The Period-Index Obstruction for Elliptic Curves

Catherine O’Neil

Massachusetts Institute of Technology, Cambridge, Massachusetts 02139
E-mail: coneil@math.mit.edu

Communicated by H. Darmon

Received July 9, 2001; revised September 12, 2001

1. INTRODUCTION

Let $K$ be a field and let $E$ be an elliptic curve over $K$. Let $G_K$ be the absolute Galois group of $K$. The elements of the group $H^1(G_K, E)$ are in one-to-one correspondence with isomorphism classes of principal homogeneous spaces $C$ of $E$. The period of such a $C$ is its order in $H^1(G_K, E)$, a torsion group. The index of such a $C$ is the smallest positive integer $d$ such that there is a $K$-rational line bundle of degree $d$ on $C$. The period-index problem is to determine when these invariants are equal. We denote the period of $C$ by $n$ and the index by $d$; then Lang and Tate [4] showed that $n$ divides $d$ and that $d$ and $n$ have the same prime factors. If $K$ is a local field, Lichtenbaum [5] showed that $d = n$. If $E$ is defined over $\mathbb{Q}$ and its analytic rank is 0, Stein [12] showed that for infinitely many integers $n$ that there exist homogeneous spaces $C$ with $n(C) = d(C) = n$. There are also examples where $n \neq d$ (see [1, 4, 5]). Finally, Cassels originally showed [1] that elements $C$ of Sha have $n(C) = d(C)$. In fact, we give another easy proof of this below.

In this paper we will first examine the special case when the elliptic curve $E$ is defined over a large enough field $K$ so that the points of $E[n](\bar{K})$ are all defined over $K$. We will relate the period-index obstruction map on such elliptic curves to the Hilbert symbol. We will then derive Hilbert symbol-like properties of this obstruction map in the general case. In particular, we show that the obstruction map is quadratic.

2. THE PERIOD-INDEX OBSTRUCTION

Throughout this paper, $E$ will denote an elliptic curve over the field $K$, $\bar{K}$ its separable closure, and $G_K$ the Galois group $Gal(\bar{K}/K)$. The notation $[P]$ is...
to be understood as $\mathbb{P}^j_K$, and similarly other group schemes will be presumed defined over $K$ unless otherwise noted.

**Proposition 2.1.** Let $n \geq 2$ be an integer prime to the characteristic of $K$. We have the following commutative diagram of group schemes:

$$
\begin{array}{cccccc}
0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{G}_n & \longrightarrow & E[n] & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & GL_n & \longrightarrow & PGL_n & \longrightarrow & 0
\end{array}
$$

where the upper row is a theta group as defined in [6, p. 221].

**Proof.** We first review some of the theory of theta groups (see [6]). Let $X$ be an abelian variety and $L \to X$ a line bundle over $X$. Mumford defines [6, p. 224] an “automorphism” of the pair $(X, L)$ to be a commutative diagram

$$
\begin{array}{ccc}
L & \longrightarrow & L \\
\downarrow & & \downarrow \\
X & \stackrel{\sigma}{\longrightarrow} & X
\end{array}
$$

where $\sigma$ is fixed-point free. Define the functors $F, F', F''$ which for a scheme $S$ have $F(S) = H^0(S, \mathcal{O}_S^*)$, $F''(S) = \text{Aut}(L/X)(S)$ and $F'(S) = \{f : S \to X|T_f^*(S \times L) \cong S \times L\}$. Here $T_f$ is the “translation by $f$” map (see [6, p. 226]). There are natural transformations $F \to F''$ and $F'' \to F'$. Theorem 1 of [6, p. 225] states that the short exact sequence of functors

$$1 \to F \to F'' \to F' \to 1$$

is representable by the following short exact sequence of group schemes:

$$1 \to \mathbb{G}_m \to G(L) \to \mathcal{K}(L) \to 1.$$
which makes the following diagram commute:

\[
\begin{array}{ccc}
E & \longrightarrow & \mathbb{P}^{n-1} \\
\downarrow & & \downarrow \\
E & \longrightarrow & \mathbb{P}^{n-1}
\end{array}
\]

Next, the group scheme \( \mathcal{X}(L) \) is \( E[n] \). Theorem 3 of [6, p. 231] implies that \( E[n] \) is a subgroup scheme of \( \mathcal{X}(L) \), which is in turn a subgroup scheme of \( E \). Moreover, degree considerations imply that \( \mathcal{X}(L) = E[n] \). We have shown \( E[n] = \text{Aut}(E \to \mathbb{P}^{n-1}) \).

