/L_i)[p]$ must be nonzero.[1]

We now refine the above argument to produce r $\mathbb{F}_p$-linearly independent classes. For this, observe first that $H^1(K_v,E)[p]$ is a finite group: it is a homomorphic image of $H^1(K_v,E[p])$, and the Galois cohomology groups of a finite module over a p-adic field are finite: [4, Prop. II.5.14]. (It is immediate that $H^1(K_v,E[p])$ is finite if K_v is Archimedean.) Starting with an element η_1 of S, the subgroup $H_1 \subseteq S$ consisting of classes which are locally trivial at all places where η_1 is locally nontrivial has finite index and is therefore infinite; choose a nontrivial η_2 in this group. Continuing in this way, we can construct a cardinality r set $\{\eta_1,\ldots,\eta_r\}$ of $\mathbb{F}_p$-linearly independent elements of S such that the sets Σ_i of places where η_i is locally nontrivial are pairwise disjoint. Accordingly, we can again find a single global extension L/K of degree p such that all r classes give elements of $Ш(E/L)[p]$. Let $\eta = a_1\eta_1 + \ldots + a_r\eta_r$ be any $\mathbb{F}_p$-linear combination of the η_i's. As above, if $\eta|_L = 0$, then η is a class in S of index p, so $\eta = 0$: i.e., $a_1 = \ldots = a_r = 0$. Thus $\dim_{\mathbb{F}_p} Ш(E/L)[p] \geq r$.

[1] This argument is due to William Stein.

3. On the period-index obstruction for elliptic curves

In this section K can be an arbitrary field, and n is a positive integer indivisible by the characteristic of K.

3.1. Two definitions of the period-index obstruction map.

We begin in a more general setting: if X/K is any (as always smooth, projective, geometrically irreducible) variety, there is an exact sequence

$$0 \to \mathrm{Pic}(X) \to \mathbf{Pic}(X)(K) \xrightarrow{\delta} \mathrm{Br}(K) \to \mathrm{Br}(K(X)). \tag{1}$$

In some sense "the right approach" to (1) is via the Leray spectral sequence in étale cohomology (of the sheaf $\mathbb{G}_{mX}$ and the morphism of sites induced by $X \to \mathrm{Spec}\, K$); the associated five-term exact sequence is a slight refinement of (1), with the last term $\mathrm{Br}(K(X))$ replaced by the smaller group $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m)$ [1, pp. 203-204]. However, the point of this section is to verify a compatibility between δ and another cohomological obstruction map, and for this we would like to have a more concrete description of δ. We begin with a geometric description of the restriction of δ to the cone of positive divisor classes in $\mathbf{Pic}(X)(K)$ and then recall why this geometric description is compatible with a rather down-to-earth cohomological description given by Cassels.

First we make precise the statement, "The positive divisors belonging to a divisor class rational over K form a Severi-Brauer variety." [5, p. 160]. Recall that an N-dimensional Severi-Brauer variety V/K is a variety such that $V/\overline{K} \cong \mathbb{P}^N/\overline{K}$. Suppose that $[D] \in \mathbf{Pic}(X)(K)$ is a positive rational divisor class. Let $N+1 = h^0(D)$, the dimension of the $\overline{K}$-space of functions f such that $\mathrm{div}(f) \geq -D$, so $V/\overline{K} := \mathbb{P}\{0 \neq f \mid \mathrm{div}(f) \geq -D\}$ is isomorphic to $\mathbb{P}^N$. We can use the K-rationality of the divisor class of D to give descent data on V: for $\sigma \in \mathfrak{g}_K$, there exists f_σ such that $\mathrm{div}(f_\sigma) = D - D^\sigma$, so that $f \mapsto f \cdot f_\sigma$ gives an isomorphism $\varphi_\sigma : V \to \sigma(V)$. Evidently this system of isomorphisms satisfies Weil's cocycle condition, so can be used to give V the structure of a Severi-Brauer variety $V[D]/K$. We have $V[D](K) \neq \emptyset$ if and only if $V[D] \cong \mathbb{P}^N$ if and only if $[D]$ can be represented by a K-rational divisor.

Since f_σ is uniquely determined by its divisor $D - D^\sigma$ up to multiplication by an element of $\mathbb{G}_m(\overline{K})$, the two-cocycle

$$(\partial(f_\sigma))(\sigma, \tau) := f_\sigma \sigma(f_\tau) f_{\sigma\tau}^{-1}$$

is an element of $H^2(K, \mathbb{G}_m)$. Thus the map

$$[D] \mapsto (f_\sigma) \mapsto \partial(f_\sigma) \tag{2}$$

defines a map from the positive cone $\mathbf{Pic}^+(X)(K)$ of $\mathbf{Pic}(X)(K)$ to $\mathrm{Br}(K)$ which is trivial on the image of $\mathrm{Pic}^+(X)$. But observe that the assignment (2) makes no use of the positivity of $[D]$; indeed it defines a homomorphism $\delta : \mathbf{Pic}(X)(K) \to \mathrm{Br}(K)$. In [2, p. 247] it is shown that this map δ fits into the exact sequence (1).

Remark: If $V(K) \neq \emptyset$, then $\delta \equiv 0$. This follows from the refined version of (1) alluded to above; see [1, p. 204, Prop. 4].

