THE PERIOD-INDEX PROBLEM IN WC-GROUPS III: BICONIC CURVES

PETE L. CLARK

Abstract.

1. Introduction

This note continues our study of the period-index problem in the Weil-Châtelet group of an elliptic curve, begun in [6]. In this paper, we conjectured that for any elliptic curve E/K defined over a number field and any prime number p, there exists an infinite subgroup G of $H^1(K,E)$, every nonzero element of which has period p and index p^2. This conjecture was proved when E has full p-torsion defined over K. In [7] we went on to pursue analogous questions in the Weil-Châtelet group of a higher-dimensional abelian variety.

In this note we give a closer analysis of what is geometrically the simplest case: namely, $A = E$ is an elliptic curve and $p = 2$. In this case, an element of $H^1(K,E)[2]$ corresponds to a genus one curve C/K with Jacobian elliptic curve E and admitting a degree two morphism $\varphi : C \to V$, where V is a conic (i.e., a smooth curve of genus zero); we call such a curve C *biconic*. (Indeed the larger group $H^1(K,E[2])$ parameterizes curves C equipped with such a map φ.) The study of biconic curves of genus one is closely related to some very classical issues, such as the geometry curves of genus one given as the intersection of two quadric surfaces in $\mathbb{P}^3$ and the invariant theory of binary quartics. ...

Conventions: In this paper we work over a perfect field k whose characteristic is different from 2 or 3. By a **curve** we always mean a smooth, projective geometrically integral curve $C_{/k}$.

2. Strongly polarized curves and maps to projective space

The **index** $I(C)$ of a curve $C_{/k}$ is the least positive degree of a divisor D on k. Equivalently, it is the gcd of all degrees $[l:k]$ of finite field extensions l/k such that C has an l-rational point. In particular, if C has a k-rational point, the index is 1.

Suppose C has genus g. By Riemann-Roch, any divisor D of degree $d \geq g$ is linearly equivalent to an effective divisor. It follows that a curve of genus 0 or 1 has index one iff if has a k-rational point. This is false for higher genera: e.g., every curve over a finite field has index one, whereas it is easy to construct for each $g \geq 2$ a hyperelliptic curve $C_{/\mathbb{F}_q}$) (for any q which is sufficiently large compared to g) without $\mathbb{F}_q$-rational points.

In this section we wish to highlight the interplay between index of C – i.e., arithmetic on C – and the morphisms of morphisms from C into projective space – i.e., the extrinsic geometry of C.

By a **polarized curve** we mean a pair (C, D), where $C_{/k}$ is a curve and $D \in \mathrm{Div}(C)$ is an effective divisor of positive degree. We say that two polarizations (C, D) and (C, D') on a curve C are equivalent if the divisors D and D' are linearly equivalent. Alternately, we may view a polarization on C as an ample line bundle L on C, and then (C, L) and (C, L') are equivalent precisely when L and L' are isomorphic. On occasion it is convenient to refer to L as the **polarizing bundle** of (C, L).

A polarization determines a morphism

$$\varphi_D : C \to \mathbb{P}^{l(D)-1}.$$

Our definitions so far allow for the possibility that $l(D) = 1$, in which case φ_D is just the map from C to a one-point space. It turns out to be convenient for the general theory to allow such polarizations, but of course they are not interesting in and of themselves. So let us say that a polarization with $l(D) = 1$ is **trivial**, and any other polarization is nontrivial. The point here is that from a trivial polarization we can build a nontrivial polarization: it follows from Riemann-Roch that if D is any polarization on the genus one curve C, then nD is nontrivial for all $n \geq g+1$.

For any nontrivial polarization the image $\varphi_D(C)$ is also a curve, which we denote by C', and $\varphi_D : C \to C'$ is a finite morphism. In fact, as we will recall shortly, either $C' \cong C$ – i.e., φ_D is an embedding into projective space – or $C \to C'$ has degree 2 and C' has genus 0. It is the latter case that we wish to study here.

Let g be the genus of C. For every value of $g \neq 1$, some integral multiple of the canonical bundle $K = \Omega_{C/k}$ is a polarizing bundle, and thus we have (pluri)canonical maps into projective space. Let us review:

Case I: $g = 0$. Let D be any divisor associated to $L = -K$, the anticanonical bundle. By Riemann-Roch, $l(D) = 3$. Moreover $\deg(L) = 2 \geq 2g(C) + 1$, so that L is very ample. Thus $C \xrightarrow{\sim} C' \subset \mathbb{P}^2$ is a plane conic curve. Under our assumption that $\mathrm{char}(k) \neq 2$, the conic can be diagonalized, so is representable in the form

$$C_{a,b} : aX^2 + bY^2 = Z,$$

for some $a, b \in k^\times$.

Remark: If C has a k-rational point P, then taking $D = [P]$ the map $\varphi_D : C \to \mathbb{P}^1$ is an isomorphism.

Proposition 1. *Let $C_{/k}$ be a genus zero curve. The index of C is either 1 or 2. Moreover, TFAE:*
(i) The index of C is equal to 1.
(ii) C has a k-rational point.
(iii) $C \cong_k \mathbb{P}^1$.
(iv) The quaternion algebra $\langle a, b\rangle$ is isomorphic to the matrix algebra $M_2(k)$.

Case II: $g \geq 2$. We may take as a polarizing bundle the canonical bundle K, so let D be any canonical divisor. We have $\deg(D) = 2g-2$, so $I(C) \mid 2g-2$. This bound is best possible: e.g., for each $g \geq 2$, there exists a number field $K = K(g)$ and a genus g curve $C_{/K}$ with $I(C) = 2g-2$ [8, Cor. 4]. By Riemann-Roch, $l(D) = g$. We wish to consider three cases:

(a) The canonical bundle is very ample. Then $\varphi_D : C \stackrel{g}{\to} \mathbb{P}^{g-1}$ embeds C as a degree g curve in $\mathbb{P}^{g-1}$. Evidently this is not possible if $g = 2$. Conversely, for any $g \geq 3$ there exists at least one curve $C_{/k}$ with very ample canonical divisor (cf. Poonen). Moreover, the curve corresponding to the generic point on the moduli space $\mathcal{M}_g$ (uniquely defined since such a curve has no nontrivial automorphisms) has very ample canonical divisor.

(b) Otherwise, the canonical bundle is ample but not very ample. In this case the map $C \to C' = \varphi_D(C)$ has degree 2, C' has genus 0, and the emedding $C' \hookrightarrow \mathbb{P}^{g-1}$ is a form of the Veronese embedding of degree $g-1$. [[Explain in more detail how to define the Veronese embedding for a conic without rational points.]] This case further subdivides:

(b1) The curve C' has a k-rational point, i.e., is isomorphic over k to $\mathbb{P}^1$. In this case we say that C is **hyperelliptic**.

For a hyperelliptic curve, the map $C \to \mathbb{P}^1$ has degree 2 and, by Riemann-Hurwitz, $2g+2$ branch points. It follows that the function field $k(C)$ can be obtained by taking the square root of a nonconstant rational function $f(t) \in k(t) = k(\mathbb{P}^1)$. Because $k(t)(\sqrt{f(t)}$ depends on $f(t)$ only modulo squares, we may assume that $f(t)$ is a polynomial which is a product of distinct irreducible factors. If k is not perfect, then one could *a priori* have an inseparable irreducible factor. But then the base change of C to the splitting field of such a factor would be a curve of strictly smaller genus, which implies that the curve $C_{/k}$ was not *smooth*, and we have agreed to exclude this case from consideration. Therefore any hyperelliptic curve of genus g has an affine model

$$y^2 = P_{2g+2}(x),$$

where $P_{2g+2} \in k[x]$ is a separable polynomial of degree $2g+2$. Here if $g \geq 1$, then the projective closure has a unique point at infinity, which is a singular point.

Remark: The point $\infty \in \mathbb{P}^1$ is not a branch point, so its pullback to C is a reduced divisor of degree 2. This divisor may correspond to two distinct k-rational points $[P_{\infty_1}] + [P_{\infty_2}]$, or a single point P_∞ whose residue field is a quadratic extension of k. The first case obtains iff the highest order coefficient $a = a_{2g+2}$ of P is a square in k; otherwise, the residue field of the unique point lying over ∞ is $k(\sqrt{a})$.

Remark: If $\pi : C \to \mathbb{P}^1$ is the degree 2 hyperelliptic map, let $P \in \mathbb{P}^1(k)$ be a k-rational point. Then $\pi^*(P)$ is a degree 2 divisor. We conclude that $I(C) \mid 2$, i.e., the index is either 1 or 2.

Certainly both values of I are possible. Indeed, let k be any formally real field

(e.g. $k = \mathbb{Q}$, $k = \mathbb{R}$), and for any $g \geq 0$, define

$$C : y^2 = -(x^{2g+2} + 1).$$

Then C has no rational points over any real closure of k, hence no rational points over any extension of odd degree: $I(C) = 2$.

Problem 1. *(Hyperelliptic index problem) Suppose we are given a genus g hyperelliptic curve C over a field k*

$$C : y^2 = P_{2g+2}(x).$$

Determine whether $I(C) = 1$ or $I(C) = 2$.

This turns out to be quite difficult: no general solution is known for (e.g.) $k = \mathbb{Q}$.

(b2) We have $C'(k) = \varnothing$. In this case we say that C is **properly biconic**.

