LECTURES ON PERIOD-INDEX PROBLEMS

PETE L. CLARK

These are the notes for an April XX, 2006 lecture given (by me) at the Mathematical Sciences Research Institute on the subject of period-index problems. There is, however, significantly more detail and ancillary material – I imagine the notes for the lecture itself as being written on paper with very ample margins, and these notes contain the marginalia. But these are still much more lectures notes than monograph: maintaining the above metaphor, we often we make recourse to "Fermat's excuse" (including for material that does not yet exist in written form!).

Some history

Period-index problems have been around for a long time: at least since the 1930's in the case of division algebras, and at least since the 1950's in the case of torsors under a commutative algebraic group. It is remarkable to note how tightly bound period-index problems once were to the mathematical mainstream: the work on division algebras of (e.g.) Nakayama, Albert, Brauer, Hasse and Noether is clearly one of the mathematical highlights of the early 20th century, and their work on Brauer groups of local and global fields cuts to the heart of classfield theory. And again, period-index problems for torsors were studied in the same papers which developed the foundations of Galois cohomology of abelian varieties: papers of Shafarevich, Ogg, Cassels, Lang and Tate. By the 1960's the focus had shifted, as locally trivial torsors over global fields became of most interest. In the late 1960's Lichtenbaum wrote two beautiful papers on the case of curves over p-adic fields, which however seemed to bring the study to a close.

It seems that almost 30 years passed without much work on either aspect of the problem. Then in 1997 Saltman published a paper on division algebras over function fields of p-adic curves. In 2002, de Jong showed that period equals index in the function field of a surface over an algebraically closed field (with some characteristic restrictions that have recently been removed). There is now what might be called (not too unfairly, I hope) a "de Jong school" which approaches period-index problems in the Brauer group of function fields using highly sophisticated algebro-geometric methods (deformation theory, stacks, moduli of vector bundles and twisted sheaves...), and thanks to work of de Jong, Graber, Mazur, Star and Lieblich, this is becoming one of the hot areas of algebraic geometry.

In 1999, the period-index problem in curves of higher genus returned triumphantly in the paper of Poonen and Stoll, who ultimately found the possible discrepancy between period and index among the various completions of a curve over a global to be responsible for the phenomenon that the order of the Shafarevich-Tate group of a Jacobian need not be a perfect square, not withstanding the fact that it admits a perfect skew-symmetric (but not necessarily alternating!) pairing. Quite recently, Liu, Lorenzini and Raynaud used the work of Poonen and Stoll, among other things, to show that the Brauer group of a surface over a finite field, if finite, is always a perfect square. The proof is amazing: they bring in the local factors of Poonen and Stoll whose parity determines whether or not the Shafarevich group of the Jacobian of a certain relative curve, and they find *another* set of local factors of the same parity as those of Poonen and Stoll. (Ironically, one can find in the literature claims that the Ш of the Jacobian is always a square and that the Ш of a surface is not.) This is all rather curious and surely deserves some sort of explanation.

In the late 90's, H. Lenstra assigned his student William Stein the problem of answering the question of Lang and Tate: do there exist genus one curves over $\mathbb{Q}$ of every index? Using Kolyvagin's Euler system, Stein was able to give an affirmative answer as long as the index was not divisible by 8. Stein, of course, went on to write a thesis concerned with explicit approaches to modular forms and modular abelian varieties, and among his interests is the prospect of "visualizing Ш in abelian varieties" (a notion due to Barry Mazur). Around the same time, Catherine O'Neil wrote her Harvard thesis (under the direction of Mazur) on matters related to explicit higher descents on elliptic curves, a topic which in the last ten years has become a flourishing branch of number theory.[1] In particular, O'Neil wrote a paper introducing the **period-index obstruction map**, which opened up a new approach.

I had the good fortune to be at Harvard[2] at the same time as Stein and O'Neil (who was later at MIT). When I heard Stein lecture about visibility dimension of abelian varieties, he mentioned that a theorem of Cassels gives the best general bound on the visibility dimension of a locally trivial curve of genus one (and in particular better than the bound one gets for an arbitrary curve of genus one). O'Neil's work gives an especially perspicuous proof of Cassels' theorem, and it occurred to me that if only one had an abelian variety version of O'Neil's obstruction map, one could get a bound for the visibility dimension of locally trivial torsors of higher-dimensional abelian varieties which is better than the bound of Agashe-Stein for not-necessarily locally trivial torsors.

From such inauspicious beginnings (it is not clear that anyone, myself included, really cares about this improved bound on the visibility dimension) I became interested in this sort of problem. Not long after, Stein remarked to me that given a genus one curve over a number field K of period p and index p^2, one can produce a locally trivial class of exact order p in a degree p extension field L of K. By producing such "period-index violations" in a systematic way when E has full p-torsion, I was able to show that there exist elliptic curves defined over number fields of degree at most $2p^3$ whose Shafarevich-Tate groups have arbitrarily large

[1] Among other things, Cathy first taught me not to say "elliptic curve" when you mean "curve of genus one."

[2] Indeed, Barry Mazur was also my thesis advisor; my thesis, however, was on Shimura curves. In the one conversation I remember having with Barry about curves of genus one, he mentioned that he believed that every genus one curve over $\mathbb{Q}$ should have a point over a metabelian extension, for reasons having to do with Kolyvagin systems. This was, I think, in late 2002, so probably he was describing Mirela Ciperiani's thesis work!

p-torsion. This improved upon a recently posted preprint of R. Kloosterman.

I have spent the last few years thinking about the period-index problem in higher-dimensional abelian varieties. My work builds upon the classical work of Lang-Tate and Cassels, and especially on the duality theory due originally to Tate and recast in terms of the period-index problem by Lichtenbaum, van Hamel and myself. It seems that van Hamel and I are the only ones currently working on the period-index problem for torsors under higher-dimensional abelian varieties. The primary goal of these lectures is to situate the period-index problem for torsors under abelian varieties relative to the period-index problems on curves and the period-index problem in the Brauer group, and to explain especially what new features and difficulties the higher-dimensional case brings. I am interested but not expert in period-index problems for curves of higher genus and in Brauer groups, so my hope is that by explaining the part of the picture that I best understand, experts in these other areas may be able to perceive more clearly the connections.

