Algebra & Number Theory

Volume 4

2010

No. 2

Period, index and potential, III

Pete L. Clark and Shahed Sharif

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 4:2(2010)

Period, index and potential, III

Pete L. Clark and Shahed Sharif

We present three results on the period-index problem for genus-one curves over global fields. Our first result implies that for every pair of positive integers (P, I) such that I is divisible by P and divides P^2, there exists a number field K and a genus-one curve $C_{/K}$ with period P and index I. Second, let $E_{/K}$ be any elliptic curve over a global field K, and let $P > 1$ be any integer indivisible by the characteristic of K. We construct infinitely many genus-one curves $C_{/K}$ with period P, index P^2, and Jacobian E. Our third result, on the structure of Shafarevich–Tate groups under field extension, follows as a corollary. Our main tools are Lichtenbaum–Tate duality and the functorial properties of O'Neil's period-index obstruction map under change of period.

1. Introduction

1.1. ***Notation and conventions.*** Throughout the paper K shall denote a global field — that is, a finite field extension of either $\mathbb{Q}$ or $\mathbb{F}_p(T)$ — and E shall denote an elliptic curve defined over K.

Let P be a positive integer which is *not* divisible by the characteristic of K. Define P^* to be P if P is odd and $2P$ if P is even.

Let $\overline{K}$ denote a fixed *separable* closure of K, and let $\mathfrak{g}_K = \mathrm{Aut}(\overline{K}/K)$ be the absolute Galois group of K.

We abbreviate the Galois cohomology group $H^1(\mathfrak{g}_K, E(\overline{K}))$ to $H^1(K, E)$ and call it the *Weil–Châtelet group* of E over K. Recall that this is a torsion abelian group.

Let $\mathbf{Pic}(C)$ be the Albanese/Picard variety of C, and $\mathbf{Pic}^d(C)$ the connected component classifying degree d invertible sheaves on C, so that $\mathbf{Pic}^0(C)$ is the Jacobian. The letter η shall denote an element of $H^1(K, E)$. Such classes η are in canonical bijection with the set of equivalence classes of pairs $(C, \imath)$, where $C_{/K}$ is a genus one curve, $\imath : \mathbf{Pic}^0(C) \to E$ is an isomorphism from the Jacobian of C to E, and the equivalence is isomorphism over K. In other words, $\imath$ endows C with

MSC2000: 11G05.

Keywords: period, index, Tate–Shafarevich group.

Clark is partially supported by the National Science Foundation grant DMS-0701771.

the structure of a principal homogeneous space (or torsor) under E. It follows that $C_{/K}$ itself determines, and is determined by, an orbit of $\mathrm{Aut}(E)$ on $H^1(K, E)$.

The *period* of $\eta \in H^1(K, E)$ is its order in the group. In terms of the corresponding torsor C, the period is the least positive degree of a K-rational divisor class on C. The *index* of η is the gcd over all degrees $[L : K]$ of field extensions L/K such that the restriction of η to $H^1(L, E)$ is trivial. In terms of C, the index is the least positive degree of a K-rational divisor. By Riemann–Roch, it is also the least degree of an extension L/K such that C has an L-rational point. Since the period and index are invariant under isomorphism over K, we will refer to the period and index of the cohomology class η and that of the curve C interchangeably.

We denote by Σ_K the set of all places of K (including Archimedean places in the number field case). For a place v of K, we denote the image of a class $\eta \in H^1(K, E)$ under the local restriction map $H^1(K, E) \to H^1(K_v, E)$ by η_v. In geometric terms, η_v is just the base extension of the curve (or rather, the principal homogeneous space) C from K to K_v. By the *support* of a class we mean the finite set of $v \in \Sigma_K$ such that $\eta_v \neq 0$. The classes η with empty support form a subgroup $Ш(K, E)$, the *Shafarevich–Tate group* of $E_{/K}$.

1.2. *Statement of the main results.* Recall that K is a global field, P is a positive integer not divisible by the characteristic of K, and P^* is P if P is odd, and $2P$ if P is even.

Theorem 1. *Let $E_{/K}$ be an elliptic curve. Suppose $\#E(K)[P^*] = (P^*)^2$. Then, for any positive integer $D \mid P$, there are infinitely many classes $\eta \in H^1(K, E)$ of period P and index $P \cdot D$. These classes can be chosen so as to be locally trivial except possibly at two places of K.*

Theorem 2. *Let $E_{/K}$ be an elliptic curve and $S_K \subset \Sigma_K$ a finite set of places of K. There exists an infinite sequence $\{\eta_i\}_{i=0}^{\infty}$ of elements of $H^1(K, E)$ such that*

- $\eta_0 = 0$;
- *for all $v \in S_K$ and all $i \in \mathbb{N}$, $\mathrm{res}_v\, \eta_i = 0$; and*
- *for all $i,\ j \in \mathbb{N}$ with $i \neq j$, $\eta_i - \eta_j$ has period P and index P^2.*

Theorem 3. *Let $E_{/K}$ be an elliptic curve. For any positive integer r, there exists a degree P field extension L/K such that $Ш(L, E)$ contains at least r elements of order P.*

1.3. *Discussion of the results.* Let C be a genus-one curve over an arbitrary field K. It is well known (see [Lang and Tate 1958, Proposition 5], for example), that the period P and the index I of C satisfy the divisibilities

$$P \mid I \mid P^2. \tag{1}$$

Conversely, Lang and Tate showed [1958, p. 678] that for any pair (P, I) of positive integers satisfying (1), there exists a genus-one curve C defined over the iterated Laurent series field $\mathbb{C}((t_1))((t_2))$ with period P and index I.

This raises the question of the possible values of P and I for genus-one curves over a local or global field. Lichtenbaum [1968] showed that $P = I$ for every genus-one curve over a nondiscrete, locally compact field. [1]

Suppose K is a field which admits at least one degree-P cyclic extension and such that there exists an elliptic curve $E_{/K}$ with full P-torsion: $\#E[P](K) = P^2$. Then Lang and Tate showed that there exists a class $\eta \in H^1(K, E)$ with period and index both equal to P.

Let us assume henceforth that K is a global field. In this case, the argument of Lang and Tate readily yields the fact that η may be taken to have support at most one place of K.

Conversely, Cassels [1962, Theorem 1.3] showed that $I = P$ for classes with empty support. Moreover $I = P$ for classes whose support has cardinality one, as was first shown by Olson [1970, Theorem 15] and "rediscovered" by the first author [Clark 2006b, Proposition 6].

The first examples of genus-one curves over a global field with $I > P$ are due to Cassels [1963], who found examples over $K = \mathbb{Q}$ with $P = 2$, $I = 4$. Cassels' examples are closely related to the theory of explicit 2-descent. More recently, the first author constructed, for any prime number p, classes η with $P = p,\ I = p^2$ in the Weil–Châtelet group of any elliptic curve $E_{/K}$ over a number field with full p-torsion [Clark 2005, Theorem 3]. The method crucially employs a period-index obstruction map due to O'Neil [2002].

Our Theorem 1 may therefore be viewed as a generalization of [Clark 2005, Theorem 3]. In particular, we now know that any pair (P, I) satisfying (1) arises as the period and index of a genus-one curve defined over some number field (depending on P). Moreover, the fact that we can construct such classes which are supported at two places is, in view of the aforementioned results of Cassels and Olson, optimal, and answers a question raised by Çiperiani.

Having established Theorem 1, we naturally wish to understand the possible values of period and index for genus-one curves defined over a *fixed* global field K, or — better yet — inside the Weil–Châtelet group $H^1(K, E)$ of a fixed elliptic curve $E_{/K}$.

Our Theorem 2 shows that for any elliptic curve E over a global field K and any $P > 1$ indivisible by the characteristic of K, there exist infinitely many genus-one curves with period P, index P^2 and Jacobian E. Of course the statement

[1] More precisely, Lichtenbaum proved this under the assumption that P is not divisible by the characteristic of K — the same assumption which is in force for us — but Milne [1972] later extended Tate's local duality theory to this case and accordingly removed this hypothesis.

of Theorem 2 is significantly more complicated than this, and its significance is probably hard to appreciate. However, we need this precise statement, especially the "difference properties" of the sequence $\{\eta_i\}$, in the proof of Theorem 3.

In order to place Theorem 3 into context, let us again recall some prior results, this time on the problem of constructing "large Shafarevich–Tate groups." More precisely, we fix a global field K, an integer $P > 1$ and a positive integer r, and the goal is prove the existence of an elliptic curve $E_{/K}$ whose Shafarevich–Tate group $Ш(K, E)$ contains at least r elements of order P.

The first results here are due to Cassels [1964], who solved the aforementioned problem for $K = \mathbb{Q}$ and $P = 3$. (This was also the first proof of the weaker fact that $Ш(\mathbb{Q}, E)$ is unbounded as E ranges over all elliptic curves $E_{/\mathbb{Q}}$.) Cassels' examples all have $j = 0$ and exploit the extra structure on such curves afforded by the existence of an order 3 automorphism. The problem has also been solved for $P = 2$ by Bölling [1975], and for $P = 5$ by Fisher [2001]. Donnelly [2003] established the result for $P = 7$. Further, the case $P = 13$ is proved separately by Donnelly (unpublished) and Matsuno [2007]. Among prime values of P, this is a transitional case: the modular curve $X_0(P)$ has genus 0 precisely for these values of P. There are as yet no such results for larger P.