We propose to call a curve C of genus $g \geq 2$ **biconic** if it is either hyperelliptic or properly biconic. Equivalently, a curve $C_{/k}$ is biconic iff $C_{/\overline{k}}$ is hyperelliptic.[1]

In this case, the function field $k(C')$ is, as above, the fraction field of $k[x,y]/(aX^2 + by^2 - 1)$ for suitable $a, b \in k^\times$. Again we can generate $k(C)$ over $k(C')$ by taking the square root of a polynomial $f(x,y)$. Since biconic curves are geometrically hyperelliptic, the ramification locus of $C \to C'$ still consists of $2g+2$ geometric points. On the other hand, the ramification locus is the locus in $\mathbb{P}^2$ of

$$f(X,Y,Z) = 0,\ aX^2 + bY^2 = Z^2.$$

Applying Bézout's theorem we conclude that the degree of the homogenized polynomial $f(X,Y,Z)$ must be $g+1$. In summary, we get an explicit model for C inside $\mathbb{P}^3$; writing our homogeneous coordinates as $[X : Y : Z : T]$, it is:

$$f(X,Y,Z) = T^2 Z^{g-1},\ aX^2 + bY^2 = Z^2 \tag{1}$$

Proposition 2. *Let C be a biconic curve of genus $g \geq 2$. If g is even, then $C' \cong \mathbb{P}^1$ and C is (canonically) hyperelliptic.*

Proof: Since C' is a degree $g-1$ curve in $\mathbb{P}^{g-1}$, if g is even, $g-1$ is odd. Therefore any hyperplane H in $\mathbb{P}^{g-1}$ intersects C' in an effective divisor of odd degree. Thus the index of C' is odd, and therefore it is 1, which implies that it has a k-rational point, and hence is isomorphic to $\mathbb{P}^1$.

Conversely:

Proposition 3. *Let $g \geq 3$ be an odd integer, and let $(C')_{/k}$ be a genus zero curve without k-rational points. Then there exists a genus g curve $C_{/k}$ such that $\varphi_K(C) \cong C'$. In particular, C is biconic and not hyperelliptic.*

Proof: By Riemann-Hurwitz, it suffices to find a morphism $f : C' \to \mathbb{P}^1$ of degree $2g+2$ such that the divisor $f^{-1}(0)$ consists of $2g+2$ distinct geometric points, for then we can take $k(C')(\sqrt{f})$ as the function field for C. Let k'/k be a quadratic extension over which $C' \cong \mathbb{P}^1$. The hypotheses imply that k is infinite, so let $q \in k'(C') \cong k'(t)$ be a polynomial of degree $g+1$ of the form $\prod_{i=1}^{g+1}(t - x_i)$,

[1]These terms are neologisms due to the author. We hope that the present work demonstrates the usefulness of the distinction between hyperellipticity and biconicity in arithmetic geometry.

and put $f = q\overline{q} = \prod_{i=1}^{g+1}(t - x_i)\prod_{i=1}^{g+1}(\overline{t} - \overline{x_i})$, where $\overline{x_i}$ denotes the k'/k-Galois conjugate of x_i (which is distinct from x_i since C' has no k-rational points), and similarly $\overline{t}$ is the conjugate rational function.

Remark: For $g \geq 3$, the bicanonical bundle $L = 2K$ has degree $4g - 4 \geq 2g + 1$, so is very ample and embeds C in $\mathbb{P}^{3g-3}$. For $g \geq 2$, the tricanonical bundle $L = 3K$ has degree $6g - g \geq 2g + 1$, so is very ample and embeds C in $\mathbb{P}^{5g-5}$. Although these embeddings certainly have their uses – especially when studying the moduli space of all curves of genus g – in terms of explicit equations they are much more complicated than the hyperelliptic and biconic models. Moreover, the hyperelliptic / biconic model has a much closer relationship to the index of C. Indeed, we have the following evident result:

Proposition 4. *The index of a properly biconic curve is either* 2 *or* 4.

Problem 2. *(Biconic index problem)*
Given a biconic curve $C_{/k}$, determine whether $I(C)$ is 1, 2 *or* 4.

Case III: $g = 1$. In this case the canonical bundle is trivial, so no integral power of it is ample. Thus this situation is quite different from the other cases: a polarization on C involves a choice of additional structure; there is no such thing as a "canonical" polarization.

So suppose we are given an effective k-rational divisor D of degree $d \geq 2$.

Case a) $d \geq 3$. Then by Riemann-Roch we the morhpism $\varphi_D : C \to \mathbb{P}^{d-1}$ is a degree d embedding. When $d = 3$, this means that $C' \cong C$ is a plane cubic curve. For $d \geq 4$, the image C' is the intersection of $\frac{d(d-3)}{2}$ quadric hypersurfaces [9, Prop. 5.3]. When $d = 4$, we get an intersection of two quadrics in $\mathbb{P}^3$, which we can describe quite explicitly, as follows. Since $h^0(2D) = 8$ and the space of quadratic forms in the variables X, Y, Z, T is 10-dimensional, there exist two linearly independent quadratic forms $Q_1(X, Y, Z, T)$, $Q_2(X, Y, Z, T)$ vanishing on C. Since the locus $Q_1 = Q_2 = 0$ is already a quartic curve, it follows that φ_D expresses the genus one curve C as the intersection of the two quadric surfaces $Q_1 = Q_2 = 0$. For $d \geq 5$ the image curve C' is not a complete intersection.

Case b): $d = 2$. Then by Riemann-Roch the morphism φ_D maps to $\mathbb{P}^1$ and has degree 2. The converse also holds: any degree two map $\pi : C \to \mathbb{P}^1$ is the morphism associated to the complete linear system $\pi^*(p)$, where p is any rational point on $\mathbb{P}^1$. Moreover, by the same argument as in Case IIbi above, we can represent C by the affine equation

$$y^2 = P_4(x).$$

It therefore seems reasonable to extend our above terminology: by a **hyperelliptic curve of genus one** we mean a polarized genus one curve (C, D), where $\deg D = 2$. We also define a **hyperelliptic involution** on a curve of genus $g \geq 1$ to an involutory (i.e., order 2) automorphism ι of C such that $C/\iota \cong \mathbb{P}^1$. The data of a hyperelliptic involution is equivalent to that of a line bundle L of degree 2 with $h^0(C, L) = 2$.

Note well the distinction between hyperellipticity in $g \geq 2$ and hyperellipticity in genus one: a curve of genus $g \geq 2$ admits at most one hyperelliptic involution, which is constructed from the geometry of the canonical bundle. However, a curve of genus one may admit multiple – indeed, continuously many – hyperelliptic involutions. Suppose for simplicity that k is algebraically closed, and choose $O \in C(k)$. Then we may take O as the origin of a group law on C, and accordingly get an involution $\iota_O : P \mapsto -P$, which has O as a fixed point and also three other fixed points, the 2-torsion points. But if now O' is any k-rational point which is not one of the four fixed points of ι_O, we similarly get another hyperelliptic involution $\iota_{O'}$ which is evidently distinct from ι. Thus, since $C(k)$ is infinite, we have infinitely many hyperelliptic involutions on C.

Having defined hyperelliptic polarized curves of genus one, it is natural to wonder about biconic polarized curves of genus one. The alert reader will notice that this is impossible: no genus one curve C admits a divisor D such that $\varphi_D(C) = C'$ is a curve of genus zero without rational points. Indeed, all possibilities have already been described.

However, we can still define a biconic curve of genus one as a genus one curve C together with a degree 2 map down to a genus zero curve C'. Arguing as above, such a morphism gives rise to an explicit model for C in $\mathbb{P}^3$, namely

$$f(X, Y, Z) = T^2, \ aX^2 + bY^2 = Z^2 \tag{2}$$

where f has degree 2. This is a smooth model, and in fact it is a special case of the model coming from a polarization of degree 4. This makes good sense, because given $\pi : C \to C'$, there exists a degree 2 divisor on C' and its preimage gives a degree 4 divisor on C. Moreover, since there is, up to isomorphism, a unique degree 2 line bundle L' on C', the isomorphism class of the pullback $L = \pi^* L'$ is well-determined. Therefore a biconic structure on C *induces* a polarization of degree 4.

There are two very natural questions:

1) Can one interpret the structure of a biconic morphism $\pi : C \to C'$ in terms of line bundles on C?

2) Suppose that C is a genus one curve endowed with a biconic structure, where $C'(k) = \emptyset$. How can we tell whether C is hyperelliptic; equivalently, when it has a divisor of degree 2?

Some further elementary geometric reasoning will answer Q1), which at the same time will reveal that Q2) is precisely the **period-index problem** for genus one curves of period 2. We will then give a complete solution to the period-index problem in this case, which is the easiest case left unsolved by prior work of Clark, Clark-Sharif and Sharif. As an application we will exhibit a field k for which there exist two elliptic curves E_1, E_2 over k such that: every torsor C under E_1 has period equals index; there exists a torsor C under E_2 with period 2 and index 4.

2.1. **Some instances of change of model.**

If $C_{/k}$ is an algebraic curve, then the set $\mathcal{P}(C) \subset \operatorname{Pic} C$ of polarizing line bundles has some natural algebraic structure. First it is a semigroup under addition: if L_1 and L_2 are polarizing bundles, so is $L_1 \otimes L_2$. Indeed, choosing corresponding effective divisors D_1 and D_2, the polarizing condition is equivalent to the existence of nonconstant rational functions f_i with polar divisor $\operatorname{div}_\infty f_i \leq D_i$. ...

Special case: Suppose O is a k-rational point on C. Then for any $d \geq 2$, $D_d = d[O]$ is an effective divisor of degree d. For $d \geq g+1$, D_d is a polarization on C. The "divisibility" of these polarizations has an impact on the arithmetic and geometry of the model. Indeed, by choosing suitable projective coordinates $[X_1 : \ldots : X_{\ell(D)}]$, the morphism $\varphi_{D_d} : C \to \mathbb{P}^{\ell(D)-1}$ has the property that if we intersect with the "hyperplane at infinity" $X_{\ell(D)} = 0$ and pull back to C, we recover the divisor $D_d = d[O]$.

When $g = 1$, $d = 2$, this means that $\infty \in \mathbb{P}^1$ is a ramification point for the morphism $\pi : C \to \mathbb{P}^1$. This leaves three ramification points on the affine line, and thus we get the function field of C by taking the square root of a cubic polynomial $P_3(x)$, giving the affine model

$$y^2 = P_3(x).$$

When $g = 1$, $d = 3$, this means that the point $\varphi_{D_3}(O) \in C' \subset \mathbb{P}^2$ is the unique intersection point of the line at infinity $Z = 0$ with the cubic curve C': it is a cubic flex point. This amounts to special conditions on the cubic defining equation $F(X, Y, Z) = 0$. Indeed, we use functoriality again and consider $L(2[D_3]) = L(6[O])$. By Riemann-Roch, there exists a nonconstant rational function x on $k(C)$ with polar divisor $2[O]$ and a nonconstant rational function y on $k(C)$ with polar divisor $3[O]$. Since $l(6[O]) = 6$, the seven elements $1, x, y, x^2, xy, x^3, y^2$ of the linear system $|6[O]|$ must be linearly dependent, which leads to the Weierstrass model

$$Y^2Z + a_1XYZ + a_3YZ^2 = cX^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

(This can be explained a little better: the map into projective space can be taken to be $[x : y : 1]$...)

