On the index of genus one curves

by

Allan Lacy Mora

(Under the Direction of Pete L. Clark)

Abstract

The central focus of this thesis is on the index of genus one curves. We prove existence of such curves with prescribed index over fields finitely generated over $\mathbb{F}_p(t)$. The proof is by induction on the transcendence degree. This generalizes – and uses as the base case of an inductive argument – an older result on the number field case. There is a separate base case in every positive characteristic p, and these use work on the conjecture of Birch and Swinnerton-Dyer over function fields.

Index words: Galois cohomology, abelian variety, elliptic curve, torsor, index, period.

On the index of genus one curves

by

Allan Lacy Mora

B.S., University of Costa Rica, 2005

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2015

On the index of genus one curves

by

Allan Lacy Mora

Approved:

Professor:	Pete L. Clark
Committee:	Daniel Krashen
	Paul Pollack
	Robert Varley

Electronic Version Approved:

Suzanne Barbour

Dean of the Graduate School

The University of Georgia

August 2015

On the index of genus one curves

Allan Lacy Mora

July 23, 2015

Acknowledgments

I would like to express my gratitude to my advisor, Pete Clark, for his expert guidance and help during my years at UGA. His passion for mathematics is certainly a motivation.

I want to thank to the math department staff, specially to Laura Ackerley, who helped me get through all the endless paperwork (on time!).

I want to express my gratitude to my Alma Mater, Universidad de Costa Rica, for its economical support during my years of study at UGA.

To my Athens friends, who made this town a home for 6 years. Specially Alicia, Beto, Jena and Ivan. To all the members of the Anoush's Barcelona FC.

Finally, I want to thank my friend and colleague (and ex-roomate), David Krumm. At some point in 2001 he made me take the decision that had brought me to this point.

Gracias totales!

Contents

List of Tables

CHAPTER 1

Introduction

The main result of this thesis is about the existence of genus one curves with prescribed index over fields finitely generated over $\mathbb{F}_p(t)$. We would like to introduce and motivate these concepts by looking at a couple of examples, over the more familiar field $\mathbb{Q}$:

Example 1.0.1. Consider the plane cubic

$$C : 3x^3 + 4y^3 + 5z^3 = 0.$$

It is a very well known fact, going back to Selmer [Sel51] that C does not have points over $\mathbb{Q}$ (although it has points over every completion of $\mathbb{Q}$). Clearly C has points defined over *cubic* extensions of $\mathbb{Q}$: for example, by letting $y_0 = -1$, $z_0 = -1$ we find, solving for x, that if $x_0 = \sqrt[3]{3}$ then the point (x_0, y_0, z_0) is in $C(\mathbb{Q}(x_0))$. Of course, any finite extension $L/\mathbb{Q}(x_0)$ will also have the property that $C(L) \neq \emptyset$, so we can produce infinitely many examples of extensions $L/\mathbb{Q}$ such that $C(L) \neq \emptyset$, all of which will have $3 \mid [L : \mathbb{Q}]$. Making different choices of pairs $y_0, z_0 \in \mathbb{Q}$ will produce infinitely many other examples of (*a priori*) cubic extensions. A natural question arises at this point is: can we do better; that is, can we find a *quadratic* extension $L/\mathbb{Q}$ such that $C(L) \neq \emptyset$?

In general, given an algebraic curve C defined over a field K, one can ask what is the

smallest degree of a finite field extension L/K such that C has a point defined over L. This number is called the *index* of C, and measures in some way the failure of C of having a K-rational point, as clearly, a curve $C_{/K}$ has index 1 if and only if has a K-rational point. The example above is of a curve of index 3 over $\mathbb{Q}$. The next one, which is due to Cassels, is a curve of index 4 over $\mathbb{Q}$.

Example 1.0.2. Consider the following curve $\mathcal{D}$, which is the intersection of two quadrics in $\mathbb{P}^3$,

$$\mathcal{D} : \begin{cases} 3x^2 = -11y^2 - t^2, \\ -33z^2 = -11y^2 + t^2 \end{cases}$$

It is not hard to prove that $\mathcal{D}$ does not have points defined over $\mathbb{Q}$. We can easily find some *quartic* points on $\mathcal{D}$, for example $(x_0, y_0, z_0, t_0) = (\sqrt{-11}, \sqrt{3}, 1, 0)$ is a point defined over the quartic number field $\mathbb{Q}(\sqrt{3}, \sqrt{-11})$. Cassels [Cas63] showed that in fact $\mathcal{D}$ has index 4.

E. Artin conjectured, and Lang and Tate proved [LT58, Proposition 7] that for every integer r there exist infinitely many genus one curves of with index r, defined over *some* (!) field. In particular, their methods left the question open over fields of arithmetic interest, such as number fields or function fields. And it remained open for almost 50 years! Clark [Cla06] proved that there exist genus one curves of any prescribed index over *any* number field. The proof required to find certain elliptic curve $E_{/\mathbb{Q}}$ with certain desirable properties (see §3.2 for more details).

One of the main goals in this thesis is to consider the existence of genus one curves over fields which are finitely generated over $\mathbb{F}_p(t)$. In Chapter 2, working towards a generalization of the proof given in [Cla06], we provide an example of a elliptic curve E defined over $\mathbb{F}_p(t)$ for each prime number p, with these "desirable" properties. Specifically the elliptic curve has trivial Mordell-Weil and Tate-Shafarevich groups.

The result from Chapter 2 should be considered as a "base case" of an inductive argument.

In Chapter 3 we consider the "inductive step" of this induction, namely, we prove that if $K/\mathbb{F}_p(t)$ is a finitely generated field extension, then there are infinitely many genus one curves of any prescribed index over K.

The results of Chapters 2 and 3 are contained in a forthcoming paper [CL], written jointly with Clark. In that paper we prove that there are genus one curves of any prescribed index over any infinite, finitely generated field. Besides expanding on the background material, we present here an independent exposition, focusing on the positive characteristic case.

CHAPTER 2

The Mordell-Weil and Tate-Shafarevich groups of certain elliptic curves over $\mathbb{F}_p(t)$

2.1 Introduction

In this chapter we will prove the following result:

Theorem 2.1.1. *For every prime number p, the elliptic curve*

$$E : y^2 + txy + t^3y = x^3 + t^2x^2 + t^4x + t^5$$

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

As discussed in the introduction, the motivation to prove such a result comes the following result in [Cla06].

Theorem. *Let K be a number field and $E_{/K}$ an elliptic curve with $E(K) = 0$ and $Ш(K, E) = 0$. Then for every number field L/K and every positive integer n, there are infinitely many genus one curves defined over L of index n.*

Taking $L = K = \mathbb{Q}$ in the previous statement provides a positive answer to an old question of Lang and Tate [LT58], where they were able to prove the existence of genus

one curves with prescribed index, but where the ground field cannot be fixed in advanced. *Luckily*, there are examples of elliptic curves over $\mathbb{Q}$ that satisfy the hypotheses of this theorem, so Clark concludes

Corollary. *There are genus one curves of any prescribed index over any number field.*

Aiming to extend the result of Clark to the function field case, Theorem 2.1.1 provides, for every prime p, an example of an elliptic curve E over each "base field" $K = \mathbb{F}_p(t)$ satisfying these same hypotheses: $E(K) = Ш(K, E) = 0$. In Chapter 3, we prove that under these hypotheses, the analogue of Clark's result holds, and then, by an inductive argument, we give a positive answer to Lang and Tate question for function fields:

Corollary (Corollary 3.6.2)**.** *There are genus one curves of any prescribed index over any field finitely generated over* $\mathbb{F}_p(t)$.

The organization of the chapter is as follows: in §2.2 we review some background material necessary to compute the Mordell-Weil and Tate-Shafarevich group of an elliptic curve over a global field. Then in §2.3 putting together these results (some of which are available only in the function field case) we give the proof of Theorem 2.1.1.

2.2 Preliminaries

2.2.1 Tate's Algorithm

Let K be a field which is complete with respect to a discrete valuation v, and let $\mathcal{O}_v$ the valuation ring and k_v be the residue field of K. Let $E_{/K}$ be an elliptic curve given by a $\mathcal{O}_v$-integral minimal Weierstrass equation. This equation defines a scheme of $\operatorname{Spec} \mathcal{O}_v$, which if E has bad reduction at v, might not be regular. By blowing up the singularity, one gets a regular scheme $\mathcal{C}_{/\operatorname{Spec} \mathcal{O}_v}$, whose generic fiber, $\mathcal{C} \times \operatorname{Spec}(K)$ is $E_{/K}$, and whose special fiber, $\mathcal{C} \times \operatorname{Spec}(k_v)$ is a union of curves (not necessarily reduced) over k_v.

Kodaira and Néron [Nér64, §17], when the residue field is perfect and not of characteristic 2 or 3, classified the possible geometries of the special fiber of these regular schemes according to the number of reduced geometric components and the multiplicities of each component. There are only a finite number of possible configurations, which are called the *Kodaira types*, and they are assigned one of the following *Kodaira symbols*: I_0, I_n ($n \geq 1$), II, III, IV, I_0^*, I_n^* ($n \geq 1$), IV^*, III^* and II^*. Note that the symbols I_n and I_n^* correspond to a family of reduction types.

Tate [Tat75], under the same restrictions on the residue field, carrying out explicitly the necessary blow ups to resolve the singularities, has given a procedure to determine the Kodaira type of the special at a place of bad reduction. When the residue characteristic is not 2 nor 3, and the Weierstrass equation is minimal, the Kodaira symbol can be read off from Table 2.1 (taken from [Szy04, Table 1]). If the Weierstrass equation is not minimal at v, Tate's algorithm also carry out the necessary changes of coordinates to reduce the valuation of the discriminant, and computes a minimal model.

Table 2.1: Kodaira types for Tate's algorithm ($\mathrm{char}\, k_v \neq 2, 3$)

	I_0	I_n	II	III	IV	I_0^*	I_n^*	IV^*	III^*	II^*
a_1		0^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+	1^+
a_2		0^+	1^+	1^+	1^+	1^+	1	2^+	2^+	2^+
a_3		1^+	1^+	1^+	1^+	2^+	2^+	2^+	3^+	3^+
a_4		1^+	1^+	1	2^+	2^+	3^+	3^+	3	4^+
a_6		1^+	1	2^+	2^+	3^+	4^+	4^+	5^+	5
b_2		0					1			
b_4				1					3	
b_6			1		2			4		5
c_4		0		1		2			3	
c_6			1		2	3		4		5
Δ	0	n	2	3	4	6	$6+n$	8	9	10

The entries of the columns 2-10 correspond to the valuations of the entries in the first column, where the a_i's, b_i's and c_i's correspond to the usual quantities associated to a

Weiertrass equation [Sil09, p. 42]. The expression $v(x) = a^+$ means $v(x) \geq a$. An empty entry means that the valuation is arbitrary. So for example, in column 2 we see that the only restriction for reduction type I_0 (good reduction) is for the discriminant to be a unit in $\mathcal{O}_v$.

The Magma command LocalInformation returns (among other things) the Kodaira symbol at the places of bad reduction. We make use this function for residue characteristic $p = 2, 3$, as Table 2.1 does not determine the reduction type in these cases. In [Szy04] there are similar tables that work in characteristic 2 and 3.

In the following example we explain how Table 2.1 can be used to determine the Kodaira symbols.

Example 2.2.1. Let $p \geq 5$, and consider the elliptic

$$E' \,:\, y^2 + txy + ty = x^3 + tx^2 + tx + t$$

over $\mathbb{F}_p(t)$. One computes

$$\Delta(E') = -t^2(t^5 + 10t^4 - 2t^3 - 117t^2 - 8t + 432) \text{ and } j(E') = \frac{t^3(t^3 + 8t^2 - 8t - 48)^3}{\Delta}$$

So E' has bad reduction at (t), $(1/t)$ and the divisors of $t^5 + 10t^4 - 2t^3 - 117t^2 - 8t + 432$. Notice that the valuation of the discriminant at these places is respectively 2, 5 and ≤ 5, so the Weierstrass equation is minimal at the places of bad reduction.

