There are genus one curves of every index over every infinite, finitely generated field

Pete L. Clark and Allan Lacy

Abstract

Every nontrivial abelian variety over a Hilbertian field in which the weak Mordell-Weil theorem holds admits infinitely many torsors with period any $n > 1$ which is not divisible by the characteristic. The corresponding statement with "period" replaced by "index" is plausible but much more challenging. We show that for every infinite, finitely generated field K, there is an elliptic curve $E_{/K}$ which admits infinitely many torsors with index any $n > 1$.

Contents

2010 Mathematics Subject Classification 12G05, 11G05

Keywords: Galois cohomology, abelian variety, torsor, period, index

1. Introduction

1.1 Review of the Period-Index Problem

Let K be a field, with a choice of separable closure K^{sep} and algebraic closure $\overline{K}$. Let $\mathfrak{g}_K = \mathrm{Aut}(K^{\mathrm{sep}}/K) = \mathrm{Aut}(\overline{K}/K)$ be the absolute Galois group of K.

By a **variety** $X_{/K}$, we will mean a finite type integral scheme over $\operatorname{Spec} K$ such that K is algebraically closed in $K(X)$. (Thus $X_{/\overline{K}}$ need not be a variety.) A field extension L/K is a **splitting extension** for X if $X(L) \neq \varnothing$. For a regular geometrically integral variety $X_{/K}$, we define the **index** $I(X)$ as the least positive degree of a K-rational zero-cycle on X. Equivalently, it is the greatest common divisor of all degrees of finite splitting extensions. We have $I(X_{/L}) \mid I(X)$ for every field extension L/K.

Let M be a commutative $\mathfrak{g}_K$-module. For $i \in \mathbb{N}$ we have the Galois cohomology groups $H^i(K, M) = H^i(\mathfrak{g}_K, M)$. For $i \geqslant 1$, $H^i(K, M)$ is a torsion commutative group. For $i \geqslant 1$ and $\eta \in H^i(K, M)$, we define the **period** $P(\eta)$ as the order of η in $H^i(K, M)$.

If L/K is algebraic, then $\mathfrak{g}_L = \mathrm{Aut}(K^{\mathrm{sep}}/L)$ is a closed subgroup of $\mathfrak{g}_K$ and there is a natural **restriction map**

$$\mathrm{Res}_L : H^i(K, M) \to H^i(L, M).$$

We shall also want to consider restriction maps associated to transcendental field extensions, and for this we need a bit more structure: let $A_{/K}$ be a locally finite type commutative group scheme. Then $M = A(K^{\mathrm{sep}})$ is a $\mathfrak{g}_K$-module, and we write $H^i(K, A)$ for $H^i(K, A(K^{\mathrm{sep}}))$. Let L/K be any field extension. There is a field embedding $\iota : \overline{K} \hookrightarrow \overline{L}$. Any automorphism $\sigma \in \mathrm{Aut}(\overline{L}/L)$ fixes K pointwise so restricts to an automorphism of $\overline{K}$. This gives a continuous group homomorphism $\mathfrak{g}_L \to \mathfrak{g}_K$ and thus for all $i \geqslant 0$ a **restriction map**

$$\mathrm{Res}_L : H^i(K, A) \to H^i(L, A).$$

The map Res_L is independent of the choice of ι [CG, § II.1.1, Remarque 2]. We put

$$\widetilde{H}^i(L/K, M) = \mathrm{Ker}\left(\mathrm{Res}_L : H^i(K, M) \to H^i(L, M)\right).$$

If $\eta \in \widetilde{H}^i(L/K, M)$, we say L is a **splitting field** for η. By the definition of Galois cohomology, every $\eta \in H^i(K, M)$ has a finite Galois splitting extension L/K. We define the **index** $I(\eta)$ to be the greatest common divisor of all degrees $[L : K]$ for L/K a finite splitting field of η. For all $\eta \in H^i(K, M)$ with $i \geqslant 1$ we have $P(\eta) \mid I(\eta)$ and $I(\eta)$ divides some power of $P(\eta)$ [WCII, Proposition 11]. To explore the relations between period and index is the **period-index problem in Galois cohomology**.

The following standard result reduces us to the case of prime power period.

Lemma 1. *(Primary Decomposition) Let $i, r \geqslant 1$, and let $\eta_1, \ldots, \eta_r \in H^i(K, M)$ be such that $P(\eta_1), \ldots, P(\eta_r)$ are pairwise coprime. Let $\eta = \eta_1 + \ldots + \eta_r$. Then*

$$P(\eta) = \prod_{j=1}^{r} P(\eta_j) \tag{1}$$

and

$$I(\eta) = \prod_{j=1}^{r} I(\eta_j). \tag{2}$$

Proof. Easy group theory gives (1). For (2) see e.g. [WCII, Proposition 11d)]. $\square$

Here we are interested in the case $M = A(K^{\mathrm{sep}})$ for an abelian variety $A_{/K}$. Then $H^1(K, A)$ is naturally isomorphic to the **Weil-Châtelet group** of $A_{/K}$, whose elements are torsors under $A_{/K}$. When $A = E$ is an elliptic curve, classes in $H^1(K, E)$ correspond to genus one curves $C_{/K}$ together with an identification $\operatorname{Pic}^0 C \cong E$.

1.2 Constructing Weil-Châtelet Classes With Prescribed Period

Fix a field K and consider the problem of characterizing all possible periods and indices of elements in $H^1(K, A)$, either for a fixed abelian variety $A_{/K}$ or as A varies in a class of abelian varieties defined over K. The point is that it is much easier to understand this problem for the period than for the index. Indeed, in the earliest days of Galois cohomology Shafarevich established the following result.

Theorem 2. *(Shafarevich [Ш57]) Let K be a number field and $A_{/K}$ a nontrivial abelian variety. For each $n > 1$, there are infinitely many classes $\eta \in H^1(K, A)$ with $P(\eta) = n$.*

We wish to indicate a vast proving ground for the period-index problem in Weil-Châtelet groups by giving a generalization of Theorem 2. In order to do so we first define some suitable classes of fields.

A field K is **Mordell-Weil** if for every abelian variety $A_{/K}$, the group $A(K)$ is finitely generated. For $n \in \mathbb{Z}^+$, a field K is **n-Weak-Mordell-Weil** if for every abelian variety $A_{/K}$, the group $A(K)/nA(K)$ is finite. (The nomenclature may be new, but the study of such fields in the Galois cohomology of abelian varieties goes back to [LT58, §5].) Finally, K is **Weak-Mordell-Weil** if it is n-Weak-Mordell-Weil for all $n \in \mathbb{Z}^+$.

Remark 3. *a) $\mathbb{F}_p$ is a Mordell-Weil field: for any variety $V_{/\mathbb{F}_p}$, $V(\mathbb{F}_p)$ is finite.*
b) $\mathbb{Q}$ is a Mordell-Weil field: the Mordell-Weil Theorem.
c) An algebraically closed field K is Weak-Mordell-Weil: for any abelian variety $A_{/K}$, $A(K)$ is a divisible commutative group, so $A(K)/nA(K) = 0$ for all $n \in \mathbb{Z}^+$.
d) $\mathbb{R}$ is a Weak-Mordell-Weil field: by Lie theory, for any g-dimensional abelian variety $A_{/\mathbb{R}}$, $A(\mathbb{R})$ is a split extension of the finite commutative group $\pi_0(A(\mathbb{R}))$ by the connected component of the identity, which is isomorphic to $(\mathbb{R}/\mathbb{Z})^g$ and thus divisible.
e) $\mathbb{Q}_p$ is a Weak-Mordell-Weil field: by p-adic Lie theory (cf. §5.1), for any g-dimensional abelian variety $A_{/\mathbb{Q}_p}$, $A(\mathbb{Q}_p)$ is a split extension of a finite commutative group by the group $\mathbb{Z}_p^d$.
f) For any prime number p, the Laurent series field $K = \mathbb{F}_p((t))$ is n-Weak-Mordell-Weil for all n prime to p. However K is not *p-Weak-Mordell-Weil: see §5.1 for stronger results.*

The following (surely known, though we may as well prove it) result gives further examples.

Proposition 4. *Let L/K be a finitely generated field extension.*
a) If K is a Mordell-Weil field, so is L.
b) If K is a Weak-Mordell-Weil field, so is L.

Proof. Let $\{t_1, \ldots, t_n\}$ be a transcendence basis for L/K, and put $K' = K(t_1, \ldots, t_n)$, so K'/K is finitely generated regular and L/K' is finite. Thus we may deal separately with the two cases L/K finitely generated regular and L/K finite.
Step 1: Let L/K be finitely generated regular, and let $A_{/L}$ be an abelian variety. By the Lang-Néron Theorem [LN59], [Co06, §7] there is an abelian variety $B_{/K}$ and an injective group homomorphism $\tau : B(K) \hookrightarrow A(L)$ with $A(L)/\tau(B(K))$ is finitely generated. So: if K is (Weak-)Mordell-Weil, so is L.
Step 2: Suppose L/K is finite. For an abelian variety $A_{/L}$, let $B_{/K}$ be the abelian variety obtained by Weil restriction. Then $A(L) = B(K)$, hence $A(L)/nA(L) \cong B(K)/nB(K)$ for all $n \in \mathbb{Z}^+$. Thus if K is (Weak-)Mordell-Weil, so is L. □

Combining Remark 3 and Proposition 4 yields:

Corollary 5. *a) (Néron) Every finitely generated field is an Mordell-Weil field.*
b) Every field which is finitely generated over an algebraically closed field, $\mathbb{R}$ or $\mathbb{Q}_p$ is Weak-Mordell-Weil.

