# THE PERIOD-INDEX PROBLEM IN WC-GROUPS II: ABELIAN VARIETIES

PETE L. CLARK

Abstract. We study the relationship between the period and the index of a principal homogeneous space over an abelian variety, obtaining results which, in particular, generalize work of Cassels and Lichtenbaum on curves of genus one. In addition, we show that the $p$-torsion in the Shafarevich-Tate group of a fixed abelian variety over a number field $k$ grows arbitarily large when considered over field extensions $l/k$ of bounded degree. Essential use is made of an abelian variety version of O'Neil's period-index obstruction.

## 1. Introduction and Statement of Results

Let $A_{/k}$ be an abelian variety and $V_{/k}$ a principal homogeneous space for $A$,[1] so $V$ represents an element of the Weil-Châtelet group $H^1(k, A)$. In this paper we are concerned with two numerical invariants associated to $V$, each of which can be viewed as quantifying the failure of $V$ to have $k$-rational points. The **period** of $V$ is the order of $V$ in $H^1(k, A)$ (a torsion abelian group), whereas the **index** of $V$ is the greatest common divisor of all degrees of field extensions $[l : k]$ such that $V(l) \neq \emptyset$.[2] One shows easily (see §2) that for all $V$, the period divides the index and the two quantities have the same prime divisors. To say more is the **period-index problem** for the Weil-Châtelet group $H^1(k, A)$.

The classic paper on the period-index problem in the context of abelian varieties is [LaTa]. Almost all subsequent work ([Li1], [Ca1], [Ca2] [St], [O'N], [Cl1]) has focused on the case where $A = E$ is an elliptic curve, when it is known that the index divides the square of the period. Here are some more precise results:

(Lichtenbaum [Li1], O'Neil [O'N]): If $k$ has vanishing Brauer group, then period equals index for all genus one curves over $k$.

(Lichtenbaum [Li1]): The period equals the index for all genus one curves over a $p$-adic field.

(Cassels [Ca1], O'Neil [O'N]) If $C/k$ is a genus one curve over a number field which has rational points everywhere locally, then the period equals the index.[3]

[1] We should write $(V, \mu)$, where $\mu : A \times V \to V$ is the structure map for $V$. For the sake of notational simplicity we neglect the $\mu$...

[2] ... but note that the period and the index are independent of the choice of principal homogeneous space structure on $V$, so that our notation is not really so bad.

[3] In fact the conclusion holds if there are local points at all places except one [Cl2, Prop. 6].

Cassels also constructed genus one curves over $\mathbb{Q}$ of period 2 and index 4 [Ca2]. A generalization was proved in [Cl1]: let $k$ be a number field, $p$ a prime number and $E/k$ an elliptic curve with full $p$-torsion defined over $k$. Then there exists an infinite subgroup of $H^1(k,E)[p]$ all of whose nonzero elements have index $p^2$.

Rather fewer results are known for abelian varieties. Most relevant to our purposes are the following:

If $A$ has dimension $g$ and $\eta \in H^1(k,A)[n]$, then the index of $\eta$ divides $n^{2g}$ (due to Lenstra; see Corollary 13). Moreover, for all $n$ and $g$ the bound can be attained with a suitable choice of $k$, $A$ and $\eta$ (due to Lang-Tate; see Proposition 14).

(Lang-Tate [LaTa]): Let $A_{/k}$ be an abelian variety over a $p$-adic field. Suppose that $A$ has good reduction, and let $n$ be prime to $p$. Then any element $V$ of $H^1(k,A)[n]$ has index $n$: indeed, the splitting fields $l$ of $V$ are precisely those for which the ramification index $e(l/k)$ is divisible by $n$.

In the case where $k$ is a $p$-adic field and $A_{/k}$ is an abelian variety admitting an analytic uniformization, there is a similarly complete account of splitting fields of principal homogeneous spaces due to Gerritzen [Ge].

Our first result provides examples of principal homogeneous spaces of $g$-dimensional abelian varieties where the index is at least the $g$th power of the period.

**Theorem 1.** *Let $g$ be a positive integer and $p$ be a prime number. Let $k$ be any one of the following fields:*
*(i) a sufficiently large $p$-adic field $k = k(p,g)$;*
*(ii) a sufficiently large number field $k = k(g)$; or*
*(iii) the maximal unramified extension $k_\infty$ of a $p$-adic field $k$ containing $\mathbb{Q}(\mu_p)$.*
*Then there exists an abelian variety $A_{/k}$ and a principal homogeneous space $V \in H^1(k,A)[p]$ of index at least $p^g$.*

Remarks: Part (i) is due to Gerritzen [Ge]. Before we were aware of his work, we had independently proved a similar (but weaker) result, namely that for any $N$, there exist principal homogeneous spaces of abelian varieties $A_{/\mathbb{Q}_p}$ with period $p$ and such that the *least* degree of a splitting field is at least $p^N$. In particular, the most naive generalization of the theorems of Lang-Tate and Lichtenbaum – that period equals index for all principal homogeneous spaces over $p$-adic fields – is false.

Parts (ii) and (iii) follow rather easily. In the case $p = 2,\ g = 3$ of (ii) we prove a more precise result (Proposition 18), showing that we may take $k = \mathbb{Q}$. The significance of (iii) is that such fields have trivial Brauer group.[4]

Nevertheless, we find higher-dimensional analogues of the "period equals index" results of [Ca1] and [Li1].

Definition: A **Lagrangian decomposition** of $A[n]$ is an isomorphism of $\mathfrak{g}_k$-modules $A[n] \cong H \oplus H^*$, where $H$ and $H^*$ are Cartier dual $\mathfrak{g}_k$-modules which

[4]Examples of period $n$ and index $n^g$ over a different field with trivial Brauer group – namely $\mathbb{C}((t))$ – were constructed by Shafarevich [Ш].

are isotropic for the Weil pairing. In particular, Lagrangian decompositions exist when $A$ is principally polarized and has full level $n$-structure, i.e., $\#A[n](k) = n^{2g}$.

**Theorem 2.** *Let $A_{/k}$ be a $g$-dimensional principally polarized abelian variety over a $p$-adic field, and let $V \in H^1(k, A)[n]$. Suppose in addition that* ***either***
*(i) $n$ is odd;* ***or***
*(ii) $A[n]$ is a Lagrangian $\mathfrak{g}_k$-module.*
*Then $V$ is split by a field extension of degree at most $(g!)n^g$.*

Remark: It is not clear that any additional hypotheses like (i) or (ii) are necessary, but to our vexation we have not been able to eliminate them. For that matter, the $g!$ factor may well be an artifice of our method, but if so it is an unavoidable one (it comes from the Riemann-Roch theorem). Nevertheless we claim at least an "asymptotic solution" to the period-index problem in WC-groups over $p$-adic fields:

**Corollary 3.** *Let $A_{/k}$ be a $g$-dimensional principally polarized abelian variety over a $p$-adic field $k$. Let $n$ be a positive integer which is divisible only by primes $\ell > g!$. Then any class $\eta \in H^1(k, A)[n]$ has index at most $n^g$.*

*Proof:* By primary decomposition (Proposition 11d)), it suffices to consider the case in which $n = \ell^a$ for $\ell > g!$. Since the hypothesis implies that either $g = 1$ or $\ell$ is odd, Theorem 2 (or Lichtenbaum's theorem [Li1]) applies to give that the index of $\eta$ is at most $(g!)\ell^{ag} < \ell^{ag+1}$. Since the index must be a power of $\ell$, we conclude that it is at most $\ell^{ag}$, completing the proof.

**Theorem 4.** *Let $A_{/k}$ be a $g$-dimensional strongly principally polarized abelian variety and $V \in H^1(k, A)[n]$ a principal homogeneous space. Suppose that* either
*(i) $k$ has trivial Brauer group;* ***or***
*(ii) $k$ is a number field and $V \in Ш(A, k)[n]$ is a locally trivial class.*
*Then $V$ is split over a field extension of degree at most $(g!)n^g$.*

There is an immediate application to an upper bound for the **visibility dimension** of a class in $Ш(A/k)[n]$. We refer the reader to [AgSt] and [CrMa] for a discussion of visibility of principal homogeneous spaces. We recall only the following fact: if $V \in H^1(k, A)$ can be split by a field extension of degree at most $N$, then the visibility dimension of $V$ is at most $g \cdot N$, where $g = \dim A$ [AgSt, Prop. 1.3]. Thus Theorem 4 gives the following upper bound for the visibility dimension of a locally trivial class (compare with [AgSt, Prop. 2.3 and Remark 2.5]).

**Corollary 5.** *Let $\eta \in Ш(A/k)[n]$, where $A_{/k}$ is a $g$-dimensional strongly principally polarized abelian variety over a number field $k$. Then the visibility dimension of $\eta$ is at most $g \cdot (g!) \cdot n^g$.*

Remark: Because there could be many other ways to visualize $V$, there is no reason to believe that the upper bound of Corollary 5 is sharp. In fact, every nontrivial element of $Ш(k, E)[3]$ has visibility dimension 2 [Ma] as does every element of $H^1(k, E)[2]$ (even those with index 4).

Although the period-index problem can be formulated in a quite general Galois-cohomological context (see §2), to my knowledge the only other case to receive serious attention is $H^2(k, \mathbb{G}_m) = \mathrm{Br}(k)$, the Brauer group of $k$. The following result exhibits the connection between the period-index problem in $\mathrm{Br}(k)$ and the period-index problem in WC-groups of higher-dimensional abelian varieties over $k$.

**Theorem 6.** *Let $n$ and $a$ be positive integers and $k$ a field such that every class in $Br(k)[n]$ can be split over a field extension of degree dividing $n^a$. Let $A$ be a strongly principally polarized abelian variety, and $V \in H^1(k, A)[n]$. Then:*
*a) $V$ can be split by a field extension of degree at most $(g!)2^a n^{a+g}$.*
*b) If we assume* either *that $n$ is odd or that $A[n]$ is a Lagrangian $\mathfrak{g}_k$-module, then $V$ can be split by a field extension of degree at most $(g!)n^{a+g}$.*

In particular:

**Corollary 7.** *Suppose $k$ is a field such that period equals index for all elements in* $\mathrm{Br}(k)$ *(e.g. a number field, a $p$-adic field, or a function field in two variables over an algebraically closed field). Then an element $\eta \in H^1(k, A)[n]$ has index at most $(2g!)n^{g+1}$, and index at most $(g!)n^{g+1}$ when $n$ is odd or $A[n]$ is Lagrangian.*

Remark: Whether or not this bound is optimal in the case of number fields is an open question. None of the methods discussed here produce classes in $H^1(\mathbb{Q}, A)[p]$ of index exceeding $p^{\max(g,2)}$.

**Theorem 8.** *Let $p$ be a prime number and $A_{/k}$ be a strongly principally polarized abelian variety over a number field. Assume that both $A[p]$ and $NS(A)$ (the Néron-Severi group of $A$) are trivial as Galois modules. Then there exists an infinite subgroup $G \subset H^1(k, A)[p]$ such that every nonzero $V \in G$ has index exceeding $p$.*

**Theorem 9.** *Let $A$, $k$, $p$ be as in the statement of Theorem 8. Then for every positive integer $a$ there exist infinitely many degree $p$ field extensions $l/k$ such that $\#Ш(A/l)[p] \geq p^a$.*

**Corollary 10.** *(Horizontal variation of* Ш*) Let $A_{/k}$ be any $g$-dimensional principally polarized abelian variety over a number field and $p$ any prime number. There exists a function $F(g, p)$ such that*

$$\sup_{l/k \ : \ [l:k] \leq F(g,p)} \#(A/l)[p] = \infty.$$

*For instance, one can take $F(g, p) = p \cdot 2^{2g} \cdot \#GSp_{2g}(\mathbb{F}_p) \cdot \#GL_{4g^2}(\mathbb{F}_3)$.*

These last three results were proved in [Cl1] when $A$ is an elliptic curve.

Remark: It seems likely that we could take $F(g, p) = p$.

The organization of the paper is as follows. Section 2 collects some preliminary results on period-index problems in general, and in the Weil-Châtelet group in particular.

In Section 3 we recall Gerritzen's work on analytically uniformized abelian varieties; this work is then used to give a proof of Theorem 1. An additional argument using modular curves is used to get 3-dimensional principal homogeneous spaces over $\mathbb{Q}$ of period 2 and index 8.

In Section 4, after disposing of some technical preliminaries we formulate two separate period-index problems for any variety $V_{/k}$, one defined in terms of the Albanese variety and the other in terms of the Picard variety. We thus get a formalism for transferring results about divisors to results about zero-cycles.

Section 5 contains an adaptation of the results of [O'N] and [Cl1] to the case of abelian varieties. Especially, we extend O'Neil's **period-index obstruction** to our higher-dimensional context. The basic theta group construction can be done

verbatim using abelian varieties instead of elliptic curves, but complications arise in the higher-dimensional case. Indeed, since the index of a variety involves its zero-dimensional geometry (least degree of an effective $k$-rational zero cycle) and the period-index obstruction $\Delta$ involves its codimension-one geometry (the obstruction to a rationally defined divisor class coming from a rational divisor), when $\dim V > 1$ it is not *a priori* clear that the non/vanishing of the obstruction map $\Delta$ should be related to the index. Nevertheless, using the Albanese/Picard formalism, we show that as in the one-dimensional case, consequences can be drawn both from the vanishing and the non-vanishing of $\Delta$. We deduce Theorem 4 immediately from this setup, as in [O'N].

In [Cl1] we used Mumford's theory of the Heisenberg group to get an "explicit" form of the period-index obstruction map for an elliptic curve with full level $n$-structure. In Section 6 we look at the Galois cohomology of Heisenberg groups in more detail. The results directly imply Theorem 6 and are used in the proofs of the remaining theorems.

In Section 7 we give the proof of Theorems 8 and 9 and Corollary 10, following roughly the same strategy as in [Cl1].

Acknowledgements: This work would not be possible without the basic insights provided by W.A. Stein and C.H. O'Neil. Many others have made valuable contributions along the way: it is a pleasure to thank K. Buzzard, R.T. Sharifi, F. Herzig, J. van Hamel, E. Z. Goren, M.H. Weissman and J.-L. Colliot-Thélène.

Notation and conventions: $k$ denotes a perfect field with (a choice of) algebraic closure $\overline{k}$, and $\mathfrak{g}_k = \mathrm{Gal}(\overline{k}/k)$ denotes the absolute Galois group of $k$. $V_{/k}$ shall always denote a smooth, projective, geometrically irreducible $k$-variety.

By a $\mathfrak{g}_k$-module, we mean an *abelian* group $M$ endowed with an action of $\mathfrak{g}_k$ which is continuous (for the profinite topology on $\mathfrak{g}_k$ and the discrete topology on $M$). A not-necessarily abelian group $G$ endowed with a continuous $\mathfrak{g}_k$-action will simply be called a $\mathfrak{g}_k$-group. We may view a $\mathfrak{g}_k$-group $G$ as a functor from algebraic field extensions $l$ of $k$ to groups, and we sometimes write $G(l)$ for $G^{\mathfrak{g}_l}$. In particular, the $\overline{k}$-valued points of a group scheme $G_{/k}$ are naturally a $\mathfrak{g}_k$-group, and the two possible meanings of $G(l)$ coincide.

A technical, but critical, theme of this paper is the consideration of $k$-rational elements in various quotients of the group $\mathrm{Div}(V_{\overline{k}})$ of geometric divisors. It may be useful to keep in mind that if $K \subset M$ are $\mathfrak{g}_k$-modules, then $(M/K)(k)$ is, in general, larger than $M(k)/K(k)$. This applies especially to the $\mathfrak{g}_k$-action on the Picard and Néron-Severi groups of $V$.

As a matter of notation, we have found it best to allow $D$ to denote either a divisor on $V$ or a divisor class. We reserve the notation $[D]$ to denote the image of a divisor (or a divisor class) in the Néron-Severi group. We also pass between line bundles and their representative divisors without comment, and because of this we have chosen to write the tensor product on line bundles as addition: especially, we write $nL$ instead of $L^{\otimes n}$.