From Table 2.1 it is clear that E' has reduction type II at (t), since that is the only column of the table with $v(a_6) = 1$ and $v(\Delta) = 2$. At the place at infinity, the valuation of the j-invariant is negative, so the reduction at this place is multiplicative and we conclude that it has reduction type I_5 at this place. Notice that reduction type I_5 is also the only possibility with $v(\Delta) = 5$. Finally, the reduction type at the divisors of $(t^5 + 10t^4 - 2t^3 -$

$117t^2 - 8t + 432$) depends on the multiplicity of each divisor, which generically is of type I_1. The only exceptions to this *generic case* occur for $p = 157$ (with reduction type II at $(t+6)$) and $p = 2297$ (with reduction type I_2 at $(t + 1008)$).

2.2.2 The torsion subgroup of elliptic curves over global fields

We consider the p-primary and prime-to-p torsion subgroups separately. In general, for a group G and a integer m we denote by $G[m^\infty]$ and $G[m']$ the m-primary and prime-to-m torsion subgroups of G, respectively.

To control the p-primary subgroup of an elliptic curve over a field of characteristic p, we use the following result.

Lemma 2.2.2. *Let K be a field of characteristic $p > 0$, and let $E_{/K}$ be an elliptic curve. If $E(K)[p^\infty] \neq 0$, then $j(E) \in K^p$.*

Proof. If $P \in E(K)$ is a point of order p^a, then $p^{a-1}P$ has order p, so it suffices to consider the case $a = 1$. 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 $\hat{\Phi} : E' \to E$ is its dual isogeny, we have a factorization of multiplication by p on E as

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

Since $[p] : E \to E$ is inseparable of degree p^2, we must have that $\hat{\Phi}$ 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 $\hat{\Phi}$ 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 2.2.3. *Let E be an elliptic curve over $\mathbb{F}_p(t)$. If $j(E) \notin \mathbb{F}_p(t^p)$, then $E(\mathbb{F}_p(t))[p^\infty] = 0$.*

Proof. As $\mathbb{F}_p(t)^p = \mathbb{F}_p(t^p)$, it follows from Lemma 2.2.2 that $E(\mathbb{F}_p)[p^\infty] = 0$. □

Now we describe how to control the prime-to-p subgroup of an elliptic curve over a global field, not necessarily of the form $\mathbb{F}_p(t)$. We recall a standard technique -as described in [Sil94, Remark 9.2.2], for example- to bound the torsion subgroup of an elliptic curve defined over a global field.

Let K be a global field, v a finite place of K, K_v be the completion of K at v and $E_{/K}$ an elliptic curve over K. Since $E(K)[p'] \hookrightarrow E(K_v)[p']$, it suffices to find a place for which $E(K_v)[p'] = 0$.

We introduce some more notation: let R_v the valuation ring of K_v, $\mathfrak{m}_v$ the maximal ideal of R_v, and $k_v = R_v/\mathfrak{m}_v$ the residue field, a field of positive characteristic, lets say p. If $E_{/K_v}$ is given by a R_v-integral model, we denote by $\widetilde{E}$ the reduction of E modulo the maximal ideal $\mathfrak{m}_v$, which is a curve (possibly singular) defined over k_v. Let $\widetilde{E}_{\mathrm{ns}}(k_v)$ be the set of nonsingular points of $\widetilde{E}(k_v)$, $E_0(K_v)$ the set of points of $E(K_v)$ with nonsingular reduction, and $E_1(K_v)$ the kernel of the reduction map $E(K_v) \to \widetilde{E}(k_v)$. The quotient $E(K_v)/E_0(K_v)$ 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. [Sil94, Corollary IV.9.2(d)]). In particular, this quotient is trivial whenever E has good reduction (trivially), or when E has additive reduction with Kodaira symbol II or II* at v ([Sil94, Table 4.1]).

Suppose that E has additive reduction II or II*, so $\widetilde{E}_{\mathrm{ns}}(k_v) = \mathbb{G}_a(k_v)$, the additive group of k_v. In this case [Sil09, Proposition VII.2.1] gives a short exact sequence

$$0 \longrightarrow E_1(K_v) \longrightarrow E(K_v) \longrightarrow \mathbb{G}_a(k_v) \longrightarrow 0$$

The subgroup $E_1(K_v)$ contains no prime-to-p torsion, as it is obtained from a formal group

law [Sil09, Proposition VII.3.1(a)]. Finally, if we assume further that $E(K_v)[p^\infty] = 0$ (by Lemma 2.2.2 this is a very mild assumption), the above short exact sequence implies

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

And we have an injection

$$E(K_v)[\text{tors}] = E(K_v)[p'] \hookrightarrow \mathbb{G}_a(k_v)$$

Since $\mathbb{G}_a(k_v)$ is a p-group, we conclude that $E(K_v)[p'] = 0$.

Summarizing:

Proposition 2.2.4. *Let $E_{/K}$ be an elliptic curve over a global field. Let v be a place of K such that E has additive reduction with Kodaira symbol* II *or* II* *at v. If the residue field at v has characteristic p, and $E(K)[p^\infty] = 0$, then $E(K)[\text{tors}] = 0$.*

2.2.3 The Shioda-Tate formula

We want to review some basic ideas on the theory of *elliptic surfaces*. Our specific goal is the *Shioda-Tate formula* (2.2.5) below, which will allow us to compute the rank of the elliptic curve in Theorem 2.1.1.

Let k be a field, and put $K = k(t)$. Let $E_{/K}$ be an elliptic curve, and consider $\pi : \mathcal{E} \to C$ its associated minimal elliptic surface ([Sil94, Proposition III.3.8]). We will always assume that E is **nonisotrivial** (that is $j(E) \notin k$), so $\mathcal{E}$ is nonsplit ([Sil94, Proposition III.5.1]). Under this assumption, it follows by the Lang-Néron theorem, that the group $E(K)$ is finitely generated ([Sil94, Theorem III.6.1]). The group $E(K)$ is canonically identified with the group of sections of $\mathcal{E}$ over C, $\mathcal{E}(C)$ ([Sil94, Proposition III.3.10(c)]), so it follows that the *Néron-Severi group* $\text{NS}(\mathcal{E})$ is finitely generated ([Shi72, Theorem 1.1]).

We have then that if $j(E) \notin k$, the groups $E(K)$ and $\mathrm{NS}(\mathcal{E})$ are finitely generated, and their ranks are related by the following result

Theorem 2.2.5 (Shioda-Tate)**.** *Let k be an algebraically closed field, let $E_{/k(C)}$ be a non-isotrivial elliptic curve, and let $\pi : \mathcal{E} \to C$ 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*

$$\mathrm{rank}(\mathrm{NS}(\mathcal{E})) = \mathrm{rank}(E) + 2 + \sum_{v \in \Sigma} (m_v - 1). \tag{2.1}$$

Proof. See [Shi72, Corollary 1.5]. □

Now let $C = \mathbb{P}^1$, so $k(C) \cong k(t)$, and let $E_{/K}$ be an elliptic curve. In this case $\pi : \mathcal{E} \to \mathbb{P}^1$ admits a Weierstrass equation

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

for some $a_i(t) \in k[t]$, where π is projection onto the second factor. We define the **height** of the Weierstrass elliptic surface to be the least $h \in \mathbb{N}$ such that $\deg(a_i) \leq hi$ for all i. The integer h controls the geometry of the total space $\mathcal{E}$. In particular, for small heights we have ([SS10, §4.10]):

- $h = 0$: E is constant, and $\mathcal{E}$ is a product of curves.
- $h = 1$: $\mathcal{E}$ is a rational elliptic surface.
- $h = 2$: $\mathcal{E}$ is a $K3$ surface.

When $E_{/k(t)}$ has height $h = 1$, we have that the rank of $\mathrm{NS}(\mathcal{E})$ is 10 ([Shi90, Lemma 10.1] or [SS10, Proposition 8.1]). Therefore, the Shioda-Tate formula (2.1) allows us to compute

the rank of a height 1 elliptic curve $E_{/k(t)}$ from the local information of the singular fibers.

Corollary 2.2.6. *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.

2.2.4 The Birch and Swinnerton-Dyer Conjecture

Let K be a global field, and let $E_{/K}$ be an elliptic curve. The *Tate-Shafarevich group* of $E_{/K}$ is defined as[1]

$$Ш(K, E) := \ker \left(H^1(K, E) \to \prod_v H^1(K_v, E) \right) \tag{2.2}$$

where v runs over all places of K.

Conjecture 2.2.7 (Tate-Shafarevich conjecture)**.** *The group $Ш(K, E)$ is finite.*

Remark 2.2.8. It was not until the late 1980's, after work of Rubin [Rub87] and Kolyvagin [Kol88], that the first examples of elliptic curves over number fields with finite Ш were given. Even to date the finiteness of Ш for arbitrary elliptic curves over $\mathbb{Q}$ is only known if the curve has *analytic rank* 0 or 1, by work of V.A. Kolyvagin [Kol91]. As we will see shortly, much more is known in the case of elliptic curves over function fields in one variable over a finite field.

Let v a place of K. Choose a *minimal integral* model for E at v. We denote by E_v the reduction of E modulo v. This is a possibly singular curve defined over the residue field k_v, a finite field. Let $q_v = \#k_v$. We define an integer a_v depending on the geometry of the reduced curve:

[1] We refer the reader to §3.3.2 for the definition of the Galois cohomology groups $H^1(-, E)$

Definition 2.2.9. For each place v of K we define an integer a_v by

$$a_v = \begin{cases} q_v + 1 - \#E_v(k_v) & \text{, if } E \text{ has good reduction at } v, \\ 1 & \text{if } E \text{ has split multiplicative reduction at } v, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } v, \\ 0 & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

We have

Lemma 2.2.10 (Hasse bound)**.**

$$|a_v| \leq 2\sqrt{q_v} \tag{2.3}$$

Proof. See [Sil09, Theorem V.1.1] for example. □

Definition 2.2.11. For each place v of K, we define the *local L-series of E at v* by

$$L_v(E_{/K}, T) = \begin{cases} 1 - a_v T + q_v T^2 & \text{if } E \text{ has good reduction at } v, \\ 1 - a_v T & \text{if } E \text{ has bad reduction at } v. \end{cases}$$

and we define the (global) *L-series of $E_{/K}$* by the Euler product

$$L(E_{/K}, s) = \prod_{v \in \Sigma_K} L_v(E_{/K}, q_v^{-s})^{-1} \tag{2.4}$$

where s is a complex variable.

Using the Hasse bounds (2.3) it can easily be seen that the product defining $L(E, s)$ converges uniformly in the region $\Re es > 3/2$. Hasse conjectured that $L(E_{/\mathbb{Q}}, s)$ has an analytic continuation to all of $\mathbb{C}$, and Birch and Swinnerton-Dyer [BSD65] assuming this was the case, stated their famous conjecture (over $\mathbb{Q}$)

Conjecture 2.2.12 (BSD)**.** *Assume that the L-function of $E_{/K}$ has an analytic continuation*

to $\mathbb{C}$. *Then*

$$\operatorname{rank} E(K) = \operatorname{ord}_{s=1} L(E_{/K}, s). \tag{2.5}$$

Remark 2.2.13. Hasse's conjecture (over $\mathbb{Q}$) is known to be true by work of Wiles [Wil95], Breuil, Conrad, Diamond and Taylor [BCDT01]. Nevertheless, the BSD conjecture remains an open problem (one of the Clay Mathematics Institute Seven Millennium Problems). By work of Kolyvagin [Kol91] it is known to hold for elliptic curves over $\mathbb{Q}$ with rank $r \leq 1$. Bhargava and Shankar [BS15] have recently proved that a positive proportion of elliptic curves over $\mathbb{Q}$ have rank zero, and therefore satisfy the BSD conjecture. For more result on the BSD conjectures over number fields we refer the reader to [Gro11, Lecture 3].