We also need the notion of a **Hilbertian field**. We refer to the text [FJ] both for the definition of Hilbertian field (p. 219) and for the proofs of the following basic results, which are the only facts about Hilbertian fields needed in the proof of Theorem 6 below:

- A Hilbertian field must be infinite.
- The field $\mathbb{Q}$ is Hilbertian [FJ, Theorem 13.4.2].
- If K is Hilbertian and L/K is finite, then L is Hilbertian [FJ, Proposition 12.3.3].
- For any field K, the rational function field $K(t)$ is Hilbertian [FJ, Theorem 13.4.2].

Thus every infinite, finitely generated field is Hilbertian.

We can now state the following generalization of Shafarevich's theorem.

Theorem 6. *Let K be Hilbertian, and let $A_{/K}$ be a nontrivial abelian variety. If $n > 1$ is an integer indivisible by* $\operatorname{char} K$ *and such that $A(K)/nA(K)$ is finite, then there are infinitely many classes $\eta \in H^1(K, A)$ of period n.*

Thus if K has characteristic 0 and is Weak-Mordell-Weil then for any nontrivial abelian variety $A_{/K}$, the Weil-Châtelet group $H^1(K, A)$ has infinitely many classes of period n for each $n \geqslant 2$.

We will prove Theorem 6 in §3.

Remark 7. *A field K is **PAC** (pseudo-algebraically closed) if every geometrically integral variety $V_{/K}$ has a K-rational point. All Weil-Châtelet groups over a PAC field are trivial. Algebraically closed fields are PAC and Weak-Mordell-Weil but not Hilbertian. So the hypothesis "K is Hilbertian" cannot be omitted from Theorem 6. There are characteristic* 0 *fields K which are Hilbertian and PAC: it follows from Theorem 6 that for every nontrivial abelian variety A over such a K and all $n \geqslant 2$, $A(K)/nA(K)$ is infinite. Thus the hypothesis "K is Weak-Mordell-Weil" cannot be omitted from Theorem 6.*

1.3 Constructing Weil-Châtelet Classes With Prescribed Index

It is much harder to construct classes in $H^1(K, A)$ with prescribed index. This problem was first studied by Lang and Tate [LT58].

Theorem 8. *(Lang-Tate [LT58]) Let $n \in \mathbb{Z}^+$, and let K be a field with infinitely many abelian extensions of exponent n. Let $A_{/K}$ be an abelian variety such that $A(K)/nA(K)$ is finite and $A(K)$ contains at least one element of order n. Then $H^1(K, A)$ contains infinitely many elements of period n and, in fact, infinitely many such that the corresponding torsors have index n as well as period n.*

Let us compare this result with Theorem 6: we have the same hypothesis on weak Mordell-Weil groups, and the hypothesis on abelian extensions holds over every Hilbertian field. On the other hand, the hypothesis on the existence of a point $P \in A(K)$ of order n is prohibitively strong: by Merel's Theorem, for each number field K, there are only finitely many $n \in \mathbb{Z}^+$ for which an elliptic curve $E_{/K}$ can have a point of order n. We expect that for any infinite, finitely generated field K and $d \in \mathbb{Z}^+$, torsion is uniformly bounded on d-dimensional abelian varieties $A_{/K}$.

Lang and Tate asked whether for every positive integer n there is some elliptic curve $E_{/\mathbb{Q}}$ and class $\eta \in H^1(\mathbb{Q}, E)$ with index n. This question remained wide open for years until W. Stein showed [St02] that for every number field K and every positive integer n which is not divisible by 8, there is an elliptic curve $E_{/K}$ and a class $\eta \in H^1(K, E)$ with $I(\eta) = P(\eta) = n$. In [Cl05] the first author showed that for any number field K and every $n \in \mathbb{Z}^+$ there is an elliptic curve $E_{/K}$ and a class $\eta \in H^1(K, E)$ with $I(\eta) = P(\eta) = n$.

Thus the answer to the question of Lang and Tate is affirmative, but it took almost 50 years to get there. More recently S. Sharif established a result which we view as a complete solution of the period-index problem for elliptic curves over number fields.

Theorem 9. *(Sharif [Sh12]) Let $E_{/K}$ be an elliptic curve over a number field, and let $P, I \in \mathbb{Z}^+$ be such that $P \mid I \mid P^2$. Then there is a class $\eta \in H^1(K, E)$ with $P(\eta) = P$ and $I(\eta) = I$.*

We find it plausible that the analogue of Sharif's result should hold for every elliptic curve over every Hilbertian, Weak-Mordell-Weil field K. However, this appears to be very challenging to prove. Consider the case of global fields of positive characteristic: i.e., finite field extensions of $\mathbb{F}_p(t)$. In this case the methods of [Sh12] work to establish the analogue of Theorem 9 as long as we require $\gcd(P, p) = 1$. The case of p-power period in characteristic p leads to additional technicalities involving an explicit form of the period-index obstruction map in flat cohomology. (The first author and S. Sharif have been working on this problem for several years.) We find it of interest to retreat to the construction of genus one curves with prescribed index over various fields, but where we get to choose the Jacobian elliptic curve to our advantage.

We can now state the main result of this paper.

Main Theorem. *Let K be any infinite, finitely generated field. There is an elliptic curve $E_{/K}$ such that for all $n > 1$, there are infinitely many classes $\eta \in H^1(K, E)$ with $I(\eta) = P(\eta) = n$.*

Remark 10. *The period-index problem has additional subtleties when the period is divisible by the characteristic of the field, e.g. requiring the use of flat cohomology. In our Main Theorem, the integer n* is allowed *to be divisible by the characteristic. We feel that a substantial part of the value of this result lies in its inclusion of this positive characteristic case.*

Remark 11. *In the statement of the Main Theorem, it is easy to replace the elliptic curve $E_{/K}$ with a g-dimensional abelian variety $A_{/K}$ for any fixed $g \geqslant 1$: for any torsor C under E with*

$P(C) = I(C) = n$, $C \times E^{g-1}$ is a torsor under E^g with $P(C) = I(C) = n$. It would be more interesting to treat abelian varieties and torsors which are not products.

Remark 12. *The hypothesis that K is infinite is necessary: by a classic result of Lang [La56], $H^1(\mathbb{F}_q, A) = 0$ for every abelian variety A over a finite field $\mathbb{F}_q$.*

1.4 Acknowledgments

This work had its genesis in a conversation with S. Sharif. In particular the main idea of the proof of Lemma 39 is due to him. We thank Cristian D. González-Avilés for technical (and moral) support. We are grateful to Kestutis Česnavičius for help strengthening the statement and clarifying the proof of Theorem 21. We thank the referee for a careful reading.

2. Linear Independence in Torsion Groups

Let A be commutative group. For a torsion element $\eta \in A$ we define the *order* of η as the least positive integer n such that $n\eta = 0$. At the request of the referee, we remark that when we say "P is a point of order n" we mean exactly that and not just that $nP = 0$.

At several points in the coming proofs, we will find ourselves in the following situation: we have an integer $n > 1$, a commutative group A, an infinite subset $S \subset A$ such that every element of S has order n and a homomorphism of groups $R : A \to B$. In what circumstances does $R(S)$ have infinitely many elements of order n?

It suffices for R to be injective, but in our applications this hypothesis is too strong. On the other hand, if $\operatorname{Ker} R$ is too large then we may have $R(S) = \{0\}$. So it is natural to assume that $\operatorname{Ker} R$ is finite. In this case R has finite fibers and thus $R(S)$ is infinite. However, it still need not be the case that $R(S)$ has infinitely many elements of order n.

Example 13. *Let p be a prime and I an infinite set. Put $A = \left(\bigoplus_{i\in I} \mathbb{Z}/p\mathbb{Z}\right) \oplus \mathbb{Z}/p^2\mathbb{Z}$, $K = \mathbb{Z}/p\mathbb{Z}^2$, $B = A/K$, and $R : A \to B$ be the quotient map. Then*

$$S = \{1 + x \mid x \in \bigoplus_{i\in I} \mathbb{Z}/p\mathbb{Z}\}$$

has cardinality $\#I$ and consists of elements of order p^2, but $R(S) \subset B = B[p]$ consists of elements of order dividing p.

Evidently stronger group-theoretic hypotheses must be imposed, which serves to motivate the definitions of the next paragraph.

Let $n \geqslant 2$, let H be a commutative group, and let $S = \{\eta_s\} \subset H[n]$. For $r \in \mathbb{Z}^+$, we say S is **r-linearly independent** over $\mathbb{Z}/n\mathbb{Z}$ if every r-element subset $\{\eta_1, \ldots, \eta_r\}$ is linearly independent over $\mathbb{Z}/n\mathbb{Z}$: if for $a_1, \ldots, a_r \in \mathbb{Z}$ we have $a_1\eta_1 + \ldots + a_r\eta_r = 0$, then $a_1 \equiv \ldots \equiv a_r \equiv 0 \pmod{n}$. Equivalently, the subgroup generated by $\eta_1, \ldots, \eta_r$ has cardinality n^r. We say S is **linearly independent** over $\mathbb{Z}/n\mathbb{Z}$ if it is r-linearly independent over $\mathbb{Z}/n\mathbb{Z}$ for all $r \in \mathbb{Z}^+$.

In particular, S is 1-linearly independent over $\mathbb{Z}/n\mathbb{Z}$ iff every element of S has order n, and S is 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$ iff for any distinct elements $\eta_i \neq \eta_j \in S$, we have $\langle \eta_i \rangle \cap \langle \eta_j \rangle = \{0\}$.