When $g = 1$, $d = 4$, we can take projective coordinates $[X : Y : Z : T]$ such that $C' \cap (T = 0)$ is again the single point $\varphi(O)$, with multiplicity 4. As above, we can choose (X, Y, Z) to be rational functions on C having poles of order $(1, 2, 3)$ at O, and then it follows that there is some constant $c \in k$ such that $XZ = cY^2$. Thus one of the quadrics in the pencil is an **isotropic conic**. The projection $[X : Y : Z : T] \in C \mapsto [X : Y : Z]$ endows C with a hyperelliptic structure, corresponding to the degree 2 divisor $2[O]$.

Example: Norm maps.

2.2. **Weakly polarized curves.**

A degree d **weak polarization** on a curve C we mean a pair $(C, \overline{D})$, where $\overline{D}$ is an effective divisor of positive degree on $C_{/\overline{k}}$ whose linear equivalence class is Galois invariant: for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we have $\sigma(\overline{D}) \sim \overline{D}$.

Via the canonical injection $\mathrm{Pic}\, C \to \mathrm{Pic}\, C_{/\overline{k}}$ we may regard any polarization as a weak polarization. Obviously there is no distinction if $k = \overline{k}$. More generally, if C has a k-rational point then any rational divisor class contains a rational divisor, so all weak polarizations are polarizations. However, for curves without rational points there is indeed a distinction to be made, which turns out to be highly relevant for us:

Proposition 5. *For a curve $C_{/k}$ of positive genus, a weak polarization $\overline{D}$ of degree 2 with $l(\overline{D}) = 2$ induces a biconic structure $\pi : C \to C'$, and conversely every biconic structure comes from such a weak polarization, uniquely up to equivalence.*

The implications of this result are much more interesting in genus one, for only in genus one can a curve have multiple biconic structures, some of them properly biconic and some of them (perhaps!) hyperelliptic.

2.3. **Biconic curves of genus one.**

Let E/K be an elliptic curve and $\eta \in H^1(K, E)[2]$. Then η corresponds to C, a genus one curve together with the structure of a principal homogeneous space over E. (Because $2 \cdot \eta = 0$, if $\mathrm{Aut}(E/\overline{K}) = \pm 1$ – as is generically the case – then C admits a unique principal homogeneous space structure.) Via the Kummer sequence, η admits at least one lift to a class $\xi \in H^1(K, E[2])$, whose elements can be viewed as parameterizing Galois twisted forms of $[2] : E \to E$, i.e., maps $\varphi : C \to E$ with geometric Galois group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The map φ determines a canonical K-rational divisor class of degree 2 on C, as follows: choose $P \in C(\overline{K})$ such that $\varphi(P) = O$, and consider $D_2' := 2[P]$. By identifying φ with $[2]$ over $\overline{K}$, we find that independent of the choice of P, D_2' is linearly equivalent to $2[O]$, so in particular we have that for all $\sigma \in \mathfrak{g}_K$, $\sigma(D_2') \sim D_2'$, so that $D_2' \in \mathbf{Pic}^2(C)(K)$. Another application of Galois descent (CITE!) associates to D_2' a morphism $\varphi_{D_2'} : C \to V$, a twisted form of the embedding associated to a divisor of degree 2. Thus:

Proposition 6. *Let E/K be an elliptic curve and $\eta \in H^1(K, E)[2]$. Then η corresponds to a biconic genus one curve C, and the lifts ξ of η to $H^1(K, E[2])$ correspond to biconic diagrams $\varphi : C \to V$.*

Corollary 7. *Let C/K be a genus one curve. The following are equivalent:*
a) C admits a rational divisor class of degree two (i.e., C has period two).
b) C admits a DC_2'-canonical model, i.e., a projective model of the form

$$aX^2 + bY^2 = Z^2$$
$$T^2 = f(X, Y, Z)$$

for some quadratic form f.

Proof: We saw above that a choice of rational divisor class of degree two on a genus one curve C induces a biconic structure $C \to V$. Earlier we saw that a biconic curve of genus g admits a projective model of the form (1), where the degree of f is $g + 1 = 2$. The converse is even more clear, as the map $(X, Y, Z, T) \mapsto (X, Y, Z)$ induces a degree two covering $C \to V$.

2.4. **The Galois set of quadratic cones.** Suppose C/K is a genus one curve embedded in $\mathbb{P}^3$ by means of a degree four divisor. It makes sense to ask whether there is a biconic morphism $C \to V$ consistent with this embedding, a notion which can be expressed in two ways. On the more algebraic side, we are asking if the divisor D_4 is in the image of $[2] : \mathbf{Pic}^2(C)(K) \to \mathbf{Pic}^4(C)(K)$, i.e., is $2D_2'$ for some rational divisor class D_2'. Geometrically, we are asking whether some element of $L(2D_4)$ is a conical quadric surface.

The embedding $C \to \mathbb{P}^3$ does not determine the quadrics Q_1 and Q_2 uniquely, but rather the entire pencil $P(x) = xQ_1 + Q_2$ of quadrics as x varies over $\mathbb{P}^1/\overline{K}$ (we get Q_1 by taking $x = \infty$). It is a well-known geometric fact that every (nondegenerate, in a sense that we are about to make precise) pencil of quadric surfaces contains, over $\overline{K}$, precisely four conical quadrics: these are the values of x for which the discriminant $f = \mathrm{disc}(P(x))$ of the quaternary quadratic form $P(x)$ vanishes. Thus we can define a hyperelliptic curve

$$C' : y^2 = f(x)$$

which is generically a quartic, but is a Weierstrass cubic precisely when Q_1 is conical (so that one of the roots of $f(x)$ is $x = \infty$). Over $\overline{K}$ the elliptic curve C' is isomorphic to the elliptic curve C, but over an arbitrary base C' is given by a D_2-canonical model so is closer to having a rational point than C. In fact [McC] give an explicit degree four map $\Psi' : C \to C'$, so that the process of finding the map $j_{D_4} : C \to J(C)$ is reduced to the (easier) construction of the Jacobian of a hyperelliptic quartic curve. Thus, when Q_1 is conical, the map $\Psi' : C \to E$ is the two-covering corresponding (under the two interpretations of $H^1(K, E[2])$ to the map $C \to V$ as above.

Assume henceforth that $Q_1 = V$ is conical. The construction then gives a bijection between the remaining quadratic cones V_2, V_3, V_4 in the pencil and the nontrivial 2-torsion points of E. Thus the Galois action on the set $\{V_2,\ V_3,\ V_4\}$ can be nontrivial. In particular, a genus one curve can be represented as the intersection of two conical quadrics if and only if it has period 2 and $E[2](K) \neq 0$.

Example (Simultaneously diagonalizable quadrics): Whereas any single quadratic form over F can be diagonalized, it is very rare that two quadrics Q_1 and Q_2 can be simultaneously diagonalized. Indeed, if $Q_1(X, Y, Z, T)$ and $Q_2(X, Y, Z, T)$ are both diagonal conics, $f(x) = \mathrm{disc}(xQ_1 + Q_2)$ has four linear factors, so we may take Q_1 and Q_2 to be conical. Over $\overline{K}$ we may take all the nonzero coefficients to be 1, and under the natural S_4-action on $\mathbb{P}^3$ (permutation of variables) we may arrange for Q_1 to omit any given variable (say X) and Q_2 to omit any other variable (say Y), so that over $\overline{K}$ we get the equations

$$Y^2 + Z^2 + T^2 = 0,\ X^2 + Z^2 + T^2 = 0 \tag{3}$$

and it remains to compute the j-invariant of this elliptic curve. However, since the defining conics lack rational points over any formally real field (so a fortiori $C(K) = \emptyset$ for such K), we might do better to choose a different K-rational model, which hopefully motivates Cassels' choice C :

$$Q_1(X, Y, Z, T) = X^2 - Y^2 + T^2 = 0,$$

$$Q_2(X,Y,Z,T) = Y^2 - Z^2 + T^2 = 0,$$

which has the rational point $O = [1:1:1:0]$. For this model, $P(x) = \mathrm{disc}(xQ_1 + Q_2) = x^3 - x$, so C is the elliptic curve $y^2 = x^3 - x$, which has CM by $\mathbb{Z}[\sqrt{-1}]$, j-invariant 1728, and Mordell-Weil group $E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Alternately, the elliptic curve can be geometrically determined by noting that

$$\Psi : (X,Y,Z,T) \mapsto (Z,Y,X,\sqrt{-1}T)$$

is an order four automorphism of C which fixes O.

2.5. **A question about splitting fields.** Let C/K be a genus one curve without K-rational points, and η a corresponding element in $H^1(K,E)$. A more ambitious question than the period-index problem is to ask for a description of all splitting fields L for η, i.e., for the collection of extensions L/K such that $C(L) \neq \emptyset$. When $\mathfrak{g}_K$ is complicated (e.g. $K = \mathbb{Q}$) this seems like too much to ask, but it is interesting to inquire about the existence of splitting fields with various properties: for instance, may we always take a splitting field which is abelian, or solvable, or Galois with degree equal to the index of η?

The example of [**?**, § 2.3] gives a negative answer to the first and third questions when $K = \mathbb{Q}_p$: let $\ell > p$ be another prime number and $E/\mathbb{Q}_p$ an elliptic curve with good reduction and $E(\mathbb{Q}_p)[\ell] \neq 0$ (as explained in *loc. cit.*, such curves can be found precisely when $p+1 \leq \ell < p+1+2\sqrt{p}$, so they exist in abundance) then there exists a class $0 \neq \eta \in H^1(\mathbb{Q}_p,E)[\ell]$. By a result of Lang and Tate, $\eta|_L = 0$ if and only if $\ell \mid e(L/K)$, but by the basic theory of local fields (especially, because $\mathbb{Q}_p$ does not contain the ℓth roots of unity) no such L is abelian over K. Note that this construction works only for odd primes ℓ.