Assuming the BSD conjecture, the L-function of $E_{/K}$ admits a Taylor expansion around $s = 1$. The refined BSD conjecture (rBSD) relates the leading coefficient in this expansion to other invariants of E. In order to state this refinement we need to introduce two more invariants associated to $E_{/K}$: its regulator, and the Tamagawa numbers[2].

Definition 2.2.14. Let $P_1, \ldots, P_r \in E(K)$ be generators of $E(K)/E(K)[\text{tors}]$. The *regulator of* $E_{/K}$ is the discriminant

$$R(K, E) = |\det(\langle P_i, P_j \rangle)_{i,j=1,\ldots r}|$$

where $\langle \cdot, \cdot \rangle : E(K) \times E(K) \to \mathbb{R}$ denotes the *Néron-Tate* pairing ([Sil09, Theorem VIII.9.3(c)]).

Definition 2.2.15. Let $K = \mathbb{F}_q(t)$. For every place v of K, we define the *Tamagawa number of* E *at* v by

$$\tau_v(K, E) = [E(K_v) : E_0(K_v)],$$

[2]We will define the Tamagawa numbers only in the case $K = \mathbb{F}_q(t)$. For the general case, see for example [Gro11, Lecture 2]

and define the *(global) Tamagawa number of* $E_{/K}$ by the product

$$\tau(K,E) = \prod_{v \in \Sigma_K} \tau_v(K,E).$$

The refined BSD conjecture states

Conjecture 2.2.16. *(rBSD) BSD holds,* $Ш(K,E)$ *is finite and*

$$\lim_{s \to 1} \frac{L(E_{/K},s)}{(s-1)^r} = \frac{R(K,E) \cdot |Ш(K,E)| \cdot \tau(K,E)}{|E(K)[\text{tors}]|^2} \tag{2.6}$$

Over function fields in one variable over finite fields, we have that both conjectures are actually equivalent.

Theorem 2.2.17. *Let* $E_{/K}$ *be an elliptic curve over a function field in one variable over a finite field. The following are equivalent:*

(a) BSD holds.

(b) For any prime number l, $Ш(K,E)[l^\infty]$ *is finite.*

(c) rBSD holds.

Proof. M. Artin and J. Tate proved this for $l \neq p$ [Tat66, Theorem 5.2], and Milne considered the case $l = p$ [Mil75, Theorem 8.1]. □

Over $K = \mathbb{F}_q(t)$ the (refined) BSD conjecture is known in some cases. We recall some of these cases which are of interest to us:

Theorem 2.2.18. *Let* $E_{/K}$ *be an elliptic curve over* $K = \mathbb{F}_q(t)$ *of height* $h \leq 2$. *Then rBSD holds for* E.

Proof. By Theorem 2.2.17, it suffices to prove $Ш(K, E)$ is finite. Let $\mathcal{E} \to \mathbb{P}^1$ be the associated elliptic surface to $E_{/K}$ (§2.2.3). There is a canonical isomorphism $\mathrm{Br}(\mathcal{E}) \cong Ш(K, E)$ [Gro68, Section 4]. Therefore, finiteness of $Ш(K, E)$ is equivalent to that of $\mathrm{Br}(\mathcal{E})$, which is known to be finite when $h \leq 2$:

- $h = 0$ is due Tate [Tat66, Theorem 4],
- $h = 1$ is due to Milne [Mil70a],
- $h = 2$ is due to Artin and Swinnerton-Dyer [ASD73].

□

Finally, we want to mention that over function fields of curves over finite fields, the L-function not only admits an analytic continuation to all of $\mathbb{C}$, but is in fact a rational function. We need a definition before we state this result.

Definition 2.2.19. The *conductor* of $E_{/K}$ is the positive divisor

$$\mathfrak{n}(K, E) = \prod_v \mathfrak{p}_v^{f_v}$$

where f_v is given by the Ogg-Saito formula ([Sil94, §IV.11])

$$f_v = \mathrm{ord}_v(\Delta_v(E)) + 1 - m_v \tag{2.7}$$

where $\Delta_v(E)$ is the discriminant of a minimal Weierstrass equation for E at v, and m_v is the number of irreducible components (without multiplicities) of the Néron model of E at v.

We have that

$$f_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v, \\ 1 & \text{if } E \text{ has multiplicative reduction at } v, \\ 2+\delta_v & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

and where $\delta_v \geq 0$ is a non-negative integer. If $\operatorname{char} k_v \neq 2, 3$ then $\delta_v = 0$.

Theorem 2.2.20 ([Gro66]). *Let $K = \mathbb{F}_q(t)$ and $E_{/K}$ a non-constant elliptic curve. The L-function of $E_{/K}$ is a polynomial in q^{-s} of degree $\deg \mathfrak{n}(K, E) - 4$, with constant coefficient 1, and its zeros lie on the line $\Re es = 1$.*

2.3 Proof of the main theorem

In this section we prove Theorem 2.1.1: for every prime p, the curve

$$E \,:\, y^2 + txy + t^3 y = x^3 + t^2 x^2 + t^4 x + t^5 \tag{2.8}$$

defines an elliptic curve over $\mathbb{F}_p(t)$ with $E(\mathbb{F}_p(t)) = 0$ and $Ш(\mathbb{F}_p(t), E) = 0$.

First of all, the discriminant of E is given by

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

so $\Delta(E) \neq 0$ independently of p, and therefore (2.8) defines an elliptic curve over $\mathbb{F}_p(t)$.

Throughout this section $K = \mathbb{F}_p(t)$ and E is the elliptic curve (2.8).

2.3.1 Computing the torsion subgroup

Proposition 2.3.1. *The elliptic curve E has $E(K)[p^\infty] = 0$.*

Proof. The j-invariant of E is given by

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

For $p \neq 47$ it is clear that $j(E) \notin K^p = \mathbb{F}_p(t^p)$, so the result follows by Corollary 2.2.3. If $p = 47$, then $j(E) = 0 \in \mathbb{F}_p$ and then Corollary 2.2.3 does not apply. Using the Magma function TorsionSubgroup we find that $E(\mathbb{F}_{47}(t))[\text{tors}] = 0$. □

Proposition 2.3.2. *The elliptic curve E has $E(K)[\text{tors}] = 0$.*

Proof. From Propositions 2.2.4 and 2.3.1, it suffices to check that E has a place of additive reduction with Kodaira symbol II or II*. We have that $\Delta(E) = -t^{10}(83t^2 - 199t + 432)$, so for every p, E has bad reduction at the prime $\mathfrak{p} = (t)$. For $p \neq 2, 3$, from the valuation of the coefficients, we see from Table 2.1 that in fact E has *additive* reduction with Kodaira symbol II* at (t). For $p = 2, 3$, we use the Magma function LocalInformation to verify that we also have reduction type II* in these cases. □

Remark 2.3.3. The coefficients $(a_1, a_2, a_3, a_4, a_6) = (t, t^2, t^3, t^4, t^5)$ of E in (2.8) were chosen precisely for the purpose of E to have additive reduction with Kodaira symbol II* at $\mathfrak{p} = (t)$. As we will see in Proposition 2.3.4, this same condition is also sufficient to prove that (2.8) has no points of infinite order. In Example 2.3.6 we will see that additive reduction with Kodaira symbol II is in general not sufficient. Notice that the degrees of these coefficients are sharp for E to have height 1 *and* reduction type II*.

2.3.2 Computing the rank

Proposition 2.3.4. *The elliptic curve E has rank zero.*

Proof. For $p \neq 47$, the elliptic curve E is non-isotrivial and has height $h = 1$, so using Shioda-Tate formula (2.2.6) (with $L = \overline{\mathbb{F}_p}(t)$) we can compute the *geometric* rank of (2.8).

We have already seen that for every prime p, the elliptic curve (2.8) has always additive reduction with Kodaira symbol II^* at $\mathfrak{p}_v = (t)$. We have $m_{\mathrm{II}^*} = 9$, so we get

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

Clearly, the rank of E over K cannot exceed that over L, so we conclude $\operatorname{rank} E(K) = 0$.

For $p = 47$, using the Magma function AnalyticRank we verify that $\operatorname{rank} E(\mathbb{F}_{47}(t)) = 0$ as well. □

Combining Propositions 2.3.1, 2.3.2 and 2.3.4 we get the first part of Theorem 2.1.1:

Proposition 2.3.5. *The elliptic curve E has $E(K) = 0$.*

As discussed in §2.2.2, if $E_{/\mathbb{F}_p(t)}$ is nonisotrivial, if $j(E) \notin \mathbb{F}_p(t^p)$, and if it has a place of additive reduction II or II^*, then $E(\mathbb{F}_p(t))[\mathrm{tors}] = 0$. The following example shows that, in general, reduction type II is not sufficient to also impose rank zero.

Example 2.3.6. Let $p = 17$, and consider the elliptic curve

$$E' \,:\, y^2 + txy + ty = x^3 + tx^2 + tx + t$$

over $\mathbb{F}_p(t)$. One computes

$$\Delta(E') = -t^2(t^5 + 10t^4 + 15t^3 + 2t^2 + 9t + 7) \text{ and } j(E') = \frac{t^3(t^3 + 8t^2 + 9t + 3)^3}{\Delta}.$$

We see that E' has bad reduction at (t), $(1/t)$ and $\mathfrak{p} = (t^5 + 10t^4 + 15t^3 + 2t^2 + 9t + 7)$ (this polynomial is irreducible over $\mathbb{F}_{17}[t]$). As we discussed in Example 2.2.1, the reduction at these bad places are of Kodaira type II at (t), I_5 at $(1/t)$ and I_1 at $\mathfrak{p}$. Using the Magma

function LFunction, we get

$$L(E', T) = 83521T^4 - 578T^2 + 1 = (17T - 1)^2 \cdot (17T + 1)^2.$$

We have that $j(E') \notin \mathbb{F}_p$ and has E' height $h = 1$, so by Theorem 2.2.18 E' satisfies BSD. Then, since $\operatorname{ord}_{s=1} L(E', p^{-s}) = 2$, we conclude that $\operatorname{rank} E'(\mathbb{F}_p(t)) = 2$.

The prime $p = 17$ is the first one for which E' has rank 2. A similar analysis shows that for $p = 19$, E' also has rank 2.

2.3.3 Computing Ш

Proposition 2.3.7. *The elliptic curve E has trivial $Ш(K, E)$.*

Proof. E has height $h = 1$, so by Theorem 2.2.18 it satisfies the refined BSD conjecture. From Proposition 2.3.5 we have that $r = 0$ and $|E(K)[\text{tors}]| = 1$ (so $R(K, E) = 1$). Finally, to compute the Tamagawa factor $\tau(K, E)$, we need to consider the other places of bad reduction of E. Recall that

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

so 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 other 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, since $v(\Delta) = 1$ for these places, from Table 2.1 we see that the reduction type is I_1 at the other place(s). Fibers of type II^* and I_1 both have Tamagawa number 1 ([Sil94, Table 4.1]), so $\tau(K, E) = 1$.