Lemma 14. *Let $n \in \mathbb{Z}^+$, let $R : H_K \to H_L$ be a homomorphism of commutative groups, and let $S \subset H_K[n]$ be a subset.*
a) If $\operatorname{Ker} R = 0$, then $\#R(S) = \#S$, and for each $r \in \mathbb{Z}^+$, S is r-linearly independent over $\mathbb{Z}/n\mathbb{Z}$ if and only if $R(S)$ is r-linearly independent over $\mathbb{Z}/n\mathbb{Z}$.
b) Suppose $\operatorname{Ker} R$ is finite and S is infinite and 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. Then there is a subset $S' \subset S$ such that $R(S')$ is an infinite subset of H_L which is 1-linearly independent over $\mathbb{Z}/n\mathbb{Z}$.

Proof. a) If $\operatorname{Ker} R = 0$, then R is an injection of n-torsion groups. Thus $R : S \to R(S)$ is a bijection and all linear independence relations are preserved.
b) By the Chinese Remainder Theorem, it suffices to consider the case of $n = l^a$, a prime power. Let $N = \# \operatorname{Ker} R$. Let $\eta_1, \ldots, \eta_{N+1}$ be any $N+1$ elements of S. We claim that for at least one i, $1 \leqslant i \leqslant N+1$, $R(\eta_i)$ has order n: if not, then for all i we have

$$0 = \ell^{a-1} R(\eta_i) = R(\ell^{a-1}\eta_i),$$

so $\ell^{a-1}\eta_i \in \operatorname{Ker} R$ for all i. By the Pigeonhole Principle we must have $\ell^{a-1}\eta_i - \ell^{a-1}\eta_j = 0$ for some $i \neq j$, contradicting the hypothesis that S is 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. This constructs an infinite $S' \subset S$ such that for all $\eta \in S$, $R(\eta)$ has order n. Since $\operatorname{Ker} R$ is finite, all the fibers of R are finite, and thus $R(S')$ is infinite. □

3. The Proof of Theorem 6

3.1 The Proof

Step 0: Let $n > 1$ be indivisible by the characteristic of K; let $A_{/K}$ be an abelian variety of dimension $g \geqslant 1$ such that $A(K)/nA(K)$ is finite. We write $A[n]$ for both the group scheme – which is étale – and the associated $\mathfrak{g}_K$-module $A[n](K^{\text{sep}})$ with underlying commutative group $(\mathbb{Z}/n\mathbb{Z})^{2g}$. Recall the **étale Kummer sequence**

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

We claim that the n-torsion group $H^1(K, A[n])$ has an infinite subset S which is linearly independent over $\mathbb{Z}/n\mathbb{Z}$. (We only need S to be 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. But the more general result is no harder to prove.) Applying Lemma 14b) with $H_K = H^1(K, A[n])$, $H_L = H^1(K, A)[n]$ and R the natural map between them, we get an infinite subset $S' \subset S$ whose image in $H^1(K, A)[n]$ is 1-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. In other words, $H^1(K, A)$ has infinitely many elements of order n, which is what we want to show. In the remainder of the argument we will establish this claim.
Step 1: Let $L = K(A[n](K^{\text{sep}}))$ – the fixed field of the kernel of the $\mathfrak{g}_K$-action on $A[n]$ – let $\mathfrak{g}_{L/K} = \operatorname{Aut}(L/K)$, and consider the associated inflation-restriction sequence [CG, I.2.6(b)]

$$0 \to H^1(\mathfrak{g}_{L/K}, A[n](L)) \to H^1(K, A[n]) \overset{\Phi}{\to} H^1(L, A[n])^{\mathfrak{g}_{L/K}} \overset{\partial}{\to} H^2(\mathfrak{g}_{L/K}, A[n](L)). \qquad (3)$$

Since $H^i(\mathfrak{g}_{L/K}, A[n](L))$ is finite for all i, the kernel and cokernel of Φ are finite. We will construct an infinite subset of $S' = \Phi(H^1(K, A[n]))$, linearly independent over $\mathbb{Z}/n\mathbb{Z}$. For each $\eta_i' \in S'$, choose $\eta_i \in \Phi^{-1}(\eta_i')$. Then $S = \{\eta_i\}_{i \in S'} \subset H^1(K, A[n])$ is infinite and linearly independent over $\mathbb{Z}/n\mathbb{Z}$.
Step 2: We have $H^1(L, A[n]) = \operatorname{Hom}(\mathfrak{g}_L, A[n](L))$, so the surjective elements $\eta \in H^1(L, A[n])$ – i.e., such that $\eta(\mathfrak{g}_L) = A[n](L)$ – parameterize Galois extensions M/L with $\operatorname{Gal}(M/L) \cong A[n](L) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ together with an isomorphism $\operatorname{Gal}(M/L) \cong A[n](L)$. The natural action of

$\mathfrak{g}_{L/K}$ on this set of order n elements in $H^1(L, A[n])$ consists of precomposing $\chi : \mathfrak{g}_L \to A[n](L)$ with the automorphism σ^* of $\mathfrak{g}_L$ obtained by restricting conjugation by $\sigma \in \mathfrak{g}_K$ to the normal subgroup $\mathfrak{g}_L$. (Because $A[n](L)$ is commutative, the map σ^* depends only on the coset of σ modulo $\mathfrak{g}_L$.) A class $\eta \in H^1(L, A[n])$ is fixed by $\mathfrak{g}_{L/K}$ if and only if the extension $(L^{\mathrm{sep}})^{\mathrm{Ker}\,\eta}/K$ is Galois. So we have shown that the surjective elements of $H^1(L, A[n])^{\mathfrak{g}_{L/K}}$ correspond to **liftings** of the Galois extension L/K to Galois extensions M/K. For $\eta' \in H^1(L, A[n])^{\mathfrak{g}_{L/K}}$, the class $\partial\eta' \in H^2(\mathfrak{g}_{L/K}, A[n](L))$ is the class of the extension

$$1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/K) \to \mathfrak{g}_{L/K} \to 1,$$

so by exactness of (3), we get: $\eta' \in \Phi(H^1(K, A[n]))$ if and only if the above extension splits. Thus: the surjective elements of $\Phi(H^1(K, A[n]))$ parameterize **split extensions** of $\mathfrak{g}_{L/K}$ by $A[n](L)$.
Step 3: It was shown by Ikeda [Ik60] that over a Hilbertian field, every split embedding problem with abelian kernel A has a proper solution: there is at least one surjective (hence order n) element of $\Phi(H^1(K, A[n]))$. The proof of Ikeda's Theorem (see [FJ, §16.4] for a nice modern treatment) goes by specializing a regular A-Galois cover of $L(t)$. Over a Hilbertian field, a regular Galois covering not only has an irreducible specialization but has an infinite linearly disjoint set of irreducible specializations, so we get an infinite set $\{M_i/L\}$ of $A[n](L)$-Galois extensions of L such that M_i/K is Galois and $\mathrm{Gal}(M_i/K) \cong A[n](L) \rtimes \mathfrak{g}_{L/K}$ (see [FJ, Lemma 16.4.2], which gives a slightly weaker statement; the stronger version needed here follows immediately by an inductive argument). The linear disjointness of the extensions M_i/L means that the Galois group of the compositum is the direct product of the Galois groups, and this implies that the set of classes η_i' is linearly independent over $\mathbb{Z}/n\mathbb{Z}$ in $H^1(L, A[n])^{\mathfrak{g}_{L/K}}$, completing the proof.

3.2 A Generalization

In the setup of Theorem 6, the hypothesis that n is not divisible by $\mathrm{char}\,K$ was used to ensure that $A[n]$ is an étale group scheme. In fact we need only that $A[n]$ admits an étale subgroup scheme H of exponent n; equivalently, $A(K^{\mathrm{sep}})$ contains a point of order n. For instance this condition holds if $A_{/K}$ is ordinary and K is perfect. Running the argument with H in place of $A[n]$ gives the following result.

Theorem 15. *Let $A_{/K}$ be a nontrivial abelian variety over a Hilbertian field. Let $n > 1$ be such that $A(K)/nA(K)$ is finite. If $\mathrm{char}\,K \mid n$, suppose $A(K^{\mathrm{sep}})$ contains a point of order n. Then in $H^1(K, A)$ there are infinitely many classes of period n.*

Remark 16. *For every prime p there is an ordinary elliptic curve E over the perfect field $\mathbb{F}_p$. Thus for every field K of characteristic p and all $g \geqslant 1$, there is a g-dimensional abelian variety A such that $A(K^{\mathrm{sep}})$ contains points of order n for all $n > 1$. Thus Theorem 15 implies: every Hilbertian Weak-Mordell-Weil field admits abelian varieties whose Weil-Châtelet groups have infinitely many elements of every period $n > 1$.*

4. The Proof of the Main Theorem: Outline

The proof of the Main Theorem is a three step argument. We go by induction on the transcendence degree. Two out of the three steps concern the base cases. Here is the first step.

Theorem 17. *Let K be a global field, and let $E_{/K}$ be an elliptic curve with $E(K) = Ш(K, E) = 0$. Then for all $n \geqslant 1$, there is an infinite subset $S \subset H^1(K, E)[n]$ which is linearly independent over $\mathbb{Z}/n\mathbb{Z}$ and such that every $\eta \in S$ has index n.*

Theorem 17 should be compared to [Cl05, Theorem 3]: the proofs are identical in the number field case, but the logical setup is a bit different: the conclusion of the earlier result is that classes of arbitrary index exist in every finite extension L/K, but that part of the argument would not work fully in positive characteristic. In the present proof, controlling the period under extensions L/K is handled in a better way in the inductive step of the argument, which comes later (and which exploits the linear independence property of S). We must give particular care to p-primary torsion in characteristic p: here this amounts to using Milne's extension of Poitou-Tate global duality. The proof of Theorem 17 is given in §5.3.

