8-5-2022 11:30 AM

Reduction of L-functions of Elliptic Curves Modulo Integers

Félix Baril Boudreau, *The University of Western Ontario*

Supervisor: Chris Hall, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Mathematics

Abstract

Let $\mathbb{F}_q$ be a finite field of size q, where q is a power of a prime $p \geq 5$. Let C be a smooth, proper, and geometrically connected curve over $\mathbb{F}_q$. Consider an elliptic curve E over the function field K of C with nonconstant j-invariant. One can attach to E its L-function $L(T, E/K)$, which is a generating function that contains information about the reduction types of E at the different places of K. The L-function of E/K was proven to be a polynomial in $\mathbb{Z}[T]$.

In 1985, Schoof devised an algorithm to compute the zeta function of an elliptic curve over a finite field by directly computing its numerator modulo sufficiently many primes ℓ. By analogy with Schoof, we consider an elliptic curve E over K with nonconstant j-invariant and study the problem of directly computing the reduction modulo ℓ of $L(T, E/K)$. In this work, we obtain results in two directions. Firstly, given an integer N different from p and an elliptic curve E with K-rational N-torsion, we give a formula for the reduction modulo N of the L-function of certain quadratic twists, extending a result from Chris Hall. We also give a formula relating the L-functions modulo 2 of any two quadratic twists of E, without any assumption on the K-rational 2-torsion. Secondly, given a prime $\ell \neq p$, we give, under some relatively general conditions, formulas for the reduction of $L(T, E/K)$ modulo ℓ.

Keywords: Elliptic Curve, Function Field, L-Function, Computing L-Function, Middle Extension Sheaf, Néron Model, Identity Component, Group of Components, Étale Cohomology

Summary for Lay Audience

The study of elliptic curves is a major area of research in the branch of number theory in mathematics. They are featured in the proof by Andrew Wiles of the famous Fermat's Last Theorem and are used in cryptography. They are smooth curves which can be represented inside some mathematical ambient space. Quite often, they can be essentially described by equations of the form $y^2 = x^3 + a \cdot x + b$, with x and y variables and a and b constants, for example $y^2 = x^3 + t \cdot x$. By replacing the variable t in the previous equation with different integers, we describe different kinds of curves. Most of the time, we get again an elliptic curve, but sometimes the curve is singular. For example, if we replace t by 0, we get the singular curve $y^2 = x^3$ with singularity at the point $(x, y) = (0, 0)$.

An important tool to study elliptic curves and which takes into account, for example, all the aforementioned substitutions of t by integer values in the equation $y^2 = x^3 + t \cdot x$ at the same time, is the L-function of this elliptic curve. A very famous and unsolved problem in number theory is the conjecture of Birch and Swinnerton-Dyer, which claims a profound relation between the points of an elliptic curve and its L-function. In practice, it is a very difficult task to even compute explicitly these L-functions. We are interested in those L-functions of the form $1 + a_1 \cdot T + \cdots + a_n \cdot T^n$, where $a_1, \cdots, a_n$ are integers. In some branch of number theory it is common to have L-functions of this form.

We explain how to directly compute algorithmically, in many interesting cases, and without knowing these integers to begin with, the remainders of the division by prime numbers of the $a_1, \cdots, a_n$. By doing so for enough prime numbers, we obtain the precise values of the $a_1, \cdots, a_n$ using the so-called Chinese remainder theorem. This thesis builds on the pioneering work of Chris Hall in 2003 and is inspired by an algorithm developed by René Schoof in 1985 to compute zeta functions of elliptic curves.

Acknowledgments

My first and sincere thanks goes to my supervisor Chris Hall. Thank you Chris for taking me where I was, for helping me build a general culture of number theory, elliptic curves and L-functions, for taking the time to teach me tools and help me develop skills that I needed to move forward in mathematics. Thank you for patiently listening, for sharing your contagious passion for your research and for your guidance. You have been a great mentor to me and I'm grateful to have learnt from you.

Thanks to Nicole Lemire, Ján Mináč, Marc Moreno Maza and Richard Griffon for accepting to be my Ph.D. examiners. Thank you for the energy and the time that you spent in reviewing my thesis and for the judicious comments that helped to improve the quality its content.

Thank you to the many friends and colleagues at Western for all the enjoyable time we spent together in these years of MSc. and PhD. In particular, thank you to Michal C. and Dennisse S.C., Maye C. M. and Sergio Z. C., Lore P. R. and Sergio C. R. and César B. M. .

Thanks to our WLA church family in London who received us with open arms, with whom we grew up, who prayed with us, helped us and encouraged us. In particular, thank you to B. and C. Postma, J.C. and J. Korten, J. and N. St-John, M. and R. St-John, L. and B. McElroy, K. and R. Magwood, M. and L. Jamieson, M. and W. Wright, A. and J. Hamilton, S. and S. Dueck., D. and J. Tembwe, J. Mitchell and S. Phillipson, R. Majoran, B. Worrad, R. Bell and R. Standish.

Merci à mes amis de l'ENS Lyon, de Jussieu et d'Orsay: Moustapha A., Hamza E., Mohamed V., Guillaume C., Yoël D., Lukas M. et Kien P. pour ces agréables moments et pour ces nombreuses conversations. J'ai beaucoup appris de vous.

Merci aussi à mes amis Joss et Riky Rakotobe pour tous ces beaux moments et pour votre soutien depuis le début de mes études universitaires.

Merci à ceux et celles qui m'ont offerts mes premières opportunités de recherche en mathématiques, pour m'encourager à continuer et pour m'avoir aidé à former ma pensée mathématique: Virginie Charette et Vasilisa Shramchenko (UdeS), Étienne Ghys (ENS Lyon) et Cédric Villani (IHP).

Gracias a Pedro Luis del Ángel (CIMAT) por tus números consejos y tu apoyo durante mi tesis. Gracias también a Cristhian Garay (CIMAT) por tu amistad y por tus consejos, y por todas esas conversaciones que tuvimos que me ayudaron a crecer como matemático.

Gracias a mi familia en México, Don Cruz, Doña Juanita, Gerardo, Victor y Sandy por ser una verdadera familia.

Merci maman, papa et Olivier pour votre amour inconditionnel et pour votre appui. Merci à Daniel pour ton aide et ton amour durant toute ces années.

Merci Matías pour tous ces moments de joie, pour ton amour et pour m'avoir permis de grandir en même temps que toi.

This thesis would not have been possible without the loving support, friendship and wise council of my wife Carolina. ¡Mi amor, esta tesis también es tuya!

Finally, nothing of this would have happen if it were not for the love and blessing of God. I'm sincerely grateful for the opportunity You gave me to pursue these studies. May they be used to glorify You. "Every good gift and every perfect gift is from above, coming down from the Father of lights, with whom there is no variation or shadow due to change." (James 1:17)

Contents

Chapter 1

Introduction

1.0.1 Motivation

Let $X/\mathbb{F}_q$ be a projective variety X defined over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. For each positive integer m, consider the set $X(\mathbb{F}_{q^m})$ of $\mathbb{F}_{q^m}$-rational points of X (i.e., those points of X which take value in the extension $\mathbb{F}_{q^m}$ of degree m of $\mathbb{F}_q$) and let $\#X(\mathbb{F}_{q^m})$ be the cardinality of such set. We can then define the *Hasse-Weil zeta function* of $X/\mathbb{F}_q$ as the following generating function

$$\mathrm{Z}(T, X/\mathbb{F}_q) := \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{q^m})}{m} T^m\right) \in \mathbb{Q}[[T]].$$

This definition was introduced by Emil Artin (for some affine algebraic curves over finite fields) in his thesis in 1921 (published in 1924 [1]). Now, let $|X|$ be the set of closed points of X and let d_v be the degree of the field extension of $\mathbb{F}_q$ by the residue field attached to v. By taking the formal logarithm of the generating function, we obtain an alternative description of the zeta function of $X/\mathbb{F}_q$ in terms of an Euler product:

$$\mathrm{Z}(T, X/\mathbb{F}_q) = \prod_{v \in |X|} \frac{1}{1 - T^{d_v}}.$$

Finally, it turns out that the zeta function of a projective variety $X/\mathbb{F}_q$ is rational function, i.e., it can be written as a ratio of polynomials. The rationality of the zeta function of a curve $X/\mathbb{F}_q$, together with a proof that it satisfies some functional equation goes back to Friedrich Karl Schmidt in 1931 [36]. The general case of a projective variety was proven by Bernard Dwork in 1960 using p-adic methods [13]. The rationality and the functional equation satisfied by a zeta function form, along with the *Riemann hypothesis* and the *Betti numbers*, the so-called *Weil's conjectures*, which were formulated by André Weil in 1949 [50] based on past evidence. This includes his own proofs of these conjectures in 1946 when $X/\mathbb{F}_q$ is a smooth projective curve or an Abelian variety [49] and the proof of the Riemann hypothesis in 1933 by Helmut Hasse when X is an elliptic curve [20],[43, p.143, V.2.4]. By an elliptic curve E over a field K, here $\mathbb{F}_q$, we mean a smooth projective curve of genus 1 defined over K, together with a K-rational point O. When embedded in the projective plane $\mathbb{P}^2_{\mathbb{F}_q}$, this point can be given the coordinates $O = [0 : 1 : 0]$. Under this embedding, if we assume moreover that the characteristic p is

different from 2 and 3, then E/K has an affine equation of the form

$$y^2 = x^3 + ax + b,$$

with $a, b \in K$, satisfying $4a^3 + 27b^2 \neq 0$. The rational form of the zeta function of an elliptic curve $E/\mathbb{F}_q$ is

$$\mathrm{Z}(T, E/\mathbb{F}_q) = \frac{\mathrm{L}(T, E/\mathbb{F}_q)}{(1-T)(1-qT)},$$

where $\mathrm{L}(T, E/\mathbb{F}_q)$ is the quadratic polynomial $1 - \alpha T + qT^2$, with α the integer $1 + q - \#E(\mathbb{F}_q)$.

If we want to compute the coefficient α in practice, we can test all pairs (x, y) in $\mathbb{F}_q \times \mathbb{F}_q$ and determine which ones satisfy the equation $y^2 = x^3 + ax + b$. As the size of q grows, this method becomes impractical. In 1985, René Schoof side-stepped this naive point-counting method [37]. He took advantage of the fact that α was bounded in absolute value by $2\sqrt{q}$ (Hasse's bound) and devised an algorithm to directly compute the reduction of α modulo any prime ℓ different from p. If one performs this algorithm for sufficiently many primes ℓ_i so that their product $\prod_i \ell_i$ is strictly larger than $4\sqrt{q}$, then α is completely determined by its reduction modulo $\prod_i \ell_i$, thanks to the Chinese remainder theorem.

The numerator $\mathrm{L}(T, E/\mathbb{F}_q)$ of $\mathrm{Z}(T, E/\mathbb{F}_q)$ has a cohomological origin. In fact, for any smooth projective variety $X/\mathbb{F}_q$, Alexander Grothendieck proved in 1964/1965 (in collaboration with Michael Artin and Jean-Louis Verdier) that the zeta function of X is a rational function [15]. In order to prove the result, Grothendieck (with others) developed the general framework of étale cohomology. In that setting, the numerator and the denominator of the zeta function are both products of characteristic polynomials of suitably defined Frobenius endomorphisms. The vector spaces they act on are étale cohomology groups. In fact, in [15] Grothendieck also defined general analogues of zeta functions of smooth projective varieties and proved their rationality, that they satisfied a functional equation and proved the conjecture about the Betti numbers. The Riemann hypothesis was proven by Pierre Deligne for the zeta function of X in 1974 [9] and in the above general context in 1980 [10]. Among the consequences of the results of [15], the L-function $\mathrm{L}(T, E/K)$ of an elliptic curve E defined over the function field K of a nice curve defined over $\mathbb{F}_q$ was proven to be a rational function. The L-function of E/K can be defined analogously to the zeta function of a curve, as a generating function and it also has a description as an Euler product [3, pp.365-366]. When the j-invariant $a^3/(4a^3 + 27b^2)$ of E/K is an element of K but not of $\mathbb{F}_q$, Deligne proved that $\mathrm{L}(T, E/K)$ is a polynomial in $1 + T \cdot \mathbb{Z}[T]$[24, p.11].

By analogy with Schoof, we study in this thesis the problem of directly computing the reduction of $\mathrm{L}(T, E/K)$ modulo an integer N not divisible by p.

1.0.2 Past Works

Not much had been done on this problem before the present work. However, the starting point of this project and the ground on which one can reasonably believe that Schoof's strategy is applicable to L-functions of elliptic curves defined over function fields with nonconstant j-invariant is the following key result by Chris Hall [18, p.133, Theorem 4].

Theorem. *Let $N \geq 2$ be an integer coprime with q and let $\mathcal{T}$ be a finite subgroup of $E(K)$ of cardinality N. If M^{sp}, resp. M^{ns}, resp. A denote the sets of places of K at which E has split*

multiplicative, resp. non-split multiplicative, resp. additive reduction, then

$$\mathrm{L}(T, E/K) \equiv \mathrm{Z}(T, C/\mathbb{F}_q)\mathrm{Z}(qT, C/\mathbb{F}_q) \times \prod_{v \in M^{sp}} (1 - q^{d_v} T^{d_v}) \times \prod_{v \in M^{ns}} \frac{(1 - T^{d_v})(1 - q^{d_v} T^{d_v})}{(1 + T^{d_v})} \times \prod_{v \in A} (1 - T^{d_v})(1 - q^{d_v} T^{d_v}) \bmod N.$$

We are aware of the following alternative approaches to the question of computing the L-function of an elliptic curve E/K with nonconstant j-invariant. Given sufficiently many Euler factors of $L(T, E/K)$ and an algorithm for computing the quadratic character of K_f/K, Salman Baig and Chris Hall show how to compute the Euler product for the twisted L-function $L(T, E_f/K)$ for any $f \in K$ [3]. To obtain the Euler factors, we end up necessitating for example, "naive" point-counting. In the direction of p-adic methods, one could think on the following idea, suggested by Andrew Sutherland (private communication). We can compute the zeta function of K and hope to adapt the work of Edgar Costa, David Harvey and Kiran S. Kedlaya [7] to compute the zeta function of the elliptic surface corresponding to E/K. This essentially determines the L-function of E/K.

1.0.3 Overview of the Results

Let k_0 be a finite field of order a power q of a prime $p \geq 5$ and let C_0/k_0 be a proper, smooth and geometrically connected curve with function field $K_0 = k_0(C_0)$. Let E be an elliptic curve over K_0 with nonconstant j-invariant.

This paper is divided into two principal parts, that we now outline.

In the first part we give, under some conditions, explicit formulas for the reduction of the L-function of quadratic twists of E modulo an integer $N \geq 2$. These results go beyond what Hall obtained in [18, p.133, Theorem 4], as we now explain.

Let $f \in K_0^\times$ be a generator of a quadratic extension $K_{f,0}$ of K_0. Denote by $U_{f,0}$, M_f, M_f^{sp}, M_f^{ns} and A_f the subsets of closed points of C_0 corresponding to the loci of good, resp. multiplicative, resp. of split multiplicative, resp. of non-split multiplicative, resp. of additive reduction of the quadratic twist E_f/K_0 of E/K_0. If v is a place of K_0 (equivalently a closed point of C_0), then we write $k_{v,0}$ for the residue field of v and d_v for the degree of the finite extension $k_{v,0}/k_0$. Let $M_{\mathrm{unr}}^{\mathrm{sp}}$ (resp. $M_{\mathrm{unr}}^{\mathrm{ns}}$) be the subset of M^{sp} (resp. M^{ns}), whose elements are unramified in $K_{f,0}$. Suppose that the group of K_0-rational points $E(K_0)$ contains a subgroup of order $N \geq 2$ with N coprime with q. Under these assumptions, our first main result gives an explicitly formula for the reduction of $L(T, E_f/K_0)$ modulo N.

Theorem A (Theorem 3.1.5)**.** Let $f \in K_0^\times$ be a generator of a quadratic extension $K_{f,0}$ of K_0 and let E_f/K_0 be the quadratic twist of E by f. Let χ be the quadratic character of the Galois group of $K_{f,0}/K_0$ and let $L(T, \chi)$ be the Artin L-function attached to χ. Let $N \geq 5$ be an integer coprime with q. Suppose that $E(K_0)$ contains a subgroup $\mathcal{T}$ of order N. Then,

$$L(T, E_f/K_0) \equiv L(T, \chi)L(qT, \chi) \times \frac{Q(T)}{P(T)} \bmod N,$$

where if $N \geq 5$, then

$$\frac{Q(T)}{P(T)} \equiv \prod_{v \in M_{\mathrm{unr}}^{\mathrm{sp}}} (1 + \varepsilon_v q^{d_v} T^{d_v}) \times \prod_{v \in M_{\mathrm{unr}}^{\mathrm{ns}}} \frac{(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + T^{d_v})}{m_v(T^{d_v})} \bmod N,$$

where

$$\varepsilon_v = \begin{cases} 1 & \text{if } v \in M_{\mathrm{inert}}, \\ -1 & \text{if } v \in M_{\mathrm{split}}, \end{cases} \quad \text{and} \quad m(T^{d_v}) = \begin{cases} 1 + T^{2d_v} & \text{if } v \in M_{\mathrm{inert}}, \\ (1 + T^{d_v})^2 & \text{if } v \in M_{\mathrm{split}}. \end{cases}$$

In Theorem 3.1.5 we also take into account the possibilities $N \in \{2, 3, 4\}$. In particular, we show in Corollary 3.1.11 that we recover the case $N = 2$ of [18, p.133, Theorem 4].

Let $f_1, f_2 \in K_0^\times$ and let E_{f_1}/K_0 and E_{f_2}/K_0 be the corresponding quadratic twists of E/K_0. The second main result describes precisely the reduction modulo 2 of the quotient of the L-functions of these quadratic twists.

Theorem B (Theorem 3.1.13)**.** Let $f_1, f_2 \in K_0^\times$ and set

$$U_{0,f_1,f_2} := \left(U_{0,f_1} \cap U_{0,f_2}\right) \cup \left(M_{f_1} \cap M_{f_2}\right) \cup \left(A_{f_1} \cap A_{f_2}\right).$$

Then

$$\frac{L(T, E_{f_1}/K_0)}{L(T, E_{f_2}/K_0)} \equiv \prod_{v \notin U_{0,f_1,f_2}} \frac{L(T^{d_v}, E_{f_2}/k_{v,0})}{L(T^{d_v}, E_{f_1}/k_{v,0})} \bmod 2.$$

Specializing Theorem B to $K_0 = k_0(t)$ puts emphasis on the computability of this formula.

Corollary A (Corollary 3.2.3)**.** Let q be a power of a prime $p \geq 5$ and let $K_0 = k_0(t)$. Suppose that E/K_0 has semistable reduction everywhere, with multiplicative reduction at $t = \infty$. Let $\Delta \in k_0[t]$ be the discriminant of a minimal Weierstrass equation for E and let $f \in k_0[t]$ be a square-free polynomial of even degree which is coprime with Δ. We have

$$\frac{L(T, E_f/K_0)}{L(T, E/K_0)} \equiv \prod_{v|f} (1 + a_v T^{d_v} + T^{2d_v}) \bmod 2,$$

where $a_v := 1 + q^{d_v} - \#E_v(k_{v,0})$ and where E_v is the elliptic curve over $k_{v,0}$ obtained from E by reducing modulo v the coefficients of that minimal Weierstrass equation. See Corollary 3.2.3 for a more general expression.

In section 3.3, we apply our formulas to an infinite family of quadratic twists of the so-called universal elliptic curve over the function field of the modular curve $X_1(5)/k_0$.

In subsection 3.3.3, we discuss the effort required to compute the reduction $L(T, E_f/K_0)$ modulo 2 for this previous elliptic curve. More precisely, we assume that f is a monic irreducible polynomial of even degree and coprime with the discriminant of a given Weierstrass equation. We compare the relative complexity of our formula and of a suitable version of the algorithm of Baig and Hall [3] to perform the same task. We find that our formula is by far more efficient.

This first principal part focuses on the description of the L-function of an elliptic curve as an Euler product.

In the second principal part of this paper, we take advantage of the étale cohomological description of L-functions by Grothendieck [23, Exposé X] to partially recover some results of the first part but also to obtain new ones. In the rest of this introduction, we adopt the convention that k_0 is a finite field of characteristic p, k is a fixed algebraic closure of k_0 and if C_0 is a curve over k_0, then C is the base change of C_0 to k. If K_0 is the function field of C_0, then $K := k(C)$ is the function field of C. Given a prime ℓ distinct from p, consider an elliptic curve E over K_0 with nonconstant j-invariant and such that the ℓ-torsion subgroup of its group $E(K_0)$ of K_0-rational points is reduced to the identity element.

Our goal is to write the reduction of $\mathrm{L}(T, E/K_0)$ modulo ℓ directly (i.e., without first computing $\mathrm{L}(T, E/K_0)$ in a way that allows an algorithmic computation of $\mathrm{L}(T, E/K_0)$ mod ℓ. Our strategy is as follows. Let $\mathcal{E}$ be the Néron model of E/K_0, which is an étale sheaf on C_0 with generic fiber E/K_0 and which satisfies some universal property. Let $\mathcal{E}[\ell]$ be its subgroup scheme of ℓ-torsion.

We first pullback the elliptic curve E to the finite Galois extension $K_{\ell,0} := K_0(E[\ell])$ of K_0 generated by the coordinates of the affine points of $E[\ell] := E(\overline{K_0})[\ell]$, where $\overline{K_0}$ is an algebraic closure of K_0. By construction, $E(K_{\ell,0})$ contains $E[\ell]$. As a consequence, the pullback of $\mathcal{E}[\ell]$ by a finite morphism π from $C_{\ell,0}$, the curve over k_0 corresponding to the function field $K_{\ell,0}$, to C_0, is a subsheaf of the constant étale sheaf $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$. The characteristic polynomials of the geometric Frobenius endomorphism acting on the first étale cohomology groups $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell])$ and $\mathrm{H}^1(C_{\ell,\text{ét}}, (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2})$ are key constituents of the étale cohomological description of the L-function of E modulo ℓ. However, the first cohomology group with coefficients in $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ has a particularly simple expression: two copies of $\mathrm{Jac}(C_\ell)(k)[\ell]$, the set of k-rational points of the ℓ-torsion subgroup of the Jacobian variety of C_ℓ.

The second step of our strategy is to relate the $\mathrm{Gal}(K_\ell/K)$-invariants $\mathrm{H}^1(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell])$ to $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell])$. The étale sheaf $\mathcal{E}[\ell]$ is an example of a middle extension sheaf (see Definition 4.3.2). It is in a more general setting involving a middle extension sheaf that we prove the desired relation of the second step. Given a group G and a G-module A, we let A^G be its submodule of G-invariants. We prove the following.

Theorem C (Theorem 4.2.5)**.** Let $\pi : U' \to U$ be a finite Galois covering of connected locally Noetherian schemes with Galois group G. Let $\overline{x}$ be a geometric point of U and choose a geometric point $\overline{x'}$ of U' whose image by π is $\overline{x}$. Let $\mathcal{F}$ be the locally constant sheaf with finite stalks on U corresponding to some continuous representation of $\pi_1(U, \overline{x})$ into a finite Abelian group A. Suppose that

(i) the continuous action of $\pi_1(U', \overline{x'})$ on A is trivial,

(ii) the group G has a normal subgroup H, which acts on A by restriction of the action of G on A, such that the orders of H and A are coprime and

(iii) the orders of G/H and A^H are coprime.

Then $\mathrm{H}^0(U_{\text{ét}}, \mathcal{F}) = A^G$ and there is a canonical isomorphism $\mathrm{H}^1(U_{\text{ét}}, \mathcal{F}) \xrightarrow{\sim} \mathrm{H}^1(U'_{\text{ét}}, \pi^*\mathcal{F})^G$.

The most general notion that we encounter in this thesis is the notion of $\mathbb{Z}/n\mathbb{Z}$-middle extension sheaf, by which we mean the following.

Definition 1.0.1. Let n be an integer different from $\mathrm{char}(k_0)$. An étale constructible sheaf $\mathcal{F}_0$ on C_0 with coefficients in $\mathbb{Z}/n\mathbb{Z}$ is called a $\mathbb{Z}/n\mathbb{Z}$-*middle extension sheaf* if given an inclusion morphism $j : U_0 \hookrightarrow C_0$ of any dense Zariski open subset U_0 of C_0, the adjunction morphism

$$\mathcal{F}_0 \to j_* j^* \mathcal{F}_0,$$

coming from the identity morphism on $j^*\mathcal{F}_0$, is an isomorphism.

In some cases, a $\mathbb{Z}/n\mathbb{Z}$-middle extension sheaf $\mathcal{F}$ corresponds to a continuous representation of an étale fundamental group on a free module A of finite rank r_A over $\mathbb{Z}/n\mathbb{Z}$.

Theorem D (Theorem 4.3.10)**.** Let $\pi : C' \to C$ be a finite morphism of connected curves over k. Let $j : U \hookrightarrow C$ be the inclusion of a connected dense Zariski open subset U of C such that the restriction morphism $\pi : U' := \pi^{-1}(U) \to U$ is a finite Galois covering with Galois group G. Let $\mathcal{F}$ be a $\mathbb{Z}/n\mathbb{Z}$-middle extension sheaf on $C_{\text{ét}}$ corresponding to a free $\mathbb{Z}/n\mathbb{Z}$-module A of finite rank r_A. Suppose that

(i) the sheaf $j^*\mathcal{F}$ is lisse on $U_{\text{ét}}$,

(ii) the sheaf $\pi^*\mathcal{F}$ isomorphic to the constant free $\mathbb{Z}/n\mathbb{Z}$-module of rank r_A and

(iii) the group G satisfies the assumptions of Theorem C.

For each v in the complement $Z := C - U$, choose exactly one point w_v in $Z' := \pi^{-1}(Z)$ lying over it and let $I(w_v|v)$ be the inertia group of the pair corresponding to these places. Then we have an exact sequence of Abelian groups

$$0 \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{F}) \to \left(\mathrm{Jac}(C')(k)[n]^G\right)^{\oplus r_A} \to \bigoplus_{v \in Z} \mathrm{H}^1\left(I(w_v|v), A\right) \to 0.$$

Under some conditions, $\mathrm{H}^1(C_{\text{ét}}, \mathcal{F})$ equals r_A copies of $\mathrm{Jac}(C)(k)[n]$. More precisely,

Corollary B (Corollary 4.3.14)**.** In the context of Theorem D, if for each $v \in Z$ the order of $I(w_v|v)$ is coprime with n, then

$$\mathrm{H}^1(C_{\text{ét}}, \mathcal{F}) \simeq \left(\mathrm{Jac}(C)(k)[n]\right)^{\oplus r_A}.$$

However, the pullback of $\mathcal{E}[\ell]$ to C_ℓ is not the constant sheaf $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ in general as we explain in section 4.8. We leave to future works the general situation.

The other key constituent needed to write the L-function modulo ℓ is the ℓ-torsion subgroup scheme $\Phi[\ell]$ of the group of components Φ. These objects are finite étale group schemes supported on subsets of Z, the finite subset of C whose points correspond to the places of K such that at each such place, the elliptic curve E/K has either multiplicative or additive reduction. The third step in our strategy is to describe the characteristic polynomial of the geometric Frobenius endomorphism Frob_q on the set of K-rational points of $\Phi[\ell]$. The sheaf $\Phi[\ell]$ decomposes into a finite direct sum of ℓ-torsion subgroups schemes of local groups of components, which are defined over the residue fields of the points of Z. These local groups can be computed by Tate's algorithm. We write $\prod_{\substack{v \in Z_0 \\ S}}$ to denote a product indexed over the closed points of Z_0 such that over them the elliptic curve E/K_0 has Kodaira symbol S. We obtain an expression for the characteristic polynomial of the geometric Frobenius endomorphism on $\Phi[\ell](Z)$.