There has also been work showing that, for a prime p, either the p-Selmer group $\mathrm{Sel}^p(K, E)$ or $Ш(K, E)[p]$ can be made arbitrarily large when one varies over all elliptic curves E defined over number fields K whose degree $[K : \mathbb{Q}]$ is bounded by a certain function of p. Notably, Kloosterman and Schaefer [2003] showed that $\dim_{\mathbb{F}_p} \mathrm{Sel}^p(K, E)$ is unbounded as K ranges over all field extensions $K/\mathbb{Q}$ of degree $f_1(p) = O(p)$. Kloosterman [2005] showed that $\dim_{\mathbb{F}_p} Ш(K, E)[p]$ is unbounded as K ranges over extensions of degree $f_2(p) = O(p^4)$.

In [Clark 2005, Theorem 1], it was shown that if $\#E(K)[p] = p^2$ for a prime p, then $Ш(L, E)[p]$ is unbounded as L ranges over all degree p field extensions. The argument can be applied to any elliptic curve defined over a global field (of characteristic not divisible by p) at the cost of first trivializing the Galois action on the p-torsion. It follows that for every $E_{/K}$, $Ш(L, E)[p]$ is unbounded as L ranges over extensions of degree at most $f_3(p) = p(p^2 - 1)(p^2 - p) \le p^5$. Moreover, upon restricting to elliptic curves with potential complex multiplication, one gets the bound $f_4(p) \le 2p^3$.

In contrast, our Theorem 3 extends the bound $[L : K] = P$ of [Clark 2005, Theorem 1] to *all* elliptic curves and all integers $P > 1$. An interesting question (which we are not able to answer) is whether Theorem 3 is in fact the optimal result of its kind.

1.4. ***Organization of the paper.*** We assume some familiarity with the literature on the period-index problem, especially [O'Neil 2002; Clark 2005]; nevertheless, we begin with a brief review of the period-index obstruction map, and then go on to discuss some new ideas and techniques. The first key point is a clarification of the relationship between O'Neil's obstruction map Δ and the quantity I/P. Whereas before it had been implicit in [O'Neil 2002] (and explicit in [Clark 2005]) that one can use Δ to determine whether or not $I = P$, here we present a simple characterization of I/P in terms of the obstruction to a rational divisor class being represented by a rational divisor. We also return to the point of the explicit computation of O'Neil's obstruction map in the case of full-level N structure for even N. These matters are detailed in Section 2.

In Section 3 we give the proofs of Theorems 1, 2, and 3.

2. On the period-index obstruction map

In this section K is an arbitrary field, $E_{/K}$ is an elliptic curve, and P is a positive integer not divisible by the characteristic of K. These hypotheses ensure that the finite flat K-group scheme $E[P]$ is étale, and so may be viewed as a $\mathfrak{g}_K$-module.

2.1. ***Three aspects of the period-index obstruction map.*** The key technical tool in the proofs of our results is the *period-index obstruction map*

$$\Delta_P : H^1(K, E[P]) \to \mathrm{Br}(K).$$

It can be defined in three different ways, which we now recall. All three characterizations either explicitly appear in or are readily deducible from [O'Neil 2002]. Note that Δ_P is *not* a homomorphism; as we shall see, it is a quadratic map.

Definition 1. For any ample line bundle L on an abelian variety $A_{/K}$, the functor $\mathcal{G}_L$ which associates to a K-scheme S the group of all isomorphisms

$$(x, \psi) : L_{/S} \xrightarrow{\sim} \tau_x^*(L_{/S})$$

between $L_{/S}$ and one of its translates is represented by a K-group scheme, Mumford's *theta group*. The subgroup of automorphisms of L gives rise to an embedding $\mathbb{G}_m \hookrightarrow \mathcal{G}_L$. The quotient is canonically isomorphic to $\kappa(L)$, the kernel of the canonical homomorphism

$$\varphi_L : A \to A^\vee, x \mapsto \tau_x^*(L) \otimes L^{-1}.$$

We now follow O'Neil's construction [2002, §2]. Let A be an elliptic curve E and L the line bundle associated to the divisor $P[O]$ on E; note that $\kappa(L) = E[P]$. Let $\varphi_L : E \to \mathbb{P}^{P-1}$ be the associated morphism into projective space (well-defined up to a linear automorphism of $\mathbb{P}^{P-1}$).

Proposition 4. *For $P \geq 2$ we have the following commutative diagram of group schemes*:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d] & \mathscr{G}_L \arrow[r] \arrow[d] & E[P] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathrm{GL}_P \arrow[r] & \mathrm{PGL}_P \arrow[r] & 0
\end{tikzcd} \tag{2}$$

Proof. This is [O'Neil 2002, Proposition 2.1]. For our purposes, we will only need to know the vertical map on the right. We view $E[P]$ as an automorphism group of $\varphi_L : E \to \mathbb{P}^{P-1}$ — that is, an element of $E[P]$ acts on the global sections of L, and thus induces an automorphism of $\mathbb{P}^{P-1}$. This gives an element of PGL_P as required. □

The machinery of nonabelian Galois cohomology [Serre 1962] supplies a connecting map from $H^1(K, E[P]) \to H^2(K, \mathbb{G}_m)$. Identifying $H^2(K, \mathbb{G}_m)$ with $\mathrm{Br}(K)$, we obtain our first definition of Δ_P.

Definition 2. Let $V_{/K}$ be any nonsingular, complete, geometrically integral variety, and let $\mathrm{Pic}(V)$ be the Picard group of V. There is an exact sequence [Bosch et al. 1990, §9.1]

$$0 \to \mathrm{Pic}(V) \to \mathbf{Pic}(V)(K) \xrightarrow{\delta_V} \mathrm{Br}(K) \xrightarrow{\gamma} \mathrm{Br}(V). \tag{3}$$

In particular, given a K-rational divisor class D on V, the obstruction to V being represented by a K-rational divisor is an element of $\mathrm{Br}(K)$. A Galois descent argument shows that $H^1(K, E[P])$ classifies pairs (C, D) — where $C \in H^1(K, E)$ and $D \in \mathbf{Pic}^P(C)(K)$ is a K-rational divisor class — modulo the relation $(C, D) \sim (C', D')$ if there exists a K-isomorphism of torsors $f : C \to C'$ with $f^*D' = D$. One may then define

$$\Delta_P((C, D)) = \delta_C(D).$$

For details, including a proof of the equivalence of this definition with the previous one, see [O'Neil 2002, Proposition 2.3] and [Clark 2005, Proposition 4].

Definition 3. On the other hand, $H^1(K, E[P])$ classifies K-morphisms $\varphi : C \to V$ which are twisted forms of $\varphi_L : E \to \mathbb{P}^{P-1}$; these forms arise as twists of the map associated to the complete linear system $P[O]$. In particular, $C \in H^1(K, E)$ and V is a twisted form of $\mathbb{P}^{P-1}$; that is, a Severi–Brauer variety [O'Neil 2002; Cremona et al. 2008, §1.2]. We may then define $\Delta_P(\varphi : C \to V) = [V]$, the class of V in $\mathrm{Br}(K)$. It follows that $\Delta_P(H^1(K, E[P]))$ consists of elements of $\mathrm{Br}(K)$ whose *index* divides P; *a fortiori* we have the important relation

$$\Delta_P(H^1(K, E[P])) \subset \mathrm{Br}(K)[P].$$

2.2. ***Lichtenbaum–Tate Duality.*** As above, we let E be an elliptic curve defined over an arbitrary field K, and now let n denote a positive integer indivisible by the characteristic of K.[2] We have the *Kummer sequence*

$$0 \to E(K)/nE(K) \xrightarrow{\iota} H^1(K, E[n]) \to H^1(K, E)[n] \to 0. \tag{4}$$

Using ι and Δ, we may define a map $\mathrm{Li} : H^1(K, E[n]) \times E(K) \to \mathrm{Br}(K)$ by

$$\mathrm{Li}(\xi, x) = \Delta(\xi + \iota(x)) - \Delta(\xi) - \Delta(\iota(x)).$$

Since $\Delta(\iota(E(K)/nE(K))) = 0$, Li depends only on the image of ξ in $H^1(K, E)[n]$ and on the image of x in $E(K)/nE(K)$; that is, it descends to give a map

$$\mathrm{Li} : H^1(K, E)[n] \times E(K)/nE(K) \to \mathrm{Br}(K)[n]. \tag{5}$$

We also have the Tate pairing

$$T : H^1(K, E)[n] \times E(K)/nE(K) \to \mathrm{Br}(K)[n]. \tag{6}$$

There are many definitions of the Tate pairing; see for example [Tate 1958; Lichtenbaum 1969]. Perhaps the most straightforward is as follows. Given (ξ, x), lift ξ to any η in $H^1(K, E[n])$. Consider the cup product

$$\eta \cup \iota(x) \in H^2(K, E[n] \otimes E[n]),$$

and follow by the Weil pairing to obtain a class in $H^2(K, \mu_n)$; the latter is canonically isomorphic to $\mathrm{Br}(K)[n]$. The resulting Brauer class is $T(\xi, x)$. Note that the pairing is independent of our choice of n, in the sense that we may replace n by any multiple without changing the value of the pairing.

