THE PERIOD-INDEX OBSTRUCTION FOR ELLIPTIC CURVES

CATHERINE O'NEIL

1. Introduction

Let K be a field and let E be an elliptic curve over K. Let G be the absolute Galois group of K. The elements of the group $H^1(G, E)$ 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 $H^1(G, E)$, 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] that n divides d and that d divides the square of n. If K is a local field, Lichtenbaum [5] showed that $d = n$. If the analytic rank of an elliptic curve E is 0, Stein [11] showed that for infinitely many integers n that there exist homogeneous spaces C with $n(C) = d(C) = n$. If the elliptic curve E has a rational n torsion point, Lang and Tate [4] showed that there are infinitely many homogeneous spaces C with $n(C) = d(C) = n$. There are also examples where $n \neq d$ (see [4], [1], [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 E has full n torsion and relate the period-index obstruction map 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.

The author wishes to thank Jordan Ellenberg for the correct statement of Claim 4.1.

2. The Period-Index Obstruction

Let the notation be as above. If the index of a curve C is d, there is a map of C to $\mathbb{P}_K^{d-1}$, namely by taking a full set of sections of the line bundle of degree d. Assume the period n of C is prime to the characteristic of K. Define $\mathcal{L}_E$ to be the line bundle on E associated to the degree n divisor $n \cdot O_E$. Then $\mathcal{L}_E$ gives rise to a map (again by a full set of sections) to $\mathbb{P}_K^{n-1}$ which will be an embedding when n is at least 3.

Claim 2.1. *The automorphism group of the diagram $E \to \mathbb{P}_K^{n-1}$ which acts fixed-point free on E is $E[n]$.*

Date: April 20, 2001.

Proof. Left to the reader. □

Remark. The above claim induces a map of group schemes

$$r : E[n] \to \mathrm{PGL}_n = Aut(\mathbb{P}^{n-1}).$$

By general theory (see [4]) the group $H^1(G, E[n])$ parameterizes twists of the above diagram, i.e. diagrams $C \to S$, where C is a principal homogeneous space of E and S is a twist of $\mathbb{P}^{n-1}$. The natural (surjective) map to $H^1(G, E)[n]$ can thus be thought of as a forgetful map using the above, and we see that if C has period n there exists a diagram $C \to S$. 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 is the trivial twist? The obstruction to such a lift is given by another forgetful map ("Ob"), this time on the other side of the diagram: namely, the map $H^1(G, E[n]) \to H^1(G, \mathrm{PGL}_n)$ induced by r above, where $H^1(G, \mathrm{PGL}_n)$ parameterizes Brauer-Severi varieties (twists of $\mathbb{P}^{n-1}$). Moreover, this cohomology group injects via the Δ map of nonabelian cohomology into the n torsion of the Brauer group of K. Altogether we see that the obstruction to the period-index problem lies in $Br(K)$.

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. Then S is actually projective space over that local field. Finally, 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 $H^1(G, E[n])$; therefore all elements of the Selmer group have trivial obstruction. This means we have a linear space (a subgroup) inside the kernel of a quadratic map.

3. When $E[n]$ is rational

Now assume $E[n]$ is totally rational. Fix a primitive nth root of unity $\zeta_n \in K$ and let e denote the level n Weil pairing on E. Choose a basis S, T for $E[n]$ such that $e(S, T) = \zeta_n$. In this case we have

$$H^1(G, E[n]) \cong K^*/K^{*n} \times K^*/K^{*n}$$

first by mapping to $H^1(G, \mu_n) \times H^1(G, \mu_n)$ by sending a cocycle ξ to the pair $(e(\xi, T), e(\xi, S))$, and then by identifying $H^1(G, \mu_n)$ with K^*/K^{*n} via Hilbert's Theorem 90 (namely, a cocycle $\varphi \in H^1(G, \mu_n)$ maps to r if $\varphi(\sigma) = \sigma(r)/r$. Denote the commutator of two elements x, y as $[x, y] = xyx^{-1}y^{-1}$.