Theorem E (Theorem 4.6.1)**.** Let E/K_0 be an elliptic curve with nonconstant j-invariant. The characteristic polynomial of Frob_q acting on $\Phi(Z)[\ell]$ is

$$\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[\ell]\right) = \prod_{v\in Z_0} \det\left(1 - \mathrm{Frob}_q^{d_v}\, T^{d_v}|\Phi_v(k_v)[\ell]\right).$$

More precisely, if $\ell \geq 5$, then

$$\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[\ell]\right) = \prod_{\substack{v\in Z_0\\ I_{\ell n}, n\geq 1}} (1 - T^{d_v}) \times \prod_{\substack{v\in Z_0\\ I_{\ell n,2}, n\geq 1}} (1 + T^{d_v}).$$

In Theorem 4.6.1 we also give formulas for $\ell \in \{2, 3\}$. A finite extension of function fields L_0/K_0 is said to be geometric if L_0 and K_0 have the same constant field k_0. Putting all these pieces together, and assuming that k_0 contains the ℓth roots of unity of k, we obtain the following.

Theorem F (Theorem 4.9.2)**.** Let E/K_0 be an elliptic curve with nonconstant j-invariant. Let $f \in K_0^\times \smallsetminus (K_0^{\times 2} \cup k_0^\times)$ be an element generating a geometric quadratic extension $K_{f,0}/K_0$ of Galois group G_f. Let E_f/K_0 be the corresponding quadratic twist of E/K_0. Assume that ℓ is a prime distinct from $\mathrm{char}(k_0)$. Suppose that $E(K_0)[\ell]$ is a 2-dimensional $\mathbb{F}_\ell$-vector space.

(*a*) If $\ell = 3$, then

$$\mathrm{L}(T, E_f/K_0) \equiv \det\left(1 - \mathrm{Frob}_q\, T|\,\mathrm{H}^1\left(C_{f,\text{ét}}, \pi^*\mathcal{E}_f[3]\right)^{G_f}\right) \times \prod_{\substack{v\in Z_0\\ I_{3n}, n\geq 1, IV, IV^*}} (1 - T^{d_v})$$
$$\times \prod_{\substack{v\in Z_0\\ I_{3n,2}, n\geq 1, IV_2, IV_2^*}} (1 + T^{d_v}) \bmod 3.$$

(*b*) If $\ell \geq 5$, then

$$\mathrm{L}(T, E_f/K_0) \equiv \det\left(1 - \mathrm{Frob}_q\, T|\,\mathrm{H}^1\left(C_{f,\text{ét}}, \pi^*\mathcal{E}_f[\ell]\right)^{G_f}\right) \times \prod_{\substack{v\in Z_0\\ I_{\ell n}, n\geq 1}} (1 - T^{d_v})$$
$$\times \prod_{\substack{v\in Z_0\\ I_{\ell n,2}, n\geq 1}} (1 + T^{d_v}) \bmod \ell.$$

Theorem G (Corollary 4.9.4)**.** Let $\pi : C_0' \to C_0$ be a k_0-finite morphism of geometrically connected curves defined over k_0. Let E/K_0 be an elliptic curve with nonconstant j-invariant and let ℓ be a prime distinct from $\mathrm{char}(k_0)$ for which $E(K_0)[\ell] = \{O\}$ and assume that $q \equiv 1 \bmod \ell$. Let G_ℓ be the Galois group of the extension $K_0(E[\ell])/K_0$. Suppose that the order of G_ℓ is not divisible by ℓ. Then

$$\mathrm{L}(T, E/K_0) \equiv \det\left(1 - \mathrm{Frob}_q\, T|\,\mathrm{H}^1\left(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell]\right)^{G_\ell}\right) \det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[\ell]\right) \bmod \ell,$$

where $\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[\ell]\right)$ is given by Theorem E.

In Theorem 4.9.3, we consider more possibilities for G_ℓ. See Proposition 4.7.3. Finally, we prove the following result which we could not find in the literature and therefore might be new.

Theorem H (Theorem 4.10.1)**.** Let C_0 be a proper, smooth, and geometrically connected curve over a finite field k_0 of characteristic $p \geq 5$ and let K_0 be the function field of C_0. Let E/K_0 be an elliptic curve with nonconstant j-invariant. If ℓ is a prime distinct from p for which k_0 contains μ_ℓ and if $E(K)[\ell] = \{O\}$, then

$$\mathrm{L}(T, E/K_0) \equiv \det\Big(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}^0[\ell])\Big) \bmod \ell.$$

This result is needed in the proof of Theorem G.

Chapter 2

Conventions, Notation and Prerequisites

2.1 Conventions and Notations

In this work, unless explicitly stated, we assume for simplicity that if a ring A (resp. a scheme X) is introduced, then it will be noetherian (resp. locally noetherian). The reader of this text is assumed to have some ease with the language of schemes as developed by Grothendieck. Suggested references are [25] and [44].

Throughout the thesis, we will use the following notation. If S is a finite set, then $\#S$ denotes its cardinality. Let G be a group and let A be a G-module. The *submodule of G-invariants*, denoted A^G, is the largest submodule of A on which G acts trivially. The *quotient module of G-coinvariants*, denoted A_G, is the is the largest quotient of A on which G acts trivially. Let H be a subgroup of G. We write $\mathrm{Res}(A)^G_H$ for the restriction of the G-module A to an H-module. If B is an H-module, we write $\mathrm{Ind}(B)^G_H$ for the induced G-module.

Let $\mathcal{G}$ be a group or a group scheme defined over a scheme X. Given an integer $n \geq 1$, if the multiplication-by-n map

$$\times n : \mathcal{G} \to \mathcal{G}$$

is defined, then we write $\mathcal{G}[n]$ for its the kernel.

We denote by k_0 a perfect field and by k a fixed algebraic closure of k_0. The letter p denotes 0 or a prime greater or equal to 5. We are mainly interested in the setting where k_0 is a finite field whose cardinality q is a finite power of $p \geq 5$. It will be explicitly stated at the beginning of a section if we assume that k_0 is a finite field. If no mention of this is made, the reader should assume that the field k_0 is only perfect.

A capital letter with subscript 0 such as K_0 denotes an *algebraic function field* over k_0. By this we mean a field extension K_0 of k_0 such that K_0 is a finite algebraic extension of $k_0(t)$ for some element $t \in K_0$ that is transcendental over k_0. If the field k_0 is finite, then K_0 is more specifically called a *global function field*. However, in this thesis all these objects will be called *function fields*. For a perfect field k_0, the *algebraic closure of k_0 in K_0* is a field called the *constant field of K_0*. If the constant field of K_0 equals k_0, then we say that K_0 is a *geometric*

function field. A function field with constant field k, a fixed algebraic closure of a perfect field k_0, is denoted by K. A fixed algebraic closure of K_0 is denoted by $\overline{K_0}$.

Given a place v of K_0, we write $K_{v,0}$ for the completion of K_0 at v, $k_{v,0}$ for the residue field attached to v and k_v for a fixed algebraic closure of $k_{v,0}$. We will work under the assumption that $k_{v,0}$ is a perfect field. If L_0 is a field among $k_0, k_{v,0}, K_0$ and $K_{v,0}$, then its absolute Galois group is denoted G_{L_0}. Note that since the fields k_0 and $k_{v,0}$ are perfect, then we have $G_{k_0} = \mathrm{Gal}(k/k_0)$ and $G_{k_{v,0}} = \mathrm{Gal}(k_v/k_{v,0})$.

A scheme defined over a field L_0 (where L_0 is k_0, K_0 or its derivatives as in the previous paragraph) almost always has a subscript 0 such as X_0/L_0. Its base change to L (which stands for k or K, respectively), $X_0 \times_{\mathrm{Spec}(L_0)} \mathrm{Spec}(L)$ is denoted X/L. The only exception to this rule are the elliptic curves, which we found convenient to denote E/L_0 and E/L for the base change of E to L. When the field over which the scheme is defined is clear from the context, we will sometimes write X_0, X and E. We write $|X|$ for the set of closed points of a scheme X.

Similarly, a (pre)sheaf over a scheme X_0/L_0 almost always has a subscript 0 such as $\mathcal{F}_0$. The pullback of $\mathcal{F}_0$ to X/L is denoted by $\mathcal{F}$. The exception to this rule is with the Néron model of E/L_0, its identity component $\mathcal{E}^0$, its group of components Φ and the n-torsion subgroup schemes of these group schemes: none of these will carry a subscript 0. However, the context will make it clear over which curve they are considered.

Finally, if a scheme is introduced and there is no mention that it could be defined over a given field, then the scheme is denoted without subscript 0, such as X. A (pre)sheaf over such scheme X is then also denoted without subscript 0, such as $\mathcal{F}$.

2.2 Prerequisites

For the convenience of the reader, we included prerequisites of algebraic geometry. We also provided useful notions of étale topology and étale cohomology by way of introduction to the subject or as a reminder.

2.2.1 Curves

Suggested references are [25] and [44]. Let k_0 be a perfect field.

Definition 2.2.1. A *curve* C_0 *over* k_0 is a scheme of finite type $C_0 \to \mathrm{Spec}(k_0)$ of pure dimension 1. We denote this C_0/k_0. We say that a curve C_0/k_0 is

- *proper* if the structure morphism $C_0 \to \mathrm{Spec}(k_0)$ is proper.
- *smooth* if the structure morphism $C_0 \to \mathrm{Spec}(k_0)$ is smooth at each point $v \in C_0$.
- *geometrically connected* (resp. *geometrically irreducible*) if for any field extension k' of k_0, the scheme $C_0 \times_{\mathrm{Spec}(k_0)} \mathrm{Spec}(k')$ is connected (resp. irreducible).

Remark 2.2.2. Because k_0 is perfect, to require the structure morphism $C_0 \to \mathrm{Spec}(k_0)$ to be smooth is equivalent to require it be *regular*. Namely that for each $v \in C_0$, the local ring $\mathcal{O}_{C_0,v}$ of Krull dimension 1 is regular [44, Tag 0B8X], i.e., if $\mathfrak{m}_v$ is the maximal ideal of $\mathcal{O}_{C_0,v}$ and $k_{v,0} := \mathcal{O}_{C_0,v}/\mathfrak{m}_v$ is its residue field, then $\dim_{k_{v,0}}(\mathfrak{m}_v/\mathfrak{m}_v^2) = 1$. Also, if the curve C_0/k_0 is smooth, then each of the local rings $\mathcal{O}_{C_0,v}$ is a discrete valuation ring [44, Tag 00D].

In our text, a curve C_0/k_0 will always be proper, smooth and geometrically connected.

Definition 2.2.3. Consider some morphisms of schemes $\phi : U \to \mathbb{A}^1_{\mathbb{Z}}, \psi : V \to \mathbb{A}^1_{\mathbb{Z}}$ defined on dense open subsets U, V of C_0. We say that ϕ is *equivalent* to ψ if $\phi|_W = \psi|_W$ for some dense open subset W of C_0 which is contained in $U \cap V$. This defines an equivalence relation. A *rational function* on C_0 is a *rational map* $f : C_0 \to \mathbb{A}^1_{\mathbb{Z}}$, i.e., an equivalence class defined by the above equivalence relation.

Definition 2.2.4. The set of rational functions on C_0 forms a ring $R(C_0)$, called the *ring of rational functions*. Since the scheme C_0 is integral, it has a unique generic point η and one can show that $R(C_0) = \mathcal{O}_{C_0,\eta} = \kappa(\eta)$ [44, Tag 01RV], where $\kappa(\eta)$ is the residue field of the local ring $\mathcal{O}_{C_0,\eta}$ (the two coincide in this case [44, Tag 00EU]). We denote $K_0 = k_0(C_0)$ the ring of rational functions and call it from now on the *function field* of C_0/k_0.

Definition 2.2.5. A *place* of K_0 is the maximal ideal of some valuation ring of K_0. We can associate to a place a discrete valuation v, so that the corresponding valuation ring is the discrete valuation ring $\mathcal{O}_{C_0,v}$ and $\mathfrak{m}_v$ is the maximal ideal. The *degree* of the place v is the degree of the (necessarily finite [45, p.6, Proposition 1.1.15]) residue field extension $k_{v,0} := \mathcal{O}_{C_0,v}/\mathfrak{m}_v$ of k_0.

Definition 2.2.6. The set $\widetilde{k_0}$ of elements of K_0 which are algebraic over k_0 is a subfield of K_0 which is an algebraic extension (even finite [45, p.7, Corollary 1.1.16]) of k_0. It is called the *constant field* of K_0. If $\widetilde{k_0} = k_0$, then K_0 is said to be a *geometric function field*.

Remark 2.2.7. We consider a curve C_0 which is integral and proper over a perfect field k_0. In particular, the curve C_0 is reduced over the perfect field k_0. Therefore, the curve C_0/k_0 is geometrically reduced [44, Tag 020I]. So we have a geometrically connected and geometrically reduced curve which is proper over k_0. Hence, $\mathrm{H}^0(C, \mathcal{O}_C) = k_0$ [25, p.105, 3.3.21] and so $k_0 = \widetilde{k_0}$. We say that k_0 is *algebraically closed* in K_0. Note also that $k_0 = \widetilde{k_0}$ is equivalent to C_0/k_0 being geometrically irreducible.

Remark 2.2.8. The category of proper, smooth curves over k_0 with nonconstant morphisms is equivalent to the category of finitely generated field extensions of k_0 of transcendence degree 1 [44, Tag 0BXX]. Under that equivalence, the closed points of C_0 correspond to the places of K_0. Because of this equivalence of categories, we will use in this text the terms *closed point* and *place* interchangeably.

Definition 2.2.9. Let C_0/k_0 be a proper, smooth and geometrically connected curve over a finite field k_0. Let $f \in K := k(C_0)$ and let $v \in C_0(k_0)$. The *order of f at v* is $\mathrm{ord}_v(f)$. If $\mathrm{ord}_v(f) > 0$ (resp. $\mathrm{ord}_v(f) < 0$) we say that f has a *zero* at v (resp. a *pole* at v). If $\mathrm{ord}_v(f) \geq 0$, then f is *defined* (or *regular*) at v and we can evaluate $f(v)$. Otherwise, f has a pole at v and we write $f(v) = \infty$.

Remark 2.2.10. Given a nonzero element $f \in K_0^\times$, there are only finitely many points v of $C_0(K_0)$ at which f has a pole or zero. In particular, if f has no poles, then $f \in k_0$. (the arguments in the proof of [43, p.18,II1.2] which are stated for K and k, but can be adapted to work in our setting). In fact, an element of $f \in K_0$ corresponds to a k_0-morphism of curves $f : C_0 \to \mathbb{P}^1$ [43, p.20, II.2.2].

Definition 2.2.11. Let $K_{f,0}/K_0$ be a quadratic extension of function fields generated by some element $f \in K_0^\times \setminus K_0^{\times 2}$. Let v be a place of K_0 and let w be a place of $K_{f,0}$ lying over v.

(a) The positive integer $e(w|v)$ with

$$\mathrm{ord}_w(\alpha) = e(w|v)\,\mathrm{ord}_v(\alpha) \quad \text{for all } \alpha \in K_0$$

is called the *ramification index* of w over v. We say that $w|v$ is ramified if $e(w|v) = 2$, and that $w|v$ is unramified if $e(w|v) = 1$.

(b) The degree of the finite field extension of residue fields $k_{w,0}/k_{v,0}$,

$$f(w|v) := [k_{w,0} : k_{v,0}]$$

is called the *(residue) degree* of w over v.

(c) If there are two distinct places of $K_{f,0}$ lying over v, then we say that v splits in $K_{f,0}$.

Remark 2.2.12. Let v be a place v of K_0 with degree d_v. If v is inert in a quadratic extension $K_{f,0}$ as above, then the unique place w of $K_{f,0}$ lying over v has degree $d_w = 2d_v$. If v is ramified in $K_{f,0}$, then the unique place w lying over it in $K_{f,0}$ has degree $d_w = d_v$. Finally, if v is split in $K_{f,0}$, then the two places w_1 and w_2 of $K_{f,0}$ lying over v have degree $d_{w_1} = d_{w_2} = d_v$.

2.2.2 Elliptic Curves

General Notions

We now introduce the main object of our studies and discuss some of its properties. References for this section are [25] and [43], from which we freely took definitions and properties. Note that [43] always assumed that the fields are perfect. However, the proofs we cite from this reference are also valid for function fields. We keep the notation from the previous subsection. In particular, K_0 is the function field of a proper, smooth and geometrically connected curve C_0/k_0, so that K_0 is a geometric function field. Let L_0 be a field.

Definition 2.2.13. An *elliptic curve defined over* L_0 is a pair $(E/L_0, O)$ comprised of a smooth projective curve E/L_0 of genus one and of an L_0-rational point $O \in E(L_0)$.

Proposition 2.2.14. *Let E/L_0 be an elliptic curve.*

(a) There exist functions $x, y \in L_0(E)$ such that the map

$$\phi : E \to \mathbb{P}^2_{L_0}, \phi = [x : y : 1]$$

gives an isomorphism E/L_0 onto a curve given by an affine equation of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

called an (affine) Weierstrass equation for E/L_0, with coefficients $a_1, a_2, a_3, a_4, a_6 \in L_0$ and satisfying $\phi(O) = [0 : 1 : 0]$.

(b) Any two Weierstrass equations for E/L_0 as in (a) are related by a linear change of variables of the form

$$X_2 = u^2X_1 + r \text{ and } Y_2 = u^2Y_1 + su^2X_1 + t,$$

with $u \in L_0^\times$ and $r, s, t \in L_0^\times$.

(c) Any smooth projective cubic given by a Weierstrass equation as in (a) is an elliptic curve defined over K_0 with base point $O = [0 : 1 : 0]$.

Proof. See [43, p.59,III.3.1]. □

Given a Weierstrass equation $W(x, y) = 0$ of an elliptic curve E/L_0, one can define its discriminant Δ_W and its j-invariant j_W [43, p.42]. If $W_1(x, y) = 0$ and $W_2(x, y) = 0$ are two Weierstrass equations for E/L_0, then there exists some $u \in \overline{K}^\times$ such that $u^{12}\Delta_{W_2} = \Delta_{W_1}$ and moreover $j_{W_1} = j_{W_2}$ [43, p.45, Table 3.1]. In particular, the j-invariant doesn't change throughout the isomorphism class of the elliptic curve and it doesn't depend on the chosen Weierstrass equation.

Definition 2.2.15. Let K_0 be a function field and let E/K_0 be an elliptic curve. We say that the j-invariant of E/K_0 is *nonconstant* if it is an element of $K_0 \setminus k_0$.

Remark 2.2.16. If the field L_0 is perfect, the smoothness of the curve E/L_0 is equivalent to its regularity (Remark 2.2.2). Moreover, the regularity of E/L_0 is equivalent to the nonvanishing of the discriminant of any Weierstrass equation of this elliptic curve [43, p.45, III.1.4(a)(i)].

Remark 2.2.17. If the characteristic of the field L_0, $\mathrm{char}(L_0)$, is different from 2 and 3, then an elliptic curve E/L_0 always [43, pp.42-43, III.1] has a Weierstrass equation of the form

$$E/L_0 : y^2 = x^3 + ax + b, \text{ with } a, b \in L_0.$$

In this case, the discriminant of the Weierstrass equation is $\Delta_W = -16(4a^3 + 27b^2)$ and the j-invariant is $j_W = -1728(4a)^3/\Delta_W$. As mentioned before, we can call the later quantity unambiguously *the j-invariant of E* and write $j(E)$ for j_W.

Given a fixed algebraic closure $\overline{L_0}$ of L_0, the set $E(\overline{L_0})$ of $\overline{L_0}$-rational points of E/L_0 is an additive abelian group whose neutral element is the point $O \in E(L_0)$. Moreover, for each algebraic field extension L_0' of L_0, the set of points of L'_0-rational $E(L'_0)$ a subgroup of $E(\overline{L_0})$ [43, p.51, III.2.2]. In particular, we have for each integer $m \in \mathbb{Z}$ a well-defined *multiplication-by-m* a nonconstant L_0-morphism $[m] : E/L_0 \to E/L_0$ of groups (sending O to O) given by

$$[m](P) = \begin{cases} P + P + \cdots + P(\text{ m terms}) & \text{if } m > 0, \\ O & \text{if } m = 0, \\ [-m](-P) & \text{if } m < 0, \end{cases}$$

for any $P \in E(L_0)$.

Definition 2.2.18. Let E/L_0 be an elliptic curve and let $m \geq 1$ be an integer. The m-torsion subgroup of $E(L_0)$, denoted $E(L_0)[m]$, is the set of points of $E(L_0)$ of order m:

$$E(L_0)[m] := \{P \in E(L_0) : [m]P = O\}.$$

The *torsion subgroup* of $E(L)$, denoted $E(L_0)_{\text{tors}}$, is the set of points of finite order:

$$E_{\text{tors}} := \cup_{m=1}^{\infty} E(L_0)[m].$$

Since E is defined over L_0, we write $E(L_0)[m]$, resp. $E_{\text{tors}}(L_0)$ the points of order m, resp. of finite order, in $E(L_0)$.

If K_0 is a function field, then group $E(K_0)$ is finitely generated by the Mordell-Weil theorem [42, p.230, III.6.1]. In particular, $E_{\text{tors}}(K_0)$ is a finite set. If E is an elliptic curve defined over a k_0 is a finite field, then the set $E(k_0)$ (and so in particular $E_{\text{tors}}(k_0)$) is necessarily finite.

Elliptic Curve Defined Over a Function Field

Now assume that L_0 is a function field K_0 of the form $k_0(C)$, where C_0 is a smooth, proper, and geometrically connected curve defined over a field k_0 which is either finite or a number field. Let E/K_0 be an elliptic curve. For each place v of K_0, let $K_{v,0}$ be the completion of K_0 at that place v and let ord_v be the discrete valuation associated to v. Let $\mathcal{O}_{C_0,v}$ be the local ring of $\mathcal{O}_{C_0}$ at v, which is also the discrete valuation ring

$$\mathcal{O}_{C_0,v} = \{\alpha \in k_{v,0} : \text{ord}_v(\alpha) \geq 0\}.$$

Its unique maximal ideal is

$$\mathfrak{m}_v = \{\alpha \in k_{v,0} : \text{ord}_v(\alpha) > 0\}$$

and the residue field is

$$k_{v,0} = \mathcal{O}_{C_0,v}/\mathfrak{m}_v.$$

Let π_v be a uniformizer for $\mathcal{O}_{C_0,v}$ so that $\mathfrak{m}_v = \pi_v \mathcal{O}_{C_0,v}$. Assume that the valuation ord_v is normalized with $\text{ord}_v(\pi_v) = 1$. Let $E/k_{v,0}$ be the pullback of the elliptic curve E/K_0 given by a chosen inclusion of fields $K_0 \hookrightarrow K_{v,0}$. Let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a Weierstrass equation for $E/K_{v,0}$. For any $u \in K_{v,0}^{\times}$, the substitution

$$(x, y) \mapsto (u^{-2}x, u^{-3}y)$$

sends the coefficient a_i to $u^i a_i$, for $i \in \{1, 2, 3, 4, 6\}$. Choosing $u = \pi_v^r$ for a large enough integer $r \geq 1$ guarantees that all the coefficients $u^i a_i$ belong to $\mathcal{O}_{C_0,v}$. The valuation $\text{ord}_v(\Delta_v)$ of the discriminant Δ_v associated to the Weierstrass equation with these coefficients $u^i a_i$ is nonnegative.

Definition 2.2.19. A Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2.1}$$

for $E/k_{v,0}$ is said to be *minimal* if $\text{ord}_v(\Delta_v)$ is minimized with respect to the condition that $a_1, a_2, a_3, a_4, a_6 \in \mathcal{O}_{C_0,v}$.

In light of the changes of variables of [43, p.45, Table 3.1], if a_1, a_2, a_3, a_4 and a_6 are all in $O_{C_0,v}$ and if $\mathrm{ord}_v(\Delta_v) < 12$, then the corresponding Weierstrass equation is minimal [43, p.186, VII.1.1]. Such minimal Weierstrass equation always exists for a given elliptic curve $E/K_{v,0}$ [43, p.186, VII.1.3(b)] and, by [43, p.186, VII.1.3(b)], is unique up to a change of variables

$$x = u^2x' + r, y = u^3y' + u^2sx' + t, u \in O^\times_{C_0,v}, r, s, t \in O_{C_0,v}.$$

Remark 2.2.20. Since we assume that $\mathrm{char}(K_{v,0}) \neq 2, 3$, by Remark 2.2.17, we can always have a Weierstrass equation of the form $y^2 = x^3 + ax + b$ with $a, b \in K_{v,0}$. Let Δ_v be the discriminant of this equation. By [43, p.45,III.1], the only changes of variables which preserve this form of Weierstrass equation are given by $(x, y) \mapsto (x/u^2, y/u^3)$ for some $u \in \overline{K_{v,0}}^\times$. The coefficients of the new Weierstrass equation are $u^{-4}a$ and $u^{-6}b$. Moreover, the discriminant of that second Weierstrass equation is $u^{-12}\Delta_v$. In particular, for a suitable choice of $u \in K^\times_{v,0}$, we can guarantee that $a, b \in O_{C_0,v}$ and $\mathrm{ord}_v(u^{-12}\Delta_v) = \mathrm{ord}_v(\Delta_v) - 12 < 12$ and so this Weierstrass equation is minimal.

Given a minimal Weierstrass equation for $E/K_{v,0}$ as in (2.2.1), the *reduction* of $E/K_{v,0}$ modulo $\mathfrak{m}_v$ (or π_v) is the curve denoted $E_v/k_{v,0}$ and obtained by reducing modulo π_v the coefficients of the minimal Weierstrass equation for $E/K_{v,0}$:

$$E_v/k_{v,0} : y^2 + a_{1,v}xy + a_{3,v}y = x^3 + a_{2,v}x^2 + a_{4,v}x + a_{6,v}.$$

An equation for $E_v/k_{v,0}$ is unique up to a change of variables as in the previous paragraph [43, p.187].

Definition 2.2.21. Let E/K_0 be an elliptic curve and let v be a place of K_0. We say that at v, E has

(a) *good reduction* if the curve $E_v/k_{v,0}$ is smooth.

(b) *multiplicative reduction* if the curve $E_v/k_{v,0}$ has a node.

(c) *additive reduction* if the curve $E_v/k_{v,0}$ has a cusp.

If the curve $E_v/k_{v,0}$ is not smooth, it is singular and we say more generally in the cases (b) and (c) that the reduction is *bad* at v. For the multiplicative reduction case, we moreover say that the reduction is *split* if the slopes of the tangents at the node are in $k_{v,0}$ and otherwise are *nonsplit*.

Definition 2.2.22. Let C_0/k_0 be a smooth, proper and geometrically connected curve with function field K_0. Let E/K_0 be an elliptic curve. The subset U_0 points of C_0 formed by the generic point and the closed points of C_0 at which E/K_0 has good reduction is a dense open subscheme of C_0. It is called the *locus of good reduction* of E/K_0. Its closed complement Z_0 in C_0 is called the *locus of bad reduction* of E/K_0.

Definition 2.2.23. Consider inside the locus of bad reduction Z_0 all closed points v according to their reduction types with respect to E/K_0. We write M, resp. M^{sp}, resp. M^{ns}, resp. A, for the divisor of points of multiplicative reduction, resp. of split multiplicative reduction, resp. of nonsplit multiplicative reduction, resp. of additive reduction.