The situation is different when E/K has full n-torsion, where to split a class $\eta \in H^1(K,E)[n]$ it suffices to split any lift to $\xi \in H^1(K,E[n]) \cong (K^\times/K^{\times n})^2$, and since the latter group parameterizes pairs of characters of order dividing n, such an η obviously has an abelian splitting field. The following is a generalization of this:

If we assume (only) that $E[2](K) \neq 0$, then C is the complete intersection of two conical quadric surfaces, say $Q_1(X,Y,Z) = Q_2(X,Y,T) = 0$, and by prescribing arbitrary values of X and Y in $K^\times$ we get independent quadratic equations to solve for Z and T; thus, as in the case of full 2-torsion, η can be split over a biquadratic extension.

Question 8. *Does there exist a field K (not of characteristic two), an elliptic curve E/K and a class $\eta \in H^1(K,E)[2]$ which cannot be split over any abelian extension?*

In fact, a rational divisor class of degree n becomes rational over a solvable extension (because every element of the Brauer group is split by a metabelian extension, a consequence of the Merkurjev-Suslin theorem), so every curve C/K of period n has a solvable point if and only if every curve of index n has a solvable point. The latter clearly holds over every field for all $n \leq 4$.

One rather suspects that there should exist a field K and a genus one curve of index 5 with no rational points over any solvable extension, but to the best of my

knowledge there are no examples of this. On the other hand, it has been suggested to me (by B. Mazur) that every genus one curve over $\mathbb{Q}$ should acquire a rational point over a solvable – indeed, metabelian – extension.

3. The explicit form of the period-index obstruction

In this section, K is an arbitrary field of characteristic different from two, so any elliptic curve E/K is given by an equation of the form

$$y^2 = (x-\theta_1)(x-\theta_2)(x-\theta_3) = f(x)$$

for some separable, monic cubic polynomial $f(x) \in K[x]$. Let $L := K[T]/(f(T))$ denote the associated étale cubic algebra. L can be one of the following four types:

(i) $L \cong K \times K \times K$, the *split case*,
(ii) $L \cong K \times M$, where M/K is a quadratic field extension, the *semisplit case*,
(iii) L is a field and L/K is a Galois extension, the *cyclic case*,
(iv) L is a field and L/K is non-normal, the *generic case*.

Remark: Although the polynomial $f(x)$ is not uniquely determined by the elliptic curve, the isomorphism class of the étale algebra L is, as follows either by a direct computation using a change of variables between Weierstrass equations as in [17] or by a characterization of L in terms of the Galois representation on the two-torsion points.

3.1. **A classical isomorphism.** In order to make explicit the obstruction map $\Delta : H^1(K, E[2]) \to \mathrm{Br}(K)$ we need an "explicit" description of $H^1(K, E[2])$. When $E[2]$ has trivial $\mathfrak{g}_K$-module structure, Kummer theory gives an isomorphism $H^1(K, E[2]) \cong (K^\times/K^{\times 2})^2$. But we cannot write "=" because there are six different isomorphisms, one for each ordered $\mathbb{Z}/2\mathbb{Z}$-basis of $E[2](\overline{K})$. We now recall a simple formalism whose motivating idea is to preserve the $S_3 = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$-symmetry of the situation by proceeding in a way that avoids making such an arbitrary choice.

A *kernel set* is an ordered triple $(\lambda_1, \lambda_2, \lambda_3)$ with $\lambda_i \in K(\theta_i)^\times$, satisfying the following two conditions:
• If θ_i and θ_j are conjugate over K, then so are λ_i and λ_j.
• $\lambda_1\lambda_2\lambda_3 = 1$.

Recall that we defined a cubic algebra $L = K[T]/(f(T))$, so there is a norm map $N : L^\times \to K^\times$. The reader should now check that the group KS is nothing but a convenient description of the kernel of the norm map. In particular, in the split case, we have $L \cong K \times K \times K$, so $KS \cong \{(a,b,c) \in K^\times \mid abc = 1\}$, so that $KS/KS^2 \cong K^\times/K^{\times 2} \times K^\times/K^{\times 2}$ (but the former being a "better" description in that the isomorphism involves a preferred choice of two out of the three coordinates). It is very well-known (e.g. [17]) that in the split case the embedding $\iota : E(K)/2E(K) \hookrightarrow KS/KS^2$ is given as

$$(x,y) \mapsto (x-\theta_1, x-\theta_2, x-\theta_3).$$

(Here we must specify that the neutral element $O = [0:1:0]$ maps to 1, and the symmetry allows us to define the map even at a two-torsion point, e.g. the first coordinate of $\iota(\theta_1, 0)$ is determined by the condition that the product be equal to 1, so is $\frac{1}{(e_1-e_2)(e_2-e_3)}$.) This motivates the following result:

Theorem 9. *There is a canonical isomorphism* $W : H^1(K, E[2]) \xrightarrow{\sim} KS/KS^2$.

Remark: This is a much-used classical result, cited in [**?**, p. 240] and [**?**, p. 215]. As far as I can tell, what is essentially the theorem is first proved in [**?**, §3], but instead of kernel sets (or, what is certainly the same thing, the kernel of the norm map) there is a somewhat different (more general but, it seems now, less useful) description in terms of "invariant sets." Recently some far-reaching generalizations of the theorem have appeared [**?**] [**?**], which will be mentioned briefly at the end of this paper. For completeness, and because it is useful to have the isomorphism at hand, we give a proof.

Proof: We begin by noting that a version of Hilbert 90 holds for the étale algebra L: namely, let G/K be the group scheme whose functor of points is $G(A) := (L \otimes_K A)^\times$, so that G is the Weil restriction of $\mathbb{G}_m/L$ via the finite étale base change L/K. Thus by Shapiro's Lemma we have $H^1_{\text{et}}(K, G) = H^1_{\text{et}}(L, \mathbb{G}_m/L) = 0$.[2] Writing $\overline{L} := L \otimes_K \overline{K}$, we thus get a corresponding Kummer isomorphism

$$H^1(K, \mu_2(\overline{L}) \xrightarrow{\sim} L^\times/L^{\times 2}.$$

We define a Galois-module map $w : E[2] \to \mu_2(\overline{L})$ by

$$w(\theta) := (e_2(\theta, \theta_1), e_2(\theta, \theta_2), e_2(\theta, \theta_3)),$$

where e_2 is the Weil pairing, and we have made the natural isomorphism $\overline{L} \cong \overline{K} \times \overline{K} \times \overline{K}$ via $P(T) \in \overline{K}[T] \mapsto (P(\theta_1), P(\theta_2), P(\theta_3))$. Let $W := H^1(w)$. Now, under the Kummer isomorphism, the norm map $L^\times/L^{\times 2} \to K^\times/K^{\times 2}$ corresponds to

$$(\eta : \sigma \mapsto (\epsilon_1(\sigma), \epsilon_2(\sigma), \epsilon_3(\sigma))) \mapsto (\eta \mapsto \prod_{i=1}^3 \epsilon_i(\sigma)),$$

which then corresponds to an element of $K^\times/K^{\times 2}$ by usual Kummer theory. Thus the identity $e_2(\theta_\sigma, \theta_1) \cdot e_2(\theta_\sigma, \theta_2) \cdot e_2(\theta_\sigma, \theta_3) = 1$ implies that $W(H^1(K, E[2]))$ is contained in the kernel of the norm map.

We will show that the map is an isomorphism by explicitly constructing the inverse map $KS/KS^2 \to H^1(K, E[2])$. Given a kernel set $(\lambda_1, \lambda_2, \lambda_3)$, choose square roots ν_i of λ_i; we must for each σ find an element θ_σ such that for $i = 1, 2, 3$,

$$\frac{\sigma(\nu_i)}{\nu_i} = e_2(\theta_\sigma, \theta_i).$$

By the nondegeneracy of e_2, any given equation $e_2(T, \theta_i) = \pm 1$ has precisely two solutions T in $E[2]$, and by checking cases one verifies immediately that the two equations

$$\frac{\sigma(\nu_1)}{\nu_1} = e_2(T, \theta_1), \ \frac{\sigma(\nu_2)}{\nu_2} = e_2(T, \theta_2),$$

have, for all four possible choices of signs on the left hand sides, a unique solution $T \in E[2]$. That this unique value of T also solves the third equation is, as above, a consequence of the relation $\lambda_1\lambda_2\lambda_3 = 1$. We leave the reader to verify that these two maps are mutually inverse.

[2]There are of course any number of other proofs: e.g. by viewing $H^1(K, G)$ as parameterizing suitable twisted forms, or indeed by a direct adaptation of any of the proofs of Hilbert 90.

Example (semisplit case): When $f(T)$ has a rational root – say θ_3 – then the elements of KS can be written down explicitly; they are just $(\lambda, \lambda^\star, \frac{1}{\lambda\lambda^\star})$, where under the decomposition $L \cong M \times K$, λ is any element of $M^\times$ and the * denotes the nontrivial automorphism of M/K.[3] In other words, $H^1(K, E[2]) \cong M^\times/M^{\times 2}$. Consider the subgroup $G \subset H^1(K, E[2])$ given by square classes of $M^\times$ represented by elements of $K^\times$. To each $g \in G$ there corresponds a diagram $\lambda : C \to V$. We claim that C has index two. Indeed, under the isomorphism of the theorem, G corresponds to the image of the map $H^1(i) : H^1(K, \mathbb{Z}/2\mathbb{Z}) = H^1(K, \langle\theta_3\rangle) \to H^1(K, E[2])$, where $i : \langle\theta_3\rangle \to E[2]$. Thus every element of G is split by a quadratic extension, the one determined by the element of $K^\times/K^{\times 2}$. It follows from §1 that C has a hyperelliptic model; this model is computed directly in terms of the Weierstrass equation for E in [17, Example X.3.7]. These considerations lead us to the following result:

Proposition 10. *Suppose $K^\times/K^{\times 2}$ is infinite and $E(K)/2E(K)$ is finite. Then, for every elliptic curve E/K with $E[2](K) \neq 0$, there exists an infinite subgroup $G' \subset H^1(K, E)[2]$ such that every nonzero element has index two.*

Proof: The first hypothesis ensures that the subgroup G is infinite and the second hypothesis ensures that its image $G' \in H^1(K, E)[2]$ is infinite. The result follows. Note that this is the case $n = 2$ of [11, Theorem 7].