Thus formula (2.6) reduces to $L(E_{/K}, 1) = |Ш(K, E)|$. If $p \neq 47$, $j(E) \notin \mathbb{F}_p$ and we can

use Theorem 2.2.20 to compute the L-function of $E_{/K}$. The support of the conductor is given by the places of bad reduction of E, discussed above, and we use the Ogg-Saito formula (2.7) to compute the exponent of the conductor at these places in characteristic $p = 2$ and $p = 3$:

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

In any case, $\deg(\mathfrak{n}(K,E)) = 4$, so by Theorem 2.2.20 we have $L(E_{/K}, s) = 1$. Using the Magma function LFunction we verify that $L(E_{/\mathbb{F}_{47}(t)}, s) = 1$ as well. Thus $|Ш(K,E)| = 1$ for all primes. □

CHAPTER 3

On the index of genus one curves over fields finitely generated over $\mathbb{F}_p(t)$

3.1 Introduction

In this chapter we prove the following result:

Theorem (Theorem 3.6.1)**.** *Let K be a field finitely generated over $\mathbb{F}_p(t)$. There is an elliptic curve $E_{/K}$ such that for all positive integer $n > 1$, there are infinitely many elements of $H^1(K, E)$ of index n.*

Since elements of $H^1(K, E)$ correspond to genus one curves $C_{/K}$ (together with an identification $E = \mathrm{Jac}(C)$), we conclude:

Corollary (Corollary 3.6.2)**.** *There are genus one curves of any prescribed index over any field finitely generated over $\mathbb{F}_p(t)$.*

The proof of Theorem 3.6.1 is done by induction on the transcendence degree of $K/\mathbb{F}_p(t)$. For the base case, $K = \mathbb{F}_p(t)$, we prove (Theorem 3.4.3) that we can take $E_{/K}$ to be *any* elliptic curve with $E(K) = Ш(K, E) = 0$. In Chapter 2 we proved that, for every prime p, there is such an elliptic curve.

The organization of the chapter is as follows: in §3.2 we review some previous work where the analogue of Theorems 3.6.1 and 3.4.3 were proved for genus one curves defined over number fields. In §3.3 we review the background material that will be needed throughout the proof of our main result. In §3.4 we prove the "base case" of the induction and in §3.5 we consider the "inductive step". Finally, with these preparations, in §3.6 we prove our main theorem, Theorem 3.6.1.

3.2 Previous work in characteristic zero

In this section we want to recall (selected) previous work on the index of genus one curves over number fields, not only for historical reasons, but also because the proof og our main theorem, Theorem 3.6.1, follows closely the ideas used in [Cla06].

W. Stein, in [Ste02] proves, using Kolyvagin's Euler system of Heegner points, that for any number field K there are infinitely many genus one curves over K with index equal to any number *not divisible by* 8. Specifically, Stein proves that if $E_{/\mathbb{Q}}$ is an elliptic curve with $L(E,1) \neq 0$, there is an integer B such that $H^1(\mathbb{Q}, E)$ contains infinitely many elements of index n, for every integer n coprime to B. By taking E the elliptic curve $X_0(17)$, he proves that $B = 2$ works (which is the best possible). Since $X_0(17)[\mathbb{Q}] = \mathbb{Z}/4\mathbb{Z}$, using a classical result of Lang and Tate [LT58, §5 Proposition 7], it is possible to handle the case of indices 2 and 4 separately, but leaving the case of integers divisible by 8 still open.

Some years later, Clark [Cla06], using different techniques was able to prove that for any number field K there are infinitely many genus one curves over K with index equal to *any* number; hence removing the divisibility condition in Stein's work. These genus one curves are realized as torsors of *any* elliptic curve $E_{/\mathbb{Q}}$ with $E(\mathbb{Q}) = 0$ and $Ш(\mathbb{Q}, E) = 0$.

We describe in detail the techniques used by Clark. We start by explaining the role of the hypotheses $E(\mathbb{Q}) = Ш(\mathbb{Q}, E) = 0$: these hypotheses, combined with the Cassels-Tate

long exact sequence are used to establish a local-to-global isomorphism of Galois cohomology classes (see §3.3.7). Over local fields, the problem of constructing classes with prescribed index is easier for two main reasons: (1) there is no distinction between period and index and (2) local duality theorems reduce the problem to that of understanding the structure of the Mordell-Weil group of elliptic curves over local fields (see §§3.3.6 and 3.4).

With this supply of "local classes" with prescribed index, using the mentioned local-to-global isomorphism (and the formal properties of O'Neil's period-index obstruction map (see §3.3.5)) it is then possible to pull back these classes to a "global class" with control on its index.

Finally, an argument is made in order to "go up" under field extensions $K/\mathbb{Q}$, and therefore the proof is complete once one finds an elliptic curve $E_{/\mathbb{Q}}$ with trivial Mordell-Weil and Tate-Shafarevich groups.

Roughly speaking, we will follow these same steps, needing to take special care of the case where the index is divisible by the characteristic of the ground field.

3.3 Preliminaries

3.3.1 Notation

A *global field* is a finite extension of $\mathbb{Q}$ (the *number field case*) or is finitely generated and of transcendence degree one over a finite field (the *function field case*). A *local field* is a field which is complete and nondiscrete with respect to a ultrametric norm, and with finite residue field. Thus a local field of characteristic 0 is (canonically) a finite extension of $\mathbb{Q}_p$, and a local field of positive characteristic is (noncanonocally) isomorphic to a finite extension of $\mathbb{F}_p((t))$.

If K is a global field, we denote by Σ_K the set of places of K (equivalence classes of

valuations on K). If $v \in \Sigma_K$, we denote by K_v the completion of K with respect to v, a local field. By $\mathcal{O}_v$ its valuation ring, $\mathfrak{m}_v$ the maximal ideal of $\mathcal{O}_v$, and k_v the residue field $\mathcal{O}_v/\mathfrak{m}_v$, a finite field. We denote by $q_v = \#k_v$ the cardinality of k_v.

For a field K, we denote by K^{s} and $\overline{K}$ the separable and algebraic closures respectively. The absolute Galois group of K, $\mathrm{Gal}(K^{\mathrm{s}}/K)$ is denoted by G_K.

If G is an abelian group and $m \in \mathbb{Z}$, we denote by $G[m]$ the m-torsion subgroup of G; i.e., the kernel of multiplication by m on G. By $G[m^\infty]$ we mean the m-primary component $\bigcup_n G[m^n]$, and by $G[\mathrm{tors}]$ its torsion subgroup $\bigcup_m G[m]$. . We write $G^\wedge$ to for pro-m-completion (the m should be understood from context). Finally, G^* will denote $\mathrm{Hom}_{cts}(G, \mathbb{Q}/\mathbb{Z})$. In particular, if G is a discrete torsion abelian group, then G^* is its Pontrjagin dual.

If A is an abelian variety, its dual abelian variety is denoted by $A^\vee$.

3.3.2 Cohomology

In what follows G will denote a profinite group.

Definition 3.3.1. A (discrete) *G-module* is a commutative group M on which G acts continuously, for the profinite topology on G, and the discrete topology on M. We denote the action of G on M by $(\sigma, m) \mapsto m^\sigma$.

For a G-module M and $n \geq 0$ we denote by $H^n(G, M)$ the *nth cohomology group of G with coefficients in M*. The groups $H^n(G, M)$ can be defined using the *continuous* cocahin complexes [Sha72, Proposition 3] or using direct limits of cohomology of finite groups ([Sha72, Corollary 1, p. 26]).

Since we will work mostly exclusively with cohomology groups in dimensions 0 and 1, we recall a more down to earth definition of H^0 and H^1. The group $H^0(K, M)$ consists of the

elements of M which are G-invariant,

$$H^0(K, M) = M^G = \{m \in M \,:\, m^\sigma - m = 0 \text{ for all } \sigma \in G\}$$

Definition 3.3.2. A 1-*cocycle* from G to M is a continuous map $\xi : G \to M$ that satisfies

$$\xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau)$$

for all $\sigma, \tau \in G$. A 1-cocycle $\xi : G \to M$ is called a 1-*coboundary* if it is of the form $\xi(\sigma) = m^\sigma - m$ for some $m \in M$. We denote the group of 1-cocycles from G to M by $Z^1(G, M)$, and its subgroup of 1-coboundaries by $B^1(G, M)$.

The group $H^1(G, M)$ is the quotient group

$$H^1(G, M) = Z^1(G, M)/B^1(G, M).$$

Remark 3.3.3. The group $H^1(G, M)$ has also an interpretation using the concept of G-*torsors*. In §3.3.4 we make this interpretation explicit in the case of Galois cohomology of elliptic curves.

Theorem 3.3.4. *Let*

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

be an exact sequence of G-modules. Taking G-invariants gives a long exact sequence of abelian groups

$$\begin{aligned} 0 \;&\to\; H^0(G, A) \;\to\; H^0(G, B) \;\to\; H^0(G, C) \;\xrightarrow{\delta}\; H^1(G, A) \;\to\; \cdots \\ \cdots \;&\to\; H^n(G, A) \;\to\; H^n(G, B) \;\to\; H^n(G, C) \;\xrightarrow{\delta}\; H^{n+1}(G, A) \;\to\; \cdots \end{aligned}$$

Proof. See e.g. [NSW08, Theorem 1.3.2] □

The *connecting homomorphism* $\delta : H^0(G, C) \to H^1(G, A)$ can be explicitly described as follows: let

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

be exact. Let $c \in H^0(G, C) = C^G$. Choose $b \in B$ such that $\beta(b) = c$ and define $\xi : G \to B$ by $\xi(\sigma) = b^\sigma - b$. Since $c = \beta(b)$ is G-invariant, it follows that $\mathrm{Im}(\xi) \subset \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$. Identifying $\mathrm{Im}(\alpha) \cong A$, ξ induces a well defined 1-cocycle (which we still call) $\xi : G \to A$. We define $\delta(c)$ to be the class of ξ in $H^1(G, A)$.

Let H be a *closed* subgroup of G. Clearly H is also a profinite group, and being closed makes the inclusion $H \hookrightarrow G$ a continuous homomorphism of profinite groups. A G-module M is naturally also an H-module (by restricting the action) and we have a natural *restriction homomorphism*

$$\mathrm{Res} = \mathrm{Res}^G_H \ : \ H^n(G, M) \to H^n(H, M). \tag{3.1}$$

If we assume further that H is a normal subgroup, the quotient G/H is profinite and the submodule M^H has naturally the structure of a G/H-module. The inclusion $M^H \hookrightarrow M$ induces a natural *inflation homomorphism*

$$\mathrm{Inf} = \mathrm{Inf}^{G/H}_G \ : \ H^n(G/H, M^H) \longrightarrow H^n(G, M). \tag{3.2}$$

Proposition 3.3.5 (Inflation-Restriction sequence)**.** *There is an exact sequence*

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M). \tag{3.3}$$

Proof. In dimension one we have a rather explicit description of the inflation homomorphism: if $\xi : G/H \to M^H$ is a 1-cocycle, we define the image of the inflation map as the class in

$H^1(G, M)$ of the 1-cocycle

$$G \longrightarrow G/H \xrightarrow{\xi} M^H \hookrightarrow M.$$

Verifying the exactness is then routine. □

Finally, if H is a normal subgroup and G/H is finite, we can also define a map in the opposite direction of restriction. In dimension zero it is given by the *trace map*,

$$M^H \longrightarrow M^G, \qquad m \mapsto \sum_{\sigma \in G/H} m^\sigma$$

This extends (uniquely) to a morphism of the functors $H^n(H, -) \to H^n(G, -)$, which induce the *corestriction homomorphism* ([Sha72, Proposition 8])

$$\text{Cores} = \text{Cores}_G^H \ : \ H^n(H, M) \longrightarrow H^n(G, M). \tag{3.4}$$

Proposition 3.3.6 (Restriction-Corestriction)**.** *If H is a normal subgroup of G with finite index, then the composition*

$$H^n(G, M) \xrightarrow{\text{Res}} H^n(H, M) \xrightarrow{\text{Cores}} H^n(G, M)$$

is multiplication by $[G : H]$ on $H^n(G, M)$.

Proof. See e.g. [Sha72, Proposition 9]. □

Lemma 3.3.7. *For $n \geq 1$, the groups $H^n(G, M)$ are torsion groups.*

Proof. See e.g. [Sha72, Corollary 2] □

Definition 3.3.8. For $n \geq 1$ and $\eta \in H^n(G, M)$ we define $P(\eta)$, the *period* of η, as the order of η in $H^n(G, M)$.

3.3.3 Galois cohomology

For a field K we denote by $\overline{K}$ and K^{s} a fixed choice of algebraic and separable closures of K. We write $G_K = \mathrm{Gal}(K^{\mathrm{s}}/K)$ for the *absolute Galois group* of K. The group G_K is a profinite group, as it is the inverse limit of $\mathrm{Gal}(L/K)$ as L varies over all finite Galois extensions L/K (contained in K^{s}).