Let K be a field of characteristic $\operatorname{char}(K)$, with *separable* algebraic closure $\overline{K}$ and absolute Galois group $\mathfrak{g}_K$. We assume that all varieties over K are nonsingular, quasiprojective and geometrically integral.

1. The two kinds of period-index problems

1.1. **Cohomological period-index problems.** Let G be a $\mathfrak{g}_K$-module (i.e., a *commutative* group endowed with an action of $\mathfrak{g}_K$ continuous for the discrete topology on G and the profinite topology on $\mathfrak{g}_K$), i a positive integer, and $\eta \in H^i(K,G)$ a Galois cohomology class. Define respectively the **period** and **index**

$$P(\eta) = \#\langle \eta \rangle.$$

$$I(\eta) = \gcd\{[L:K] \mid \eta|_L = 0\}.$$

Fact 1.
a) $P \mid I$.
b) $I \mid P^\infty$ (i.e., $\exists\ \alpha$ such that $I \mid P^\alpha$.)

Proof: This is classical; see e.g. [**?**, Prop. 11].

The period-index problem is then: what can be said about the α (for fixed η, as η varies in a fixed group $H^i(K,G)$, or as G varies in some family)? Especially, when can we take $\alpha = 1$?

Variant: define

$$M(\eta) = \min\{[L:K] \mid \eta|_L = 0\}.$$

Evidently $I \mid M$, but there is no reason to expect $I = M$ in general.

Problem 1*: Find an explicit example of a class η with $I \neq M$.

Nevertheless we have

$$M = 1 \iff I = 1 \iff P = 1 \iff \eta = 0. \tag{1}$$

Fact 2. *Suppose G is finite, and $\eta \in H^1(K,M)$. Then $M(\eta) \leq \#G$ and $I(\eta) \mid \#G$.*

Proof: This is due to Lenstra; see [**?**, Prop. 12].

So far so good, so general, and so unmotivated (*si francais*?). To come back down to earth, take G to be a commutative algebraic group.

Example 1.1.1: The group $H^1(K,G)$ parameterizes torsors X under G in the category of varieties. We will revisit this example in the next section; the case of $G = A$ an abelian variety will be our primary focus in these lectures. Note that unipotent groups are acyclic for Galois cohomology, so the most general *connected* commutative group that we would need to consider is a semi-abelian variety.

Example 1.1.2: $H^2(K,\mathbb{G}_m) = \mathrm{Br}(K)$, the Brauer group of K. Here $I(\eta) = M(\eta)$ is interpreted as $\sqrt{[D:K]}$, where D is the unique division algebra representative of η, and P is the least n such that $D^{\otimes n}$ is a matrix algebra.

Definition: For a non-negative integer α, we say that a field K has property $\mathrm{Br}(\alpha)$ if for any finite extensions L/K and any $\eta \in \mathrm{Br}(L)[P]$, $I(\eta) \mid P^\alpha$. (We will say that a field has property $\mathrm{Br}(-1)$ if it is separably closed.)

Remark X.X.X: The property $\mathrm{Br}(\alpha)$ is preserved upon passage to algebraic field extensions.

Remark X.X.X: The property $\mathrm{Br}(0) \setminus \mathrm{Br}(-1)$ is equivalent to "dimension one" in the sense of Serre.

Fact 3. *The following fields have the property* $\mathrm{Br}(0)$*:*
a) $\mathbb{F}_p$.
b) $\overline{k}(t)$.
c) A complete discretely valued field (CDVF) with algebraically closed residue field.
d) A pseudoalgebraically closed (PAC) field.

In fact it is known that each of these fields has the property C_1, except possibly for a PAC field of positive characteristic.

Fact 4. *The following fields have the property* $\mathrm{Br}(1)$*:*
a) $\mathbb{R}$.
b) A CDVF whose residue field is $\mathrm{Br}(0)$ *(e.g.* $\mathbb{Q}_p$, $\mathbb{F}_p((t))$*).*
c) $\mathbb{Q}$, $\mathbb{F}_p(t)$.
d) $\overline{k}(t_1,t_2)$.

Conjecture 1. *If k is* $\mathrm{Br}(\alpha)$ *and K/k has transcendence degree* 1*, then K is* $\mathrm{Br}(\alpha+1)$.

Remark: For a finitely generated field K, let $\dim(K)$ denote its Kronecker dimension: one more than the absolute transcendence degree in characteristic zero, and precisely the absolute transcendence degree in positive characteristic). Thus the problem asks whether K is $\mathrm{Br}(\dim(K))$. It has been known since Nakayama that K is not $\mathrm{Br}(\dim(K)-1)$.

Remark: A special case of the conjecture predicts that a field with property $C_{\alpha-1}$

has property Br(α) (cf. Lieblich).

Remark: The conjecture is known when $k = \mathbb{F}_p(t)$ (a C_2 field) by work of Lieblich and when $k = \mathbb{Q}_p$ (which is not C_α for any α) by work of Saltman. The most notable outstanding case is $k = \mathbb{Q}$ (and I would be interested to hear whether the experts believe the conjecture in this case).

Remark: Merkurjev has constructed fields of cohomological dimension 2 which are not Br(α) for any α, but they are of infinite absolute transcendence degree.

Summary: For any Galois cohomology class, we have a well-defined period and index. The former quantity seems more natural, and the latter seems more mysterious.

1.2. **Geometric period-index problems.**

Let $V_{/K}$ be a variety. We define its **index** $I(V)$ to be the least positive degree of a K-rational 0-cycle. Equivalently, it is the cardinality of the cokernel of the map $\deg : CH_0(X) \to \mathbb{Z}$, and also the gcd of $[L : K]$ such that $V(L) \neq \emptyset$.

To define the period, we need to recall that there exists a variety $\mathbf{Alb}^1(V)$ which is a torsor under a semiabelian variety $\mathbf{Alb}^0(V)$, and a morphism $V \to \mathbf{Alb}^1(V)$ which is universal for morphisms into semiabelian torsors. In particular, $\mathrm{Alb}^1(V)$ corresponds to a class $\eta_V \in H^1(K, \mathbf{Alb}^0(V))$, and we define the **period** of $P(V)$ to be the period of $P(\eta_V)$.