Theorem 5 [O'Neil 2002, §5]. *The map* Li *coincides with the Tate pairing* T.

Since T is bilinear, the theorem implies that so is Li, and together with the fact that $\Delta(d\xi) = d^2\Delta(\xi)$ [O'Neil 2002, Lemma 4.2] this means that Δ itself is a quadratic map. This also follows from the first definition of Δ as a connecting map in nonabelian cohomology, together with [Zarhin 1974]. Note that if K is complete, discretely valued, and has finite residue field, then $\mathrm{Br}(K)[n] = (\frac{1}{n}\mathbb{Z})/\mathbb{Z}$, and Li puts the finite abelian groups $H^1(K, E)[n]$ and $E(K)/nE(K)$ in Pontrjagin duality ("Tate local duality").

[2] Thus n satisfies exactly the same requirements as our "fixed"' positive integer P. The merit of considering both "fixed P" and "variable n" will become clear in the next section.

2.3. ***Theta functoriality.*** Let η be a class in $H^1(K, E)[n]$. The exactness of the Kummer sequence (4) means that η has at least one lift to an element

$$\xi \in H^1(K, E[n]).$$

Following O'Neil and Clark, we attempt to use the obstruction maps Δ to study the discrepancy between the period and the index of η.

Now a key point: in [Clark 2005] we only considered the case where n is equal to the period P of η. But certainly we can also choose lifts $\xi_n \in H^1(K, E[n])$ whenever n is any multiple of the period of η. It turns out to be quite useful to do so, and in particular to compare various obstruction maps Δ_n of differing levels. Geometrically speaking this amounts to considering along with the theta group $\mathscr{G}_L$ of our fixed line bundle $L = L(P[O])$ the theta groups of all tensor powers L^m of L and various natural homomorphisms between them. The study of such homomorphisms is an integral part of Mumford's theory.

So let m be yet another positive integer indivisible by the characteristic of K. The natural inclusion $E[P] \hookrightarrow E[mP]$ of $\mathfrak{g}_K$-modules induces a map

$$j_m : H^1(K, E[P]) \to H^1(K, E[mP]).$$

Under the interpretation 2 of $H^1(K, E[P])$ as equivalence classes of pairs (C, D), where $C \in H^1(K, E)$ and $D \in \mathbf{Pic}^P(C)$, j_m is the map $(C, D) \mapsto (C, mD)$.

Similarly, multiplication by m induces a map

$$[m] : H^1(K, E[mP]) \to H^1(K, E[P]).$$

Proposition 6. *If $\xi \in H^1(K, E[P])$ and $\eta \in H^1(K, E[mP])$, then*:

(a) $\Delta_{mP}\, j_m(\xi) = m\Delta_P(\xi)$, *and*

(b) $m\Delta_{mP}\eta = \Delta_P([m]\eta)$.

Proof. Mumford [1966, pp. 309–310] shows that both j_m and $[m]$ extend to morphisms of the theta group sequences:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, "{[m]}"] & \mathscr{G}_L \arrow[r] \arrow[d, "\epsilon_m"] & E[P] \arrow[r] \arrow[d, "j_m"] & 0 \\
0 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathscr{G}_{L^m} \arrow[r] & E[mP] \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, "{[m]}"] & \mathscr{G}_{L^m} \arrow[r] \arrow[d, "\eta_m"] & E[mP] \arrow[r] \arrow[d, "{[m]}"] & 0 \\
0 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathscr{G}_L \arrow[r] & E[P] \arrow[r] & 0
\end{tikzcd}$$

In each case the restriction to $\mathbb{G}_m$ is simply the mth power map. We remark that the map $\epsilon_m : \mathscr{G}_L \to \mathscr{G}_{L^m}$ is relatively straightforward to define: an isomorphism $\psi : L \overset{\sim}{\to} \tau_x^* L$ induces, by passage to the mth power, a canonical isomorphism $\psi^{\otimes m} : L^m \overset{\sim}{\to} \tau_x^*(L^m)$, so $\epsilon_m : (x, \psi) \mapsto (x, \psi^m)$. These commutative ladders induce commutative ladders in nonabelian Galois cohomology, and the commutativity of these last two diagrams gives the desired result. □

2.4. ***Applications to the quantity I/P.*** We begin with the following result, which was known to O'Neil:

Proposition 7 [Clark 2005, Theorem 5]. *Let $E_{/K}$ be an elliptic curve over a field K, and P a positive integer indivisible by the characteristic of K. Let $\eta \in H^1(K, E)$ be of period P. The following are equivalent*:

(a) *η has index P.*

(b) *There exists some lift $\xi \in H^1(K, E[P])$ of η such that $\Delta_P(\xi) = 0$.*

Proof. If C is the genus-1 curve represented by η, then in light of the second definition of Δ_P, both conditions express the fact that C admits a rational divisor of degree P. □

We are therefore interested in the remaining case in which $\Delta_P(\xi) \neq 0$ for every lift ξ of η to $H^1(K, E[P])$.

Let $C_{/K}$ be a curve of any genus, of period P and index I. Referring back to (3), we may define the *relative Brauer group* $\kappa(C/K) = \mathrm{Im}(\delta_C) = \mathrm{Ker}(\gamma)$. For any $n \in \mathbb{Z}$, define moreover $\kappa^n(C/K) = \delta_C(\mathbf{Pic}^n(C)(K))$.

Proposition 8. *The quotient $\kappa(C/K)/\kappa^0(C/K)$ is cyclic of order I/P.*

This is a reasonably well-known result [Ciperiani and Krashen 2007, Theorem 2.1.1; Clark 2006a, Proposition 24], the standard proof of which employs a snake lemma argument. But the following proof offers some additional insight.

Proof. By the definition of P we have $\mathbf{Pic}^n(C)(K) = \varnothing$ unless n is a multiple of P, so

$$\kappa(C/K) = \delta_C(\mathbf{Pic}(C)(K)) = \delta_C\Bigl(\bigcup_{n\in\mathbb{Z}} \mathbf{Pic}^{nP}(C)(K)\Bigr)$$
$$= \bigcup_{n\in\mathbb{Z}} \delta_C(\mathbf{Pic}^{nP}(C)(K)) = \bigcup_{n\in\mathbb{Z}} \kappa^{nP}(C/K).$$

Choose a rational divisor class D of degree P; this in turn determines a rational divisor class of each degree nP, namely $D_{nP} = nD$. Put $\alpha = \delta_C(D)$, so that $\delta_C(D_{nP}) = n\alpha$. Adding D_{nP} induces a bijection of sets $\mathbf{Pic}^0(C)(K) \to \mathbf{Pic}^{nP}(C)$, and exhibits

$$\kappa^{nP}(C/K) = n\alpha + \kappa^0(C/K)$$

as a coset of the subgroup $\kappa^0(C/K)$ of $\mathrm{Br}(K)$. This shows that $\kappa(C/K)$ is the subgroup generated by α and $\kappa^0(C/K)$. Moreover, C admits a rational divisor of degree nP if and only if $0 \in \kappa^{nP}(C/K)$ if and only if $n\alpha \in \kappa^0(C/K)$. The quantity I/P is the least such value of n, that is, the order of

$$\langle \alpha + \kappa^0(C/K)\rangle / \kappa^0(C/K) = \kappa(C/K)/\kappa^0(C/K). \qquad \square$$

Proposition 9. *Let $\eta \in H^1(K, E)$ be a class with period P and index I, and let ξ be any lift of η to $H^1(K, E[P])$. Then*

$$I/P \le \min_{x \in E(K)/PE(K)} \operatorname{order}(\Delta_P(\xi + \iota(x))). \tag{7}$$

Proof. As x runs through $E(K)/PE(K)$, the elements $\xi + x$ run through all lifts of η to $H^1(K, E[P])$. For any such lift ξ, let $D = \operatorname{order}(\Delta_P(\xi))$. Then $\Delta_{PD}(j_D(\xi)) = D\Delta_P(\xi) = 0$, so that there is a rational divisor of degree PD on the corresponding torsor, and $I \le PD$. □

Concerning the inequality (7), Proposition 7 says that the left-hand side equals 1 if and only if the right-hand side does. When $P = p$ is prime, we have a simple dichotomy: either $I/P = 1$ or $I/P = p$, so equality holds in (7) when the period is prime, a fact which was exploited in [Clark 2005]. By a primary decomposition argument, we also have equality when P is square-free. It is not hard to see that equality holding in (7) is equivalent to the *splitting* of the short exact sequence

$$0 \to \kappa^0(C/K) \to \kappa(C/K) \to Q \to 0, \tag{8}$$

where the last term Q is cyclic of order I/P. It is natural to wonder whether this sequence *always* splits. This innocuous-looking question lies at the heart of the relationship between the period, the index and the period-index obstruction map, and it turns out to be surprisingly difficult. We believe that the answer is in general negative. However it is possible to show that equality holds for certain specially constructed classes. In the proofs of the main theorems we use Lichtenbaum–Tate duality to ensure equality, following [Sharif 2006].