3.2. **Cassels' formula.** Having a convenient description of $H^1(K, E[2])$ as parameterizing kernel sets $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ modulo squares, in order to make the period-index obstruction map explicit we would like to have a formula for the corresponding genus one curve in terms of λ. This is provided by a formula of Cassels. We first introduce some notation: for any $i \neq j$, let $e_{ij} = \theta_i - \theta_j$, and let $\Delta = e_{23}e_{31}e_{12}$. For $1 \leq j \leq 3$, we introduce the new variables $Y_j = X_0 + X_1\theta_j + X_2\theta_j^2$.

Now we have the following formula, which (except for the e_{ij} notation), is taken verbatim from XX:

Theorem 11. *(Cassels) a) Under the bijection $H^1(K, E[2]) \to KS/KS^2$ of Theorem X, the element $C_\lambda \to V$ corresponding to the kernel set $(\lambda_1, \lambda_2, \lambda_3)$ is*

$$\Delta H_0(X_1, X_2, X_3) = \Delta\left(e_{23}\lambda_1 Y_1^2 + e_{31}\lambda_2 Y_2^2 + e_{12}\lambda_3 Y_3^2\right) = 0,$$

$$G_1(X_1, X_2, X_3) - \Delta T^2 = \theta_1 e_{23}\lambda_1 Y_1^2 + \theta_2 e_{31}\lambda_2 Y_2^2 + \theta_3 e_{12}\lambda_3 Y_2^2 - \Delta T^2 = 0,$$

b) Under the same bijection, the map $\iota : E(K)/2E(K) \hookrightarrow H^1(K, E[2])$ is induced by passage to the quotient from

$$(x, y) \mapsto (x - \theta_1, x - \theta_2, x - \theta_3).$$

Remark: We must emphasize that, since Theorems 4 and 6 can be found in the papers of Cassels, it follows that the explicit form of the period-index obstruction map for $n = 2$ is also in essence due to Cassels. It is only the explicit recognition of this formula as giving the Brauer group obstruction to a rational divisor class containing a rational divisor that is new. This is related to the fact that Theorem 6 is usually discussed in the context of 2-descent, where one is interested not in the entire group $H^1(K, E[2])$ but only the Selmer subgroup $S^2 \subset H^1(K, E[2])$ of classes whose image in $H^1(K, E)[2]$ is everywhere locally trivial. But the genus

[3]By allowing M to be the split quadratic algebra $K \times K$, we may include the split case in the discussion as well.

zero curve corresponding to a Selmer class has rational points everywhere locally, hence represents the trivial element of $\mathrm{Br}(K)$ by Hasse's theorem.

In the remainder of this section we work out the consequences of Cassels' formula for the period-index obstruction map. Most importantly, we work out the Galois descent implicit in the change of variables $X_i \mapsto Y_i$ and give, in the split and semisplit cases, explicit formulas for $\Delta(\lambda)$ as a Hilbert symbol.

3.3. **Symmetrized Hilbert symbols and Galois descent.** Recall that if $a,\ b \in K^\times$, the Hilbert symbol $\langle a, b\rangle$ is an element of $Br(K)[2]$.[4] Recall that $\langle a, b\rangle$ can be identified with the obstruction, in $\mathrm{Br}(K)[2]$, to the unique rational divisor divisor class of degree one on the conic curve $V_{a,b} := aX^2 + bY^2 = Z^2$ being represented by a K-rational divisor. Thus as far as the Brauer group is concerned, Hilbert symbols and conic curves are essentially interchangeable.

However, as above, the representation $\langle a, b\rangle$ of the conic $V_{a,b}$ entails a loss of symmetry. Descent arguments in particular will be facilitated if we work instead with *symmetrized* Hilbert symbols: namely, for $a, b, c \in K^\times$, we define $\langle a, b, c\rangle$ to be the class of the conic curve $aX^2 + bY^2 + cZ^2 = 0$; algebraically, we just have

$$\langle a, b, c\rangle = \langle -ac, -bc\rangle.$$

Using this "desymmetrization" the following result is immediate:

Corollary 12. *Let E/K be an elliptic curve with full 2-torsion. The period-index obstruction map $\Delta : H^1(K, E[2]) \to Br(K)$ is given as*

$$(\lambda_1, \lambda_2, \lambda_3) \mapsto \langle e_{31}e_{21}\lambda_1, e_{23}e_{21}\lambda_2\rangle.$$

Remark and acknowledgement: This formula is a sharpening of [**?**, Theorem 6] in the case $n = 2$; there it was only claimed that $\Delta(a, b) := \langle C_1 a, C_2 b\rangle - \langle C_1, C_2\rangle$ for suitable elements $C_1, C_2 \in K^\times/K^{\times 2}$. We now know that $C_1 = e_{31}e_{21},\ C_2 = e_{23}e_{21}$. Note that $\langle C_1, C_2\rangle = \langle e_{31}e_{21}, e_{23}e_{21}\rangle = \langle e_{31}/e_{21}, e_{23}/e_{21}\rangle = 0$ by the Steinberg relation, since $\frac{e_{31}}{e_{21}} + \frac{e_{23}}{e_{21}} = 1$.

In a preliminary draft of [**?**] the obstruction map in the split case was claimed, following [**?**], to be simply $\langle \lambda_1, \lambda_2\rangle$. The referee supplied a counterexample and also was of the opinion that the formula of Corollary 7 as the correct one, noting as supporting evidence that it vanished on the image of the $E[2](K)$ under the Kummer map. At the end of the paper, we give another explanation for the special form of the characters C_1 and C_2 using Mumford's theta groups.

The following remark could have been made in [6]:

Proposition 13. *If $\mathrm{Br}(K)[2] \neq 0$, then there exist genus one curves C/K without K-rational points: indeed, for any elliptic curve E/K with full 2-torsion, we have $H^1(K, E)[2] \neq 0$.*

Proof: By a well-known result of Merkurjev, if $\mathrm{Br}(K) \neq 0$, there exist $a, b \in K^\times$ such that $\langle a, b\rangle \neq 0$ (equivalently, there exists an anisotropic conic over K). Let E/K be any elliptic curve with full 2-torsion: since $\#K > 2$. such curves certainly exist. But by the explicit form of the period-index obstruction map, every conic

[4]For every positive integer n such that $\mu_n \subset K$ there is a modulo n norm-residue symbol $\langle a, b\rangle_n$; since in this paper $n = 2$ always, we omit the subscripted 2 – later we will want to use subscripts to denote localization in the Brauer group of a global field.

V, up to isomorphism, is covered by some principal homogeneous space C over E. Since C covers a curve without K-rational points, it certainly cannot itself have any K-rational points.

Question: Is it true that if K is a field (say of characteristic zero) such that every genus one curve over a finite extension of L/K has an L-rational point, then K has cohomological dimension at most one? Because of the existence of elliptic curves E_p/K admitting full p-torsion over $K(\mu_p)$ for $p = 2,\ 3,\ 5$ (e.g. [**?**]), one has at least $\mathrm{Br}(L)[30] = 0$ for all L/K.

Now assume we are *not* in the split case, and let M be the splitting field of the cubic polynomial $f(T)$.

Proposition 14. *Let $\Lambda = (\lambda_1, \lambda_2, \lambda_3) \in (K(\theta_1), K(\theta_2), K(\theta_3)) \subset M^3$ be a kernel set, and consider the curve*

$$C_\Lambda = \lambda_1 X^2 + \lambda_2 Y^2 + \lambda_3 Z^2 = 0,$$

a priori *defined over M. Then Galois descent by permutation of variables provides a distinguished K-model C of C_Λ.*
b) Suppose $\lambda_3 \in K$, so $M = K(\sqrt{D})$ is a proper quadratic extension of K. Write $N(\lambda) = \lambda\overline{\lambda}$ and $T(\lambda) = \lambda + \overline{\lambda}$, where $\overline{\lambda}$ is the Galois conjugate of $\lambda \in M$. Then the symmetrized Hilbert symbol corresponding to the curve $\lambda X_1^2 + \overline{\lambda} X_2^2 + N(\lambda) X_3^2$ is

$$c(\lambda) = \langle N(\lambda), T(\lambda), D\rangle,$$

which we may (correctly!) regard as trivial if $\mathrm{Tr}(\lambda_1) = 0$.

Proof: The first step is to observe that there is an evident permutation of the variables that leads to descent data on the curve from M to K. In detail: let $G := \mathrm{Gal}_{M/K}$. If we let G act on the variables (X, Y, Z) in the same way that it does on the roots $(\theta_1, \theta_2, \theta_3)$ (and hence also on $(\lambda_1, \lambda_2, \lambda_3)$) – say $(X, Y, Z) \mapsto (X_\sigma, Y_\sigma, Z_\sigma)$ – then by defining

$$\varphi_\sigma : C_\Lambda \to \sigma(C_\Lambda),\ (x, y, z) \mapsto (\sigma(x_{\sigma^{-1}}), \sigma(y_{\sigma^{-1}}), \sigma(z_{\sigma^{-1}}))$$

we get a collection of isomorphisms which satisfy Weil's descent condition $\varphi_{\tau\circ\sigma} = \sigma(\varphi_\tau) \circ \varphi_\sigma$, hence specify a *canonical* model for C over K.

The proof of part b) is a calculation, which is omitted at the moment (but come back and do it!)

Remark: In the cyclic and generic cases one can, of course, get an expression for $\Delta((\lambda_1, \lambda_2, \lambda_3))$ by making the change of variables indicated in Cassels' formula and diagonalizing the resulting ternary quadratic form. However, there does not seem to be any merit in doing this generically either from a computational perspective (one will not, it seems, get a very nice formula) or from a theoretical perspective. Indeed, as far as theory is concerned, we may always reduce to the semisplit case by passing from K to $K(\theta_1)$ – because this is a cubic extension, the restriction map $\mathrm{Br}(K)[2] \mapsto \mathrm{Br}(K(\theta_1))[2]$ is injective, and the K-model of the conic is uniquely determined by its model over $K(\theta_1)$.