For the remainder of these notes we will content ourselves with the case of a *projective* variety V, so that $\mathbf{Alb}^1(V)$ is a torsor under the *abelian* variety $\mathbf{Alb}^0(V)$.

Example 1.2.1: Let V be a Severi-Brauer variety, so $[V] \in \mathrm{Br}(K)$. Then $I(V) = I([V])$, but since V is simply connected, $\mathbf{Alb}^0(V) = 0$ and $P(V) = 1$ (so is usually not equal to $P([V])$).

Example 1.2.2: Let V be a curve, so Alb = Pic. Then the index of V is the least positive degree of a K-rational divisor and the period is the least positive degree of a K-rational divisor class (a significantly more enlightening definition than in the general case). We have that the period of V is the period of $\mathbf{Pic}^1(V)$. Since we have a morphism $V \to \mathbf{Pic}^1(V)$, we clearly have

$$I(\mathbf{Pic}^1(V)) \mid I(V).$$

A very important open problem is to understand the discrepancy between these two indices.

Consider the intersection of these two examples, namely genus zero curves $V_{/K}$. If $V(K) = \emptyset$, $I(V) = 2$, whereas $P(V) = 1$ implies $I(\mathbf{Pic}^1(V)) = 1$, i.e., the two indices differ by a factor of 2. A result of Harase gives an upper bound on $I'(V) = \frac{I(V)}{I(\mathbf{Pic}^1(V))}$.

Open Problem 1. *What are the possible values of $I'(C)$ for a curve of genus g? Can we have $I'(C) > 2$?*

Example 1.2.3: For a quadric surface V over a field of characteristic different from 2, $P(V) = 1$ and $I(V) = 2 \iff V(K) \neq \emptyset$ (as follows from a theorem of Springer).

Moral: the geometric and cohomological period-index problems are distinct but closely related, and it would be of interest to understand the relationships between them more clearly.

In what remains, we will consider the case in which the two problems are the same, namely:

Example 1.2.4: Suppose that $X \mapsto \mathrm{Alb}^1(X)$ is an isomorphism, i.e., X is a torsor under the abelian variety $\mathbf{Alb}^0(X)$.

In light of all of this, the best case scenario is when X simultaneously a torsor under an abelian variety and a curve, i.e., is a curve of genus one.

2. Curves of genus one

2.1. **Generalities.**

Let $C_{/K}$ be a genus one curve, with Jacobian elliptic curve E.

Proposition 2. *For all curves of genus one, $I \mid P^2$.*

The proof we will give requires K to be perfect or P to be indivisible by $\mathrm{char}(K)$. For a proof avoiding these assumptions, see [**?**].

Proof: Because of the Kummer sequence

$$0 \to E(K)/PE(K) \to H^1(K, E[P]) \to H^1(K, E)[P] \to 0 \tag{2}$$

we can lift η to a class $\xi \in H^1(K, E[P])$, which splits over an extension of degree dividing P^2 by Fact X.

Remark X.X.X: Note that when K is perfect of characteristic $p > 0$, the proof shows that $I = P$ when P is a power of p. that P is not divisible by the characteristic of K.

The Kummer sequence shows that the period-index problem in the WC-group of an elliptic curve depends upon the Galois cohomology of the finite modules $E[P]$ as well as on the structure of the weak Mordell-Weil groups $E(L)/PE(L)$ as L ranges over the finite extensions of K.

Theorem 3. *(Lang-Tate)*
a) Suppose that $E_{/K}$ is such that
(i) $\#E(K)[P] = P^2$.
(ii) For all finite L/K, $E(L) = PE(L)$.
(iii) There exists a surjection $\mathfrak{g}_K \to (\mathbb{Z}/P\mathbb{Z})^2$.
Then for $P \mid I \mid P^2$, there exists $\eta \in H^1(K, E)$ with period P and index I.
b) For $K = \mathbb{C}((t_1))((t_2))$, $(E_0)_{/\mathbb{C}}$ any elliptic curve and $E = E_0 \times_{\mathbb{C}} K$, the hypotheses of a) are satisfied for all $P \in \mathbb{Z}^+$.

Exercise X: Prove it. Show also that with $\mathbb{C}$ replaced by any algebraically closed field k, the result remains valid provided $\mathrm{char}(k)$ does not divide P.

In some sense, this gives an answer to the period-index problem for genus one curves. To say more, we need to make some assumptions on the field.

2.2. Some fields with $P = I$.

Example 2.1: Suppose that $H^1(K, E) = 0$. Then $I \mid P^0$. This obviously holds when: K is algebraically closed, K is PAC, K is weakly PAC in the sense of Jarden.[3]

It also holds when K is finite, as a special case of a theorem of Lang. A proof was discussed in a previous talk. Here is another proof, more relevant to present considerations: the Weil bounds for curves over finite fields imply that every $V_{/\mathbb{F}_q}$ has $I(V) = 1$. Now if V is a torsor under an algebraic group, $I(V) = 1$ implies $V(K) \neq \emptyset$ (1).

Theorem 4. *(Ogg, Shafarevich) Let K be a one variable function field over an algebraically closed field, or discretely valued Henselian with algebraically closed residue field. Then $I = P$ for all genus one curves $C_{/K}$ of period indivisible by* $\mathrm{char}(K)$*.*

Remark 2.1.X: Note that all the fields of Theorem 4 have trivial Brauer group.

Theorem 5. *(Lichtenbaum) Suppose* $\mathrm{Br}(K) = 0$*. Then $I = P$ for* all *curves $C_{/K}$.*

Proof: To show that $I = P$ on a curve, we must show that if D is a rational divisor class on C, there is some other rational divisor class of the same degree that is represented by a rational divisor. In fact, if $\mathrm{Br}(K) = 0$ we have that every rational divisor class is represented by a rational divisor. For this, we use the following fundamental sequence

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

Thus given a rational divisor class D, there is a well-defined element $\delta(D) \in Br(K)$ whose nontriviality is precisely the obstruction to D being represented by a divisor. The result is now clear.

The following result exploits a similar idea.