The following definitions and facts will be needed in the proof of Lemma 2.4.5. Given a point $P \in E(k_{v,0})$, we can find homogeneous coordinates $P = [x_0 : y_0 : z_0]$ with $x_0, y_0, z_0 \in \mathcal{O}_{C_{0,v}}$. where at least one of these coordinates in $\mathcal{O}_{C_{0,v}}$ is nonzero. The reduced point $P_v = [x_{0,v} : y_{0,v} : z_{0,v}]$ therefore belongs to $E_v(k_{v,0})$ and there is a reduction map

$$E(K_{v,0}) \to E_v(k_{v,0}) : P \mapsto P_v.$$

The subset $E_{v,\mathrm{sm}}(k_{v,0})$ of the points of $E_v(k_{v,0})$ which are smooth forms a group [43, p.56, III.2.5 and p.105, Exercise 3.5]. Now, let $E_0(K_{v,0})$ be the subset of points of $E(K_{v,0})$ whose reduction is smooth and let $E_1(K_{v,0})$ be the kernel of the reduction map. In other words:

$$E_0(K_{v,0}) := \{P \in E(K_{v,0}) : P_v \in E_{v,\mathrm{sm}}(k_{v,0})\}$$
$$E_1(K_{v,0}) := \{P \in E(K_{v,0}) : P_v = O_v\}.$$

The definition of these two sets do not depend on the choice of the minimal Weierstrass equation [43, p.186, VII.1.3b]. There is a short exact sequence of abelian groups

$$0 \to E_1(K_{v,0}) \to E_0(K_{v,0}) \to E_{v,\mathrm{sm}}(k_{v,0}) \to 0, \tag{2.2.2}$$

where the map $E_0(K_{v,0}) \to E_{v,\mathrm{sm}}(k_{v,0})$ is the reduction modulo the uniformizer π_v [43, p.188, VII.2.1].

2.2.3 Quadratic Twists of an Elliptic Curve

In this subsection, we define the quadratic twists of elliptic curves and state some of its elementary properties. For more details, we refer to reader to [43, X.2 and X.5]. Let $(E/K_0, O)$ be an elliptic curve E defined over K_0 together with a rational point $O \in E(K_0)$.

Definition 2.2.24. A *twist of the elliptic curve* E/K_0 is the data of a second elliptic curve E'/K_0 together with an isomorphism of elliptic curves $\phi : E'/\overline{K} \to E/\overline{K}$ (so that ϕ sends $O_{E'}$ to O_E). On the set $\mathcal{T}(E/K_0)$ of twists of the elliptic curve E/K_0, we introduce the equivalence relation $\sim_{K_0}$ that two twists are equivalent if they are K_0-isomorphic and set

$$\mathbf{Tw}(E/K_0) := \mathcal{T}(E/K_0)/\sim_{K_0}.$$

The set $\mathrm{Aut}(E)$ of $\overline{K_0}$-automorphisms the group structure of the elliptic curve E/K_0 forms an abelian group [43, p.69]. Using twists of E/K_0, one can construct 1-cocycles in $\mathrm{Gal}(\overline{K_0}/K_0) \to \mathrm{Aut}(E)$ and moreover a canonical set bijection [43, p.319, X.2.2(c) and X.2.3]:

$$\mathbf{Tw}(E/K_0) \to \mathrm{H}^1(G_{K_0}, \mathrm{Aut}(E)).$$

Now, let

$$n := \begin{cases} 2 & \text{if } j(E) \neq 0, 1728, \\ 4 & \text{if } j(E) = 1728, \\ 6 & \text{if } j(E) = 0. \end{cases}$$

Then, there is a canonical isomorphism of $\mathrm{Gal}(\overline{K_0}/K_0)$-modules $\mu_n \xrightarrow{\simeq} \mathrm{Aut}(E)$ [43, p.104, III.10.2]. By group cohomology, we have a canonical group isomorphism $K_0^\times/K_0^{\times n} \xrightarrow{\simeq} \mathrm{H}^1(G_{K_0}, \mu_n)$.

Therefore, $\mathbf{Tw}(E/K_0)$ is canonically isomorphic to $K_0^\times/K_0^{\times n}$. In this thesis, an elliptic curve E/K_0 is assumed to have nonconstant j-invariant and so we are only concerned with the case $n = 2$. In this, situation, if we choose a Weierstrass equation of the form $y^2 = x^3 + ax + b$ for E/K_0 and an element $d \in K_0^\times$, then by [43, p.343, X.5.4], a representative E_d/K_0 of a class in $\mathbf{Tw}(E/K_0)$ corresponding to d mod $K_0^{\times 2}$ has a Weierstrass equation of the form

$$y^2 = x^3 + d^2ax + d^3b.$$

We call the elliptic curve E_d/K_0 the *quadratic twist of E/K_0 by d*. When $d = 1$, E_d/K_0 is precisely the "original" elliptic curve E/K_0.

The following observations will become handy in Chapter 3.

Lemma 2.2.25. *Let L_0 be any field of characteristic different from 2 and 3. Let E/K_0 be an elliptic curve, let $d \in K_0^\times$ and let E_d/K_0 be the corresponding quadratic twist. Choose a Weierstrass equation of the form $W : y^2 = x^3 + ax + b$ for E/K_0 and let Δ_W be its discriminant. The corresponding Weierstrass equation for E_d/K_0 is $W_d : y^2 = x^3 + d^2ax + d^3$ and we denote by Δ_{W_d} its discriminant. We have*

$$\Delta_{W_d} = d^6\Delta_W.$$

In particular, $j(E_d) = j(E)$.

Proof. The discriminant Δ_W is $-16(4a^3 + 27b^2)$, while

$$\Delta_{W_d} = -16(4(d^2a)^3 + 27(d^3b)^2) = d^6\Delta_W.$$

In particular,

$$j(E_d) = \frac{d^2a}{\Delta_{W_d}} = \frac{a}{\Delta_W} = j(E).$$

□

2.2.4 Proper Minimal Regular Model

We refer the reader to [42, IV.4]. In order to speak about the Néron model of an elliptic curve, which is one of the central objects of this text, we need to introduce the proper minimal regular model of an elliptic curve defined over a local field.

Let C_0/k_0 be a smooth proper and geometrically connected curve with function field K_0. Given a place v of K_0, let $\mathcal{O}_{C_0,v}$ be its discrete valuation ring, let $k_{v,0}$ be the fraction field of $\mathcal{O}_{C_0,v}$ and let $k_{v,0}$ be the (perfect by assumption) residue field.

Definition 2.2.26. An *arithmetic surface* over $\mathcal{O}_{C_0,v}$ is an integral, normal, excellent scheme $\mathcal{C}_0$ which is flat and of finite type over $\mathcal{O}_{C_0,v}$. Moreover, the generic fiber $\mathcal{C}_{0,\eta}$ is a regular connected projective curve $C_0/k_{v,0}$ and the special fiber $\mathcal{C}_{0,v}$ is a union of curves over the appropriate residue fields.

Remark 2.2.27. An excellent scheme is a scheme which can be covered by open affine subschemes Spec(R) for which the ring R is excellent [44, 07QS]. Examples of such rings include [44, Tag 07QW]: fields, noetherian complete local rings, the ring of integers $\mathbb{Z}$, Dedekind domains with fraction field of characteristic 0 and finite type ring extensions of any of these.

Let $E/k_{v,0}$ be an elliptic curve. From [42, p.317, IV.4.5], we can say the followings. There exists a regular arithmetic surface $C_{0,v} \to \mathrm{Spec}(O_{C_{0,v}})$, which is proper over $\mathrm{Spec}(O_{C_{0,v}})$ and whose generic fiber is isomorphic to $E/K_{v,0}$. The surface $C_{0,v}/\mathrm{Spec}(O_{C_{0,v}})$ is called a *proper regular model* for $E/K_{v,0}$. Since $E/K_{v,0}$ has genus 1, there exists a proper regular model $\mathcal{X}_{0,v} \to \mathrm{Spec}(O_{C_{0,v}})$ for $E/K_{v,0}$ which satisfies the following property: Let $C_{0,v} \to \mathrm{Spec}(O_{C_{0,v}})$ be a proper regular model for $E/K_{v,0}$. Fix an isomorphism $C_{0,v,\eta} \to \mathcal{X}_{0,v,\eta}$ between the generic fibers. Then the induced $C_{0,v,\eta}$-birational map $C_{0,v} \to \mathcal{X}_{0,v}$ is an $C_{0,v}$-isomorphism.

Definition 2.2.28. We call $\mathcal{X}_{0,v}/\mathrm{Spec}(O_{C_{0,v}})$ *the minimal proper regular model* for $E/k_{v,0}$. This surface is unique up to unique $\mathrm{Spec}(O_{C_{0,v}})$-morphism.

Let $E/K_{v,0}$ be an elliptic curve. Kodaira [21],[22] and Néron [31] have classified the different possible configurations of the irreducible components of the special fiber its minimal proper regular model. We adopt Kodaira's notation to describe the different types of configurations of the irreducible components. The broad classification of these symbols is as follows.

(i) Good reduction: I_0;

(ii) Multiplication reduction : $I_n, n \geq 1$;

(iii) Additive reduction : $II, III, IV, I_0^*, I_n^*, n \geq 1, IV^*, III^*, II^*$

See [42, pp.352-353, IV.8.2] for more details. In that reference, the residue field k_v is algebraically closed. In this thesis we will need to consider the case where the residue field $k_{v,0}$ is not algebraically closed. As the author of *loc. cit.* comments [42, p.353, 8.2.1], in this situation some irreducible components of the special fiber may not be geometrically irreducible. As a result, the absolute Galois group $G_{k_{v,0}}$ may act nontrivially on the k_v-irreducible components of the special fiber and then the $k_{v,0}$-irreducible components of the special fiber are the $G_{k_{v,0}}$-orbits. We carefully consider this situation in Theorem 4.6.1.

2.2.5 Étale Cohomology

Suggested references for this subsection are the books of Milne [26], Tamme [47] and Fu [14] as well as the Stacks Project [44]. The reader is also encouraged to consult the original sources SGA 1 [16], the third volume of SGA 4 [2], SGA 5 [23], the first volume of SGA 7 [17] and Deligne's SGA 4 1/2 [8].

Étale Topology

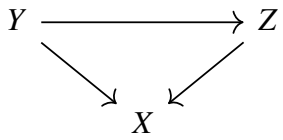
Definition 2.2.29. A morphism $f : X \to Y$ of schemes which is locally of finite type is said to be *étale* if it is *flat* and *unramified*. In other words, for each point $x \in X$, the induced map of local rings $f^{\#} : O_{Y,f(x)} \to O_{X,x}$ is local, turns $O_{X,x}$ into a flat $O_{Y,f(x)}$-module, it satisfies $f^{\#}(\mathfrak{m}_{Y,f(x)})O_{X,x} = \mathfrak{m}_{X,x}$ and the residue field $O_{X,x}/\mathfrak{m}_{X,x}$ is a finite separable field extension of the residue field $O_{Y,y}/\mathfrak{m}_{Y,y}$.

Example 2.2.30. A finite separable extension of fields L/K gives rise to an étale morphism $\mathrm{Spec}(L) \to \mathrm{Spec}(K)$. More generally, if K is a field and A is a commutative K-algebra which

is isomorphic to a finite product of finite separable extensions of K, then the morphisms $\mathrm{Spec}(A) \to \mathrm{Spec}(K)$ is an étale morphism. [26, p.27, I.3.2]. Such K-algebra A is called an *étale* K-algebra.

We now define the notion of étale site on a scheme X which will be the data of that scheme X together with a (pre)grothendieck topology since we want to talk about sheaves for the étale topology. Under our definition, an étale morphism is open [26, p.14, I.2.12] and an open immersion is étale [26, p.22, I.3.3(a)].

Definition 2.2.31 (Definition/Proposition)**.** Fix a scheme X. Consider the category $\text{Ét}/X$ whose objects are schemes Y with a fixed étale morphism to X and where a morphism from the fixed étale morphism $Y \to X$ to the fixed étale morphism $Z \to X$ is a commutative triangle as follows.



In particular, the morphism $Y \to Z$ is also étale [26, p.24, I.3.6]. An *étale covering* of an object $Y \to X$ of Ét/X is a family $\{g_i : U_i \to Y\}_{i\in I}$ of étale morphisms such that $Y = \cup_{i\in I} g_i(U_i)$. The category $\text{Ét}/X$ is closed under fiber products [26, p.22, I.3.3(c)] and given an object $f : Y \to X$ in $\text{Ét}/X$ and an étale morphism $g : U \to Y$, the composition $f \circ g : U \to X$ is an object of $\text{Ét}/X$ [26, p.22, I.3.3(b)]. It follows that the collection of étale coverings of objects in Ét/X satisfies the axioms of a *(pre-)grothendieck topology* and we call it the *étale topology* on $\text{Ét}/X$. Namely, the following three axioms are satisfied.

(i) If an étale morphism $Y \to X$ is an isomorphism, then $\{Y \to X\}$ is a covering.

(ii) If $\{U_i \to X\}_{i\in I}$ is an étale covering and $Y \to X$ is an étale morphism, then $\{U_i \times_X Y \to Y\}_{i\in I}$ is an étale covering.

(iii) If $\{U_i \to X\}_{i\in I}$ is an étale covering and if for each $i \in I$ the family $\{V_{i,j} \to U_i\}_{i,j\in J}$ is an étale covering for U_i, then the family $\{V_{i,j} \to X\}_{i\in I, j\in J}$ obtained by composition of morphisms is an étale covering for X.

The *(small) étale site* on X is the data, denoted $X_{\text{ét}}$, of the category $\text{Ét}/X$ together with the collection of coverings of objects of $\text{Ét}/X$.

We now define the notions of an étale presheaf and of an étale sheaf.

Definition 2.2.32 (Definition/Proposition)**.** Let X be a scheme. An *(abelian) presheaf* on the site $X_{\text{ét}}$ (or abelian étale presheaf on X) is covariant functor $\mathcal{F}$ from the opposite category $(\text{Ét}/X)^{\text{op}}$ to the category **Ab** of abelian groups.

Definition 2.2.33. Let X be a scheme. A presheaf $\mathcal{F} : (\text{Ét}/X)^{\text{op}} \to \mathbf{Ab}$ on $X_{\text{ét}}$ is a *sheaf* on $X_{\text{ét}}$ (or *étale sheaf* on X) if for any object $U \to X$ in $\text{Ét}/X$, the following two conditions hold.

(i) If $s \in \mathcal{F}(U)$ and if $\{U_i \to U\}_{i\in I}$ is an étale covering such that the restriction $s|_{U_i} = 0$ for each $i \in I$, then $s = 0$.

(ii) If $\{U_i \to U\}_{i\in I}$ is an étale covering and if we are given a family $(s_i)_{i\in I} \in \prod_{i\in I}\mathcal{F}(U_i)$ such that, for each $(i, j) \in I \times I$, the restriction of $s_i \in \mathcal{F}(U_i)$ to $U_i \times_U U_j$ is equal to the restriction of $s_j \in \mathcal{F}(U_j)$ to $U_i \times_U U_j$, then there exists $s \in \mathcal{F}(U)$ such that for each $i \in I$, the restriction of s to U_i equals s_i.

In other words, the diagram

$$\mathcal{F}(U) \longrightarrow \prod_{i\in I}\mathcal{F}(U_i) \rightrightarrows \prod_{i,j\in I}\mathcal{F}(U_i \times_U U_j),$$

where the arrow on the left is the restriction $s \mapsto (s|_{U_i})_{i\in I}$ and where the two parallel arrows are respectively given by $(s_i)_{i\in I} \mapsto \left(s_i|_{U_i\times_U U_j}\right)$ and $(s_i)_{i\in I} \mapsto \left(s_j|_{U_i\times_U U_j}\right)$, is an equalizer diagram in the category of abelian groups. The abelian sheaves on $X_{\text{ét}}$ form a category that we denote $\left(\widetilde{X_{\text{ét}}}\right)_{\mathbf{Ab}}$.

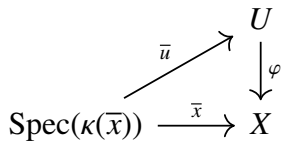
Remark 2.2.34. Just as with presheaves for the Zariski topology, one can associate an étale presheaf to obtain an étale sheaf [26, pp.61,62, 2.11],[47, pp.46-49, (3.1)].

We now introduce the notions of geometric point and of geometric stalk of a presheaf.

Definition 2.2.35. Let X be a scheme.

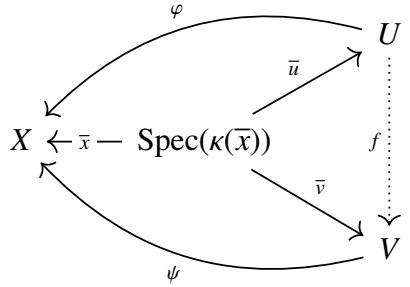
(i) A *geometric point* of X is a morphism $\mathrm{Spec}(k) \to X$, where k is an algebraically closed field. If the image in X of that morphism is the point x, then this morphism is denoted $\overline{x}$ and we write $\kappa(\overline{x})$ for k.

(ii) An *étale neighborhood* of a geometric point $\overline{x}$ of X is a commutative diagram



where $\overline{u}$ is a geometric point of U and φ is an étale morphism. As a shorthand, such étale neighbourhood is denoted $(U, \overline{u}) \to (X, \overline{x})$.

(iii) A *morphism of étale neighbourhoods* $(U, \overline{u}) \to (V, \overline{v})$ is an X-morphism $f : U \to V$ for which $\overline{v} = f \circ \overline{u}$:



Remark 2.2.36. Since φ and ψ are étale morphisms, the morphism f of étale neighbourhoods is also étale [26, p.24, I.3.6].

Definition 2.2.37. Let X be a scheme, let $\mathcal{F}$ a presheaf on $X_{\text{ét}}$ and let $\overline{x}$ be a geometric point of X. The *geometric stalk* of $\mathcal{F}$ at $\overline{x}$ is the colimit

$$\mathcal{F}_{\overline{x}} := \varinjlim_{(U,\overline{u})} \mathcal{F}(U),$$

where $(U, \overline{u})$ runs over all the étale neighbourhoods of $\overline{x}$ in X.

Definition 2.2.38. Let X be a locally noetherian scheme. A sheaf $\mathcal{F}$ on $X_{\text{ét}}$ is said to

(i) be *constant* if there exists an abelian group A such that $\mathcal{F}$ is the sheaf associated to the constant presheaf which sends an étale morphism $U \to X$ to A. In this case, by abuse of notation, we write A for $\mathcal{F}$.

(ii) be *locally constant*, if there exists an étale covering $\{U_i \xrightarrow{f_i} X\}_{i\in I}$ such that for each $i \in I$, the pulled back sheaf $f_i^*\mathcal{F}$ is constant on $U_{i,\text{ét}}$.

(iii) be *finite* if for each quasi-compact étale X-scheme U, the set $\mathcal{F}(U)$ is finite.

(iv) have *finite stalks* if for each geometric point $\overline{x}$ of X, the geometric stalk $\mathcal{F}_{\overline{x}}$ is finite.

Remark 2.2.39. If $\mathcal{F}$ is a constant sheaf corresponding to an abelian group A, then for each étale morphism $U \to X$, where U is connected, we have $A(U) = A$. Moreover, the sheaf A is represented by the X-scheme

$$\coprod_{a\in A} X_a,$$

where X_a is a copy of X.

Our next goal is to define a constructible sheaf.

Definition 2.2.40. A subset Z of a topological space X is called *constructible in* X if it can be written as a finite union

$$\bigcup_{i=1}^{n} (U_i \cap (X - V_i)),$$

where $U_i, V_i \subset X$ are open and retro-compact, i.e., if W is a quasi-compact open subset of X then the intersections $U_i \cap W$ and $V_i \cap W$ are also quasi-compact.

Definition 2.2.41. A subscheme Z of a scheme X is said to be *constructible in* X if the underlying topological space of Z is constructible in the underlying topological space of X.

Remark 2.2.42. Let X be a noetherian topological space. Then every open subset of X is quasi-compact and therefore retro-compact [44, Tag 04ZA]. Observing that every closed subset of X is retro-compact, we can characterize the constructible subsets of X as the finite unions of locally closed subsets [44, Tag 005L]. If X is a noetherian scheme, then each subscheme of X is constructible.

Definition 2.2.43. Let X be a scheme and let R be a noetherian ring. A sheaf $\mathcal{F}$ of sets or of abelian groups (resp. of R-modules) on $X_{\text{ét}}$ is *constructible* if every affine open subset $U \subset X$ has a decomposition into finitely many constructible reduced subschemes U_i of U such that for each i, $\mathcal{F}|_{U_i}$ is locally constant and has finite stalks (resp. is locally constant and each geometric stalk $\mathcal{F}_{\overline{x}}$ is a finitely generated R-module.)

Proposition 2.2.44. *Let X be a quasi-compact and quasi-separated scheme. Let $\mathcal{F}$ be a sheaf of sets or of abelian groups (resp. of R-modules if R is a noetherian ring) on $X_{ét}$. Then the following are equivalent.*

(i) $\mathcal{F}$ is constructible on $X_{ét}$.

(ii) There exists a finite decomposition of X into constructible reduced subschemes X_i such that for each i, $\mathcal{F}|_{X_i}$ is locally constant and has finite stalks.

Proof. The proofs are similar in each case. When $\mathcal{F}$ is a sheaf of sets, see [44, Tag 095E]. When $\mathcal{F}$ is a sheaf of abelian groups, see [47, p.155, (9.3.2) Proposition]. □

We now define some rings which appear frequently in the text. We will denote by $(A, \mathfrak{m}, k)$ the triple formed by a local ring A with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$.

Definition 2.2.45. Let $(A, \mathfrak{m}, k)$ be a local ring. The ring A is said to be

(i) *Henselian* if it satisfies Hensel's lemma, namely: for any monic polynomial $f \in A[t]$ and any $a \in A$ satisfying
$$f(a) \equiv 0 \bmod \mathfrak{m} \text{ and } f'(a) \not\equiv 0 \bmod \mathfrak{m},$$
there exists a unique element $\alpha \in A$ satisfying
$$\alpha \equiv a \bmod \mathfrak{m} \text{ and } f(\alpha) = 0.$$

(ii) *strictly Henselian* if it is Henselian and if moreover its residue field k is separably closed.

Example 2.2.46. A complete local ring is Henselian.

Proof. See [26, p.35, I.4.5]. □

Definition 2.2.47. Let $(A, \mathfrak{m}, k)$ be a local ring.

(i) The *henselization* of A is the datum of a local ring A^{h} together with a local morphism $\varphi : A \to A^{\mathrm{h}}$, such that A^{h} is Henselian and if $\psi : A \to B$ is a local morphism of local rings, then ψ factors uniquely through ϕ. In particular, if the pair (A^h, ϕ) exists, then it is unique up to isomorphism.

(ii) The *strict henselization* of A is the datum of a local ring A^{sh} together with a local morphism $\varphi : A \to A^{\mathrm{sh}}$, such that A^{sh} is a strictly Henselian ring and if $\psi : A \to B$ is a local morphism with H strictly Henselian, then ψ extends to a local morphism $\psi' : A^{\mathrm{sh}} \to H$. Moreover ψ' is uniquely determined once we give the induced morphism $A^{\mathrm{sh}}/\mathfrak{m}^{\mathrm{sh}} \to B/\mathfrak{m}_B$ on the residue fields.

Definition 2.2.48. An *étale neighbourhood of a local ring* $(A, \mathfrak{m}, k)$ is a pair $(B, \mathfrak{p}, k_{\mathfrak{p}})$ where B is an étale A-algebra and $\mathfrak{p}$ is a prime ideal of B lying over $\mathfrak{m}$ such that the induced morphism of residue fields $k \to k_{\mathfrak{p}}$ is an isomorphism.

Proposition 2.2.49. *Let $(A, \mathfrak{m}, k)$ be a local ring.*

(i) The henselization A^h of A exists.

(ii) The strict henselization A^{sh} of A exists.

Proof. (i) From [26, p.36, I.4.8], the étale neighbourhoods $(B, \mathfrak{p}, k_{\mathfrak{p}})$ of $(A, \mathfrak{m}, k)$ for which $\mathrm{Spec}(B)$ is connected form a filtered inductive system. We define

$$(A^{\mathrm{h}}, \mathfrak{m}^{\mathrm{h}}) := \varinjlim (B, \mathfrak{p}).$$

It satisfies all the desired properties. See [26, p.37].

(ii) We fix a separable closure k^{sep} of k and take the inductive limit $A^{\mathrm{sh}} := \varinjlim B$ over all commutative diagrams

$$\begin{array}{ccc} B & \longrightarrow & k^{\mathrm{sep}} \\ \uparrow & \nearrow & \\ A & & \end{array}$$

in which the morphism $A \to B$ makes B into an étale A-algebra.

□

Example 2.2.50. Let $(A, \mathfrak{m}, k)$ be a discrete valuation ring with perfect residue field k. Let K be the fraction field of A and K^{sep} be a fixed separable closure of K. Let O be the integral closure of A in K^{sep} and choose an ideal of $\mathfrak{n}$ of O lying over $\mathfrak{m}$. Let

$$\begin{aligned} D &:= \{\sigma \in G_K : \sigma(\mathfrak{n}) = \mathfrak{n}\}, \\ I &:= \{\sigma \in D : \sigma(x) - x \in \mathfrak{n} \text{ for all } x \in O\} \end{aligned}$$

be the corresponding decomposition and inertia groups. These groups act on O in the usual way.

(i) The henselization A^{sh} of A is the localization of O^D at the maximal ideal $\mathfrak{n} \cap O$.

(ii) The strict henselization A^{sh} of A is the localization of O^I at the maximal ideal $\mathfrak{n} \cap O$.

(iii) The maximal ideal $\mathfrak{m}^{\mathrm{h}}$ (resp. $\mathfrak{m}^{\mathrm{sh}}$) of A^{h} (resp. A^{sh}) is $\mathfrak{m}A^{\mathrm{h}}$ (resp. $\mathfrak{m}A^{\mathrm{sh}}$) and its residue field k^{h} (resp. k^{sh}) is k (resp. $\bar{k}$). Furthermore, the canonical morphism $\mathrm{Gal}(K^{\mathrm{sh}}/K^{\mathrm{h}}) \to G_k$ is an isomorphism.

Proof. See [42, p.332, IV.6.5]. □

The category $\left(\widetilde{X_{\text{ét}}}\right)_{\mathbf{Ab}}$ has enough injectives [26, p.83, III.1.1]. Moreover, the functor $\Gamma(X, \cdot) : \left(\widetilde{X_{\text{ét}}}\right)_{\mathbf{Ab}} \to \mathbf{Ab} : \mathcal{F} \mapsto \Gamma(X, \mathcal{F}) = \mathcal{F}(X)$ is left exact. Therefore, we have right derived functors $\mathrm{R}^i\Gamma(X, \cdot) =: \mathrm{H}^i(X_{\text{ét}}, \cdot) : \left(\widetilde{X_{\text{ét}}}\right)_{\mathbf{Ab}} \to \mathbf{Ab}$ and we call the abelian group $\mathrm{H}^i(X_{\text{ét}}, \mathcal{F})$ the ith étale cohomology group of $X_{\text{ét}}$ with values in $\mathcal{F}$.