Now let E/K be an elliptic curve, n a positive integer indivisible by the chraracteristic of K, and $L = L(n[O])$. The functor on K-schemes which associates to

S/K the collection of all isomorphisms $L/S \xrightarrow{\sim} \tau_s^*(L/S)$ between the line bundle L/S and one of its translates is represented by an algebraic K-group $\mathcal{G}_L$, the **theta group**. The theory of theta groups is due to D. Mumford [11, §1]. We shall briefly recall some parts of this theory which are relevant for our purposes; this material is discussed in more detail in [12, §2].

There is a natural embedding of $\mathbb{G}_m \hookrightarrow \mathcal{G}_L$ as the subfunctor of automorphisms of L. The quotient $\mathcal{G}_L/\mathbb{G}_m$ is canonically isomorphic to the kernel of the natural map $\varphi_L : A \rightarrow A^\vee$, so in this case to $E[n]$. Moreover, $\mathcal{G}_L$ has a natural (faithful and irreducible) representation on the K-vector space of global sections $\Gamma(E, L)$: if $g \in \mathcal{G}_L(\overline{K})$ carries $L \xrightarrow{\sim} \tau_x^* L$ and $s \in \Gamma(E, L)$, then $g \cdot (s) := \tau_{-x}^*(g(s))$ [11, p. 295]. Thus, choosing a basis $(f_1, \ldots, f_n)$ of $\Gamma(E, L)$ we get a homomorphism $\mathcal{G}_L \rightarrow GL_n$, which carries $\mathbb{G}_m$ (the center of $\mathcal{G}_L$) identically onto the subgroup $\mathbb{G}_m \subset GL_n$ of scalar matrices.

In summmary, we have the following commutative diagram, in which both the top and bottom rows are central extensions of group schemes:

(3)
$$\begin{tikzcd}
1 \arrow[r] \arrow[d] & \mathbb{G}_m \arrow[r] \arrow[d] & \mathcal{G}_L \arrow[r] \arrow[d] & E[n] \arrow[r] \arrow[d, "\gamma"] & 1 \arrow[d] \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & GL_n \arrow[r] & PGL_n \arrow[r] & 1
\end{tikzcd}$$

Especially important for us is the morphism $\gamma : E[n] \rightarrow PGL_n$. Let $E \rightarrow \mathbb{P}^{n-1}$ be the morphism into projective space associated to the divisor $n[O]$ (it is an embedding if $n \geq 3$ and is two-to-one onto its image if $n = 2$). We may view $E[n]$ as the group of translations of E which extend to automorphisms of $\mathbb{P}^{n-1}$ such that the following diagram commutes:

(4)
$$\begin{tikzcd}
E \arrow[r, "\tau_P"] \arrow[d, "\varphi"'] & E \arrow[d, "\varphi"] \\
\mathbb{P}^{n-1} \arrow[r, "\gamma(\tau_P)"] & \mathbb{P}^{n-1}
\end{tikzcd}$$

We summarize this situation by saying (perhaps abusively) that $E[n]$ is the automorphism group of the morphism $\varphi : E \rightarrow \mathbb{P}^{n-1}$.

Now consider the **Kummer sequence**

$$0 \rightarrow E(K)/nE(K) \rightarrow H^1(K, E[n]) \rightarrow H^1(K, E)[n] \rightarrow 0.$$

The group $H^1(K, E)[n]$ parameterizes genus one curves C/K equipped with the structure of a principal homogeneous space for $E = J(C) = \mathbf{Pic}^0(C)$ and having period dividing n. This geometric interpretation "lifts" to $H^1(K, E[n])$ as follows.

Proposition 4. *The group $H^1(K, E[n])$ classifies isomorphism classes of pairs $(C, [D])$, where C is a principal homogeneous space for E and $[D] \in \mathbf{Pic}^n(C)(K)$ is a K-rational divisor* class *of degree n. Two such pairs are isomorphic if and only if there exists an isomorphism of principal homogeneous spaces $f : C_1 \rightarrow C_2$ such that $f^*([D_2]) = [D_1]$.*

I have been unable to find this proposition in the literature in the precise form in which we have stated it, but I am told that it has been well-known for a long time. Indeed, Proposition 4 can readily be deduced either from work of Cassels or of O'Neil.

Proof: In either case, the idea is to interpret $E[n]$ as an automorphism group of a suitable structure $\mathcal{S}$, so that by Galois descent $H^1(K, E[n])$ parameterizes the twisted forms of $\mathcal{S}$. But there is some latitude in the choice of $\mathcal{S}$. The classical choice [3, Lemma 13.1] is to view $E[n]$ as the deck transformation group of $[n] : E \rightarrow E$, so that $H^1(K, E[n])$ parameterizes finite étale maps $f : C \rightarrow E$ which are geometrically Galois (and for which C is, as always, geometrically connected), with group $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. To any such map $f : C \rightarrow E$ we associate the pair $(C, [nQ])$, where Q is any element of $f^{-1}(O)$. O'Neil's choice [12, Prop 2.2] is, as above, to view $E[n]$ as the automorphism group of the morphism $\varphi_L : E \rightarrow \mathbb{P}^{n-1}$, so that $H^1(K, E[n])$ parameterizes **diagrams** $C \rightarrow V$, where C is a principal homogeneous space for E and V is a Severi-Brauer variety. Note that the additional data of the diagram $C \rightarrow V$ is, by Galois descent, equivalent to giving a rational divisor class $[D]$ on C, for which $V = V[D]$. In particular, two diagrams $C \rightarrow V$ and $C' \rightarrow V'$ are isomorphic if they fit into a commutative diagram of the form

$$\begin{tikzcd}
C \arrow[r, "\tau_P"] \arrow[d] & C' \arrow[d] \\
V \arrow[r] & V'
\end{tikzcd}$$

the twisted analogue of (4). This completes the proof.