The map from the theta group exact sequence to the lower exact sequence in Proposition 2.1 is the forgetful map once we have chosen a basis of global sections of \( L = \mathcal{O}(n \cdot O_E) \). Indeed, an automorphism on the diagram \( L \to E \) acts in particular on this basis and gives us an element of \( GL_n \). Similarly, an automorphism of the diagram \( E \to \mathbb{P}^{n-1} \) acts in particular on \( \mathbb{P}^{n-1} \), giving an element of \( PGL_n \).

**Proposition 2.2.** \( H^1(G_K, E[n]) \) parameterizes diagrams \( C \to S \) up to \( K \)-isomorphism, where \( C \) is a principal homogeneous space for \( E \) and \( S \) is a twist of \( \mathbb{P}^{n-1} \).

**Proof.** This argument is similar to [10, p. 160] which displays \( H^1(G_K, PGL_n(\bar{K})) \) as parameterizing Brauer–Severi varieties (up to \( K \)-isomorphism). There Serre reduces to showing the following. Let \( L \) be a Galois field extension of \( K \) sufficiently large so that \( C(L) \) is not empty. Then we have \( f : C \times L \cong E \times L \), where \( f \) is defined over \( L \), and which extends to a diagram

\[
\begin{array}{ccc}
C \times L & \longrightarrow & S \times L \\
\downarrow & & \downarrow \\
E \times L & \longrightarrow & \mathbb{P}^{n-1}
\end{array}
\]

For \( \sigma \in G(L/K) \), the map \( \sigma(f) \cdot f^{-1} \) is an element of \( \text{Aut}(E \to \mathbb{P}^{n-1})(L) \), in other words \( \sigma \mapsto \sigma(f) \cdot f^{-1} \) is a cocycle in \( H^1(Gal(L/K), E[n](L)) \).

The natural surjective map \( H^1(K, E[n]\langle \bar{K} \rangle) \to H^1(K, E(\bar{K}))|n \) can now be thought of as another forgetful map, this time forgetting the \( \mathbb{P}^{n-1} \). The surjectivity implies that if \( C \) has period dividing \( n \) there exists a diagram \( C \to S \); moreover, if \( C \) has index dividing \( n \), then \( C \) has a line bundle of degree \( n \), which, by taking a basis of global sections, gives a diagram \( C \to \mathbb{P}^{n-1} \). There may exist many diagrams involving \( C \), and the period-index problem for \( C \) is thus translated to the following: is there a lift of \( C \) to
a diagram $C \to S$ where $S \cong \mathbb{P}^{n-1}$. To answer this we will define the “period-index obstruction”, $Ob$, to take values on diagrams $C \to S$, that is on elements of the cohomology group $H^1(G,E[n])$.

**Proposition 2.3.** The period-index obstruction $Ob$ takes values in the Brauer group of $K$, denoted by $Br(K)$, and is given by the following commutative diagram:

$$
\begin{array}{ccc}
H^1(G_K,E[n](\overline{K})) & \longrightarrow & H^1(G_K,PGL_n(\overline{K})) \\
Ob \downarrow & & \downarrow \Delta \\
H^2(G_K,\mathbb{G}_m(\overline{K})) & \longrightarrow & H^2(G_K,\mathbb{G}_m(\overline{K})) = Br(K)
\end{array}
$$

where we use the notation $\Delta$ from [10, p. 124] to distinguish it as a map in nonabelian cohomology.

**Proof.** This results directly from the long exact sequences of cohomology of the Proposition 2.1, and from the theory of Brauer–Severi varieties (see [10, p. 160]).