The letters $n$ and $p$ shall always denote respectively a positive integer and a prime

number, and they are always assumed to be *indivisible* by the characteristic of $k$. If $G$ is an abelian group (resp. $G_{/k}$ a commutative algebraic $k$-group scheme), then $G[n]$ denotes the subgroup (resp. subgroup scheme) defined as the kernel of $[n]$, the multiplication by $n$ map. Because of our assumption on $n$, $G[n]$ is a finite étale group scheme, so may be identified with its associated $\mathfrak{g}_k$-module. $\mathbb{G}_m$ denotes the multiplicative group, and we put $\mu_n = \mathbb{G}_m[n]$.

If $M$ is a $\mathfrak{g}_k$-module, we write $H^i(k, M)$ for the Galois cohomology group $H^i(\mathfrak{g}_k, M)$. For an arbitrary $\mathfrak{g}_k$-group, we have $H^1(k, G) = H^1(\mathfrak{g}_k, G)$, which has the structure of a pointed set.

If $M$ is a finite $\mathfrak{g}_k$-module, we write $M^* = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z}(1)) = \mathrm{Hom}(M, \mathbb{G}_m[\mathrm{tors}])$ for its Cartier dual and $M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ for its Pontrjagin dual.

If $M$ is a trivial $\mathfrak{g}_k$-module, we may speak of elements of $H^1(k, M) = \mathrm{Hom}(\mathfrak{g}_k, M)$ as "characters," even though the extension cut out by such a class need not be cyclic. The point is that such classes behave in a very easily understood way: they have a *unique* minimal splitting field, which is an abelian extension of $k$.

## 2. Period-index problems in Galois cohomology

The first two sections contain foundational material on period-index problems in general and in Weil-Châtelet groups in particular. None of these results are new, but we have preferred to collect them here for the convenience of the reader (and so that authors of subsequent papers may give a single reference). The third section contains some discussion of possible variants on the index.

2.1. **The period and index of a cohomology class.** Let $M$ be a $\mathfrak{g}_k$-module, $i > 0$ an integer and $\eta \in H^i(k, M) = H^i(\mathfrak{g}_k, M)$ a Galois cohomology class. The **period** $n = p(\eta)$ is its order as an element of the torsion abelian group $H^i(k, G)$. The **index** $i(\eta)$ is the greatest common divisor of all degrees of finite field extensions $l/k$ that split $\eta$, i.e., such that $\eta|_{\mathfrak{g}_L} = 0$.

**Proposition 11.** *Let $\eta \in H^i(k, M)$ be any Galois cohomology class, with $i > 0$.*
*a) The period $n$ of $\eta$ divides its index $i(\eta)$.*
*b) The period and index of $\eta$ have the same prime divisors.*
*c) If $l/k$ has degree prime to the period of $\eta$, then $p(\eta|_l) = p(\eta)$ and $i(\eta|_l) = i(\eta)$.*
*d) (Primary decomposition) Let $\eta = \eta_1 + \ldots + \eta_r$ be the primary decomposition of $\eta$ corresponding to the factorization $n = p(\eta) = p_1^{a_1} \cdots p_r^{a_r}$, i.e., $\eta_i = \frac{n}{p_i^{a_i}}\eta$. Then $i(\eta) = \prod_{i=1}^r i(\eta_i)$.*

*Proof*: $l/k$ is a degree $n$ splitting field for $\eta$, then $0 = \mathrm{Cor}(\mathrm{Res}(\eta)) = n\eta$ (see [Se2, Prop. 7.6]), showing that the period divides the index.

For part b): let $p$ be a prime number which is prime to the period of $\eta$. Let $f/k$ be a finite Galois splitting field, and let $l/k$ be the subextension corresponding to some Sylow $p$-subgroup of $\mathfrak{g}_{f/k}$. Consider the restriction of $\eta$ to $\mathfrak{g}_l$. On the one hand, its period divides the period of $\eta$ hence remains prime to $p$, but on the other hand by construction this class is split over a field extension whose degree is a power of $p$, so by the first part of the proposition its period is a power of $p$. Therefore $l$ is a splitting field for $\eta$, so the index of $\eta$ is prime to $p$.

The remaining parts are routine and left to the reader.

**Proposition 12.** *Let $M$ be a finite $\mathfrak{g}_k$-module and $\eta \in H^1(k, M)$.*
*a) The class $\eta$ can be split by a field extension of degree at most $\#M$, so $i(\eta)|\#M$.*
*b) If $M$ is a trivial $\mathfrak{g}_k$-module, the index of $\eta$ is attained: there exists $l/k$ of degree $i(\eta)$ such that $\eta|_l = 0$.*

*Proof* (Lenstra): Let $\xi : \mathfrak{g}_k \to M$ be a one-cocycle representing $\eta$. Define $H \subset \mathfrak{g}_k$ to be the subset of elements $\sigma$ such that $\eta(\sigma) = 0$. Despite the fact that $\xi$ is not necessarily a homomorphism, one nevertheless has that $H$ is a subgroup of $\mathfrak{g}_k$ and that $\xi$ induces an injective map of sets

$$\xi : \mathfrak{g}_k/H \hookrightarrow M,$$

where $\mathfrak{g}_k/H$ is the right coset space. Thus $H = \mathfrak{g}_l$ corresponds to a splitting field of degree at most $\#M$, giving the first statement of part a). In particular $i(\eta) \leq \#M$. If $M$ has prime-power order, then we must have that $i(\eta)|\#M$, and the general case follows by primary decomposition. For part b), if $M$ is trivial, then $H^1(k, M) = \mathrm{Hom}(\mathfrak{g}_k, M)$ is just the group of "$M$-valued characters of $\mathfrak{g}_k$." In particular, every class $\eta \in H^1(k, M)$ has a unique minimal splitting field, namely the fixed field $l$ of $\ker(\eta)$, an abelian extension. In this case $\mathfrak{g}_{l/k} \hookrightarrow M$ is a homomorphism of groups and part b) follows.

Remark: The hypothesis $i = 1$ in the proposition is necessary: e.g., elements of $Br(k)[n] = H^2(k, \mu_n)$ need not have index $n$.

2.2. **Results on Weil-Châtelet groups.**

**Corollary 13.** *Let $A_{/k}$ be an abelian variety of dimension $g$, $n$ a positive integer – indivisible, as always, by the characteristic of $k$ – and $V \in H^1(k, A)[n]$. Then $V$ is split by some field extension $l/k$ of degree at most $n^{2g}$; in particular $i(V)$ divides $n^{2g}$. If $A[n]$ is $\mathfrak{g}_k$-trivial, $V$ is split by a field extension of degree dividing $n^{2g}$.*

*Proof:* For any field extension $l/k$ we have a Kummer sequence

$$0 \to A(l)/nA(l) \to H^1(l, A[n]) \to H^1(l, A)[n] \to 0,$$

compatible with the restriction maps from $k$ to $l$. Thus it is sufficient to trivialize any lift $\xi$ of $V$ to $H^1(k, A[n])$. Since $\#A[n] = n^{2g}$, the conclusion follows from Proposition 12.

If there is no restriction on the field $k$, the bound $i \mid n^{2g}$ is optimal:

**Proposition 14.** *(Lang-Tate)*
*a) Suppose we have a field $k$, a $g$-dimensional abelian variety $A_{/k}$ and a positive integer $n$ satisfying the following hypotheses:*

- *$A[n]$ is $\mathfrak{g}_k$-trivial.*
- *For every finite extension $l/k$, $A(l)$ is $n$-divisible.*
- *There exists a Galois extension $l_0/k$ with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$.*

*Then for all $a$, $1 \leq a \leq 2g$, there is a cohomology class $\eta \in H^1(k, A)$ of period $n$ and index $n^a$.*
*b) The hypotheses of part a) are satisfied for an isotrivial abelian variety (i.e., one arising by basechange from $\mathbb{C}$) over the iterated Laurent series field $k_{2g} := \mathbb{C}((t_1))\cdots((t_{2g}))$.*

We will also need the following simple result [LaTa, Theorem 6]:

**Proposition 15.** *(Lang-Tate) Let $v$ be a discrete valuation on a field $k$, with completion $k_v$. Let $n$ be a positive integer and $A_{/k}$ be an abelian variety with $A[n]$ a trivial $\mathfrak{g}_k$-module. Suppose moreover that $k$ contains the $n$th roots of unity. Then the local restriction map $H^1(k, A)[n] \to H^1(k_v, A)[n]$ is surjective.*

Remark: If $A$ is principally polarized, then, because of Weil's $\mathfrak{g}_k$-equivariant pairing $A[n] \times A[n] \to \mu_n$, $A[n] = A[n](k)$ implies $\mu_n = \mu_n(k)$.

2.3. **Variations on the index.** If $k$ were not perfect we would have to decide whether, in the definition of the index, to allow not necessarily separable splitting fields. The standard practice (cf. [Li1]) is to define the index as the gcd of degrees of *all* finite splitting fields, and the **separable index** $i_s(\eta)$ to be the gcd restricted to separable splitting fields. It is easy to see that the results of §2.1 hold for both the index and the separable index. It may well be that $i(V) = i_s(V)$ for all principal homogeneous spaces $V$ – in the terminology of §4, this is true for the Picard index of any variety and in particular in dimension one [Li1], [Ha].

Each of the main theorems of this paper has an analogue over an arbitrary field, but sometimes one needs to use the separable index and sometimes the index. As we are, to our taste, already entertaining enough technical issues, it seems wise to concentrate on the case of perfect $k$.

The Galois index: The definition of the index does of course allow not-necessarily normal field extensions $l/k$. The **Galois index** $i_G(\eta)$, defined using this restriction, can properly exceed the index. The question of equality $i_G(\eta) = i(\eta)$ for classes in the Brauer group is equivalent to the question of whether a division algebra is a crossed-product algebras. By deep work of Amitsur [Am] we know that the answer to this question is – for most periods $n$ – generically negative.

Here is an example to show that $i_G > i$ can occur in WC-groups. Let $k$ be a $p$-adic field with residue cardinality $p^a$ and $A_{/k}$ an abelian variety with good reduction. Suppose that $\ell > p^a$ is a prime and $V \in H^1(k, A)[\ell]$ is a nontrivial element. Then $i_G(V) > i(V)$. This is obtained by repeated application of an aforementioned result of Lang and Tate, which can be rephrased as: let $m/f$ be an extension of $p$-adic fields and $A/f$ an abelian variety with good reduction. Then the natural map $H^1(f, A)[\ell] \to H^1(m, A)[\ell]$ is the zero map if $\ell \mid e(m/f)$ and is injective otherwise. In particular, $i(V) = \ell$. But let $l/k$ be any Galois splitting field for $V$. We claim that $l$ must contain $\mu_\ell$, hence $\ell - 1 = [k(\mu_\ell) : k] \mid [l : k]$, so that $\ell - 1$ divides $i_G(V)$. Indeed, $l/k$ can be decomposed as a tower $k \subset l_1 \subset l_2 \subset l_3 = l$, where $l_1/k$ is unramified, $l_2/l_1$ is totally ramified of degree prime to $p$, and $l_3/l_2$ is totally ramified and of degree a power of $p$. We get that the restriction maps from $l$ to $l_1$ and from $l_2$ to $l_3$ are both injective on elements of period $\ell$, so $V|_{l_1} \neq 0$ and $V|_{l_2} = 0$. That is, $V|_{l_1}$ is killed by the totally tamely ramified extension $l_2/l_1$, which is necessarily of the form $l_2 = l_1[T]/(T^a - \pi)$, where $\ell \mid a$ and $\pi$ is a uniformizer of $l_1$. But if this extension is Galois, $l_1$ contains the $\ell$th roots of unity, establishing the claim. Of course we assumed that such a nontrivial $V$ exists, which is not always the case (indeed, for fixed $A_{/k}$ such a $V$ exists for at most finitely many primes $\ell$), but we may certainly arrange for such classes to exist: e.g., fix a prime $p$, and let $\ell$ be a prime such that $p + 1 < \ell < p + 1 + \sqrt{2}p$. By the Hasse-Deuring-Waterhouse theorem, there is an (ordinary) elliptic curve $E/\mathbb{F}_p$ such that $E(\mathbb{F}_p) \cong \mathbb{Z}/\ell\mathbb{Z}$; let

$\tilde{E}/\mathbb{Q}_p$ be its canonical lift. Then $\mathbb{Z}/\ell\mathbb{Z} \cong \tilde{E}(\mathbb{Q}_p)/\ell\tilde{E}(\mathbb{Q}_p) \cong H^1(\mathbb{Q}_p, E)[\ell]$. The last isomorphism is by Tate's duality theorem (recalled later as Theorem 32).

Remark: The above argument can be adapted to produce examples of genus one curves over $\mathbb{Q}_p$ without any abelian splitting field. For applications of this to the construction of algebraic curves of higher genus without abelian points, see [Cl3].

This example should be compared with the case of principal homogeneous spaces $V$ over $p$-adically uniformized abelian varieties discussed in the next section: for all such $V$ we have $i(\eta) = i_G(\eta)$. It would be nice to know whether $i = i_G$ in the case of good reduction and period divisible by the residue characteristic.

Finally and most importantly, one can ask for examples in which the index is not attained, i.e., such that the greatest common divisor of degrees of splitting fields is not itself the degree of a splitting field. I do not know of such an example (anywhere in Galois cohomology). It is well-known that the index is attained for classes in the Brauer group $H^2(k, \mathbb{G}_m)$. The attainment of the index for elements of the Weil-Châtelet group of an elliptic curve was observed in [LaTa]. In contrast, the attainment of the index is an important *open problem* in the Weil-Châtelet group of a higher-dimensional abelian variety, and our ignorance of this attainment leads us to define the **m-invariant** $m(\eta)$ of a Galois cohomology class as the minimal degree of a splitting field.

Clearly the best response to the possibility of $i(V) < m(V)$ is to give upper bounds on the m-invariant and lower bounds on the index. Fortunately enough, it turns out that most of our main results results are phrased in this way.

## 3. Large indices over local, strictly local and global fields

3.1. **Travaux de Gerritzen.** In this section we give an account of some work of Gerritzen on the period-index problem in the Weil-Châtelet group of an analytically uniformized abelian variety. Because these results are closely related to the proof of Theorem 1, we will give complete proofs.

**Proposition 16.** *(Gerritzen) Let $k$ be any field, with absolute Galois group $\mathfrak{g}_k$. Let $\tilde{A}$ be a $\mathfrak{g}_k$-module and $\Gamma \subseteq \tilde{A}$ a $\mathfrak{g}_k$-submodule which is torsionfree as a $\mathbb{Z}$-module and such that $\Gamma^{\mathfrak{g}_k} = \Gamma$; put $A := \tilde{A}/\Gamma$. Suppose also that $H^1(l, \tilde{A}) = 0$ for all finite extensions $l/k$. Let $\eta \in H^1(k, A)$ be a class of exact period $n$. Then:*
*a) $\eta$ has a* unique *minimal splitting field $L = L(\eta)$.*
*b) The extension $l/k$ is abelian of exponent $n$.*
*c) $i(\eta) \mid n^g$, where $g = \dim_{\mathbb{Q}}(\Gamma \otimes \mathbb{Q})$ is the rank of $\Gamma$.*

*Proof:* We take $\mathfrak{g}_k$-cohomology of the short exact sequence

$$0 \to \Gamma \to \tilde{A} \to A \to 0, \tag{1}$$

and using $H^1(k, \tilde{A}) = 0$, we get an injection $\delta : H^1(k, A) \hookrightarrow H^2(k, \Gamma)$. Also, since $\overline{\Gamma} = \Gamma \otimes \mathbb{Q}$ is cohomologically trivial, there is a canonical isomorphism $H^2(k, \Gamma) \cong H^1(k, (\mathbb{Q}/\mathbb{Z})^g) = H^1(k, \mathbb{Q}/\mathbb{Z})^g =: X_A(\mathfrak{g}_k)$, i.e., $g$ copies of the character group of $\mathfrak{g}_k$. Indeed, the assumptions are such that for any finite extension $l/k$, we may view (1) as a sequence of $\mathfrak{g}_l$ modules and get the same result: we get

for every $l$ an injection $\delta_l : H^1(l, A) \hookrightarrow H^1(l, \mathbb{Q}/\mathbb{Z})^g = X_A(\mathfrak{g}_l)$, and these various maps are compatible with restriction. Thus splitting $\eta$ is equivalent to splitting the character $\delta_k(\eta)$. But $\delta_k(\eta)$ cuts out a field extension $l(\eta)/k$ which is abelian of exponent $n$, of order dividing $n^g$, and evidently the unique minimal splitting field, completing the proof.