Let X be a scheme, $i : Z \to X$ be a closed immersion of schemes and let $j : U \to X$ an open immersion of schemes, such that X is the disjoint union of $i(Z)$ and $j(U)$. Given a sheaf $\mathcal{F}$ on $X_{\text{ét}}$, we obtain a sheaf $i^*\mathcal{F}$ on $Z_{\text{ét}}$ and a sheaf $j^*\mathcal{F}$ on $U_{\text{ét}}$. Moreover, the sheaf $j_!j^*\mathcal{F}$ is the "extension by zero" of $j^*\mathcal{F}$ and the sheaf $i^!\mathcal{F}$ is the "subsheaf of sections with support on Z". We refer the reader to [26, p.76, II.2] for more details. There is then a short exact sequence

$$0 \to j_!j^*\mathcal{F} \to \mathcal{F} \to i_*i^*\mathcal{F} \to 0$$

of sheaves on $X_{\text{ét}}$ [26, p.76]. Now, the sheaf $i_*i^!\mathcal{F}$ is the largest subsheaf of $\mathcal{F}$ that is zero outside Z. In this situation, we have the following.

Definition 2.2.51 (Definition/Proposition)**.** The group

$$\Gamma(X, i_*i^!\mathcal{F}) = \Gamma(Z, i^!\mathcal{F}) = \ker\left(\mathcal{F}(X) \to \mathcal{F}(U)\right)$$

is called the *group of sections of $\mathcal{F}$ with support on Z*. The functor

$$\Gamma(Z, i^!(\cdot)) : \left(\widetilde{X_{\text{ét}}}\right)_{\mathbf{Ab}} \to \mathbf{Ab} : \mathcal{F} \mapsto \Gamma(Z, i^!\mathcal{F})$$

is left exact and for each integer $r \geq 0$, its right derived functors is denoted $H^r_Z(X, \cdot)$. The evaluation of such functor at $\mathcal{F} \in \left(\widetilde{X_{\text{ét}}}\right)_{\mathbf{Ab}}$, denoted $H^r_Z(X, \mathcal{F})$, is called *the rth cohomology group of $\mathcal{F}$ with support on Z.* For each integer $r \geq 0$, the functor $H^r_Z(X, \mathcal{F})$ is contravariant in (X, U).

Proposition 2.2.52. *For any sheaf $\mathcal{F}$ on $X_{ét}$, there is a long exact sequence,*

$$0 \longrightarrow (i^!\mathcal{F})(Z) \longrightarrow \mathcal{F}(X) \longrightarrow \mathcal{F}(U) \longrightarrow \cdots$$

$$\longrightarrow \mathrm{H}^r(X_{ét}, \mathcal{F}) \longrightarrow \mathrm{H}^r(U_{ét}, j^*\mathcal{F}) \longrightarrow \mathrm{H}^{r+1}_Z(X_{ét}, \mathcal{F}) \longrightarrow \cdots$$

Proof. See [26, p.92, III.1.25]. □

Let C_0/k_0 be a proper smooth connected curve (and in particular a complete variety). Consider an open immersion $j : U_0 \to C_0$ of an affine open U_0/k_0. Let $\mathcal{F}_0$ be a sheaf on $U_{0,\text{ét}}$. For each integer $r \geq 0$, we define the *rth cohomology group with compact support of $\mathcal{F}_0$ on U_0* as

$$\mathrm{H}^r_c(U_0, \mathcal{F}_0) := \mathrm{H}^r(C_0, j_!\mathcal{F}_0).$$

The Étale Fundamental Group

In this section we mention some facts that we will need about the étale fundamental groups. Suggested references are [16], [30] and [26].

Definition 2.2.53. A morphism of schemes $f : X \to Y$ is said to be

(i) *affine* if for each open affine subset U of Y, $f^{-1}(U)$ is an open affine subset of X.

(ii) *finite* if f is affine and if for every open affine subset U of Y, the ring $\Gamma\left(f^{-1}(U), \mathcal{O}_X\right)$ is a finite $\Gamma(U, \mathcal{O}_Y)$-algebra.

Let X be a connected scheme and let $\overline{x} : \mathrm{Spec}(\kappa(\overline{x})) \to X$ be a geometric point of X. Let FEt/X be the category of schemes over X with a fixed finite étale morphism to X. Define the *fiber functor*

$$F_{\overline{x}} : \mathrm{FEt}/X \to \mathrm{Set} : Y \mapsto \mathrm{Hom}_X(\mathrm{Spec}(\kappa(\overline{x})), Y).$$

This functor is strictly prorepresentable by which we mean that there exists a directed set I, a projective system $(X_i, \phi_{i,j})_{i,j \in I}$ in FEt/X where the transition morphisms $\phi_{i,j} : X_j \to X_i$ for $i \leq j$ are epimorphisms and there are elements $f_i \in F_{\overline{x}}(X_i)$ such that

(i) $f_i = \phi_{i,j} \circ f_j$, and

(ii) the natural map $\varinjlim \mathrm{Hom}(X_i, Z) \to F_{\overline{x}}(Z)$ induced by the f_i is an isomorphism for any $Z \to X$ in FEt/X.

Definition 2.2.54 (Definition/Proposition)**.** If $Y \to X$ is a morphism of schemes, then $\mathrm{Aut}_X(Y)$ will denote the group of X-automorphisms of Y which act on the right. Given the projective system $(X_i, \phi_{i,j})_{i,j\in I}$, we can define, for each $j \geq i$, a map

$$\psi_{i,j} : \mathrm{Aut}_X(X_j) \to \mathrm{Aut}_X(X_i)$$

by requiring that $\psi_{i,j}(\sigma) f_i = \phi_{i,j} \circ \sigma \circ f_j$. We define

$$\pi_1(X, \overline{x}) := \varprojlim_i \mathrm{Aut}_X(X_i).$$

A second choice $\overline{y}$ of geometric point of X yields an isomorphism $\pi_1(X, \overline{y}) \to \pi_1(X, \overline{x})$. This isomorphism is canonically determined up to an inner automorphism of $\pi_1(X, \overline{x})$.

Here is a concrete description of the étale fundamental group of a dense Zariski open affine subset of a curve.

Definition 2.2.55. Let G be a group and let S be a subset of G. The normal closure $\mathrm{ncl}_G(S)$ of S is the intersection of the normal subgroups of G which contain S:

$$\mathrm{ncl}_G(S) := \bigcap_{S \subseteq N \trianglelefteq G} N.$$

This is the smallest normal subgroup of G which contains S. This group is generated by the set of all conjugates of elements of S in G and so we can also write

$$\mathrm{ncl}_G(S) = \{g_1^{-1} s_1^{\varepsilon_1} g_1 \cdots g_n^{-1} s_n^{\varepsilon_n} g_n : n \geq 0, \varepsilon \in \{\pm 1\}, s_i \in S, g_i \in G\}.$$

Let C_0 be a curve over a field k_0 which is either finite of characteristic $p > 0$ or algebraically closed of characteristic $p \geq 0$. Let $K_0 = k_0(C_0)$ be the function field of C_0. Let U_0 be a dense Zariski open subset of C_0 and let

$$S = \bigcup_{v \in |U_0|} I(v),$$

then we have the short exact sequence

$$1 \to \mathrm{ncl}_{G_{K_0}}(S) \to G_{K_0} \to \pi_1(U_0, \overline{x}) \to 1, \tag{2.2.3}$$

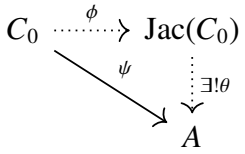
with $\overline{x}$ a chosen geometric point of a point $x \in U_0$.

The Jacobian Variety of a Curve

Definition 2.2.56. An abelian variety is a commutative, projective and geometrically integral algebraic group A defined over a field k_0.

Definition 2.2.57. Let C_0 be a curve a smooth, proper and geometrically connected curve of genus g defined over a field k_0. The Jacobian variety $\mathrm{Jac}(C_0)$ is an abelian variety over k_0 of dimension g.

If $C_0(k_0) \neq \emptyset$ it has the following universal properties. For any extension k'/k_0 there is a functorial isomorphism from $\mathrm{Jac}(C_0)(k')$ to $\mathrm{Pic}^0(C_0/k')$, the group of divisors on C_0 of degree 0, modulo linear equivalence. Given a point $P \in C_0(k_0)$, we have a well-defined map $\phi : C_0(k_0) \to \mathrm{Pic}^0(C_0/k_0)$ which sends a point $Q \in C_0(k_0)$ to the class of $Q - P$ in $\mathrm{Pic}^0(C_0/k_0)$. One can show that this map induces an injective morphism of varieties $\phi : C_0 \to \mathrm{Jac}(C_0)$. The morphism ϕ has the following universal property. Let A/k_0 be an abelian variety and let $\psi : C_0 \to A$ be a morphism which sends P to $0 \in A$. Then there is a unique homomorphism $\theta : \mathrm{Jac}(C_0) \to A$ of abelian varieties such that the following diagram commutes.



This property uniquely characterizes $\mathrm{Jac}(C_0)$. [39, p.98, § 3.11]. Without necessarily assuming that C_0 has a k_0-rational point, $\mathrm{Jac}(C_0)$ is an abelian variety representing the relative picard functor [5, p.244, 9.2/3].
We recall the following result.

Proposition 2.2.58. *Let k be an algebraically closed field. Let C be a smooth, proper and connected curve over k. Let n be a positive integer prime to* $\mathrm{char}(k)$*. Let μ_n be the sheaf on $C_{ét}$ corresponding to the nth-roots of unity. We have an isomorphism of abelian groups*

$$\mathrm{H}^1(C_{ét}, \mu_n) \simeq \mathrm{Jac}(C)(k)[n].$$

Proof. The algebraic curve C over k is normal over k and so quasi-projective over k [11, p.150, Chapitre II, Corollaire (7.4.10)]. Since the curve C is moreover proper over k, then it is projective over k [11, p.104, Chapitre II, Théorème (5.5.3)(ii)]. By [44, Tag 03RQ] there is an isomorphism $\mathrm{H}^1(C_{\text{ét}}, \mu_n) \simeq \mathrm{Pic}^0(C)[n]$ and the latter is isomorphic to $\mathrm{Jac}(C)(k)[n]$ by [28, p.168, §1. Definitions, Theorem 1.1]. Alternatively, see the proof of [2, pp.41-42, Exposé IX, Corollaire 4.7]. □

The ℓ-adic Sheaves

In this section, based on [23, Exposés V and VI] and [8, Exposé 2], we define the (constructible) $\mathbb{Z}_\ell$-sheaves and $\mathbb{Q}_\ell$-sheaves.

The $\mathbb{Z}_\ell$-Sheaves

Let X be a locally noetherian scheme. Let $\mathrm{Abc}(X)$ be the abelian category of constructible abelian sheaves on $X_{\text{ét}}$ and let $\mathrm{P} = \underline{\mathrm{Hom}}\,(\mathbb{N}^{\mathrm{op}}, \mathrm{Abc}(X))$ be the category of projective systems indexed by the ordered set $(\mathbb{N}, \geq)$ of nonnegative integers and with values in $\mathrm{Abc}(X)$.

Definition 2.2.59. Let $\mathcal{F} = (\mathcal{F}_n, u_n)_{n\geq 0}$ be an object of P. We say that $\mathcal{F}$ is an *ℓ-adic* sheaf if it satisfies the following two conditions.

(i) For any integer $n \geq 0$, $\ell^{n+1}\mathcal{F}_n = 0$.

(ii) For any pair of nonnegative integers (m, n) with $m \geq n$, the morphism

$$\mathbb{Z}/\ell^{n+1}\mathbb{Z} \otimes_{\mathbb{Z}} \mathcal{F}_m \to \mathcal{F}_n,$$

deduced from the composition of transition morphisms $\mathcal{F}_m \to \mathcal{F}_n$, is an isomorphism.

Remark 2.2.60. Let $\mathcal{F} = (\mathcal{F}_n)_{n\geq 0}$ be an ℓ-adic sheaf over X. For each integer $n \geq 0$, the condition $\ell^{n+1}\mathcal{F}_n = 0$ induces an action of the ring $\mathbb{Z}_\ell$ on $\mathcal{F}_n$. This yields an action of $\mathbb{Z}_\ell$ on $\mathcal{F}$. An ℓ-adic sheaf will alternatively be called a *$\mathbb{Z}_\ell$-sheaf*. The $\mathbb{Z}_\ell$-sheaves over X form a category.

Definition 2.2.61. Let $\mathcal{F} = \{\mathcal{F}_n\}_{n\geq 0}$ be a $\mathbb{Z}_\ell$-adic sheaf over X. The *geometric stalk* of $\mathcal{F}$ at a geometric point $\overline{x}$ of X is defined to be the projective limit of the geometric stalks at $\overline{x}$ of each $\mathcal{F}_n$:

$$\mathcal{F}_{\overline{x}} := \varprojlim_{n\geq 0} \mathcal{F}_{n,\overline{x}}.$$

Let $\mathcal{F} = (\mathcal{F}_n)_{n\geq 0}$ be a $\mathbb{Z}_\ell$-sheaf. The ith cohomology group of X with coefficients in $\mathcal{F}$ is defined to be the projective limit

$$\mathrm{H}^r(X, \mathcal{F}) := \varprojlim_{n\geq 0} \mathrm{H}^r(X_{\text{ét}}, \mathcal{F}_n).$$

2.2.6 The $\mathbb{Q}_\ell$-sheaves

The full subcategory of the category of $\mathbb{Z}_\ell$-sheaves over X that is generated by torsion constructible $\mathbb{Z}_\ell$-sheaves (i.e., those annihilated by a power of ℓ) is *thick*. By thick, we mean that given a short exact sequence

$$0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$$

in the category of $\mathbb{Z}_\ell$-sheaves over X, the sheaf $\mathcal{G}$ is a torsion sheaf if and only if both $\mathcal{F}$ and $\mathcal{H}$ are torsion sheaves.

Definition 2.2.62. The category of constructible $\mathbb{Q}_\ell$-sheaves over X is the quotient abelian category of the category of $\mathbb{Z}_\ell$ sheaves over X by the thick abelian subcategory of torsion $\mathbb{Z}_\ell$-sheaves. An object of that quotient category is called a *constructible $\mathbb{Q}_\ell$-sheaf*.

Remark 2.2.63. From [23, Exposé VI, pp.265-266], [8, Exposé 2, 2.9]: The $\mathbb{Q}_\ell$-sheaves are the same as the $\mathbb{Z}_\ell$-sheaves. Moreover, if $\mathcal{F}$ and $\mathcal{G}$ are two such sheaves, and if $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{F},\mathcal{G})$ (resp. $\mathrm{Hom}_{\mathbb{Q}_\ell}(\mathcal{F},\mathcal{G})$) denotes the set of morphisms from $\mathcal{F}$ to $\mathcal{G}$ in the category $\mathbb{Z}_\ell$-sheaves (resp. $\mathbb{Q}_\ell$-sheaves) over X, then we have

$$\mathrm{Hom}_{\mathbb{Q}_\ell}(\mathcal{F},\mathcal{G}) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{F},\mathcal{G}).$$

We often write $\mathcal{F} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ when we see a $\mathbb{Z}_\ell$-sheaf $\mathcal{F}$ as a $\mathbb{Q}_\ell$-sheaf. The geometric stalk of a $\mathbb{Q}_\ell$-sheaf $\mathcal{F} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ at a geometric point $\overline{x}$ of X is defined to be

$$(\mathcal{F} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)_{\overline{x}} := \mathcal{F}_{\overline{x}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Let X be a separated scheme of finite type defined over an algebraically closed field k and let $\mathcal{G}$ be a $\mathbb{Q}_\ell$-sheaf. By [8, Exposé 2, 2.8], we can write

$$\mathcal{G} = \mathcal{F} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

with $\mathcal{F}$ a torsion-free $\mathbb{Z}_\ell$-sheaf. We then set, for each integer $i \geq 0$,

$$\mathrm{H}^i(X,\mathcal{G}) := \mathrm{H}^i(X,\mathcal{F}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

2.3 The L-Function of an Elliptic Curve

We now introduce the main object of study of this thesis: the L-function of an elliptic curve E defined over a function field K_0. Recommended references are [23, Exposé XIV, §3] and [48].

Let C_0 be a smooth, proper and geometrically connected curve defined over a finite field k_0. Let K_0 be the function field of C_0/k_0. We assume that the field of constants k_0 has characteristic $\mathrm{char}(k_0) \geq 5$. Let E/K_0 be an elliptic curve. For each place v of K_0, we define the following integer.

$$a_v := \begin{cases} 1 + q^{d_v} - \#E_v(k_{v,0}) & \text{if } E/K_0 \text{ has good reduction at } v, \\ -1 & \text{if } E/K_0 \text{ has split multiplicative reduction at } v, \\ 1 & \text{if } E/K_0 \text{ has nonsplit multiplicative reduction at } v, \\ 0 & \text{if } E/K_0 \text{ has additive reduction at } v. \end{cases} \tag{2.3.1}$$

Definition 2.3.1. For each place v of K_0, we define the *local exponent of the conductor* at v to be the integer

$$n_v = \begin{cases} 0 & \text{if } E/K_0 \text{ has good reduction at } v, \\ 1 & \text{if } E/K_0 \text{ has multiplicative reduction at } v, \\ 2 & \text{if } E/K_0 \text{ has additive reduction at } v. \end{cases}$$

The *global conductor* of E/K_0 is the divisor $N(E/K_0) := \sum_{v \in |C_0|} n_v[v]$. Its degree is $\deg N(E/K_0) = \sum_v n_v \deg(v)$.

Definition 2.3.2. Given a formal indeterminate T, set

$$L_v(T) = \begin{cases} (1 - a_v T^{d_v} + q^{d_v} T^{2d_v})^{-1}, & \text{if } E/K_0 \text{ has good reduction at } v, \\ (1 - a_v T^{d_v})^{-1}, & \text{if } E/K_0 \text{ has bad reduction at } v. \end{cases}$$

We define L-function of E/K_0 is defined to be the Euler product

$$L(T, E/K_0) = \prod_{v \in |C_0|} L_v(T) \tag{2.3.2}$$

Moreover, if s is a complex number, define $L(s, E) := L(q^{-s}, E)$.

One can show [48, p.231] that the product $L(s, E)$ converges absolutely for $\mathrm{Re}(s) > 3/2$ and that it has a meromorphic continuation to all s.

The L-function of the elliptic curve E/K_0 can be also be written as a rational function using étale cohomology [23, Exposé XIV]. Now assume that the j-invariant of E/K_0 is nonconstant. It follows from the work of Grothendieck, Deligne and others [24, p.11] that $L(T, E/K_0)$ is a polynomial in $1 + T \cdot \mathbb{Z}[T]$. If we let g be the genus of the curve C_0/k_0, then the degree d of such polynomial equals

$$d = 2(2g - 2) + \deg N(E/K_0) = 2(2g - 2) + \deg(M) + 2\deg(A), \tag{2.3.3}$$

where M (resp. A) denotes the divisor of places of K_0 at which E/K_0 has multiplicative (resp. additive) reduction. Moreover, the L-function satisfies the following functional equation: There exists $\varepsilon\{-1, 1\}$, called the *sign* of the function equation, such that

$$L(T, E/K_0) = \varepsilon \cdot (qT)^d \cdot L\left(\frac{1}{q^2 T}, E/K_0\right). \tag{2.3.4}$$

Finally, for a complex number s, $L(q^{-s}, E/K_0)$ has all its zeroes on the real line $\mathrm{Re}(s) = 1$. See [24, p.11], [48, p.232, Theorem 9.3] and [18, p.134, Remark and Corollary 5] for more details.

Moreover, see Section 4.10 where, for an elliptic curve E/K_0 with nonconstant j-invariant, we give and prove in Theorem 4.10.1 an explicit description of $L(T, E/K_0)$ mod ℓ under the assumptions that $q \equiv 1 \bmod \ell$ and $E(K_0)[\ell] = \{0\}$.

2.4 Néron Model of an Elliptic Curve

2.4.1 Construction of the Néron Model of an Elliptic Curve

In this subsection we briefly discuss the notion of Néron model of an elliptic curve. The reader is encouraged to consult [5, Chapter 1], [25, Chapters 9 and 10] and [42, Chapters 3 and 4] for more details.

Let E/K_0 be an elliptic curve, where K_0 is the function field of a smooth, proper and geometrically connected curve C_0/k_0, where k_0 is a perfect field. Let η be the generic point of C_0. Recall that in this case the residue field k_η of η equals the function field K_0 (see section 2.2.1).

Definition 2.4.1. The *Néron model of E over C_0* is a scheme $\mathcal{E} \to C_0$ which is smooth [1] and separated, with generic fiber $\mathcal{E}_\eta := E \times_{C_0} \mathrm{Spec}(K_0)$ isomorphic to E/K_0, and that verifies the following universal property (called *Néron mapping property*): for any smooth scheme X_0 over C_0, the canonical

$$\mathrm{Mor}_{C_0}(X_0, \mathcal{E}) \to \mathrm{Mor}_{K_0}(X_0 \times_{C_0} \mathrm{Spec}(K_0), E)$$

is bijective.

Remark 2.4.2. If the scheme $\mathcal{E}$ exists, then this universal property implies that $\mathcal{E}$ is unique up to isomorphism. Now, the scheme $\mathcal{E} \times_{C_0} \mathcal{E}$ is smooth over C_0. Therefore, the universal property implies that the canonical map

$$\mathrm{Mor}_{C_0}(\mathcal{E} \times_{C_0} \mathcal{E}, \mathcal{E}) \to \mathrm{Mor}_{K_0}(E \times_{\mathrm{Spec}(K_0)} E, E)$$

is bijective. This implies that the structure of algebraic group of E extends uniquely to the structure of a group scheme on $\mathcal{E} \to C_0$.

We now briefly recall the construction of a global Néron model $\mathcal{E}$ over C_0 of an elliptic curve E/K_0. Since $\mathrm{char}(K_0) \neq 2, 3$ we can write a Weierstrass equation for E/K_0 in $\mathbb{P}^2_{K_0}$ in the form

$$W : Y^2Z = X^3 + aXZ^2 + bZ^3$$

with nonzero discriminant $\Delta_W = -16(4a^3 + 27b^2)$. For almost all closed points v of C_0, we have $a, b, \Delta_W, {\Delta_W}^{-1} \in \mathcal{O}_{C_0,v}$. So there exists a nonempty open subscheme $U_0 \subset C_0$ for which a, b, and Δ_E extend to sections of $\mathcal{O}_{C_0}(U_0)$ and such that $\Delta_W, 2$ and 3 are invertible in $\mathcal{O}_{C_0}(U_0)$. It follow that E/K_0 extends to a smooth projective family $\mathcal{E}'$ of elliptic curves in $\mathbb{P}^2_{U_0}$. Then $\mathcal{E}' \to I_0$ is a Néron model of E/K_0 by [5, p.19, 1.4/2]. For each closed point v of C_0 in the complement Z_0 of U_0, we construct a local Néron model $\mathcal{E}_v \to \mathrm{Spec}(\mathcal{O}_{C_0,v})$ of $E/K_{v,0}$ as the open subscheme of smooth points of the minimal regular model $\mathcal{X}_v \to \mathrm{Spec}(\mathcal{O}_{C_0,v})$ of $E/K_{v,0}$ (See section 2.2.4). The constructions of the $\mathcal{E}_v$'s can be done algorithmically via Tate's algorithm [42, pp.364-379, IV, §9]. The Néron model defined over U_0 can then be suitably glued with all the local Néron models defined over $\mathrm{Spec}(\mathcal{O}_{C_0,v})$, with v in Z_0, to obtain a global Néron model $\mathcal{E} \to C_0$ of E/K_0 [5, p.18, 1.4/1].

From [5, p.19, 1.4/3], the subset U_0 of C_0 consisting of the generic point and of all the closed points of C_0 at which E/K_0 has good reduction is a dense open subscheme of C_0.

Definition 2.4.3. The subscheme U_0 is called the *locus of good reduction* of E/K_0. Its closed complement Z_0 in C_0 is called the *locus of bad reduction* of E/K_0.

Remark 2.4.4. The sets U_0 and Z_0 are the same as in Definition 2.2.22.

2.4.2 The Group of Components Φ and the identity component $\mathcal{E}^0$ of $\mathcal{E}$

Given the algebraic variety $\mathcal{E}_v \to \mathrm{Spec}(k_{v,0})$, we have [25, p.495, Proposition 10.2.18(a),(b)], [25, p.496, Corollary 10.2.21] a unique scheme Φ_v, called the *group of components of* $\mathcal{E}_v$, which

[1] A smooth morphism is of finite type in [25, p.142, Definition 4.3.35].

is finite étale group scheme over $\mathrm{Spec}(k_{v,0})$, a surjective morphism $f_v : \mathcal{E}_v \to \Phi_v$ through which any $\mathrm{Spec}(k_{v,0})$-morphism from $\mathcal{E}_v$ to a finite étale $\mathrm{Spec}(k_{v,0})$-scheme factors uniquely. The set of rational points $\Phi_v(k_{v,0})$ corresponds to the set of connected components of $\mathcal{E}_v$ which are geometrically connected and there is a short exact sequence

$$0 \to \mathcal{E}_v^0 \to \mathcal{E}_v \xrightarrow{f_v} \Phi_v \to 0$$

of étale group schemes over $\mathrm{Spec}(k_{v,0})$, where $\mathcal{E}_v^0$ is the fiber $\mathcal{E}_{v,f_v(e)}$, with e the identity element of $\mathcal{E}_v$. This fiber is the connected component of that element and moreover, $\mathcal{E}_v^0$ is an open algebraic group scheme of $\mathcal{E}_v$. The *group of components* of $\mathcal{E}$ is then defined to be

$$\Phi := \bigoplus_{v \in Z} i_{v*}\Phi_v,$$

where $i_v : \mathrm{Spec}(k_{v,0}) \to C_0$ is the inclusion of the closed point v into C_0. This induces a surjective morphism $\mathcal{E} \to \Phi$ whose kernel $\mathcal{E}^0$, called the *identity component of* $\mathcal{E}$. We therefore have a short exact sequence of étale sheaves on C_0

$$0 \to \mathcal{E}^0 \to \mathcal{E} \to \Phi \to 0.$$

Since $\mathcal{E}$ is smooth over C_0 at the points of the identity section, then $\mathcal{E}^0$ is an open subgroup scheme of $\mathcal{E}$, which is smooth over C_0 [4, p.344, Exposé VI, Théorème 3.10 (i) implies (iv)].

2.4.3 The Prime-to-p-Torsion Injects into the Component Group

This subsection is devoted to prove a result that we believe must appear in the literature, but for which we were not able to find a reference. The proof we provide uses the language of Néron models introduced in the previous subsections. Compare with the proof of [18, p.132, Lemma 3].