2.5. ***The case of full-level P structure.*** In this section we assume that $E[P](\overline{K}) \subset E(K)$. By the theory of the Weil pairing, the Pth roots of unity μ_P are contained in K. Fix a basis (S, T) for $E[P]$ once and for all. Note that this induces, via the Weil pairing, a basis for μ_P — that is, a specific primitive Pth root of unity $\zeta = e_P(S, T)$. After making this choice, we get an isomorphism

$$\Phi : H^1(K, \mu_P) \times H^1(K, \mu_P) \xrightarrow{\sim} H^1(K, E[P]). \tag{9}$$

The composition of the cup product with the map $\mu_P \otimes \mu_P \to \mu_P$ given by

$$\zeta^a \otimes \zeta^b \mapsto \zeta^{ab}$$

gives a pairing

$$\langle\, ,\rangle_P : H^1(K,\mu_P)\times H^1(K,\mu_P)\to H^2(K,\mu_P)=\mathrm{Br}(K)[P],$$

the *level P norm-residue symbol* (or *Hilbert symbol*) [Serre 1962, p. 207].

Via the canonical Kummer isomorphism $H^1(K,\mu_P) = K^\times/K^{\times P}$, we may equally well view Φ and $\langle\, ,\rangle_P$ as maps defined on $(K^\times/K^{\times P})^2$.

Theorem 10. *If $E[P^*]\subset E(K)$, then $\Delta_P\circ\Phi=\langle\, ,\rangle_P$.*

As a prelude to the proof, we consider the *special theta group*. Recall the theta group scheme $\mathscr{G}_L$, where L is the class of $P[O]$. We found a homomorphism from $\mathscr{G}_L$ to GL_P. Form the fiber product

$$\mathscr{S}_L=\mathscr{G}_L\times_{\mathrm{GL}}\mathrm{SL}_P,$$

where $\mathrm{SL}_P\subset\mathrm{GL}_P$ is the special linear group. Then we have an exact sequence

$$0\to\mu_P\to\mathscr{S}_L\to E[P]\to 0,$$

where the maps are the restrictions of the maps in (2). If we identify $H^2(K,\mu_P)$ with $(\mathrm{Br}\,K)[P]$, then the coboundary $H^1(K,E[P])\to H^2(K,\mu_P)$ is the obstruction map. Let $c:H^0(K,E[P])\to H^1(K,\mu_P)$ be the lower dimension coboundary. Define

$$d:H^1(K,E[P])\to(\mathrm{Br}\,K)[P]$$

to be given by $d\xi(\sigma,\tau)=c(\xi(\tau))(\sigma)$. (Note that since $E[P]$ is a trivial Galois module, each cohomology class in $H^1(K,E[P])$ consists of a single cocycle.)

Lemma 11. $\Delta=\langle\, ,\rangle\circ\Phi^{-1}+d.$

Proof. As mentioned above, we have earlier shown [Clark 2005, Theorem 6] that

$$\Delta-\langle\, ,\rangle\circ\Phi^{-1}$$

is a homomorphism of groups. Therefore it suffices to prove the claim for any subset of $H^1(K,E[P])$ which generates the group. We will consider the subset given by the images of $H^1(K,\mathbb{Z}/P\mathbb{Z})$ induced by the two maps $(1\mapsto S)$ and $(1\mapsto T)$. By symmetry, it suffices to consider the case $(1\mapsto S)$ only. Let $a\in\mathrm{Hom}(\mathfrak{g}_K,\mathbb{Z}/P\mathbb{Z})$, and let ξ be the image of a under the map $(1\mapsto S)$. Clearly $\langle\Phi^{-1}(\xi)\rangle=0$. Map S down to $\mathrm{PGL}_P(K)$, then lift to an element M_S in $\mathrm{SL}_P(\overline{K})$. We set $M_{aS}=M_S^a$. Note that since $\det M_S=1$ and S has order P, we must have

$M_S^P = I$. Then

$$\begin{aligned}(\Delta\xi)(\sigma,\tau) &= M_S^{a(\sigma)}(\sigma M_S^{a(\tau)})M_S^{-a(\sigma\tau)}\\ &= M_S^{a(\sigma)}a(\tau)\cdot c(S)(\sigma)M_S^{a(\tau)}M_S^{-a(\sigma\tau)}\\ &= a(\tau)\cdot c(S)(\sigma)\\ &= c(\xi(\tau))(\sigma)\\ &= d\xi(\sigma,\tau).\end{aligned}$$

The second equality follows from the fact that $c(S)(\sigma) = (\sigma M_S)M_S^{-1}$. □

Lemma 12. $2d = 0$.

Proof. It suffices to show that $2c = 0$. Let ι be the group inverse map on $E[P]$. According to [Mumford 1966, p. 308], ι extends to a map on the theta group $\mathcal{G}_L$ which acts as the identity on $\mathbb{G}_m$. We restrict ι to $\mathcal{S}_L$. By the functoriality of c, if $x \in H^0(K, E[P]) = E[P]$, then $c \circ \iota(x) = c(x)$. But $c \circ \iota(x) = c(-x) = -c(x)$, which proves the claim. □

Proof of Theorem 10. If P is odd, then $H^1(K, \mu_P)$ has trivial 2-torsion. Therefore Lemma 12 implies that $d = 0$. By Lemma 11, the conclusion follows.

Now suppose P is even. According to [Mumford 1966, p. 310], there is a map $\eta_2 : \mathcal{G}_{L^2} \to \mathcal{G}_L$ which, upon restriction to the subgroup schemes $\mathcal{S}_L$ and $\mathcal{S}_{L^2}$, induces the commutative diagram

$$\begin{tikzcd} H^0(K, E[2P]) \arrow[r, "c"] \arrow[d, "{[2]}"] & H^1(K, \mu_{2P}) \arrow[d, "{[2]}"] \\ H^0(K, E[P]) \arrow[r, "c"] & H^1(K, \mu_P) \end{tikzcd}$$

By the proof of Lemma 12, $[2] \circ c$ is the zero map. Therefore $c \circ [2]$ is zero. The hypothesis $E[2P] \subset E(K)$ implies that the left-hand map above is surjective, and therefore the lower map c is zero. By Lemma 11, the result follows. □

3. Proofs of Theorems 1, 2 and 3

We first remind the reader of a standard trick: in all work on the period-index problem it suffices to treat the case where the period P is a prime power $P = p^a$. Indeed, if a class $\eta \in H^1(K, E)$ (or any other Galois cohomology group, for that matter) has period $P = p_1^{a_1} \dots p_r^{a_r}$, then putting $\eta_i = (P/p_i^{a_i})\eta$, one easily checks that $\eta = \sum_{i=1}^r \eta_i$ and that $I(\eta) = \prod_{i=1}^r I(\eta_i)$ (that is, the index of η is the product of the indices of the classes η_i). The advantage of reducing to the case $P = p^a$ is that then the index $I = p^b$ for $a \le b \le 2a$ and then for any $D = p^c$, if the index I is less than DP, then indeed I is a proper divisor of DP.

3.1. ***Conditions on prime ideals and their generators.*** Several times in the proofs we will be choosing pairs of prime ideals v, v' of $\mathbb{O}_K$ so as to satisfy certain conditions. Let us first say that a prime ideal v of K is "bad" (for E and $P = p^a$) if v is Archimedean, v divides p, or E has bad reduction at v, and is "good" otherwise. All but finitely many primes are good.

The conditions we will impose on v and v' can all be achieved by using the Chebotarev density theorem. The conditions are:

(SC1) The primes $v = (\pi)$ and $v' = (\pi')$ are principal, with totally positive generators π and π'.

(SC2) All elements of $E(K)$ are P-divisible in $E(K_v)$.

(SC3) The generators π and π' lie in $K_w^{\times P}$ for all bad primes w.

(SC4) The order of the image of π' in $K_v^\times / K_v^{\times P}$ is P.

Lemma 13. *Suppose that $E[P] \subset E(K)$. Then there exist infinitely many pairs of primes $v = (\pi)$ and $v' = (\pi')$ satisfying conditions* (SC1)–(SC4).

Proof. In order to satisfy condition (SC4), we will need to choose v first, as v' depends on this choice. However, the procedure for choosing the two is similar, so the argument below is presented for both at once.

Condition (SC1) is equivalent to v and v' splitting completely in the Hilbert class field of K, while condition (SC2) is equivalent to v splitting completely in $K([P]^{-1}E(K))$, the field obtained by adjoining to K all points $Q \in E(\overline{K})$ such that $[P]Q \in E(K)$. (Recall that under the hypothesis $E[P] \subset E(K)$, $K([P]^{-1}E(K))$ is a finite abelian extension of K unramified outside the bad primes [Silverman 1986, p. 194].)

Let $\mathfrak{m}$ be the modulus given by the product of all bad primes $\mathfrak{p}$ and P^2. Then one can find π and π' as in (SC3) provided v and v' split completely in the ray class field for K modulo $\mathfrak{m}$. For if v splits completely, it has trivial Frobenius and, by class field theory, has a generator π which is congruent to $1 \pmod{\mathfrak{m}}$. The condition follows from Hensel's Lemma.

Therefore, to satisfy conditions (SC1)–(SC3), we need v and v' to split completely in the abelian extension F which is the compositum of the Hilbert class field of K, $K([P]^{-1}E(K))$, and the ray class field $K_{\mathfrak{m}}$.