4. Cassels' condition

Recall from Section 2.5 Cassels' elliptic curve, given as the intersection of two simultaneously diagonalizable conical quadric surfaces, which had $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. In [2], Cassels explicitly writes down a family of simultaneously diagonalizable conical quadrics C each with Jacobian elliptic curve E (in fact, he shows that E is the Jacobian by giving explicitly the principal homogeneous space structure). He then remarks that if C is any curve in the family, then since the rational divisor classes of degree 2 on C are acted upon simply transitively by $\mathbf{Pic}^0(\mathbb{Q}) = E(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$, there are exactly four rational divisor classes of degree two on C. These are the classes corresponding to the four biconic structures provided by the four conical quadrics in the pencil, so that a rational divisor class will be represented by a rational divisor if and only if the corresponding conic has a $\mathbb{Q}$-rational point. Thus, one needs only to find values of the paramters such that all four Hilbert symbols are nontrivial, which Cassels remarks (but does not prove) can be done in infinitely many ways, and he exhibits one.

Using the results of the preceding section, we can certainly write down an explicit formula for the four quaternion algebras corresponding to the four quadratic cones of a biconic curve $C_\Lambda \in KS/KS^2$ whenever E/K has full 2-torsion. In the notation of the last section, the classes are:

$$c_\Lambda = (e_{21}e_{23}\lambda_2, e_{21}e_{31}\lambda_1)_2. \tag{4}$$
$$c_\Lambda(1) = C_\Lambda + \iota((\theta_1, 0)) = (\lambda_1, e_{32}\lambda_2)_2.$$
$$c_\Lambda(2) = C_\Lambda + \iota((\theta_2, 0)) = (\lambda_2, e_{31}\lambda_1)_2.$$
$$c_\Lambda(3) = C_\Lambda + \iota((\theta_3, 0)) = (e_{12}\lambda_2, e_{21}\lambda_1)_2.$$

Let us say that an elliptic curve satisfies *Cassels' condition* (CC) if it has full 2-torsion and the natural map $E(K)[2] \to E(K)/2E(K)$ is a surjection. Then the following result is a repackaging/generalization of the argument of [2]:

Proposition 15. *Let E/K be an elliptic curve satisfying (CC). Let $\Lambda = (\lambda_1, \lambda_2, \lambda_3) \in H^1(K, E[2])$ be any biconic curve with Jacobian E. Then Λ has index two if and only if one the four Hilbert symbols $c_\Lambda, c_\Lambda(i)(1 \leq i \leq 3)$ is zero in the Brauer group of K.*

In the remainder of this section we will give some applications of this Proposition.

First, if $E(K)$ is a finitely generated abelian group – e.g., if K is a finitely generated field! – then condition (CC) means $E(K)$ is a torsion group with $\#E(K)[4] = \#E(K)[2] = 4$. (Discuss in terms of the generalized Cassels' condition.)

4.1. **WC-groups over $\mathbb{R}$.** We will use Cassels' condition to solve the WCE-problem over $\mathbb{R}$. We stress that the results are very well-known: the computation of $H^1(\mathbb{R}, E)$ is often given as an exercise in texts on elliptic curves (e.g. [17, Exercise 10.7]), and a complete solution can be found in [**?**, SSV.2]. Moreover, since the index of any Galois cohomology class over $\mathbb{R}$ is at most two, and period and index share the same prime divisors, it is clear *a priori* that the period-index problem has an affirmative solution over $\mathbb{R}$. Nevertheless our direct calculation seems enlightening, and serves as a simplest nontrivial prototype for a highly important duality theorem.

First note that every elliptic curve over $\mathbb{R}$ satisfies (CC'). Indeed, $E(\mathbb{R})$ is a compact real-analytic curve, i.e., a disjoint union of finitely many copies of S^1. S^1 is a divisible group, so $E(\mathbb{R})/2E(\mathbb{R}) = \pi_0(E(\mathbb{R}))/2\pi_0(E(\mathbb{R}))$, where π_0 denotes the group of connected components in the usual topological sense (or, if you like, the group of semialgebraic connected components). Just by contemplating the graph of the equation $y^2 = f(x)$ it becomes clear that there is one component if $f(x)$ has one real root (semisplit case) and two components if $f(x)$ has three real roots (split case). (See e.g. [**?**, p. 420] for the relevant picture.) In the split case, we order the roots so that $\theta_1 < \theta_2 < \theta_3$, and then the same picture shows that θ_1 and θ_2 lie in the non-identity component, whereas θ_3 lies in the identity component.

In the semisplit case, the étale algebra $L \cong \mathbb{C} \times \mathbb{R}$, so $H^1(K, E[2]) \cong \mathbb{C}^\times/\mathbb{C}^{\times 2} = 0$; *a fortiori* $H^1(K, E)[2] = H^1(K, E) = 0$.

In the split case, Prop. XX tells us that $H^1(K, E) \neq 0$. To confirm this, $H^1(K, E[2]) \cong (\mathbb{R}^\times/\mathbb{R}^{\times 2})^2$, so has order four, so by the exactness of the Kummer sequence $H^1(K, E)[2]$ has order two. This is a case where (CC) holds, so to compute the index of the curve underlying the class $(\lambda_1, \lambda_2) \in H^1(K, E[2])$, we look at the Hilbert symbols $c_\Lambda = (\lambda_2, \lambda_1)$ and $c_\Lambda(1) = (-\lambda_2, \lambda_1)$. We see that the two classes $(\pm 1, 1)$ lie above the trivial element of $H^1(K, E)[2]$ and the classes $(\pm 1, -1)$ lie above an element of $H^1(K, E)[2]$ which must be nontrivial, since it covers an anisotropic conic curve.

These considerations can be recast as follows: the Kummer sequence

$$0 \to E(K)/2E(K) \to H^1(K, E)[2] \to H^1(K, E)[2] \to 0$$

is a short exact sequence of $\mathbb{Z}/2\mathbb{Z}$-modules, so of course it splits, in general in many different ways. However, when $K = \mathbb{R}$, we showed that for each $\eta \in H^1(K, E)[2]$, there exists a *unique* lift to an element with trivial period-index obstruction: this defines a canonical splitting, and then Δ induces a perfect pairing

$$\Delta : H^1(K, E)[2] \times E(\mathbb{R})/2E(\mathbb{R}) \to \mathrm{Br}(\mathbb{R})[2] = \mathbb{Z}/2\mathbb{Z}.$$

In turn, we can regard this as a Pontrjagin duality between $\widehat{E(\mathbb{R})}$ (where for any group G, $\hat{G}$ denotes its profinite completion) and $H^1(\mathbb{R}, E)$.

The point is that this last statement is true for any locally compact field K, a very important fact which might be called the Tate-Lichtenbaum-Milne duality theorem.

4.2. **Some WC-groups over $\mathbb{R}((t))$.** In this section we will solve the WCE-problem for certain elliptic curves over the field $K = \mathbb{R}((t))$. In particular, we find that the period-index problem for elliptic curves over K does *not* always have an affirmative solution. This is perhaps a bit surprising, since over the quadratic extension field $L = \mathbb{C}((t))$, WC-groups of elliptic curves are admirably well-behaved. Indeed, the calculation of $H^1(L, E)$ was achieved 40 years ago by Ogg and Shafarevich (independently): it is $(\mathbb{Q}/\mathbb{Z})^a$, where $a = 2$ if E has good reduction, $a = 1$ if E has multiplicative reduction and $a = 0$ when E has additive reduction. Since L has vanishing Brauer group (CITE), O'Neil's period-index obstruction map Δ vanishes identically, so period equals index for all classes in $H^1(L, E)$. Moreover, the

structure of the field L is very simple: its algebraic closure is the field of Puiseux series $\bigcup_{n=1}^{\infty} \mathbb{C}((t^{1/n}))$ and $G_L = \hat{\mathbb{Z}}$, with a topological generator σ which carries $t^{1/n} \mapsto \zeta_n t^{1/n}$. It follows that there is a solution to the "WCE problem" over K: for each finite extension L_n/L, we know $H^1(L_n, E)$ and the restriction map $H^1(L, E) \to H^1(L_n, E)$ is just n times the natural inclusion $(\mathbb{Q}/\mathbb{Z})^a \hookrightarrow (\mathbb{Q}/\mathbb{Z})^{a_n}$.[5]

In contrast, fields like $K = \mathbb{R}((t))$ – i.e., of *virtual* cohomological dimension one – have come to be studied much more recently, via work of Colliot-Théléne, Ducros and (especially) Scheiderer. The computation of WC-groups of all abelian varieties over K was achieved by [**?**], using not only the above (rather elementary, by 21st century standards) results of Ogg and Shafarevich over L, but also much deeper results of Scheiderer. Naturally enough, Ducros' description of $H^1(K, E)$ depends on the Néron special fibre of E: there are altogether 16 cases, including 5 in which $H^1(K, E) = 0$. Here we will handle the two cases of good reduction, for which (CC') is verified. Our argument applies verbatim to the case where the connected component of the Néron special fibre is an anisotropic torus and the component group is μ_2. The other cases can be handled as well with the methods of this paper (although in some cases one needs to translate by a torsion point of higher order).

Theorem 16. *Let E/K be an elliptic curve with good reduction. Then all elements of $H^1(K, E)$ have period equals index if and only if $\#E[2](K) = 2$.*

Proof: Since E has good reduction, we may choose a defining equation of the form $y^2 = (x - \theta_1)(x - \theta_2)(x - \theta_3)$ where $\theta_1,\ \theta_2,\ \theta_3$ lie in the valuation ring $\mathbb{R}[[t]]$ of t. The field K is formally real and has precisely two orderings, one in which t is infinitesimal and positive, and one in which t is infinitesimal and negative; we choose the former, and assume that the roots are ordered so that $\theta_1 < \theta_2 < \theta_3$. (For either choice, the reduction map is order-preserving.) By Hensel's Lemma, f has the same number of rational roots as does its reduction, so by the last subsection we are either in the semisplit or the split case.