Lemma 2.4.5. *Let $K_{v,0}$ be a field complete for a non-archimedean valuation* ord_v *and residue field $k_{v,0}$ of characteristic $p \geq 0$. Let $E/K_{v,0}$ be an elliptic curve with additive reduction. Then, the prime-to-p-torsion of $E(K_{v,0})$ injects into the group of components $\Phi_v(k_{v,0})$.*

Proof. If N is an integer coprime with p, then $E_1(k_{v,0})[N] = \{O\}$ [43, p.192, VII.3.1(a)] and since $E/k_{v,0}$ has additive reduction, then $E_{v,\mathrm{sm}}(k_{v,0})$ is isomorphic to the p-group $k_{v,0}$ [43, p.56, III.2.5 and p.105, Exercise 3.5]. Therefore, $E_{v,\mathrm{sm}}(k_{v,0})[N] = \{O\}$. In view of the short exact sequence (2.2.2):

$$0 \to E_1(K_{v,0}) \to E_0(K_{v,0}) \to E_{v,\mathrm{sm}}(k_{v,0}) \to 0$$

we deduce that $E_0(K_{v,0})[N] = \{O\}$. Now, there is a short exact sequence of abelian groups

$$0 \to E_0(K_{v,0}) \to E(K_{v,0}) \to E(K_{v,0})/E_0(K_{v,0}) \to 0.$$

Since $E_0(K_{v,0})[N] = \{O\}$, then $E(k_{v,0})[N]$ injects into $E(k_{v,0})/E_0(k_{v,0})$. Let $\mathcal{E}_{k_{v,0}}$ (resp. $\mathcal{E}^0_{k_{v,0}}$) be the special fiber of the Néron model $\mathcal{E}_v/\mathrm{Spec}(\mathcal{O}_v)$ of $E/K_{v,0}$, (resp. of the identity component $\mathcal{E}_v^0/\mathrm{Spec}(\mathcal{O}_v)$ of $\mathcal{E}_v/\mathrm{Spec}(\mathcal{O}_v)$), where $\mathcal{O}_v$ is the discrete valuation ring associated to v. Since the field $K_{v,0}$ is complete (and in particular Henselian), then

$$E(K_{v,0})/E_0(K_{v,0}) \simeq \mathcal{E}_{k_{v,0}}(k_{v,0})/\mathcal{E}^0_{k_{v,0}}(k_{v,0}) \simeq \Phi_v(k_{v,0}).$$

Therefore, the prime-to-p-part $\cup_{(N,p)=1} E(K_{v,0})[N]$ of $E(K_{v,0})$ injects in $\Phi_v(k_{v,0})$. □

Chapter 3

Analytic Approach

For the convenience of the reader, we recall some of the notation already introduced in Chapter 2 and fix some assumptions for the current chapter. Let q be a power of a prime $p \geq 5$. Let k_0 be a finite field of cardinality q. Let C_0/k_0 be a proper, smooth, and geometrically connected curve, with function field $K_0 := k_0(C_0)$. Let E/K_0 be an elliptic curve with nonconstant j-invariant. For each closed point $v \in |C_0|$, the residue field of v is denoted by $k_{v,0}$. This is a finite extension of k_0 of degree d_v, which we call the degree of v. The subset of points of C_0 formed by the generic point and all the closed points of C_0 over which E/K_0 has good reduction is denoted by U_0. It is an open dense subset of C_0. Its closed complement is the finite set Z_0. It is the set of places of K_0 over which E/K_0 has bad reduction. We write M, resp. M^{sp}, resp. M^{ns}, resp. A, for the divisor of points of multiplicative reduction, resp. of split multiplicative reduction, resp. of nonsplit multiplicative reduction, resp. of additive reduction.

3.1 Function Fields of Arbitrary Genus

Let $f \in K_0^\times \smallsetminus K_0^{\times 2}$ be a non-square element and let E/K_0 be an elliptic curve with nonconstant j-invariant. Modulo $K_0^{\times 2}$, the element f determines a unique quadratic extension $K_{f,0}$ of K_0 as well as a unique quadratic twist E_f/K_0 (2.2.3.)

Let $|C_0|_{\mathrm{split}}$ (resp. $|C_0|_{\mathrm{inert}}$, resp. $|C_0|_{\mathrm{ram}}$) be the subset of places of K_0 which are split (resp. inert, resp. ramified) in $K_{f,0}$, so that $|C_0| = |C_0|_{\mathrm{split}} \cup |C_0|_{\mathrm{inert}} \cup |C_0|_{\mathrm{ram}}$ is a disjoint union. For convenience, define $|C_0|_{\mathrm{unr}} := |C_0|_{\mathrm{split}} \cup |C_0|_{\mathrm{inert}}$ and if $S \in \{M^{\mathrm{sp}}, M^{\mathrm{ns}}, A\}$ and $r \in \{\text{inert, ram, split, unr}\}$, set $S_r := S \cap |C_0|_r$.

Definition 3.1.1. Let $f \in K_0^\times \smallsetminus K_0^{\times 2}$ and let $K_{f,0}$ be the quadratic extension of K_0 generated by f. Let G_f be the Galois group of this extension and let χ be the associated quadratic character. For each place v of K_0, set

$$L_v(T^{d_v}, \chi) := \begin{cases} (1 - T^{d_v})^{-1} & \text{if } v \in |C_0|_{\mathrm{split}}, \\ (1 + T^{d_v})^{-1} & \text{if } v \in |C_0|_{\mathrm{inert}}, \\ 1 & \text{if } v \in |C_0|_{\mathrm{ram}}. \end{cases}$$

The *Artin L*-function of χ is the formal Euler product

$$L(T, \chi) := \prod_{v \in |C_0|} L_v(T^{d_v}, \chi).$$

Remark 3.1.2. We have $v \in |C_0|_{\text{ram}}$ if and only if $\text{ord}_v(f)$ is odd.

We now prove two lemmas which will be used in the proofs of Theorems 3.1.5 and 3.1.13.

Lemma 3.1.3. *Let v be a place of K_0 and let w be a place of $K_{f,0}$ lying over v. For a given Kodaira symbol for $E/K_{v,0}$ at v, we describe the corresponding Kodaira symbols for $E_f/K_{v,0}$ and $E/K_{f,0,v}$.*

(a) If $v \in |C_0|_{unr}$, then E/K_0 and E_f/K_0 have the same reduction type (good, multiplicative, additive). Let f_v be the image of f via a chosen field injection $K_0 \hookrightarrow K_{v,0}$. Suppose that $E/K_{v,0}$ is given by a minimal Weierstrass equation of the form $y^2 = x^3 + a_v x + b_v$, with $a_v, b_v \in \mathcal{O}_{C_0,v}$ and let Δ_v be the discriminant of this Weierstrass equation. Suppose that E/K_0 has multiplicative reduction. Then E/K_0 and E_f/K_0 have the same splitting behaviour (split multiplicative or nonsplit multiplicative) if and only if the image of f_v is a square in the residue field $k_{v,0}$. In particular, if v splits in $K_{f,0}$, then E/K_0 and E_f/K_0 always have the same splitting behaviour.

(b) If $v \in |C_0|_{ram}$, then the Kodaira symbols of $E/K_{v,0}$ and $E_f/K_{v,0}$ are

$E/K_{v,0}$	I_0	$I_n, n \geq 1$	I_0^*	$I_n^*, n \geq 1$	II	III	IV	IV^*	III^*
$E_f/K_{v,0}$	I_0^*	$I_n^*, n \geq 1$	I_0	$I_n, n \geq 1$	IV^*	III^*	II^*	II	III

Proof. The corresponding Weierstrass equation for $E_f/K_{v,0}$ is

$$y^2 = x^3 + f_v^2 a_v x + f_v^3 b_v$$

This Weierstrass equation might not be minimal. However, there exists $u \in K_{v,0}^\times$ such that the change of variables $(x, y) \mapsto (x/u^2, y/u^3)$ will make the Weierstrass equation

$$y^2 = x^3 + (f_v/u^2)^2 a_v x + (f_v/u^2)^3 b_v$$

minimal. The discriminant of this Weierstrass equation is $(f_v/u^2)^6 \Delta_v$. In particular,

$$(f_v/u^2)^2 a_v, (f_v/u^2)^3 b_v, (f_v/u^2)^6 \Delta_v \in \mathcal{O}_{C_0,v},$$

and so all these quantities have nonnegative v-adic valuation. Thus, multiplying by a square of a u unit in $K_{v,0}$, we can assume that

$$y^2 = x^3 + f_v a_v x + f_v^3 b_v$$

is minimal and that f_v is a unit in $K_{v,0}$, in which case $\text{ord}_v(f_v) = 0$, or that f_v is the power $\pi_v^{\text{ord}_v(f)}$ of a normalized uniformizer π_v (with $\text{ord}_v(\pi_v) = 1$).

For part (a) $v \in |C_0|_{\text{unr}}$ and so $\text{ord}_v(f)$ is even. So for this part of the lemma we can assume that f_v is a unit with $\text{ord}_v(f_v) = 0$. We have

$$\text{ord}_v(f_v^6 \Delta_v) = \text{ord}_v(\Delta_v) \text{ and } \text{ord}_v(f_v^2 a_v) = \text{ord}_v(a_v).$$

Since both $y^2 = x^3 + a_v x + b_v$ and $y^2 = x^3 + f_v a_v x + f_v^3 b_v$ are minimal Weierstrass equations, then [43, p.196, VII.5.1] immediately tells us that E/K_0 and E_f/K_0 have the same reduction type

(good, multiplicative, additive) at v. Now assume that $v \in M$, so that $v \in M_f$. From [3, p.364, Lemma 2.1], we know that $v \in M_f^{\mathrm{sp}}$ if and only if the image of $6f_v^3 b_v$ in the residue field $k_{v,0}$ is a square and that $v \in M^{\mathrm{sp}}$ if and only if the image of $6b_v$ in the residue field $k_{v,0}$ is a square. This shows that if f_v is a unit in $k_{v,0}$, then E/K_0 and E_f/K_0 have the same splitting behaviour at the place of multiplicative reduction v (either both split or both nonsplit) if and only if the image of f_v in the residue field $k_{v,0}$ is a square and otherwise that they have opposite splitting behaviours.

The residue field $k_{v,0}$ is obtained from k_0 by adding a square-root of the f_v. If v splits in $K_{f,0}$, then the residue field $k_{v,0}$ is k_0 and the image of f_v is a square in k_0. If v is inert in $K_{f,0}$, then $k_{v,0}$ is a quadratic extension of k_0 and in this case, the image of f_v in $k_{v,0}$ might or might not be a square.

For part (b) we can assume that f_v is a normalized uniformizer, so that $\mathrm{ord}_v(f_v) = 1$. Therefore,

$$\mathrm{ord}_v(f_v\Delta_v) = 6 + \mathrm{ord}_v(\Delta_v).$$

It follows from [42, p.365, Table 4.1] that we have

$E/k_{v,0}$	I_0	$I_n, n \geq 1$	I_0^*	$I_n^*, n \geq 1$	II	III	IV	IV^*	III^*
$E_f/k_{v,0}$	I_0^*	$I_n^*, n \geq 1$	I_0	$I_n, n \geq 1$	IV^*	III^*	II^*	II	III

.

□

Lemma 3.1.4. *Let $v \in |U_0|_{unr}$. Let $\chi : k_{v,0}^\times \to \{\pm 1\}$ be the unique character of order 2 defined by $\chi_v(a) = 1$ if and only if a is a square in $k_{v,0}$ and extend χ_v to $k_{v,0}$ by setting $\chi_v(0) = 0$.*

Let $E_v(k_{v,0})$ and $E_{f,v}(k_{v,0})$ be the sets of $k_{v,0}$-rational points of the elliptic curves defined over $k_{v,0}$ obtained by reduction of $E/K_{v,0}$ and $E_f/K_{v,0}$. Then,

$$\#E_v(k_{v,0}) + \#E_{f,v}(k_{v,0}) \equiv 0 \bmod 2.$$

Proof. Write a Weierstrass equation $y^2 = \alpha(x)$ for $E_v/k_{v,0}$. Then, by [43, p.139, V.1.3] we have

$$\#E_v(k_{v,0}) = 1 + q^{d_v} + \sum_{x \in k_{v,0}} \chi_v(\alpha(x)).$$

A corresponding Weierstrass equation for $E_{f,v}/k_{v,0}$ is given by $y^2 = f_v^{-1}\alpha(x)$ and by the same reference, we have

$$\#E_{f,v}(k_{v,0}) = 1 + q^{d_v} + \sum_{x \in k_{v,0}} \chi_v\left(f_v^{-1}\alpha(x)\right) = 1 + q^{d_v} + \sum_{x \in k_{v,0}} \chi_v(\alpha(x)).$$

Since $q \equiv 1 \bmod 2$, we see that by summing the two expressions and then reducing their sum modulo 2 gives the desired result. □

Suppose that the group of K_0-rational points $E(K_0)$ contains a subgroup of order $N \geq 2$ with N coprime with q. Under these assumptions, our first main result gives an explicit formula for the reduction of $L(T, E_f/K_0)$ modulo N.

Finally, let χ be the quadratic character associated with the extension $K_{f,0}/K_0$ and let $L(T,\chi)$ be its Artin L-function.

Theorem 3.1.5. *Suppose that $E(K_0)$ contains a subgroup $\mathcal{T}$ of order $N \geq 2$ with N coprime with q. Then,*

$$L(T, E_f/K_0) \equiv L(T,\chi)L(qT,\chi) \times \frac{Q(T)}{P(T)} \bmod N,$$

where if $N \geq 5$, then

$$\frac{Q(T)}{P(T)} \equiv \prod_{v \in M_{unr}^{sp}} (1 + \varepsilon_v q^{d_v} T^{d_v}) \times \prod_{v \in M_{unr}^{ns}} \frac{(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + T^{d_v})}{m_v(T^{d_v})} \bmod N,$$

and if $N \in \{2, 3, 4\}$, then

$$\begin{aligned}\frac{Q(T)}{P(T)} \equiv & \prod_{v \in M_{unr}^{sp}} (1 + \varepsilon_v q^{d_v} T^{d_v}) \times \prod_{v \in M_{unr}^{ns}} \frac{(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + T^{d_v})}{m_v(T^{d_v})} \\ & \times \prod_{v \in A_{unr}} (1 + \varepsilon_v T^{d_v})(1 + \varepsilon_v q^{d_v} T^{d_v}) \\ & \times \gamma_{ram} \bmod N,\end{aligned}$$

where

$$\varepsilon_v = \begin{cases} 1 & \text{if } v \in M_{inert} \cup A_{inert}, \\ -1 & \text{if } v \in M_{split} \cup A_{split}, \end{cases} \quad \text{and } m(T^{d_v}) = \begin{cases} 1 + T^{2d_v} & \text{if } v \in M_{inert}, \\ (1 + T^{d_v})^2 & \text{if } v \in M_{split}, \end{cases}$$

$$\gamma_{ram} := \begin{cases} 1, & \text{if } N = 3, \\ \prod\limits_{\substack{v \in A_{ram} \cap U_f \\ A_{ram} \text{ is } I_0^*}} (1 - T^{d^v})^{-1}(1 - q^{d_v} T^{d_v})^{-1} \times \prod\limits_{\substack{v \in A_{ram} \cap U_f \\ A_{ram} \text{ is } I_n^*, n \geq 1}} (1 + \alpha_v T^{d_v})^{-1}, & \text{if } N = 2, 4, \end{cases}$$

where

$$\alpha_v = \begin{cases} -1, & \text{if } w \text{ is split multiplicative}, \\ 1, & \text{if } w \text{ is nonsplit multiplicative}. \end{cases}$$

More precisely, for $N \in \{2, 3, 4\}$ the possible Kodaira symbols of additive reduction with respect to $E/k_{v,0}$ which contribute to $L(T, E_f/K_0) \bmod N$ are as follows.

N	A_{unr}	$A_{ram} \cap M_f$
2	$III, III^*, I_n^*, n \geq 0, I_{m,2}^*, m \geq 0$	$I_n^*, n \geq 0$
3	IV, IV^*	*no contribution*
4	$I_n^*, n \geq 0$	$I_n^*, n \geq 0$

Before proving Theorem 3.1.5, we recall the following useful lemma.

Lemma 3.1.6. *Let $K_{v,0}$ be a complete field with respect to some non-archimedean valuation ord_v and with finite residue field of characteristic p. Let $E/K_{v,0}$ be an elliptic curve with additive reduction and let $\mathcal{T}$ be a torsion subgroup of $E(K_{v,0})$ of order prime to p. Then $\mathcal{T}$ has order at most 4. If it has order at least 2, then we have the following classification.*

Isomorphism Type of $\mathcal{T}$	*Possible Kodaira Symbols*
$\mathbb{Z}/2\mathbb{Z}$	III, III^*, I_n^* *with* $n \geq 0$, $I_{m,2}^*$ *with* $m \geq 0$
$\mathbb{Z}/3\mathbb{Z}$	IV, IV^*
$\mathbb{Z}/4\mathbb{Z}$	I_{2n+1}^*, *with* $n \geq 1$
$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	I_{2n}^*, *with* $n \geq 0$

Remark 3.1.7. In the notation of [25, p.497, 10.2.24], the symbol $I_{m,2}^*, m \geq 0$ is the Kodaira symbol $I_m^*, m \geq 0$ where the special fiber of the corresponding minimal model only has 2 irreducible components of multiplicity 1 defined over the residue field $k_{v,0}$.

Proof. (of Lemma 3.1.6) By Lemma 2.4.5, the prime-to-p torsion of $E(K_{v,0})$ injects into the group of components $\Phi_v(k_{v,0})$. The first part of the statement follows from the fact that $\mathcal{T}$ is then identified with a subgroup $\Phi_v(k_{v,0})$ and the latter has order at most 4 [42, p.362, IV.9.2(d)]. To show the second part of the statement, we obtain the following classification for the isomorphism type of the group of components $\Phi_v(k_{v,0})$ associated to the place v of additive reduction, based on the tables in [25, p.497, 10.2.24].

Isomorphism Type of $\Phi_v(k_{v,0})$	Possible Kodaira Symbols
$\mathbb{Z}/2\mathbb{Z}$	$III, III^*, I_{m,2}^*, m \geq 0$
$\mathbb{Z}/3\mathbb{Z}$	IV, IV^*
$\mathbb{Z}/4\mathbb{Z}$	I_{2n+1}^* with $n \geq 1$
$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	I_{2n}^* with $n \geq 0$

We conclude from the fact that the groups $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ have subgroups of order 2. □

Proof. (of Theorem 3.1.5) We have the well-known identity

$$L(T, E/K_{f,0}) = L(T, E/K_0)L(T, E_f/K_0).$$

Let $C_{f,0}/k_0$ be the curve corresponding to $K_{f,0}$. By assumption, E has over K_0 a subgroup of order $N \geq 2$ with N coprime with q. Therefore, $E(K_{f,0})$ also contains this subgroup of order N. Hence, we can apply [18, p.133, Theorem 4] to E/K_0 and $E/K_{f,0}$ and obtain expressions of the form

$$L(T, E/K_0) \equiv Z(T, C_0/k_0)Z(qT, C_0/k_0) \times P(T) \bmod N,$$
$$L(T, E/K_{f,0}) \equiv Z(T, C_{f,0}/k_0)Z(qT, C_{f,0}/k_0) \times Q(T) \bmod N,$$

for some formal rational functions $P(T)$ and $Q(T)$ in T with coefficients in $\mathbb{Z}/N\mathbb{Z}$, that we will describe shortly. From [32, p.524,(10.5) Corollary], we have the identity

$$Z(q^iT, C_{f,0}/k_0) = Z(q^iT, C_0/k_0)L(q^iT, \chi)$$

for $i = 0, 1$. Therefore, we can write

$$L(T, E_f/K_0) \equiv L(T, \chi)L(qT, \chi) \times \frac{Q(T)}{P(T)} \bmod N.$$

The rational function $P(T)$ is

$$P(T) \equiv \prod_{v \in M^{\mathrm{sp}}} (1 - q^{d_v} T^{d_v}) \times \prod_{v \in M^{\mathrm{ns}}} \frac{(1 - T^{d_v})(1 - q^{d_v} T^{d_v})}{(1 + T^{d_v})} \times \prod_{v \in A} (1 - T^{d_v})(1 - q^{d_v} T^{d_v}) \bmod N$$

and the expression for $Q(T)$ is identical to the one of $P(T)$, except that the products are taken over places of the field $K_{f,0}$. From the above description of $P(T)$, we see that in order to compute $L(T, E_f/K_0) \bmod N$, it suffices to study the places of K_0 over which E has bad reduction. To achieve this, we perform a case-by-case analysis on the factors of the ratio $Q(T)/P(T) \bmod N$, based on the decomposition types of these places in the field extension $K_{f,0}$.

Remark 3.1.8. In light of Lemma 3.1.6, the elliptic curve E/K_0 has no place of additive reduction when $N \geq 5$. Therefore, considerations involving places of additive reduction will only be relevant when $N \in \{2, 3, 4\}$.

Let $v \in M \cup A$ of degree d_v. First suppose that v is unramified in $K_{f,0}$. From part (a) of Lemma 3.1.3, we have the following tables.

Enhanced Reduction Type of E/K_0	$M^{\mathrm{sp}}_{\mathrm{inert}}$	$M^{\mathrm{ns}}_{\mathrm{inert}}$	A_{inert}
Factor of $P(T) \bmod N$	$1 - q^{d_v} T^{d_v}$	$\frac{(1-T^{d_v})(1-q^{d_v}T^{d_v})}{1+T^{d_v}}$	$(1 - T^{d_v})(1 - q^{d_v} T^{d_v})$
Factor of $Q(T) \bmod N$	$1 - q^{2d_v} T^{2d_v}$	$\frac{(1-T^{2d_v})(1-q^{2d_v}T^{2d_v})}{1+T^{2d_v}}$	$(1 - T^{2d_v})(1 - q^{2d_v} T^{2d_v})$
Factor of $Q(T)/P(T) \bmod N$	$1 + q^{d_v} T^{d_v}$	$\frac{(1+T^{d_v})^2(1+q^{d_v}T^{d_v})}{1+T^{2d_v}}$	$(1 + T^{d_v})(1 + q^{d_v} T^{d_v})$

Enhanced Reduction Type of E/K_0	$M^{\mathrm{sp}}_{\mathrm{split}}$	$M^{\mathrm{ns}}_{\mathrm{split}}$	A_{split}
Factor of $P(T) \bmod N$	$1 - q^{d_v} T^{d_v}$	$\frac{(1-T^{d_v})(1-q^{d_v}T^{d_v})}{1+T^{d_v}}$	$(1 - T^{d_v})(1 - q^{d_v} T^{d_v})$
$Q(T) \bmod N$	$(1 - q^{d_v} T^{d_v})^2$	$\frac{(1-T^{d_v})^2(1-q^{d_v}T^{d_v})^2}{(1+T^{d_v})^2}$	$(1 - T^{d_v})^2(1 - q^{d_v} T^{d_v})^2$
Factor of $Q(T)/P(T) \bmod N$	$1 - q^{d_v} T^{d_v}$	$\frac{(1-T^{d_v})(1-q^{d_v}T^{d_v})}{1+T^{d_v}}$	$(1 - T^{d_v})(1 - q^{d_v} T^{d_v})$

Finally, suppose that $v \in M_{\mathrm{ram}} \cup A_{\mathrm{ram}}$. From part (b) of Lemma 3.1.3, the reductions of E over v and w are either both split multiplicative or nonsplit multiplicative. Thus, all factors of $Q(T)/P(T) \bmod N$ over M_{ram} are equal to 1 mod N. According to Remark 3.1.8, this ends the case-by-case analysis when $N \geq 5$. Set

$$\varepsilon_v = \begin{cases} 1, & \text{if } v \in M_{\mathrm{inert}}, \\ -1, & \text{if } v \in M_{\mathrm{split}}, \end{cases} \text{ and } m(T^{d_v}) = \begin{cases} 1 + T^{2d_v}, & \text{if } v \in M_{\mathrm{inert}}, \\ (1 + T^{d_v})^2, & \text{if } v \in M_{\mathrm{split}}. \end{cases}$$

Then for $N \geq 5$ we have

$$\frac{Q(T)}{P(T)} \equiv \prod_{v \in M^{\mathrm{sp}}_{\mathrm{unr}}} (1 + \varepsilon_v q^{d_v} T^{d_v}) \times \prod_{v \in M^{\mathrm{ns}}_{\mathrm{unr}}} \frac{(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + \varepsilon_v q^{d_v} T^{d_v})(1 + T^{d_v})}{m_v(T^{d_v})} \bmod N.$$

Now, suppose that $v \in A_{\mathrm{ram}}$ (which is only relevant for $N \in \{2, 3, 4\}$). Lemma 3.1.8 lists the only Kodaira symbols that we need to take into account. From part (b) of Lemma 3.1.3, we obtain the following table.

$E/K_{v,0}$	$E_f/K_{v,0}$	$E/K_{f,0,v}$	Factor of $Q(T)/P(T)$ mod N
III	III^*	I_0^*	1
III^*	III	I_0^*	1
IV	II^*	IV^*	1
IV^*	II	IV	1
$I_{2n+1}^*, n \geq 1$	$I_{2n+1}, n \geq 1$	$I_{4n+2}, n \geq 1$	$(1+\alpha_v T^{d_v})^{-1}$
$I_{2n}^*, n \geq 1$	$I_{2n}, n \geq 1$	$I_{4n}, n \geq 1$	$(1+\alpha_v T^{d_v})^{-1}$
I_0^*	I_0	I_0	$(1-T^{d_v})^{-1}(1-q^{d_v}T^{d_v})^{-1}$

where we set

$$\alpha_v = \begin{cases} -1 & \text{if w is split multiplicative,} \\ 1 & \text{if w is nonsplit multiplicative.} \end{cases}$$

Remark 3.1.9. From Tate's algorithm [42, pp.366, IV. §9, Steps 1 and 2], we see that if $v \in A_{\text{ram}}$, and E/K_0 has Kodaira symbol $I_{m,2}^*, m \geq 0$ over v, then E_f/K_0 has good reduction if $m = 0$ and multiplicative reduction if $m \geq 1$. Therefore, the information of the Kodaira symbol $I_{m,2}^*, m \geq 0$ is already contained in the above table.

Remark 3.1.10. We simply clarify, if needed, how the last three lines of the column "Factor of $Q(T)/P(T)$ mod N were obtained. Since $E/k_{v,0}$ has additive reduction in these cases, the factor of $P(T)$ mod N is $(1-T^{d_v})^{-1}(1-q^{d_v}T^{d_v})^{-1}$.

For the Kodaira symbols $I_n^*, n \geq 1$, $E/K_{f,0,w}$ has multiplicative reduction over w. If the reduction is split multiplicative, then the factor of $Q(T)/P(T)$ mod N is

$$(1-q^{d_v}T^{d_v}) \times \frac{1}{(1-T^{d_v})(1-q^{d_v}T^{d_v})} = \frac{1}{1-T^{d_v}} \bmod N.$$

If the reduction is nonsplit multiplicative, then the factor of $Q(T)/P(T)$ mod N is

$$\frac{(1-T^{d_v})(1-q^{d_v}T^{d_v})}{1+T^{d_v}} \times \frac{1}{(1-T^{d_v})(1-q^{d_v}T^{d_v})} = \frac{1}{1+T^{d_v}} \bmod N.$$

Now, if $E/K_{v,0}$ has Kodaira symbol I_0^* over v, then $E/K_{f,0,w}$ has Kodaira symbol I_0 over w. Since $Q(T)$ mod N only considers places of bad reduction, there is no factor of $Q(T)$ mod N which corresponds to the factor of $P(T)$ mod N. The place w is one of good reduction and so the factor corresponding to the one of $P(T)$ mod N is found inside the product $Z(T, C_{f,0}/k_0)Z(qT, C_{f,0}/k_0)$ mod N. Since $E(K_{f,0})$ has a subgroup of order $N \geq 2$ coprime with q, then according to [18, p.132, Lemma 3] that factor is $(1-T^{d_v})(1-q^{d_v}T^{d_v})$ mod N. Observe that the two factors cancel in the quotient $L(T, E/K_{f,0})/L(T, E/K_0)$ mod N.