Now we consider (SC4). Suppose that we have chosen v already. Let α be a unit in K_v which has order P in $K_v^\times / K_v^{\times P}$. Let F' be the ray class field with modulus v. By class field theory, the Galois group of F'/K is isomorphic to the ideal class group with modulus v, C_v. In particular, if v' and (α) lie in the same class in C_v, then v' has a generator π' which is congruent to $\alpha \pmod{v}$, and hence satisfies (SC4).

Thus, we have reduced conditions (SC1)–(SC4) to two splitting-type conditions in the abelian extensions F and F'. It suffices to show that these splitting conditions are compatible, since then the Chebotarev density theorem shows there are infinitely many primes satisfying the conditions.

The extension F/K is unramified at v, while F'/K is unramified outside v. Therefore $F \cap F'$ is contained in the Hilbert class field of K. This is enough to choose v. Any v' which lies in the same class as (α) in C_v must be principal, and hence splits in $F \cap F'$. We conclude that the splitting conditions are compatible, which proves the lemma. □

3.2. ***Proof of Theorem 1.*** We assume in this section that E has full level P^*-structure, and maintain the setup of §2.5. In particular, we have a fixed isomorphism

$$\Phi : (K^\times/K^{\times P})^2 \cong H^1(K, E[P]).$$

Let $v = (\pi)$ and $v' = (\pi')$ satisfy conditions (SC1)–(SC4). Put

$$\xi := \Phi(\pi^{P/D}, \pi') \in H^1(K, E[P]),$$

so by Theorem 10 we have

$$\Delta_P(\xi) = \langle \pi^{P/D}, \pi' \rangle_P \in \mathrm{Br}(K).$$

Observe that $\Delta_P(\xi)$ is locally trivial away from π and π'. Indeed, by condition (SC3), the norm-residue symbol is trivial at the Archimedean places and at the places of residue characteristic dividing P. At all other places the norm residue symbol is "tame" and hence vanishes locally at w when evaluated on a pair of w-adic units.

Let C be the genus-one curve corresponding to the image η of ξ in $H^1(K, E)[P]$. Certainly the period of η divides P. Suppose that the period of η is less than P; then (since $p^a\eta = 0$) it has period P' for some proper divisor P' of P: $P'\xi = \iota_P(x)$. Then $\iota_P(x)$ is unramified at π' [Silverman 1986, Proposition VIII.2.1], whereas $P'\xi = (\pi^{PP'/D}, (\pi')^{P'})$ is ramified at π', a contradiction. So C has period P. Moreover, by Proposition 6,

$$\Delta_{PD} j_D(\xi) = D\Delta_P(\xi) = D\langle \pi^{P/D}, \pi' \rangle_P = \langle \pi^P, \pi' \rangle_P = 0,$$

so there exists a rational divisor of degree PD on C and $I(C) \mid PD$.

Coming now to the heart of the matter, we suppose that the index I of C strictly divides PD. Then, by Proposition 7 there exists some lift ν of η to $H^1(K, E[I])$ (under (4) with $n = I$) such that $\Delta_I(\nu) = 0$. On the other hand, the local-at-π norm-residue symbol $\langle \pi^{P/D}, \pi' \rangle_{P,\pi}$ has exact order D, since, by condition (SC4), the corresponding central simple algebra trivializes over the Brauer group of an extension L/K_v if and only if π' is a norm from the extension $L(\pi^{1/D})/L$ if and only if $D \mid e(L/K)$. Therefore the global norm-residue symbol $\langle \pi^{P/D}, \pi' \rangle_P = \Delta_P(\xi)$ has order at least D; since $I/P < D$ we must have

$$0 \neq (I/P) \cdot \Delta_P(\xi) = \Delta_I(j_{I/P}(\xi)).$$

For the remainder of the proof we shall abbreviate $j_{I/P}(\xi)$ to $j(\xi)$. The classes $j(\xi)$ and $\nu \in H^1(K, E[I])$ are both lifts of η, so there exists $x \in E(K)$ with

$$\iota_I(x) = \nu - j(\xi).$$

Applying Δ, we get

$$0 = \Delta_I(\nu) = \Delta_I(j(\xi)) + \mathrm{Li}(j(\xi), x).$$

Now recall that (π) splits completely in $K([P]^{-1}E(K))$ by condition (SC2). This forces $E(K)$ to be divisible by P in $E(K_v)$, and in particular $x \in PE(K_v)$. It follows that the (π)-component of $\mathrm{Li}(j(\xi), x)$ and hence also of $\Delta_I(j(\xi))$ are trivial. Thus $\Delta_I(j(\xi)) = (I/P)\Delta_P(\xi)$ is locally trivial at all places except possibly at (π'), and by the reciprocity law and Hasse principle in the Brauer group of a local field this implies that it is globally trivial — $\Delta_I(j(\xi)) = 0$ — a contradiction.

Finally, we claim that the image η of ξ under $H^1(K, E[P]) \to H^1(K, E)[P]$ is locally trivial away from v and v'. First let w be a bad prime. Then, by construction, $\pi, \pi' \in K_w^{\times P}$ so $\xi|_{K_w} = 0$; *a fortiori* $\eta_w = 0$. Now suppose $w \neq v, v'$ is a good prime. Let K_w^{unr} be the maximal unramified extension of K_w. Recall that the restriction map $H^1(K_w, E)[P] \to H^1(K_w^{\mathrm{unr}}, E)[P]$ is injective [Lang and Tate 1958, Corollary 1]; this follows, for instance from the triviality of WC-groups over finite fields together with the fact that formation of the Néron model of a genus-one curve commutes with unramified base change. Since $K_w((\pi')^{1/P})/K_w$ is unramified, ξ trivializes over K_w^{unr}. But this implies that $\zeta|_{K_w^{\mathrm{unr}}} = 0$ and hence that $\eta|_{K_w} = 0$. This completes the proof of Theorem 1.

3.3. *Proof of Theorem 2: preliminaries.* First, we wish to reduce to Theorem 1, that is, to the case where $E[P^*]$ has trivial Galois module structure. To this end we introduce the splitting field $K_P = K(E[P^*])$ of the P^*-torsion. We will construct classes θ_n in $H^1(K_P, E[P])$ in a similar manner as in the proof of Theorem 1, then we will set $\xi_n = \mathrm{cores}_{K_P/K}\, \theta_n$, and let η_n be the image of ξ_n in $H^1(K, E)$. In order to prove that the η_n have the right properties, we will need to compute $\mathrm{res}_{K_P/K}\, \xi_n = \mathrm{res} \circ \mathrm{cores}\, \theta_n$ explicitly.

In the following, let $\langle\, , \rangle$ denote the P-Hilbert symbol on $({K_P}^{\times}/{K_P}^{\times P})^2$.

3.4. *Proof of Theorem 2: choosing pairs of primes.* In this section, we choose pairs of primes in a similar manner as in Lemma 13. The main difference is that we wish to choose an infinite sequence of pairs of primes v_i, v_i' in K_P inductively. We will require conditions which are similar, and in some cases identical, to (SC1)–(SC4). These conditions are as follows:

(SC1′) The primes $v_i = (\pi_i)$ and $v_i' = (\pi_i')$ are principal, with totally positive generators π_i and π_i'.

(SC2′) Let $\tilde{v}_i$ and $\tilde{v}_i'$ be primes of K lying below v_i and v_i' respectively (for fixed i). Then all elements of $E(K)$ are P-divisible in $E(K_{\tilde{v}_i})$ and in $E(K_{\tilde{v}_i'})$.

(SC3′) The generators π_i and π_i' lie in $(K_P)_w^{\times P}$ for all bad primes w, primes lying above S_K, and for $w = v_j, v_j'$ where $j < i$.

(SC4′) The order of the image of π_i' in $(K_P)_{v_i}^\times/(K_P)_{v_i}^{\times P}$ is P. Additionally, $\sigma\pi_i'$ lies in $(K_P)_{v_i}^{\times P}$ for all nontrivial $\sigma \in \mathrm{Gal}(K_P/K)$.

(SC5′) The primes $\tilde{v}_i, \tilde{v}_i'$ are totally split in K_P.

Lemma 14. *There exist* $v_i = (\pi_i)$, $v_i' = (\pi_i')$ *satisfying conditions* (SC1′)–(SC5′).

Proof. We argue inductively: suppose that we have chosen v_j, v_j' for $j < i$. We let $\mathfrak{m}$ be the modulus given by the product of all bad primes in K, P^2, and all σv_j and $\sigma v_j'$ for $j < i$, $\sigma \in \mathrm{Gal}(K_P/K)$; and let F be the compositum of $K_P([P]^{-1}E(K))$ and the $\mathfrak{m}$-ray class field of K_P. Note that $\mathfrak{m}$ is rational over K, so F is Galois over K. As before, F is an abelian extension of K_P. By the Chebotarev density theorem, there exists a prime $\tilde{v}_i$ of K which splits completely in F. Let v_i be any prime of K_P which lies over $\tilde{v}_i$. Then, provided (SC5′) holds, the same reasoning as in Lemma 13 shows that v_i satisfies all the conditions. (We need (SC5′) only for condition (SC2′), for otherwise we know only that $E(K_P)$ is P-divisible in $E((K_P)_{v_i})$.)