Recall that a $g$-dimensional abelian variety defined over a $p$-adic field admits an analytic uniformization if it is isomorphic, as a rigid $k$-analytic group, to $\mathbb{G}_m^g/\Gamma$, where $\Gamma \cong \mathbb{Z}^g$ is a discrete subgroup.

**Theorem 17.** *(Gerritzen) Let $A_{/k}$ be a $g$-dimensional analytically uniformized abelian variety over a $p$-adic field.*
*a) For any $V \in H^1(k, A)[n]$, $i(V) \mid n^g$.*
*b) If $\Gamma \subseteq nA(k)$, then $\delta_k : H^1(k, A)[n] \to H^1(k, \mathbb{Z}/n\mathbb{Z})^g$ is an isomorphism of finite groups.*

*Proof:* Part a) follows immediately from the previous proposition by taking $\tilde{A} = \mathbb{G}_m^g(\overline{k})$: note that $H^1(l, \tilde{A}) = 0$ for all $l/k$ by Hilbert 90. As for part b), we have an injection of finite groups, so it's enough to see that they have the same cardinality. We recall the following important theorem of Tate: for all finite $\mathfrak{g}_k$-modules $M$, $H^1(k, M^*) \cong H^1(k, M)^\vee$ [Se1, § II.5.2, Theorem 2]. Applying this to $M = \mathbb{Z}/n\mathbb{Z}$, we get that $H^1(k, \mathbb{Z}/n\mathbb{Z}) \cong H^1(k, \mu_n) \cong k^*/k^{*n} \cong (\mathbb{Z}/n\mathbb{Z})^r$ for some positive integer $r$. Thus

$$\#H^1(k, \mathbb{Z}/n\mathbb{Z})^g = n^{rg}.$$

On the other hand, by Tate's duality theorem (Theorem 32),

$$H^1(k, A)[n] \cong \frac{A(k)}{nA(k)} = \frac{\mathbb{G}_m^g(k)/\Gamma}{(\mathbb{G}_m^g(k))^n/(\Gamma \cap \mathbb{G}_m^g(k)^n)} \cong \left(\frac{k^*}{k^{*n}}\right)^g,$$

the last isomorphism because of the assumption that every element of $\Gamma$ is an $n$th power in $\mathbb{G}_m^g(k)$. Thus we also have $\#H^1(k, A)[n] = n^{rg}$, completing the proof.

3.2. **The proof of Theorem 1 in the $p$-adic case.** We now specialize to the following situation: let $k/\mathbb{Q}_p$ be a finite extension of degree $a$; we assume that $k$ contains the $p$th roots of unity. One knows [Ta] that

$$[k^* : k^{*p}] = p^{a+2}. \tag{2}$$

Let $E/\mathbb{Q}_p$ be an elliptic curve with analytic uniformization $\mathbb{G}_m/\langle q \rangle$, where $q$ is a $p$th power in $\mathbb{Q}_p$, *a fortiori* in $k$ – this choice is so that the hypothesis of Theorem 17b) is satisfied for $n = p$. As we saw in the proof of Theorem 17, $\dim_{\mathbb{F}_p} H^1(k, E)[p] = p^{a+2}$. Let $P_1, \ldots, P_{a+2}$ be an $\mathbb{F}_p$-basis for $H^1(k, E)[p]$. Then Proposition 16 associates to each $E_i$ a unique minimal splitting field $l_i$, such that $l_i/k$ is cyclic of degree $p$. Because of the injectivity of $\delta_k$, the characters $\{\delta_k(P_i)\}_{i=1}^{a+2}$, remain $\mathbb{F}_p$-linearly independent, so cut out an abelian extension $l^{(p)} = l_1 \cdots l_{a+2}$ of exponent $p$. Let $P = P_1 \times \cdots \times P_{a+2}$, viewed as a principal homogeneous space over the (analytically uniformized) abelian variety $A = E^{a+2}$. Evidently a field $l$ splits $P$ exactly when it splits each $P_i$, so $l^{(p)}$ is the unique minimal splitting field of $P$, which therefore has index $p^{a+2} = p^{\dim A}$.

3.3. **Applications to $k_\infty$.** Let $k$ be a $p$-adic field containing the $p$th roots of unity, and denote by $k_\infty$ the maximal unramified extension of $k$. Let $l_1/k$ be the unique unramified extension of degree $p$, and let $l_1, l_2, \dots, l_{a+2}$ be an $\mathbb{F}_p$-basis for the set of abelian $p$-extensions of $k$ (i.e., a linearly disjoint set of extension fields whose compositum is the maximal abelian extension of exponent $p$). Under the bijection $\delta_k$ the $l_i$'s are splitting fields of homogeneous spaces $P_1, \dots, P_{a+2}$; let $Q := P_2 \times P_3 \times \cdots \times P_{a+2}$.

We claim that the index of $Q/k_\infty$ is the same as its index over $k$, namely $p^{a+1}$. Indeed, let $m/k_\infty$ be a degree $N$ splitting field of $Q/k_\infty$. Then $Q/k$ is split by some finite extension $m'/k$, such that $m' \cap k_\infty = k_b$ (the unramified extension of degree $b$) for some $b$, and $[m' : k_b] \leq N$. By construction, the unique minimal splitting field for $Q$ is disjoint from $k_b$, so the index of $Q$ is not reduced by restriction to $k_b$. Thus $p^{a+1} \mid N$, and we conclude that the index of $Q/k_\infty$ is $p^{a+1}$. Since we may view $k_\infty$ as the maximal unramified extension not just of $k$ but of any $k_b$, we may arrange for $a + 1 = [l : \mathbb{Q}_p] \geq g$, completing the proof.

3.4. **Applications to number fields.** Fix $p$ and $g$. Let $E/\mathbb{Q}$ be any elliptic curve with potentially multiplicative reduction at $p$ (e.g., one with $j$-invariant $\frac{1}{p}$). Choose a number field $k$ which is sufficiently large so as to satisfy all of the following:

a) $E[p]$ is a trivial $\mathfrak{g}_k$-module ($\implies \mathbb{Q}(\mu_p) \subset k$),
b) $k$ has a place $v \mid p$ of local degree at least $g - 2$,
c) $E/k_v$ has split multiplicative reduction.

From §3.2, we have a class $\eta_v \in H^1(k_v, E^g)$ with period $p$ and index $p^g$; by Proposition 15 there exists a class $\eta \in H^1(k, E^g)[p]$ mapping to $\eta_v$. Thus $\eta$ is a global class of period $p$ and index *at least* $p^g$.

Examples over $\mathbb{Q}$: Let $A_{/k}$ be as above and consider $\mathrm{Res}_{k/\mathbb{Q}} A$, the abelian variety over $\mathbb{Q}$ obtained from $A_{/k}$ by restriction of scalars. There is a canonical isomorphism $\iota : H^1(k, A) \xrightarrow{\sim} H^1(\mathbb{Q}, \mathrm{Res}_{k/\mathbb{Q}} A)$ (cf. [AgSt]); if $\eta \in H^1(k, A)[p]$ has index $p^i$, then the corresponding class $\iota(\eta)$ in $H^1(\mathbb{Q}, \mathrm{Res}_{k/\mathbb{Q}} A)$ must have period $p$ and index at least $p^i$: indeed, if $m/\mathbb{Q}$ is a splitting field for $\iota(\eta)$, then $ml/l$ splits $\eta$.

Notice however that $\dim \mathrm{Res}_{k/\mathbb{Q}} A = [k : \mathbb{Q}] \dim A$, so in general we do not get classes of period $p$ and index $p^{\dim A}$ over $\mathbb{Q}$ using this trick. But let us look at the case $p = 2,\ g = 3$.[5]

**Proposition 18.** *There exists an abelian 3-fold $A/\mathbb{Q}$ and a principal homogeneous space $X \in H^1(\mathbb{Q}, A)$ of period 2 and index at least 8.*

*Proof*: From the above discussion, we need only find an elliptic curve $E/\mathbb{Q}$ with $E[2] = E[2](\mathbb{Q})$ and with split multiplicative reduction at 2. To do this:

[5] *A fortiori* the construction works for $g = 2$. Indeed, when $g = 2$ one may take the period to be prime to $p$; cf. [Li1].

On the one hand, the elliptic curve labeled 4290Z2 in Cremona's tables, with minimal Weierstrass model $E : y^2 + xy = x^3 - 66x$ fits the bill.[6] Alternately, we have the following

**Proposition 19.** *Let $X$ be the modular curve corresponding to the congruence subgroup $\Gamma = \Gamma(2) \cap \Gamma_1(4)$ of $SL_2(\mathbb{Z})$. Then there are infinitely many $P \in X(\mathbb{Q})$ with split multiplicative reduction at 2.*

*Proof*: One knows that $X/\mathbb{Q}$ is the fine moduli space for $\Gamma$-structured elliptic curves over $\mathbb{Q}$, and also that it has genus 0. As a smooth genus 0 curve, $X$ is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ if and only if it has points everywhere locally, or even at every finite place $p$. But the Tate curve $\mathbb{G}_m/ < p^4 >$ gives a point on $X(\mathbb{Q}_p)$. So $X \cong_{\mathbb{Q}} \mathbb{P}^1$, as is well-known.[7] Now let $P_0 \in X(\mathbb{Q}_2)$ be a "Tate point" as above. We claim that there is an analytically open neighborhood $U$ of $P_0$ in $X(\mathbb{Q}_2)$ consisting of points with Tate uniformizations – i.e. with split multiplicative reduction. Indeed, consider the universal $\Gamma$-structured elliptic curve $\mathcal{E}$ over an analytic neighborhood of $P_0$ – it is given by a Weierstrass equation with analytically varying coefficients. The condition that the $\Gamma$-structured elliptic curve over $P$ have split multiplicative reduction is that the quantity $c_4$ be nonzero and that the quadratic (lowest-degree) form of the Weierstrass equation factor over $\mathbb{Q}_2$ – these are both open conditions. Since $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_2)$, $X(\mathbb{Q}) \cap U$ is infinite, which was to be shown.

## 4. Albanese and Picard varieties

4.1. **Background on Albanese, Picard and Néron-Severi.** This section contains foundational material on Albanese varieties, Picard varieties and Néron-Severi groups in the context of arithmetic geometry. Apart from fixing notation, our goal here is to record a technical fact about Néron-Severi groups of principal homogeneous spaces (Proposition 20) which will come in handy later on.

For $X/k$ a variety, $\mathbf{Alb}(X)$ denotes the total Albanese scheme of $X$ and $\mathbf{Pic}(X)$ denotes the total Picard scheme of $X$. These are the reduced subschemes of the schemes parameterizing, respectively, zero-cycles on $V$ modulo Albanese equivalence[8], and divisors modulo linear equivalence. That is to say, these are objects representing sheafified versions of the usual Albanese and Picard groups, so that e.g. $\mathbf{Alb}(X)(k) = \mathrm{Alb}(X/\overline{k})^{\mathfrak{g}_k}$, and similarly for the Picard scheme.

One must keep in mind that the natural map $\mathrm{Pic}(X/k) \to \mathbf{Pic}(X)(k)$ is injective but not generally surjective (unless $X(k) \neq \emptyset$): that is, not every $k$-rational divisor class need be represented by a $k$-rational divisor. Indeed, there is a well-known (e.g. [BLR, §9.1]) exact sequence

$$0 \to \mathrm{Pic}(X) \to \mathbf{Pic}(X)(k) \xrightarrow{\delta} \mathrm{Br}(k) \xrightarrow{\epsilon} \mathrm{Br}(X). \tag{3}$$

In other words, the obstruction to a $k$-rational divisor class admitting a $k$-rational divisor is an element of the Brauer group of $k$.

[6]Thanks to Kevin Buzzard, who came up with this equation by pure thought.

[7]Alternately, recall that all modular curves corresponding to congruence subgroups have $\mathbb{Q}$-rational cusps.

[8]Rationally equivalent zero cycles are Albanese equivalent, i.e., there is a canonical surjective map $\mathbf{CH}_0(X) \to \mathbf{Alb}(X)$. In dimension greater than one, this map is very often not an injection.

Remark: It follows (e.g. [BLR, p.204, Prop. 4]) that if $X$ has a $k$-rational point, $\delta \equiv 0$. In particular, if $A_{/k}$ is an abelian variety, we have $\mathrm{Pic}(A) = \mathbf{Pic}(A)(k)$.

The Albanese and Picard schemes are locally algebraic; indeed, each is an extension of a finite rank $\mathbb{Z}$-module by an abelian variety. In the Albanese case this is induced by the degree map:

$$0 \to \mathbf{Alb}^0(X) \to \mathbf{Alb}(X) \stackrel{\deg}{\to} \mathbb{Z} \to 0. \tag{4}$$

In the Picard case we have the subgroup scheme $\mathbf{Pic}^0(X)$ parameterizing divisor classes algebraically equivalent to zero:

$$0 \to \mathbf{Pic}^0(X) \to \mathbf{Pic}(X) \to NS(X) \to 0; \tag{5}$$

here $NS(X)$ is the Néron-Severi group of $X$.

The abelian varieties $\mathbf{Alb}^0(X)/k$ and $\mathbf{Pic}^0(X)/k$ are in duality. Especially, if $A_{/k}$ is an abelian variety, the map $P \mapsto [P]-[O]$ induces an isomorphism $A \stackrel{\sim}{\to} \mathbf{Alb}^0(A)$, and this duality becomes the usual $\mathrm{Pic}^0(A) = A^\vee$.

By taking $\overline{k}$-valued points in (1) or (2), we get short exact sequences of $\mathfrak{g}_k$-modules. The $\mathfrak{g}_k$-module structure on $\mathbf{Alb}(X)/\mathbf{Alb}^0(X)$ is necessarily trivial, but it need not be so for the Néron-Severi group.

Now let $V_{/k}$ be a principal homogeneous space for $A$, so $\mathbf{Alb}^0(V) = A$, $\mathbf{Pic}^0(V) = A^\vee$. (In fact, a principal homogeneous space structure on $V$ is equivalent to the choice of an isomorphism of $\mathbf{Alb}^0(V)$ with $A$.) We have also that $V_{/\overline{k}} \cong A_{/\overline{k}}$, so that $NS(A) \cong NS(V)$ as $\mathbb{Z}$-modules. But more is true.

**Proposition 20.** *There exists a map $\psi : NS(A) \to NS(V)$ which is an isomorphism of $\mathfrak{g}_k$-modules.*

*Proof:* Let $\mu : A \times V \to V$ denote the $A$-action on $V$. Also let $m : V \times V \to A$ denote the corresponding subtraction map, i.e., the $k$-map such that $m(\mu(a,v),v) = a$ for all $v \in V(\overline{k})$, $a \in A(\overline{k})$. Fix any $\overline{p} \in V(\overline{k})$, and consider the isomorphism

$$\tau : V/\overline{k} \to A/\overline{k}, \ v \mapsto m(v, \overline{p}).$$

We may use $\tau$ to pull back geometric line bundles from $A$ to $V$. Since the property of a line bundle being algebraically equivalent to zero is preserved under all isomorphisms of abelian varieties, $\tau^*$ induces a $\mathbb{Z}$-module isomorphism $\psi : NS(A) \to NS(V)$. We claim that $\psi$ is necessarily $\mathfrak{g}_k$-equivariant, i.e., that for all $\sigma \in \mathfrak{g}_k$ and $L \in \mathrm{Pic}(A/\overline{k})$,

$$\psi(\sigma(L)) - \sigma(\psi(L)) \in \mathrm{Pic}^0(V/\overline{k}).$$

Indeed

$$\psi(\sigma(L)) - \sigma(\psi(L)) = \mu(\sigma(L), \overline{p}) - \sigma(\mu(L, \overline{p})) =$$

$$\mu(\sigma(L), \overline{p}) - \mu(\sigma(L), \sigma(\overline{p})) = \mu(\sigma(L), \overline{p}) - \mu((\mu(\sigma(L), \overline{p}), m(\sigma(\overline{p}), \overline{p}))$$

i.e., the difference between a line bundle and its translate, which is algebraically equivalent to zero.