The second step of the proof is to verify that for every *prime global field* K there is an elliptic curve satisfying the hypotheses of Theorem 17. In the case of $K = \mathbb{Q}$ we may take the same elliptic curve used in [Cl05]: namely Cremona's $1813B1$ curve

$$E : y^2 + y = x^3 - 49x - 86. \tag{4}$$

That $E(\mathbb{Q}) = Ш(\mathbb{Q}, E) = 0$ is a deep theorem of Kolyvagin [Ko89, Theorem H].

We also we need such a curve $E_{/\mathbb{F}_p(t)}$ for every prime p. We will show:

Theorem 18. *For every prime number p, the elliptic curve*

$$E : \quad y^2 + txy + t^3y = x^3 + t^2x^2 + t^4x + t^5 \tag{5}$$

defined over $\mathbb{F}_p(t)$ has $E(\mathbb{F}_p(t)) = 0$ and $Ш(\mathbb{F}_p(t), E) = 0$.

The proof of Theorem 18 takes advantage of known cases of the Birch-Swinnerton Dyer conjecture in the function field case. It is given in §6.

Here is the inductive step.

Theorem 19. *Let $n > 1$, K a Weak-Mordell-Weil field, $A_{/K}$ an abelian variety, and L/K be a finitely generated separable field extension. Let $S \subset H^1(K, A)[n]$ be infinite and 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. Then there is an infinite subset $S' \subset S$ such that $\operatorname{Res}_L S' \subset H^1(L, A)[n]$ is infinite and consists of elements of order n. Moreover, if each element of S has index n, then each element of $\operatorname{Res}_L S'$ has index n.*

We will prove Theorem 19 in §7.

Let us now explain how to put Theorems 17, 18 and 19 together to prove the Main Theorem. Let L be an infinite, finitely generated field. Let k_0 be its prime subfield: either $\mathbb{Q}$ or $\mathbb{F}_p$. Since k_0 is perfect, L/k_0 is separable.

Case 1: Suppose $k_0 = \mathbb{Q}$. Then we take the elliptic curve $E_{/\mathbb{Q}}$ of (4), with $E(\mathbb{Q}) = Ш(\mathbb{Q}, E) = 0$. By Theorem 17, for each $n > 1$ there is an infinite subset $S \subset H^1(K, E)$ which is linearly independent over $\mathbb{Z}/n\mathbb{Z}$ and such that every element of S has index n. We apply Theorem 19 with $K = \mathbb{Q}$ and $A = E$ to get the desired result.

Case 2: Suppose $k_0 = \mathbb{F}_p$. Since k_0 is perfect, the finitely generated extension L/k_0 admits a separating transcendence basis $t, t_2, \ldots, t_d$. We take the elliptic curve $E_{/\mathbb{F}_p(t)}$ of Theorem 18. The rest of the argument proceeds as in Case 1.

5. The Proof of Theorem 17

5.1 Mordell-Weil Groups of Abelian Varieties Over Local Fields

By a **local field** we mean a field K which is complete and nondiscrete with respect to an ultrametric norm $|\cdot|$, and with finite residue field k. A local field of characteristic 0 is (canonically) a finite extension of $\mathbb{Q}_p$, and a local field of positive characteristic is (noncanonically) isomorphic to $\mathbb{F}_q((t))$.

If K is a local field and $G_{/K}$ is an algebraic group, then the set G of K-rational points of G has the structure of a **K-analytic Lie group** in the sense of [LALG, LG, Ch. IV]. Since G is quasi-projective, G is homeomorphic to a subspace of $\mathbb{P}^N(K)$ for some K and is thus second countable. When $G = A$ is an abelian variety, G is commutative and compact. In this case, we can use K-adic Lie theory to analyze the structure of the Mordell-Weil group $G = A(K)$ and – crucially for us in what follows – the weak Mordell-Weil groups $A(K)/nA(K)$.

This was done somewhat breezily in [Cl05]: we asserted (6) below, and our justification was "by p-adic Lie theory". Here we need also the positive characteristic case, which although known to some experts, seems not to appear in the literature. This time around we give a careful treatment of both the p-adic and Laurent series field cases, with an eye towards providing a suitable reference for future work.

Lemma 20. *Let H be a commutative, torsionfree pro-p-group, endowed with its profinite topology. Then, as a topological group, $H \cong \prod_{i\in I}\mathbb{Z}_p$ for some index set I. If H is second countable, then I is countable.*

Proof. The Pontrjagin dual H^* of H is a commutative p-primary torsion group. Since $H[p] = 0$, $H^*/pH^* = 0$, so H^* is divisible. It is a classical result that a divisible commutative group is a direct sum of copies of $\mathbb{Q}$ and $\mathbb{Q}_p/\mathbb{Z}_p$ for various primes p [Sc, 5.2.12], and the number of summands of each isomorphism type is invariant of the chosen decomposition. (Or: an injective module over a commutative Noetherian ring R is a direct sum of copies of injective envelopes of modules of the form $R/\mathfrak{p}$ as $\mathfrak{p}$ ranges over prime ideals of R. [Ma, Thms. 18.4 and 18.5]: applying this with $R = \mathbb{Z}_{(p)}$ recovers this classical result.) Thus for some index set I,

$$H^* \cong \bigoplus_{i\in I}\mathbb{Q}_p/\mathbb{Z}_p,$$

and taking Pontrjagin duals gives

$$H \cong \prod_{i\in I}\mathbb{Z}_p.$$

An uncountable product of second countable Hausdorff spaces, each with more than a single point, is not second countable [Wi, Theorem 16.2c)], so if H is second countable, I is countable. □

Theorem 21. *Let K be a local field, with valuation ring R, maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}_q = \mathbb{F}_{p^a}$. If $\operatorname{char} K = 0$, let $d = [K : \mathbb{Q}_p]$. Let G be a compact commutative second countable K-analytic Lie group, of dimension $g \geqslant 1$.*
a) If $\operatorname{char} K = 0$, then $G[\text{tors}]$ is finite and we have a topological group isomorphism

$$G \cong \mathbb{Z}_p^{dg} \oplus G[\text{tors}]. \tag{6}$$

b) If $\operatorname{char} K = p$*, then* $G[\mathrm{tors}]$ *is finite if and only if* $G[p]$ *is finite. When these equivalent conditions hold then we have a topological group isomorphism*

$$G \cong \left(\prod_{i=1}^{\infty} \mathbb{Z}_p\right) \oplus G[\mathrm{tors}]. \tag{7}$$

Proof. Step 0: By [LALG, pp. 116, 117-121], G has a filtration by open subgroups

$$G = G^0 \supset G^1 \supset \ldots \supset G^n \supset \ldots$$

such that
(0) for $i \geqslant 1$, G^0/G^i is finite (this holds because $G = G^0$ is compact and G^i is open).
(i) for $i \geqslant 1$, G^i is obtained by evaluating a g-dimensional formal group law on $(\mathfrak{m}^i)^g$;
(ii) $\bigcap_{i\geqslant 0} G^i = \{0\}$;
(iii) for all $i \geqslant 1$, $G^i/G^{i+1} \cong (k, +)$ is finite of exponent p; and
(iv) $G^1[\mathrm{tors}] = G^1[p^\infty]$ [LALG, p. 118, Theorem 3].
Step 1: We show that $G[\mathrm{tors}]$ is finite if and only if $G[p]$ is finite. Clearly $G[\mathrm{tors}]$ finite implies $G[p]$ finite. Conversely, if $G[p]$ is finite, then (ii) implies that $G^i[p] = 0$ for some i; hence also $G^i[p^\infty] = 0$ and thus, by (iv), $G^i[\mathrm{tors}] = 0$. Then

$$G[\mathrm{tors}] \hookrightarrow G^0/G^i,$$

so by (0) we have that $G[\mathrm{tors}]$ is finite.
Step 2: From now on we assume that $G[\mathrm{tors}]$ is finite. Then we have a short exact sequence of commutative profinite groups

$$0 \to G[\mathrm{tors}] \to G \to G/G[\mathrm{tors}] \to 0. \tag{8}$$

Taking Pontrjagin duals, we get a short exact sequence of discrete torsion groups

$$0 \to (G/G[\mathrm{tors}])^* \to G^* \to G[\mathrm{tors}]^* \to 0. \tag{9}$$

The group $G/G[\mathrm{tors}]$ is torsionfree. The image of the finite index pro-p-subgroup G^1 of G in $G/G[\mathrm{tors}]$ is a finite index pro-p-subgroup, so by Sylow theory [CG, §I.1.4] $G/G[\mathrm{tors}]$ is pro-p. By Lemma 20 we have

$$G/G[\mathrm{tors}] \cong \prod_{i\in I} \mathbb{Z}_p$$

and thus

$$(G/G[\mathrm{tors}])^* \cong \bigoplus_{i\in I} \mathbb{Q}_p/\mathbb{Z}_p.$$

This shows that $(G/G[\mathrm{tors}])^*$ is divisible, hence injective. So (9) splits, hence so too does (8), and we get an isomorphism of topological groups

$$G \cong G/G[\mathrm{tors}] \oplus G[\mathrm{tors}] \cong \prod_{i\in I} \mathbb{Z}_p \oplus G[\mathrm{tors}].$$

Since G is second countable, Lemma 20 implies that I is countable.
Step 3: Suppose $\operatorname{char} K = 0$. Then every g-dimensional compact, commutative K-adic Lie group has an open subgroup isomorphic to $R^g \cong \mathbb{Z}_p^{dg}$ [LALG, p. 151, Corollary 4]. Thus $G/G[\mathrm{tors}] \cong \prod_{i\in I} \mathbb{Z}_p$ and $\mathbb{Z}_p^{dg}$ are both open subgroups of G, and it follows easily that $\#I = dg$. This completes the proof of part a).
Step 4: If $\operatorname{char} K = p > 0$, then in the formal group G_1, we have $[p] \in R[[X_1^p, \ldots, X_g^p]]^g$ [LALG, p. 115, Corollary and p. 121, Exercise 7]. (A different proof using invariant differentials is given

in the $g = 1$ case – which is the case of our Main Theorem – in [AECI, Corollary 4.4]. It is straightforward to adapt this argument to the general case using the corresponding properties of invariant differentials on abelian varieties.) Consider pG_1 as a subset of the profinite space $G_1 = (t\mathbb{F}_q[[t]])^g$. It is compact, hence closed. Moreover, it lies in $(t\mathbb{F}_q[[t^p]])^g$, so it is not open. We deduce that G_1/pG_1 is infinite. Since G_1 and H are finite index subgroups of G, it follows that H/pH is infinite, and thus I is infinite. Since I is countable, we have $G \cong \prod_{i=1}^{\infty} \mathbb{Z}_p \oplus G[\mathrm{tors}]$. □

Remark 22. *In the setting of Theorem 21, when* $\operatorname{char} K = p > 0$*, the group* $G[\mathrm{tors}]$ *need not be finite: take* $G = (\mathbb{G}_a)_{/K}(K) = (\mathbb{F}_q[[t]], +)$.