**Remark.** When $K$ is a global field, the above correspondence gives an easy proof that the elements of the Tate–Shafarevich group of $E$ have trivial period-index obstruction; namely, base changing the diagram $C \to S$ to a local field gives by assumption a point on $C$ and thus a point on $S$. Brauer–Severi varieties satisfy the Hasse Principle, so $S$ is actually projective space over the global field. Note that this proof does not depend on the lift of an element of Sha to $H^1(G_K,E[n])$; therefore all elements of the Selmer group have trivial obstruction. As we shall see, this means we have a linear space (a subgroup) inside the kernel of a quadratic map.

**Proposition 2.4.** Let $C$ be a homogeneous space of $E$ with (exact) period $n$. The element $Ob(C \to S)$ is in the $n$-torsion of the Brauer group of $K$, and if the order of $Ob(C \to S)$ as an element of $Br(K)$ is $l$, then $d \leq ln$. In particular, we always have $d \leq n^2$.

**Proof.** The order $l$ of $Ob(C \to S)$ is the order of $\Delta(S)$, and by the theory of Brauer–Severi varieties there is a field extension $L$ of $K$ of degree $l$ which splits $S$, i.e. so $\mathbb{P}^{n-1}_L \cong S \times_K L$. Then over $L$, $C$ has a degree $n$ line bundle. We can then produce a degree $nl$ line bundle on $C$ over $K$, namely by taking the tensor product of all $l$ of the $Mor(L,\overline{K})$-conjugates of the one over $L$.

**Question.** Proposition 2.4 gives us an upper bound for the period $d$ of $C$. Is this an equality? In other words, if $d = ln$ for some $l$, can we descend the
degree \( l \)n line bundle on \( C \) to a degree \( n \) line bundle, defined over a field \( L \) of degree \( l \) over \( K \).

3. THE CASE OF FULL LEVEL \( n \)-STRUCTURE

Now assume all the elements of \( E[n](\bar{K}) \) are defined over \( K \). Fix a primitive \( n \)th root of unity \( \zeta \in K \) and let

\[
e : E[n] \times E[n] \to \mu_n,
\]
de note the level \( n \) Weil pairing. Fix a basis \( S, T \) for \( E[n]/C_1 \) such that

\[
e(S, T) = \zeta.
\]

**Lemma 3.1.**

\[
H^1(G_K, E[n](\bar{K})) \cong K^*/K^{*n} \times K^*/K^{*n}.
\]

**Proof.** For any point \( P \in E[n](K) \), define \( \xi_P \in H^1(G_K, \mu_n(\bar{K})) \) as the cocycle \( \sigma \mapsto e(\xi(\sigma), P) \). Define the map \( H^1(G_K, E[n](\bar{K})) \to H^1(G_K, \mu_n(\bar{K})) \times H^1(G_K, \mu_n(\bar{K})) \) by sending a cocycle \( \xi \) to the pair \( (\xi_S, \xi_T) \), and then identify \( H^1(G_K, \mu_n(\bar{K})) \) with \( K^*/K^{*n} \) via Hilbert’s Theorem 90 (namely, a cocycle \( \phi \in H^1(G, \mu_n) \) maps to \( r^n \) if \( \phi(\sigma) = \sigma(r)/r \) for all \( \sigma \in G_K \)).

Denote the commutator of two elements \( x, y \) as \( [x, y] = x y x^{-1} y^{-1} \).

**Lemma 3.2.** The Weil pairing \( e \) can be computed as follows: for \( P \in E[n](K) \), denote by \( M_P \) a lift of the image of \( P \) under the map \( E[n] \to PGL_n \) from the diagram in Proposition 2.1. Then

\[
e(P_1, P_2) \cdot I = [M_{P_1}, M_{P_2}],
\]

where \( I \) is the \( n \times n \) identity matrix.