Now recall that PGL_n is itself the automorphism group of $\mathbb{P}^{n-1}$, so that by Galois descent $H^1(K, PGL_n)$ parameterizes $n-1$-dimensional Severi-Brauer varieties. One of the merits of O'Neil's setup is that the geometric interpretation of the map $H^1(K, E[n]) \rightarrow H^1(K, PGL_n)$ is very simple: it is just the forgetful functor $(C \mapsto V) \mapsto V$, whereas the *other* forgetful functor $(C \mapsto V) \mapsto C$ has the cohomological interpretation $H^1(K, E[n]) \rightarrow H^1(K, E)[n]$.

This brings us to our "geometric" definition of the period-index obstruction map:

$$\mathcal{D} : H^1(K, E[n]) \rightarrow \mathrm{Br}(K)$$

by

$$(C, [D]) \mapsto [D] \mapsto (f_\sigma) \mapsto \partial(f_\sigma),$$

i.e., we extract the divisor class $[D]$ and associate the Severi-Brauer variety and then its coboundary in the Brauer group as at the beginning of the section.

The following result justifies the name.

Theorem 5. *A class $\eta \in H^1(K, E)[n]$ of exact period n has index n if and only if some lift of η to $\xi \in H^1(K, E[n])$ has $\mathcal{D}(\xi) = 0$.*

Proof: η has index n if and only if there exists a K-rational divisor of degree n on the corresponding principal homogeneous space C, i.e., if and only if some K-rational divisor class of degree n on C has vanishing obstruction. Thus the result is clear.

Now we must admit that this is not quite the definition of the period-index obstruction given in [12]. Rather, O'Neil considers the cohomological connecting map

$$\Delta : H^1(K, E[n]) \rightarrow H^2(K, \mathbb{G}_m)$$

associated to the central extension of $\mathfrak{g}_K$-modules

$$1 \to \mathbb{G}_m(\overline{K}) \to \mathcal{G}_L(\overline{K}) \to E[n](\overline{K}) \to 1.$$

Whereas $\mathcal{D}$ satisfies Theorem 5, it is Δ that can be explicitly computed, as we shall see shortly. Fortunately there no need to choose between them.

Claim: $\Delta = \mathcal{D}$.

Proof: The commutativity of (3) means that Δ factors as

$$\Delta : H^1(K, E[n]) \to H^1(K, PGL_n) \to H^2(K, \mathbb{G}_m),$$

where the latter map is "the Δ" associated to the central extension of $\mathfrak{g}_K$-modules given by the bottom row of (X). Since we know that $H^1(K, E[n]) \to H^1(K, PGL_n)$ is just $(C \mapsto V) \mapsto V$, the only thing that remains to be shown is that $\partial(V[D]) = \Delta(V[D])$. To see this: if $m(\sigma) \in GL_n(\overline{K})$ is the matrix defined by

$$\sigma(f_1, \ldots, f_n) = m(\sigma)(f_1, \ldots, f_n),$$

and $\overline{m}(\sigma)$ is its image in $PGL_n(\overline{K})$, then the one-cocycle associated to $V[D]$ is $\eta : \sigma \mapsto \overline{m}(\sigma)$. But then $\Delta(\eta)$ can be computed by lifting η to $GL_n(\overline{K})$, and if we choose the lift $\sigma \mapsto m(\sigma)$, then we have an equality of cocycles

$$\Delta(\eta)(\sigma, \tau) = f_\sigma \sigma(f_\tau) f_{\sigma\tau}^{-1} = \partial(f_\sigma).$$

This completes the proof of the claim.

We end this section by noting, as in [12], that $\Delta(\iota(E(K)/nE(K))) = 0$; in other words, Δ vanishes on the image of the Kummer map. It may be tempting to conclude that Δ factors through $H^1(K, E)[n]$, but this is absolutely *not* the case. Since Δ is defined by nonabelian Galois cohomology, it need not be a homomorphism of groups, and in fact [12, Prop. 4.1] shows that it is always a quadratic map. This leads us directly into the issues of the next section, in which we will compute Δ in a special case.