We will use the following results of Ducros: in the semisplit case $H^1(K, E) \cong \mathbb{Q}/\mathbb{Z}$, and in the split case $H^1(K, E) \cong \mathbb{Q}/\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2$. In either case, the $\mathbb{Q}/\mathbb{Z}$ factor is isomorphic under the restriction map to $H^1(L, E)^G_{L/K}$.

The equality of period and index in the semisplit case follows immediately from this: indeed, for any positive integer n we have a commutative diagram

$$H^1(\mathbb{R}((t)), E)[n] \hookrightarrow H^1(\mathbb{C}((t)), E)[n]$$

$$H^1(\mathbb{R}((t^{\frac{1}{n}}))), E[n] \hookrightarrow H^1(\mathbb{C}((t^{\frac{1}{n}})), E)[n]$$

where the two horizontal arrows are the restriction maps. As discussed above, the right vertical arrow is the zero map, hence by commutativity so is the left vertical map.

It remains to understand the $(\mathbb{Z}/2\mathbb{Z})^2$ factor in the split case, but we start the discussion anew in $H^1(K, E)[2]$ and this part of the proof does not use any of the

[5]This reverses the argument of Ogg and Shafarevich – they showed directly that $H^1(L, E)$ behaves functorially as above, and deduced the affirmative answer to the period-index problem.

cited results. First, we claim that $E(K)/2E(K)$ is, again, equal to 1 in the semisplit case and 2 in the split case. Indeed, we have an exact sequence

$$0 \to E^0(K) \to E(K) \stackrel{\mathcal{R}}{\to} \tilde{E}(\mathbb{R}) \to 0,$$

where $\mathcal{R}$ is the reduction map and $E^0(K)$ is the kernel of reduction, which is a standard K-analytic group in the sense of [**?**]: that is, it is obtained by plugging points of the maximal ideal $t\mathbb{R}[[t]]$ into a formal group law over $\mathbb{R}$. By the known structure of standard groups, $E^0(K)$ is uniquely n-divisible for all positive integers n. It follows immediately that $E(K)/2E(K) \cong \tilde{E}(\mathbb{R})/2\tilde{E}(\mathbb{R})$. Just as in the previous subsection, in the split case, a representative for the nontrivial element of $E(K)/2E(K)$ is given by either of the torsion points $(0, \theta_1)$ or $(0, \theta_2)$.

In order to compute $H^1(K, E[2])$, observe that G_K is the profinite completion of the infinite dihedral group $D_\infty = \langle \sigma, \tau \mid \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$. Here σ is the above automorphism of the Puiseux series field and τ is the automorphism which acts as complex conjugation on each of the coefficients of a Puiseux series. It follows that $G_K^{ab} \cong (\mathbb{Z}/2\mathbb{Z})^2 \cong K^\times/K^{\times 2}$, with representatives for the four square classes being $\{1, -1, t, -t\}$. So in the split case we have $H^1(K, E[2]) \cong X(G_K)^2 \cong (\mathbb{Z}/2\mathbb{Z})^4$, so $H^1(K, E)[2] \cong (\mathbb{Z}/2\mathbb{Z})^3$. In the nonsplit case, base change to L splits the reduction of f, hence f itself, so that the cubic algebra $A \cong K \otimes L$ and $H^1(K, E[2]) \cong L^\times/L^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$, and $H^1(K, E)[2] \cong \mathbb{Z}/2\mathbb{Z}$.

From now on we look only at the split case. Note that the duality of the previous section no longer holds: $E(K)/2E(K)$ has fewer elements than $H^1(K, E)[2]$. Also $Br(K) \cong Br(\mathbb{R}) \oplus X(\mathbb{R}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ (cite), with all four classes being given by quaternion algebras. Indeed, $(-1, -1)_2$, $(t, t)_2$, $(-t, -t)_2$ represent three nontrivial classes, which are distinct since $K(\sqrt{t})$ splits only the second class and $K(\sqrt{-t})$ splits only the third class. (What we have shown is that period equals index in $\mathrm{Br}(K)$ – in general, the quaternion algebras generate $\mathrm{Br}(K)[2]$ but need not form a subgroup.) Thus, of the eight elements of $H^1(K, E[2])$ at least four must have nontrivial obstruction, since the image of $\Delta(H^1(K, E[2])$ is always the set of all Brauer group elements represented by quaternion algebras. But it is still conceivable that modification of each of these four classes by the nontrivial element of $E(K)/2E(K)$ gives a class with trivial obstruction.

However, we now apply Proposition XX to show that this is not the case. Indeed, the two symbols that we need to look at are $c_\Lambda = (-e_{21}e_{32}\lambda_2, e_{21}e_{31}\lambda_1)_2$ and $c_\Lambda(1) = (\lambda_1, e_{32}\lambda_2)_2$. By making the change of variables $\lambda_2' = e_{32}\lambda_2$, we may look instead at $(-e_{21}\lambda_2', e_{21}e_{31}\lambda_1)_2$ and (λ_1, λ_2'). Now e_{21} and e_{31} are both positive, so they are either in the same squareclass, or their squareclasses differ by t. In the first case, we get the symbols (λ_1, λ_2') and $(-e_{21}\lambda_2', \lambda_1)$. If $e_{21} \equiv e_{31} \equiv 1$, take $(\lambda_1, \lambda_2') = (-1, t)$ and both symbols are nontrivial. If $e_{21} \equiv e_{31} \equiv t$, take $(\lambda_1, \lambda_2') = (t, -1)$. If $e_{21} \equiv 1$ and $e_{31} \equiv t$, take $(\lambda_1, \lambda_2') = (-1, t)$, and if $e_{21} \equiv t$, $e_{31} \equiv 1$, take $(\lambda_1, \lambda_2') = (-t, -1)$. This completes the proof of the theorem.

Remark: A similar case-by-case analysis reveals that there is always only one element C_1 of period two and index four. Moreover, there is always exactly one element C_2 of $H^1(K, E)[2]$ which, despite being nontrivial, does not cover any anisotropic

conic; combining with the element $C_3 \in \mathbb{Q}/\mathbb{Z}$, we get a $\mathbb{Z}/2\mathbb{Z}$-basis for $H^1(K,E)[2]$. (In fact, a moment's thought reveals that such elements will always exist when E is split and $\#E(K)/2E(K) < \#K^\times/K^{\times 2}$, since in this case not all of the elements $(1,\lambda_2) \in H^1(K,E[2])$ can represent the trivial class.) To solve the WCE-problem completely (in the good reduction case), we must specify which quadratic extensions split these classes. By definition of index four, no quadratic extension splits C_1. [**?**, Lemme, p. 316] shows that $K(\sqrt{t})$ and $K(\sqrt{-t})$ split only C_3; by construction, C_3 is not split by $K(\sqrt{-1})$; and finally, since C_2 has index two, it *must* be split by $K(\sqrt{-1})$.

5. The proof of the Main Theorem

In this section, K is either a number field or one-variable function field over a finite field whose characteristic is different from 2,

$$E/K : y^2 = f(x) = (x-\theta_1)(x-\theta_2)(x-\theta_3)$$

is an elliptic curve, and A is the cubic algebra $K[x]/(f)$.

We want to prove the existence of infinite subgroups $G_1,\ G_2 \subset H^1(K,E)[2]$ such that each element of G_1 has index 2 and each nonzero element of G_1 has index 4. The existence of G_1 in the split case $A = K \oplus K \oplus K$ was handled in [**?**], whereas the existence of G_2 in this case (viewed as a special case of the semisplit case) is Proposition 5, which is itself a special case of a result of Lang and Tate. It remains to show the existence of G_1 in the semisplit case and the existence of both subgroups in the cyclic and generic cases. We proceed by a separate analysis of each of the remaining cases.

5.1. **The semisplit case.** We take θ_3 to be rational and write $A = L \oplus K$. Recall that in this case $L^\times/L^{\times 2} \cong KS/KS^2 \cong H^1(K,E[2])$, so that the symmetric Hilbert symbol of the element corresponding to $\lambda \in L^\times$ is $\langle \lambda_1, \lambda_2, N(\lambda_1)\rangle$ as an element of the Brauer group of L. Here we are using the notation $\lambda_1 = \lambda,\ \lambda_2 = \overline{\lambda_1},\ N(\lambda_1) = \lambda_1\lambda_2$, where the overbar denotes the nontrivial Galois automorphism of L/K.

Note well that the explicit Galois descent of Section X.X is not needed here: what we shall be showing is that certain symmetric Hilbert symbols which are in fact defined over K are nonvanishing upon restriction to the Brauer group of L; *a fortiori* they are nonvanishing in $\mathrm{Br}(K)$!

The content of the theorem in this case resides essentially in the following lemma, which we will state and prove first, and then use it to deduce the existence of G_1.

Lemma 17. *Let $H \subset KS/KS^2 \cong L^\times/L^{\times 2}$ be a finite subgroup. Then there exists an infinite subgroup $G \subset KS/KS^2$ with the property that for every $h \in H$ and every $1 \neq g \in G$, $\langle h_1 g_1, h_2 g_2\rangle_2$ is nonzero in $Br(L)$.*

Proof: We build the subgroup $G = \bigcup_n G_n$ inductively as the union of a sequence of subgroups of order 2^n. The basic idea is to present a fairly robust procedure for producing infinite *subsets* of elements g satisfying the condition of the lemma. We take G_1 to be the subgroup generated by one such element, and then enlarge H to H_2, the subgroup generated by H and by the first element g, then use the procedure to give ourselves a second element g_2. The point of this is that it is then automatic that g_2 is $\mathbb{F}_2$-linearly independent from the subgroup generated by g_1

and that $g_1 + g_2$ is also an element satisfying the desired nontriviality upon modification by elements of $H = H_1$. Then we add the third element g_3, and so on.