Therefore, and if $N \in \{2, 3, 4\}$, then

$$\begin{aligned} \frac{Q(T)}{P(T)} \equiv & \prod_{v \in M_{\text{unr}}^{\text{sp}}} (1+\varepsilon_v q^{d_v}T^{d_v}) \times \prod_{v \in M_{\text{unr}}^{\text{ns}}} \frac{(1+\varepsilon_v q^{d_v}T^{d_v})(1+\varepsilon_v q^{d_v}T^{d_v})(1+T^{d_v})}{m_v(T^{d_v})} \\ & \times \prod_{v \in A_{\text{unr}}} (1+\varepsilon_v T^{d_v})(1+\varepsilon_v q^{d_v}T^{d_v}) \\ & \times \gamma_{\text{ram}} \bmod N, \end{aligned}$$

where

$$\varepsilon_v = \begin{cases} 1, & \text{if } v \in M_{\text{inert}} \cup A_{\text{inert}}, \\ -1, & \text{if } v \in M_{\text{split}} \cup A_{\text{split}}, \end{cases} \text{ and } m(T^{d_v}) = \begin{cases} 1 + T^{2d_v}, & \text{if } v \in M_{\text{inert}}, \\ (1 + T^{d_v})^2, & \text{if } v \in M_{\text{split}}, \end{cases}$$

$$\gamma_{\text{ram}} := \begin{cases} 1, & \text{if } N = 3, \\ \prod\limits_{\substack{v \in A_{\text{ram}} \cap U_f \\ A_{\text{ram}} \text{ is } I_0^*}} (1 - T^{d^v})^{-1}(1 - q^{d_v} T^{d_v})^{-1} \times \prod\limits_{\substack{v \in A_{\text{ram}} \cap U_f \\ A_{\text{ram}} \text{ is } I_n^*, n \geq 1}} (1 + \alpha_v T^{d_v})^{-1}, & \text{if } N = 2, 4, \end{cases}$$

where

$$\alpha_v = \begin{cases} -1, & \text{if } w \text{ is split multiplicative}, \\ 1, & \text{if } w \text{ is nonsplit multiplicative}. \end{cases}$$

More precisely, for $N \in \{2, 3, 4\}$ the possible Kodaira symbols of additive reduction with respect to $E/K_{v,0}$ which contribute to $L(T, E_f/K_0)$ mod N are as follows.

N	A_{unr}	A_{ram}
2	$III, III^*, I_n^*, n \geq 0, I_{m,2}^*, m \geq 0$	$I_n^*, n \geq 0$
3	IV, IV^*	no contribution
4	$I_n^*, n \geq 0$	$I_n^*, n \geq 0$

□

We can be more precise when $N = 2$. Let $|U_{f,0}|$ (resp. M_f, resp. A_f) be the closed points of $C_{f,0}$ at which E_f/K_0 has good (resp. multiplicative, resp. additive) reduction.

Corollary 3.1.11 (of Theorem 3.1.5)**.** *If $E(K_0)$ has nontrivial 2-torsion, then*

$$L(T, E_f/K_0) \equiv Z(T, C_0/k_0)^2 \times \prod_{v \in M_{f,ram}} (1 - T^{d_v}) \times \prod_{v \in A_{f,unr}} (1 - T^{d_v})^2 \bmod 2.$$

Remark 3.1.12. This is a more precise version of the case $N = 2$ in [18, p.133, Theorem 4], noting that places of additive reduction for E_f/K_0 which ramify in $K_{f,0}$ do not contribute to the reduction $L(T, E_f/K_0)$ mod 2.

Proof. We summarize the different factors of $Q(T)/P(T)$ mod 2.

If $v \in M_{\text{unr}}$, then v is a place of multiplicative reduction for E_f/K_0. Its contributing factor is

$$1 - T^{d_v} \bmod 2.$$

If $v \in A_{\text{unr}}$, then v is also a place of additive reduction for E_f/K_0. The possible Kodaira symbols are $III, III^*, I_n^*, n \geq 0$ (and for a given v, E/K_0 and E_f/K_0 have the same Kodaira symbol). Its contributing factor is

$$(1 - T^{d_v})^2 \bmod 2.$$

Let $v \in A_{\text{ram}}$. If the Kodaira symbol of v with respect to E/K_0 is $I_n^*, n \geq 0$, then it is $I_n, n \geq 0$ with respect to E_f/K_0. Its contributing factor is

$$1/(1 - T^{d_v}) \bmod 2$$

if $n \geq 1$ and

$$1/(1-T^{d_v})^2 \bmod 2$$

if $n = 0$. Hence,

$$\begin{aligned}\frac{Q(T)}{P(T)} &\equiv \prod_{v\in M_{\text{unr}}}(1-T^{d_v}) \times \prod_{v\in A_{\text{unr}}}(1-T^{d_v})^2 \\ &\times \prod_{\substack{v\in A_{\text{ram}}\cap U_f \\ A_{\text{ram}} \text{ is } I_0^*}} \frac{1}{(1-T^{d^v})^2} \times \prod_{\substack{v\in A_{\text{ram}}\cap M_{f,\text{ram}} \\ A_{\text{ram}} \text{ is } I_n^*, n\geq 1}} \frac{1}{(1-T^{d_v})} \bmod 2 \\ &\equiv \prod_{v\in M_{f,\text{unr}}}(1-T^{d_v}) \times \prod_{v\in A_{f,\text{unr}}}(1-T^{d_v})^2 \\ &\times \prod_{\substack{v\in A_{\text{ram}}\cap U_f \\ A_{\text{ram}} \text{ is } I_0^*}} \frac{1}{(1-T^{d^v})^2} \times \prod_{\substack{v\in A_{\text{ram}}\cap M_{f,\text{ram}} \\ A_{\text{ram}} \text{ is } I_n^*, n\geq 1}} \frac{1}{(1-T^{d_v})} \bmod 2\end{aligned}$$

Recall that the zeta function of C_0/k_0 is defined by the Euler product

$$Z(T, C_0/k_0) := \prod_{v\in|C_0|}(1-T^{d_v})^{-1},$$

while the Artin L-function of χ is defined by the Euler product

$$L(T,\chi) := \prod_{v\in|C_0|_{\text{split}}}(1-T^{d_v})^{-1} \times \prod_{v\in|C_0|_{\text{inert}}}(1+T^{d_v})^{-1}$$

and so $L(T,\chi) \equiv Z(T, C_0/k_0) \times \prod_{v\in|C_0|_{\text{ram}}}(1-T^{d_v}) \bmod 2$. Hence,

$$\begin{aligned}L(T, E_f/K_0) &\equiv L(T,\chi)^2 \times \frac{Q(T)}{P(T)} \\ &\equiv Z(T, C_0/k_0)^2 \times \prod_{v\in M_{f,\text{ram}}}(1-T^{d_v}) \times \prod_{v\in A_{\text{f,unr}}}(1-T^{d_v})^2 \bmod 2.\end{aligned}$$

□

Let $f_1, f_2 \in K_0^\times$ and let E_{f_1} and E_{f_2} be the corresponding quadratic twists of E. Since E has nonconstant j-invariant $j(E)$, then $L(T, E/K_0) \in 1 + T\cdot\mathbb{Z}[T]$ [24, p.11]. Since $j(E) = j(E_{f_i})$ for $i = 1, 2$ by Lemma 2.2.25, then $L(T, E_{f_i}/K_0) \in 1 + T\cdot\mathbb{Z}[T]$ for $i = 1, 2$. Therefore, $L(T, E_{f_1}/K_0)/L(T, E_{f_2}/K_0) \in 1+T\cdot\mathbb{Z}[[T]]$ and the expression $L(T, E_{f_1}/K_0)/L(T, E_{f_2}/K_0) \bmod 2$ is a well-defined element of $1 + T\cdot(\mathbb{Z}/2\mathbb{Z})[[T]]$. In the second main result of this chapter, we write explicitly the reduction modulo 2 of this quotient.

Theorem 3.1.13. *Let $f_1, f_2 \in K_0^\times$ and let*

$$U_{f_1,f_2} := \left(U_{f_1} \cap U_{f_2}\right) \cup \left(M_{f_1} \cap M_{f_2}\right) \cup \left(A_{f_1} \cap A_{f_2}\right).$$

Then,

$$\frac{L(T, E_{f_1}/K_0)}{L(T, E_{f_2}/K_0)} \equiv \prod_{v \notin U_{f_1, f_2}} \frac{L_v(T^{d_v}, E_{f_2}/K_0)}{L_v(T^{d_v}, E_{f_1}/K_0)} \bmod 2.$$

Proof. The ratio of Euler products modulo 2 is congruent to the product of the ratios modulo 2 of the Euler factors:

$$\frac{L(T, E_{f_1}/K_0)}{L(T, E_{f_2}/K_0)} \equiv \prod_{v} \frac{L_v(T^{d_v}, E_{f_2}/K_0)}{L_v(T^{d_v}, E_{f_1}/K_0)} \bmod 2.$$

If $v \in A_{f_1} \cap A_{f_2}$, then the Euler factor is $L_v(T, E_{f_i}/K_0) = 1$ for $i = 1, 2$. Now, we can assume that $f_1 = f$ and $f_2 = 1$. Note that $M \cap M_f = M_{\mathrm{unr}}$ and $|U_0| \cap |U_{f,0}| = |U_{\mathrm{unr}}|$ by part (a) of Lemma 3.1.3.

If $v \in M \cap M_f$, then by part (b) of Lemma 3.1.4, we have

$$L_v(T, E_f/K_0) \equiv L_v(T, E/K_0) \bmod 2.$$

Finally, if $v \in |U_0| \cap |U_{f,0}|$, then by part (a) of Lemma 3.1.4, we have

$$\#E_v(k_{v,0}) + \#E_{f,v}(k_{v,0}) \equiv 0 \bmod 2.$$

It follows from the definition (2.3.1) of the terms a_v and $a_{f,v}$ of the corresponding Euler factors of E/K_0 and E_f/K_0, respectively, that $a_{f,v} \equiv a_v \bmod 2$, and so

$$L_v(T, E_f/K_0) \equiv L_v(T, E/K_0) \bmod 2.$$

□

3.2 Function Fields of Genus 0

In this section, we illustrate some ways in which we can be more explicit about the description of Theorems 3.1.5 and 3.1.13 when the curve C_0/k_0 is the genus zero curve $\mathbb{P}^1/k_0$. For simplicity, we restrict ourselves to the following context.

Context 3.2.1. Let $k_0 := \mathbb{F}_q$, let $K_0 := k_0(t)$ be a rational function field and let E/K_0 be an elliptic curve with nonconstant j-invariant and either good or multiplicative reduction at $t = \infty$. Suppose that over the affine plane $\mathbb{P}^1/k_0 - \{\infty\}$, E/K_0 is given by a minimal Weierstrass equation of the form $y^2 = u(x)$, with $u(x) := x^3 + ax + b$ irreducible in $K_0[x]$ and $a, b \in k_0[t]$. Let Δ be the discriminant of this Weierstrass equation, which is the discriminant of the cubic polynomial $u(x)$. Finally, suppose given a monic square-free polynomial $f \in \mathbb{F}_q[t]$.

Let us first examine Theorem 3.1.5 in this context.

Lemma 3.2.2. *Assuming Context 3.2.1, the following holds.*

(i) We have the identity $L(T, \chi)L(qT, \chi) = L(T, C_{f,0}/k_0)L(qT, C_{f,0}/k_0)$.

(ii) The set $|C_0|_{split} - \{\infty\}$ *is*

$$\{v \in k_0[t] \text{ monic irreducible }, v \nmid f : x^2 - f \in k_0(t)[x] \text{ has a root in } k_0[t]/(v)\}.$$

(iii) The set $|C_0|_{inert} - \{\infty\}$ *is*

$$\{v \in k_0[t] \text{ monic irreducible }, v \nmid f : x^2 - f \in k_0(t)[x] \text{ has no roots in } k_0[t]/(v)\}.$$

(iv) If $\deg(f)$ *is even, then* $\infty \in |C_0|_{split}$.

(v) If $\deg(f)$ *is odd, then* $\infty \in |C_0|_{ram}$.

Proof. Let $C_{f,0}/k_0$ be the curve corresponding to $K_{f,0}$ and let $L(T, C_{f,0}/k_0)$ be the numerator of its zeta function. Since C_0/k_0 has genus 0, the numerator of its equals to 1. Moreover, the denominators of $Z(q^iT, C_0/k_0)$ and $Z(q^iT, C_{f,0}/k_0)$ are equal to each other. Therefore, the identity

$$Z(q^iT, C_{f,0}/k_0) = Z(q^iT, C_0/k_0)L(q^iT, \chi)$$

simplifies to

$$L(q^iT, \chi) = L(q^iT, C_{f,0}/k_0)$$

for $i = 0, 1$, where $L(T, C_{f,0}/k_0)$ is the numerator of the zeta function $Z(q^iT, C_{f,0}/k_0)$. A finite place of K_0 corresponds to a monic irreducible polynomial in $k_0[t]$. Let v be a finite place K_0 which is unramified in $K_{f,0}$. By the Dedekind-Kummer theorem [32, I.3.8, pp.47-48], v splits (resp. is inert) in $K_{f,0}$ if and only if the polynomial $x^2 - f$ has a root (resp. no roots) in $k_{v,0}$.

A finite place v of K_0 which is ramified in $K_{f,0}$ corresponds to a monic irreducible polynomial, also denoted by v, which divides f.

The place at infinity ∞ of $k_0(t)$ corresponds to the maximal ideal (s) of $k_0[s]$ if we set $s := 1/t$. Let w_∞ be a place of $K_{f,0}$ lying over the place ∞. One can see that

$$\mathrm{ord}_{w_\infty}(f(t)) = \frac{2}{\gcd(\deg(f), 2)} \mathrm{ord}_{1/t}(f(t))$$

with $2/\gcd(\deg(f), 2)$ being the ramification index $e(w_\infty|\infty)$.

If $\deg(f)$ is even, then the place ∞ is unramified in $K_{f,0}$ and has the same reduction type for both E and E_f, i.e., good, or split multiplicative or else nonsplit multiplicative reduction. By performing the change of variables

$$(t, x) \mapsto (1/t, x/u^{\deg(f)/2})$$

to $x^2 - f$, we obtain a polynomial congruent to $(x - 1)(x + 1)$ modulo $u(x)$, since f is monic. Thus, the Dedekind-Kummer theorem tells us that this place splits in $K_{f,0}$. If $\deg(f)$ is odd, then $t = \infty$ ramifies in $K_{f,0}$ and becomes a place of additive reduction for $E_f/K_{f,0}$. □

We now consider Theorem 3.1.13 in Context 3.2.1.

Corollary 3.2.3 (of Theorem 3.1.13)**.** *Under the assumptions of Context 3.2.1, we have*

$$\frac{L(T, E_f/K_0)}{L(T, E/K_0)} \equiv (1 - a_\infty T + T^2)^{\varepsilon_U}(1 - T)^{\varepsilon_M} \times \prod_{v|f} \left(\prod_{v \in |U_0|} (1 - a_v T^{d_v} + T^{2d_v}) \times \prod_{v \in M} (1 - T^{d_v}) \right) \bmod 2,$$

where

$$(\varepsilon_U, \varepsilon_M) = \begin{cases} (0,0) & \text{if } \deg(f) \text{ is even}, \\ (1,0) & \text{if } \deg(f) \text{ is odd and } \infty \in |U_0|, \\ (0,1) & \text{if } \deg(f) \text{ is odd and } \infty \in M. \end{cases}$$

In particular, the degree of $L(T, E_f/K_0)$ is equal to

$$\deg L(T, E_f/K_0) = 2\varepsilon_U + \varepsilon_M + \sum_{v|f} \left(2 \sum_{v \in |U_0|} d_v + \sum_{v \in M} d_v \right) + \deg(M) + 2\deg(A) - 4.$$

Proof. This follows directly from Theorem 3.1.13 with $f_1 = f$, $f_2 = 1$ and the following observations. If $v \in U \cup M$ is a finite place which divides f, then $v \in A_f$ by part (b) of Lemma 3.1.3. If $\deg(f)$ is odd, then $\infty \in A_f$ as we just observed. Otherwise, a place of K_0 which is unramified in $K_{f,0}$ has the same reduction type before and after twisting by f by part (a) of Lemma 3.1.3. The formula for the degree of $L(T, E_f/K_0)$ follows immediately from the expression of $L(T, E_f/K_0)$ mod 2 and the fact that $\deg(L, E/K_0) = \deg(M) + 2\deg(A) - 4$ (2.3.3). □

3.3 Application: The Universal Elliptic Curve over $X_1(5)$

In this section, we apply the results of subsection 3.2 to an infinite family of quadratic twists of the so-called "universal" elliptic curve E over the function field $K_0 = k_0(t)$ "of the modular curve $X_1(5)/k_0$". We now suppose $p \geq 7$. The elliptic curve E/K_0 is defined by the Weierstrass equation

$$y^2 + (1-t)xy - ty = x^3 - tx^2$$

together with the point at infinity $O = [0:1:0]$. The distinguished point $P = (0,0)$ has order 5. Indeed, on one hand we have $[-1]P = (0,t)$ and $[-2]P = (t,0)$ and on the other hand, we have $[2]P = (t,t^2)$ and $[3]P = (t,0)$. This Weierstrass equation has discriminant $\Delta = t^5\tau$, where $\tau := t^2 - 11t - 1$. The places of bad reduction "are" $t, 1/t$ and the irreducible factors of τ. The discriminant of τ equals $5^2 \cdot 5$. Therefore, τ splits into two linear factors if and only if 5 is the square of some element θ in k_0, if and only if $q \equiv 1, 4 \bmod 5$. For simplicity, we will assume that q is of the form p^{4r} for some positive integer r. As a consequence, $q \equiv 1 \bmod 5$ and the discriminant splits as a product of linear factors $\Delta = t^5(t-\alpha_1)(t-\alpha_2)$, with $\alpha_1 := (11 - 5\theta)2^{-1}$ and $\alpha_2 := (11 + 5\theta)2^{-1}$.

3.3.1 Reduction types of E/K_0

We now find the reduction types of the places of bad reduction.

To do this, we first find a minimal Weierstrass equation of the form $y^2 = u(x)$ over $k_0[t]$. Since $char(k_0) \geq 5$, the curve has over the places $(t), (t-\alpha_1)$ and $(t-\alpha_2)$, after a standard change of variables [43, Table 3.1, p.45], an affine minimal Weierstrass equation of the form $y^2 = x^3 + ax + b$, where

$$a = -27(t^4 - 12t^3 + 14t^2 + 12t + 1) \text{ and } b = 54(t^2+1)(t^4 - 18t^3 + 74t^2 + 18t + 1).$$

Hence, the j-invariant of this elliptic curve is

$$j(E) = \frac{(t^4 - 12t^3 + 14t^2 + 12t + 1)^3}{t^5(t^2 - 11t - 1)},$$

which is in particular nonconstant. This Weierstrass equation $y^2 = x^3 + ax + b$ is indeed minimal for (t) and $(t - \alpha_i), i = 1, 2$, since $a, b \in k_0[t]$ and the t-adic and $(t - \alpha_i)$-adic valuations of Δ are respectively 5 and 1, all of which are strictly smaller than 12 [43, Remark 1.1, p.186]. The (t)-adic valuation of a is 0. Over the finite fields $k_{t-\alpha_1,0}$ and $k_{t-\alpha_2,0}$, the Weierstrass polynomial $x^3 + ax + b$ becomes respectively

$$x^3 - 135(123 - 55\theta)2^{-1}x - 270(1525 - 682\theta)$$

and

$$x^3 - 135(123 + 55\theta)2^{-1}x - 270(1525 + 682\theta).$$

Hence, for $i = 1, 2$, the $(t - \alpha_i)$-adic valuation of a is 0 and so by [43, p.196, VII.5.1(b)], the places (t) and $(t - \alpha_i)$, $i = 1, 2$ are places of multiplicative reduction for E/K_0. Now, the image of $6b$ ins $k_{t,0}$ is the square $6 \cdot 54 = (2 \cdot 3^2)^2$. Therefore, $(t) \in M^{\text{sp}}$ by [3, Lemma 2.1].

Since $q = p^{4r}$, the image of $6b$ in $k_{t-\alpha_i,0}$ is necessarily a square and so these places of multiplicative reduction are split by [3, Lemma 2.1]. There is a unique integer e such that the substitution $(t, x, y) \mapsto (1/u, x/u^{2e}, y/u^{3e})$ yields a Weierstrass equation over $k_0[u]$ which will be minimal at u. We take $e = 1$ and this gives the Weierstrass equation

$$y^2 = x^3 + a_\infty x + b_\infty,$$

where

$$a_\infty = -27(u^4 + 12u^3 + 14u^2 - 12u + 1) \text{ and } b_\infty = 54(u^2 + 1)(u^4 + 18u^3 + 74u^2 - 18u + 1).$$

We have $a_\infty, b_\infty \in k_0[u]$ and the (u)-adic valuation of a_∞ is 0. Hence, this Weierstrass equation is indeed minimal. The discriminant of this Weierstrass equation is

$$\Delta_\infty = u^5(u^2 + 11u - 1),$$

which has positive (u)-adic valuation. Therefore, ∞ is a place of multiplication reduction. Since, the image of $6b_\infty$ in $k_{u,0}$ is the square $6 \cdot 54 = (2 \cdot 3^2)^2$, then $(1/t) \in M^{\text{sp}}$ by by [3, Lemma 2.1].

3.3.2 Reduction of $L(T, E_f/K_0)$ Modulo 2 and Modulo 5

In this subsection, we describe the reduction of $L(T, E_f/K_0)$ modulo N for the infinite family of quadratic twists of E/K_0 by $f \in k_0[t]$ monic square-free polynomials, when $N \in \{2, 5\}$.

Note that since $0, \infty$ and the irreducible factors of $t^2 - 11t - 1$ are all places of multiplicative reduction and that $\mathbb{P}^1$ has genus 0, then

$$\deg L(T, E/K_0) = 4 - 4 = 0.$$

First suppose that $N = 5$. If f is coprime with Δ, then we can write

$$L(T, E_f/K_0) \equiv L(T, C_{f,0}/k_0)^2 \times (1 + \varepsilon_0 T)(1 + \beta T) \times (1 + \varepsilon_{t-\alpha_1} T)(1 + \varepsilon_{t-\alpha_2} T) \bmod 5,$$

where β equals -1 if $\deg(f)$ is even and equals 0 otherwise, as explained in the summary table before Corollary 3.2.3. From that table we can also deduce, for example, that if $\deg(f)$ is even and $f(0)$, $f(\alpha_1)$ and $f(\alpha_2)$ are all nonzero squares in k_0, then

$$L(T, E_f/K_0) \equiv L(T, C_{f,0}/k_0)^2 \times (1 - T)^4 \bmod 5.$$

Suppose $f = \Delta$. As the places of bad reduction for E/K have multiplicative reduction and as they all ramify in $K_{\Delta,0}$, then they do not contribute to $L(T, E_\Delta/K_0)$ mod 5. In this case,

$$L(T, E_\Delta/K_0) \equiv L(T, C_{\Delta,0}/k_0)^2 \bmod 5.$$

Finally, suppose that $N = 2$. The places of bad reduction of E/K_0 are all multiplicative, and ∞ is a place of multiplicative reduction. Moreover, we know that $L(T, E/K_0) = 1$. Therefore, we can use Corollary 3.2.3 to describe explicitly $L(T, E_f, K_0)$ mod 2. In particular, if f is coprime with Δ, then

$$L(T, E_f/K_0) \equiv (1 - T)^{\varepsilon_M} \times \prod_{v|f} (1 - a_v T^{d_v} + T^{2d_v}) \bmod 2,$$

where $\varepsilon_M = 0$ if $\deg(f)$ is even and $\varepsilon_M = 1$ otherwise, while if $f = \Delta$, then

$$L(T, E_f/K_0) \equiv (1 - T)^4 \bmod 2.$$

3.3.3 Remark on Computational Effort

Let E/K_0 be the universal elliptic curve over $X_1(5)$ with k_0 a field of cardinality $q = p^{4r}$ as before. Let $f \in k_0[t]$ be a monic irreducible polynomial of even degree $\deg(f)$ and where f is coprime with the discriminant $\Delta = t^5(t^2 - 11t - 1)$ of the Weierstrass equation $y^2 + (1-t)xy - ty = x^3 - tx^2$. Our goal is to compare the relative costs of computing $L(T, E_f/K_0)$ mod 2 using our formula and using the algorithm presented in [3]. Our formula in this case reads

$$L(T, E_f/K_0) \equiv 1 - a_f T^{\deg(f)} + T^{2\deg(f)} \bmod 2.$$

We need to compute the single term a_f mod 2.

Remark 3.3.1. Since f is coprime with Δ, f corresponds to a place of good reduction for the elliptic curve E/K_0. The Weierstrass equation $y^2 = x^3 + ax + b$ that we gave above is minimal for the place f. Let $y^2 = x^3 + (a \bmod v)x + (b \bmod v)$ be the corresponding Weierstrass equation for the reduced elliptic curve $E_v/k_{v,0}$. Since q is odd, then

$$a_f = 1 + q^{\deg(f)} - \#E_f(k_{f,0}) \equiv \#E_f(k_{f,0}) \bmod 2.$$

A non-identity point of order 2 in $E_f(k_{f,0})[2]$ is of the form $(\alpha, 0)$, where $\alpha \in k_{f,0}$ is, if it exists, a root of $x^3 + (a \bmod f)x + (b \bmod f)$. Therefore, $x^3 + (a \bmod f)x + (b \bmod f)$ is irreducible in $k_{f,0}[x]$ if and only if $a_f \equiv 1 \bmod 2$.

We can adapt the algorithm of Baig and Hall [3, pp.364-365] to compute $L(T, E_f/K_0)$ mod 2 as follows. One can write $L(T, E_f/K_0) = \sum_{n=0}^{2\deg(f)} c_n T^n$ with $c_0 = 1$ and for $1 \leq n \leq 2\deg(f)$, the coefficient c_n satisfies the recurrence relation ([3, pp.364-365, Lemma 2.2]

$$c_n = \frac{1}{n} \sum_{m=1}^{n} b_m \cdot c_{n-m},$$

where

$$b_m = \sum_{\substack{v \in |U_{f,0}| \\ d_v | m}} d_v \cdot a_{v^{m/d_v}} + \sum_{\substack{v \in M_f^{\mathrm{sp}} \\ d_v | m}} d_v + \sum_{\substack{v \in M_f^{\mathrm{ns}} \\ d_v | m}} (-1)^{m d_v} d_v,$$

with the meaning that the subscript f refers to the sets of places of good, resp. split multiplicative, resp. nonsplit multiplicative reduction for E_f/K_0. The amount of effort to compute $L(T, E_f/K_0)$ mod 2 using this algorithm is bounded below by the computation, for each $1 \leq n \leq 2\deg(f)$, of a_{v^m/d_v} mod 2, for $1 \leq m \leq n$ and $d_v | m$, where $v \in |U_{f,0}|$. One can use the functional equation to roughly cut the number of computations in two [3, p.365]:

$$c_n = \varepsilon(E_f/K_0) q^{2n-2\deg(f)} c_{2\deg(f)-n}, 0 \leq n \leq 2\deg(f).$$

For each integer d_v as above, there are

$$\frac{1}{d_v} \sum_{d | d_v} \mu(d_v | d) \cdot q^{d_v}$$

monic irreducible polynomials of degree d_v over the finite field $k_{v,0}$ with q^{d_v} elements. [12, pp.567-568, Chapter 14]. Here, μ is the Möbius inversion formula. Most of these polynomials correspond to a place of good reduction for E_f/K_0 and we roughly to compute quantities of the form a_{v^m/d_v} mod 2 for half of them. Our formula is therefore clearly more efficient than the algorithm of [3] for this task.

Chapter 4

Cohomological Approach

This chapter assumes the reader has a certain familiarity with the theory of étale cohomology as can be found in [14] and [26]. Some prerequisites are given in Chapter 2. We remind the reader the convention from Chapter 2 that unless otherwise stated, all rings are commutative and Noetherian and all schemes are locally Noetherian. We continue to use the notation of Chapter 2 and Chapter 3.