The following consequence of Theorem 21 is immediate.

Corollary 23. *We retain the notation of Theorem 21.*
a) If $A(K)$ has a point of order n, then so does $A(K)/nA(K)$.
b) For all $a \geqslant 1$, $A(K)/p^a A(K)$ contains a point of order p^a.
c) If $\operatorname{char} K > 0$*, then for all $a \geqslant 1$, $A(K)/p^a A(K)$ contains an infinite subset which is linearly independent over $\mathbb{Z}/p^a\mathbb{Z}$.*

The following key technical result records a global consequence of this local analysis.

Lemma 24. *Let K be a global field, and let $A_{/K}$ be an abelian variety of dimension $g \geqslant 1$. Let $n > 1$ be an integer.*
a) If $\operatorname{char} K \nmid n$*, then there is a positive density set $\mathcal{P}$ of finite places of K such that for all $v \in \mathcal{P}$, $H^1(K_v, A)$ has an element of order n.*
b) If $\operatorname{char} K = p$ *is a prime and $n = p^a$ for $a \geqslant 1$, then for every place v of K, $H^1(K_v, A)$ has infinitely many elements of order n.*

Proof. Step 1: For any finite place v of K, the discrete torsion group $H^1(K_v, A)$ is Pontrjagin dual to the compact profinite group $A(K_v)$: this celebrated **Local Duality Theorem** is due to Tate [Ta57, Proposition 1] when $\operatorname{char} K = 0$ and to Milne [Mi70], [Mi] when $\operatorname{char} K > 0$. It follows that for $n \geqslant 1$, the groups $H^1(K_v, A)[n]$ and $A(K_v)/nA(K_v)$ are Pontrjagin dual.
Step 2: Suppose $\operatorname{char} K \nmid n$. Then, as already recalled, $A[n]$ is a finite *étale* group scheme, so there is a finite Galois extension L/K such that $A(L)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. By the Cebotarev Density Theorem, the set of finite places v which split completely in L has positive density (which one can explicitly bound below in terms of n and g, if needed). For each such v, there is a K-algebra embedding $L \hookrightarrow K_v$ and thus $A(K_v)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. By Corollary 23, $A(K_v)/nA(K_v)$ has a point of order n (in fact $2g$ points which are linearly independent over $\mathbb{Z}/n\mathbb{Z}$), so by Local Duality so does $H^1(K_v, A)$. This establishes part a).
Step 3: Suppose $\operatorname{char} K = p$ and $n = p^a$ for $a \geqslant 1$. In this case $A[p^a]$ is never étale and need not admit an étale subgroup scheme of exponent p^a: cf. Remark 30, so the argument of Step 2 breaks down. Fortunately it is not needed. Combining Corollary 23 with Local Duality yields the (stronger!) result in this case. □

5.2 A Local-Global Isomorphism in Weil-Châtelet Groups

Let K be a global field, $A_{/K}$ an abelian variety, and p be a prime number. Put

$$T_p \operatorname{Sel} A = \varprojlim_n \operatorname{Ker}\left(H^1(K, A[p^n]) \to \bigoplus_{v \in \Sigma_K} H^1(K_v, A) \right).$$

We need the following result of González-Avilés-Tan, a generalization of work of Cassels-Tate. In what follows, $A^\vee$ denotes the dual abelian variety of the abelian variety A, $G^\wedge$ denotes the pro-p-completion of the commutative group G, and G^* denotes the Pontrjagin dual of the commutative group G.

Theorem 25. *For $A_{/K}$ an abelian variety over a global field, and p any prime number – the case $p = \operatorname{char} K$ is allowed – we have an exact sequence*

$$0 \to T_p \operatorname{Sel} A^\vee \to \prod_{v \in \Sigma_K} (A^\vee(K_v))^\wedge \xrightarrow{\alpha} (H^1(K,A)[p^\infty])^* \to (Ш(K,A)[p^\infty])^* \to 0. \tag{10}$$

Using Tate-Milne Local Duality to identify $H^1(K_v, A)$ and $A^\vee(K_v)$ as Pontrjagin duals, the map α is the Pontrjagin dual of the natural map

$$H^1(K,A)[p^\infty] \to \bigoplus_{v \in \Sigma_K} H^1(K_v, A)[p^\infty].$$

Proof. This is the main result of [GAT07]. □

Corollary 26. *Let $A_{/K}$ be an abelian variety defined over a global field. If $A^\vee(K) = Ш(K,A) = 0$, then the local restriction maps induce an isomorphism of groups*

$$H^1(K,A) \xrightarrow{\sim} \bigoplus_{v \in \Sigma_K} H^1(K_v, A).$$

Proof. Since Weil-Châtelet groups are torsion, it is enough to restrict to p-primary components for all primes p. Since $Ш(K,A) = 0$, we also have $Ш(K,A^\vee) = 0$ [Mi, Theorem I.6.13 and Remark I.6.14(c)]. Since also $A^\vee(K) = 0$, we get $T_p \operatorname{Sel} A^\vee = 0$, and then (10) gives an isomorphism

$$\prod_{v \in \Sigma_K} (A^\vee(K_v))^\wedge \xrightarrow{\sim} \left(H^1(K,A)[p^\infty]\right)^*.$$

Taking Pontrjagin duals and applying Tate-Milne Local Duality, we get

$$H^1(K,A)[p^\infty] \xrightarrow{\sim} \bigoplus_{v \in \Sigma_K} H^1(K_v, A)[p^\infty].$$ □

Lemma 27. *Let $E_{/K}$ be an elliptic curve over a global field, and let $\eta \in H^1(K,E)$ be locally trivial at all places of Σ_K except (possibly) one. Then $P(\eta) = I(\eta)$.*

Proof. In the number field case this is [Cl05, Proposition 6]. Two proofs are given. The second proof works verbatim in the function field case. The first proof, which makes use of the period-index obstruction map Δ, works if one uses the extension of Δ given in [WCIV, §2.3]. □

5.3 Proof of Theorem 17

Let K be a global field, and let $E_{/K}$ be an elliptic curve with $E(K) = Ш(K,E) = 0$. Let $n > 1$; we must show that there is an infinite subset of $H^1(K,E)$ which is linearly independent over $\mathbb{Z}/n\mathbb{Z}$ consisting of classes with index n.

By Corollary 26 have an isomorphism

$$H^1(K,E) \xrightarrow{\sim} \bigoplus_{v \in \Sigma_K} H^1(K_v, E). \tag{11}$$

With all our preparations in hand, the proof is simple: for each of an infinite set $\mathcal{P}$ of finite places v of K, we find a class $\eta_v \in H^1(K_v, E)$ of period n, realize this class as an element of the right hand side of (11) supported at v, and pull back via the isomorphism to get a class η in $H^1(K,E)$. This class has period n, and since it is locally trivial except at v, by Lemma 27 it also has index n. Doing this for each $v \in \mathcal{S}$ we get a infinite subset $S \subset H^1(K,E)[n]$ which is linearly independent over $\mathbb{Z}/n\mathbb{Z}$ because each class lies in a different direct summand. We implement this in several steps, corresponding to the preliminary results we have established.

Step 1: Suppose $\operatorname{char} K \nmid n$. We apply Lemma 24a) to get our infinite set $\mathcal{P}$ of finite places of v and $\eta_v \in H^1(K_v,E)$ of order n. This completes the proof if $\operatorname{char} K = 0$.
Step 2: Suppose $\operatorname{char} K = p > 0$ and $n = p^a$. We apply Lemma 24b) and may take $\mathcal{P} = \Sigma_K$.
Step 3: Finally, suppose $\operatorname{char} K = p > 0$ and write $n = p^a m$ with $\gcd(m,p) = 1$. By Step 1, there is an infinite subset S_1 of $H^1(K,E)[m]$ linearly independent over $\mathbb{Z}/m\mathbb{Z}$ such that every $\eta_1 \in S_1$ has index m. By Step 2, there is an infinite subset S_2 of $H^1(K,E)[p^a]$ linearly independent over $\mathbb{Z}/p^a\mathbb{Z}$ such that every $\eta_2 \in S_2$ has index p^a. Using Lemma 1 we find (easily) that $S_1 + S_2$ is an infinite subset of $H^1(K,E)[n]$ linearly independent over $\mathbb{Z}/n\mathbb{Z}$ such that every $\eta \in S$ has index n.

6. The Proof of Theorem 18

Now we will prove Theorem 18: for every prime number p, the elliptic curve

$$E_{/\mathbb{F}_p(t)} : y^2 + txy + t^3y = x^3 + t^2x^2 + t^4x + t^5$$

has trivial Mordell-Weil and Shafarevich-Tate groups.