Claim 3.1. *The Weil pairing e can be computed using the map r as follows:*

$$e(P_1, P_2) = [M_{P_1}, M_{P_2}],$$

where M_{P_1} and M_{P_2} are lifts to GL_n of $r(P_1)$ and $r(P_2)$ respectively.

Proof. See Theorem 2.5 on page 6 of [6]. □

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

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

for all $\sigma \in G$, where $\overline{\xi}(\sigma)$ is a lift of $\xi(\sigma)$ to $\mathrm{GL}_n(K)$, and where $\alpha^n = a$ and $\beta^n = b$. In such a situation we have the following:

Theorem 3.1. *The period-index obstruction for the diagram $C \to S$ corresponding to the the pair $(a, b) \in K^*/K^{*n} \times K^*/K^{*n}$ is given by the Hilbert symbol $(a, b)_{Hilb}$ defined in* [9]*; symbolically, $Ob\,(a, b) = (a, b)_{Hilb}$.*

Proof. Define the K-algebra $A_{k,l}$ to be generated by elements $x_{k,l}, y_{k,l}$ such that $x^n_{k,l} = k$, $y^n_{k,l} = l$, and $x_{k,l}y_{k,l}x^{-1}_{k,l} = \zeta_n y_{k,l}$. By exercise 28 on page 139 of [2], $A_{k,l}$ is the algebra in $Br(K)$ corresponding to $(k, l)_{Hilb}$. An identification of such algebras with elements of $H^1(G, \mathrm{PGL}_n)$ is as follows (see [9]): the set of isomorphisms of $A_{1,1}$ with $A_{k,l}$ (actually, the scheme $\underline{Isom}(A_{1,1}, A_{k,l})$) is a principal homogeneous space of $\mathrm{PGL}_n(K)$. In particular, PGL_n is identified with $\underline{Aut}(A_{1,1})$, by sending $x \in \mathrm{PGL}_n$ to the automorphism $y \mapsto inn_x(y) = xyx^{-1}$ (here we identify $A_{1,1}$ with the set of matrices $M_n(K)$ and take any lift of x to GL_n). A given isomorphism λ (defined over $\overline{K}$) of $A_{1,1}$ with $A_{k,l}$ acts as a "basepoint" of $\underline{Isom}(A_{1,1}, A_{k,l})$ in the sense that any other isomorphism λ' is the composition of λ with an element of PGL_n. Then the cocycle representation is as follows: $\sigma \mapsto h(\sigma)$, where $\lambda^\sigma = \lambda \circ inn_{h(\sigma)}$. We will fix $k = a^{-1}, l = b^{-1}$, and a given basepoint λ. Then we will show the cocycle h which arises from $A_{a^{-1},b^{-1}}$ is in the same class as $r^*(\xi)$. In other words, we will be showing that the period-index obstruction is given by $(a^{-1}, b^{-1})_{Hilb}$. Since the Hilbert symbol is bilinear this is enough. Take $\lambda(x_{1,1}) = \alpha\, x_{a^{-1},b^{-1}}$ and $\lambda(y_{1,1}) = \beta\, y_{a^{-1},b^{-1}}$, where $\alpha^n = a$ and $\beta^n = b$. Then $\lambda^{-1}\lambda^\sigma(u) = inn_{h(\sigma)}(u)$ for all $u \in A_{1,1}$; when $u = x_{1,1}$ we get $\lambda^{-1}\lambda^\sigma(x_{1,1}) = \sigma(\alpha)/\alpha\, x_{1,1} = inn_{h(\sigma)}(x_{1,1}) = h(\sigma)\, x_{1,1}\, h(\sigma)^{-1}$. Since $x_{1,1}$ is invertible, we work in $\mathrm{GL}_n(K) : [\,h(\sigma), x_{1,1}] = \sigma(\alpha)/\alpha$. Similarly for $u = y_{1,1}$ we get $[\,h(\sigma), y_{1,1}] = \sigma(\beta)/\beta$.