Notation. If L/K is a Galois extension and M is a $\mathrm{Gal}(L/K)$-module, we write $H^n(L/K, M) := H^n(\mathrm{Gal}(L/K), M)$. In the case $L = K^{\mathrm{s}}$ we write $H^n(K, M) := H^n(G_K, M)$, and refer to it as the nth *Galois cohomology* group of K with coefficients in M. If A is a commutative group scheme over K, locally of finite type, then $M = A(K^{\mathrm{s}})$ is a G_K-module, and we write $H^n(K, M) = H^n(K, A)$.

The main example of G_K-module that we will consider is that of abelian varieties over K. An important application of Theorem 3.3.4 is the following.

Example 3.3.9. Let $A_{/K}$ be an abelian variety, and let $n \geq 2$ a positive integer. If $\mathrm{char}\, K \nmid n$, we have a short exact sequence of G_K-modules

$$0 \longrightarrow A[n] \longrightarrow A \xrightarrow{[n]} A \longrightarrow 0. \tag{3.5}$$

Taking Galois cohomology we obtain a long exact sequence

$$\begin{aligned} 0 \to A(K)[n] \to A(K) \xrightarrow{[n]} A(K) \xrightarrow{\delta} H^1(K, A[n]) \to \\ H^1(A, E) \xrightarrow{[n]} H^1(A, E) \to \dots \end{aligned}$$

from where we obtain the following short exact sequence, which we refer as the *Kummer sequence* for $A_{/K}$:

$$0 \to A(K)/nA(K) \to H^1(K, A[n]) \to H^1(K, A)[n] \to 0. \tag{3.6}$$

Remark 3.3.10. When $\mathrm{char}\, K \mid n$, the map $A(K^{\mathrm{s}}) \xrightarrow{[n]} A(K^{\mathrm{s}})$ need not to be surjective, and therefore the sequence (3.5) is not exact. Also, when $\mathrm{char}\, K \mid n$, the finite K-group scheme $A[n]$ is not étale, so it is not determined by the G_K-module $A[n](K^{\mathrm{s}})$. The sequence (3.5) can be viewed as a short *exact sequence of abelian sheaves on the flat site of* K ([Sha72, §IV.3]), and then using *flat cohomology* we get a Kummer sequence (3.6), where the groups H^1 need to be interpreted accordingly. For details we refer the reader to [Cla10, §2]. If $\mathrm{char}\, K \nmid n$, then the finite K-group scheme $A[n]$ is étale, and both interpretations coincide ([Sha72, Theorem 43]).

If L/K is an *algebraic* extension, then G_L is a closed subgroup of G_K, so the inclusion $G_L \hookrightarrow G_K$ is continuous and we have the natural *restriction* map (3.1)

$$\mathrm{Res}_{L/K} := \mathrm{Res}^{G_K}_{G_L} \,:\, H^n(K, M) \to H^n(L, M).$$

We will also need to consider transcendental field extensions and the corresponding restriction maps in Galois cohomology. We make the following observation, which is the content of [Ser02, §II.1.1]: let A be a commutative group scheme over K, locally of finite type. Then $M = A(K^{\mathrm{s}})$ is a G_K-module. 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 in $\mathrm{Aut}(\overline{K}/K) = G_K$. This gives a continuous group homomorphism $G_L \to G_K$, so we again can argue as in 3.1 to define the *restriction map* $\mathrm{Res}_{L/K} \,:\, H^n(K, M) \to H^n(L, M)$ (which does not depend on the field embedding $\iota : \overline{K} \hookrightarrow \overline{L}$).

Definition 3.3.11. Let L/K be a field extension. Whenever the restriction $\mathrm{Res}_{L/K}$ is defined, we put

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

Remark 3.3.12. Let L/K be a finite Galois extension. The group $\mathrm{Gal}(K^{\mathrm{s}}/L)$ is a normal subgroup of $G_K = \mathrm{Gal}(K^{\mathrm{s}}/K)$, and the quotient G_K/G_L is the finite group $\mathrm{Gal}(L/K)$. From the inflation-restriction sequence (3.3) we get

$$\widetilde{H}^1(L/K, A) = H^1(L/K, A) = H^1(\mathrm{Gal}(L/K), A(L)). \tag{3.7}$$

So, in dimension one, one usually drops the tilde from the notation of the kernel of restriction.

As $H^n(K, M) = \widetilde{H}^n(K^{\mathrm{s}}/K, M)$, by definition of Galois cohomology, for every $\eta \in H^n(K, M)$ there is a *finite* extension L/K (contained in K^{s}) such that $\eta \in \widetilde{H}^n(L/K, M)$.

Definition 3.3.13. If $\eta \in \widetilde{H}^n(L/K, M)$, we say that L is a *splitting field* for η. We define $I_s(\eta)$, the *separable index* of η, as the greatest common divisor of all degrees of finite splitting fields of η.

Remark 3.3.14. Although we have gone into some trouble defining the restriction map for transcendental extensions, we will see in §3.5 that for purely transcendental extensions L/K, the restriction is an injection, and therefore the groups $\widetilde{H}^n(L/K, M)$ are trivial in this case.

In the case of Galois cohomology, for $\eta \in H^n(K, M)$ we have define to numerical invariants to η: its period $P(\eta)$, and its separable index $I_s(\eta)$. We summarize some of their basic properties in the following

Proposition 3.3.15. *For $\eta, \eta' \in H^n(K, M)$ we have*

(a) $P(\eta) \mid I_s(\eta)$, and they have the same prime divisors.

(b) If $\gcd(P(\eta), P(\eta')) = 1$, then $I_s(\eta + \eta') = I_s(\eta) \cdot I_s(\eta')$.

Proof. (a) [LT58, Proposition 5] Let L/K be a splitting field of η. By Proposition 3.3.6, the composition

$$H^n(K, M) \xrightarrow{\mathrm{Res}} H^n(L, M) \xrightarrow{\mathrm{Cores}} H^n(K, M)$$

is multiplication by $[L:K]$ on $H^n(K,M)$. Therefore $[L:K]\cdot\eta = 0$, that is $P(\eta)$ divides $[L:K]$. Since L/K was an arbitrary splitting field of η, we have that $P(\eta)$ divides every degree of a splitting field, so in particular divides the greatest common divisor of such degrees, and therefore divides $I_s(\eta)$.

For the second claim, let p be a prime not dividing $P(\eta)$. Let L/K be any finite splitting field of η. By replacing L with its Galois closure, we may as well, assume L/K is Galois. Let $H_p < \mathrm{Gal}(L/K)$ be a p-Sylow subgroup, and take$L_p = L^{H_p}$ be the subfield of L fixed H_p. Then, on one hand, the period of $\mathrm{Res}_{L_p/K}(\eta) \in \widetilde{H}^1(L/L_p, M)$ divides the p-power $[L:L_p]$, and in the other hand, divides $P(\eta)$. Therefore $\mathrm{Res}_{L_p/K}(\eta) = 0$, that is L_p splits η. Consequently $I_s(\eta)$ divides $[L_p:K]$, so p cannot divide $I_s(\eta)$.

(b) Let F/K be a splitting field for $\eta+\eta'$. Then clearly F is also a splitting field of $P(\eta)\cdot(\eta+\eta') = P(\eta)\cdot\eta'$, so F splits η'. Similarly, F is also a splitting field of η. Therefore $I_s(\eta+\eta')$ is divisible by both $I_s(\eta)$ and $I_s(\eta')$, which by part (a) are relatively prime, so $I_s(\eta)\cdot I_s(\eta') \mid I_s(\eta+\eta')$. For the reverse divisibility, let L/K and L'/K be separable splitting fields of η and η' respectively. Again, by part (a), the degrees $[L:K]$ and $[L':K]$ are relatively prime. The compositum $L.L'$ clearly splits $\eta+\eta'$. Thus $I_s(\eta+\eta')$ divides $[L.L':K] = [L:K]\cdot[L':K]$. □

We are interested in the case where $M = A(K^{\mathrm{s}})$ for an abelian variety $A_{/K}$. In this case, elements of $H^1(K,A)$ correspond to geometric objects, called *principal homogeneous spaces* for A.

3.3.4 Principal homogeneous spaces

In this section $A_{/K}$ will denote an abelian variety defined over a field K. We denote by $+$ the group law on A, and by $0 \in A(K)$ the identity element for this group law.

Definition 3.3.16. Let $A_{/K}$ be an abelian variety defined over a field K. A *principal*

homogeneous space for $A_{/K}$ is a variety $V_{/K}$ together with a simply transitive algebraic action on K^{s}-points, also defined over K.

In other words, a principal homogeneous space for $A_{/K}$ is a pair (V, μ) where

$$\mu : A \times V \to V$$

is a K-morphism with the following properties:

(a) $\mu(0, v) = v$, for all $v \in V(K^{\mathrm{s}})$.

(b) $\mu(a + b, v) = \mu(a, \mu(b, v))$ for all $v \in V(K^{\mathrm{s}})$ and all $a, b \in A(K^{\mathrm{s}})$.

(c) For all $x, y \in V(K^{\mathrm{s}})$ there is a unique $a \in A(K^{\mathrm{s}})$ such that $\mu(a, x) = y$.

As a *trivial* example of a principal homogeneous space for $A_{/K}$ we can take $(V, \mu) = (A, +)$. In this case, property (b) above in this case is just the associativity of $+$, and property (c) above is simply the fact that we can subtract elements in A: $a = x - y$.

In general, given a principal homogeneous space (V, μ) for $A_{/K}$, property (c) can be used to define a *subtraction map* $\nu : V \times V \to A$ as the unique point $\nu(x, y) \in A$ such that $\mu(\nu(x, y), x) = y$.

Proposition 3.3.17. *Let $A_{/K}$ be an abelian variety, and let (V, μ) be a principal homogeneous space for $A_{/K}$. Let $x_0 \in V(K^{\mathrm{s}})$, and define*

$$\theta : A \to V, \quad \theta(a) = \mu(a, x_0)$$

(a) The map θ is an isomorphism defined over $K(x_0)$.

(b) For all $x \in V(K^{\mathrm{s}})$ and $a \in A(K^{\mathrm{s}})$,

$$\mu(a, x) = \theta(\theta^{-1}(x) + a)$$

(c) The subtraction map $\nu : V \times V \to A$ is a morphism defined over K.

(d) For all $x, y \in V(K^{\mathrm{s}})$,

$$\nu(x, y) = \theta^{-1}(x) - \theta^{-1}(y)$$

Proof. This is given in [Sil09, Proposition X.3.2] in the case of A an elliptic curve, but the proof applies without change to abelian varieties. □

Definition 3.3.18. Two homogeneous spaces (V, μ) and (V', μ') of $A_{/K}$ are *equivalent* if there is an isomorphism $\theta : V \to V'$ defined over K compatible with the action of A on V and V', that is, the following diagram commutes:

$$\begin{array}{ccc} A \times V & \xrightarrow{\mu} & V \\ {\scriptstyle 1\times\theta}\downarrow & & \downarrow{\scriptstyle \theta} \\ A \times V' & \xrightarrow{\mu'} & V' \end{array}$$

The collection of equivalence classes of homogeneous spaces of $A_{/K}$ is called the *Weil-Châtelet group* of $A_{/K}$, and it is denoted $\mathrm{WC}(K, A)$. The equivalence class containing $(A, +)$ is called the *trivial class*.

Remark 3.3.19. Weil [Wei55] showed that the *set* $\mathrm{WC}(K, A)$ admits a composition law, making it into a *torsion* commutative group. We will endow -indirectly- the set $\mathrm{WC}(K, A)$ with the structure of a torsion commutative group in Proposition 3.3.21 below.

Lemma 3.3.20. *A homogeneous space $V \in \mathrm{WC}(K, A)$ is in the trivial class if and only $V(K) \neq \emptyset$.*

Proof. Suppose that $V_{/K}$ is in the trivial class, and let $\theta : A \to V$ be an isomorphism defined over K. Then $\theta(0) \in V(K)$.