Let β be a unit in $(K_P)_{v_i}$ which has order P in $(K_P)_{v_i}^\times/(K_P)_{v_i}^{\times P}$. By the Chinese Remainder Theorem, there exists $\alpha \in K_P$ such that

$$\begin{aligned} &\alpha \equiv \beta \pmod{v_i}, \\ &\alpha \equiv 1 \pmod{\sigma v_i} \quad \text{for all } \sigma \in \mathrm{Gal}(K_P/K),\ \sigma \neq 1. \end{aligned} \tag{10}$$

Let F' be the ray class field for K_P with modulus $\mathfrak{m}' = \prod \sigma v_i$. Again, $\mathfrak{m}'$ is rational over K, so that F' is Galois over K. Let $C_{\mathfrak{m}'}$ be the class group for K_P with modulus $\mathfrak{m}'$. The Artin reciprocity map gives an isomorphism $C_{\mathfrak{m}'} \to \mathrm{Gal}(F'/K_P)$. Let $\gamma_{F'}$ be the image of (α) under this isomorphism. Since $F \cap F'$ is contained in the Hilbert class field of K_P and (α) is principal, there exists $\gamma \in \mathrm{Gal}(FF'/K_P)$ such that $\gamma|_{F'} = \gamma_{F'}$ and $\gamma|_F$ is the identity. Since FF' is Galois over K, we view $\mathrm{Gal}(FF'/K_P)$ as a subgroup of $\mathrm{Gal}(FF'/K)$. Let $[\gamma]$ be the conjugacy class of γ in this larger Galois group. By Chebotarev, there exists a prime $\tilde{v}_i'$ of K such that any Frobenius associated to $\tilde{v}_i'$ in the extension FF'/K lies in $[\gamma]$. Let v_i' be a prime of K_P lying over $\tilde{v}_i'$. By replacing v_i' by a conjugate if necessary, we may assume that the Frobenius of v_i' in the extension FF'/K_P is precisely γ (the extension here is abelian, so saying "the" Frobenius makes sense). By the same arguments as in Lemma 13, v_i' satisfies the first three conditions.

One sees that $\pi_i' \equiv \alpha \pmod{(\pi_i)}$, so that the order of π_i' in $(K_P)_{v_i}^\times/(K_P)_{v_i}^{\times P}$ is P. Also, $\pi_i' \equiv 1 \pmod{(\sigma\pi_i)}$ for nontrivial σ, so that $\sigma\pi_i' \equiv 1 \mod (\pi_i)$. Therefore v_i' satisfies condition (SC4′).

Any Frobenius associated to $\tilde{v}_i'$ in the extension K_P/K is trivial, so that $\tilde{v}_i'$ splits in K_P, thus satisfying (SC5′). □

3.5. ***Proof of Theorem 2: corestrictions.*** As in the proof of Theorem 1, a choice of basis for $E[P]$ yields an isomorphism

$$\Phi : (K_P{}^\times/K_P{}^{\times P})^2 \to H^1(K_P, E[P]).$$

Let θ_n be either $\Phi(\pi_n, \pi_n')$ or $\Phi(\pi_n, 1)$; that is, we will need to consider both cases. Let cores be the corestriction map

$$H^1(K_P, E[P]) \to H^1(K, E[P]),$$

and write $\xi_n = \operatorname{cores}\theta_n$. In order to prove Theorem 2, we would like to compute $\Delta_P(\xi_n - \xi_m)$ as well as the period of $(\xi_n - \xi_m)$. To do this, we will instead compute the obstruction and period of $\operatorname{res}(\xi_n - \xi_m)$, where res is the restriction map

$$H^1(K, E[P]) \to H^1(K_P, E[P]).$$

Both res and cores are $\mathbb{Z}$-linear, so it will suffice to compute $\operatorname{res}\circ\operatorname{cores}(\Phi(\pi_n, 1))$ and $\operatorname{res}\circ\operatorname{cores}(\Phi(1, \pi_n'))$.

Let $\mathrm{Nm} \in \mathrm{End}(H^1(K_P, E[P]))$ be given, on the level of cocycles, by

$$\mathrm{Nm}(\theta)(\sigma) = \sum_{\bar{\gamma}\in\mathrm{Gal}(K_P/K)} \gamma\cdot\theta(\gamma^{-1}\sigma\gamma),$$

where γ is a fixed lift of $\bar{\gamma}$ to $\mathfrak{g}_K$. Since $E[P]$ is rational over K_P, there is a unique cocycle in each cohomology class, so that Nm is well-defined as an endomorphism of $H^1(K_P, E[P])$.

Lemma 15. *If* $\theta \in H^1(K_P, E[P])$, *then* $\operatorname{res}\circ\operatorname{cores}\theta = \mathrm{Nm}\,\theta$.

Proof. The lemma follows from the definition of cores on $H^0(K_P, E[P])$ and dimension shifting; see for example [Serre 1962, p. 119]. □

In the remainder of this section, we drop the subscript n.

Lemma 15 shows that $\operatorname{res}\circ\operatorname{cores}(\Phi(\pi, 1)) = \mathrm{Nm}(\Phi(\pi, 1))$. Unfortunately, Nm and Φ do not commute, as the Galois actions on $E[P]$ and $\mu_P \times \mu_P$ differ. The representation on $E[P]$ gives, with respect to our fixed basis, a homomorphism

$$\begin{aligned}\mathrm{Gal}(K_P/K) &\to \mathrm{GL}_2(\mathbb{Z}/P\mathbb{Z})\\ \sigma &\mapsto M_\sigma = \begin{pmatrix} i(\sigma) & j(\sigma)\\ k(\sigma) & \ell(\sigma)\end{pmatrix}.\end{aligned}$$

Then we have

Proposition 16. *Let $\sigma \in \mathrm{Gal}(K_P/K)$ and $(a, b) \in ({K_P}^\times/{K_P}^{\times P})^2$. Then*

$$\Phi(a,b)^\sigma = \Phi\Big(\frac{M_\sigma}{\det M_\sigma}(\sigma a, \sigma b)\Big),$$

where $M_\sigma(a, b)$ is given by the natural action of $\mathrm{GL}_2(\mathbb{Z}/P\mathbb{Z})$ on $({K_P}^\times/{K_P}^{\times P})^2$; that is, $M_\sigma(a,b) = (a^{i(\sigma)}b^{j(\sigma)}, a^{k(\sigma)}b^{\ell(\sigma)})$.

Proof. Our choice of basis for $E[P]$ gives rise to a group isomorphism

$$\rho\colon E[P] \to \mu_P \times \mu_P.$$

Define a $\mathbb{Z}[\mathrm{Gal}(K_P/K)]$-module $(\mu_P \times \mu_P)_\rho$ which, as a $\mathbb{Z}$-module, is $\mu_P \times \mu_P$, but which possesses a Galois structure making ρ into a $\mathrm{Gal}(K_P/K)$-equivariant map. In particular, if $(\zeta_1, \zeta_2) \in (\mu_P \times \mu_P)_\rho$ and $\sigma \in \mathrm{Gal}(K_P/K)$, we have

$$\rho \circ \sigma \circ \rho^{-1}(\zeta_1, \zeta_2) = \sigma(\zeta_1, \zeta_2) = M_\sigma(\zeta_1, \zeta_2).$$

On the other hand, for $(\zeta_1', \zeta_2') \in \mu_P \times \mu_P$ the Galois action is

$$\sigma(\zeta_1', \zeta_2') = \det M_\sigma \cdot (\zeta_1', \zeta_2'),$$

where the action on the right is the diagonal action of $\mathbb{Z}/P\mathbb{Z}$.

Let $i : \mu_P \times \mu_P \to (\mu_P \times \mu_P)_\rho$ be the canonical group isomorphism; it does not respect the $\mathrm{Gal}(K_P/K)$-action. If A is any $\mathfrak{g}_{K_P}$-module, write $H^1(A)$ for $H^1(K_P, A)$. Then i induces a map

$$i_* : H^1(\mu_P \times \mu_P) \to H^1((\mu_P \times \mu_P)_\rho).$$

Let M be either $(\mu_P \times \mu_P)_\rho$ or $\mu_P \times \mu_P$. Since in either case M is a trivial $\mathfrak{g}_{K_P}$-module, the set of coboundaries $B^1(K_P, M)$ is zero, and so $H^1(K_P, M) = Z^1(K_P, M)$, the set of 1-cocycles from $\mathfrak{g}_{K_P}$ to M. We can therefore identify cohomology classes with cocycles in both cases.