Alternate proof: let $k(V)$ be the function field of $V$. Then, since $V_{/k(V)} \cong A_{/k(V)}$,

their Néron-Severi groups are isomorphic as $\mathfrak{g}_{k(V)}$-modules, hence (since $k$ is algebraically closed in $k(V)$) as $\mathfrak{g}_k$-modules.

4.2. **Polarizations versus strong polarizations.** Recall that a **polarization** on an abelian variety $A_{/k}$ is given by an ample line bundle $L$ on $A_{/\overline{k}}$ which is algebraically equivalent to each of its Galois conjugates: that is to say, the $k$-rationality condition on the polarization takes place in $NS(A)$. We must distinguish this from the notion of an element of $NS(A)$ represented by a $k$-rational ample line bundle, so we call the latter a **strong polarization**.

We shall call a line bundle $P \in \mathrm{Pic}(A)$ inducing a principal polarization a principal line bundle and an abelian variety endowed with a principal line bundle a strongly principally polarized abelian variety.

The obstruction to a polarization being strong comes from taking Galois cohomology of the exact sequence

$$0 \to A^\vee(\overline{k}) \to \mathbf{Pic}(A)(\overline{k}) \to NS(A) \to 0$$

to get

$$0 \to A^\vee(k) \to \mathrm{Pic}(A) \to NS(A)(k) \to H^1(\mathfrak{g}_k, A^\vee(k)).$$

(Here we have used the fact that $\mathrm{Pic}(A) = \mathbf{Pic}(A)(k)$, since $A(k) \neq \emptyset$.) In other words, to every $\lambda \in NS(A)^{\mathfrak{g}_k}$ we associate a class $c_\lambda \in H^1(k, A^\vee)$. In fact, since $A^\vee = \mathrm{Pic}^0(A)$ classifies skew-symmetric divisor classes on $A$, we have that $[-1]_A$ induces $-1$ on $\mathrm{Pic}^0(A)$, whereas $[-1]_A$ acts as the identity on $NS(A)$, so that $c_\lambda \in H^1(k, A^\vee)[2]$. A thorough analysis of these classes is the subject of [PoSt]; they show in particular that $c_\lambda$ vanishes when $k$ is a $p$-adic field, so that when $k$ is a number field the class $c_\lambda$ lies in $Ш(k, A)[2]$ but is not necessarily trivial.

We will call an abelian variety $A_{/k}$ **unobstructed** if $NS(A)(k) \to H^1(k, A^\vee)$ is the zero map. Note well that every abelian variety defined over a $p$-adic field is unobstructed.

4.3. **Separate period-index problems for the Albanese and the Picard.** Let $V_{/k}$ be any variety. Define the **Albanese period** $p_{\mathrm{Alb}}(V)$ of $V$ to be the order of the cokernel of the degree map $\mathbf{Alb}(V)(k) \stackrel{\deg}{\to} \mathbb{Z}$. For any $i \in \mathbb{Z}$, we denote $\mathbf{Alb}^i(V)$ to be the degree $i$ component of the Albanese scheme, so $\mathbf{Alb}^i(V)$ is a principal homogeneous space for $A := \mathbf{Alb}^0(V)$. Then the Albanese period is the period of the sequence $\mathbf{Alb}^1(V)$, $\mathbf{Alb}^2(V)\ldots$, or the least positive $i$ such that $\mathbf{Alb}^i(V)(k) \neq \emptyset$. (Note that the Albanese period could also be computed in $\mathbf{CH}_0(V)$.) In addition, using the exact sequence in Galois cohomology derived from taking $\overline{k}$-valued points in (4), the Albanese period is equal to the order of the kernel of the map $\mathbb{Z} \to H^1(k, \mathbf{Alb}^0(V))$.

The **index** of $V$ is the cokernel of the map $Z_0(V)^{\mathfrak{g}_k} \to \mathbb{Z}$, the least positive degree of a $k$-rational zero-cycle.

For any variety $V$ there is a natural morphism $V \to \mathbf{Alb}^1(V)$. The functor $\mathbf{Alb}^1$ is idempotent: for a principal homogeneous space $V$ of an abelian variety $A = \mathrm{Alb}^0(V)$ the map $V \to \mathbf{Alb}^1(V)$ is an isomorphism. For every field extension $l/k$ for which

$V(l) \neq \emptyset$, we also have $\mathbf{Alb}^1(V)(l) \neq \emptyset$. In other words, if we define the **Albanese index** $i_{\mathrm{Alb}}(V)$ of $V$ to be the index of $\mathbf{Alb}^1(V)$, then we have $i_{\mathrm{Alb}}(V) \mid i(V)$. In general we do not have equality: e.g., for any $i$, there exists a Severi-Brauer variety $X_{/\mathbb{Q}}$ of index $i$. Since projective space is simply connected, we have $\mathrm{Alb}^0(X) = 0$ so that $i_{\mathrm{Alb}}(X) = 1$. However, when $C$ is a curve, Harase has shown that $i_{\mathrm{Alb}}(C) \mid 2i(C)^2$ [Ha, Theorem 5].

Define the **Picard period** $p_{\mathrm{Pic}}(V)$ of $V_{/k}$ to be the exponent of the cokernel of the map $\mathbf{Pic}(V)(k) \to NS(V)(k)$. Using the exact sequence (2), the Picard period is also the exponent of the image of the connecting map $\delta : NS(V)(k) \to H^1(k, \mathbf{Pic}^0(V))$. Finally, define the **Picard index** $i_{\mathrm{Pic}}(V)$ of $V_{/k}$ to be the exponent of the cokernel of the map $\mathrm{Div}(V)(k) \to NS(V)(k)$.

**Proposition 21.** *Let $V_{/k}$ be a principal homogeneous space of $A = \mathbf{Alb}^0(V)$, and consider the map $\delta : NS(V)(k) \to H^1(k, \mathbf{Pic}^0(V))$. Suppose that $P \in NS(V)(k)$ corresponds, under the identification of $NS(V)$ with $NS(A)$, to the class of a $k$-rational line bundle $L$ on $A$. Then $\delta(P)$ is the image of $[V] \in H^1(k, \mathbf{Alb}^0(V))$ under the map $H^1(\varphi_L) : H^1(k, \mathbf{Alb}^0(V)) \to H^1(k, \mathbf{Pic}^0(V))$.*

*Proof:* We use the same notation as in the proof of Proposition 18; especially, recall we have chosen a $\overline{p} \in V(\overline{k})$. Our assumption is then that $P$ is algebraically equivalent to a line bundle $L' = \psi(L) = \mu(L, \overline{p})$ for some $L \in \mathrm{Pic}(A)$. A cocycle representative for $\delta(P)$ is then given by $\sigma \mapsto \sigma(L') - L'$, where

$$\sigma(L') - L' = \sigma(\mu(L, \overline{p})) - \mu(L, \overline{p}) = \mu(\sigma(L), \sigma(\overline{p})) - \mu(L, \overline{p}).$$

On the other hand, $\sigma \mapsto m(\sigma(\overline{p}), \overline{p})$ gives a cocycle representative for $V \in H^1(k, A)$. The map $\varphi_L : A \to A^\vee$ is just $q \mapsto L_q - L$, so the image of the cocycle under $H^1(k, A) \to H^1(k, A^\vee)$ carries $\sigma$ to

$$L_{m(\sigma(\overline{p}), \overline{p})} - L.$$

Translating by $\overline{p}$ to view this as a line bundle on $V$, we get $\mu(\sigma(L), \sigma(\overline{p})) - \mu(L, \overline{p})$, completing the proof.

**Corollary 22.** *For a principal homogeneous space $V_{/k}$ over an* unobstructed *abelian variety $A_{/k}$ we have $p_{\mathrm{Pic}}(V) \mid p_{\mathrm{Alb}}(V)$. If $A_{/k}$ is principally polarizable then $p_{\mathrm{Alb}}(V) = p_{\mathrm{Pic}}(V)$.*

*Proof*: Put $n = p_{\mathrm{Alb}}(V)$. From the above proposition we get a factorization

$$\delta : NS(V)^{\mathfrak{g}_k} \to H^1(k, A)[n] \to H^1(k, A^\vee)$$

so that $\mathrm{Im}(\delta)$ is $n$-torsion. Conversely, a principal polarization induces an isomorphism $H^1(k, A) \to H^1(k, A^\vee)$ so that the image of $V$ has exact order $n$.

Remark: The hypotheses can be weakened somewhat: it is enough to assume the existence of a not necessarily positive $k$-rational line bundle $L$ such that $\varphi_L : A \to A^\vee$ is an isomorphism. Moreover, if the Albanese period of $V$ is odd, one does not need to assume that $A$ is unobstructed.

Remark: Proposition 21 shows that if $V \in H^1(k, A)[n]$ and $P$ is a $k$-rational line bundle on $A$, then $n[P]$ is represented by a $k$-rational divisor *class* on $V$.

4.4. **Some exact sequences.** In this section we recall some exact sequences which relate the Albanese and Picard indices of a variety $V$ to the image of the obstruction map $\delta : \mathbf{Pic}(V)(k) \to \mathrm{Br}(k)$ featured in (3). Except to explain the notation $\mathrm{Br}(V/k)$ and $\mathrm{Br}^0(V/k)$, this material is not used later in the paper, so it may safely be omitted. (Nevertheless Proposition 24 and its corollaries seem enlightening.)

Define
$$\mathrm{Br}(V/k) := \mathrm{Ker}(\epsilon) = \delta(\mathbf{Pic}(V)(k)),$$
and
$$\mathrm{Br}^0(V/k) := \delta(\mathbf{Pic}^0(V)(k)).$$
The discrepancy between these two groups is essentially the discrepancy between the Picard period and the Picard index. To see this, put
$$\mathcal{I}(V) := \mathrm{Im}(\mathrm{Div}(V) \to NS(V)(k)),$$
$$\mathcal{P}(V) := \mathrm{Ker}(NS(k) \to H^1(k, \mathbf{Pic}^0(V)) = \mathrm{Im}(\mathbf{Pic}(V)(k) \to NS(k)),$$
so that $\mathcal{I}(V) \subset \mathcal{P}(V)$ are finite index subgroups of $NS(V)(k)$. We can thus define finite abelian groups
$$I_{\mathrm{Pic}}(V) = NS(V)(k)/\mathcal{I}(V).$$
$$P_{\mathrm{Pic}}(V) = NS(V)(k)/\mathcal{P}(V),$$
and immediately from the definitions we get:

**Lemma 23.**
*a) The Picard index $i_{\mathrm{Pic}}(V)$ is the exponent of $I_{\mathrm{Pic}}(V)$.*
*b) The Picard period $p_{\mathrm{Pic}}(V)$ is the exponent of $P_{\mathrm{Pic}}(V)$.*

Applying the snake lemma to the diagram
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Pic}(V) & \longrightarrow & \mathbf{Pic}(V)(k) & \longrightarrow & \mathrm{Br}(V/k) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & NS(V)(k) & \longrightarrow & NS(V)(k) & \longrightarrow & 0 & \longrightarrow & >0 \end{array},$$
we get:

**Proposition 24.** *There is a short exact sequence*
$$0 \to \mathrm{Br}^0(V/k) \to \mathrm{Br}(V/k) \to \frac{I_{\mathrm{Pic}}(V)}{P_{\mathrm{Pic}}(V)} \to 0.$$

**Corollary 25.** *The following are equivalent:*
*a) $I_{\mathrm{Pic}}(V) = P_{\mathrm{Pic}}(V)$.*
*b) $\mathrm{Br}^0(V/k) = \mathrm{Br}(V/k)$.*
*If $V$ is a principal homogeneous space of an abelian variety $A$ then a) and b) imply*
*c) $p_{\mathrm{Pic}}(V) = i_{\mathrm{Pic}}(V)$;*
*and are equivalent to c) if $A$ has cyclic Néron-Severi group.*

**Corollary 26.** *Let $(A, P)_{/k}$ be an unobstructed, strongly principally polarized abelian variety, and let $V \in H^1(k, A)$.*
*a) If $\mathrm{Br}^0(V/k) = \mathrm{Br}(V/k)$, then $p_{\mathrm{Alb}}(V) = p_{\mathrm{Pic}}(V) = i_{\mathrm{Pic}}(V)$.*
*b) If $NS(A) \cong \mathbb{Z}$, then conversely $p_{\mathrm{Pic}}(V) = i_{\mathrm{Pic}}(V)$ implies $\mathrm{Br}(V/k) = \mathrm{Br}^0(V/k)$.*

## 5. The period-index obstruction

The first subsections echo [Cl1, §3.1] with elliptic curves replaced by principally polarized abelian varieties: we define different period-index obstruction maps and show that they coincide.

5.1. **First definition of the period-index obstruction.** For this and the following two subsections, we fix $A_{/k}$ an abelian variety and $L \in \mathrm{Pic}(A)$ a line bundle which is ample and without basepoints. We further put $N = \dim_k H^0(A, L)$. Recall that the ampleness of $L$ implies that the homomorphism $\varphi_L : A \to A^\vee$, $x \mapsto t_x^*(L) \otimes L^{-1}$ has finite kernel, denoted $\kappa(L)$. Let $\mathcal{G}(L)$ denote the theta group associated to $L$ (e.g. [Mu], [AV]); as a functor, $\mathcal{G}(L)$ associates to a $k$-scheme $S$ the group of all isomorphisms $L_{/S} \xrightarrow{\sim} \tau_x^*(L_{/S})$ between $L_{/S}$ and one of its translates. The subgroup of automorphisms of $L$ gives rise to an embedding $\mathbb{G}_m \hookrightarrow \mathcal{G}_L$. The quotient $\mathcal{G}_L/\mathbb{G}_m$ is canonically isomorphic to $\kappa(L)$, i.e., we have a short exact sequence

$$1 \to \mathbb{G}_m \to \mathcal{G}_L \to \kappa(L) \to 0.$$

Moreover, $\mathcal{G}_L$ has a (faithful and irreducible) representation on the $k$-vector space of global sections $\Gamma(A, L)$: if $g \in \mathcal{G}_L(\overline{k})$ carries $L \xrightarrow{\sim} \tau_x^* L$ and $s \in \Gamma(A, L)$, then $g \cdot s := \tau_{-x}^*(g(s))$ [Mu, p. 295]. Thus, choosing a basis $(f_1, \ldots, f_N)$ for $\Gamma(A, L)$, we get a homomorphism $\omega : \mathcal{G}_L \to GL_N$ which carries $\mathbb{G}_m$, the center of $\mathcal{G}$, identically onto the subgroup of $GL_N$ consisting of scalar matrices.

Our choices induce identifications $\mathrm{Aut}(\mathbb{P}|L|) \cong \mathrm{Aut}(\mathbb{P}^{N-1}) \cong PGL_N$. Upon passage to the quotient by $\mathbb{G}_m$, $\omega$ induces a homomorphism $\gamma : \kappa(L) \hookrightarrow PGL_N$ identifying $\kappa(L)$ as the group of translations on $A$ extending to automorphisms of projective space. In particular, we get the following diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathcal{G}_L & \longrightarrow & \kappa(L) & \longrightarrow & 1 \\ & & {\scriptstyle =}\downarrow & & {\scriptstyle \omega}\downarrow & & {\scriptstyle \gamma}\downarrow & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & GL_N & \longrightarrow & PGL_N & \longrightarrow & 1 \end{array} \tag{6}$$

in which each row is a central extension of $\mathfrak{g}_k$-groups. Thus we have a connecting map $\Delta_1 : H^1(k, \kappa(L)) \to H^2(k, \mathbb{G}_m) = \mathrm{Br}(k)$. This is our first definition of the period-index obstruction.