**Proof.** See Theorem 2.5 of [7, p. 6].

We conclude that a cocycle \( \xi \) corresponding to the pair \( (a, b) \) has

\[
[M_{\xi(\sigma)}, M_S] = \sigma(\alpha)/\alpha \quad \& \quad [M_{\xi(\sigma)}, M_T] = \sigma(\beta)/\beta
\]

for all \( \sigma \in G \), where \( \tilde{\xi}(\sigma) \) is a lift of \( \xi(\sigma) \) to \( GL_n(K) \), and where \( \alpha^n = a \) and \( \beta^n = b \).
**Lemma 3.3.** The following diagram commutes:

\[
\begin{array}{ccc}
H^1(G_K, E[n](\mathbb{K})) & \xrightarrow{=} & H^1(G_K, \mu_n(\mathbb{K})) \\
\downarrow & & \downarrow \cup \\
H^1(G_K, \text{PGL}_n(\mathbb{K})) & & H^2(G_K, \mu_n(\mathbb{K}) \otimes \mu_n(\mathbb{K})) \\
\text{Br}(\mathbb{K}) = H^2(G_K, \mathcal{G}_m(\mathbb{K})) & \xleftarrow{=} & H^2(G_K, \mu_n(\mathbb{K}))
\end{array}
\]

where the left column is the \(\text{Ob}\) map and the map

\[
H^2(G_K, \mu_n(\mathbb{K}) \otimes \mu_n(\mathbb{K})) \to H^2(G_K, \mu_n(\mathbb{K}))
\]

is induced from the map \(\mu_n(\mathbb{K}) \otimes \mu_n(\mathbb{K}) \to \mu_n(\mathbb{K})\) sending \(\zeta^a \otimes \zeta^b\) to \(\zeta^{ab}\).

**Proof.** Since all the elements of \(E[n](\mathbb{K})\) are defined over \(K\), a cocycle \(\xi \in H^1(G_K, E[n](\mathbb{K}))\) is a homomorphism from \(G_K\) to \(E[n](\mathbb{K})\). Define, for \(\sigma \in G_K\), \(\xi(\sigma) = a(\sigma)S + b(\sigma)T\), where both \(a\) and \(b\) are homomorphisms from \(G_K\) to \(\mathbb{Z}/n\mathbb{Z}\).

The map \(\text{Ob}\) takes a 1-cocycle \(\xi\) to the 2-cocycle

\[
(\sigma, \tau) \mapsto \text{Ob}(\xi)(\sigma, \tau) = \Delta(M_\xi)(\sigma, \tau) = M_\xi^{a(\sigma)}M_\xi^{b(\sigma)}M_\xi^{-1}.
\]

We may choose any lifting of elements of \(E[n](\mathbb{K})\) to \(GL_n(\mathbb{K})\) for this, and we will assume that \(M_{aS+bT} = M_S^a M_T^b\). Then we can write

\[
\text{Ob}(\xi)(\sigma, \tau) = M_S^{a(\sigma)}M_T^{b(\sigma)}[M_S^{a(\tau)}M_T^{b(\tau)}]^{-1} = M_S^{a(\sigma)}M_T^{b(\sigma)}[M_S^{a(\tau)+\sigma}M_T^{b(\tau)+b(\sigma)}]^{-1} = M_S^{a(\sigma)}M_T^{b(\sigma)}M_S^{a(\tau)}M_T^{b(\sigma)} = \xi^{-a(\sigma)-a(\tau)}.
\]

by Lemma 3.2 and because we have fixed \(e(S, T) = \xi\).

The map on the right first takes \(\xi\) to \((\xi_S, \xi_T)\) (see p. 4 for the definition) and then takes the cup product of the pair, which in the above notation can be rewritten as

\[
e(a(\sigma)S + b(\sigma)T, S) \otimes e(a(\tau)S + b(\tau)T, S)^{\sigma} = \xi^{-b(\sigma)} \otimes \xi^{a(\tau)}.
\]

Finally, we compose with the final map to get \((\sigma, \tau) \mapsto \xi^{-b(\sigma)} a(\tau)\).