Consider the commutative diagram

$$\begin{tikzcd}({K_P}^\times/{K_P}^{\times P})^2 \arrow[r, "\psi"] \arrow[dr, "\psi_\rho"'] & H^1(\mu_P \times \mu_P) \arrow[d, "i_*"] & \\ & H^1((\mu_P \times \mu_P)_\rho) \arrow[r, "\lambda"'] & H^1(E[P])\end{tikzcd} \tag{11}$$

The horizontal maps are $\mathrm{Gal}(K_P/K)$-isomorphisms. The map λ is induced by $(i \circ \rho)^{-1}$, and ψ is the Kummer map. The diagonal map ψ_ρ is $\psi \circ i_*$. Thus, $\Phi = \lambda \circ \psi_\rho$. Note that $\mathfrak{g}_K$ acts on all of the groups in (11) through its quotient $\mathrm{Gal}(K_P/K)$. Let γ be an element of $\mathfrak{g}_{K_P}$ and σ an element of $\mathfrak{g}_K$. Then

$$\begin{aligned}
[\psi_\rho(a,b)]^\sigma(\gamma) &= [i_*\psi(a,b)]^\sigma(\gamma) \\
&= \sigma[i(\psi(a,b)(\sigma^{-1}\gamma\sigma))] \\
&= \sigma[i(\sigma^{-1}\sigma\,\psi(a,b)(\sigma^{-1}\gamma\sigma))] \\
&= \sigma[i(\sigma^{-1}\psi(\sigma a,\sigma b)(\gamma))] \\
&= M_\sigma[(i(\det M_\sigma^{-1}\cdot\psi(\sigma a,\sigma b)(\gamma))] \\
&= \frac{M_\sigma}{\det M_\sigma}[i(\psi(\sigma a,\sigma b)(\gamma))] \\
&= \frac{M_\sigma}{\det M_\sigma}\psi_\rho(\sigma a,\sigma b)(\gamma). \qquad (12)
\end{aligned}$$

Applying λ on both sides, we obtain the result. □

Corollary 17. *We have*

$$\mathrm{Nm}\,\Phi((a,b)) = \Phi\Big(\prod \frac{1}{\det M_\sigma}\left(\sigma a^{i(\sigma)}\sigma b^{j(\sigma)}, \sigma a^{k(\sigma)}\sigma b^{\ell(\sigma)}\right)\Big),$$

where the product extends over all $\sigma \in \mathrm{Gal}(K_P/K)$ and is taken component-wise.

Let $(c,d) = \Phi^{-1}\,\mathrm{Nm}\,\Phi(\pi,1)$ and $(c',d') = \Phi^{-1}\,\mathrm{Nm}\,\Phi(1,\pi')$.

Lemma 18. *Let v be the place of K_P corresponding to π. Either* $\mathrm{order}(\langle c,d\rangle_v) = P$ *or* $\mathrm{order}(\langle cc',dd'\rangle_v) = P$.

Proof. If $\mathrm{order}(\langle c,d\rangle) = P$, then we are done. So suppose that $\mathrm{order}(\langle c,d\rangle) < P$. In fact, since P is a prime power, the order strictly divides P.

Expanding out the Hilbert symbol, we get

$$\langle cc',dd'\rangle = \langle c,d\rangle + \langle c,d'\rangle + \langle c',d\rangle + \langle c',d'\rangle.$$

We have $\langle c',d\rangle_v = \langle c',d'\rangle_v = 0$ since all are v-adic units. By our assumption at the start of the proof, $\langle c,d\rangle_v$ has order strictly dividing P. That leaves $\langle c,d'\rangle_v$. By Corollary 17,

$$d' = \pi'\cdot\prod_{\sigma\neq 1}(\sigma\pi')^{e_\sigma}$$

for some integers e_σ. Our choice of π' implies that $\pi' \equiv \alpha \pmod{(\pi)}$, where α was chosen to have order P in $K_v^{\times P}$, while $\sigma\pi' \equiv 1 \pmod{(\pi)}$ for nontrivial σ (see (10)). Thus $d' \equiv \alpha \pmod{(\pi)}$. Therefore $K_v(d'^{1/P})/K$ is the unramified extension of degree P. (Equivalently, we may appeal to condition (SC4′).)

We now use similar reasoning as in the proof of Theorem 1 to see that $\langle \pi, d' \rangle_v$ has order P. Since $v(c) = 1$, the order of $\langle c, d' \rangle_v$ is exactly P. This shows $\langle cc', dd' \rangle_v$ has exact order P. □

If $\langle c, d \rangle$ has order P, let $\theta = \Phi(\pi, 1)$, so that $\xi = \operatorname{cores} \theta$ satisfies

$$\operatorname{res} \xi = \operatorname{Nm} \Phi(\pi, 1) = \Phi(c, d);$$

otherwise, let $\theta = \Phi(\pi, \pi')$, so that $\operatorname{res} \xi = \Phi(cc', dd')$. Let (a, b) denote whichever pair we've chosen, (c, d) or (cc', dd').

Let us now reintroduce subscripts, so that

$$\begin{aligned} \xi_n &= \operatorname{cores} \theta_n \\ &= \begin{cases} \operatorname{cores} \Phi(\pi_n, \pi_n') \text{ or} \\ \operatorname{cores} \Phi(\pi_n, 1) \end{cases} \\ (a_n, b_n) &= \Phi^{-1} \operatorname{res} \xi_n. \end{aligned}$$

Lemma 19. *Let $0 \le m < n$. Then $\Delta_P(\operatorname{res}(\xi_m - \xi_n))$ has order P at v_m.*

Proof. Write v for v_m. Since $E[P^*] \subset E(K_P)$, the obstruction map can be computed using the Hilbert symbol. Thus we wish to compute the order of

$$\left\langle \frac{a_m}{a_n}, \frac{b_m}{b_n} \right\rangle_v .$$

By the bilinearity of the Hilbert symbol, it suffices to compute

$$\langle a_m, b_m \rangle_v - \langle a_m, b_n \rangle_v - \langle a_n, b_m \rangle_v + \langle a_n, b_n \rangle_v .$$

By Lemma 18, the first term has order P. Since a_n, b_m and b_n are all units at v, the last two terms are zero. That leaves the term $\langle a_m, b_n \rangle_v$. By Corollary 17, b_n is a product of $\sigma\pi_n$ and $\sigma\pi_n'$. By condition (SC3′), these all lie in $K_v^{\times P}$. Therefore the second term is also zero. The Lemma follows. □

3.6. *Proof of Theorem 2: conclusion.* Let C be the curve represented by the class $\xi := \xi_i - \xi_j$ for some $i \neq j$. Clearly, $P(C) \mid P$. If we can show that $I(C) = P^2$, then by (1) we must have $P(C) = P$.

Since $E[P] \subset E(K_P)$ (and $E[2P] \subset E(K_P)$ when P is even), the obstruction map on $H^1(K_P, E[P])$ is given by the Hilbert symbol. In view of Lemma 19, $\Delta_P(\operatorname{res}_{K_P/K} \xi)$ has order P at v_i. Therefore $\Delta_P(\xi)$ has order P at the prime w satisfying $v_i \mid w$.

Suppose that C has index $P \cdot D$ for some $D \mid P$. Then there exists some $\eta \in H^1(K, E[PD])$ representing C such that $\Delta_{PD}(\eta) = 0$. Let j_D be the natural map $H^1(K, E[P]) \to H^1(K, E[PD])$. The classes η and $j_D(\xi)$ represent the same curve C, so there exists some $x \in E(K)$ such that $\eta = j_D(\xi) + \imath_{PD}(x)$. Since $\Delta_{PD}(\imath_{PD}(x)) = 0$, by the remarks at the start of Section 2.1,

$$\Delta_{PD}(\eta) = \Delta_{PD}(j_D(\xi)) + \mathrm{Li}(\eta, x).$$

Recall that $\mathrm{Li}(\eta, x)$ is the Tate pairing. Let us consider this equality locally, at w. The left-hand side is zero by hypothesis. By condition (SC2′), x lies in $P \cdot E(K_w)$. Since $P(C) \mid P$, the Tate pairing at w is trivial. Hence $\Delta_{PD}(j_D(\xi))$ must be zero at w. But by Proposition 6,

$$\Delta_{PD}(j_D(\xi)) = D\Delta_P(\xi).$$

We showed earlier that $\Delta_P(\xi)$ has order P at w. Therefore $D = P$, and so $I(C) = P^2$.

Let η_i be the image of ξ_i in $H^1(K, E)$. It remains to show that $\mathrm{res}_v\, \eta_i = 0$ for $v \in S_K$. Recall that $\eta_i = \mathrm{cores}\, \Phi(\pi_i, 1)$ or $\mathrm{cores}\, \Phi(\pi_i, \pi_i')$. For $w \mid v$ a place of K_P, the proof of Theorem 1 showed that the curves corresponding to $\Phi(\pi_i, 1)$ and $\Phi(\pi_i, \pi_i')$ were trivial at w. But the corestriction map induces a homomorphism

$$\oplus_{w|v} H^1((K_P)_w, E) \to H^1(K_v, E)$$

which proves that η_i is trivial at v. This completes the proof of Theorem 2.

3.7. ***Proof of Theorem 3.*** Recall the following two "classical" instances of period equals index.

(i) [Lang and Tate 1958] F is the completion of a global field at a place v, $E = \mathrm{Jac}(C)$ has good reduction, and v does not divide the period of C.

(ii) [Cassels 1963] F is global and $C \in Ш(F, E)$.

Note that Lichtenbaum showed that $P = I$ for all genus-one curves defined over the completion of a global field. However, the result of Lang and Tate, apart from being more elementary, is also more precise: they show also that a finite extension field F'/F splits a genus-one curve $C_{/K}$ if and only if the period P of C divides the relative ramification index $e(F'/F)$. This will be used in the proof.

Take S to be the union of the infinite places, the finite places which divide P and the places of bad reduction for E. Let $\{\eta_i\}_{i=0}^{\infty}$ be the sequence of classes constructed in Theorem 2. We will show that for any positive integer r, there exists a degree P field extension L/K such that the restrictions of $\eta_1, \ldots, \eta_r$ to L are pairwise distinct, locally trivial, and of period P.