5.2. **Second definition of the period-index obstruction.** Let $\mathcal{T}_2(L)$ be the set of equivalence classes of morphisms $V \to X$ such that: (i) $V$ is a principal homogeneous space of $A$; (ii) $X$ is an $(N-1)$-dimensional Severi-Brauer variety; and (iii) there exists an isomorphism of principal homogeneous spaces $\tau : V_{/\overline{k}} \to A_{\overline{k}}$ and an isomorphism $\gamma(\tau) : X_{\overline{k}} \to \mathbb{P}^{N-1}$ rendering commutative the following diagram:

$$\begin{array}{ccc} V_{\overline{k}} & \longrightarrow & X_{\overline{k}} \\ {\scriptstyle \tau}\downarrow & & {\scriptstyle \gamma(\tau)}\downarrow \\ A_{\overline{k}} & \longrightarrow & \mathbb{P}^{N-1} \end{array} .$$

Two such morphisms are regarded as equivalent if there exists an isomorphism of principal homogeneous spaces $\tau : V_1 \to V_2$ and an isomorphism $\gamma(\tau) : X_1 \to X_2$ fitting into a commutative diagram as above.

**Proposition 27.** *There is a natural bijection from the set $\mathcal{T}_2(L)$ to $H^1(k, \kappa(L))$.*

*Proof:* This follows immediately from the principle of Galois descent: namely, $\mathcal{T}(L)$ is the set of $\overline{k}/k$-twisted forms of the "diagram" $A \to \mathbb{P}^N$, whose automorphism group is $\kappa(L)$.

This gives a map $\Delta_2 : H^1(k, \kappa(L)) \to \mathrm{Br}(k)$, namely, $\Delta_2(V \to X) = [X]$, the element of the Brauer group corresponding to the Severi-Brauer variety $X$.

Remark: We shall sometimes speak of elements of $\mathcal{T}(L)$ as "diagrams of type $L$."

5.3. **Third definition of the period-index obstruction map.** Let $\mathcal{T}_3(L)$ be the set of equivalence classes of pairs $(V, D)$, where $V$ is a principal homogeneous space for $A$ and $D \in \mathbf{Pic}(V)(k)$ is a divisor class whose image in $NS(V) = NS(A)$ is equal to $[L]$. Two such pairs $(V_1, D_1)$, $(V_2, D_2)$ are regarded as isomorphic if and only if there exists an isomorphism of principal homogeneous spaces $f : V_1 \to V_2$ such that $f^*(D_2) = D_1$.

**Proposition 28.** *There is a natural bijection from the set $\mathcal{T}_3(L)$ to $H^1(k, \kappa(L))$.*

*Proof:* Again we need only appeal to Galois descent: an automorphism of the pair $(A, L)$ is given by translation $\tau_P$ by an element $P \in A(\overline{k})$ such that $\tau_P^*(L) = L$, i.e., by $P \in \kappa(L)$. Thus $H^1(k, \kappa(L))$ parameterizes the twisted forms of $(A, L)$, i.e., the elements of $\mathcal{T}_3(L)$.

We can thus define a map $\Delta_3 : H^1(k, A[n]) \to \mathrm{Br}(k)$, by $\Delta_3((V, D)) = \delta(D)$.

Remark: In all three cases, the map $\Delta_i$ visibly depends only on the Néron-Severi class of $L$.

5.4. **Compatibility.**

**Proposition 29.** *For any ample, basepoint free line bundle $L$ on $A_{/k}$, we have*

$$\Delta_1 = \Delta_2 = \Delta_3.$$

*Proof:* By the commutativity of (6), the map $\Delta_1$ factors as

$$H^1(k, \kappa(L)) \stackrel{H^1(\gamma)}{\longrightarrow} H^1(k, PGL_N) \stackrel{\partial}{\to} H^2(k, \mathbb{G}_m) = \mathrm{Br}(k),$$

where $\partial$ is the cohomological connecting map associated to the central extension

$$1 \to \mathbb{G}_m \to GL_N \to PGL_N.$$

Thus it suffices to show the same for $\Delta_2$ and $\Delta_3$.

Under the bijections $\mathcal{T}_2(L) = H^1(k, \kappa(L))$ and

$$H^1(k, PGL_N) = (N-1) - \text{dimensional Severi-Brauer varieties},$$

the map $(V \to X) \mapsto X$ corresponds to $H^1(\gamma) : H^1(k, \kappa(L)) \to H^1(k, PGL_N)$. Moreover, the assignment $X \mapsto [X]$ (which we did not explicitly define above) is given by the connecting map $\partial : H^1(k, PGL_N) \to \mathrm{Br}(k)$. Thus $\Delta_1 = \Delta_2$.

Similarly, recall that $\Delta_3$ is defined by $(V, D) \mapsto \delta(D)$. In [Cl1, §3] it is shown that for an effective divisor $D$, the obstruction map $D \mapsto \delta(D)$ can be given by constructing a Severi-Brauer variety $V[D]$ and then taking its class $\partial(V[D]) \in H^2(k, \mathbb{G}_m)$.

(In the notation of §5.3, $(\sigma,\tau) \mapsto f_\sigma \sigma(f_\tau) f_{\sigma\tau}^{-1}$ gives an explicit cocycle representative.) In other words, $\Delta_3$ is also given as the composition of the canonical maps $H^1(k,\kappa(L)) \to H^1(k,PGL_N) \to H^2(k,\mathbb{G}_m)$, so $\Delta_1 = \Delta_3$.

Remark: For any (nonsingular, projective, geometrically irreducible) algebraic variety $V$, there is a correspondence between ample, basepointfree rational divisor classes $D \in \mathbf{Pic}(V)(k)$ and morphisms from $V$ to the Severi-Brauer variety $V[D]$ (which, when $V(k) \neq \emptyset$, becomes the usual correspondence between ample basepointfree line bundles and morphisms into projective space). This gives directly a bijection between $\mathcal{T}_2(L)$ and $\mathcal{T}_3(L)$ and hence another way to see $\Delta_2 = \Delta_3$.

In the sequel, $L$ will always denote $nP$, for $P$ a principal line bundle, so that $\kappa(L) = A[n]$. When we refer to the period-index obstruction map $\Delta_L : H^1(k,A[n]) \to \mathrm{Br}(k)$, we will freely use any of the three above forms.

5.5. **Applications to the period-index problem.** Throughout this section we fix $(A,P)_{/k}$ a strongly principally polarized abelian variety, a positive integer $n$, and write $L = nP$, $\Delta = \Delta_L$.

**Theorem 30.** *Let $V_{/k}$ be a principal homogeneous space for $A_{/k}$ of (Albanese) period $n$. Suppose there exists some lift of $V$ to $\xi \in H^1(k,A[n])$ such that $\Delta_L(\xi) = 0$. Then $V$ can be split over a field extension of degree at most $(g!) \cdot n^g$.*

*Proof*: Put $N = n^g$. Consider first the map $\varphi_L : A \to \mathbb{P}^{N-1}$ attached to the line bundle $L = nP$ on $A$. We recall:

(i) If $n \geq 3$, $\varphi_L$ is an embedding.
(ii) If $n = 2$, $\varphi_L$ is a morphism which is two-to-one onto its image.
(iii) The degree of $\varphi_L$ is $(g!) \cdot n^g$.

Specifically, assertion (iii) means: if $H \subset \mathbb{P}^{N-1}$ is a linear subvariety of codimension $g$, then $\varphi_L^*(\varphi_L(A) \cap H)$ is a $k$-rational zero-cycle of degree $(g!) \cdot n^g$ on $A$.

Now using our second interpretation of the period-index obstruction, an element $\xi \in H^1(k,A[n])$ with $\Delta(\xi) = 0$ corresponds to a diagram $\varphi : V \to \mathbb{P}^N$, i.e., a twisted form of $\varphi_L$ whose target is a projective space. So taking again $H$ to be any codimension $g$ linear subvariety $H$ of $\mathbb{P}^N$, $\varphi^*(\varphi(V) \cap H)$ gives a zero-cycle of degree $(g!) \cdot n^g$ on $V$, proving the theorem.

By assuming in addition the $\mathfrak{g}_k$-module triviality of $NS(A)$ (which is automatic in the one-dimensional case), we can get a sort of converse result.

**Theorem 31.** *Let $V \in H^1(k,A)[n]$ a principal homogeneous space.* Suppose *that the $\mathfrak{g}_k$-module action on $NS(A) = NS(V)$ is trivial. If $\Delta(\xi) \neq 0$ for every lift $\xi$ of $V$, then $V$ cannot be split over a degree $n$ field extension. If $n = p^a$ is a prime power, we have moreover that the index of $V$ exceeds $n$.*

*Proof*: We will prove the second statement first, so assume that $n = p^a$. Seeking a contradiction, we assume that the index of $\eta$ is $p^a$, so that there exists some splitting field $l_1/k$ of $\eta$ such that $[l_1 : k] = m_1 p^a$ with $m_1$ prime to $p$. On the other hand, since by Proposition 9 the index of $\eta$ is a power of $p$, for every prime $r$ dividing $m$ there exists a splitting extension $l_l/k$ such that $[l_l : k] = m_r$ for some $m_r$ prime

to $r$. Since $V_{/l_1} \cong A_{/l_1}$, we may view the strong principal polarization $P$ as an $l_1$-rational divisor on $V$. Let $D_1$ be the class of $Tr_k^{l_1} P$ in $\mathrm{Pic}(V)$. By the assumed $\mathfrak{g}_k$-module triviality of $NS(V)$, we must have $[D_1] = [m_1 p^a P]$. Repeating the previous sentence with $l_r$ in place of $l_1$, we get a $D_2 \in \mathrm{Pic}(V)$ such that $[D_r] = [m_r P]$. By varying over all $r$ dividing $m_1$, it follows that there exists $D \in \mathrm{Pic}(V)$ such that $[D] = [p^a P]$, contradicting the nonvanishing of the period-index obstructions of $\eta$.

A similar (but simpler) argument shows the first statement: if $l/k$ is a degree $n$ field extension splitting $\eta$, then $Tr_{l/k} P$ exhibits a rational divisor in the Néron-Severi class of $nP$.

5.6. **The proof of Theorem 3.** Maintain the notation of the previous section. If $V \in H^1(k, A)[n]$, then in order to show that $V$ can be split over a field extension of degree at most $(g!) \cdot n^g$ it is enough, by the preceding theorem, to show that there exists some lift $\xi$ of $V$ with vanishing period-index obstruction. Of course every lift has this property if $Br(k) = 0$, so we look at the case where $k$ is a number field and $V$ has rational points everywhere locally. The proof is the same as in [O'N]: namely, at every completion $k_v$ of $k$, $V(k_v) \neq \emptyset$ implies that the obstruction map $\Delta : \mathbf{Pic}(V)(k_v) \to Br(k)$ vanishes identically. (Alternately, the image under $\phi$ of a $k_v$-rational point of $V$ gives a $k_v$-rational point on the Severi-Brauer variety $X$, making $X_V \cong \mathbb{P}^N_v$.) But the Hasse principle holds in the Brauer group of a number field, so again *any* lift of $V$ to $\xi \in H^1(k, A[n])$ has $\Delta_v(\xi) = 0$ for all $v$, hence $\Delta(\xi) = 0$.

Remark: The proof of Theorem 3 still works when $k$ is a number field and $V$ is locally trivial at all but at most one place of $k$, for then $\Delta(\xi)$ is an element of the Brauer group of $k$ which has at most one nontrivial localization and is therefore trivial by the global reciprocity law. Whereas $Ш(k, A)[n]$ is finite, the subset $\mathcal{K}(k, A)[n]$ of $H^1(k, A)[n]$ of elements locally trivial at all but at most one place may well be infinite. After the present paper was submitted for publication, the fact that period equals index for elements of $\mathcal{K}(k, E)$ was used by the author to show the existence of genus one curves of every index over every number field [Cl2].

5.7. **A result of Tate-Lichtenbaum-van Hamel.** Given an abelian variety $A$ defined over a field $k$, Tate defined a bilinear pairing

$$T : H^1(k, A^\vee) \times A(k) \to \mathrm{Br}(k),$$

and proved the following theorem, whose importance for the present work cannot be overstated:

**Theorem 32.** *(Tate,* [Ta]*) If $k$ is a $p$-adic field – so $\mathrm{Br}(k) = \mathbb{Q}/\mathbb{Z}$ – then $T$ puts the torsion abelian group $H^1(k, A^\vee)$ and the profinite abelian group $A(k)$ in Pontrjagin duality. It follows that for all positive integers $n$, $T$ induces a duality between the finite abelian groups $A(k)/nA(k)$ and $H^1(k, A^\vee)[n]$.*

Tate's pairing was crucially used by Lichtenbaum in his proof that period equals index for elliptic curves over $p$-adic fields. As O'Neil has observed [O'N, §5], Lichtenbaum's proof can be viewed as giving a redefinition of Tate's duality pairing in terms of the period-index obstruction map $\Delta$. The key result is the following:

**Proposition 33.** *(Lichtenbaum) Let $C_{/k}$ be a genus one curve defined over a p-adic field, with period $n$. Then $\mathrm{Br}^0(C/k) = \mathrm{Br}(k)[n] \cong \mathbb{Z}/n\mathbb{Z}$.*

As it turns out, we will not need to make explicit the connection between Tate's duality pairing and the period-index obstruction map in the higher-dimensional case, because the desired higher-dimensional analogue of Proposition 33 has recently been proved by J. van Hamel:

**Proposition 34.** *(*[vH, Prop. 4.4]*) Let $V$ be a smooth, proper, geometrically irreducible variety over a p-adic field $k$. Then $\mathrm{Br}^0(V/k) = \mathrm{Br}(k)[n] \cong \mathbb{Z}/n\mathbb{Z}$, where $n$ is the Albanese period of $V$.*

Let $V$ be a period $n$ principal homogeneous space of a principally polarized abelian variety $(A, L)$ over a $p$-adic field. *Suppose* that the following holds:

$$\Delta_L(H^1(k, A[n])) \subset \mathrm{Br}(k)[n]. \tag{7}$$

Let $\xi = (V, D) \in H^1(k, A[n])$ be any lift of $V$. Then $\Delta_L(\xi) \in \mathrm{Br}(k)[n] = \mathrm{Br}^0(V/k)$, so that there exists a rational divisor class $D_0 \in \mathbf{Pic}^0(V)(k)$ whose obstruction $\delta(D_0)$ to being given by a rational divisor is equal to $\delta(D)$. Taking $D' = D - D_0$, we get a lift $(V, D')$ of $V$ with trivial obstruction, so by Theorem 30, we conclude that $V$ is split over a field extension of degree at most $(g!)n^g$. This is the desired conclusion in Theorem 2.

Thus we are reduced to establishing the containment (7), which is rather easy to prove in dimension one, but in general will occupy us for much of the remainder of the paper. Here is the situation:

As we saw in §5.4, the obstruction map $\Delta_L$ factors through $H^1(k, PGL_{n^g})$, so that the image of $\Delta_L$ consists of the Brauer classes $[X]$ of certain $n^g - 1$-dimensional Severi-Brauer varieties $X$. Such a variety $X$ corresponds to a central simple algebra $F$ of dimension $n^{2g}$ over $k$. If we write $F \cong M_k(D)$ where $D$ is a division algebra, then the index of $[X] \in \mathrm{Br}(k)$ is $\sqrt{[D:k]}$, hence divides $n^g$. In other words, the image of the period-index obstruction map consists of Galois cohomology classes in $\mathrm{Br}(k) = H^2(k, \mathbb{G}_m)$ with index dividing $n^g$. By Proposition 11a), their periods also divide $n^g$, so we get

$$\Delta_L(H^1(k, A[n]) \subset \mathrm{Br}(k)[n^g].$$

When $g = 1$, this is what we wanted to show, and we have recovered Lichtenbaum's theorem (and essentially Lichtenbaum's proof).