On p. 206 of [10], Serre defines a "symbol" \((a, b)\) which takes values in the Brauer group of \(K\) and factors through \(K^*/K^*n \times K^*/K^*n\). It is a natural
generalization of the Hilbert symbol (see [9, p. 19]) and so we will refer to it as a Hilbert symbol and denote it by \((a, b)_{\text{Hilb}}\) to distinguish from the ordered pair \((a, b)\).

**Proposition 3.4.** The period-index obstruction for the diagram \(C \rightarrow S\) corresponding to the pair \((a, b) \in K^*/K^{*n} \times K^*/K^{*n}\) as above is given by the Hilbert symbol \((a, b)_{\text{Hilb}}\); symbolically, \(\text{Ob}(a, b) = (a, b)_{\text{Hilb}}\).

**Proof.** This results from Lemma 3.3 and Proposition 5 of [10, p. 207].

**Remark.** The Hilbert symbol depends on the choice of \(n\)th root of unity \(\zeta\) which is the Weil pairing of \(S\) and \(T\); a different choice of basis for \(E[n]\) would also change the Hilbert symbol.

**Corollary 3.5.** If we restrict to the curves of the form \((1, a)\), we get a subgroup of \(H^1(G_K, E[n](\bar{K}))\) all of whose elements have trivial period-index obstruction (hence there exist “addition formulas” for such curves).

**Proof.** The symbol \((1, a)_{\text{Hilb}}\) is trivial.

**Remark.** (1) When \(K\) is a number field large enough so that \(E[n](\bar{K}) = E[n](K)\), the above theorem demonstrates the existence of an infinite number of curves \(C\) with trivial and nontrivial period-index obstruction. (2) We can start with different line bundles on \(E\) to produce different correspondences between \(H^1(G_K, E[n](\bar{K}))\) and \(\{C \rightarrow S\}\); two such line bundles will differ by a degree 0 line bundle on \(E\) which can be identified with a point of \(E(K)\). The correspondences then will be translates of each other by the image of that point under the natural map \(E(K) \rightarrow H^1(G_K, E[n](\bar{K}))\). This “shift” will be seen below (Section 5) to define the Tate pairing in the case where \(K\) is a local field.

A nontrivial characteristic of the Hilbert symbol is that \((t, 1 - t)_{\text{Hilb}} = 1\) whenever \(t(t - 1) \neq 0\). For any \(E\) with full \(n\)-torsion as above then we have a \(\mathbb{P}^1_K\) of examples of homogeneous spaces of \(E\) embeddable in \(\mathbb{P}^{n-1}\). In other words, we have a sampling surface, isomorphic to \(\mathbb{P}^1 \times X(n)\), of such curves.

**Proposition 3.6.** For \(n = 3\) the family \(C_{(t, 1 - t)}\) is given by

\[
(3t(1 - \zeta_3) + \lambda(1 - t))(t^2 X^3 + t Y^3 + Z^3) + 9t(2\zeta_3 + 1)(tX^2 Z + t Y^2 X + Z^2 Y) + 9t(t^2 + 1)(tX^2 Y + Y^2 Z + Z^2 X) + 3t(6t(1 - \zeta_3) - \lambda(1 - t))XYZ = 0,
\]

where the Jacobian of \(X(3)\) is given by \(\delta(3): X^3 + Y^3 + Z^3 + \lambda XYZ = 0\).
4. THE GENERAL CASE

The goal of this section is to prove that the period-index map $Ob$ is quadratic, so it is in a sense “generalised Hilbert symbol”:

**Proposition 4.1.** $Ob$ is quadratic as a function on the $\mathbb{Z}$-module $H^1(G_K, E[n](\bar{K}))$.

**Proof.** By Definition 1 on p. 27 of [9], $Ob$ is quadratic if $Ob(ax) = a^2 Ob(x)$ for $a \in \mathbb{Z}$ and for $\xi \in H^1(G_K, E[n](\bar{K}))$ and if the associated function $B_{Ob}$ (defined below) is bilinear. These two facts will follow from Lemmas 4.2 and 4.4.

**Lemma 4.2.** Denote by $\xi$ the cocycle (class) representing the diagram $C \to S$ in $H^1(G_K, E[n])$. Let $a$ be an integer. Then $Ob(ax) = a^2 Ob(x)$.