6.1 Controlling the torsion

We deal with the p-primary torsion and prime-to-p torsion in $E(\mathbb{F}_p(t))$ separately.

Lemma 28. *Let k be a field of characteristic $p > 0$, and $E_{/k}$ an elliptic curve. If $E(k)[p^\infty] \neq 0$, then $j(E) \in k^p$.*

Proof. Let $P \in E(k)$ be a point of order p. Let $E' = E/\langle P\rangle$ be the quotient of E by the cyclic group generated by P. We have a separable isogeny $\Phi : E \to E'$ with kernel $\langle P\rangle$ and of degree p. If $\Phi^\vee : E' \to E$ is its dual isogeny, we have a factorization of multiplication by p on E as

$$[p] : E \xrightarrow{\Phi} E' \xrightarrow{\Phi^\vee} E.$$

Since $[p] : E \to E$ is inseparable of degree p^2, we must have that $\Phi^\vee$ is inseparable of degree p. But an elliptic curve in characteristic p has a unique inseparable isogeny of degree p, namely the quotient by the kernel of Frobenius, so $\Phi^\vee$ must be the Frobenius map on E', and thus $E \cong (E')^{(p)}$ and $j(E) = j((E')^{(p)}) = (j(E'))^p \in k^p$. □

We get as an immediate consequence:

Corollary 29. *Let $E_{/\mathbb{F}_p(t)}$ an elliptic curve. If $j(E) \notin \mathbb{F}_p(t^p)$, then $E(\mathbb{F}_p(t))[p^\infty] = 0$.*

Remark 30. *In the setting of Corollary 29 we have that E is an ordinary elliptic curve which has no point of order p over the separable closure of $\mathbb{F}_p(t)$. This is a concrete instance of a phenomenon encountered in §3.2. In particular, it serves to clarify why assuming "A is ordinary" in Theorem 6 would not be enough (in order for our argument to succeed, at least).*

To control the prime-to-p torsion we use the following standard strategy: let $E_{/K}$ be an elliptic curve over a global field, let v be a finite place of K, and denote by K_v the corresponding completion. Since $E(K) \hookrightarrow E(K_v)$, it suffices to find a place for which $E(K_v)$ contains no prime-to-p torsion. For a group G, we denote by $G[p']$ its prime-to-p torsion subgroup. Much as above, we let R_v the valuation ring of K_v, $\mathfrak{m}_v$ the maximal ideal of R_v, and k_v its residue field, of characteristic p. We denote by $\tilde{E}_{/k_v}$ the reduction of E modulo $\mathfrak{m}_v$, $\tilde{E}_{\mathrm{ns}}(k_v)$ the set of nonsingular points of $\tilde{E}(k_v)$, $E_0(K_v)$ the set of points of $E(K_v)$ with nonsingular reduction, and $E_1(K_v)$ the kernel of the reduction map $E(K_v) \to \tilde{E}(k_v)$. We have a short exact sequence

$$0 \longrightarrow E_0(K_v) \longrightarrow E(K_v) \longrightarrow E(K_v)/E_0(K_v) \longrightarrow 0$$

The group $E(K_v)/E_0(K_v)$ is always finite, and its order is the number of reduced geometric components of the special fiber of a minimal regular model of E over R_v (see e.g. [AECII, Corollary IV.9.2(d)]). We see from [AECII, Table 4.1] that $E(K_v)/E_0(K_v)$ is the trivial group whenever the special fiber is of type II or II*, and in those cases we have $\tilde{E}_{\mathrm{ns}}(k_v) = k_v^+$. In this case, by [AECI, Proposition VII.2.1] we have a short exact sequence

$$0 \longrightarrow E_1(K_v) \longrightarrow E(K_v) \longrightarrow k_v^+ \longrightarrow 0$$

As recalled in §4.2.2, $E_1(K_v)$ is obtained from a formal group law, so contains no prime-to-p torsion. In particular, if $j(E) \notin (K_v)^p$, Lemma 28 and the above short exact sequence imply

$$E_1(K_v)[\mathrm{tors}] = E_1(K_v)[p^\infty] \subset E(K_v)[p^\infty] = 0.$$

In this case we have an injection

$$E(K_v)[\mathrm{tors}] = E(K_v)[p'] \hookrightarrow k_v^+.$$

Since k_v^+ is a p-group, we conclude that $E(K_v)[p'] = 0$.

We will see that for the elliptic curve in Theorem 18, there is always a place ν of $\mathbb{F}_p(t)$ for which the fiber of a minimal model for E at ν is of type II*.

6.2 Controlling the rank

Let k be a field, C a smooth projective curve over k, and $K = k(C)$ the function field of C. Let $E_{/K}$ be an elliptic curve, and consider $\pi : \mathcal{S} \to C$ its associated minimal elliptic surface. We will always assume that E is **nonisotrivial**, i.e., $j(E) \notin k$. By Lang-Néron, this implies that $E(K)$ is finitely generated. It implies also that $\Delta(E) \notin k$, so the morphism $\pi : \mathcal{S} \to C$ contains singular fibers, and that the **Néron-Severi group** $NS(\mathcal{S})$ is finitely genereated. The ranks of $E(K)$ and $NS(\mathcal{S})$ are related by the following result

Theorem 31 Shioda-Tate. *Let k be an algebraically closed field, let $E_{/k(C)}$ be an nonisotrivial elliptic curve, and let $\pi : \mathcal{S} \to C$ be its associated minimal elliptic surface. Let Σ denote the finite set of points $v \in C$ for which the fiber $\pi^{-1}(v)$ is singular. For each $v \in \Sigma$, let m_v denote the number of irreducible components of $\pi^{-1}(v)$. We have*

$$\mathrm{rank}(NS(\mathcal{S})) = \mathrm{rank}(E) + 2 + \sum_{v \in \Sigma} (m_v - 1).$$

Proof. See [Sh72, Corollary 1.5]. □

Now let $C = \mathbb{P}^1$, so $k(C) \cong k(t)$. Then $\mathcal{S} \to \mathbb{P}^1$ admits a Weierstrass equation

$$\mathcal{S} = \{([X : Y : Z], t) \in \mathbb{P}^2 \times \mathbb{P}^1 : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}$$

for some $a_i(t) \in k[t]$. We define the **height** of the Weierstrass elliptic surface to be the least $n \in \mathbb{N}$ such that $\deg(a_i) \leqslant ni$ for all i. The height controls the geometry of the total space $\mathcal{S}$.

If $E_{/k(t)}$ has height $n = 1$, the associated minimal elliptic surface $\mathcal{S}$ is isomorphic to $\mathbb{P}^2$ blown up at 9 points, so the rank of $NS(\mathcal{S})$ is 10. See [Sh90, Lemma 10.1] for a different computation of this. Therefore, the Shioda-Tate formula allows us to compute the rank of a height 1 elliptic curve $E_{/k(t)}$ from the local information of the singular fibers:

Corollary 32. *For a nonisotrivial elliptic curve $E_{/k(t)}$ of height 1, we have*

$$\operatorname{rank} E = 8 - \sum_{v\in\Sigma}(m_v - 1),$$

where Σ denotes the places of $k(t)$ where E has bad reduction.

Our strategy is to find an elliptic curve for which the contribution from the singular fibers is exactly 8, so $\operatorname{rank} E_{\overline{k}(t)} = 0$ and *a fortiori* $\operatorname{rank} E_{k(t)} = 0$. By Shioda-Tate, this occurs if there is a place v of bad reduction with $m_v = 9$. So we choose the Weierstrass equation in Theorem 18 so as to "force" Tate's algorithm to give us one fiber of reduction type II* (so $m_v = 9$).

6.3 Controlling Ш

In order to compute (the size of) the Shafarevich-Tate group of the elliptic curve in Theorem 1 we use some special features of elliptic curves of small height over function fields.

Theorem 33. *Let $E_{/\mathbb{F}_q(t)}$ be an elliptic curve of height $\leqslant 2$. Then E satisfies the Birch and Swinnerton-Dyer conjecture:*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(\mathbb{F}_q(t),E)\cdot R\cdot\tau}{(\#E(\mathbb{F}_q(t))[\text{tors}])^2}, \qquad (12)$$

where $r = \operatorname{rank}(E)$, τ is the product of the Tamagawa numbers, R is the regulator of E, and $L(E,s)$ is the L-function of E.

Proof. Write $K = \mathbb{F}_q(t)$. The main result of [KT03] (specialized to elliptic curves) states that (12) holds whenever $Ш(K,E)$ is finite (in fact, it suffices that $Ш(K,E)[l]$ is finite for some prime l). The finiteness of $Ш(K,E)$ is known for elliptic curves over K of height $\leqslant 2$. We refer the reader to [Ul11, Lectures 2,3] and the references therein for details. □

Therefore, we can compute the order of $Ш(\mathbb{F}_p(t),E)$ from the L-function of E, $E(\mathbb{F}_p(t))$ and data from Tate's algoriTheorem As we will see, the L-function of the elliptic curve (5) contributes trivially, by virtue of the following result.

Proposition 34 Grothendiek, Raynaud, Deligne. *Let $E_{/\mathbb{F}_q(t)}$ be a nonisotrivial elliptic curve. Then the L-function of E, $L(E,s)$, is a polynomial in $\mathbb{Z}[q^{-s}]$ with constant coefficient* 1 *and degree* $\deg(\mathfrak{n}) - 4$, *where $\mathfrak{n} = \mathfrak{n}(E)$ is the conductor of E.*

Proof. See e.g. [Gro11, Theorem 2.6]. □

6.4 Proof of Theorem 18

Now we will put together the pieces to show that the elliptic curve

$$E_{/\mathbb{F}_p(t)}: \quad y^2 + txy + t^3y = x^3 + t^2x^2 + t^4x + t^5$$

of Theorem 18 has $E(\mathbb{F}_p(t)) = Ш(\mathbb{F}_p(t),E) = 0$.