But clearly this argument is not sufficient when $g > 1$. We will see later that the bound of $n^g$ it establishes on the *indices* of elements of $\Delta(H^1(k, A[n]))$ *can* be attained for suitably complicated fields $k$. Thus it seems less clear that (7) should continue to hold when $g > 1$. Indeed, we are at present only able to show that (7) holds under certain additional hypotheses, namely when $A[n]$ admits a Lagrangian decomposition (Proposition 40) or when $n$ is odd (Corollary 44). These are exactly the additional hypotheses of Theorem 2, so as soon as these two cases of (7) are established, the proof of Theorem 2 will be complete.

5.8. **A pseudoindex computation.** As we have seen, for $V_{/k}$ a variety over a field $k$, the abelian groups $\mathrm{Br}(V/k)$ and $\mathrm{Br}^0(V/k)$ are important invariants, and it

is a very interesting problem to compute them for a given variety, or to determine all possible groups that occur for varieties in a given class. In general, one has

$$\mathrm{Br}^0(V/k) \subset \mathrm{Br}(V/k) \subset \mathrm{Br}(k)[i(V)].$$

When $k$ is $p$-adic, these are of course finite cyclic groups, determined by their order, and by Proposition 34, $\#\,\mathrm{Br}^0(V/k)$ is the period of $V$ (i.e., of $\mathrm{Alb}^1(V)$). Evidently then $\#\,\mathrm{Br}(V/k)$ lies somewhere between the period and the index of $V$.

The precise answer is known when $V$ is a curve:

**Theorem 35.** *(Roquette-Lichtenbaum) For a curve $C$ over a $p$-adic field, the order of $\mathrm{Br}(C/k)$ is equal to the index of $C$.*

See [Li2] for a proof and for further relations between the period and index of a genus $g$ curve over a $p$-adic field: in particular, the $p(C)$ divides $g-1$, $i(C)$ is either $p(C)$ or $2p(C)$, and the latter can occur only when $\frac{g-1}{p(C)}$ is odd.

Of course the period and index of an algebraic curve need not coincide: a curve of genus zero without rational points has period 1 and index 2. In [PoSt] Poonen and Stoll ultimately trace the phenomenon of nonsquare order Shafarevich-Tate groups of Jacobians of curves of genus $g$ over a number field to the *oddness* of the number of places $v$ of $k$ for which $i(C_{k_v})$ does not divide $g-1$ (so in particular is not equal to $p(C_{k_v})$). Many examples of nonsquare Ш have since been produced, so the phenomenon of $i(C) = 2p(C)$ over $p$-adic fields is quite common.

The work of van Hamel constructs a new homology theory for varieties over a $p$-adic field $k$ ("pseudo-motivic homology") in which there is a natural degree map ${}^1H(V,\mathbb{Z}) \to \mathbb{Z}$ whose cokernel is called the **pseudoindex** $\psi(V)$. This is compared to the period (the cokernel of the map $\mathbf{Alb}(V) \to \mathbb{Z}$) and the index (the cokernel of the map $\mathbf{CH}_0(X) \to \mathbb{Z}$) and fits naturally between them: $p(V) \mid \psi(V) \mid i(V)$. He then proves the following theorem:

**Theorem 36.** *(*[vH, Theorem 2]*) For a variety $V$ over a $p$-adic field, the finite abelian groups $\mathrm{Br}(V/k)$ and $\mathbb{Z}/\psi(V)\mathbb{Z}$ are isomorphic.*

This is a very appealing result, but it does not in itself seem to address the question of exactly where $\#\,\mathrm{Br}(V/k)$ lies in between $p(V)$ and $i(V)$. The results of this paper allow us to answer this question for principal homogeneous spaces, at least under certain addditional hypotheses:

**Theorem 37.** *Let $A$ be an abelian variety over a $p$-adic field $k$ whose Néron-Severi group is generated by a principal polarization $P$. Let $V \in H^1(k,A)$ be a principal homogeneous space of period $n$. Assume that* either *$n$ is odd or $A[n]$ is Lagrangian. Then*

$$p_{\mathrm{Alb}}(V) = n = i_{\mathrm{Pic}}(V) = \#\,\mathrm{Br}(V/k).$$

Proof: Let $D \in \mathbf{Pic}(V)(k)$ be a rational divisor class. Put $L = nP$ as usual. From Corollary 22, $p_{\mathrm{Pic}}(V) = n$, so that the class $[L] \in NS(A)(k) = NS(V)(k)$ is represented by some $k$-rational divisor class on $V$, which we will denote by $D_n$. That corollary also tells us that $[D] = [kD_n]$ for some positive integer $k$, i.e., $D_0 = D - kD_n \in \mathbf{Pic}^0(V)$. Since, under the given hypotheses, $\delta_L(H^1(k,A[n])) \subset \mathrm{Br}(k)[n]$, in particular $\delta(D_n) \in \mathrm{Br}(k)[n]$, so

$$\delta(D) = \delta(D_0) + k\delta(L) \in \mathrm{Br}(k)[n].$$

In the previous section we showed that there is a rational divisor on $V$ in the Néron-Severi class of $[L]$, so that $i_{\mathrm{Pic}}(V) = n$.

Remark: It seems likely that a more careful analysis would allow us to remove the hypothesis of cyclic Néron-Severi group (and perhaps also the requirement that $A$ be principally polarized).

Remark: Certainly the pseudoindex $\psi(V) = \#\,\mathrm{Br}(V/k)$ can be smaller than the index of $V$ (Theorem 17a)). On the other hand, it seems that $\psi(V) = i_{\mathrm{Pic}}(V)$ in all known cases.

## 6. Twisted Heisenberg groups

### 6.1. **Introduction.**

From this point on, all our results turn on an understanding of the map $\Delta : H^1(k, A[n]) \to \mathrm{Br}(k)$ associated to the $n$th power of a principal line bundle $P$ on $A$. Our first aim is to give an "explicit" description of $\Delta$, whatever that may mean. In practice, we will be content with a description which enables us, when $k$ is a number field, to construct examples of principal homogeneous spaces with unequal period and index, as in Theorem 8. Moreover, we have reduced our study of the period-index problem over $p$-adic fields to the statement that $\Delta(H^1(k, A[n])) \subset \mathrm{Br}(k)[n]$, so our second aim in this section is to find necessary and sufficient conditions for this containment to hold.

Clearly, in order to understand the cohomological connecting map $\Delta$ associated to the exact sequence

$$1 \to \mathbb{G}_m \to \mathcal{G}_L \to A[n] \to 0,$$

we should seek to understand the structure of $\mathcal{G}_L$ as an algebraic $k$-group. These groups were introduced by Mumford in the case when $k = \overline{k}$, and in this case the structure is completely understood: in particular, over $\overline{k}$, for fixed $n$ all theta groups are isomorphic to a common algebraic group, the **Heisenberg group**. Moreover, this Heisenberg group has a natural model $\mathcal{H}_{/k}$; if we suppose that $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, it is a central extension of the constant group scheme $(\mathbb{Z}/n\mathbb{Z})^{2g}$ by $\mathbb{G}_m$. In this case, there is a very clean description of the cohomological connecting map; after making appropriate identifications, it is a sum of $g$ norm-residue symbols.[9]

Thus the computation of $\Delta$ can be viewed as a problem in Galois descent: namely, Mumford's theorem says that our theta group is a $\mathfrak{g}_k$-twisted form of a Heisenberg group. This suggests that it would be profitable to consider the larger class of group schemes which are *twisted Heisenberg groups*. Now there are two possible approaches to take: (i) try to solve the above problems for any twisted Heisenberg group; or (ii) try to characterize theta groups among all twists of Heisenberg groups.

As it turns out, what we are able to prove concerning computation of $\Delta$ and of the containment relation (7) holds either in the context of arbitrary twists of Heisenberg groups, or for arbitrary twists preserving the $\mathfrak{g}_k$-module structure on $A[n]$; so we

[9]This nice description was explained to me by R. Sharifi, and appears in his 1999 Chicago thesis [Sh].

mostly follow (i) here. The problem of characterizing theta groups is nevertheless a very interesting one: in particular, it is *not* the case that every twisted Heisenberg group is a theta group of a line bundle, as we shall see later on. It seems conceivable that the relation (7) could hold for all theta groups but not for all twisted Heisenberg groups. In summary, the structure theory of twisted Heisenberg groups deserves a fuller treatment than we are willing (and indeed, able) to give here.

6.2. **Twisted Heisenberg groups.**

A **twisted Heisenberg group** over a field $k$ is an algebraic $k$-group scheme $\mathcal{G}$ fitting into a short exact sequence

$$1 \to \mathbb{G}_m \to \mathcal{G} \to K \to 0,$$

and satisfying the following additional properties:

(THG1) The center of $\mathcal{G}$ is $\mathbb{G}_m$.
(THG2) $K$ is finite étale with underlying abelian group of the form $A \oplus A$.
(THG3) The characteristic of $k$ does not divide the order of $K$.

Let $\delta = (d_1, \ldots, d_g)$ denote the sequence of elementary divisors of the finite abelian group $A$; we say $\mathcal{G}$ is **of type** $\delta$. Let $d = \operatorname{lcm}(d_i)$ denote the exponent of $K$. If $d_1 = \ldots = d_g = n$, we will write $\underline{n}$ for $(n, n, \ldots, n)$. We shall sometimes speak of $\#A$ as the **order** of $\mathcal{G}$.

We define, for any twisted Heisenberg group $\mathcal{G}$, the commutator pairing $e : K \times K \to \mathbb{G}_m$, as follows: for any $(P, P') \in K \times K$, lift to any elements $\tilde{P}, \tilde{P'}$ in $\mathcal{G}$. Then $e(P, P')$ is defined to be the commutator $[\tilde{P}, \tilde{P'}]$. Note that since $\tilde{P}$ and $\tilde{P'}$ are unique up to central elements, $e(P, P')$ is well-defined; moreover, since $K$ is commutative, $e(P, P') \in \mathbb{G}_m$. It is not hard to check that the condition that $\mathbb{G}_m$ be the precise center of $\mathcal{G}$ is equivalent to the *nondegeneracy* of $e$. So $e$ is a symplectic form, taking values in $\mu_d \subset \mathbb{G}_m$, and placing $K$ into Cartier duality with itself.

Example 1: let $H/k$ be a finite étale group scheme of order indivisible by the characteristic of $k$; put $K(H) = H \oplus H^*$ (remember that $H^* = \operatorname{Hom}(H, \mathbb{G}_m)$ denotes the Cartier dual of $H$). We define a group scheme $\mathcal{H}(H)$, the **Heisenberg group associated to H**, as follows: as a $\mathfrak{g}_k$-set, $\mathcal{H} = \mathbb{G}_m \times H \times H^*$, with the group law given by

$$(\alpha, x, \ell) \star (\alpha', x', \ell') = (\alpha\alpha'\ell'(x), x + x', \ell + \ell').$$

In this case the commutator pairing is $e((x, \ell), (x', \ell')) = x'(\ell)x(\ell')^{-1} \in \mu_d$ (here $d$ is the exponent of $H$). We define the **standard Heisenberg group** $\mathcal{H}(\delta)$ of type $\delta = (d_1, \ldots, d_g)$ by taking $H$ to be the constant group scheme $\bigoplus_{i=1}^g \mathbb{Z}/d_i\mathbb{Z}$.

**Theorem 38.** *(Mumford) Suppose that $k = \overline{k}$ is algebraically closed. Then every twisted Heisenberg group of type $\delta$ is isomorphic to $\mathcal{H}(\delta)$.*

*Proof:* See [Mu, Cor. to Thm. 1].

Thus, as advertised, the twisted Heisenberg groups of type $\delta$ over a field $k$ are the $\overline{k}/k$-twisted forms of the standard Heisenberg group $\mathcal{H}(\delta)$.

Example 2: For $L$ an ample line bundle on an abelian variety $A$, the theta group $\mathcal{G}_L$ is a twisted Heisenberg group. If $L = nP$ for a principal line bundle $P$, then $\mathcal{G}_L$ has type $\underline{n}$.

Remark: In general, $\mathcal{G}_{nP}$ is *not* isomorphic to any Heisenberg group $\mathcal{H}(H)$ over the ground field. Indeed, such an isomorphism would induce, upon modding out by the respective centers, an isomorphism $A[n] \cong H \oplus H^*$, whereas in general $A[n]$ is irreducible as a $\mathfrak{g}_k$-module. The more interesting question of whether the existence of such a decomposition on $A[n]$ implies that $\mathcal{G}_{nP} \cong \mathcal{H}(H)$ will be addressed (but not completely answered) in §6.9.

6.3. **The automorphism group.** Let $\Theta_\delta(k)$ be the set of all abstract theta groups $\mathcal{G}$ of type $\delta$. By Mumford's theorem, every element of $\Theta_\delta(k)$ is a $\overline{k}/k$-twisted form of $\mathcal{H}(\delta)$, so $\Theta_\delta(k)$ should be identified as a Galois cohomology set $H^1(k, G_1)$, where $G_1$ is a suitable automorphism group. The goal of this section is to identify $G_1$ as a subgroup of the full automorphism group of $\mathcal{H}(\delta)$ and to determine its structure.

First we look carefully at the relevant descent problem: when we say that $\mathcal{G}/\overline{k} \cong \mathcal{H}(\delta)/\overline{k}$, we mean by an isomorphism $\iota$ which restricts to the identity map on $\mathbb{G}_m$. Thus, if $G_1 \subset \mathrm{Aut}(\mathcal{H})$ is group of automorphisms of the Heisenberg group acting trivially on the center, we get a map of pointed sets $\Theta_\delta(k) \to H^1(k, G_1)$. On the other hand, any centrally trivial isomorphism $\iota : \mathcal{G} \to \mathcal{H}$ induces an isomorphism $\overline{\iota} : K(\mathcal{G}) \to K(\mathcal{H})$. Now $K(\mathcal{G})$ and $K(\mathcal{H})$ are both equipped with symplectic forms $e$. Since both symplectic forms are defined in terms of the respective commutator pairings, a diagram chase reveals that $\overline{\iota}$ necessarily respects the symplectic structure. It follows that every twisted form $\mathcal{T} \in H^1(k, G_1)$ is an abstract theta group, so that $\Theta_\delta(k) = H^1(k, G_1)$. Moreover, the map $H^1(k, G_1) \to H^1(k, Sp(K))$ corresponds to $\mathcal{G} \to K(\mathcal{G}) = \mathcal{G}/\mathbb{G}_m$.

From now on we restrict our attention to type $\delta = \underline{n}$, the case of interest to us in the sequel. (The general case would only be notationally more cumbersome.)

The next result gives a complete description of the group $G_1$.

**Proposition 39.** *Suppose that* $\mathrm{char}(k) \neq 2$. *Then there is a split exact sequence*

$$1 \to K^* \to G_1 \to Sp(K) \to 0.$$

*Proof:* The map $G_1 \to Sp(K)$ is the one occurring in the definition of $G_1$; let $G_2$ be its kernel, the group of automorphisms of $\mathcal{H}$ acting trivially on both $\mathbb{G}_m$ and the quotient $K$.

Step 1: We claim that $G_2$ is canonically isomorphic to the character group of $K$. Indeed, suppose that $\chi \in \mathrm{Hom}(K, \mathbb{G}_m)$ is any character of $K$. Then $\chi : (\alpha, x, \ell) \mapsto (\chi(x, \ell)\alpha, x, \ell)$ gives an automorphism of $\mathcal{H}(\underline{n})$ acting trivially on the center. For the converse, since the Heisenberg group is generated together by $\mathbb{G}_m$ together with any $\mathbb{Z}/n\mathbb{Z}$-basis $\{x_1, \ldots x_g\} \cup \{\ell_1, \ldots, \ell_g\}$ for $H \oplus H'$, given an arbitrary $\psi \in G_2$, there is a unique character $\chi$ such that the action of $\chi^{-1} \circ \psi$ acts trivially on all elements of the form $(\alpha, x_i, 0)$ and $(\alpha, 0, \ell_j)$ hence is the identity map on all of $\mathcal{H}$.