**Proof.** We will use an alternative definition of the $Ob$ map; see the definition of $\psi_1$ on p. 1212 of [5]. Namely, a diagram $C \to S$ corresponds to a pair $(C, D)$ where $C$ is the same genus one curve and where $D$ is a degree $n$ $\bar{K}$-rational divisor on $C$ whose class is $G$-invariant, in other words, for all $\sigma \in G$, $D \sim D^\sigma$. For every $\sigma$, fix a function $f_\sigma \in K(C)$ such that $\text{div}(f_\sigma) = D - D^\sigma$. Then the cocycle in $Br(K)$ representing $(C, D)$ is

$$Ob(\xi)(\sigma, \tau) = \frac{f_\sigma f_\tau^\sigma}{f_{\tau^\sigma}}.$$  

There is a natural map $\varphi_a$ from $C$ to $aC$. One way to visualize $\varphi_a$ is to identify $C$ with $\text{Pic}^1(C)$ and $aC$ with $\text{Pic}^a(C)$ (via the Riemann–Roch Theorem) and then $\varphi_a$ is given by sending a geometric point $x$ to the point $ax$. Then $\varphi_a$ is of degree $a^2$, since over $\bar{K}$ these schemes are elliptic curves and the map is essentially multiplication by $a$. Moreover, $\varphi_a$ induces “multiplication by $a$” on the level of cocycles. Let $x_0 \in C(\bar{K})$ be a basepoint of $C$; then since $(a\xi)(\sigma) = a(x_0^\sigma - x_0) = ax_0^\sigma - ax_0 = \phi(x_0)^\sigma - \phi(x_0) = \phi^a(\xi)(\sigma)$. Finally, $\varphi_a$ induces an injection of function fields $K(aC) \subset K(C)$, of relative degree $a^2$. The norm map $N$ goes the other way, and brings the functions $f_\sigma$ to functions on $aC$ which have the property that $\text{div}(N(f_\sigma)) = a(D^\sigma - D)$. Then $Ob(ax)$ is represented by the cocycle

$1$Over $\bar{K}$, the class of $D$ gives rise to the line bundle $\mathcal{L}(D)$ which in turn induces the diagram $C_k \to P_{\bar{K}}^{a-1}$. Since $|D|$ is $G$-invariant, this diagram descends to $K$ as $C \to S$; $S$ will be isomorphic to $P^{a-1}$ over $K$ exactly when $|D|$ is representable by a $K$-rational divisor.
\[
Ob(a\tilde{\zeta})(\sigma, \tau) = \frac{N(f_\sigma)N(f_\tau^\sigma)}{N(f_{\sigma\tau})} = N\left(\frac{f_\sigma f_\tau^\sigma}{f_{\sigma\tau}}\right).
\]

Since \(\frac{f_\sigma f_\tau^\sigma}{f_{\sigma\tau}} \in K\), we have

\[
Ob(a\tilde{\zeta})(\sigma, \tau) = \left(\frac{f_\sigma f_\tau^\sigma}{f_{\sigma\tau}}\right)^{\deg(K(aC)/K(C))} = a^2 Ob(\tilde{\zeta})(\sigma, \tau).
\]

Let \(G\) be a group. Given a central extension of \(G\) modules:

\[
0 \to A \to B \to C \to 0,
\]

where \(C\) is abelian, we have two maps from \(H^1(G, C) \times H^1(G, C) \to H^2(G, A)\). The first, \(B_D\), takes \((\tilde{\xi}, \tilde{\psi})\) to \(\Delta(\tilde{\xi} + \tilde{\psi}) - \Delta(\tilde{\xi}) - \Delta(\tilde{\psi})\), where \(\Delta\) is the map of nonabelian cohomology (see [10, p. 123]). The second is induced from the natural pairing of elements of \(C\) given by \(\langle c_1, c_2 \rangle = [\tilde{c}_1, \tilde{c}_2]\), where \(\tilde{c}_i\) is a lift of \(c_i\) to \(B\). Namely,

\[
H^1(G, C) \xrightarrow{\text{diag}} H^1(G, C) \times H^1(G, C) \xrightarrow{\cup} H^2(G, C \otimes C) \xrightarrow{\langle \cdot, \cdot \rangle^*} H^2(G, A).
\]