Theorem 6. *(C—) Let K be a global field, and $C_{/K}$ a curve which has points everywhere locally except possibly at one place of K. Then $P(C) = I(C)$.*

Exercise X.X: Prove Theorem 6. (Hint: what can be said about an element of $\mathrm{Br}(K)$ which is locally trivial except possibly at one place?)

Theorem 7. *(Lichtenbaum) Let K be a locally compact field. Then $I = P$ for genus one curves $C_{/K}$.*

It would hardly be overstating things to say that all subsequent work on geometric period-index problems builds on the ideas behind this theorem in some way. We will postpone a discussion of the proof until the next section, where we will explain generalizations to higher-dimensional abelian varieties.

[3] In fact it seems conceivable that the condition $H^1(K, A) = 0$ for all abelian varieties is equivalent to weakly PAC, which by definition requires also that geometrically rational varieties have K-points.

Exercise X.X.X: Let K be a locally compact ultrametric field.
a) Suppose that P is not divisible by $\operatorname{char}(K)$ and E has good reduction. Let $\eta \in H^1(K,E)$ be a class of period P. Show that a finite L/K splits η if and only if $P \mid e(L/K)$ (the relative ramification index).
b) Let K be any complete DVF, assume E has split multiplicative reduction, and let $\eta \in H^1(K,E)[P]$. Show: there exists a finite extension L_η/K such that
(i) L_η/K is cyclic of degree dividing P.
(ii) L/K splits η iff $L_\eta \subset L$.

Keeping in mind that $I \mid P^0$ for genus one curves over finite fields, one can view Theorem 7 as a sort of"transition theorem" for the period-index problem. This has recently led me to ask the following

Question 8. *Suppose that K is a CDVF k, with perfect residue field k, and suppose that every torsor under an k-abelian variety has a k-rational point. Does it follow that $I = P$ for genus one curves $C_{/K}$?*

Theorem 9. *Under the hypotheses of Question 8, $I \mid 48P$ for all $C_{/K}$.*

At the time of writing, it seems to me that stronger results should be true, but that on the other hand the existence of a biquadratic extension of k should lead to an example with $I = 2P$.

Theorem 10. *(C—, '04)*
a) Let K be a number field, and $E_{/K}$ an elliptic curve with $E(K) = 0$. Then for all $n \in \mathbb{Z}^+$, there exists $\eta \in H^1(K,E)$ with $P(\eta) = I(\eta) = n$.
b) If moreover $Ш(K,E) = 0$, then for any finite L/K and any $n \in \mathbb{Z}^+$, there exists $\eta \in H^1(K,E)$ such that $\eta|_L$ has period equals index equals n.

Remark X.X.X: There *do* exist elliptic curves $E_{/\mathbb{Q}}$ with $E(\mathbb{Q}) = Ш(\mathbb{Q},E) = 0$, as was shown by Kolyvagin. Admittedly this "fact" lies deeper than all of the results discussed so far.

Remark X.X.X: Earlier W. Stein had shown that over any number field there exists a curve of any given index which is not divisible by 8. The proof of Theorem 10 does not rely on Stein's work, but *a posteriori* one can see some connections between them. See [**?**, §4] for a discusson.

Let us sketch the proof of part a). If $E(K) = 0$, one can produce for all n a class $\eta \in H^1(K,E)$ which is locally trivial except at a single place of K and has local period n at that place. One reduces to the case $n = p^a$, and the key observation is that *either* $Ш(K,E)$ is p-divisible – in which case Theorem 6 implies there exist elements of $P = I = p^a$ for all a – or $Ш(K,E)[p^\infty]$ is finite, in which case one can apply the duality theory of Poitou-Tate to construct such a class. By Theorem 6, every multiple of η has period equals index, and clearly some multiple of η has period n.

Presumably one should be able to make do with part a) alone:

Open Problem 2. *Show that for every number field K, there exists an elliptic curve $E_{/K}$ with $E(K) = 0$.*

2.3. $P < I$ over Global Fields.

Cassels produced an example of a genus one curve $C_{/Q}$ with $P = 2,\ I = 4$. In his example, $E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. The following is therefore a generalization:

Theorem 11. *(C— '03, Sharif '06) Let K be a global field, and p a prime such that $E(K)[P] \cong (\mathbb{Z}/P\mathbb{Z})^2$. For any $P \mid I \mid P^2$, there exist infinitely many classes of period P and index I.*

Remarks: The case of prime P was established in [**?**], whereas the general case appears in Sharif's 2006 Berkeley thesis. It seems to me that the methods of [**?**] could also be used to establish the general case. This would, however, require replacing a messy Hilbert symbol calculation by a *messier* Hilbert symbol calculation, whereas Sharif's approach exploits work of Lichtenbaum to proceed in a much more elegant way. For instance, his construction produces classes which are nontrivial at exactly two places of K, which serves as a sort of converse to Theorem 6.

Theorem 12. *(Sharif '06) For any odd P, there exist genus one curves $C_{/\mathbb{Q}}$ with period P and index P^2.*

It seems to me that, building on the ideas of this theorem, one should be able to prove the following stronger result:

Theorem? 13. *Let K be a global field, P a positive integer not divisible by* $\mathrm{char}(K)$ *and $E_{/K}$ an elliptic curve. Then there are infinitely many classes in $H^1(K, E)$ of period P and index P^2.*

Ideally, one would like to establish the following result:

Conjecture 14. *Let K be an infinite, finitely generated field and $E_{/K}$ an elliptic curve. Then for all $P \mid I \mid P^2$, there exist infinitely many classes $\eta \in H^1(K, E)$ of period P and index I.*

In light of the previous results, the conjecture appears to be within reasonable striking distance, except possibly for the case in which P is a power of $\mathrm{char}(K)$. In this case, it seems that the present Galois-cohomological methods should be replaced by "flat-cohomological analogues." (To be sure, to say exactly what these analogues may be, let alone construct them, would be a worthy project.)

2.4. Sketches of some proofs.

At this point we have accrued quite a debt of results stated with no indication of proofs given. While we could wait and discuss everything in the context of abelian varieties, it seems better to me to sketch out some broad ideas in the (simpler) one-dimensional case, and then return in more detailed fashion. (Also the talk is designed this way, so that one can attend the first hour only and still get some sense of what's going on.)