Lemma 3.2. *There exists a $G \in GL_n(K)$ such that $x_{1,1} = G^{-1}M_SG$ and $y_{1,1} = G^{-1}M_TG$ where M_S and M_T are lifts of $r(S)$ and $r(T)$.*

Proof of Lemma. This follows from the results of [6] or an application of the Skolem-Noether Theorem. □

In light of the above lemma, we can rewrite the above formulas as:

$$[\,(Gh(\sigma)G^{-1}), M_S] = \sigma(\alpha)/\alpha \quad \& \quad [\,(Gh(\sigma)G^{-1}), M_T] = \sigma(\beta)/\beta.$$

We see that in PGL_n, $Gh(\sigma)G^{-1}$ commutes with $r(E[n])$; this is enough to show it in inside $r(E[n])$ (a computation left to the reader). Moreover, by Claim 3.1, $\xi(\sigma)$

and $Gh(\sigma)G^{-1}$ pair the same way with the basis elements S and T. By the non-degeneracy of e, we conclude that $\xi(\sigma) = Gh(\sigma)G^{-1}$. Since G is K-rational, this is exactly saying that ξ and h represent the same cocycle class. □

Remark. The Hilbert symbol depends on the choice of nth root of unity ζ which is the Weil pairing of S and T; a different choice of basis for $E[n]$ would also change the Hilbert symbol.

Corollary 3.3. *If we restrict to the curves of the form* $(1, a)$, *we get a subgroup of* $H^1(G, E[n])$ *all of whose elements have trivial period-index obstruction (hence there exist "addition formulas" for such curves).*

Proof. trivial. □

Remarks. 1) 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 $H^1(G, E[n])$ and $\{C \to S\}$; 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 $E(K) \to H^1(G, E[n])$. This "shift" will be seen below (section 5) to define the Tate pairing in the case where K is a local field.

A non-trivial characteristic of the Hilbert symbol is that $(t, 1-t)_{Hilb} = 1$ 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.

Claim 3.2. *For* $n = 3$ *the family* $C_{(t,1-t)}$ *is given by*

$$(3\,t\,(1-\zeta_3) + \lambda\,(1-t))\,(t^2X^3 + tY^3 + Z^3) + 9\,t\,(2\zeta_3 + 1)\,(tX^2Z + tY^2X + Z^2Y) +$$

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

where the Jacobian $X(3)$ *is given by* $E : X^3 + Y^3 + Z^3 + \lambda XYZ = 0$.

Proof. This is a calculation using Theorem 3.1 of [7].

4. The General Case

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

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

where C is abelian, we have two maps from $H^1(G, C) \to H^2(G, A)$. The first is the Δ map of nonabelian cohomology (see page 123 of [9]) and the second, Γ, is induced from the natural pairing of elements of C given by $< c_1, c_2 >= [\overline{c_1}, \overline{c_2}]$, where $\overline{c_i}$ is a lift of c_i to B. Namely, Γ is given by:

$$\Gamma : H^1(G,C) \xrightarrow{diag} H^1(G,C) \times H^1(G,C) \xrightarrow{\cup} H^2(G, C\otimes C) \xrightarrow{<,>^*} H^2(G,A).$$

Let B_Δ be the bilinear form associated to Δ, namely, for $\xi, \eta \in H^1(G,C)$,

$$B_\Delta(\xi,\eta) = \Delta(\xi+\eta) - \Delta(\xi) - \Delta(\eta).$$

Claim 4.1. $B_\Delta =<,>^* \circ \cup$.

Proof. We work on the level of cocycles, where we may assume that for all $\sigma \in G, \overline{\xi+\eta}\,(\sigma) = \overline{\xi}\,(\sigma)\,\overline{\eta}\,(\sigma)$:

$$B_\Delta(\xi,\eta)(\sigma,\tau) = \Delta(\xi+\eta)(\sigma,\tau) - \Delta(\xi)(\sigma,\tau) - \Delta(\eta)(\sigma,\tau) =$$

$$[\overline{\xi+\eta}\,(\sigma)\,\overline{\xi+\eta}\,(\tau)^\sigma\,\overline{\xi+\eta}\,(\sigma\tau)^{-1}][\overline{\xi}\,(\sigma)\,\overline{\xi}\,(\tau)^\sigma\,\overline{\xi}\,(\sigma\tau)^{-1}]^{-1}[\overline{\eta}\,(\sigma)\,\overline{\eta}\,(\tau)^\sigma\,\overline{\eta}\,(\sigma\tau)^{-1}]^{-1}.$$