3.2. **Heisenberg groups and the explicit period-index obstruction.** The goal of this section is to compute Δ in the case when E/K has full n-torsion defined over K. That is, we assume that the finite étale K-group scheme $E[n]$ is *constant*, and choose a Galois module isomorphism $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. The Galois-equivariance of Weil's e_n-pairing implies that $\mathbb{Z}/n\mathbb{Z} = \bigwedge^2 E[n] = \mu_n$ as Galois modules, so the above choice of basis induces an isomorphism

$$H^1(K, E[n]) \cong H^1(K, \mu_n)^2 = (K^*/K^{*n})^2.$$

So in this case the period-index obstruction can be viewed as a map

$$\Delta : (K^*/K^{*n})^2 \to \mathrm{Br}(K).$$

Now we must point out that [12, Prop. 3.4] gives a computation of Δ which is not quite correct: it is claimed that $\Delta(a, b) = \langle a, b\rangle_n$, the **norm-residue symbol**. But the following counterexample was supplied by the referee:

Suppose $n = 2$, so E is given as $y^2 = (x - e_1)(x - e_2)(x - e_3)$. Then the map

$\iota : E(K)/2E(K) \to (K^*/K^{*2})^2$ is given explicitly for any point $(x, y) \in E(K)$ with $x \neq e_1, e_2$ as

$$\iota(x, y) = (x - e_1, x - e_2) \pmod{K^{*2}}$$

[14, Prop. X.1.4]. But Δ vanishes on $\iota(E(K)/2E(K))$, so in particular $\Delta(e_3 - e_1, e_3 - e_2) = 0$. But as $e_1,\ e_2,\ e_3$ vary over all triples of distinct elements of K, $(e_3 - e_1, e_3 - e_2)$ runs through all elements of $K^\times/K^{\times 2}$, and all Hilbert symbols $\langle a,\ b\rangle_2$ vanish only if $\mathrm{Br}(K)[2]$ vanishes.

On the other hand, the following result shows that the obstruction map Δ is close to being the norm residue symbol $\langle\ ,\ \rangle_n$.

Theorem 6. *Let E/K be an elliptic curve over a field K and n a positive integer not divisible by the characteristic of K and such that $E[n]$ is a trivial $\mathfrak{g}_K$-module. Then there exist $C_1,\ C_2 \in K^*/K^{*n}$ such that for all $a,\ b \in K^*/K^{*n}$,*

$$\Delta(a, b) = \langle C_1 a, C_2 b\rangle_n - \langle C_1, C_2\rangle_n.$$

Before we begin the proof we will need to recall some facts about Heisenberg groups. There is an algebraic K-group scheme $\mathcal{H}_n$, which is, like $\mathcal{G}$, a central extension of $E[n]$ by $\mathbb{G}_m$. To define $\mathcal{H}_n$, one chooses a decomposition $E[n] = H_1 \oplus H_2$ into a direct sum of two cyclic order n subgroup schemes. (With a view towards the higher-dimensional case, one should think of this as a **Lagrangian decomposition**, i.e., that each H_i is maximal isotropic for the Weil e_n-pairing; of course this is automatic for elliptic curves.) Then $\mathcal{H}_n$ is defined by the following 2-cocycle $f_{H_1,H_2} \in Z^2(E[n], \mathbb{G}_m)$:

$$(P_1 + P_2, Q_1 + Q_2) \mapsto e_n(P_1, Q_2).$$

In the course of the proof of Theorem 6 we will see that the connecting map $\Delta_{\mathcal{H}_n} : H^1(K, E[n]) \to \mathrm{Br}(K)$ associated to the Heisenberg group is precisely the norm residue symbol $\langle a, b\rangle_n$. This result is a very special case of thesis work of R. Sharifi [13, Prop. 2.3]. Moreover, Mumford [11, Cor. of Th. 1] shows that when $K = \overline{K}$, the theta group $\mathcal{G}$ is isomorphic to the Heisenberg group $\mathcal{H}_n$. (To be entirely precise, Mumford works over an *algebraically* closed field, but his proof [11, p. 293] shows that the identification of $\mathcal{G}$ with $\mathcal{H}_n$ is attained over an abelian extension of K of exponent dividing n, hence certainly over the separable closure.) Thus in general $\mathcal{G}$ is a Galois twisted form of $\mathcal{H}_n$. Combining these two results with the above counterexample, it must be the case that $\mathcal{G}$ can be a nontrivial twisted form of $\mathcal{H}_n$.

Nevertheless, we can completely understand the possible twists: they are parameterized by $H^1(K, \mathrm{Aut}_\star(\mathcal{H}_n))$, where the $\star$ indicates that we want not the full automorphism group of $\mathcal{H}_n$ but only the automorphisms which act trivially on the subgroup $\mathbb{G}_m$ and on the quotient $E[n]$. It will turn out that $\mathrm{Aut}_\star(\mathcal{H}_n) \cong (H_1 \oplus H_2)^\vee$, so that the twisted forms of the Heisenberg group will be parameterized by pairs of order n characters of $\mathfrak{g}_K$.