Suppose first that $C_{/K}$ is an algebraic curve of any genus, so that the period P is the least positive a such that $\mathbf{Pic}^a(C)(K) \neq \emptyset$ and the index I is the least positive degree of an element of $\mathrm{Pic}(C)$. As above, the exact sequence **??** will be of fundamental importance. Let us also define, for any variety $V_{/K}$, the **Brauer kernel**

$$\kappa(V/K) = \mathrm{Im}(\delta) = \mathrm{Ker}(\gamma),$$

i.e., the image in the Brauer group of obstructions of K-rational divisor classes. Let us also define

$$\kappa^0(V/K) = \delta(\mathbf{Pic}^0(V)(K)),$$

the obstructions of rational divisor classes which are algebraically equivalent to zero (for a curve, this just means degree zero).

Proposition 15. *The quotient $\kappa(C/K)/\kappa^0(C/K)$ is cyclic of order I/P.*

For a proof in the general case (which involves nothing more than applying the snake lemma to a certain commutative diagram), see [**?**,]. However, the following seems more enlightening.

Proof: Let us define, for each integer n, $\kappa^{nP}(C/K) = \delta(\mathbf{Pic}^{nP}(C)(K))$. Note that in other degrees d, $\mathbf{Pic}^d(C)(K) = \emptyset$, so

$$\delta(\mathbf{Pic}(C)(K)) = \delta(\bigcup_n \mathbf{Pic}^{nP}(C)(K)) = \bigcup_n \delta(\mathbf{Pic}^{nP}(C)(K)) = \bigcup_n \kappa^{nP}(C/K).$$

Choose a rational divisor class D of degree P; this choice induces a choice of rational divisor class of each degree nP, namely $D_{nP} = nD$. Put $\alpha = \delta(D)$, so $\delta(D_{nP}) = n\alpha$. Note that addition of D_{nP} induces an isomorphism $\mathbf{Pic}^0(C)(K) \cong \mathbf{Pic}^{nP}(C)$, and exhibits

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

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

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

It is also the case that $\kappa^0(C/K)$ is the set of differences of degree n divisor classes, so the quantity P/I depends upon (i) the orders of the Brauer classes $\delta(D_i)$ as D_i ranges over the degree n divisor classes on C, and (ii) how "spread out" these classes are in the above sense.

We now return to consideration of genus one curves. For an elliptic curve $E_{/K}$ and a positive integer P, there is a natural equivalence relation on pairs (C, D), where C is a torsor under E and D is a degree P divisor class on C: namely, $(C, D) \sim (C', D')$ if there exists an isomorphism of torsors $f : C \rightarrow C'$ such that $f^*(D') = D$.

Proposition 16.
a) The group $H^1(K, E[P])$ parameterizes equivalence classes of pairs (C, D) as above.
b) The forgetful map $(C, D) \mapsto C$ corresponds to the map $H^1(K, E[P]) \rightarrow H^1(K, E)[P]$ in Galois cohomology, and the kernel, namely equivalence classes of degree P divisors on E itself, is identified with $E(K)/PE(K)$.

Exercise X.X.X: Prove it.

Corollary 17. *(Sharif) Suppose that $E(K)/PE(K) = 0$. Then for all $C \in H^1(K, E)$, let D be any rational divisor class of order $P = P(C)$. Then*

$$I(C) = P(C) \cdot \#\delta(D).$$

Proof: The preceding proposition shows that $\kappa^P(C/K)$ consists of a single element, so

$$\kappa^0(C/K) = \kappa^P(C/K) - \kappa^P(C/K) = 0.$$

In particular, if we take an elliptic curve over a field with trivial Mordell-Weil group $E(K)$, then unless Δ is identically zero on $H^1(K, E[P])$, there will be a torsor C under E with period P and index exceeding P.

The proposition allows to define a map

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

by $(C, D) \mapsto \delta(D)$.

The following is a key point:

Proposition 18. $\Delta(H^1(K, E[P])) \subset \mathrm{Br}(K)[P]$.

Proof: To any ample divisor class on a variety V, one can associate a Severi-Brauer variety $V[D]$ by Galois descent from the complete linear system associated to the line bundle $D_{\overline{K}}$. In particular, the dimension of $V[D]$ is equal to one less than the dimension of the space of global sections of D. One can check that the Brauer class associated to the Severi-Brauer variety $V(D)$ coincides with the obstruction $\delta(D)$. In the case of a class of degree P on a curve of genus one, Riemann-Roch gives that $V(D)$ has dimension $P-1$, so that $V(D)$ corresponds to a central simple algebra of dimension P^2, and hence the *index* of $\delta(D)$ divides P, which is, of course, stronger than the claimed statement.

Note that it would have been easier to show that the image of Δ is P^2-torsion. Indeed:

Exercise X.X.X: Let $V_{/K}$ be any variety. Show that

$$\kappa(V/K) \subset \mathrm{Br}(K)[I(V)].$$

Let $\{Q_j\}_{j\in J}$ be a set of representatives for $E(K)/PE(K)$ in E. Recall that this "weak Mordell-Weil group" is finite in almost every reasonable case: e.g., if K is finitely generated over $\mathbb{Q}$ or any field in which $K^\times/K^{\times P}$ is finite (e.g. K algebraically closed or locally compact). Let $(C, D) = \xi \in H^1(K, E[P])$. Then

$$\kappa^P(C) = \{\Delta(\iota(Q_j) + \xi)\}_{j\in J}.$$

Note that $\Delta(\iota(Q_j)) = 0$, since these represent divisor classes on E itself, however the term $\iota(Q_j)$ cannot be omitted because Δ is *not* a homomorphism of groups; rather it is a quadratic map. This means that the associated thingie (first moment?)

$$L(\xi, \psi) := \Delta(\xi + \psi) - \Delta(\xi) - \Delta(\psi)$$

is bilinear; this was shown by O'Neil by reduction to the work of Zarhin. In fact, in our present situation we are naturally led to consider this bilinear form, since we are interested in the difference group $\kappa^0 = \kappa^P - \kappa^P$, which consists of elements

$$\{\Delta(\xi + \iota(Q_j)) - \Delta(\xi)\}_{jinJ},$$

because, since $\Delta(\iota(Q_j)) = 0$, this is precisely the set of elements $\{L(\xi, Q_j)\}_{j\in J}$. Moreover, for exactly the same reason, this expression depends only on the image of ξ in $H^1(K,E)$, i.e., on $\eta = \eta_C$. Thus we have defined a bilinear pairing