Step 2: We will construct a section $Sp(K) \to G_1$, which clearly suffices to prove the result. The idea is as follows: the group law defining the Heisenberg group uses the bilinear form $f((x,\ell),(x',\ell')) = \ell'(x)$, which is not such a nice form: it is degenerate and neither symmetric nor alternating. Moreover, we have in sight a symplectic form $e : K \times K \to \mathbb{G}_m$. So we wish we were dealing with the group $\mathcal{H}'$ constructed using $e$ instead of $f$, i.e.,

$$(\alpha, x, \ell) \star (\alpha', x', \ell') := (\alpha\alpha' e(\ell, \ell'), x + x', \ell + \ell'),$$

as in this case there is an evident faithful action of $Sp(K)$ by automorphisms of $\mathcal{H}'$:

$$g \mapsto ((\alpha, (x \oplus \ell)) \mapsto (\alpha, g(x \oplus \ell))).$$

But – thanks to our assumption that $\mathrm{char}(k) \neq 2$ – it turns out that $\mathcal{H} \cong \mathcal{H}'$. Indeed, let $W_1 = \{(1, x, 0)\}$ $W_2 = \{(1, 0, \ell)\}$ be the standard level subgroups of $\mathcal{H}$, so that every element of $\mathcal{H}$ has a unique expression of the form $w_1 w_2 \alpha$, with $\alpha \in \mathbb{G}_m$. Following [Yu, §10], we define a map $\Phi : \mathcal{H} \to \mathcal{H}'$,

$$w_1 w_2 \alpha \mapsto \left(\alpha + \frac{1}{2} e(\overline{w_1}, \overline{w_2}), \overline{w_1}, \overline{w_2}\right),$$

which gives an isomorphism of groups preserving the $\mathfrak{g}_k$-module structures and acting trivially on the center and on the quotient $K$. Thus $\Phi$ induces an isomorphism $G_1/G_2 \xrightarrow{\sim} \mathrm{Sp}(K)$.

6.4. **The Lagrangian case.** We will now give an explicit computation of $\Delta$ when $K(\mathcal{G})$ has a **Lagrangian Galois-module structure**. Namely, in this section we work with an abstract theta group $\mathcal{G}$ which "could be" a Heisenberg group in the sense that $\mathcal{G}/\mathbb{G}_m = K$ admits a $\mathfrak{g}_k$-module decomposition $K = H \oplus H^*$ with $H$ and $H^*$ isotropic subspaces for the symplectic form $e$.

Remark: In case $\mathcal{G} = \mathcal{G}_{p[O]}$ is the theta group associated to a degree $p$ line bundle on an elliptic curve, this is equivalent to assuming that the mod $p$ Galois representation is of **split Cartan** type. When $k$ is a number field, such a Galois-module structure occurs for half of all primes $p$ when $E$ has $k$-rational complex multiplication; otherwise, by Serre's theorem, it can occur for at most finitely many $p$. (Indeed, even for $E/K$ a Tate curve over a $p$-adic field, $E[n]$ can be Lagrangian for only finitely many $n$: see [Si, Prop. V.6.1].) For higher-dimensional abelian varieties, the assumption of a Lagrangian structure on $A[n]$ is not quite so restrictive, but certainly one expects that for "most" abelian varieties over number fields and "most" positive integers $n$, $A[n]$ will be an irreducible $\mathfrak{g}_k$-module.

What is gained by restricting to the Lagrangian case is that $\mathcal{G}$ is a twisted form of the corresponding Heisenberg group $\mathcal{H}(H)$ by an element of the smaller group $H^1(k, G_2) = H^1(k, (H \oplus H^*)^*)$. Let $\chi \in Z^1(k, G_2)$ be a one-cocycle with values in the character group of $K(H)$. We view $\mathcal{G}$ as a "doubly twisted" form of $\mathbb{G}_m \times K(H)$: twisted as a group according to the cocycle $f$ as above, and with twisted Galois-module structure using $\chi$.

We employ a more compact notation: write $P = (x, \ell) \in K(H)$, so that an arbitrary element of $\mathcal{G}$ is written now as $(\alpha, P)$ and the group law is written as $(\alpha, P) \star (\alpha', P') = (\alpha\alpha' f(P, P'), P + P')$, where $f(P, P') = \ell'(P)$ as before. Note that $(\alpha, P)^{-1} = (\alpha^{-1} f(P, -P)^{-1}, -P)$.

Now we can compute the coboundary map $\Delta_{\mathcal{G}} : H^1(k, K(H)) \to H^2(k, \mathbb{G}_m)$ directly: let $\eta \in Z^1(k, K(H))$. Then

$$\Delta(\eta)(\sigma, \tau) = N_\sigma \sigma(N_\tau) N_{\sigma\tau}^{-1},$$

where $N_\sigma,\ N_\tau, N_{\sigma\tau}$ are any lifts of $\eta(\sigma), \eta(\tau)$ and $\eta(\sigma\tau)$ to $\mathcal{G}$. We choose the simplest possible lifts, namely $N_\sigma = (1, \eta(\sigma))$ and so on. So we get:

$$\Delta(\eta)(\sigma, \tau) = (1, \eta(\sigma)) \star \sigma(1, \eta(\tau)) \star (1, \eta(\sigma\tau))^{-1} =$$

$$(1, \eta(\sigma)) \star (\chi(\sigma)(\sigma(\eta(\tau))), \sigma(\eta(\tau))) \star (f(\eta(\sigma\tau), -\eta(\sigma\tau))^{-1}, -\eta(\sigma\tau)) =$$

$$(\chi(\sigma)(\sigma(\eta(\tau)))f(\eta(\sigma), \sigma(\eta(\tau))), \eta(\sigma)\sigma(\eta(\tau)) \star (f(\eta(\sigma\tau), -\eta(\sigma\tau))^{-1}, -\eta(\sigma\tau)) =$$

$$(\chi(\sigma)(\sigma(\eta(\tau)))f(\eta(\sigma), \sigma(\eta(\tau))), 0). \tag{8}$$

We immediately read off the following consequence:

**Corollary 40.** *Let $\mathcal{G}$ be a Lagrangian twisted Heisenberg group of type $\underline{n}$. Then*

$$\Delta_{\mathcal{G}}(H^1(k, K)) \subset Br(k)[n].$$

6.5. **The case of full level $n$ structure.** We now specialize further: we assume that $H \cong H^* \cong (\mathbb{Z}/n\mathbb{Z})^g$ are *both* constant: notice that this assumption implies that $k$ contains the $n$th roots of unity. So Kummer theory applies and we get

$$H^1(k, K) \overset{\beta}{\cong} H^1(k, \mu_n)^{2g} \cong (k^*/k^{*n})^{2g}.$$

The "$\beta$" denotes a choice of isomorphism, which is equivalent to a choice of a $\mathbb{Z}/n\mathbb{Z}$-basis for $K(\overline{k})$. In fact we want a careful choice of basis: first fix $\zeta_n$ a primitive $n$th root of unity in $k$. We choose a basis $x_1, \ldots, x_d, y_1, \ldots, y_g$ which is "$\zeta_n$-symplectic" with respect to $e$: for all $i$ and $j$, $e_n(x_i, x_j) = 0$, $e_n(x_i, y_j) = \delta_{ij}\zeta_n$. Then $\Delta = \Delta_{\mathcal{G}}$ may be viewed as a map

$$\Delta : (k^*/k^{*n})^{2g} \to Br(k).$$

Let $(a_1, \ldots, a_d, b_1, \ldots, b_d)$ be an element of $(k^*/k^{*n})^{2g}$. For $x, y \in k^*/k^{*n}$, let $\langle x, y\rangle_n \in Br(k)[n]$ denote the norm-residue symbol [Se2, Ch. XIV], and recall that the definition of the norm-residue symbol requires a choice of a primitive $n$th root of unity (we choose the same $\zeta_n$).

**Theorem 41.** *For $1 \leq i \leq g$, there exist $C_{1,i},\ C_{2,i} \in (k^*/k^{*n})$ such that*

$$\Delta(a_1, \ldots, a_d, b_1, \ldots, b_d) = \sum_{i=1}^{g} \langle C_{1,i}a_i, C_{2,i}b_i\rangle - \langle C_{1,i}, C_{2,i}\rangle =$$

$$\left(\sum_{i=1}^{g} \langle a_i, b_i\rangle_n\right) + \left(\sum_{i=1}^{g} \langle C_{1,i}, b_i\rangle_n + \langle a_i, C_{2,i}\rangle_n\right).$$

Given what has already been said, the proof of this theorem is straightforward: the linear part of equation (5) is a sum of $2g$ characters of $\mathfrak{g}_k$, so with Kummer-theoretic identifications is given by elements $C_{1,i},\ C_{2,i} \in k^*/k^{*n}$. The quadratic part is a sum of $g$ cup-products of pairs of characters, so under the same identifications becomes the sum of $g$ norm-residue symbols. A detailed treatment of the $g = 1$ case can be found in [Cl1, §3], and the general case is handled in exactly the same way.

6.6. **Quadraticity of obstruction maps.** Let $X$ and $Y$ be abelian groups and let $f : X \to Y$ be a map (*not* necessarily a homomorphism) between them. We shall say $f$ is **quadratic** if $B : X \times X \to Y$, $(x_1, x_2) \mapsto f(x_1 + x_2) - f(x_1) - f(x_2)$ is bilinear. Note that this implies $f(0) = 0$. We shall say $f$ is a **quadratic form** if it is quadratic and moreover satisfies $f(nx) = n^2 f(x)$ for $n \in \mathbb{Z},\ x \in X$.

When $X$ and $Y$ are uniquely 2-divisible, quadratic maps have a simple structure. Indeed, define $Q : X \to Y$, $Q(x) = \frac{1}{2}B(x, x)$ and $L = f - Q$. One checks easily that $L$ is linear, and is the zero map if $f$ is a quadratic form. It follows that $f(X[n]) \subset Y[n]$.

Unfortunately this is not a general property of quadratic maps. For example, the map $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ which takes $0 \pmod 2 \mapsto 0 \pmod 4$ and $1 \pmod 2 \mapsto 1 \pmod 4$ is quadratic.

If $X$ is an abelian group, let $X_q = I(X)/I(X)^2$, where $I(X)$ is the augmentation ideal of the group algebra $\mathbb{Z}[X]$. Then the map $q : X \to X_q$, $x \mapsto x - 1 \pmod{I(X)^2}$ is the *universal* quadratic map on $X$: any quadratic map $f : X \to Y$ factors as $l \circ q$ for a unique linear map $l : X_q \to Y$. One knows [Pa]

$$(X \oplus Y)_q \cong X_q \oplus Y_q \oplus (X \otimes Y).$$

$$(\mathbb{Z}/2^a\mathbb{Z})_q \cong \mathbb{Z}/2^{a+1}\mathbb{Z} \oplus \mathbb{Z}/2^{a-1}\mathbb{Z},\ a \in \mathbb{Z}^+.$$

$$(\mathbb{Z}/p^a\mathbb{Z})_q \cong (\mathbb{Z}/p^a\mathbb{Z})^2,\ p > 2.$$

Since the restriction of a quadratic map to a subgroup is quadratic, we conclude:

**Lemma 42.** *Let $f : X \to Y$ be a quadratic map on abelian groups.*
*a) For any $n \in \mathbb{Z}^+$, $f(X[n]) \subset Y[2n]$.*
*b) If $n \in \mathbb{Z}^+$ is* odd*, $f(X[n]) \subset Y[n]$.*

On the other hand we have the following result of Zarhin (see also [O'N, §4]):

**Proposition 43.** *(*[Za]*) Let $0 \to A \to B \to C \to 0$ be a central extension of non-abelian $\mathfrak{g}_k$-modules, with $C$ commutative. Then the associated obstruction map $\Delta : H^1(k, C) \to H^2(k, A)$ is quadratic.*

Combining these two results, we get:

**Corollary 44.** *Let $\mathcal{G}$ be a twisted Heisenberg group, and let $n$ the exponent of $K(\mathcal{G})$. Then:*
*a) $\Delta_{\mathcal{G}}(K) \subset \mathrm{Br}(k)[2n]$.*
*b) If $n$ is odd, $\Delta_{\mathcal{G}}(K) \subset \mathrm{Br}(k)[n]$.*

6.7. **Proof of Theorem 6.** Let $A_{/k}$ be a strongly principally polarized abelian variety over a $p$-adic field, and $n$ a positive integer. By Proposition 40 and Corollary 44 we know that $\Delta(H^1(k, A[n]))$ is contained in $\mathrm{Br}(k)[2n]$, and is contained in $\mathrm{Br}(k)[n]$ if $A[n]$ is Lagrangian or $n$ is odd.

Let $V \in H^1(k, A)[n]$ be any principal homogeneous space, and let $\xi$ be any lift of $V$ to $H^1(k, A[n])$. As above, $\Delta(\xi) \in Br(k)[2n]$. By our hypothesis on the relation between period and index in the Brauer group there exists a field extension

$l/k$ of degree dividing $(2n)^a$ such that $\Delta(\xi)|_l = 0$. Thus $V_{/l}$ has trivial period-index obstruction, so by Theorem 30, $V_{/l}$ can be split over a field extension of degree at most $(g!) \cdot n^g$. Thus $V$ itself can be split over a field extension of degree at most $(g!)2^a n^{g+a}$, giving part a) of Theorem 6. Similarly, under either of the additional assumptions of part b), the above argument gives a splitting field of degree at most $(g!)n^{g+a}$.

6.8. **Applications to the period-index problem in the Brauer group.** It is interesting to reconsider the construction of Lang and Tate (Proposition 14) in light of Theorem 6. Namely, let $k_g = \mathbb{C}((T_1)) \cdots ((T_{2g}))$, let $(A, P)_{/\mathbb{C}}$ be a strongly principally polarized abelian variety and view $A_{/k_g}$ by basechange. The proof of Proposition 14 goes by observing that for any finite extension $l/k_g$, in the Kummer sequence

$$0 \to A(l)/nA(l) \to H^1(l, A[n]) \to H^1(l, A)[n] \to 0$$

we have $A(l)/nA(l) = 0$; in other words, compatibly with restriction we have that $H^1(k_g, A)[n] \cong H^1(k_g, A[n]) \cong (k_g^*/k_g^{*n})^{2g}$. Thus, for any $1 \leq k \leq 2g$, the class $(T_1, \ldots, T_k, 1, \ldots, 1)$ corresponds to an element $V$ of period $n$ and index $n^k$. Let $V$ be a class of index $n^{2g}$, $\xi$ the (unique!) lift of $V$, and consider $\Delta(\xi)$. The period of $\Delta(\xi)$ divides $n$, whereas in §5.7 we saw that the index of $\Delta(\xi)$ divides $n^g$. At least if $n = p > g$, we *must* have that the index of $\Delta(\xi)$ is $n^g$, since otherwise Theorem 5 would tell us that $\mathrm{ord}_p(i(V)) < p^{2g}$. Thus we deduce period-index violations in the Brauer group of $k$. Moreover, because $(A, P)$ arises by basechange from an algebraically closed field, we have that $\mathcal{G}_{nP} \cong \mathcal{H}_g$, so that in this case the period-index obstruction map is a sum of norm residue symbols.

Put $k = \bigcup_{g \geq 1} k_g$. Since $k$ contains all roots of unity, it follows from a famous theorem of Merkurjev-Suslin [MS] that the union of the images of the period-index obstruction maps of all strongly principally polarized abelian varieties $A_{/k}$ is the entire Brauer group of $k$. Moreover it is indeed necessary to use abelian varieties of arbitarily large dimension in order to get the entire Brauer group of $k$.