Indeed, let $S_r = \bigcup_{i=1}^{r} \mathrm{supp}(\eta_i)$. We have $S_r \cap S = \varnothing$, so that each $v_i \in S_r$ is a finite place of good reduction for E and residue characteristic prime to P.

For each $v_i \in S_r$, let L_i/K_{v_i} be a totally ramified extension of degree P. There exists a degree P global extension $L = L(r)$ of K such that for all $v_i \in S_r$, $L \otimes_K$

$K_{v_i} \cong L_i$.[3] By the results (i) of Lang and Tate cited above, $\eta_i|_L$ is locally trivial. Moreover, since $\eta_i = \eta_i - \eta_0$ has index P^2 and L/K is a degree P extension, $I(\eta_i|_L) \geq P$. But on the other hand, by (ii) above, $I(\eta_i|_L) = P(\eta_i|_L) \mid P(\eta_i) = P$, so for all i, $1 \leq i \leq r$, $\eta_i|_L$ has period and index equal to P.

The only worry is that their restrictions are not distinct. But suppose that $\eta_i|_L = \eta_j|_L$. Then $\eta_i - \eta_j$ would lie in the kernel res_L. This would imply that $I(\eta_i - \eta_j) \mid P$, which we have arranged not to be the case.

3.8. ***Remarks about ramification.*** The proof of Theorem 3 differs from that of [Clark 2005, Theorem 1] in that we explicitly make use of extensions L/K that are ramified at many primes. Given our strategy of proof, this is unavoidable: using (i), the number of order P elements in $\mathrm{res}_L(H^1(K, E)) \cap \text{Ш}(L, E)$ can be bounded in terms of the number of ramified primes of L/K. It is interesting to ask whether this same boundedness result holds for order P elements in $\text{Ш}(L, E)$, and conversely, whether the number of order P elements of $\text{Ш}(L, E)$ necessarily approaches infinity with the number of ramified primes.

Both of these questions have affirmative answers when $P = 2$, according to work of Yu [2004]. Given a quadratic extension L/K, Yu computes the order of the kernel and cokernel of the natural map $\text{Ш}(K, E) \oplus \text{Ш}(K, E^\chi) \to \text{Ш}(L, E)$; here E^χ is the twist of $E_{/K}$ by the quadratic character χ of L/K. In particular, one can deduce Theorem 3 for $P = 2$ from Yu's work, with one caveat: his analysis is conditional on the finiteness of $\text{Ш}(K, E)$. That the existence of an infinite subgroup of $\text{Ш}(K, E)$ would hamper our ability to show that $\text{Ш}(L, E)[2]$ is large is somewhat curious, but seems to be the true state of affairs.

The consistency of Theorem 3 with the results of [Yu 2004] might thus be regarded as some confirmatory evidence for the finiteness of Shafarevich–Tate groups. How seriously such evidence ought to be taken is, of course, up to the reader to decide.

References

[Bölling 1975] R. Bölling, "Die Ordnung der Schafarewitsch–Tate–Gruppe kann beliebig groß werden", *Math. Nachr.* **67** (1975), 157–179. MR 52 #5684

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Math. **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Cassels 1962] J. W. S. Cassels, "Arithmetic on curves of genus 1, III: The Tate–Šafarevič and Selmer groups", *Proc. London Math. Soc.* (3) **12** (1962), 259–296. MR 29 #1212 Zbl 0106.03705

[Cassels 1963] J. W. S. Cassels, "Arithmetic on curves of genus 1, V: Two counterexamples", *J. London Math. Soc.* **38** (1963), 244–248. MR 26 #6171 Zbl 0113.03701

[Cassels 1964] J. W. S. Cassels, "Arithmetic on curves of genus 1, VI: The Tate–Šafarevič group can be arbitrarily large", *J. Reine Angew. Math.* **214/215** (1964), 65–70. MR 29 #104 Zbl 0236.14012

[3] This is a standard weak approximation/Krasner's Lemma argument [Clark 2005, p. 2].

[Ciperiani and Krashen 2007] M. Ciperiani and D. Krashen, “Relative Brauer groups of genus 1 curves”, preprint, 2007. arXiv math/0701614

[Clark 2005] P. L. Clark, “The period-index problem in WC-groups, I: Elliptic curves”, *J. Number Theory* **114**:1 (2005), 193–208. MR 2006f:11059 Zbl 1087.11036

[Clark 2006a] P. L. Clark, “Period-index problems in WC-groups, II: Abelian varieties”, preprint, 2006, Available at http://math.uga.edu/~pete/wc2.pdf.

[Clark 2006b] P. L. Clark, “There are genus one curves of every index over every number field”, *J. Reine Angew. Math.* **594** (2006), 201–206. MR 2007b:11080 Zbl 1097.14024

[Cremona et al. 2008] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, “Explicit n-descent on elliptic curves. I. Algebra”, *J. Reine Angew. Math.* **615** (2008), 121–155. MR 2009g: 11067

[Donnelly 2003] S. Donnelly,“Elements of given order in Tate-Shafarevich groups of elliptic curves”, 2003.

[Fisher 2001] T. Fisher, “Some examples of 5 and 7 descent for elliptic curves over **Q**”, *J. Eur. Math. Soc. (JEMS)* **3**:2 (2001), 169–201. MR 2002m:11045 Zbl 1007.11031

[Kloosterman 2005] R. Kloosterman, “The p-part of the Tate–Shafarevich groups of elliptic curves can be arbitrarily large”, *J. Théor. Nombres Bordeaux* **17**:3 (2005), 787–800. MR 2006k:11102 Zbl 1153.11313

[Kloosterman and Schaefer 2003] R. Kloosterman and E. F. Schaefer, “Selmer groups of elliptic curves that can be arbitrarily large”, *J. Number Theory* **99**:1 (2003), 148–163. MR 2003m:11081 Zbl 1074.11032

[Lang and Tate 1958] S. Lang and J. Tate, “Principal homogeneous spaces over abelian varieties”, *Amer. J. Math.* **80** (1958), 659–684. MR 21 #4960 Zbl 0097.36203

[Lichtenbaum 1968] S. Lichtenbaum, “The period-index problem for elliptic curves”, *Amer. J. Math.* **90** (1968), 1209–1223. MR 38 #5788 Zbl 0187.18602

[Lichtenbaum 1969] S. Lichtenbaum, “Duality theorems for curves over p-adic fields”, *Invent. Math.* **7** (1969), 120–136. MR 39 #4158 Zbl 0186.26402

[Matsuno 2007] K. Matsuno, “Construction of elliptic curves with large Iwasawa λ-invariants and large Tate–Shafarevich groups”, *Manuscripta Math.* **122**:3 (2007), 289–304. MR 2008h:11106 Zbl 1152.11045

[Milne 1972] J. S. Milne, “Addendum to ‘Weil–Châtelet groups over local fields’ (Ann. Sci. École Norm. Sup. (4) **3** (1970), 273–284)”, *Ann. Sci. École Norm. Sup.* (4) **5** (1972), 261–264. MR 48 #6121 Zbl 0241.14022

[Mumford 1966] D. Mumford, “On the equations defining abelian varieties. I”, *Invent. Math.* **1** (1966), 287–354. MR 34 #4269 Zbl 0219.14024

[Olson 1970] L. D. Olson, “Galois cohomology of cycles and applications to elliptic curves”, *Amer. J. Math.* **92** (1970), 75–85. MR 41 #8421 Zbl 0197.17301

[O’Neil 2002] C. O’Neil, “The period-index obstruction for elliptic curves”, *J. Number Theory* **95**:2 (2002), 329–339. MR 2003f:11079 Zbl 1033.11029

[Serre 1962] J.-P. Serre, *Corps locaux*, Actualités Sci. Indust. **1296**, Hermann, Paris, 1962. MR 27 #133 Zbl 0137.02601

[Sharif 2006] S. Sharif, *Construction of curves with prescribed period and index*, Ph.D. thesis, University of California, Berkeley, 2006.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Tate 1958] J. Tate, “WC-groups over $\mathfrak{p}$-adic fields”, Séminaire Bourbaki 1957/1958 (Exposé 156) **13**, Secrétariat mathématique, Paris, 1958. Reprinted as pp. 265–277 in *Séminaire Bourbaki* **4**, Soc. Math. France, Paris, 1995. MR 21 #4162

[Yu 2004] H. Yu, “On Tate–Shafarevich groups over Galois extensions”, *Israel J. Math.* **141** (2004), 211–220. MR 2005d:14034 Zbl 1071.11033

[Zarhin 1974] J. G. Zarhin, “Noncommutative cohomology and Mumford groups”, *Mat. Zametki* **15** (1974), 415–419. MR 50 #7090

Communicated by Karl Rubin
Received 2009-01-15 Revised 2009-11-12 Accepted 2009-11-16

pete@math.uga.edu
*University of Georgia, Department of Mathematics,
Athens, GA 30602, United States*
http://www.math.uga.edu/~pete/

sharif@math.duke.edu
*Department of Mathematics, Duke University,
Durham, NC 27708, United States*
http://www.math.duke.edu/~sharif