We now begin the proof of Theorem 6. Let $\psi \in \mathrm{Aut}_\star(\mathcal{H}_n)$, and let (P_1, P_2, ϵ) denote an arbitrary element of the Heisenberg group. Since ψ is the identity modulo the center, we have $\psi(P_i) = P_i$ for $i = 1,\ 2$; together with the fact that $\psi(0, 0, \epsilon) = (0, 0, \epsilon)$, this implies that $\psi : (P_1, P_2, \epsilon) \mapsto (P_1, P_2, \chi(\psi)(P_1, P_2)\epsilon)$. That is, an automorphism of $\mathcal{H}_n$ as an extension determines a map $\chi : H_1 \oplus H_2 \to \mathbb{G}_m$, i.e., a *character* of $H_1 \oplus H_2$. Conversely, any such character defines an automorphism, and we have canonically $\mathrm{Aut}_\star(\mathcal{H}_n) = (H_1 \oplus H_2)^\vee$ (Pontrjagin = Cartier dual). It follows that the collection of twisted forms of the Heisenberg group is $H^1(K, (H_1 \oplus H_2)^\vee) \cong H^1(K, H_1 \oplus H_2)$, since the Weil pairing gives an autoduality $E[n]^\vee \cong E[n]$.

Changing notation slightly, let

$$\chi \in H^1(K, \mathrm{Aut}_\star(\mathcal{H}_n)) = H^1(K, (H_1 \oplus H_2)^\vee) \cong (K^*/K^{*n})^2$$

be a one-cocycle. Using χ we build a twisted form $\mathcal{H}_\chi$ of $\mathcal{H}_n$, i.e., the group scheme whose $\overline{K}$-points are the same as the $\overline{K}$-points of $\mathcal{H}_n$, but with twisted $\mathfrak{g}_K$-action, as follows:

$$\sigma \cdot (P_1, P_2, \epsilon) = (P_1, P_2, \chi(\sigma)(P_1, P_2)\sigma(\epsilon)).$$

We may now compute the cohomological coboundary map Δ directly from its definition. For this, we view $\mathcal{H}_\chi/\overline{K}$ as $\mathbb{G}_m \times E[n]$ "doubly twisted," i.e., twisted as a $\mathfrak{g}_K$-set as just discussed, and twisted as a group via the cocycle f introduced above:

$$(\alpha, P) \star (\beta, Q) = (\alpha\beta f(P, Q), P + Q).$$

We note that the inverse of (α, P) is $(\alpha^{-1} f(P, -P)^{-1}, -P)$. Let $\eta \in Z^1(K, E[n])$; we want to compute $\Delta(\eta)(\sigma, \tau)$. The basic recipe for this allows us to choose arbitrary lifts $N_\sigma,\ N_\tau,\ N_{\sigma\tau}$ of $\eta_\sigma,\ \eta(\tau),\ \eta(\sigma\tau)$ to $\mathcal{H}_\chi$ and put $\Delta(\eta)(\sigma, \tau) = N_\sigma \sigma(N_\tau) N_{\sigma\tau}^{-1}$. We choose to lift by the set-theoretic identity section: $\eta(\sigma) \mapsto (1, \eta(\sigma))$, and so on. Keeping in mind that $\sigma(\eta(\tau)) = \eta(\tau)$ and $\eta(\sigma\tau) = \eta(\sigma)\eta(\tau)$, we get:

$$\Delta(\eta)(\sigma, \tau) = (1, \eta(\sigma)) \star \sigma(1, \eta(\tau)) \star (1, \eta(\sigma\tau))^{-1} =$$
$$(1, \eta(\sigma)) \star (\chi(\sigma)(\eta(\tau)), \eta(\tau)) \star (f(\eta(\sigma\tau), -\eta(\sigma\tau))^{-1}, -\eta(\sigma\tau) =$$
$$(\chi(\sigma)(\eta(\tau)) f(\eta(\sigma), \eta(\tau)), \eta(\sigma)\eta(\tau)) \star (f(\eta(\sigma\tau), -\eta(\sigma\tau))^{-1}, -\eta(\sigma\tau)) =$$
$$(\chi(\sigma)(\eta(\tau)) f(\eta(\sigma), \eta(\tau)), 0).$$

That is, the coboundary map $\Delta : H^1(K, E[n]) \to \mathrm{Br}(K)[n]$ is a product of two terms:

$$\Delta(\eta)(\sigma, \tau) = \Delta_1 \cdot \Delta_2 = \chi(\sigma)(\eta(\tau)) \cdot f(\eta(\sigma), \eta(\tau)).$$

Indeed Δ_2 and Δ_1 are respectively the *quadratic form* and the *linear form* comprising the quadratic map Δ.

Proposition 7. *We have – with suitable identifications to be explained below – that*

$$\Delta_2(a, b) = \Delta_{\mathcal{H}_n}(a, b) = \langle a, b \rangle_n.$$

Proof: Note that the first equality in the statement of the Proposition is clear, since $\Delta = \Delta_2$ if χ is trivial. Our choice of a basis $P_1,\ P_2$ for $E[n](K)$ determines a primitive nth root of unity $\zeta_n = e_n(P_1, P_2)$, and we use ζ_n to identify μ_n with $\mathbb{Z}/n\mathbb{Z}$. This same choice of basis gave us a Kummer isomorphism $H^1(K, E[n]) \cong (K^\times/K^{\times n})^2$, so we may identify $(a, b) \in (K^\times/K^{\times n})^2$ with a pair of characters $\varphi_a,\ \varphi_b : \mathfrak{g}_K \to \mathbb{Z}/n\mathbb{Z}$. Then there is a cup-product map