4.1 Summary

In this chapter, we study the reduction $\mathrm{L}(T, E/K_0)$ mod ℓ from a cohomological point of view. More precisely, this polynomial in $1 + \mathbb{F}_\ell[T]$ can be expressed as follows. Let C_0 be the curve corresponding to the function field K_0. Then the reduction of $\mathrm{L}(T, E/K_0)$ modulo ℓ is an alternating product of characteristic polynomials of geometric Frobenius endomorphisms acting on étale cohomology groups over the curve C/k with coefficients in $\mathcal{E}^0_\ell$, the ℓ-torsion of the identity component of the Néron model $\mathcal{E}$ over E/K. These cohomology groups are finite-dimensional $\mathbb{F}_\ell$-vector spaces. Using dévissage we can suitably re-express this alternating product in way that the étale cohomology groups involved will be the global sections of C with coefficients in Φ_ℓ, the ℓ-torsion of the component group of E/K, and the zeroth, first and second étale cohomology groups of C with coefficients in $\mathcal{E}[\ell]$, the ℓ-torsion of the Néron model $\mathcal{E}$.

The sheaf Φ_ℓ can be described via Tate's algorithm. We compute the action of the geometric Frobenius endomorphism Frob_q on its global sections in each case (Theorem 4.6.1). The action of Frob_q on $H^0(C_{\text{ét}}, \mathcal{E}[\ell])$ and on $\mathrm{H}^2(C_{\text{ét}}, \mathcal{E}[\ell])$ is computed directly.

In most cases, the action of Frob_q on $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell])$ is more complex to describe explicitly. If $E[\ell] \subset E(K_0)$, then this cohomology group is isomorphic to the direct product of two copies of $\mathrm{Jac}(C)(k)[\ell]$, the k-rational points of the ℓ-torsion subgroup of the Jacobian group of the curve C/k.

If $E[\ell]$ is not a subgroup of $E(K_0)$ (so that the $\mathbb{F}_\ell$-vector space $E(K_0)[\ell]$ is either zero or one-dimensional), then our strategy is as follows. Let $K_{\ell,0}$ be the field extension of K_0 generated by the coordinates of the affine points of $E[\ell]$. This extension is finite and Galois and its Galois group G_ℓ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Moreover, when μ_ℓ is contained in k_0, the constant field of K_0, then G_ℓ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$. We make that assumption starting in Section 4.7. By construction $E[\ell] \subset E(K_{\ell,0})$. Let $C_{\ell,0}$ be the curve corresponding to the function field $K_{\ell,0}$ and let

$\pi : C_{\ell,0} \to C_0$ be the finite morphism corresponding to the field extension $K_{\ell,0}/K_0$. We show that $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell])$ is a subgroup of the G_ℓ-invariants of $\mathrm{H}^1(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell])$ and precisely identify the cokernel of this inclusion. The pullback $\pi^*\mathcal{E}[\ell]$ of $\mathcal{E}[\ell]$ to $C_{\ell,0}$ is a subsheaf of the constant sheaf $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. In fact, $\mathcal{E}[\ell]$ is an example of *middle extension sheaf* and its pullback to the open locus of good reduction of E/K is an example of a lisse sheaf. It is in this more general setting that we prove some of the main results of this chapter (Theorem 4.2.5 and Theorem 4.3.10). The corresponding result for $\mathcal{E}[\ell]$ is then a consequence of these general results. Moreover, these general theorems also include the particular case of the ℓ-torsion of the Néron model of an Abelian variety. However, the focus of our thesis being on elliptic curves, and since there are extra technicalities to deal with for general Abelian varieties, we leave the general case to some of our future works.

As a corollary of Theorem 4.3.10, we show that when, for example, the order of G_ℓ is not divisible by ℓ, then $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell])$ and the G_ℓ-invariants of $\mathrm{H}^1(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell])$ coincide. Then, we give general formulas for the reduction of $L(T, E/K_0)$ modulo ℓ under the assumptions of Theorem 4.3.10 and that $\mu_\ell \subset k_0$. Namely, we deal with quadratic twists of elliptic curves in Theorem 4.9.1 and deal with the reduction modulo ℓ under the assumption that $E(K_0)[\ell] = \{O\}$ in Theorem 4.9.3. Finally, in Theorem 4.10.1, we show, assuming $\mu_\ell \subset k_0$ and $E(K_0)[\ell] = \{O\}$, that

$$L(T, E/K_0) \equiv \det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}^0[\ell]\right) \bmod \ell.$$

We could not find the result in the literature, and so it might be new.

4.2 Locally Constant Sheaf on a Galois Covering

Definition 4.2.1. Let U be a connected locally Noetherian scheme and let $\overline{x}$ be a geometric point of U. Let $\mathrm{F\acute{E}t}/U$ be the category of locally Noetherian schemes with a finite étale morphism to U. The functor $\mathrm{F}_{\overline{x}} : \mathrm{F\acute{E}t}/U \to$ **Finite Sets** defined on objects by $\mathrm{F}_{\overline{x}}(U') := \mathrm{Hom}_U(\overline{x}, U')$ and in a natural way on the morphisms, is called a *fundamental functor*.

Definition 4.2.2. An object $(f : U' \to U) \in \mathrm{F\acute{E}t}/U$ which is a connected finite étale morphism $f : U' \to U$ for which the order of the automorphism group $\mathrm{Aut}_U(U')$ equals the cardinality of the set $\mathrm{F}_{\overline{x}}(U')$ is called a *Galois covering of* U.

Proposition 4.2.3. *Let $f : U' \to U$ be a finite étale morphism between connected locally Noetherian schemes. Let $\overline{x}$ be a geometric point of U and let $\overline{x'}$ be a geometric point of U' such that $f(\overline{x'}) = \overline{x}$. If U' is Galois over U of Galois group $G = \mathrm{Aut}_U(U')$, then we have the short exact sequence of profinite groups*

$$1 \to \pi_1(U', \overline{x}') \to \pi_1(U, \overline{x}) \to G \to 1.$$

Proof. We simply sketch the argument and refer the reader to [26, p.40, I.5] and [30, p.73, 5.2.6] for more details. We have the fundamental functor $F_{\overline{x}} : \mathrm{F\acute{E}t}/U \to$ **Finite Sets**. For each object $(f : U' \to U) \in \mathrm{F\acute{E}t}/U$, the group $\mathrm{Aut}_U(U')$ acts on the right on $F_{\overline{x}}(U')$. If U' is connected, then this action is faithful, i.e., for every $g \in F_{\overline{x}}(U')$, the map

$$\mathrm{Aut}_U(U') \to F_{\overline{x}}(U') : \sigma \mapsto \sigma \circ g$$

is injective (injectivity follows from [26, p.26, I.3.13]). Now, if U' is Galois over U, then $\mathrm{Aut}(U')$ acts transitively on $F_{\overline{x}}(U')$ and the above morphism $\mathrm{Aut}_U(U') \to F_{\overline{x}}(U')$ is bijective.

Now, let U' be a connected locally Noetherian scheme together with a Galois covering $f : U' \to U$ as in the statement of the proposition. Consider the category $(\mathrm{F\acute{E}t}/U)/U'$ and fix some element $u' \in F_{\overline{x}}(U')$. We have an exact functor $\Phi : \mathrm{F\acute{E}t}/U \to (\mathrm{F\acute{E}t}/U)/U'$ defined by $Y \mapsto Y \times U'$. We then define a functor $F' : (\mathrm{F\acute{E}t}/U)/U' \to$ **Finite Sets** by setting, for each $X \in Ob((\mathrm{F\acute{E}t}/U)/U')$,

$$F'(X) := \text{ inverse image of } u' \text{ under the map } F_{\overline{x}}(X) \to F_{\overline{x}}(U').$$

One verifies that $((\mathrm{F\acute{E}t}/U)/U', F')$ forms a Galois category. Let H be the stabilizer subgroup of $u' \in F(U')$ in $\pi_1(U, \overline{x})$. Using the fact that $\pi_1(U, \overline{x})$ acts transitively on $F_{\overline{x}}(U')$ [44, Tag 0BN3], one deduces that $\pi_1(U, \overline{x})/H \simeq F_{\overline{x}}(U')$, that $\pi_1(U', \overline{x}') \simeq H$, that the functor $F' \circ \Phi$ is isomorphic to the functor $F_{\overline{x}}$ and is therefore a fundamental functor. Finally, one concludes that the corresponding continuous homomorphism $\pi_1(U', \overline{x}') \to \pi_1(U, \overline{x})$ is the canonical inclusion of H in $\pi_1(U, \overline{x})$. □

Lemma 4.2.4. *Let X be a connected locally Noetherian scheme. Let $\overline{x}$ be a geometric point of X. Let $\mathcal{F}$ be an Abelian locally constant sheaf over X with finite stalks. The following hold.*

(i) There is an equivalence between the category of finite locally constant sheaves of Abelian groups on $X_{\acute{e}t}$ and the category of finite $\pi_1(X, \overline{x})$-modules which sends $\mathcal{F}$ to $\mathcal{F}_{\overline{x}}$.

(ii) There is a canonical identification $\mathrm{H}^0(X_{\acute{e}t}, \mathcal{F}) = \mathrm{H}^0(\pi_1(X, \overline{x}), \mathcal{F}_{\overline{x}})$.

(iii) There is a canonical identification $\mathrm{H}^1(X_{\acute{e}t}, \mathcal{F}) = \mathrm{H}^1(\pi_1(X, \overline{x}), \mathcal{F}_{\overline{x}})$.

Proof. For part (i) see [26, p.156, V.1.2(b)] or [44, Tag 0DV5]. Part (ii) then follows from part (i) since X is connected. Part (iii) is proven in [16, pp.299-300, Exposé XI, Section 5]. □

We now state and prove our first main result of this chapter.

Theorem 4.2.5. *Let $\pi : U' \to U$ be a finite Galois covering of connected locally Noetherian schemes with Galois group G. Let $\overline{x}$ be a geometric point of U and choose a geometric point $\overline{x'}$ of U' whose image by π is $\overline{x}$. Let $\mathcal{F}$ be the locally constant sheaf with finite stalks on U corresponding to some continuous representation of $\pi_1(U, \overline{x})$ into a finite Abelian group A. Suppose that*

(i) the continuous action of $\pi_1(U', \overline{x'})$ on A is trivial,

(ii) the group G has a normal subgroup H , which acts on A by restriction of the action of G on A, such that the orders of H and A are coprime and

(iii) the orders of G/H and A^H are coprime.

Then $\mathrm{H}^0(U_{\acute{e}t}, \mathcal{F}) = A^G$ and there is a canonical isomorphism $\mathrm{H}^1(U_{\acute{e}t}, \mathcal{F}) \xrightarrow{\simeq} \mathrm{H}^1(U'_{\acute{e}t}, \pi^*\mathcal{F})^G$.

Proof. Since π is a finite Galois covering of schemes and $\mathcal{F}$ is a sheaf on $U_{\text{ét}}$, then there is a hochschild-serre spectral sequence [26, p.105, III.2.20]

$$E_2^{p,q} := H^p\left(G, H^q\left(U'_{\text{ét}}, \pi^*\mathcal{F}\right)\right) \Longrightarrow H^{p+q}\left(U_{\text{ét}}, \mathcal{F}\right) =: E^{p+q}.$$

As with any first quadrant cohomological spectral sequence with initial terms $(E_2^{p,q})_{p,q\geq 0}$, we have [26, Appendix B, p.309]

$$H^0(U'_{\text{ét}}, \pi^*\mathcal{F})^G = E_2^{0,0} = E^0 = H^0(U_{\text{ét}}, \mathcal{F})$$

and an exact sequence of groups

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_2^{1,0} & \longrightarrow & E^1 & \longrightarrow & E_2^{0,1} & \longrightarrow & E_2^{2,0} \\
 & & \| & & \| & & \| & & \| \\
0 & \to & \mathrm{H}^1\left(G, \mathrm{H}^0\left(U'_{\text{ét}}, \pi^*\mathcal{F}\right)\right) & \to & \mathrm{H}^1\left(U_{\text{ét}}, \mathcal{F}\right) & \to & \mathrm{H}^1\left(U'_{\text{ét}}, \pi^*\mathcal{F}\right)^G & \to & \mathrm{H}^2\left(G, \mathrm{H}^0\left(U'_{\text{ét}}, \pi^*\mathcal{F}\right)\right).
\end{array}$$

We want to show that the canonical map $E^1 \to E_2^{0,1}$ is bijective. To do this, it suffices to show that $E_2^{p,0} = 0$ for $p = 1, 2$. Since U' is connected and $\pi^*\mathcal{F}$ is a locally constant sheaf on U' with finite stalks, Lemma 4.2.4 (ii) implies that

$$E_2^{p,0} = \mathrm{H}^p\left(G, \left(\mathrm{Res}(A)^{\pi_1(U,\overline{x})}_{\pi_1(U',\overline{x'})}\right)^{\pi_1(U',\overline{x'})}\right) \text{ for all } p \geq 0,$$

Since $\pi_1(U', \overline{x'})$ acts trivially on A, then the action of $\pi_1(U, \overline{x})$ on A factors through the finite quotient G by Proposition 4.2.3, which canonically turns A into a G-module ${}_GA$. In particular,

$$\left(\mathrm{Res}(A)^{\pi_1(U,\overline{x})}_{\pi_1(U',\overline{x'})}\right)^{\pi_1(U',\overline{x'})} =_G A = A.$$

As H is a normal subgroup of G, we have a Lyndon-Hochschild-Serre spectral sequence [33, p.111, (2.4.1) Theorem]

$$\mathrm{H}_2^{p,q} := \mathrm{H}^p\left(G/H, \mathrm{H}^q(H, A)\right) \Longrightarrow \mathrm{H}^{p+q}(G, A) =: \mathrm{H}^{p+q}.$$

Now, $\mathrm{H}^p = \mathrm{H}^p(G, A) = E_2^{p,0}$ for all $p \geq 0$. Since the orders of H and A are coprime, then [33, p.60, (1.6.1) Proposition] implies that $H^q(H, A) = 0$ for all $q \geq 1$ and so $\mathrm{H}_2^{p,q} = 0$ for all $p \geq 0$ and all $q \geq 1$. As a consequence, the only possibly nonzero terms of the H_2-page are the $\mathrm{H}_2^{p,0}$ with $p \geq 0$ and moreover all the differentials on this page are zero. Thus, the Lyndon-Hochschild-Serre spectral sequence degenerates and yields for each $p \geq 0$ a canonical isomorphism

$$\mathrm{H}^p(G, A) \xrightarrow{\simeq} \mathrm{H}^p\left(G/H, A^H\right).$$

But we assumed that the orders of G/H and A^H are coprime. Therefore, it follows, again from [33, p.60, (1.6.1) Proposition], that

$$\mathrm{H}^p(G, A) = \mathrm{H}^p\left(G/H, A^H\right) = 0$$

for all $p \geq 1$. As we observed, this means that $E_2^{p,0} = 0$ for all $p \geq 1$, which gives the result. □

4.3 Middle Extension Sheaves and Galois Invariants

In this section, we fix the following context.

Context 4.3.1. Let k_0 be a perfect field. Let C_0 be a smooth, proper and geometrically connected curve over k_0. Let $K_0 := k_0(C_0)$ be its function field. Let n be an integer which is not divisible by the characteristic of the residue field $k_{v,0}$ for any $v \in C_0$. Let k be a fixed algebraic closure of k_0.

Definition 4.3.2. A constructible sheaf $\mathcal{F}_0$ on $C_{0,\text{ét}}$ with coefficients in $\mathbb{Z}/n\mathbb{Z}$ is called a $\mathbb{Z}/n\mathbb{Z}$-*middle extension sheaf* if given an inclusion morphism $j : U_0 \hookrightarrow C_0$ of any dense Zariski open subset U_0 of C_0, the adjunction morphism

$$\mathcal{F}_0 \to j_* j^* \mathcal{F}_0,$$

coming from the identity morphism on $j^*\mathcal{F}_0$, is an isomorphism.

Definition 4.3.3. A constructible locally constant sheaf $\mathcal{F}_0$ over a scheme U_0 which has finite stalks is called a *lisse sheaf*.

Remark 4.3.4. Since a middle extension sheaf $\mathcal{F}_0$ is a constructible sheaf on $C_{0,\text{ét}}$, there is an open affine $j : U_0 \to C_0$ over which $j^*\mathcal{F}_0$ is lisse.

Lemma 4.3.5. *Let $\mathcal{F}_0$ be an étale constructible sheaf over a smooth, proper, and geometrically connected curve C_0/k_0. Let $j : U_0 \hookrightarrow C_0$ be the inclusion of a dense Zariski open subset. If the sheaf $j^*\mathcal{F}_0$ on U_0 is lisse and if the adjunction morphism $\mathcal{F}_0 \to j_* j^* \mathcal{F}_0$ is an isomorphism, then $\mathcal{F}_0$ is a middle extension sheaf.*

Proof. The proof of [19, p.75, Lemma A.0.1 (i)] is also valid when $\mathbb{Q}_\ell$ is replaced by $\mathbb{Z}/n\mathbb{Z}$ if n and k_0 satisfy the assumptions of Context 4.3.1. □

4.3.1 Cohomology of a Middle Extension Sheaf

The goal of this subsection is to compute the étale cohomology groups $\mathrm{H}^i(C_{\text{ét}}, \mathcal{F})$. The results are certainly known to experts. We thank Chris Hall for sharing private notes on the subject which served as a basis for the arguments that follows. In his notes, k_0 is a finite field, but observe that the following arguments work more generally for a perfect field k_0. Throughout this subsection and the rest of this section, we work in the following context.

Context 4.3.6. Let $\mathcal{F}_0$ be a $\mathbb{Z}/n\mathbb{Z}$-middle extension sheaf on $C_{0,\text{ét}}$ and fix an inclusion $j : U_0 \to C_0$ of a dense Zariski open subset such that $\jmath^*\mathcal{F}_0 \to U_0$ is lisse (see Remark 4.3.4). Up to shrinking U_0, we can assume that it is connected. Let $\overline{\eta}$ be the generic geometric point corresponding to the generic point η of U_0. The middle extension sheaf $\mathcal{F}_0$ then corresponds to a unique, up to isomorphism, free $\mathbb{Z}/n\mathbb{Z}$-module A of finite rank r_A which is in a compatible way a continuous $\pi_1(U_0, \overline{\eta})$-module [19, p.76, Proposition A.0.4]. Let $i : Z_0 \to C_0$ be the closed immersion of the finite complement Z_0 of U_0 in C_0 and denote also by $i : Z \to C$ the pullback of the previous map to k.

Let M be a finite rank free $\mathbb{Z}/n\mathbb{Z}$-module and let μ_n be the group of nth roots of unity in the algebraic closure k of k_0. We define

$$M(-1) := M \otimes_{\mathbb{Z}/n\mathbb{Z}} \mathrm{Hom}(\mu_n, \mathbb{Z}/n\mathbb{Z}).$$

Lemma 4.3.7. *Assuming Context 4.3.6, we have canonical isomorphisms*

$$H^r_Z(C, j_! j^* \mathcal{F}) \simeq \begin{cases} 0 & \text{if } r = 0, \\ \bigoplus_{v \in Z} A^{D(v)} & \text{if } r = 1, \\ \bigoplus_{v \in Z} A_{D(v)}(-1) & \text{if } r = 2, \\ 0 & \text{if } r \geq 3. \end{cases}$$

Proof. Now, write Z as the disjoint union of two closed subsets $Z = Z_1 \coprod Z_2$. For $s \in \{1, 2\}$, denote by j_r the inclusion $j_s : C - Z_s \to C$. Applying [26, p.92, III.1.26] to $C \supset C - Z_s \supset C - Z$ yields for each $i \geq 0$ the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^r_{Z_2}(C, j_! j^* \mathcal{F}) & \longrightarrow & \mathrm{H}^r_Z(C, j_! j^* \mathcal{F}) & \longrightarrow & \mathrm{H}^r_{Z_1}(U_1, j_1^* j_! j^* \mathcal{F}) & \overset{\exists}{\dashrightarrow} & 0 \\ & & \| & & \| & & \| & & \\ 0 & \overset{\exists}{\dashleftarrow} & \mathrm{H}^r_{Z_2}(C, j_! j^* \mathcal{F}) & \longleftarrow & \mathrm{H}^r_Z(C, j_! j^* \mathcal{F}) & \longleftarrow & \mathrm{H}^r_{Z_1}(U_1, j_1^* j_! j^* \mathcal{F}) & \longleftarrow & 0 \end{array}$$

Therefore, we have a splitting of the projection of $\mathrm{H}^r_Z(C, j_! j^* \mathcal{F}) \to Hc^r_{Z_1}(U_1, j_1^* j_! j^* \mathcal{F})$ given by the above commutative right square. Applying the argument inductively, we find that

$$\mathrm{H}^r_Z(C, j_! j^* \mathcal{F}) \simeq \bigoplus_{v \in Z} \mathrm{H}^r_v(C, j_! j^* \mathcal{F}).$$

Since $\mathcal{F}$ is a sheaf on $C_{\text{ét}}$, then for each closed point v of C we have a canonical isomorphism

$$\mathrm{H}^r_v\left(C, j_!(j^* \mathcal{F})\right) \xrightarrow{\simeq} \mathrm{H}^r_v\left(\mathrm{Spec}(\mathcal{O}^h_{C,v}), j_!(j^* \mathcal{F})\right) \tag{4.3.1}$$

by excision [26, p.93,III.1.28]. Let $K_{\{v\}}$ be the field of fractions of $\mathcal{O}^h_{C,v}$. Since the latter is the henselization of a local ring at a prime [1], then from [27, p.182,II.1.1(a)], we have, for all $i \geq 0$, a canonical isomorphism

$$\mathrm{H}^r_v\left(\mathrm{Spec}(\mathcal{O}^h_{C,v}), j_!(j^* \mathcal{F})\right) \xrightarrow{\simeq} H^{r-1}\left(\mathrm{Spec}(K_{\{v\}})_{\text{ét}}, j^* \mathcal{F}\right). \tag{4.3.2}$$

Let $D(v) = \mathrm{Gal}(K^{\mathrm{sep}}_{\{v\}} / K_{\{v\}})$ be the decomposition subgroup of v in G_K. By [44, Tag 03QU], we have a canonical isomorphism

$$\mathrm{H}^{r-1}\left(\mathrm{Spec}(K_{\{v\}})_{\text{ét}}, j^* \mathcal{F}\right) = \mathrm{H}^{r-1}\left(D(v), A\right). \tag{4.3.3}$$

[1] More generally it is because this is an excellent Henselian discrete valuation ring.

By assumption, the integer n is not divisible by the characteristic of the residue field k_v of $K_{\{v\}}$ for any $v \in C$. Since $K_{\{v\}}$ is the field of fractions of a strictly Henselian discrete valuation ring, then by [14, p.414, 8.1.4] we have canonical isomorphisms

$$H^r(D(v), A) \simeq \begin{cases} A^{D(v)} & \text{if } r = 0, \\ A_{D(v)}(-1) & \text{if } r = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Here,

$$A_{D(v)}(-1) := \mathrm{Hom}\left(\varprojlim_{(n,p)=1} \mu_n(k_v), A_{D(v)} \right).$$

Therefore, we have canonical isomorphisms

$$H^r_Z(C, j_! j^* \mathcal{F}) \simeq \begin{cases} 0 & \text{if } r = 0, \\ \bigoplus_{v \in X} A^{D(v)} & \text{if } r = 1, \\ \bigoplus_{v \in X} A_{D(v)}(-1) & \text{if } r = 2, \\ 0 & \text{if } r \geq 3. \end{cases}$$

Since for each $v \in Z$, the residue field of $K_{\{v\}}$ is separably closed, then

$$D(v) = I(v) := \mathrm{Gal}\left(K^{\mathrm{sep}}_{\{v\}} / K^{\mathrm{unr}}_{\{v\}} \right).$$

This gives the result. □

Proposition 4.3.8. *Assuming Context 4.3.6, we have*

$$\mathrm{H}^r\left(U_{\acute{e}t}, j^*\mathcal{F}\right) \simeq \begin{cases} A^{\pi_1(U,\overline{\eta})} & \text{if } r = 0, \\ \mathrm{H}^1(\pi_1(U,\overline{\eta}), A) & \text{if } r = 1, \\ 0 & \text{if } r \geq 2, \end{cases}$$

$$\mathrm{H}^r_Z\left(C, \mathcal{F}\right) \simeq \begin{cases} \bigoplus_{v \in Z} A_{I(v)}(-1) & \text{if } r = 2, \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathrm{H}^r(C_{\acute{e}t}, \mathcal{F}) \simeq \begin{cases} A^{\pi_1(U,\overline{\eta})} & \text{if } r = 0, \\ A_{\pi_1(U,\overline{\eta})(-1)} & \text{if } r = 2, \\ 0 & \text{if } r \geq 3 \end{cases}$$

and there is an exact sequence of Abelian groups

$$0 \to \mathrm{H}^1(C_{\acute{e}t}, \mathcal{F}) \to \mathrm{H}^1(\pi_1(U,\overline{\eta}), A) \to \bigoplus_{v \in Z} A_{I(v)}(-1) \to A_{\pi_1(U,\overline{\eta})}(-1) \to 0.$$

Proof. Since $\mathcal{F}$ is a sheaf on the scheme $C_{\text{ét}}$, then by [26, p.76, II.3.13] there is a short exact sequence of sheaves on $C_{\text{ét}}$

$$0 \to j_! j^* \mathcal{F} \to \mathcal{F} \to i_* i^* \mathcal{F} \to 0. \tag{4.3.4}$$

The sheaf $i_* i^* \mathcal{F}$ is a skyscraper sheaf supported on Z, the finite complement of U and by [47, p.159, (10.1.2) Lemma] we have $\mathrm{H}^r(C_{\text{ét}}, i_* i^* \mathcal{F}) = 0$ for $r \geq 1$.

Now, if $\mathcal{G}$ is one of the sheaves $j_! j^* \mathcal{F}, \mathcal{F}, i_* i^* \mathcal{F}$, then there is a long exact sequence [26, p.92, III.1.25]

$$0 \to \mathrm{H}^0_Z(C, \mathcal{G}) \to \cdots \to \mathrm{H}^r(C_{\text{ét}}, \mathcal{G}) \to \mathrm{H}^r(U_{\text{ét}}, j^* \mathcal{G}) \to \mathrm{H}^{r+1}_Z(C, \mathcal{G}) \to \cdots . \tag{4.3.5}$$

First suppose that $\mathcal{G} = i_* i^* \mathcal{F}$.

Since the skyscraper sheaf $i_* i^* \mathcal{F}$ is supported on the finite set Z, we have $j^* i_* = 0$. Therefore, $\mathrm{H}^r_Z(C, i_* i^* \mathcal{F}) \simeq \mathrm{H}^r(C_{\text{ét}}, i_* i^* \mathcal{F})$ and these groups vanish for $r \geq 1$. Moreover,

$$\mathrm{H}^0(C_{\text{ét}}, i_* i^* \mathcal{F}) \simeq \mathrm{H}^0(Z_{\text{ét}}, i^* \mathcal{F}) \simeq \mathrm{H}^0\left(\left(\coprod_{v \in Z} v\right)_{\text{ét}}, i^* \mathcal{F}\right) \simeq \prod_{v \in Z} \mathrm{H}^0(v_{\text{ét}}, i^* \mathcal{F}) \simeq \prod_{v \in Z} \mathcal{F}_{\overline{v}} \simeq \prod_{v \in Z} \left(\mathcal{F}_{\overline{\eta}}\right)^{I(v)}.$$

The last equality follows because the adjunction morphism $\mathcal{F} \to j_* j^* \mathcal{F}$ is an isomorphism (since $\mathcal{F}$ is a middle extension sheaf) and on the geometric stalk $\overline{v}$ over $v \in Z$ this is an isomorphism $\mathcal{F}_{\overline{v}} \to \left(\mathcal{F}_{\overline{\eta}}\right)^{I(v)}$.