Conversely, suppose that $p \in V(K)$. Consider the isomorphism $\theta : A \to V$ defined by $\theta(a) = \mu(a, p)$. By Proposition 3.3.17 (a), θ is defined over K, and it follows from the

properties of μ that the following diagram commutes

$$\begin{array}{ccc} A \times A & \xrightarrow{+} & A \\ {\scriptstyle 1\times\theta}\downarrow & & \downarrow{\scriptstyle \theta} \\ A \times V & \xrightarrow{\mu} & V \end{array}$$

That is (V, μ) is equivalent to $(A, +)$. □

We now relate the Weil-Châtelet group $WC(K, A)$ to the Galois cohomology group $H^1(K, A)$.

Proposition 3.3.21. *There is a canonical isomorphism between the Weil-Châtelet group $WC(K, A)$ and the Galois cohomology group $H^1(K, A)$. This isomorphism is given by*

$$\begin{array}{ccccc} \Phi : WC(K, A) & \longrightarrow & H^1(K, A) \\ \{(V, \mu)\} & \mapsto & \{\sigma \mapsto \nu(p^\sigma, p)\} \end{array}$$

where $p \in V(K^{\mathrm{s}})$. This is independent of the choice of p.

Proof. See e.g. [LT58, Proposition 4] □

Using this isomorphism we can endow $WC(K, A)$ with the structure of a torsion commutative group. In §3.3.2 we defined the period and separable index for elements of Galois cohomology groups.

Definition 3.3.22. Let (V, μ) a principal homogeneous space for $A_{/K}$ and let $\eta = \Phi(V, \mu)$. We define the *period* and *separable index* of (V, μ) as $P(\eta)$ (Definition 3.3.8) and $I_s(\eta)$ (Definition 3.3.13), respectively.

It is clear, by Lemma 3.3.20, that the separable index of $V \in WC(K, A)$ corresponds to the greatest common divisor of all degrees of finite *separable* field extensions L/K such that $V(L) \neq \emptyset$. If one allows arbitrary field extensions, not necessarily separable, one gets

a priori a possibly smaller integer, called the *index* of V. The following proposition shows that one gets the same answer.

Proposition 3.3.23. *Let $V \in WC(K, A)$. The separable index of V is the greatest common divisor of all degrees of finite field extensions L/K such that $V(L) \neq \emptyset$.*

Proof. This is due to Lichtenbaum [Lic68, Theorem 4]. □

Remark 3.3.24. By the previous proposition, in the case of principal homogeneous spaces for abelian varieties, we do not need to make a distinction between the separable index and the index.

When $A_{/K}$ is an elliptic curve, we can interpret the period and index of $V \in WC(K, A)$ in terms of divisors on V. Let $\mathrm{Div}(V)$ denote the group of K^{s}-rational divisors on V, and $\mathrm{Pic}(V)$ the group of K^{s}-rational divisors modulo linear equivalence. Let $\mathrm{Div}^0(V)$ and $\mathrm{Pic}^0(V)$ denote the corresponding objects of degree zero. Finally, let $\mathrm{Div}_K(V)$ denote the subgroup of K-rational divisors, i.e., $D \in \mathrm{Div}(K)$ such that $D^\sigma = D$ for all $\sigma \in G_K$. Similarly for $\mathrm{Div}^0_K(V)$.

Proposition 3.3.25. *Let $E_{/K}$ be an elliptic curve and let $C \in WC(K, E)$.*

(a) The period of C is equal to the least positive degree of a divisor class $D \in \mathrm{Pic}(V)$ which is G_K-invariant.

(b) The (separable) index of C is equal to the least positive degree of a K-rational divisor.

Proof. These are Lemmas 1 and 2 of [Lic68][1]. □

Remark 3.3.26. Notice that we can use the previous proposition to define the period and index of a smooth genus one curve $C_{/K}$ with out reference to the elliptic curve for which C was a principal homogeneous space. It is clear from Proposition 3.3.25 that the period of C

[1]Notice that there is a typo in the statement of Lemma 2: period should read index

divides its index (we proved this in Proposition 3.3.15). The following example of Cassels shows that the index can exceed the period.

Example 3.3.27 ([Cas63])**.** Consider the elliptic curve given by

$$\mathcal{C} : \begin{cases} x^2 = y^2 - t^2, \\ z^2 = y^2 + t^2. \end{cases}$$

Let l, m, n be nonzero rational numbers, and consider the curve

$$\mathcal{D} : \begin{cases} mnX^2 = nlY^2 - T^2, \\ lmZ^2 = nlY^2 + T^2. \end{cases}$$

Notice that $\mathcal{D}$ is birationally equivalent to $\mathcal{C}$ over $\mathbb{Q}(\sqrt{l}, \sqrt{m}, \sqrt{n})$, but in general, not over $\mathbb{Q}$. Cassels shows, by explicitly describing the structure of $\mathcal{D}$ as a principal homogeneous space for $\mathcal{C}_{/\mathbb{Q}}$, that $\mathcal{D}$ has period 2 and that for infinitely many choices of l, m, n ($l = -11$, $m = 3$, $n = 1$ for example) $\mathcal{D}$ has index 4.

□

Proposition 3.3.28. *Let $E_{/K}$ an elliptic curve and $C \in WC(K, E)$. We have an isomorphism of G_K-modules $E \cong \mathrm{Pic}^0(C)$ over K^{s}.*

Proof. See e.g. [Sil09, Theorem X.3.8]. □

Definition 3.3.29. Let $C_{/K}$ be a smooth genus one curve. We define the *Jacobian elliptic curve of C* to be $\mathrm{Pic}^0(C)$.

Remark 3.3.30. It is a known,but deep, fact [BLR90, Chapters 8,9] that for any smooth, projective, geometrically integral curve C over a field K, the sheafification of the fpqc presheaf $T \mapsto \mathrm{Pic}(C_{/T})$ is representable by a K-group scheme $\mathrm{Pic}\, C$ which is locally of

finite type but with connected components $\mathrm{Pic}^n C$ parameterized by the integers. The identity component $\mathrm{Pic}^0 C$ is an abelian variety of dimension equal to the genus of C. Especially, when C has genus one, then Riemann-Roch gives a canonical identification of C with $\mathrm{Pic}^1 C$, and then the natural action of $\mathrm{Pic}^0(C)$ on $\mathrm{Pic}^1(C)$ gives C the structure of a principal homogeneous space over $\mathrm{Pic}^0(C)$.

3.3.5 The period-index obstruction map

Let $E_{/K}$ be an elliptic curve, and $n \geq 1$ a positive integer. The *period-index obstruction map* is a map in flat cohomology (see Remark 3.3.10)

$$\Delta = \Delta_n \,:\, H^1(K, E[n]) \to \mathrm{Br}(K)[n] \tag{3.8}$$

functorial in K, satisfying the following properties:

- Let $\eta \in H^1(K, E)[n]$ be a class of period n. Then η has index n if and only if there is a Kummer lift of η to $\xi \in H^1(K, E[n])$ (see (3.6)) such that $\Delta(\xi) = 0$.
- If $\eta = 0$ then $\Delta(\xi) = 0$ for any Kummer lift.

Remark 3.3.31. The definition of the period-index obstruction map Δ_n was given by C. O'Neil in [O'N02] in the case that $\mathrm{char}\, K \nmid n$. Clark [Cla10] extended this definition, using *flat cohomology*, in order to include the case $\mathrm{char}\, K \mid n$. We will only need to use the formal properties of the map Δ_n listed above, which hold regardless whether the comohology group $H^1(K, E[n])$ should be interpreted as a Galois cohomology group or as a flat cohomology group. See Remark 3.3.10.

Lemma 3.3.32. *Let K be a field with $\mathrm{Br}(K) = 0$, and $E_{/K}$ an elliptic curve. Then every element of $H^1(K, E)$ has period equal index.*

Proof. It follows directly from the definition and the properties of Δ highlighted above.

This result is actually due to Lichtenbaum [Lic68, Theorem 1]. We quote: "*... the obstruction to the existence of a k-rational divisor in a given k-rational divisor class lies in the Brauer group of k*". See also [O'N02, §5]. □

The following lemma will play an important role in the proof of our main theorem:

Lemma 3.3.33. *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 K except (possibly) one. Then η has period equal index.*

Proof. If K is a number field and η is *everywhere* locally trivial, that is if $\eta \in Ш(K, E)$, it is classically known that $P(\eta) = I(\eta)$ [Cas62, Theorem 1.3]. C. O'Neil gives a very short proof of this for arbitrary K, except possibly when $\operatorname{char} K \mid P(\eta)$. If $\operatorname{char} K \mid P(\eta)$, the argument goes though when one uses the aforementioned extension of the obstruction map by Clark.

So let's assume that η is locally trivial except, say at $\mathfrak{p} \in \Sigma_K$. The following argument appears in [Ols70, Corollary 16] (and was rediscovered in [Cla06, Proposition 6]).

Let $n = P(\eta)$, and write $\Delta = \Delta_n$ for the obstruction map. Let $\xi \in H^1(K, E[n])$ be a Kummer lift of η. For $\mathfrak{q} \in \Sigma_K$ we denote by $\xi_\mathfrak{q}$ the image of ξ under the restriction $H^1(K, E) \to H^1(K_\mathfrak{q}, E[n])$. Let $\operatorname{inv}_\mathfrak{q} : \operatorname{Br}(K_\mathfrak{q}) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ denote the *Hasse invariant*, and consider the commutative diagram

$$\begin{array}{ccccccccc} & & & & H^1(K, E[n]) & \longrightarrow & \bigoplus H^1(K_\mathfrak{q}, E[n]) & & \\ & & & & \downarrow{\scriptstyle \Delta} & & \downarrow & & \\ 0 & \longrightarrow & \operatorname{Br}(K) & \longrightarrow & \bigoplus \operatorname{Br}(K_\mathfrak{q}) & \xrightarrow{\sum \operatorname{inv}_\mathfrak{q}} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

where $\mathfrak{q}$ runs over all places of K, and the bottom row is the exact sequence coming from the *Reciprocity Law in the Brauer group*. By assumption, for $\mathfrak{q} \neq \mathfrak{p}$, $\eta_\mathfrak{q} = 0$ so $\Delta(\xi_\mathfrak{q}) = 0$ in $H^1(K_\mathfrak{q}, E[n])$, so a quick diagram chase shows that $\operatorname{inv}_\mathfrak{p}(\Delta(\xi)) = 0$. Since $\operatorname{inv}_\mathfrak{p}$ is an injection, it follows $\Delta(\xi) = 0$. Thus η has trivial obstruction, hence period equal index □

3.3.6 Local duality theorems

Let $A_{/K}$ be an abelian variety over a local field, and denote by $A^\vee$ its dual abelian variety. In [Tat58] Tate defines a pairing

$$A^\vee(K) \times H^1(K, A) \to H^2(K, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z} \tag{3.9}$$

between the discrete torsion group $H^1(K, A)$ and the compact profinite group $H^0(K, A^\vee) = A^\vee(K)$. This pairing is continuous with respect to the canonical compact topology on H^0 and the discrete topology on H^1.

Tate's pairing (3.9) is known to be non-degenerate in full generality:

- If $\operatorname{char} K = 0$, or if $\operatorname{char} K = p$ except possibly on the p-primary components is due to Tate [Tat58].
- If $\dim A = 1$ and A does not have potential good reduction is due to Shatz [Sha67].
- Milne [Mil70b] consider the case where A has potential good reduction, and shortly after Milne himself [Mil72], removed this restriction.