$$\cup : H^1(K, \mathbb{Z}/n\mathbb{Z}) \times H^1(K, \mathbb{Z}/n\mathbb{Z}) \to H^2(K, \mathbb{Z}/n\mathbb{Z}) = H^2(K, \mu_n) = Br(K)[n],$$

and it is well-known [5, Prop. XIV.5] that $\langle a, b\rangle_n = \varphi_a \cup \varphi_b$. With this notation $\eta(\sigma) = (\varphi_a(\sigma), \varphi_b(\sigma))$, so

$$\Delta_2(\eta)(\sigma, \tau) = e_n(\varphi_a(\sigma), \varphi_b(\tau)) = \varphi_a(\sigma) \cdot \varphi_b(\tau),$$

where the last product is just multiplication in $\mathbb{Z}/n\mathbb{Z}$. It remains to remark that $(\varphi_a \cup \varphi_b)(\sigma, \tau) = \varphi_a(\sigma) \cdot \varphi_b(\tau)$ – see e.g. the first displayed equation of [5, p. 208]. This completes the proof of Proposition 7.

To evaluate Δ_1, choose a basis (P_1, P_2) of $E[n]$ and use the induced decomposition of $E[n] = H_1 \oplus H_2$ and the corresponding decomposition of the dual space $E[n]^\vee$ (i.e., we decompose any character ϕ into $\psi_1 \oplus \psi_2$, where $\chi_i(H_j) = 0$ for $i \neq j$). This induces decompositions $\eta = \eta_1 \oplus \eta_2$ and $\chi = \chi_1 \oplus \chi_2$, so that

$$\chi(\sigma)(\eta(\tau)) = \chi_1(\sigma)(\eta_1(\tau)) \cdot \chi_2(\sigma)(\eta_2(\tau)).$$

Now under our identification $H^1(K, E[n]) = (K^*/K^{*n})^2$, η_1 corresponds to $a \pmod{K^{*n}}$ and η_2 corresponds to $b \pmod{K^{*n}}$, so Δ_1 is just the sum of the cyclic algebras (a, χ_1) and (b, χ_2). Using Kummer theory to identify the characters with elements (say) C_2, C_1' of K^*/K^{*n}, we get

$$\Delta_1(a, b) = \langle a, C_2\rangle + \langle b, C_1'\rangle = \langle a, C_2\rangle + \langle C_1, b\rangle,$$

where $C_1 = C_1'^{-1}$. Thus we have

$$\Delta(a, b) = \langle a, b\rangle + \langle a, C_2\rangle + \langle C_1, b\rangle = \langle C_1 a, C_2 b\rangle - \langle C_1, C_2\rangle,$$

completing the proof of the theorem.

4. The Proof of Theorem 3

In this section the following hypotheses are in force: $n = p$ is prime, K is a number field, and E/K is an elliptic curve with $E[p](\overline{K}) = E[p](K)$. We note that this implies, by the Galois-equivariance of the Weil pairing, that K contains the pth roots of unity. Since for any class $\eta \in H^1(K, E)[p]$ the possible lifts of η to $H^1(K, E[p])$ are parameterized by the *finite* abelian group $E(K)/pE(K)$ (weak Mordell-Weil theorem), by Theorem 5 the proof of Theorem 3 is reduced to the following result.

Proposition 8. *Let K be a number field containing the pth roots of unity and $H \subseteq (K^*/K^{*p})^2$ a finite subgroup. Then there exists an infinite subgroup $G \subseteq (K^*/K^{*p})^2$ with the property that for every nonzero element g of G and every element $h \in H$, $\Delta(hg) \neq 0$.*

By Theorem 6, $\Delta = \langle\ ,\ \rangle_p$ up to a linear term, and essentially what must be shown is the same statement with $\langle\ ,\ \rangle_p$ in place of Δ; this says, morally, that Brauer groups of number fields are "large" in a certain sense. We prove this directly (if inelegantly) using exactly what the reader expects: local and global class field theory, especially the nondegeneracy of the local norm residue symbol.

Along these lines we will need the following routine result, whose proof we include for completeness.

Lemma 9. *Let n be a positive integer, K be a number field containing the nth roots of unity, and $L_1, \ldots, L_k$ be k cyclic degree n extensions of K. Then the image in K^*/K^{*n} of the subgroup of K^* consisting of simultaneous norms from each L_i is infinite.*

Proof: By Hasse's norm theorem, if L/K is a cyclic extension of number fields, then $a \in K^*$ is a norm from L if and only if it is everywhere a local norm. Let S be the set of places of K consisting of the real Archimedean places (if any) together with all finite places which ramify in any L_i/K (if any). Let $G_1 \subseteq K^*$ be the subgroup of elements which are nth powers locally at every $v \in S$; notice that G_1 has finite index. Recalling that the norm map on an unramified local extension is surjective onto the unit group, we get that any $a \in G_1$ is a simultaneous local norm except possibly at the unramified places v at which it has nontrivial valuation. Let h be the class number of K. Then the set of primes which split completely in the Hilbert class field as well as in each L_i has density at least $\frac{1}{hn^k}$. For such a v, let π_v be a generator of the corresponding prime ideal, and let G_2 be the (infinite) subgroup of K^* generated by these elements π_v. Since G_1 has finite index, $G := G_1 \cap G_2$ remains infinite and visibly has infinite image in K^*/K^{*n}; by Hasse, every element of G is a simultaneous norm.