This computation takes place in B, but the elements in braces are in its center A, so we may move them at will to get:

$$\overline{\xi+\eta}\,(\sigma)\,\overline{\xi}\,(\tau)^\sigma\,\overline{\eta}\,(\tau)^\sigma\,\overline{\eta}\,(\sigma\tau)^{-1}\,\overline{\xi}\,(\sigma\tau)^{-1}\overline{\xi}\,(\sigma\tau)\,\overline{\eta}\,(\sigma\tau)\,\overline{\eta}\,(\tau)^{\sigma\,-1}\,\overline{\eta}\,(\sigma)^{-1}\,\overline{\xi}\,(\tau)^{\sigma\,-1}\,\overline{\xi}\,(\sigma)^{-1},$$

which simplifies to

$$\overline{\xi}\,(\sigma)\,\overline{\eta}\,(\sigma)\,\overline{\xi}\,(\tau)^\sigma\,\overline{\eta}\,(\sigma)^{-1}\overline{\xi}\,(\tau)^{\sigma\,-1}\,\overline{\xi}\,(\sigma)^{-1};$$

we can cancel the two ends because the whole thing is a central element in B to get

$$B_\Delta(\xi,\eta)(\sigma,\tau) = [\,\overline{\eta}\,(\sigma), \overline{\xi}\,(\tau)^\sigma\,] =<,>^* \circ \cup\,(\eta,\xi)(\sigma,\tau).$$

Since $B_\Delta(\xi,\eta) = B_\Delta(\eta,\xi)$ we are done.$\square$

In our situation we have

$$0 \longrightarrow \mu_n(\overline{K}) \longrightarrow \mathcal{H} \longrightarrow E[n](\overline{K}) \longrightarrow 0,$$

where $\mathcal{H}$ is the Heisenberg group of dimension n (for more about the Heisenberg group, see page 11 of [3]). Here $<,>$ is the Weil pairing e and Δ is none other than the period-index obstruction map Ob.

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

Proof. We will use an alternative definition of the Ob map; see the definition of ψ_1 on page 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 $\overline{K}$-rational divisor on C whose class is G-invariant, in other words, for all $\sigma \in G$, $D \sim D^\sigma$.[1] For every σ,

[1]Over $\overline{K}$, the class of D gives rise to the line bundle $\mathcal{L}(D)$ which in turn induces the diagram $C_{\overline{K}} \to \mathbb{P}^{n-1}_{\overline{K}}$. Since $[D]$ is G-invariant, this diagram descends to K as $C \to S$; S will be isomorphic to $\mathbb{P}^{n-1}$ over K exactly when $[D]$ is representable by a K-rational divisor.

fix a function $f_\sigma \in K(C)$ such that $div(f_\sigma) = D - D^\sigma$. Then the cocycle in $Br(K)$ representing (C, D) is

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

There is a natural map φ_a from C to $a\,C$. One way to visualize φ_a is to identify C with $\underline{Pic}^1(C)$ and $a\,C$ with $\underline{Pic}^a(C)$ (via the Riemann-Roch Theorem) and then φ_a is given by sending a geometric point x to the point ax. Then φ_a is of degree a^2, since over $\overline{K}$ these schemes are elliptic curves and the map is essentially multiplication by a. Moreover, φ_a induces "multiplication by a" on the level of cocycles, since $(a\,\xi)\,(\sigma) = a(x_0^\sigma - x_0) = ax_0^\sigma - ax_0 = \varphi(x_0)^\sigma - \varphi(x_0) = \varphi^*(\xi)(\sigma)$. Finally, φ_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_σ to functions on aC which have the property that $div(N(f_\sigma)) = a(D^\sigma - D)$. Then we have $Ob(a\xi)$ is represented by the cocycle

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

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

$$Ob(a\xi)(\sigma, \tau) = \left(\frac{f_\sigma f_\tau^\sigma}{f_{\sigma\tau}}\right)^{deg(K(aC)/K(C))} = a^2 Ob(\xi)(\sigma, \tau).\Box$$

Corollary 4.1. $2\,Ob = \Gamma$.