**Question 45.** *Let $k$ be a number field, $(A, P)_{/k}$ be a strongly principally polarized abelian variety, and $n \geq 2$. Is the image of $\Delta_{nP}(H^1(k, A[n])) = \mathrm{Br}(k)[n]$?*

Remark: Since every division algebra over a number field is cyclic, the answer is yes when $\mathcal{G}_L$ is isomorphic to the standard Heisenberg group $\mathcal{H}(\underline{n})$, but note that a necessary condition for this is that $k$ contain the $n$th roots of unity. In any event, this motivates the question of the next section.

6.9. **When is $\mathcal{G}_L$ a Heisenberg group?** As we have seen, the obstruction to an $H$-Lagrangian twisted Heisenberg group being isomorphic to $\mathcal{H}(H)$ is the character $\chi \in H^1(k, K(\mathcal{G}))$. In particular, when $\mathcal{G} = \mathcal{H}(H)$, the obstruction map is

$$\Delta(\eta)(\sigma, \tau) = f(\eta(\sigma), \sigma(\eta(\tau)))$$

and is a quadratic *form* on $H^1(k, A)$, whereas in the presence of a nontrivial $\chi$ it may be merely a quadratic *map*.

Even if $A[n]$ is a trivial $\mathfrak{g}_k$-module, $\mathcal{G}_L$ need not be isomorphic to a Heisenberg group; if so, then the obstruction map would be given as a sum of $g$-norm residue symbols. As discussed in [Cl1, §3.2], this is in general not the case for $A = E$ and $n = 2$. However, O'Neil showed [O'N] the validity of the result for $g = 1$ and all odd $n$. The following theorem gives a higher-dimensional analogue:

**Theorem 46.** *(Polishchuk) Let $\mathcal{G} = \mathcal{G}_{nP}$ be the theta group of a strongly principally polarized abelian variety $A[n]$. Suppose:*
*a) $A \cong H \oplus H^*$.*
*b) $n$ is odd.*
*c) $P$ is a symmetric principal line bundle: $P \cong [-1]^* P$.*
*Then $\mathcal{G} \cong \mathcal{H}(H)$.*

*Proof:* Under the given hypotheses, a result of Polishchuk [Po, Cor. 1.3] says that $\mathcal{G} \cong \mathbb{G}_m \times K(\mathcal{G})$ as $\mathfrak{g}_k$-sets, or in other words that the character $\chi$ is trivial and $\mathcal{G} \cong \mathcal{H}(H)$.

Remark: The symmetry hypothesis is satisfied, for instance, whenever $A$ is the Jacobian of a curve $C$ with $C(k) \neq \emptyset$, so in particular when $g = 1$.

In order to complete our analysis of theta groups in the case of full level $n$ structure, we ought to compute the linear part of $\Delta$ when $n$ is even. We have done this when $g = 1,\ n = 2$, as will appear in a forthcoming work [Cl4]. In general, it should be the case that having full level $2n$-structure is sufficient for $\mathcal{G}_{nP} \cong \mathcal{H}(\underline{n})$, at least in the case of symmetric $P$. We hope to return to this point (which requires a bit more of Mumford's theory than we wish to enter into here) in a later work.

## 7. Horizontal growth of the $p$-part of the Shafarevich-Tate group

In this section we give the proofs of Theorems 8 and 9 and of Corollary 10. These results were proved in [Cl1] in the elliptic curve case.

Suppose that $A_{/k}$ is a strongly principally polarized abelian variety over a number field and $p$ is a prime number such that $A[p]$ and $NS(A)$ are both trivial $\mathfrak{g}_k$-modules. In order to show that a principal homogeneous space $V \in H^1(k, A)[p]$ has index exceeding $p$, it suffices, by Theorem 31, to show that for every lift $\xi$ of $V$ to $H^1(k, A[n])$, $\Delta(\xi) \neq 0$. Using the Kummer sequence

$$0 \to A(k)/pA(k) \to H^1(k, A)[p] \to H^1(k, A)[p] \to 0$$

and the finiteness of $A(k)/pA(k)$ (weak Mordell-Weil theorem), the proof of Theorem 8 is reduced to the following elementary claim.

**Proposition 47.** *Let $k$ be a number field containing the pth roots of unity, and let $H \subset (k^*/k^{*p})^{2g}$ be any finite subgroup. Then there exists an infinite subgroup $G \subseteq (k^*/k^{*p})^{2g}$ such that for every nonidentity element $g$ of $G$ and every element $h \in H$, the Brauer group element $\Delta(hg)$ is nonzero.*

This is proven in [Cl1] in the $g = 1$ case, using standard results from local and global class field theory. The general case can be proven in the same way – in fact one can find such a subgroup consisting of elements $(a_1, b_1, \ldots, a_d, b_d)$ for which $a_i = b_i = 1$ for $1 \leq i \leq d-1$, thereby reducing to the one-dimensional case.

This completes the proof of Theorem 8.

For the proof of Theorem 9, let $G \subseteq H^1(k, A)[p]$ be an infinite subgroup each of

whose nontrivial elements cannot be split by a degree $p$ field extension.[10] Let $G' \subseteq G$ be a complementary subspace to the finite-dimensional $\mathbb{F}_p$-subspace $Ш(A_{/k})[p] \cap G$, so that $G'$ has finite index in $G$. We define a finite set $B \subset \Sigma_k$ of "bad places" of $k$ as follows: $B$ consists of all real places of $k$, all places lying over $p$ and all places at which $A$ has bad reduction. Define $H^1(k_B, A)[p] = \bigoplus_{v \in B} H^1(k_v, A)[p]$; this is a finite abelian group. So letting $k_{\Phi_1}$ be the kernel of the natural map $\Phi_1 : H^1(k, A)[p] \to H^1(k_B, A)[p]$, we have that $G_1 := G' \cap k_{\Phi_1}$ has finite index in $G'$ and is therefore infinite.

Each nonzero element $\eta_1 \in G_1$ yields nontrivial elements of Ш over degree $p$ field extensions: let $\Sigma_1$ be the finite set of places of $k$ at which $\eta_1$ is locally nontrivial, and consider any such place $v$. By the theorem of Lang and Tate, $\eta_1 \in H^1(k_v, A)[p]$ can be split by a degree $p$ extension $l_v/k_v$, indeed by any ramified extension of degree $p$. (More precisely, we invoke [LaTa] in the non-Archimedean case: if $v$ is a real Archimedean place – at which $g_1$ can only be nontrivial if $p = 2$ – then obviously the class splits over $\mathbb{C}$.) By weak approximation, we can find infinitely many degree $p$ global extensions $l/k$ completing to each $L_v/k_v$ for all $v \in \Sigma_L$. By construction, the restriction of $\eta_1$ to $l$ is everywhere locally trivial, so represents an element of $Ш(A/L)[p]$. Since $\eta_1$ does not split over any degree $p$ field extension of $k$, $\eta_1$ represents a nonzero element in $Ш(A/L)[p]$.

Finally, we can inductively build increasingly large finite subgroups $H_i$ of $G'$ such that the restriction to suitable degree $p$ field extensions $l_i/k$ is injective on $H_i$, as follows: start with any nonzero $\eta_1 \in G_1$ as above. Put $B_2 := B \cup \Sigma_1$ and $G_2 := G_1 \cap k_{\Phi_2}$. For any nonzero element $\eta_2 \in G_2$, the set $\Sigma_2$ of places at which $\eta_2$ is locally nontrivial is disjoint from $\Sigma_1$, so again we can find infinitely many degree $p$ global extensions with prescribed global behavior at $\Sigma_1 \cup \Sigma_2$, and so on. Continuing in this way, we can for any $N$ construct a cardinality $N$ set of classes $\{\eta_1, \ldots, \eta_N\}$; since their sets $\Sigma_1, \ldots, \Sigma_r$ are pairwise disjoint and nonempty, these classes automatically form an $\mathbb{F}_p$-linearly independent set. Let $l/k$ be any of the infinitely many global degree $p$ extensions that simultaneously locally trivialize each $\eta_i$. We finish by remarking that the $\eta_i$ remain $\mathbb{F}_p$-independent as elements of $Ш(A/L)[p]$: if there exist $a_1, \ldots, a_N \in \mathbb{F}_p$ such that

$$a_1 \eta_1|_l + \ldots + a_N \eta_N|_l = 0,$$

then the class $a_1\eta_1 + \ldots + a_N\eta_N$ is an element of $G$ which gets split over a degree $p$ field extension, so that $a_1 = \ldots = a_N = 0$.

Proof of Corollary 10: We proceed by extending the base field of an arbitrary principally polarized abelian variety over a number field so that the hypotheses of Theorem 7 are satisfied. That is, given $A_{/k}$, we need to bound the degree of a field extension $l_1/k$ such that namely, that $A[p]$ and $NS(A)$ are trivial Galois modules, and that the polarization comes from a $l_1$-rational line bundle; we then apply Theorem 9 and pick up an extra factor of $p$. First trivialize $A[p]$ as a Galois module – because of the Galois-equivariance of the Weil pairing, the mod $p$ Galois representation lands in the general symplectic group $GSp_{2g}(\mathbb{F}_p)$. The obstruction $c_\lambda$ to

[10] Note that we showed the existence of an infinite subgroup $G$ all of whose elements have index exceeding $p$, but we only use the weaker property that their m-invariant exceeds $p$.

the principal polarization being a strong polarization lives in $H^1(k, A)[2]$, so that by Proposition 12 this class can be split over an extension of degree dividing $2^{2g}$. It remains to trivialize the $\mathfrak{g}_k$-action on the Néron-Severi group. We claim that the $\mathfrak{g}_k$-action on $NS(A)$ of any $g$-dimensional abelian variety over any field $k$ can be trivialized over a field extension of degree at most $\#GL_{4d^2}(\mathbb{F}_3)$.[11] Indeed $NS(A) \cong \mathbb{Z}^g$, where $g$ is the $\mathbb{Q}$ rank of Rosati-fixed subalgebra of $\mathrm{End}^0(A) = \mathrm{End}(A/\overline{k}) \otimes \mathbb{Q}$, so in any case $g \leq \dim_{\mathbb{Q}} \mathrm{End}^0(A) \leq 4d^2$. Letting $l/k$ be the splitting field for the Galois action, we get a faithful representation $\rho : \mathfrak{g}_{l/k} \hookrightarrow GL_{4d^2}(\mathbb{Z})$, whence $[L : k]$ is bounded above by the order of some finite subgroup of $GL_{4d^2}(\mathbb{Z})$. But the finite subgroups of $GL_N(\mathbb{Z})$ are uniformly bounded, and indeed – see e.g. [Se3] – there is the stronger fact that for any odd prime $\ell$, a finite subgroup $G$ of $GL_N(\mathbb{Z}_\ell)$ has trivial intersection with the kernel of reduction of $GL_N(\mathbb{Z}_\ell) \to GL_N(\mathbb{F}_\ell)$ hence has order at most $\#GL_N(\mathbb{F}_\ell)$. Taking $\ell = 3$ establishes the claim and completes the proof of Corollary 10.

## References


[AgSt] A. Agashe and W. Stein. *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory 97 (2002), 171-185.

[Am] A. Amitsur. *On central division algebras*, Israel J. Math., 12 (1972), 408-420.

[AV] G. van der Geer and B. Moonen. *Abelian varieties*, manuscript available at `http://turing.wins.uva.nl/~ bmoonen/boek/BookAV.html`.

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

[Ca1] J.W.S. Cassels. *Arithmetic on a curve of genus one. (IV) Proof of the Hauptvermutung*, Proc. London Math. Soc. 46 (1962), 259-296.

[Ca2] J.W.S. Cassels. *Arithmetic on a curve of genus one. (V) Two counterexamples*, J. London Math Soc. 36 (1961), 177-184.

[Cl1] P.L. Clark. *The period-index problem in WC-groups I: elliptic curves*, J. Number Theory 114 (2005), 193-208.

[Cl2] P.L. Clark. *There are genus one curves of every index over every number field*, to appear in J. Reine Angew. Math.

[Cl3] P.L. Clark. *Abelian points on algebraic curves*, submitted for publication.

[Cl4] P.L. Clark. *Period-index problems in WC-groups III: biconic curves*, in preparation.

[CrMa] J.L. Cremona and B. Mazur. *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. 9 (2000), 13-28.

[dJ] A.J. de Jong. *The period-index problem for the Brauer group of an algebraic surface*, preprint, 2002.

[Ge] L. Gerritzen. *Periode und Index eines prinzipal-homogenen Raumes über gewissen abelschen Varietäten*, Manuscripta Math. 8 (1973), 131-142.

[Ha] T. Harase. *On the index-period problem for algebraic curves and abelian varieties*, J. Fac. Sci. Univ. Tokyo Sect. 1A Math. 20 (1973), 13-20.

[Kl] T. Klenke. *Visualizing elements of order two in the Weil-Châtelet group*, J. Number Theory 110 (2005), 387-395.

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

[Li1] S. Lichtenbaum. *The period-index problem for elliptic curves*, Amer. J. Math. (90), 1968, 1209-1223.

[Li2] S. Lichtenbaum. *Duality theorems for curves over p-adic fields*, Inventiones math. (7) 120-136 (1969).

[Ma] B. Mazur. *Visualizing elements of order 3 in the Shafarevich-Tate group*, Asian J. Math. 3 (1999), 221-232.


[11] At least in characteristic zero this bound is certainly not optimal. Our intent is merely to write down an explicit bound which can be obtained without too much trouble.

[MS] A.S. Merkurjev and A.A. Suslin. *K-cohomology of Severi-Brauer varieties and the norm-residue homomorphism*, Math. USSR-Izv. 21 (1983), 307-340.

[Mu] D. Mumford. *On the equations defining abelian varieties. I*, Inventiones math. (1) 1966, 287-354.

[O'N] C.H. O'Neil. *The period-index obstruction for elliptic curves*, J. Number Theory 97 (2002), 329-339.

[Pa] I. Passi. *Polynomial maps on groups*, J. Algebra 9 (1968), 121-151.

[Po] A. Polishchuk. *Analogue of Weil representation for abelian schemes*, J. Reine Angew. Math. 543 (2002), 1-37.

[PoSt] B. Poonen and M. Stoll. *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of. Math. (2) 150 (1999), 1109-1149.

[Se1] J.-P. Serre. *Cohomologie Galoisienne*. Lecture Notes in Mathematics 5, 5th revised edition, Springer-Verlag 1994.

[Se2] J.-P. Serre. *Corps Locaux*, Hermann, Paris, 1962.

[Se3] J.-P. Serre. *Lie Algebras and Lie groups*, Lecture Notes in Mathematics 1500, Springer-Verlag, 1992.

[Ш] I. Shafarevich. *Principal homogeneous spaces defined over a function field*, Trudy Mat. Inst. Steklov. 64 (1961), 316-346.

[Sh] R. Sharifi. *Twisted Heisenberg representations and local conductors*, 1999 Chicago Thesis, available at `http://abel.math.harvard.edu/~sharifi`.

[Si] J. Silverman. *Advanced topics in the arithmetic of elliptic cruves*, Graduate Texts in Mathematics, 151, Springer, 1994.

[St] W. Stein. *There are genus one curves over $\mathbb{Q}$ of every odd index*, J. Reine Agnew. Math. 547 (2002), 139-147.

[Ta] J. Tate. *WC-groups over p-adic fields*, Sem. Bourbaki, Exp. 156, 1957.

[vH] J. van Hamel. *Lichtenbaum-Tate duality for varieties over p-adic fields*, J. Reine Agnew. Math. 575 (2004), 101-134.

[Yu] J.K. Yu. *Construction of tame supercuspidal representations*, J. Amer. Math. Soc. 14 (2001), 579-622.

[Za] Yu. Zarkhin. *Noncommutative cohomologies and Mumford groups*, Mathematical Notes 15 (1974), 241-244.

Mathematical Sciences Research Institute, 17 Gauss Way, Berkeley, CA 94720-5070
*E-mail address*: `plclark@msri.org`