Now we begin the proof of Proposition 8. Write out the elements of H as follows:

$$H = \{(h_{1i}, h_{2i})\}| \ 1 \leq i \leq k\}.$$

Moreover, let $B = B_H$ be the finite set of places of K containing the Archimedean places, the places at which any h_{1i} or h_{2i} has nonzero valuation, and the places for which, for any $e \pmod p$, any expression $e\langle C_1, C_2\rangle_v - \langle h_{1i}, h_{2i}\rangle_v$ is nonzero in $\mathrm{Br}(K_v)$.

Clearly it is enough to construct arbitrarily large finite subgroups G such that every nontrivial element (g_1, g_2) of G has the property that for all i,

$$\Delta(h_i g) = \langle C_1 h_{1i} g_1, C_2 h_{2i} g_2\rangle_p \neq \langle C_1, C_2\rangle_p.$$

We make two preliminary simplifying assumptions: first, let C be the cyclic subgroup generated by $\langle C_1, C_2\rangle_p$ in $\mathrm{Br}(K)[p]$. Rather than constructing elements g such that all modifications of g by elements of H have $\Delta(hg) \neq \langle C_1, C_2\rangle_p$, it is convenient for a later inductive argument to require the stronger property that for all $h \in H$, $\Delta(hg)$ is not an element of C. Second, by replacing H by $H + C$, we reduce to the following problem: find arbitrarily large finite subgroups G such that all nontrivial elements (g_1, g_2) have the property that for all $h = (h_{1i}, h_{2i})$ in H,

$$\langle h_{1i} g_1, h_{2i} g_2\rangle_p \text{ is not in } C. \tag{5}$$

In order to accomplish this, we first claim that we can choose $g_2 \in K^*/K^{*p}$ such that:

- For $1 \leq i \leq k$, $\langle h_{1i}, g_2\rangle = 0$; and
- For $1 \leq i \leq k$, $g_2 h_{2i}$ is not in K^{*p}.

Indeed, the elements g_2 satisfying the first condition are precisely the simultaneous norms from the k cyclic field extensions $K(h_{1i}^{1/p})/K$, so in the notation of Lemma 9 there is a positive density set S_1 of principal prime ideals $v = (\pi_v)$ such that $\pi_v \in K^*$ is a simultaneous norm from these k extensions. The second condition is also satisfied as long as $v \in S_1 \setminus B$, so choose any such v and take $g_2 = \pi_v$.

If we now choose any g_1 with the property that for all i and any $e \pmod p$

$$\langle g_1, g_2 h_{2i} \rangle \neq e \langle C_1, C_2 \rangle_p - \langle h_{1i}, h_{2i} \rangle,$$

then the element $g = (g_1, g_2)$ will have the desired property (5). For each i, since $g_2 h_{2i}$ is not a pth power, there exists an infinite set of places $v = v(i)$ such that $g_2 h_{2i}$ is not a pth power in K_v. Hence we may choose places $v_1, \ldots, v_k$, distinct and disjoint from B, such that for all i, $g_2 h_{2i}$ is not a pth power in K_{v_i}. By weak approximation, we can choose an element g_1 of K^*/K^{*p} such that for all i, g completes to a class of $K^*_{v_i}/K^{*p}_{v_i}$ making all the local norm residue symbols $\langle g_1, g_2 h_{2i} \rangle_{v_i}$ nontrivial (this is possible because of the nondegeneracy of the local norm residue symbol). But by definition of B, $e\langle C_1, C_2 \rangle_{v_i} - \langle h_{1i}, h_{2i} \rangle_{v_i} = 0$ for all i, so we have constructed an element $g = (g_1, g_2)$ satisfying (5). Now observe that if $1 \leq j < p$, g_2^j satisfies the same two bulleted properties as g_2; moreover, since H is a subgroup, $h_{2i} = h^j_{2i'}$ for some other index i', and the nontriviality of $\langle g_1, g_2 h_{2i} \rangle_v$ implies the nontriviality of $\langle g_1^j, g_2^j h^j_{2i} \rangle_v$, so that indeed the entire cyclic subgroup A generated by (g_1, g_2) has property (5).

We finish by iterating the construction: running through the above argument with H replaced by $A \oplus C$ gives a two-dimensional $\mathbb{F}_p$-subspace of $K^*/K^{*p} \times K^*/K^{*p}$, and so on.

5. Concluding remarks

I. In the derivation of Theorem 1 from Theorem 3, instead of appealing to Lichtenbaum's theorem on the equality of the period and index for *all* classes in the Weil-Châtelet group of an elliptic curve over a local field, we could instead have used an earlier result [8, Corollary 2, p. 677] giving the same equality for abelian varieties of arbitrary dimension over local fields in the case when p is prime to the residue characteristic and A has good reduction. Indeed the set of places of K lying over p together with those places of bad reduction for E/K form a finite set, and as in the proof we need only restrict to the finite index subgroup of classes trivial at all these places.