Let Π_1, Π_2 be a Galois-conjugate pair of elements of L such that (Π_1), (Π_2) are prime ideals of L; these principal ideals lie over the principal prime ideal $(\Pi_1\Pi_2) = (\pi)$ of K. We take $g_1 = u_1\Pi_1$, where $u_1 \in L^\times$ is to be determined. The Hilbert symbol in question is then

$$\langle h_1 g_1, h_2 g_2\rangle_2 = \langle h_1, h_2\rangle_2\langle h_1, u_2\Pi_2\rangle_2\langle h_2, u_1\Pi_1\rangle_2 \cdot \langle u_1, u_2\rangle_2\langle u_1, \Pi_2\rangle_2\langle u_2, \Pi_1\rangle_2\langle \Pi_1, \Pi_2\rangle_2.$$

By a suitable choice of π and u_1, we will arrange for this quantity to be nontrivial even in $Br_\pi(L)[2]$, which we define to be the projection of the global Brauer group onto $Br(L_{\Pi_1}) \oplus Br(L_{\Pi_2})$. We will only consider principal prime ideals (π) of K which split in L, whose residue characteristic is odd, such that (for all $h = h_1$ in H) $h_1 h_2$ is a unit in K_π, and for which h_1 is a square in L_{Π_1} (hence also h_2 is a square in L_{Π_2}). A moment's thought gives that each of these conditions either excludes finitely many primes or can be enforced by requring π to split in a sufficiently large finite extension of K. Hence by Cebotarev such primes π have positive density, and there are infinitely many.

These choices imply that the first three Hilbert symbols appearing in the right-hand side of the above equation vanish, so we are left to evaluate $\langle u_1, \Pi_2\rangle_2\langle u_2, \Pi_1\rangle_2\langle \Pi_1, \Pi_2\rangle_2$. Now if $\langle \Pi_1, \Pi_2\rangle_2$ is nonzero in $\mathrm{Br}_\pi(L)$, we may take $u_1 = u_2 = 1$ to get the desired nontriviality. If on the other hand this symbol is trivial (obviously it will be trivial at Π_1 iff it is trivial at Π_2), then we are looking at the expression $\langle u_1, \Pi_2\rangle_2\langle u_2, \Pi_1\rangle_2$, which is nontrivial in $\mathrm{Br}_\pi(L)$ iff $\langle u_1, \Pi_2\rangle_2$ is nontrivial in $\mathrm{Br}(L_{\Pi_2})$. But by the well-known explicit computation of the Hilbert symbol at a non-dyadic place, we just want u_1 to be a quadratic nonresidue modulo Π_2, which – since for any completion of a global field M at a place v, the natural map $M^\times \to M_v^\times / M_v^{\times 2}$ is surjective – we may certainly take it to be. Thus we have, for each of an infinite set of primes π of K, found an element $g = g_1$ of L such that $\langle g_1 h_1, g_2 h_2\rangle_2 \neq 0 \in \mathrm{Br}(L)$ for all $h = h_1 \in H$. Enumerating such a sequence of primes $\pi_1, \pi_2, \ldots$ and applying the inductive argument at the beginning then proves the lemma.

Remark: The element u is a "fudge factor" which keeps us from having to explicitly evaluate the symbol $\langle \Pi_1, \Pi_2\rangle_2$. Presumably the set of primes π of K satisfying the above conditions and such that this symbol is nontrivial has positive density, but showing this seems to be more trouble than it's worth.

Now to prove the theorem, recall the fundamental fact that $E(K)/2E(K)$ is finite. Let $H \subset KS/KS^2$ be any finite subgroup containing H, $e_{23}e_{21}$, and $e_{31}e_{21}$. (As we shall briefly remind the reader at the end of this section, for "effectivity" it would be best to assume that H contains not just $E(K)/2E(K)$ but the complete preimage of $Ш(K, E)[2]$, i.e., the 2-Selmer group.) Then for each $1 \neq g \in G$ and $h \in H$, $\Delta(gh) \neq 0$, so that nontrivial elements of G have index four. This completes the proof of the theorem in the semisplit case.

5.2. **The cyclic case.** Here $A = L$ is a Galois cubic extension of K. In this section N always stands for the norm from L to K. This time for an element $\lambda \in L$, we write $\lambda_1 = \lambda,\ \lambda_2,\ \lambda_3$ for the $\mathfrak{g}_{L/K}$-conjugates of λ. Again we are content to consider

elements of $H^1(K, E[2]) = KS/KS^2$ only upon restriction to L. Since we now have that $[L : K]$ is odd, restriction to L is injective from $\mathrm{Br}(K)[2] \to \mathrm{Br}(L)[2]$; thus nothing is lost in considering the class of a kernel set $(\lambda_1, \lambda_2, \lambda_3)$ in $\mathrm{Br}(L)$.

The condition on λ that it be "the λ_1" of a kernel set is now that $N(\lambda) \in K^{\times 2}$. Notice that, for an arbitrary field K, it is not so clear how to find kernel sets, or even how many there are. Thus the following construction depends more strongly on the fact that K is a global field than the semi/split cases.

Namely, consider generators π of principal prime ideals of K which split (necessarily completely) in L: $\pi = \Pi_1\Pi_2\Pi_3$. Then elements of the form $\lambda_1 = \Pi_1\Pi_2$ give rise to kernel sets, since $N(\lambda_1) = \pi^2$. Again such primes have positive density, so at least we know that $H^1(K, E[2])$ is infinite. We prove now exactly the same lemma as in the quasisplit case.

Lemma 18. *Let $H \subset KS/KS^2 \cong H^1(K, E[2])$ be a finite subgroup. Then there exists an infinite subgroup $G \subset KS/KS^2$ with the property that for every $h \in H$ and every $1 \neq g \in G$, $\langle -h_1h_3g_1g_3, -h_2h_3g_2g_3\rangle_2$ is nonzero in $Br(L)$.*

Proof: As we are working over L, we may view H as a subgroup of $L^\times/L^{\times 2}$ (the restriction map is injective). By replacing H by the larger subgroup generated by pairs of elements of the form $\pm h_j, 1 \leq j \leq 3$, we are reduced to finding elements $(g_1, g_2, g_3) \in KS/KS^2$ such that for all $h, h' \in H$, $\langle hg_1g_3, h'g_2g_3\rangle_2$. Taking $g_1 = u_1\Pi_1\Pi_2$ for some $u_1 \in KS/KS^2$ which is a local unit at Π_1, and restricting only to primes π of odd characteristic and at which each $N(h), N(h')$ is a local unit at π and a square in $K^\times$, the Hilbert symbol $\langle hu_2\Pi_2\Pi_3, h'u_1\Pi_1\Pi_3\rangle$ can be decomposed in the "semi-localized Brauer group" $\mathrm{Br}_\pi(L) = \bigoplus_{i=1}^3 \mathrm{Br}(L_{\Pi_i})$ as:

$$\langle hg_1, h'g_2\rangle_2 = \langle u_2, \Pi_1\Pi_3\rangle_2\langle u_1, \Pi_2\Pi_3\rangle_2\langle \Pi_1\Pi_3, \Pi_2\Pi_3\rangle_2.$$

Let $\epsilon = \langle \Pi_1\Pi_3, \Pi_2\Pi_3\rangle_{\Pi_2}$. Since the product $\langle u_2, P_1P_3\rangle\langle u_1, P_2P_3\rangle$ localized at Π_2 is $\langle u_1, P_2\rangle_{\Pi_2}$, it is enough to choose $u_1 \in KS/KS^2$ such that $\langle u_1, \Pi_2\rangle_{\Pi_2} = -\epsilon$. Suppose q is a principal prime ideal of K which splits into $Q_1Q_2Q_3$ in L and such that $\langle Q_1, \Pi_2\rangle_{\Pi_2} = 1$ and $\langle Q_1, P_1\rangle_{\Pi_1} = -\epsilon$. Then also $\langle Q_2, P_2\rangle_{\Pi_2} = -\epsilon$, so $\langle Q_1Q_2, \Pi_2\rangle_{\Pi_2} = -\epsilon$.

It is not hard to see that the conditions imposed on q are incompatible only if $L(\sqrt{\Pi_2})$ is contained in the Hilbert class field of L. This eliminates only finitely many primes π, so we are left with a set of primes of positive density for which such an element $u_1 = Q_1Q_2$ exists to make all the Hilbert symbols nontrivial. The remainder of the proof of the lemma is the same as above.

5.3. **The generic case.**

THIS SECTION STILL NEEDS TO BE WRITTEN!

References

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

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

[3] J. W. S. Cassels. *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), 193-291.
[4] J.-P. Serre, *Cohomologie Galoisienne*, Fifth edition. Lecture Notes in Mathematics 5, Springer-Verlag, 1994.
[5] J.-P. Serre. *Corps Locaux*, Hermann, Paris, 1962.
[6] P.L. Clark, *The period-index problem in WCI groups I: elliptic curves*, J. Number Theory 114 (2005), 193–208.
[7] P.L. Clark, *The period-index problem in WC-groups II: abelian varieties*, submitted.
[8] P.L. Clark, *On the indices of curves over local fields*, Manuscripta Math. 124 (2007), no. 4, 411-426.
[9] T.A. Fisher, *The invariants of a genus one curve*, to appear, Proc. London Math. Soc.
[10] R. Kloosterman. *The p-part of Shafarevich-Tate groups of elliptic curves can be arbitarily large*, preprint available at `http://www.arXiv.math.NT/0303143v1`.
[11] S. Lang and J. Tate. *Principal homogeneous spaces over abelian varieties*, Amer. J. Math (80), 1958, 659-684..
[12] S. Lichtenbaum. *The period-index problem for elliptic curves*, Amer. J. Math. (90), 1968, 1209-1223.
[13] J. Milne. *Weil-Châtelet groups over local fields*, Ann. Sci. École Norm. Sup. 3 (1970), 273-284.
[14] D. Mumford. *On the equations definining abelian varieties. I.* Invent. Math. (1) 1966, 287-354.
[15] C.H. O'Neil. *The period-index obstruction for elliptic curves*, J. Number Theory 95 (2002), 329-339.
[16] R. Sharifi. *Twisted Heisenberg representations and local conductors*, 1999 Chicago Thesis, available at `http://abel.math.harvard.edu/~sharifi`.
[17] J. Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics 106, Springer-Verlag, 1986.

1126 Burnside Hall, Department of Mathematics and Statistics, McGill University, 805 Sherbrooke West, Montreal, QC, Canada H3A 2K6
E-mail address: `clark@math.mcgill.ca`