We refer to the non-degeneracy of the Tate pairing as the *(Milne-Tate) Local Duality Theorem*. The Tate pairing induces induces then an isomorphism

$$H^1(K, A) \to \operatorname{Hom}(A^\vee, \mathbb{Q}/\mathbb{Z}) = (A^\vee(K))^*. \tag{3.10}$$

In particular, for $n \geq 1$ we have

$$H^1(K, A)[n] \cong \left(A^\vee(K)/nA^\vee(K)\right)^*. \tag{3.11}$$

Remark 3.3.34. A key ingredient in Lichtenbaum's solution to the period-index problem

for elliptic curves over local fields of *characteristic zero* [Lic68] is Tate's version of the local duality. An immediate consequence of Milne's and Shatz's extension of Tate's local duality, is that Lichtenbaum's solution holds for all local fields.

3.3.7 A local-global isomorphism in WC groups

Let K be a global field and let $l \geq 1$ a positive integer *not* divisible by the characteristic of K. Let $A_{/K}$ an abelian variety, and assume that the l-primary subgroup of $Ш(K, A)$ is finite (that is, conjecturally always). There is a short exact sequence ([Cas64], [Tat63], [Mil06, Theorem I.6.26(b)])

$$0 \to Ш(K, A)[l^\infty] \to H^1(K, A)[l^\infty] \to \bigoplus_{v \in \Sigma_K} H^1(K_v, A)[l^\infty] \to (A^\vee(K)^\wedge)^* \longrightarrow 0 \qquad (3.12)$$

which is known as the *Cassels-Tate* exact sequence.

This exact sequence played an important role in [Cla06], where the ground field K had characteristic zero, and therefore the restriction on l was irrelevant. In our application we will need to consider the case of $\operatorname{char} K \mid l$. The following result of González-Avilés-Tan, which generalizes the Cassels-Tate exact sequence provides exactly what we need. For $m \geq 2$ a positive integer, let

$$\operatorname{Sel}_m A^\vee = \operatorname{Ker}\left(H^1(K, A^\vee[m]) \longrightarrow \bigoplus_{v \in \Sigma_K} H^1(K_v, A^\vee) \right)$$

the *m-Selmer group* of $A^\vee_{/K}$. For a prime p we put

$$T_p \operatorname{Sel} A^\vee = \varprojlim_n \operatorname{Sel}_{p^n} A^\vee$$

Theorem 3.3.35. *For $A_{/K}$ an abelian variety over a global field, and p any prime number*

- the case $p = \mathrm{char}\, K$ is allowed - we have an exact sequence

$$0 \to T_p \,\mathrm{Sel}\, A^\vee \to \prod_{v\in\Sigma_K} (A^\vee(K_v))^\wedge \to (H^1(K,A)[p^\infty])^* \to (Ш(K,A)[p^\infty])^* \to 0. \qquad (3.13)$$

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

We deduce from this exact sequence

Corollary 3.3.36. *Let $A_{/K}$ be an abelian variety over a global field. If $A^\vee(K) = 0$ and $Ш(K,A) = 0$ we have an isomorphism*

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

Proof. Since the cohomology groups $H^1(-,A)$ are torsion groups, it suffices to restrict to the p-primary components for all primes p. If $Ш(K,A)$ is finite -in particular if it is trivial-, then so is $Ш(K,A^\vee)$ ([Mil06, Remark I.6.14(c)]). Then $Ш(K,A^\vee) = 0$ as well, and from the exact sequence

$$0 \longrightarrow A^\vee(K)/p^n A^\vee(K) \longrightarrow \mathrm{Sel}_{p^n} A^\vee \longrightarrow Ш(K,A^\vee)[p^n] \longrightarrow 0$$

it follows that $\mathrm{Sel}_{p^n} A^\vee = 0$, so $T_p \,\mathrm{Sel}\, A^\vee = 0$. Then (3.13) gives an isomorphim

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

Taking Pontrjagin duals,

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

Finally, using Tate-Milne local duality (3.10) to identify $A^\vee(K_v) \cong H^1(K_v,A)$, we get the

desired isomorphism,

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

□

3.3.8 Weak Mordell-Weil fields

The following results will be necessary for our inductive arguments:

Definition 3.3.37. A field K is *weak Mordell-Weil* if for every abelian variety $A_{/K}$ and for every positive integer $n \geq 1$, the quotient $A(K)/nA(K)$ is finite.

Lemma 3.3.38. *Let K be a weak Mordell-Weil field and L/K be a finite separable field extension. Then L is also a weak Mordell-Weil field.*

Proof. Let $A_{/L}$ be an abelian variety, and consider $A_* = N_{L/K}A$ the be the *variety* obtained by Weil restriction (in the sense of [Wei82, §1.3]). Let $m = [L : K]$, and let $\sigma_1, \ldots, \sigma_m$ the distinct embeddings of L into K^{s} over K. There is a K^{s}-isomorphism $A_* \cong A^{\sigma_1} \times \ldots \times A^{\sigma_m}$ [Wei82, page 5], so it follows that A_* is also an abelian variety (defined over K) and $A_*(K) = A(L)$.

Then for all $n \geq 1$, $A(L)/nA(L) = A_*(K)/nA_*(K)$ is finite, since K is weak Mordell-Weil. Therefore L is a weak Mordell-Weil field □

Lemma 3.3.39. *Let K be a weak Mordell-Weil field and L/K finitely generated regular field extension. Then L is also a weak Mordell-Weil field.*

Proof. Let $A_{/L}$ be an abelian variety. By the Lang-Nerón Theorem [LN59, Theorem 1], there is an abelian variety $B_{/K}$ together with an injective homomorphism $\tau : B \hookrightarrow A$ defined over K (the pair (B, τ) is called a *L/K-trace of A*) that satisfies $A(L)/\tau B(K)$ is finitely generated. It follows that $A(L)/nA(L)$ is finite, so L is a weak Mordell-Weil field. □

Corollary 3.3.40. *Every finitely generated field is weak Mordell-Weil.*

Proof. Let k be the prime subfield of K: either $\mathbb{Q}$ or $\mathbb{F}_p$. In either case, k is a weak Mordell-Weil field. Since k is perfect, K/k admits a separating transcendence basis, say $\{t_1, \ldots, t_n\}$. Put $K' = k(t_1, \ldots, t_n)$. We have K'/k is finitely generated regular, so by Lemma 3.3.39 K' is a weak Mordell-Weil field. We have K/K' is finite separable, so by Lemma 3.3.38 so is K. □

3.4 The base case

Theorem 3.4.1. *Let K_v be a local field of equicharacteristic $p > 0$, and let $A_{/K}$ an abelian variety. The structure of the Mordell-Weil group $E(K_v)$ is given by*

$$A(K_v) \cong \left(\prod_{i=1}^{\infty} \mathbb{Z}_p \right) \oplus T$$

for some finite group T.

Proof. This appears in [CL, Theorem 21]. □

Lemma 3.4.2. *Let $A_{/K}$ be an abelian variety over a global field K. Let $n \in \mathbb{N}$ be an integer.*

(a) If $\mathrm{char} K \nmid n$, then there is a positive density set $\mathcal{P} \subset \Sigma_K$ such that for all $v \in \mathcal{P}$, $H^1(K_v, A)$ has an element of order n

(b) If $\mathrm{char} K = p$ and $n = p^a$ for $a \geq 1$, then for every place v of K, $H^1(K_v, A)$ has infinitely many elements of order n.

Proof. We will prove that there is always an infinite set of places v of K such that $H^1(K_v, A)[n]$ contains a nontrivial element.

Let v be a finite place of K. By *Tate-Milne local duality Theorem*, for every $n \geq 1$ we have an isomorphism (3.11)

$$H^1(K_v, A)[n] \cong A^\vee(K_v)/nA^\vee(K_v),$$

so it suffices to exhibit an element of order n in the weak Mordell-Weil quotient $A(K_v)/nA(K_v)$ (clearly we can replace $A^\vee$ with A in doing so). Recall from Theorem 3.4.1 that

$$A(K_v) \equiv \left(\prod_{i\in I} \mathbb{Z}_p\right) \oplus T$$

for some nonempty indexing set I. So, if $n = p^a$, the quotient $A(K_v)/p^aA(K_v)$ contains at least $\#I$ elements of order p^a. Notice that in this case ($n = p^a$), this holds for every finite place v of K.

If $p \nmid n$, then $A[n]$ is a finite *étale* group scheme, and as $A[n](K^{\mathrm{s}}) \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$, there is a finite Galois extension L/K such that $A[n](L) \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$. Let v a place of K which splits completely in L. For such v we have a K-algebra embedding $L \hookrightarrow K_v$ and thus $A(K_v) \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$. Then, the quotient $A(K_v)/nA(K_v)$ contains $2\dim A$ elements of order n. Finally, by the *Cebotarev Density Theorem*, the set of finite places splitting completely in the Galois extension L/K has positive density, hence is infinite. □

The next theorem takes advantage of the latter construction of classes with period n over local fields, to construct classes with index n over global fields.

Theorem 3.4.3. *Let $K/\mathbb{F}_p(t)$ be a global field, and let $E_{/K}$ be an elliptic curve with $E(K) = Ш(K, E) = 0$. Then for all $n > 1$, there is an infinite subset $S \subset H^1(K, E)[n]$ such that every element has index n.*

Proof. From Corollary 3.3.36 we have that whenever $E(K) = Ш(K, E) = 0$ we have an

isomorphism

$$H^1(K,E) \xrightarrow{\phi} \bigoplus_{v\in\Sigma_K} H^1(K_v,E)$$

Invoking Lemma 3.4.2, let $v \in \Sigma_K$ be any of the infinitely many finite places such that $H^1(K_v,E)$ contains a nontrivial element of period n, say η_v. Let $\eta = \phi^{-1}(0,\ldots,\eta_v,0,\ldots) \in H^1(K,E)$. Clearly η has period n, as ϕ is a group isomorphism. On the other hand, η is locally trivial at all places except v, so it follows from Lemma 3.3.33 that η has index n. □

Remark 3.4.4. The infinite set $S \subset H^1(K,E)[n]$ in Theorem 3.4.3 is also linearly independent over $\mathbb{Z}/n\mathbb{Z}$ (in the sense of Definition 3.5.3 below) as every element $\eta \in S$ is supported in a different direct summand.

3.5 The inductive arguments

In this section we prove the necessary results in order to perform the "inductive steps" in the proof of Theorem 3.6.1.

Lemma 3.5.1. *Let $A_{/K}$ be an abelian variety over a Weak Mordell-Weil field. Let L/K be a finite separable field extension. Then the kernel $\widetilde{H}^1(L/K,A)$ 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 without loss of generality that L/K is finite Galois, say of degree $n = [L:K]$.