First, the discriminant and j-invariant of E are given by

$$\Delta(E) = -t^{10}(83t^2 - 199t + 432),$$

$$j(E) = -\frac{(47)^3 t^{12}}{\Delta} = \frac{(47)^3 t^2}{83t^2 - 199t + 432}$$

so we do indeed have an elliptic curve for all p. For $p \neq 47$, $j(E) \notin (\mathbb{F}_p(t))^p$, so by Lemma 28, $E(\mathbb{F}_p(t))$ has no p-primary torsion. We verify, using Tate's algorithm that E has reduction of type II* at (t), so in particular it has additive reduction with trivial component group, so by the results of §6.1, we conclude that $E(\mathbb{F}_p(t))[\mathrm{tors}] = 0$. For $p = 47$, $j(E) = 0$, so E is isotrivial and $j(E)$ is a pth power – so we verify using Magma that $E(\mathbb{F}_{47}(t)) = 0$.

To compute the rank of $E(\mathbb{F}_p(t))$ we examine the other singular fibers: for $p = 2$ and $p = 3$, we have $\Delta(E) = t^{11}(t+1)$, so E has bad reduction also at $(t+1)$. For $p > 3$ and $p \neq 83$, E has one or two more places of bad reduction, depending whether the quadratic $83t^2 - 199t + 432$ factors over $\mathbb{F}_p[t]$ into two (different) linear factors or not. Finally, for $p = 83$, E has bad reduction at $(t+2)$ and at the place at infinity $(1/t)$. In any case we verify, using Tate's algorithm, that E has reduction type II* at (t) and reduction type I1 and the other place(s), so Corollary 32 gives

$$\mathrm{rank}(E) = 8 - (9 - 1) = 0.$$

Thus $E(\mathbb{F}_p(t)) = 0$ for all primes p.

Now we compute the order of $Ш(\mathbb{F}_p(t), E)$: E has height 1, and since $E(\mathbb{F}_p(t)) = 0$ we have $r = 0$, $\#E(\mathbb{F}_p(t))[\mathrm{tors}] = 1$ and $R = 1$. Fibers of type II* and I1 have both Tamagawa number 1, so $\tau = 1$. Thus formula (12) reduces to $L(E, 1) = \#Ш(E)$, so we need to compute the L-function of E. Luckily for us, E has trivial L-function: The support of the conductor is given by the places of bad reduction of E, discussed in the previous paragraph, and we use Ogg-Saito formula to compute the exponent of the conductor at these places:

$$\mathfrak{n}(E) = \begin{cases} 3(t) + (t+1) & , p = 2, 3 \\ 2(t) + (\mathrm{Linear}_1) + (\mathrm{Linear}_2) \text{ or } 2(t) + (\mathrm{Quadratic}) & , p > 3, p \neq 83 \\ 2(t) + (t+2) + (1/t) & , p = 83 \end{cases}$$

In any case, $\deg(\mathfrak{n}) = 4$, so by Proposition 34 we have $L(E, s) = 1$. Thus $\#Ш(\mathbb{F}_p(t), E) = 1$ for all primes. This completes the proof of Theorem 18.

Remark 35. *When $p \neq 47$, our arguments show $E(\overline{\mathbb{F}_p}(t)) = 0$. However the case $p = 47$ is really exceptional: here $j(E) = 0$ so E is isotrivial. Since $47 \equiv -1 (mod\ 3)$, by Deuring's Criterion E is supersingular, so $E(\overline{\mathbb{F}_p(t)})[p] = 0$. We still have a fiber of type II*, so $E(\overline{\mathbb{F}_p}(t))[\mathrm{tors}] = 0$.*

7. The Proof of Theorem 19

7.1 Some preliminaries

Let $A_{/K}$ be an abelian variety. We want to give conditions on a field extension L/K for the group $\widetilde{H}^1(L/K, A)$ to be finite. We treat regular extensions first, then finite extensions.

Lemma 36. *Let L/K be a purely transcendental field extension.*
a) Let $V_{/K}$ be an algebraic variety. Suppose either *that K is infinite or V is complete. Then $V(L) \neq \varnothing \implies V(K) \neq \varnothing$.*
b) For every abelian variety $A_{/K}$, we have $\widetilde{H}^1(L/K, A) = 0$.

Proof. a) Step 1: Let $\{t_i\}_{i \in I}$ be a transcendence basis for L/K. If $P \in V(L)$, there is a finite subset $J \subset I$ such that $P \in V(K(\{t_i\}_{i \in J})$. So we may assume that L/K has finite transcendence

degree. Induction reduces us to the case $L = K(t)$.
Step 2: A point $P \in V(K(t))$ corresponds to a rational map $\varphi : \mathbb{P}^1 \to V$. The locus on which φ is not defined is a finite set of closed points of $\mathbb{P}^1$. If K is infinite, so is $\mathbb{P}^1(K)$, so there is $P \in \mathbb{P}^1(K)$ at which φ is defined, and then $\varphi(P) \in V(K)$. Moreover any rational map from a regular curve to a complete variety is a morphism, so if V is complete then e.g. $\varphi(0) \in V(K)$.
b) Since $\eta \in H^1(K, A)$ corresponds to a torsor V under A and thus a projective variety, this follows immediately from part a). □

Remark 37. *a) If in the statement of Lemma 36a) we strengthen "complete" to "projective", there is an easier proof: let $\varphi : V \to \mathbb{P}^N$ be a K-embedding. Since $K(t)$ is the fraction field of the UFD $K[t]$, if $P \in V(L)$, we can write $\varphi(P) = [f_0(t) : \ldots : f_N(t)]$ with $\gcd(f_0, \ldots, f_N) = 1$. In particular, some $f_i(t)$ is not divisible by t and thus $(f_0(0) : \ldots : f_N(0)) \in V(K)$.*
b) The affine curve $V = \mathbb{P}^1_{\mathbb{F}_q} \setminus \mathbb{P}^1(\mathbb{F}_q)$ has $K(t)$-rational points but no K-rational points.

Let K be a field, M a commutative $\mathfrak{g}_K$-module, $i \geqslant 1$, L/K a field extension, and consider the restriction map $\operatorname{Res}_L : H^i(K, M) \to H^i(L, M)$. For $\eta \in H^i(K, M)$ it is natural to compare both the period and index of η to the period and index of $\operatorname{Res}_L \eta$. Let us say that the extension L/K is **index-nonreducing** if $I(\operatorname{Res}_L \eta) = I(\eta)$ for all η and **period-nonreducing** if $P(\operatorname{Res}_L \eta) = P(\eta)$ for all η. It is then easy to see:

- If L/K is index-nonreducing, it is also period-nonreducing.
- L/K is period-nonreducing if and only if $\widetilde{H}^i(L/K, M) = 0$.

Thus Lemma 36 may be viewed as a result on period-nonreduction.

However an extension can be period-nonreducing but not index-nonreducing. In our context the difference is immaterial, because our inductive argument gives us classes with period equals index, but in general it would be more useful to have index-nonreduction results. So in the interest of completeness and applicability to future work we also include the following result.

Proposition 38. *Let $X_{/K}$ and $V_{/K}$ be regular, geometrically integral varieties with $X_{/K}$ complete.*[1] *Then:*
a) We have $I(V) \mid I(X)I(V_{/K(X)})$.
b) If $I(X) = 1$ – in particular if $X(K) \neq \varnothing$ – we have $I(V_{/K(X)}) = I(V)$.

Proof. a) It suffices to show the following: for every finite splitting extensions M of $V_{/K(X)}$, there is a K-rational zero-cycle on V of degree $[M : K(X)]I(X)$. Let L be the algebraic closure of K in M, so there is an L-variety $\tilde{X}$ and a dominant morphism $\pi : \tilde{X} \to X$ such that $L(\tilde{X}) = M$. By hypothesis, there is $P \in V(M)$, which corresponds to an L-rational map $\varphi : \tilde{X} \to V$. There is a nonempty Zariski-open subset $U \subset X$ such that: if $\tilde{U} = \pi^{-1}(U)$, then $\varphi|_{\tilde{U}} : \tilde{U} \to V$ is a morphism and $\pi|_{\tilde{U}} : \tilde{U} \to U$ is a finite morphism. By [Cl07, Lemma 12], there is a K-rational zero-cycle on U of degree $I(X)$. Then $\operatorname{Trace}_{L/K} \varphi_* \pi^* D$ is a divisor on V of degree

$$[M : L(X)] \cdot [L : K] \cdot I(X) = I(X)[M : L(X)][L(X) : K(X)] = [M : K(X)]I(X).$$

b) If $I(X) = 1$, then by part a) we have $I(V) \mid I(V_{/K(X)})$. Since for any extension L/K we have $I(V_{/L}) \mid I(V)$, we conclude $I(V_{/K(X)}) = I(V)$. □

Let L/K be a finite extension. Obviously $\widetilde{H}^1(L/K, A)$ can be nontrivial. We give a sufficient condition for it to be finite.

[1] It is enough to assume that X admits a resolution of singularities.