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

and now a miracle occurs:

Theorem 19. *(Lichtenbaum) The pairing L is nothing else than Tate's duality pairing T.*

This beautifully succinct statement is the heart of Lichtenbaum's paper on curves of genus one. Its usefulness in the case of locally compact fields is immediate: then $\mathrm{Br}(K)[P] \cong \mathbb{Z}/P\mathbb{Z}$ and (as was shown by Tate when P is indivisible by $\mathrm{char}(K)$ and by Shatz and Milne in general) $L = T$ gives a perfect pairing between these two finite abelian groups. It follows immediately that for any genus one curve over a locally compact field ($\mathbb{R}$ and $\mathbb{C}$ included!),

$$\kappa(C) \subset \mathrm{Br}(K)[P(C)] = \kappa^0(C),$$

and hence $\kappa(C) = \kappa^0(C)$ so $P(C) = I(C)$.

What is interesting about this proof is that it shows that $P = I$ over locally compact fields for "the opposite reason" that $P = I$ for locally trivial curves over number fields: $\kappa(C/K)$ is always nontrivial if C is. It is just that $\mathrm{Br}(K)$ is so small that it is not possible for the elements of $\kappa^P(K)$ to be "spread out."

Over any infinite, finitely generated field, however, $G = \iota(E(K)/PE(K))$ is finite, say of order N, and $\mathrm{Br}(K)[P]$ is infinite, and most N-tuples of order P elements are spread out in the above sense. The more serious issue is to construct obstruction classes of all possible orders dividing P. Indeed:

Proposition 20. *Fix $R \mid P$. Suppose $(C,D) = \xi \in H^1(K,E[P])$ is such that for all $g_i \in G$, $\#\Delta(g_i\xi) = R$. Then $I(C) = RP$.*

But really, how do we compute Δ? We use the following

Theorem 21. *Suppose that $E_{/K}$ has full level P structure if P is odd and full level $2P$ structure if P is even. Then*

$$H^1(K,E[P]) \cong H^1(K,\mathbb{Z}/P\mathbb{Z})^2 \cong H^1(K,\mu_P)^2 \cong (K^\times/K^{\times P})^2,$$

and $\Delta(a,b)$ may be identified with the order P norm residue symbol $\langle a,b\rangle$.

Remark: This is due to O'Neil when P is odd and Sharif when P is even (in fact he claims a more precise result). In [**?**] and [**?**] I give a different proof for odd P which generalizes nicely to the higher-dimensional case, and also prove a result which says, essentially, that if we assume only that E has full level P structure in all cases, Δ is "close enough" to the norm residue symbol for applications.

It ought to be clear that the last two results, together with the weak Mordell-Weil theorem, reduce the proof of Theorem 11 to a fact about Hilbert symbols over global fields which is not especially difficult to prove (but neither is it very much fun). This "unfun calculation" appears in [**?**] (in the case of prime P). Sharif's proof, however, uses the identity $\Delta(g_i\xi) = \Delta(\xi) + L(Q_i,\eta)$ to simplify the calculation.

In the case that E does not have full level P structure, one can try to reduce to this case using the following "extended inflation-restriction sequence": let $L = K(E[P])$; then

$$0 \to H^1(L/K, E[P]) \to H^1(K, E[P]) \to H^1(L, E[P])^{\mathfrak{g}_{L/K}} \to H^2(L/K, E[P])$$

is exact. It is a well-known consequence of Serre's work on torsion points that for a given non-CM elliptic curve over a number field, there exists a positive integer N such that the first and last terms will be 0 whenever $(P, N) = 1$. Sharif works with an elliptic curve $E_{/\mathbb{Q}}$ whose Galois representation is "maximal" and is thus able to take $N = 2$. He also constructs a large family of $\mathfrak{g}_{L/K}$-invariant classes in $H^1(L, E[P])$. He is therefore able to construct classes in $H^1(K, E[P])$ whose obstructions have maximal order P even upon restriction to L; *a fortiori* they have maximal order over K. When $E(K) = 0$, this suffices to prove the result.

It seems to me that one should be able to construct, for every elliptic curve over a number field and any P, an arbitrarily large number of Galois-invariant classes in $H^1(L, E[P])$ which are spread out enough – by virtue of being supported at different primes – so that their pairwise differences (and their modifications by elements of $G = \iota(E(L)/PE(L))$ still have obstruction order P), and since $H^2(L/K, E[P])$ is finite, some of these differences will come from $H^1(K, E[P])$.

The really difficult case is constructing classes with $I < P^2$ when the Galois module structure on $E[P]$ is maximal (as it ususally is). In the case of an elliptic curve E over a number field K with $E(K) = 0$, it seems that we can produce, for all P, classes with $I = P$ and also classes with $I = P^2$, but I do not yet see how to get the intermediate cases.

3. Curves of higher genus

A proper treatment is beyond the scope of these notes; we will concentrate on Lichtenbaum's theorems and their converses.

Theorem 22. *(Lichtenbaum) Let $C_{/K}$ be a curve of genus g.*
a) $I \mid 2g - 2$.
b) $P \mid I \mid 2P^2$.
c) If $\frac{2P(g-1)}{I}$ is even, $I \mid P^2$.

Remark: Of course 0 is even, so this recovers the fact that $I \mid P^2$ for curves of genus one as a special case.

Theorem 23. *(Lichtenbaum) Suppose that K is locally compact, and $C_{/K}$ has genus g.*
a) $P \mid g - 1$.
b) $P \mid I \mid 2P$.
c) If $I = 2P$, then $\frac{g-1}{P}$ is odd.

Following Sharif, we define a triple (g, P, I) as **admissible** if it satisfies the conditions of Theorem 22 and **locally admissible** if it satisfies the conditions of Theorem 23.