**Proposition 4.3.** \(B_D = \langle \cdot, \cdot \rangle^* \circ \cup\).

**Proof.** See [14, p. 242].

In our situation we have

\[
0 \to \mu_\eta(\bar{K}) \to \mathcal{H} \to E[n](\bar{K}) \to 0,
\]

where \(\mathcal{H}\) is the Heisenberg group of dimension \(n\) (for more about the Heisenberg group, see [3, p. 11]). We can obtain the above exact sequence from Proposition 2.1 by intersecting the image of the theta-group \(\mathcal{G}_n\) with \(SL_n\). Then by Lemma 3.2, \(\langle \cdot, \cdot \rangle\) is the Weil pairing \(e\) and by Proposition 2.3, \(\Delta\) is the period-index obstruction map \(Ob\).

**Lemma 4.4.** \(B_{Ob}\) is bilinear.

**Proof.** This follows from Proposition 4.3, since both the cup product and the pairing are evidently bilinear. Note they are also both anti-commutative, but their composition is not.
5. RELATIONSHIP WITH THE TATE PAIRING

Let K be a local field. Then there exists a perfect pairing, called the Tate pairing, as follows:

\[ \langle \cdot, \cdot \rangle_T : E(K)/nE(K) \times H^1(G_K, E)[n] \rightarrow Br(K). \]

In [5], it was shown that we can represent the Tate pairing in terms of Ob as follows: to compute \( \langle P, C \rangle_T \), choose any lift \( \tilde{C} \) of \( C \) to the group \( H^1(G_K, E[n](\bar{K})) \) and identify \( P \) with its image in that group via the \( \delta \) map of cohomology. Then \( \langle P, C \rangle_T = Ob(\tilde{C} + P) - Ob(\tilde{C}) \). Moreover, since \( Ob \) vanishes on the Selmer group, and in particular \( Ob(P) = 1 \), we can rewrite the above as \( \langle P, C \rangle_T = B_{Ob}(P, \tilde{C}) \). In this notation the proof of the equality of the period and index over a local field can be reproduced from [5] as follows: Let \( C \) be a homogeneous space of \( E \) with period \( n \). The Brauer group of a local field is \( \mathbb{Q}/\mathbb{Z} \), and the \( n \)-torsion is \( \frac{1}{n} \mathbb{Z}/\mathbb{Z} \). By the nondegeneracy of the Tate pairing, there exists \( P \in E(K) \) so that \( \langle P, C \rangle = \frac{1}{n} \), the image of \( \langle - , C \rangle \) is a cyclic subgroup, say generated by \( \frac{1}{a} \) for \( a \) dividing \( n \). For all \( P \in E(K) \), \( a \cdot \langle P, C \rangle = 0 = \langle P, aC \rangle \), so \( aC = 0 \), but since \( C \) has period \( n \) we conclude that \( a = n \). Next, choose an arbitrary lift \( \tilde{C} \) of \( C \) to \( H^1(G_K, E[n](\bar{K})) \), and say \( Ob(\tilde{C}) = -\frac{b}{n} \). Then we need only find a \( Q \in E(K) \) so that \( \langle Q, C \rangle = \frac{b}{n} \), since \( Ob(Q + \tilde{C}) = Ob(\tilde{C}) + \langle Q, C \rangle \). Take \( Q = b \cdot P \).

ACKNOWLEDGMENTS

The author thanks Jordan Ellenberg for the correct statement of Proposition 4.3.

REFERENCES

8. C. O’Neil, Explicit descent over $X(3)$ and $X(5)$, preprint 328 on the Algebraic Number Theory Preprint Archives.
12. W. A. Stein, There are genus one curves over $\mathbb{Q}$ of every odd index, *J. Reine Angew. Math.* 547 (2002), 139–147.