Lemma 39. *Let K be a Weak-Mordell-Weil field, L/K be a finite separable field extension, and $A_{/K}$ an abelian variety. Then $\widetilde{H}^1(L/K,A)$ is finite.*

Proof. Let M be the Galois closure of L/K. Since $\widetilde{H}^1(L/K,A) \subset \widetilde{H}^1(M/K,A)$, we may replace L with M and thus assume that L/K is finite Galois, say of degree n. Because the period divides the index, we have $\widetilde{H}^1(L/K,A) = \widetilde{H}^1(L/K,A)[n]$. The short exact sequence of K-group schemes

$$0 \to A[n] \to A \overset{[n]}{\to} A \to 0$$

may be viewed as a short exact sequence of sheaves on the flat site of $\operatorname{Spec} K$, so we may take cohomology, getting the **flat Kummer sequence**

$$0 \to A(K)/nA(K) \to H^1(K,A[n]) \to H^1(K,A)[n] \to 0. \tag{13}$$

(The finite flat group scheme $A[n]$ is étale iff $\operatorname{char} K \nmid n$; in this case the Kummer sequence can be more simply viewed as a sequence of étale = Galois cohomology groups. But in our application we need the general case.) There is also a Kummer sequence associated to multiplication by n on $A_{/L}$. Restriction from K to L gives a commutative ladder

$$\begin{tikzcd}
0 \arrow[r] & A(K)/nA(K) \arrow[r] \arrow[d] & H^1(K,A[n]) \arrow[r] \arrow[d] & H^1(K,A)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A(L)/nA(L) \arrow[r] & H^1(L,A[n]) \arrow[r] & H^1(L,A)[n] \arrow[r] & 0
\end{tikzcd} \tag{14}$$

Let $\mathcal{K}$ and $\mathcal{C}$ be the kernel and cokernel of the restriction map $A(K)/nA(K) \to A(L)/nA(L)$. The Snake Lemma gives an exact sequence

$$0 \to \widetilde{H}^1(L/K,A[n])/\mathcal{K} \to \widetilde{H}^1(L/K,A) \to \mathcal{C},$$

so to show that $\widetilde{H}^1(L/K,A)$ is finite it is sufficient to show that $\mathcal{C}$ and $\widetilde{H}^1(L/K,A[n])$ are both finite. The group $A(L)/nA(L)$ is finite because K (hence L, by Proposiotion 4) is Weak-Mordell-Weil, so its quotient $\mathcal{C}$ is also finite. Finally, because L/K is Galois, by [W, Theorem, §17.7] we have $\widetilde{H}^1(L/K,A[n]) = H^1(\operatorname{Aut}(L/K),A[n](L))$. The right hand side of the last equation is the cohomology of a finite group with coefficients in a finite module, so it is a quotient of a finite group of cochains and thus is certainly finite. □

Example 40. *Let $K = \mathbb{F}_p((t))$, and $K_n = K^{p^{-n}}$, so $[K_n : K] = p^n$. Let $E_{/K}$ be a supersingular elliptic curve. We will show that $H^1(K_2/K,E)$ is infinite.*
Step 1: We claim $H^1(K,E)[p] \subset \widetilde{H}^1(K_2/K,E)$. Indeed, let $\eta \in H^1(K,E)[p]$, and using (13) let ξ be a lift of η to $H^1(K,E[p])$. Since $E[p]$ is a finite connected group scheme of Frobenius height 2, by [Sh, Proposition 76] we have $\widetilde{H}^1(K_2/K,E[p]) = H^1(K,E[p])$. Thus $\xi|_{K_2} = 0$, and using (14) we deduce $\eta|_{K_2} = 0$.
Step 2: By Theorem 21b), $E(K)/pE(K)$ is infinite. By the Local Duality Theorem, $H^1(K,E)[p]$ is infinite. Thus $\widetilde{H}^1(K_2/K,E) \supset H^1(K,E)[p]$ is infinite.
Similarly, if $A_{/K}$ is any nontrivial abelian variety with $A[p](\overline{K}) = 0$, then if n is the Frobenius height of $A[p]$ we have that $\widetilde{H}^1(K_n/K,A)$ is infinite.

Remark 41. *In Lemma 39 we assumed that K is Weak-Mordell-Weil and L/K is separable. In Example 40 neither of these hypotheses holds. It would be interesting to know whether either of the hypotheses of Lemma 39 can be individually removed.*

7.2 Proof of Theorem 19

Let $t_1, \ldots, t_d$ be a separating transcendence basis for L/K and put $K' = K(t_1, \ldots, t_d)$. By Lemma 36, $\widetilde{H}^1(K'/K, A) = 0$, so by Lemma 14a), $\operatorname{Res}_{K'} S \subset H^1(K', A)[n]$ is infinite and 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. Moreover, since K is Weak-Mordell-Weil, by Proposition 4 so is K'. Thus we may as well assume that $K' = K$ and L/K is a finite separable. By Lemma 39, $\widetilde{H}^1(L/K, A)$ is finite. By Lemma 14b), there is $S' \subset S$ such that $\operatorname{Res}_L S' \subset H^1(L, A)[n]$ is infinite and 1-linearly independent over $\mathbb{Z}/n\mathbb{Z}$, and the latter condition means that every element of $\operatorname{Res}_L S'$ has period n. Finally, we suppose that every element of S has index n. Then on the one hand every element of $\operatorname{Res}_L S'$ has index dividing n, whereas on the other hand every element of $\operatorname{Res}_L S'$ has period dividing its index, hence every element of $\operatorname{Res}_L S'$ has index n.

References

AECI J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, 1986.

AECII J. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

Ca61 J.W.S. Cassels. *Arithmetic on a curve of genus one. (V) Two counterexamples*, J. London Math. Soc. 36 (1961), 177–184.

CL J.-P. Serre. *Corps locaux.* Deuxi‘eme édition. Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968.

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

Cl05 P.L. Clark, *There are genus one curves of every index over every number field.* J. Reine Angew. Math. 594 (2006), 201-206.

Cl07 P.L. Clark, *On the indices of curves over local fields.* Manuscripta Math. 124 (2007), 411-426.

Co06 B. Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem.* Enseign. Math. (2) 52 (2006), 37-108.

FJ M.D. Fried and M. Jarden, *Field arithmetic.* Third edition. Revised by Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Springer-Verlag, Berlin, 2008.

GAT07 C.D. González-Avilés and K.-S. Tan, *A generalization of the Cassels-Tate dual exact sequence.* Math. Res. Lett. 14 (2007), 295-302.

GLL13 O. Gabber, Q. Liu and D. Lorenzini, *The index of an algebraic variety.* Invent. Math. 192 (2013) 567-626.

Gro11 B. H. Gross, *Lectures on the conjecture of Birch and Swinnerton-Dyer.* Arithmetic of L-functions, 169209, IAS/Park City Math. Ser., 18, Amer. Math. Soc., Providence, RI, 2011

Ik60 M. Ikeda, *Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren.* Abh. Math. Sem. Univ. Hamburg 24 (1960), 126-131.

KT03 K. Kato and Fabien Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic* $p > 0$, Invent. Math. 153 (2003), no. 3, 537592.

Ko89 V. Kolyvagin. *On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Math. USSR-Izv. 33 (1989), 473–499.

La56 S. Lang, *Algebraic groups over finite fields.* Amer. J. Math. 78 (1956), 555-563.

LALG J.-P. Serre. *Lie algebras and Lie groups*, Lecture Notes in Mathematics, 1500, Springer-Verlag, 1992.

LN59 S. Lang and A. Néron, *Rational points of abelian varieties over function fields.* Amer. J. Math. 81 (1959), 95-118.

LT58 S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties.* Amer. J. Math. 80 (1958), 659-684.

Ma H. Matsumura, *Commutative ring theory.* Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

Mi J. Milne. *Arithmetic Duality Theorems*, Perspectives in Mathematics, 1. Academic Press Inc., 1986.

Mi70 J. Milne, *Weil-Châtelet groups over local fields.* Ann. Sci. École Norm. Sup. (4) 3 (1970), 273-284.

Ol70 L.D. Olson, *Galois cohomology of cycles and applications to elliptic curves.* Amer. J. Math. 92 (1970), 75-85.

Sc W.R. Scott, *Group Theory.* Second edition. Dover Publications, Inc., New York, 1987.

Sh S.S. Shatz, *Profinite groups, arithmetic, and geometry.* Annals of Mathematics Studies, No. 67. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972.

Sh72 T. Shioda, *On elliptic modular surfaces.* J. Math. Soc. Japan 24 (1972), 20-59.

Sh90 T. Shioda, *On the Mordell-Weil lattices.* Comment. Math. Univ. St. Paul. 39 (1990), no. 2, 211-240.

Sh12 S. Sharif, *Period and index of genus one curves over global fields.* Math. Ann. 354 (2012), 1029-1047.

Ш57 I.R. Shafarevich, *Exponents of elliptic curves.* Dokl. Akad. Nauk SSSR (N.S.) 114 (1957), 714-716.

St02 W.A. Stein, *There are genus one curves over $\mathbb{Q}$ of every odd index.* J. Reine Angew. Math. 547 (2002), 139-147.

Ta57 J. Tate. *WC-groups over p-adic fields*, Sem. Bourbaki, Exp. 156, 1957.

Ul11 D. Ulmer, *Elliptic curves over function fields.* Arithmetic of L-functions, 211-280, IAS/Park City Math. Ser., 18, Amer. Math. Soc., Providence, RI, 2011.

W W.C. Waterhouse, *Introduction to affine group schemes.* Graduate Texts in Mathematics, 66. Springer-Verlag, New York-Berlin, 1979.

WCI P.L. Clark, *Period-index problems in WC-groups I: elliptic curves*, J. Number Th. 114 (2005), 193-208.

WCII P.L. Clark, *Period-index problems in WC-groups II: abelian varieties.* Preprint.

WCIV P.L. Clark, *The period-index problem in WC-groups IV: a local transition theorem.* J. Théor. Nombres Bordeaux 22 (2010), 583-606.

Wi S. Willard, *General topology.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1970.

Pete L. Clark plclark@gmail.com
Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602-7403, USA

Allan Lacy alacy@math.uga.edu
Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602-7403, USA