II. The proof of the main theorem shows that each nonzero element g of $G \subseteq H^1(K, E)[p]$ gives rise to at least one set of "local conditions" on a degree p extension L/K sufficient to ensure that g restricts to a nonzero element of $\text{Ш}(E/L)$. On the other hand, the proof of Theorem 3 shows that G is not only an infinite subgroup but has (in some sense) "positive measure," bounded away from zero in terms of $\#E(K)/pE(K)$. Thus the argument should lead to an explicit lower bound on the function

$$f(N) = f(E/K, p, N) := \sum_{L/K,\ [L:K]=p,\ ||\Delta_{L/K}|| \leq N} \dim_{\mathbb{F}_p} \text{Ш}(E/L)[p],$$

where $\Delta_{L/K}$ is the discriminant of L/K. What is to be expected about the asymptotics of f?

III. The hypothesis that E has full p-torsion defined over K is used only in the appeal to the "explicit" period-index obstruction of Theorem 5 in the proof of Theorem 3. My hope is that Theorem 3 should be valid for every elliptic curve over a number field – namely, there should always exist an infinite subgroup of principal homogeneous spaces of order p and index p^2. The challenge here is to make sufficiently explicit the period-index obstruction map $\Delta : H^1(K, E[p]) \rightarrow \mathrm{Br}(K)$ in the case of an arbitrary Galois module structure on $E[p]$. Notice that the setup of Theorem 4 can be generalized to the case of elliptic curves E such that $E[n]$ has a Lagrangian decomposition: i.e., a decomposition into one-dimensional subspaces $H_1 \oplus H_2$ as Galois module. This is still quite a stringent condition, but it can be satisfied over $\mathbb{Q}$ for the primes 2, 3 and 5, since for such primes p, elliptic curves $E/\mathbb{Q}$ with Galois module structure $E[n] \cong \mu_p \oplus \mathbb{Z}/p\mathbb{Z}$ are known to exist. In these cases, an analogue of Theorem 4 would show the existence of genus 1 curves $C/\mathbb{Q}$ of period p and index p^2 for $p \leq 5$. While this may not sound very impressive, we must point out that heretofore the *only* examples in the literature of genus one curves over *any* number field with index exceeding their period are those of period 2 and index 4 (over $\mathbb{Q}$) constructed by Cassels [2, (V)] more than 40 years ago. Indeed, Cassels' Jacobian elliptic curves have full 2-torsion over $\mathbb{Q}$, so his results are a special case of our Theorem 3.

IV. Theorems 1 and 3 continue to hold when K is a global field of positive characteristic (i.e., a one-variable function field over a finite field) as long as the prime p is not the characteristic of K: we need only use the aforementioned positive characteristic version of Lichtenbaum's theorem due to Milne [10, Corollary, p. 283]. But in fact the point of Milne's paper is to prove that Tate local duality holds (even) on the p-primary component of $H^1(K, E)$ and accordingly that Lichtenbaum's theorem holds even for Weil-Châtelet classes whose period is divisble by p. Perhaps Theorems 1 and 3 hold even for such classes, but they cannot be proved using the present methods, which require $E[n]$ to be an étale group scheme.

V. There are versions of Theorem 1 and Theorem 3 for principal homogeneous spaces over abelian varieties of any dimension. The proofs require a higher dimensional period-index obstruction map and are pursued in a separate paper [6].

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud. *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete 21, Springer-Verlag, 1990.

[2] J.W.S. Cassels. *Arithmetic on a curve of genus one. (IV) Proof of the Hauptvermutung*, Proc. London Math. Soc. 46 (1962), 259-296. *(V) Two counterexamples*, J. London Math Soc. 36 (1961), 177-184.

[3] J. W. S. Cassels. *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), 193-291.

[4] J.-P. Serre, *Cohomologie Galoisienne*, Fifth edition. Lecture Notes in Mathematics 5, Springer-Verlag, 1994.

[5] J.-P. Serre. *Corps Locaux*, Hermann, Paris, 1962.

[6] P.L. Clark. *The period-index problem in WC-groups II: abelian varieties*, submitted.

[7] R. Kloosterman. *The p-part of Shafarevich-Tate groups of elliptic curves can be arbitarily large*, preprint available at `http://www.arXiv.math.NT/0303143v1`.

[8] S. Lang and J. Tate. *Principal homogeneous spaces over abelian varieties*, Amer. J. Math (80), 1958, 659-684..

[9] S. Lichtenbaum. *The period-index problem for elliptic curves*, Amer. J. Math. (90), 1968, 1209-1223.

[10] J. Milne. *Weil-Châtelet groups over local fields*, Ann. Sci. École Norm. Sup. 3 (1970), 273-284.

[11] D. Mumford. *On the equations defininining abelian varieties. I.* Invent. Math. (1) 1966, 287-354.

[12] C.H. O'Neil. *The period-index obstruction for elliptic curves*, J. Number Theory 95 (2002), 329-339.

[13] R. Sharifi. *Twisted Heisenberg representations and local conductors*, 1999 Chicago Thesis, available at `http://abel.math.harvard.edu/~sharifi`.

[14] J. Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics 106, Springer-Verlag, 1986.

1126 Burnside Hall, Department of Mathematics and Statistics, McGill University, 805 Sherbrooke West, Montreal, QC, Canada H3A 2K6

E-mail address: `clark@math.mcgill.ca`