Proof. By Claim 4.2, $B_{Ob}(\xi, \xi) = Ob(2\xi) - 2Ob(\xi) = 2Ob(\xi)$. By Claim 4.1, $B_{Ob}(\xi, \xi) = e^*(\xi \cup \xi) = \Gamma(\xi)$. $\Box$

Remark. In light of the representation we now have for Ob in terms of the cup product, the fact that it specializes to the Hilbert symbol is not surprising; see [9], Proposition 5, p. 207 and [12] for the known relationship between the Hilbert symbol and the cup product.

Corollary 4.2. *Ob is quadratic as a function on the $\mathbb{Z}$-module $H^1(G, E[n])$.*

Proof. By Definition 1 on page 27 of [8], Ob is quadratic if $Ob\,(\,a\,\xi) = a^2\,Ob\,(\xi)$ for $a \in \mathbb{Z}$ and for $\xi \in H^1(G, E[n])$ and if the associated function B_{Ob} defined as above is bilinear. These two facts follow from Claims 4.1 and 4.2. $\Box$

5. Relation to the Tate Pairing

Let K be local. Then we have a perfect pairing, called the Tate pairing, as follows:

$$<,>_T\colon E(K)/nE(K) \times H^1(G, E)[n] \to Br(K).$$

In [5], it was shown that we can represent the Tate pairing in terms of Ob as follows: to compute $< P, C >_T$, choose any lift $\tilde{C}$ of C to the group $H^1(G, E[n])$

and identify P with its image in that group via the δ map of cohomology. Then $< P, C >_T = Ob(\tilde{C}+P) - Ob(\tilde{C})$. Moreover, since Ob vanishes on the Selmer group, and in particular $Ob(P) = 1$, we can rewrite the above as $< P, C >_T = B_{Ob}(P, \tilde{C})$, where B_{Ob} is the bilinear form associated to Ob. In this notation the proof of the equality of the period and index over a local field can reproduced from [5] as follows: The period of C is $d \Leftrightarrow Ob(\tilde{C})^d = 1$ for all lifts $\tilde{C}$ of $C \Rightarrow B_{Ob}(P, \tilde{C})^d = 1\ \forall P \Leftrightarrow B_{Ob}(P, d\tilde{C}) = 1\ \forall P \Leftrightarrow < P, dC >_T = 1\ \forall P \Leftrightarrow dC = 0 \Leftrightarrow n \mid d \Rightarrow d = n$.

References

[1] Cassels, J. W. S. *Arithmetic on curves of genus 1, V. Two counterexamples*, J. London Math. Soc. 38, pp. 244-248 (1963).

[2] Farb, B. and Dennis, R. K., *Noncommutative algebra,* Graduate Texts in Mathematics, 144, Springer-Verlag, New York (1993).

[3] Hulek, K. *Projective Geometry of Elliptic Curves*, Astérisque 137, Société Mathématique de France (1986).

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

[5] Lichtenbaum, S., *The Period-Index Problem for Elliptic Curves*, Amer. J. Math., pp. 1209-1223 (1968).

[6] O'Neil, C., *Jacobians of Genus One Curves*, Mathematical Research Letters 8, no. 1-2, pp. 125-140 (2001).

[7] O'Neil, C. *Explicit 3-descent over $X(3)$*, to appear.

[8] Serre, J.-P., *A Course in Arithmetic,* Graduate Texts in Mathematics, 7, Springer-Verlag, New York (1973).

[9] Serre, J.-P., *Local Fields,* Graduate Texts in Mathematics, 67, Springer-Verlag, New York (1979).

[10] Silverman, J. H., *The Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics 106, Springer-Verlag, New York (1986).

[11] Stein, W. A., *There are Genus One Curves over Q of Every Odd Index*, http://modular.fas.harvard.edu/papers/index/.

[12] Tate, J., *Relations between K_2 and Galois Cohomology*, Invent. Math. 36, pp. 257-274 (1976).