The Kummer sequences (3.6) associated to multiplication by n on $A_{/K}$ and $A_{/L}$, gives a

commutative ladder

$$\begin{array}{ccccccccc} & & & & \mathcal{K} & \longrightarrow & \widetilde{H}^1(L/K, A[n]) & \longrightarrow & \widetilde{H}^1(L/K, A) \\ & & & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A(K)/nA(K) & \longrightarrow & H^1(K, A[n]) & \longrightarrow & H^1(K, A)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(L)/nA(L) & \longrightarrow & H^1(L, A[n]) & \longrightarrow & H^1(L, A)[n] & \longrightarrow & 0 \\ & & \downarrow & & & & & & \\ & & \mathcal{C} & & & & & & \end{array}$$

where the middle vertical maps are restriction maps induced by $K \hookrightarrow L$, and $\mathcal{C}$ and $\mathcal{K}$ denote respectively the cokernel and kernel of the respective restriction maps. The snake lemma gives an exact sequence

$$0 \longrightarrow \mathcal{K} \longrightarrow \widetilde{H}^1(L/K, A[n]) \longrightarrow \widetilde{H}^1(L/K, A) \longrightarrow \mathcal{C} \longrightarrow 0. \tag{3.14}$$

By assumption $A(K)/nA(K)$ is finite, so $\mathcal{K} \hookrightarrow A(K)/nA(K)$ is finite. By Lemma 3.3.38 the quotient $A(L)/nA(L)$ is also finite, so $\mathcal{C}$, being the cokernel between finite groups, is finite. Finally, since L/K is Galois, by [Wat79, Theorem §17.7] $\widetilde{H}^1(L/K, A[n]) = H^1(\mathrm{Gal}(L/K), A[n](L))$, where the right hand side is the cohomology of a finite group with coefficient in a finite module, so it is a quotient of a finite group of cochains and thus is certainly finite. From the exact sequence (3.14), we conclude that $\widetilde{H}^1(L/K, A)$ is finite, as claimed. □

Lemma 3.5.2. *Let L/K be a purely transcendental field extension. For every abelian variety $A_{/K}$, the kernel $\widetilde{H}^1(L/K, A)$ is trivial.*

Proof. Suppose first that $L = K(t)$. Let $\eta \in H^1(K, A)$. By the bijection $H^1(K, A) \cong \mathrm{WC}(K, A)$ (Proposition 3.3.21), η corresponds to a principal homogeneous space $V_{/K}$ for $A_{/K}$, in particular a projective variety. We want to prove that if $V(L) \neq \emptyset$, in fact $V(K) \neq \emptyset$

already. Let $\phi : V_{/K} \to \mathbb{P}^N$ be a projective embedding. If $p \in V(L)$, then $\phi(p) = (f_0(t) : \ldots : f_N(t))$ for some $f_i(t) \in K[t]$. By specializing to, say $t = 0$, we have $(f_0(0) : \ldots : f_N(0)) \in V(K)$. By Lemma 3.3.20 $V_{/K}$ represents the trivial class in $\mathrm{WC}^1(K, A)$. Since η (hence V) was arbitrary, we conclude that $\widetilde{H}^1(L/K, A) = 0$. For the general case, let $\{t_i\}_{i \in I}$ be a transcendence basis for L/K. Since (the coordinates of) a point $p \in V(L)$ would involve only finitely many of the t_i's, we can assume without loss of generality that L/K has a finite transcendence degree. Then, arguing by induction on the transcendence degree, we reduce to the case just considered: $L = K(t_1)$. □

We make the following *ad hoc* definition.

Definition 3.5.3. Let G be a commutative group, $n > 1$ be a positive integer, and $S \subset G[n]$. For $m \in \mathbb{Z}^+$, we say that S is *m-linearly independent over $\mathbb{Z}/n\mathbb{Z}$* if a linear dependence relation

$$a_1\eta_1 + \cdots + a_m\eta_m = 0, \quad a_i \in \mathbb{Z},\ \eta_i \in S$$

implies $a_i \equiv 0 (\mathrm{mod}\ n)$ for all $i = 1, \ldots, m$. We say that S is *linearly independent over $\mathbb{Z}/n\mathbb{Z}$* if it is m-linearly independent over $\mathbb{Z}/n\mathbb{Z}$ for all $m \in \mathbb{Z}^+$.

Lemma 3.5.4. *Let $\phi : G_K \to G_L$ be a homomorphism of commutative groups. Let $n > 1$ be a positive integer and $S \subset G_K[n]$ an infinite subset which is 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. If $\operatorname{Ker}\phi$ is finite, then there is a subset $S' \subset S$ such that $\phi(S')$ is infinite and 1-linearly independent over $\mathbb{Z}/n\mathbb{Z}$; i.e., every element of $\phi(S')$ has order n.*

Proof. By the Chinese Remainder Theorem, it suffices to consider the case where $n = q^a$ is a prime power of some prime q. Let $m = \#\operatorname{Ker}\phi$ and consider any $(m+1)$-element subset $\{\eta_1, \ldots, \eta_{m+1}\} \subset S$. There must be at least one of these η_i's such that $\phi(\eta_i) \in G_L$ has order q^a. If not, given that q is prime, we would have $q^{a-1}\eta_i = 0$, and since ϕ is a homomorphism, that

$$\phi(q^{a-1}\eta_i) = q^{a-1}\phi(\eta_i)$$

so $q^{a-1}\eta_i \in \operatorname{Ker}\phi$ for all i. By the Pigeonhole Principle, we must have $q^{a-1}\eta_i = q^{a-1}\eta_j$ for some $i \neq j$. But this contradicts the assumption that S is 2-linearly independent over $\mathbb{Z}/q^a\mathbb{Z}$.

Therefore, any subset of S with at least $m+1$ elements contains an element η such that $\phi(\eta)$ has order n. Since S is infinite, this constructs inductively an infinite subset $S' \subset S$ such that for every $\eta \in S'$, $\phi(S')$ has order n. □

Combining the previous results we are ready to state prove the "inductive argument":

Proposition 3.5.5. *Let $n > 1$ be a positive integer, K be a weak Mordell-Weil field, 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 every element of $\operatorname{Res}_{L/K}(S') \subset H^1(L, A)[n]$ has order n. Moreover, if each element of S has index n, then each element of $\operatorname{Res}_{L/K}(S')$ has index n.*

Proof. Let $\{t_1, \ldots, t_d\}$ a separating transcendence basis for L/K and put $K' = K(t_1, \ldots, t_d)$. The restriction map $\operatorname{Res}_{L/K} : H^1(K, A) \to H^1(L, A)$ factors as

$$H^1(K, A) \xrightarrow{\operatorname{Res}_{K'/K}} H^1(K', A) \xrightarrow{\operatorname{Res}_{L/K'}} H^1(L, A)$$

By Lemma 3.5.2, the restriction map $\operatorname{Res}_{K'/K}$ is an injection, so its image $S_1 = \operatorname{Res}_{K'/K}(S)$ is still infinite and 2-linearly independent over $\mathbb{Z}/n\mathbb{Z}$. By 3.3.39, K' is also a weak Mordell-Weil field, and since L/K' is finite and separable, it follows from Lemma 3.5.1 that $\operatorname{Ker}\operatorname{Res}_{L/K'}$ is finite. Then by Lemma 3.5.4, there is an infinite subset $S_2 \subset S_1$ such that $\operatorname{Res}_{L/K'}(S_2)$ is infinite and every element has order n in $H^1(L, A)$. Then $S' = \operatorname{Res}^{-1}_{K'/K}(S_2)$ has the desired property. Notice that if every element of S has index n, then every element of $\operatorname{Res}_{L/K}(S')$ has index at most n, but since the period divides the index (Proposition 3.3.15 (a)) it is at least n, hence equal to n. □

3.6 The proof of the main theorem

With all our preparations, the proof of our main theorem now follows easily:

Theorem 3.6.1. *Let K be a field finitely generated over $\mathbb{F}_p(t)$, and let $n > 1$ a positive integer $n > 1$. Then there exists an elliptic curve $E_{/K}$ such that there are infinitely many classes $\eta \in H^1(K, E)$ with $I(\eta) = P(\eta) = n$.*

Proof. If we consider K as being finitely generated over $\mathbb{F}_p$, since the latter is perfect, we can assume without loss of generality that $K/\mathbb{F}_p(t)$ is a separable field extension.

Let E be any elliptic curve over $k = \mathbb{F}_p(t)$ with $E(k) = 0$ and $Ш(k, E) = 0$ (take for example E the elliptic curve (2.8)). By Theorem 3.4.3 and Remark 3.4.4 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 element has period and index equal n. Finally, the inductive argument in Proposition 3.5.5 gives the desired result. □

Finally, since elements of $H^1(K, E)$ correspond to genus ones curves $C_{/K}$ (Propositions 3.3.21 and 3.3.25) we conclude

Corollary 3.6.2. *There are infinitely many genus one curves of any prescribed index over any field finitely generated over $\mathbb{F}_p(t)$.*

CHAPTER 4

Bibliography

[ASD73] M. Artin and H. P. F. Swinnerton-Dyer, *The Shafarevich-Tate conjecture for pencils of elliptic curves on $K3$ surfaces*, Invent. Math. **20** (1973), 249–266.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR 1045822 (91i:14034)

[BS15] Manjul Bhargava and Arul Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108.

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112.

[Cas63] ———, *Arithmetic on curves of genus 1. V. Two counterexamples*, J. London Math. Soc. **38** (1963), 244–248.

[Cas64] ———, *Arithmetic on curves of genus* 1*. VII. The dual exact sequence*, J. Reine Angew. Math. **216** (1964), 150–158.

[CL] Pete L. Clark and Allan Lacy, *There are infinitely many genus one curves of every index over every infinite, finitely generated field*, preprint.

[Cla06] Pete L. Clark, *There are genus one curves of every index over every number field*, J. Reine Angew. Math. **594** (2006), 201–206.

[Cla10] ———, *The period-index problem in WC-groups IV: a local transition theorem*, J. Théor. Nombres Bordeaux **22** (2010), no. 3, 583–606.

[GAT07] Cristian D. González-Avilés and Ki-Seng Tan, *A generalization of the Cassels-Tate dual exact sequence*, Math. Res. Lett. **14** (2007), no. 2, 295–302.

[Gro66] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki; Exp. No. 279, vol. 9, Soc. Math. France, Paris, 1964-1966.

[Gro68] ———, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam; Masson, Paris, 1968, pp. 88–188.

[Gro11] Benedict H. Gross, *Lectures on the conjecture of Birch and Swinnerton-Dyer*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 169–209.

[Kol88] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671.

[Kol91] Victor Alecsandrovich Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, pp. 429–436.

[Lic68] Stephen Lichtenbaum, *The period-index problem for elliptic curves*, Amer. J. Math. **90** (1968), 1209–1223.

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

[LT58] Serge Lang and John Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[Mil70a] J. S. Milne, *The Brauer group of a rational surface*, Invent. Math. **11** (1970), 304–307.

[Mil70b] ———, *Weil-Châtelet groups over local fields*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 273–284.

[Mil72] James S. Milne, *Addendum: "Weil-Châtelet groups over local fields" (Ann. Sci. École Norm. Sup. (4)* **3** *(1970), 273–284)*, Ann. Sci. École Norm. Sup. (4) **5** (1972), 261–264.

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533.

[Mil06] ———, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.

[Nér64] André Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Inst. Hautes Études Sci. Publ.Math. No. **21** (1964), 128.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[Ols70] Loren D. Olson, *Galois cohomology of cycles and applications to elliptic curves*, Amer. J. Math. **92** (1970), 75–85.

[O'N02] Catherine O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), no. 2, 329–339.

[Rub87] Karl Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), no. 3, 527–559.

[Sel51] Ernst S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362 (1 plate).

[Ser02] Jean-Pierre Serre, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author.

[Sha67] Stephen S. Shatz, *The cohomology of certain elliptic curves over local and quasi-local fields*, Illinois J. Math. **11** (1967), 234–241.

[Sha72] ———, *Profinite groups, arithmetic, and geometry*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972, Annals of Mathematics Studies, No. 67.

[Shi72] Tetsuji Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59.

[Shi90] ———, *On the Mordell-Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), no. 2, 211–240.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[SS10] Matthias Schütt and Tetsuji Shioda, *Elliptic surfaces*, Algebraic geometry in East Asia—Seoul 2008, Adv. Stud. Pure Math., vol. 60, Math. Soc. Japan, Tokyo, 2010, pp. 51–160.

[Ste02] William A. Stein, *There are genus one curves over $\mathbb{Q}$ of every odd index*, J. Reine Angew. Math. **547** (2002), 139–147.

[Szy04] Michael Szydlo, *Elliptic fibers over non-perfect residue fields*, J. Number Theory **104** (2004), no. 1, 75–99.

[Tat58] John Tate, *WC-groups over $\mathfrak{p}$-adic fields*, Séminaire Bourbaki; 10e année: 1957/1958. Textes des conférences; Exposés 152 à 168; 2e éd. corrigée, Exposé 156, vol. 13, Secrétariat mathématique, Paris, 1958.

[Tat63] ———, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm,1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[Tat66] ———, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Tat75] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

[Wat79] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979.

[Wei55] André Weil, *On algebraic groups and homogeneous spaces*, Amer. J. Math. **77** (1955), 493–512.

[Wei82] ———, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser, Boston, Mass., 1982, With appendices by M. Demazure and Takashi Ono. MR 670072 (83m:10032)

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.