Theorem 24. *(Sharif) a) Let (g, P, I) be admissible with $4 \nmid I$. Then there is a number field K and a genus g curve $C_{/K}$ with $P(C) = P$, $I(C) = I$.*

b) Let (g, P, I) be a locally admissible triple. Then for every *locally compact ultrametric field K with* $\mathrm{char}(K) \neq 2$*, there is a genus g curve $C_{/K}$ with $P(C) = P$, $I(C) = I$.*

Remark X.X.X: Note that Theorem 11 gives a stronger result than part a) in the case that $g = 1$.

Remark: Obviously the theorem does not hold for $K = \mathbb{C}$, where the problem is trivial, nor for $K = \mathbb{R}$, where $I \mid 2$ for all g. See Gross-Harris for more information about this latter case.

Recently I have proven the following result, which applies for instance to locally compact fields of characteristic 2 (but says nothing about the period).

Theorem 25. *(C—) Fix a non-negative integer g and a positive integer $n \mid 2g-2$. Suppose that K is a complete DVF whose residue field k admits a degree n cyclic extension (e.g. k is finite). Then there exists a curve $C_{/K}$ of genus g and index n.*

4. Torsors under abelian varieties

Let $A_{/K}$ be a g-dimensional abelian variety.

Proposition 26. *Suppose that K is perfect or P is indivisible by* $\mathrm{char}(K)$*. Then for all classes $\eta \in H^1(K, A)$, $I \mid P^{2g}$.*

Exercise X.X.X: Prove it.

Open Problem 3. *Does $I \mid P^{2g}$ for all torsors under a g-dimensional abelian variety?*

Exercise X.X.X: Let $K_g = \mathbb{C}((t_1)) \cdots ((t_{2g}))$. Show that for all $P \mid I \mid P^{2g}$, there exists a g-dimensional abelian variety $A_{/K_g}$ and a class $\eta \in H^1(K_g, A)$ of period P and index I.

Note that K_g is quite a complicated field. In the case of $g = 1$, we saw that such esoterica was unnecessary, in that all possible values of P and I arise over suitable number fields. In higher dimensions, this is not at all the case.

In all the remaining results of the section, we assume that A possesses a **principal bundle**, i.e., an ample line bundle λ such that the induced map

$$\Phi_L : A \to A^\vee, \ x \mapsto \tau_x^* L \otimes L^{-1},$$

is an isomorphism.[4]

Theorem 27. *If K has property* $\mathrm{Br}(\alpha)$*, then for $X \in H^1(K, A)[P]$,*

$$M(X) \leq 2^\alpha g! P^{g+\alpha}.$$

Theorem 28. *Let K be a locally compact field. For P indivisible by* $\mathrm{char}(K)$ *and $X \in H^1(K, A)[P]$. Then*

$$M(X) \leq 2g! P^g.$$

[4] This is subtly stronger than saying "Let $(A, \lambda)_{/K}$ be a principally polarized abelian variety." We will not pause to discuss the difference, rather referring the reader to [**?**] for the full story. However, when K is locally compact, there is no distinction.

Supplement: In the setting of Theorems 27 and 28, assume **any** of the following additional hypotheses:
a) $g = 1$.
b) P is odd.
c) $A[P]$ is isomorphic as a $\mathfrak{g}_K$-module to $H \oplus \operatorname{Hom}(H, \mathbb{G}_m)$.
d) K is locally compact and A has split semistable reduction.
Then we may replace $2g!$ by $g!$.

Remark: On the other hand it is known that for K a sufficiently large p-adic field (depending on g), there exist g-dimensional torsors of period p and index p^g.

Open Problem 4. *Can the factor $2g!$ be replaced by $g!$? By 1?*

Remark: Without the assumption that A admits a principal bundle, the proof goes through with $g!$ replaced by $2^g \cdot g!$ multiplied by the type of any polarization.

Theorem 29. *Suppose that K is p-adic, $NS(A)$ is cyclic, $X \in H^1(K, A)$ of period P, and that at least one of the hypotheses a)-c) is satisfied. Then the Brauer kernel*

$$\kappa(X) = \operatorname{Ker}(\operatorname{Br}(K) \to \operatorname{Br}(X))$$

is cyclic of order P.

Remark: This is to be contrasted with the case of curves over p-adic fields, where the Brauer kernel has equal order to the index of C. (Recall that the period and index need not coincide in either case.)

Example X.X.X: Let X be a quadric surface over a p-adic field K which is anisotropic with nonsquare discriminant d. Then $I(X) = 2$ but $\kappa(X) = 0$: [**?**]. In this case, it turns out that after basechanging to $L = K(\sqrt{d})$ we get $I = 2 = \#\kappa(X/L)$.

Definition: For a variety $V_{/K}$ the **Picard index** $I_{\operatorname{Pic}}(V)$ is the exponent of the cokernel of the natural map $\mathbf{Pic}(V)(K) \to NS(V)(K)$.

Then, under the hypotheses of Theorem 29, we are showing that the period is equal to the Picard index. Note that in case of example X.X.X, the Picard index is equal to $\#\kappa(V)$, both over K (where they are both 1) and over $K(\sqrt{d})$ (where they are both 2). Thus, it seems natural to ask:

Open Problem 5. *Let $V_{/K}$ be a variety over a p-adic field. Is it the case that*

$$I_{\operatorname{Pic}}(V) = \#\kappa(V/K)?$$

What if we assume moreover that $NS(V)(K)$ is cyclic?

In asking this question we are also motivated by a result of van Hamel that we will discuss shortly.

4.1. **Some proofs.** In what follows, we fix $L = P\lambda$, where λ is our principal line bundle on A. Associated to the finite morphism $\Phi_L : A \to A^\vee$, we get a Kummer sequence

$$A^\vee(K)/PA(K) \to H^1(K, A[P]) \to H^1(K, A)[P] \to 0.$$

Let $X \in H^1(K, A)[P]$. It is not hard to show that $NS(X)$ is canonically isomorphic, as a $\mathfrak{g}_K$-module to $NS(A)$. We can thus speak of $\mathbf{Pic}^\lambda(X)$, the set of rational divisor classes on X which are algebraically equivalent to λ.

We now have the following result, which directly generalizes the one-dimensional case:

Proposition 30.
a) The group $H^1(K, E[P])$ parameterizes equivalence classes of pairs (X, D), where $X \in H^1(K, A)$ and $D \in \mathbf{Pic}^\lambda(X)(K)$.
b) The forgetful map $(C, D) \mapsto C$ corresponds to the map $H^(K, A[P]) \rightarrow H^1(K, A)[P]$ in Galois cohomology, and its kernel, namely the equivalence classes of such lines bundles on A itself, is identified with $A^\vee(K)/PA^\vee(K)$.

Thus as before we may define the **period-index obstruction map**

$$\Delta = \Delta_L : H^1(K, A[P]) \rightarrow \mathrm{Br}(K),$$

by

$$(X, D) \mapsto \delta(D).$$

Notice, however, that in contrast to the one-dimensional case, it is not immediately clear what this divisorial construction has to do with the index of V, a quantity defined in terms of zero-cycles. (Of course it is not so farfetched that on a principally polarized abelian variety, there should be some connection....) To see the relevance, we need another interpretation of $H^1(K, A[P])$:

Proposition 31. *The group $H^1(K, A[P])$ classifies equivalence classes of "diagrams" $X \rightarrow V$ which are twisted forms of $\varphi_L : A \rightarrow \mathbb{P}^{P^g-1}$. Two diagrams are regarded as equivalent if they fit into a commutative square*

$$INSERT.$$

We can pass directly from the first interpretation to the second by noticing that V is the Severi-Brauer variety associated to the ample, basepointfree divisor class D on X. The key point is thus that, whereas on a variety over an algebraically closed field, an ample basepointfree divisor class corresponds to a (projective equivalence class of) morphisms into projective space, on an arbitrary variety, such a class corresponds to a morphism into a Severi-Brauer variety.

But this is an important distinction: given an embedding into projective space, we can take a hyperplane section to recover the divisor class. On the other hand, we can intersect with a lower-dimensional linear subspace to get a K-rational effective *zero-cycle* on X. The order of this zero-cycle is precisely the **degree** of the morphism. The degree of a morphism is of course a geometric property ("numerical properties are geometric"), so the degree is equal to the degree of the morphism $\varphi_L : A \rightarrow \mathbb{P}^{P^g-1}$, which is well-known (Riemann-Roch) to be $g!P^g$. Thus we get the following:

Theorem 32. *Let $\eta_X \in H^1(K, E)[P]$. Suppose there exists a Kummer lift ξ of η with $\Delta(\xi) = 0$. Then $M(\eta) \leq g!P^g$.*

The next step is an analogue of Proposition 18. We begin with the following:

Proposition 33. *Assume that P is odd. Then* $\mathrm{Im}(\Delta) \subset \mathrm{Br}(K)[P]$.

Notice that the proof given in the one-dimensional case does not work: the Severi-Brauer varieties which intervene are now of dimension $P^g - 1$, so that the bound on the *index* of the Brauer classes that we get is P^g: no good. (In fact, in [**?**] I showed that this bound is sharp for certain fields, namely those for which the period-index discrepancy in $\mathrm{Br}(K)$ is sufficiently large.)

On the other hand, O'Neil's interpretation of Δ in terms of nonabelian Galois cohomology of theta groups immediately gives, using a general theorem of Zarhin, the statement that Δ is a **quadratic** map, i.e.,

$$L(\xi, \psi) := \Delta(\xi + \psi) - \Delta(\xi) - \Delta(\psi).$$

Unfortunately quadratic maps between abelian groups need not preserve orders of elements: you can check that the map from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/4\mathbb{Z}$ which sends 0 to 0 and 1 (mod 2) to 2 (mod 4) is quadratic! But in fact this is essentially "as bad as it gets":

Proposition 34. *Let $f : X \rightarrow Y$ be a quadratic map between abelian groups, with $f(0) = 0$. Then:*
a) $f(X[P]) \subset Y[2P]$.
b) For odd P, $f(X[P]) \subset Y[P]$.

In fact there is another way of seeing the quadraticity of Δ which avoids Galois cohomology of theta groups (which we do not consider in these notes). Namely, as before, $L(\xi, \psi)$ descends to a map

$$L : A^\vee(K)/PA^\vee(K) \times H^1(K, A)[P] \rightarrow \mathrm{Br}(K)$$

and now a miracle recurs:

Theorem 35. *The map L is nothing else than Tate's duality map applied to the dual variety $A^\vee$. (In particular it is bilinear!)*

As yet the proof of this theorem has not been written down. Rather, as a consequence of his more elaborate *pseudo-motivic homology*, he derives:

Corollary 36. *For any locally compact field K, and $X \in H^1(K, A)$ of period P,*

$$\kappa^0(V/K) = \delta(\mathbf{Pic}^0(V)(K)) = \mathrm{Br}(K)[P].$$

Quite recently, van Hamel was kind enough to sketch a proof of the theorem itself. His proof is too "high tech" (in particular, it takes place in the derived category) to be included here.[5]

Anyway, as in the one-dimensional case, the corollary is exactly what we need, together with the inclusion $\kappa(V/K) \subset \mathrm{Br}(K)[P]$, to conclude that we can modify any given Kummer lift of V by a divisor class algebraically equivalent to zero to get one with vanishing obstruction.

What about when P is even (and $g > 1$)? In fact, we are able to prove that the image of the obstruction is still contained in $\mathrm{Br}(K)[P]$ provided we have the existence of a **Lagrangian decomposition** $A[P] \cong H \oplus H^*$, so in particular when we have full level structure. The proof of this requires more work – namely, an

[5] I would be very happy to receive a writeup for a later edition of these notes. . .

investigation into the Galois cohomology of Heisenberg-type group schemes – so we shall say nothing about it here.

Finally, if we assume that the Néron-Severi group is generated by λ, then $\kappa(V/K)$ is generated by $\kappa^0(V/K)$ together with $\Delta(\xi)$ for any Kummer lift ξ of η, so combining with Tate-Lichtenbaum-van Hamel duality, we get that

$$\kappa(V/K) = \mathrm{Br}(K)[P].$$

The Mathematical Sciences Research Institute, 17 Gauss Way, Berkeley, CA 94709
E-mail address: plclark@msri.org