Second, suppose that $\mathcal{G} = \mathcal{F}$. There is a Leray spectral sequence [26, p.89, III Theorem 1.18(a)]

$$\mathrm{H}^p(C_{\text{ét}}, R^q j_*(j^* \mathcal{F})) \Rightarrow \mathrm{H}^{p+q}(U_{\text{ét}}, j^* \mathcal{F})$$

from which we deduce that

$$H^0(C_{\text{ét}}, j_* j^* \mathcal{F}) = H^0(U_{\text{ét}}, j^* \mathcal{F}). \tag{4.3.6}$$

Since $\mathcal{F}$ is a middle extension sheaf on $C_{\text{ét}}$, then $H^0(C_{\text{ét}}, j_* j^* \mathcal{F}) = H^0(C_{\text{ét}}, \mathcal{F})$. Looking at the zeroth cohomology terms of the long exact sequence (4.3.5), we deduce that $\mathrm{H}^0_Z(C, \mathcal{F}) = 0$.

Third, suppose that $\mathcal{G} = j_! j^* \mathcal{F}$ and consider the long exact sequence (4.3.5). In light of Lemma 4.3.7, this exact sequence reads

$$0 \longrightarrow \mathrm{H}^0(C_{\text{ét}}, j_! j^* \mathcal{F}) \longrightarrow \mathrm{H}^0(U_{\text{ét}}, j^* j_! j^* \mathcal{F}) \longrightarrow \bigoplus_{v \in Z} A^{D(v)}$$

$$\cdots \longrightarrow \mathrm{H}^1(C_{\text{ét}}, j_! j^* \mathcal{F}) \longrightarrow \mathrm{H}^0(U_{\text{ét}}, j^* j_! j^* \mathcal{F}) \longrightarrow \bigoplus_{v \in Z} A_{D(v)}(-1)$$

$$\cdots \longrightarrow \mathrm{H}^2(C_{\text{ét}}, j_! j^* \mathcal{F}) \longrightarrow \mathrm{H}^2(U_{\text{ét}}, j^* j_! j^* \mathcal{F}) \longrightarrow 0$$

and $\mathrm{H}^r(C_{\text{ét}}, j_! j^* \mathcal{F}) = 0$ for $r \geq 3$ since C is a smooth curve over an algebraically closed field [44, Tag 03SC (1)].

We now consider simultaneously the long exact sequence (4.3.5) for $j_!j^*\mathcal{F}, \mathcal{F}$ and $i_*i^*\mathcal{F}$. This gives us a commutative square with exact rows and columns that we will make explicit in a moment. Note the canonical isomorphisms $j^*j_!j^*\mathcal{F} \simeq j^*\mathcal{F}$ [26, p.76], $j^*\mathcal{F} \simeq j^*j_*j^*\mathcal{F}$, since $\mathcal{F}$ is a middle extension, and $j^*i_*i^*\mathcal{F} = 0$ [26, p.76.II.3.14(d)]. The claimed commutative diagram with exact rows and columns is the following.

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & & \\
 & \downarrow & & \downarrow & & & \\
\cdots \longrightarrow & \mathrm{H}^r_Z(C, j_!j^*\mathcal{F}) & \longrightarrow & \mathrm{H}^r(C_{\text{ét}}, j_!j^*\mathcal{F}) & \longrightarrow & H^r(U_{\text{ét}}, j^*\mathcal{F}) & \longrightarrow \cdots \\
 & \downarrow & & \downarrow & & \| & \\
\cdots \longrightarrow & \mathrm{H}^r_Z(C, j_*j^*\mathcal{F}) & \longrightarrow & \mathrm{H}^r(C_{\text{ét}}, j_*j^*\mathcal{F}) & \longrightarrow & H^r(U_{\text{ét}}, j^*\mathcal{F}) & \longrightarrow \cdots \\
 & \downarrow & & \downarrow & & & \\
 & \mathrm{H}^r_Z(C, i_*i^*\mathcal{F}) & = & \mathrm{H}^r_Z(C, i_*i^*\mathcal{F}) & & & \\
 & \downarrow & & \downarrow & & & \\
 & \vdots & & \vdots & & &
\end{array}$$

Since $\mathrm{H}^0_Z(C, j_*j^*\mathcal{F}) = 0$ and $\mathrm{H}^1_Z(C, i_*i^*\mathcal{F}) = 0$, then from the first column of this diagram we have the exact sequence

$$0 \to \mathrm{H}^0_Z(C, i_*i^*\mathcal{F}) \to \mathrm{H}^1_Z(C, j_!j^*\mathcal{F}) \to \mathrm{H}^1_Z(C, j_*j^*\mathcal{F}) \to 0.$$

In particular, the above identifications of $\mathrm{H}^0_Z(C, i_*i^*\mathcal{F})$ and $\mathrm{H}^1_Z(C, j_!j^*\mathcal{F})$ show that the first map of this sequence is an isomorphism.

Therefore, we have an isomorphism

$$\mathrm{H}^2_Z(C, j_*j^*\mathcal{F}) \simeq \bigoplus_{v \in Z} A_{I(v)}(-1)$$

and $\mathrm{H}^i_Z(C, j_*j^*\mathcal{F})$ vanishes for $i \neq 2$. From the middle column of the above commutative square and the fact that $\mathcal{F}$ is a middle extension sheaf, we deduce that

$$\mathrm{H}^r(C_{\text{ét}}, \mathcal{F}) = \mathrm{H}^r(C_{\text{ét}}, j_*j^*\mathcal{F}) = \mathrm{H}^r(C_{\text{ét}}, j_!j^*\mathcal{F}), \tag{4.3.7}$$

for $r \geq 2$.

We now go back to the long exact sequence

$$0 \to \mathrm{H}^0_Z(C, \mathcal{F}) \to \cdots \to \mathrm{H}^r(C_{\text{ét}}, \mathcal{F}) \to \mathrm{H}^r(U_{\text{ét}}, j^*\mathcal{F}) \to \mathrm{H}^{r+1}_Z(C, \mathcal{F}) \to \cdots, \tag{4.3.8}$$

The sheaf $j^*\mathcal{F}$ is an étale sheaf of $\mathbb{Z}/n\mathbb{Z}$-modules on the affine curve U/k and so $\mathrm{H}^r(U_{\text{ét}}, j^*\mathcal{F})$ vanishes for $i \geq 2$ [44, Tag 03SC (2)]. This, coupled with Lemma 4.2.4, gives

$$\mathrm{H}^r\left(U_{\text{ét}}, j^*\mathcal{F}\right) \simeq \begin{cases} A^{\pi_1(U,\overline{\eta})} & \text{if } r = 0, \\ \mathrm{H}^1(\pi_1(U, \overline{\eta}), A) & \text{if } r = 1, \\ 0 & \text{if } r \geq 2. \end{cases}$$

The curve U_0/k_0 is smooth and geometrically connected. There is therefore a canonical group isomorphism

$$\mathrm{H}^2_c(U, j^*\mathcal{F}) = A_{\pi_1(U,\overline{\eta})}(-1)$$

of G_{k_0}-modules by [44, Tag 03VK]. The groups $\mathrm{H}^i(C_{\text{ét}}, \mathcal{F})$ vanish for $i \geq 3$ since C is a smooth curve over an algebraically closed field [44, Tag 03SC (1)]. Since C is a smooth completion of U then $\mathrm{H}^2_c(U, j^*\mathcal{F}) = \mathrm{H}^2(C_{\text{ét}}, j_!j^*\mathcal{F})$ [26, p.93, paragraph before III.1.29].

Combining (4.3.6) and (4.3.7), we find

$$\mathrm{H}^i(C_{\text{ét}}, \mathcal{F}) \simeq \begin{cases} A^{\pi_1(U,\overline{\eta})} & \text{if } r = 0 \\ A_{\pi_1(U,\overline{\eta})(-1)} & \text{if } r = 2, \\ 0 & \text{if } r \geq 3 \end{cases}$$

and the long exact sequence (4.3.8) reads

$$0 \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{F}) \to \mathrm{H}^1(\pi_1(U, \overline{\eta}), A) \to \bigoplus_{v \in Z} A_{I(v)}(-1) \to A_{\pi_1(U,\overline{\eta})(-1)} \to 0.$$

□

Corollary 4.3.9. *In 4.3.6, the characteristic polynomial of the geometric Frobenius automorphism* Frob_q *acting on* $\mathrm{H}^2_Z(C, \mathcal{F})$ *is*

$$\det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^2_Z(C, \mathcal{F})\right) = \prod_{v \in Z} \det\left(1 - \mathrm{Frob}_q^{d_v}\, T^{d_v} \,|\, \mathrm{H}^1(I(v), A)\right).$$

Proof. There is a functorial action of the geometric Frobenius Frob_q on the group $\mathrm{H}^2_Z(C, \mathcal{F}) = \mathrm{H}^2(Z_{\text{ét}}, i^!\mathcal{F})$ [44, Tag 03SV]. The groups $\mathrm{H}^2_Z(C, \mathcal{F})$ and $\mathrm{H}^2_Z(C, j_!j^*\mathcal{F})$ being functorially isomorphic, we have an action of Frob_q on the latter group by transport of structure. Now, consider the isomorphism

$$\mathrm{H}^2_Z(C, j_!j^*\mathcal{F}) \simeq \bigoplus_{v \in Z} \mathrm{H}^2_v(C, j_!j^*\mathcal{F}).$$

For each point $v \in Z$, let i_v be the closed immersion $\mathrm{Spec}(k_v) \to Z$ which picks up the point v in Z. The pullback of Frob_q to $\mathrm{Spec}(k_v)$ is $\mathrm{Frob}_q^{d_v}$, which acts functorially on

$$\mathrm{H}^2_v(C, j_!j^*\mathcal{F}) = \mathrm{H}^2\left(\mathrm{Spec}(k_v)_{\text{ét}}, (i_v \circ i)^* j_!j^*\mathcal{F}\right).$$

If $\det\left(1 - \mathrm{Frob}_q^{d_v}\, T \,|\, \mathrm{H}^2_v(C, j_!j^*\mathcal{F})\right)$ is the characteristic polynomial of $\mathrm{Frob}_q^{d_v}$ action on $\mathrm{H}^2_v(C, j_!j^*\mathcal{F})$, then the contribution of the place v to the characteristic polynomial $\det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^2_Z(C, j_!j^*\mathcal{F})\right)$ is $\det\left(1 - \mathrm{Frob}_q^{d_v}\, T^{d_v} \,|\, \mathrm{H}^2_v(C, j_!j^*\mathcal{F})\right)$. Therefore,

$$\det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^2_Z(C, \mathcal{F})\right) = \prod_{v \in Z} \det\left(1 - \mathrm{Frob}_q^{d_v}\, T^{d_v} \,|\, \mathrm{H}^2_v(C, j_!j^*\mathcal{F})\right).$$

The isomorphisms (4.3.1), (4.3.2) and (4.3.3) are all canonical. We believe that through these isomorphisms there is an action of $\mathrm{Frob}_q^{d_v}$ by transport of structure on each of these groups. At

the moment, we cannot provide a detailed proof of this claim, but we hope to do so in the near future. As a consequence, we have equalities

$$\begin{aligned}\det\left(1 - T^{d_v}\operatorname{Frob}_q^{d_v} \mid \mathrm{H}^2_v(C, j_!j^*\mathcal{F})\right) &= \det\left(1 - T^{d_v}\operatorname{Frob}_q^{d_v} \mid \mathrm{H}^2_v(\operatorname{Spec}(\mathcal{O}^h_{C,v}), j_!j^*\mathcal{F})\right)\\ &= \det\left(1 - T^{d_v}\operatorname{Frob}_q^{d_v} \mid \mathrm{H}^1(\operatorname{Spec}(K_v), j^*\mathcal{F})\right)\\ &= \det\left(1 - T^{d_v}\operatorname{Frob}_q^{d_v} \mid \mathrm{H}^1(D(v), A)\right)\\ &= \det\left(1 - T^{d_v}\operatorname{Frob}_q^{d_v} \mid \mathrm{H}^1(I(v), A)\right).\end{aligned}$$

This gives the result. □

4.3.2 A Trivializing Covering for the Middle Extension Sheaf

In this subsection we state and prove our second main result of this chapter.

Theorem 4.3.10. *Let $\pi : C' \to C$ be a finite morphism of connected curves over k. Let $j : U \hookrightarrow C$ be the inclusion of a connected dense Zariski open subset U of C such that the restriction morphism $\pi : U' := \pi^{-1}(U) \to U$ is a finite Galois covering with Galois group G. Let $\mathcal{F}$ be a $\mathbb{Z}/n\mathbb{Z}$-middle extension sheaf on $C_{ét}$ corresponding to a free $\mathbb{Z}/n\mathbb{Z}$-module A of finite rank r_A. Suppose that*

(i) the sheaf $j^*\mathcal{F}$ is lisse on $U_{ét}$,

(ii) the sheaf $\pi^*\mathcal{F}$ isomorphic to the constant free $\mathbb{Z}/n\mathbb{Z}$-module of rank r_A and

(iii) the group G satisfies the assumptions of Theorem C.

For each v in the complement $Z := C - U$, choose exactly one point w_v in $Z' := \pi^{-1}(Z)$ lying over it and let $I(w_v|v)$ be the inertia group of the pair corresponding to these places. Then we have an exact sequence of Abelian groups

$$0 \to \mathrm{H}^1(C_{ét}, \mathcal{F}) \to \left(\operatorname{Jac}(C')(k)[n]^G\right)^{\oplus r_A} \to \bigoplus_{v\in Z} \mathrm{H}^1\left(I(w_v|v), A\right) \to 0.$$

Definition 4.3.11 (Standard Induction)**.** Let G be a group, let H be a subgroup of G, let R be a commutative ring and let N be a left $R[H]$-module. The *standard induction* of N from H to G is

$$\operatorname{Ind}_H^G(N) := R[G] \otimes_{R[H]} N.$$

It has a structure of left $R[G]$-module by multiplication on the left factor of the tensor product.

Lemma 4.3.12. *In the context of Theorem 4.3.10, the group $\mathrm{H}^2_{Z'}(C'_{ét}, \pi^*\mathcal{F})^G$ is isomorphic to $\bigoplus_{v\in Z} (A(-1))^{I(w_v|v)}$.*

Proof. From Proposition 4.3.8, we know that $\mathrm{H}^2_{Z'}(C', \pi^*\mathcal{F})$ is isomorphic to $\bigoplus_{w\in Z'} A_{I(w)}(-1)$. Since $\pi_1(U', \overline{x'})$ acts trivially on A, then for each $w \in Z'$, the inertia group $I(w)$ acts trivially on A. Therefore, $\mathrm{H}^2_{Z'}(C', \pi^*\mathcal{F})$ is isomorphic to $\bigoplus_{w\in Z'} A(-1)$.

For each $v \in Z$, choose a unique preimage w_v in Z'. The cohomology group $\mathrm{H}^1(I(w_v), A)$ is a left $(\mathbb{Z}/n\mathbb{Z})[I(v)]$-module on which $I(w)$ acts trivially. It therefore acquires a canonical structure of left $(\mathbb{Z}/n\mathbb{Z})[I(w_v|v)]$-module. The finite index of $I(w_v)$ in G equals the cardinality of the Galois G-orbit Σ_v of v. By Shapiro's lemma [33, p.62, (1.6.4) Proposition], we have a group isomorphism

$$\left(\bigoplus_{w\in\Sigma_v} \mathrm{H}^1(I(w_v), A)\right)^G \simeq \mathrm{H}^1(I(w_v), A)^{I(w_v|v)}.$$

Since G acts trivially on the set Z, the G-invariants of a direct sum indexed by Z equals the direct sum indexed by Z of the G-invariants of each summand. Hence,

$$\left(\mathrm{H}^2_{Z'}(C', \pi^*\mathcal{F})\right)^G \simeq \left(\bigoplus_{w\in Z'} A(-1)\right)^G \simeq \bigoplus_{v\in Z}\left(\bigoplus_{w\in\Sigma_v} A(-1)\right)^G \xrightarrow{\simeq} \bigoplus_{v\in Z} (A(-1))^{I(w_v|v)}.$$

□

Proof of Theorem 4.3.10. Let $j' : U' \hookrightarrow C'$ be the inclusion coming from j. We have an exact sequence of G-modules. We believe that the G-equivariance of this exact sequence follows from the functoriality of its construction. We haven't been able to provide a detailed proof of this claim, but we hope to do so in the near future.

$$0 \to \mathrm{H}^1(C'_{\text{ét}}, \pi^*\mathcal{F}) \to \mathrm{H}^1(U'_{\text{ét}}, j'^*\pi^*\mathcal{F}) \to H^2_{Z'}(C', \pi^*\mathcal{F}).$$

Since the functor of G-invariants is left exact, this yields the exact sequence of groups

$$0 \to \mathrm{H}^1(C'_{\text{ét}}, \mathcal{F}')^G \to \mathrm{H}^1(U'_{\text{ét}}, j'^*\mathcal{F}')^G \to H^2_{Z'}(C', \mathcal{F}')^G.$$

Now, we have a morphism

$$\gamma : \bigoplus_{v\in Z} \mathrm{H}^1(I(v), A) \to \bigoplus_{v\in Z} \mathrm{H}^1(I(w_v), A)^{I(w_v|v)}$$

given on the summand indexed by $v \in Z$ by the restriction morphism

$$\rho_{w_v|v} : \mathrm{H}^1(I(v), A) \to \mathrm{H}^1(I(w_v), A)^{I(w_v|v)}.$$

In other words,

$$\gamma = \bigoplus_{v\in Z} \rho_{w_v|v}.$$

This morphism corresponds to a morphism

$$\mathrm{H}^2_Z(C, \mathcal{F}) \to \mathrm{H}^2_{Z'}(C', \pi^*\mathcal{F})^G$$

in view of Proposition 4.3.8 and Lemma 4.3.12. For each $v \in Z$, part of the inflation-restriction-transgression exact sequence for $I(v)$ and its open subgroup of finite index $I(w_v)$ is

$$0 \to \mathrm{H}^1(I(w_v|v), A) \xrightarrow{\mathrm{Inf}_{w_v|v}} \mathrm{H}^1(I(v), A) \xrightarrow{\rho_{w_v|v}} \mathrm{H}^1(I(w_v), A)^{I(w_v|v)} \xrightarrow{\mathrm{trg}_{w_v|v}} \mathrm{H}^2(I(w_v|v), A).$$

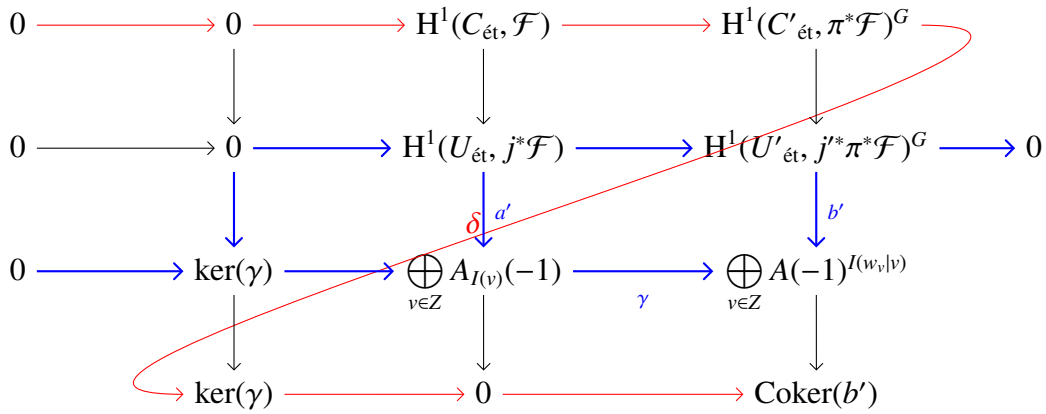
Thus, the kernel of the morphism γ is

$$\ker(\gamma) \simeq \bigoplus_{v\in Z} \mathrm{H}^1(I(w_v|v), A).$$

We then have the following solid commutative diagram with exact rows and columns.

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & 0 & \dashrightarrow & \mathrm{H}^1(C_{\text{ét}}, \mathcal{F}) & \overset{\alpha}{\dashrightarrow} & \mathrm{H}^1\left(C'_{\text{ét}}, \pi^*\mathcal{F}\right)^G & & \\
 & & & & \downarrow a & & \downarrow b & & \\
 & & 0 & \longrightarrow & \mathrm{H}^1(U_{\text{ét}}, j^*\mathcal{F}) & \overset{\beta}{\longrightarrow} & \mathrm{H}^1(U'_{\text{ét}}, j'^*\pi^*\mathcal{F})^G & \longrightarrow & 0 \\
 & & & & \downarrow a' & & \downarrow b' & & \\
0 & \longrightarrow & \bigoplus_{v\in Z} \mathrm{H}^1(I(w_v|v), A) & \longrightarrow & \bigoplus_{v\in Z} A_{I(v)}(-1) & \overset{\gamma}{\longrightarrow} & \bigoplus_{v\in Z} A(-1)^{I(w_v|v)} & \longrightarrow & \bigoplus_{v\in Z} \mathrm{H}^2(I(w_v|v), A) \\
 & & & & \downarrow & & & & \\
 & & & & 0 & & & &
\end{array}$$

Let $\xi \in \mathrm{H}^1(C_{\text{ét}}, \mathcal{F})$ By commutativity of the solid square, we have $(b' \circ \beta)(a(\xi)) = 0$, so that $a\left(\mathrm{H}^1(C_{\text{ét}}, \mathcal{F})\right) \subset \ker(b' \circ \beta)$. This induces a morphism $\alpha : \mathrm{H}^1(C_{\text{ét}}, \mathcal{F}) \to \mathrm{H}^1(C'_{\text{ét}}, \pi^*\mathcal{F})^G$ given by $\xi \mapsto \beta(a(\xi))$. Since β is injective, the morphism α is injective as well. We can then apply the snake lemma to the following diagram.



Thus, we have a short exact sequence

$$0 \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{F}) \to \mathrm{H}^1(C'_{\text{ét}}, \pi^*\mathcal{F})^G \to \ker(\gamma) \to 0.$$

Now, the sheaf $\pi^*\mathcal{F}$ is isomorphic to the constant free $\mathbb{Z}/n\mathbb{Z}$-module of finite rank r_A. By choosing an isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\simeq} \mu_n$ of sheaves on $C'_{\text{ét}}$, we find, using Proposition 2.2.58, the isomorphisms

$$\mathrm{H}^1(C'_{\text{ét}}, \pi^*\mathcal{F})^G \simeq \mathrm{H}^1\left(C'_{\text{ét}}, (\mathbb{Z}/n\mathbb{Z})^{\oplus r_A}\right)^G \simeq \left(\mathrm{H}^1\left(C'_{\text{ét}}, \mathbb{Z}/n\mathbb{Z}\right)^G\right)^{\oplus r_A} \simeq \left(\mathrm{Jac}(C')(k)[n]^G\right)^{\oplus r_A}.$$

□

Corollary 4.3.13. *If $\pi : C_0' \to C_0$ is a k_0-finite morphism of geometrically connected curves defined over k_0, and if H_n denotes the kernel of the canonical (necessarily)* Frob_q*-equivariant homomorphism*

$$H^2_Z(C, \mathcal{F}) \to H_{Z'}(C', \pi^*\mathcal{F})^G,$$

then the sequence

$$0 \to \mathrm{H}^1(C_{ét}, \mathcal{F}) \to \left(\mathrm{Jac}(C')(k)[n]^G\right)^{\oplus r_A} \to H_\ell \to 0$$

is exact in the category of Frob_q*-modules. In fact, the sequence*

$$0 \to \mathrm{H}^1(C_{ét}, \mathcal{F}) \to \left(\mathrm{Jac}(C')(k)[n]^G\right)^{\oplus r_A} \to \bigoplus_{v \in Z} \mathrm{H}^1\left(I(w_v|v), A\right) \to 0$$

is exact in the category of Frob_q*-modules. In particular, the characteristic polynomial of* Frob_q *on* $\bigoplus_{v \in Z} \mathrm{H}^1\left(I(w_v|v), A\right)$ *is*

$$\prod_{v \in Z} \det\left(1 - \mathrm{Frob}_q^{d_v}\, T^{d_v} | \, \mathrm{H}^1(I(w_v|v), A)\right).$$

Proof. Since π is defined over k_0, the action of G commutes with the action of Frob_q. Therefore, Frob_q acts canonically on $\left(\mathrm{Jac}(C')(k)[n]^G\right)^{\oplus r_A}$ and on $\mathrm{H}^1(C_{\text{ét}}, \mathcal{F})$ and the inclusion morphism is Frob_q-equivariant by canonicity of its construction. The canonicity of the morphism from the snake lemma implies that the morphism $\left(\mathrm{Jac}(C')(k)[\ell]^G\right)^{\oplus r_A} \to H_n$ is Frob_q-equivariant. We've shown in Corollary 4.3.9 that Frob_q acts in an equivariant way on the chain of isomorphisms

$$\mathrm{H}^2_Z(C, \mathcal{F}) \xrightarrow{\simeq} \bigoplus_{\overline{v} \in Z} \mathrm{H}^1(I(\overline{v}), A).$$

Its subgroup $\bigoplus_{\overline{v} \in Z} \mathrm{H}^1\left(I(\overline{w_v}|\overline{v}), A\right)$ therefore inherits a canonical action of Frob_q. In particular, the characteristic polynomial of Frob_q on $\bigoplus_{\overline{v} \in Z} \mathrm{H}^1\left(I(\overline{w_v}|\overline{v}), A\right)$ is deduced from the one of $\mathrm{H}^2_Z(C, \mathcal{F})$ which is given in Corollary 4.3.9. □

We finish this section by proving the following corollary.

Corollary 4.3.14. *In the context of Theorem 4.3.10, if for each $v \in Z$ the order of $I(w_v|v)$ is coprime with n, then*

$$\mathrm{H}^1(C_{ét}, \mathcal{F}) \simeq \left(\mathrm{Jac}(C)(k)[n]\right)^{\oplus r_A}.$$

The following proposition probably exists in the literature, but we could not find a reference.

Proposition 4.3.15. *Let C be a smooth, proper and geometrically connected curve over an algebraically closed field k. Let K be the function field of C. Let also U be a dense Zariski open subset of C and let Z be its finite closed complement. Let n be a positive integer that is not divisible by* $\mathrm{char}(k)$*. Then there is a group isomorphism from* $\mathrm{H}^1(U_{ét}, \mu_n)$ *to the group*

$$K(Z, n) := \{fK^{\times n} : \mathrm{ord}_v(f) \equiv 0 \bmod n, \forall v \in U\}$$

Proof. Let $\overline{x}$ be a geometric point of some point $x \in U$. By Lemma 4.2.4 we have

$$\mathrm{H}^1\left(U_{\text{ét}}, \mu_n\right) = \mathrm{H}^1\left(\pi_1(U, \overline{x}), \mu_n\right).$$

The latter equals $\mathrm{Hom}\left(\pi_1(U, \overline{x}), \mu_n\right)$ since $\mu_n \subset k$. Applying the left exact contravariant functor $\mathrm{Hom}(\bullet, \mu_n)$ to Equation (2.2.3), we find the exact sequence

$$1 \to \mathrm{Hom}\left(\pi_1(U, \overline{x}), \mu_n\right)) \to \mathrm{Hom}(G_K, \mu_n) \to \mathrm{Hom}(\mathrm{ncl}_{G_K}(S), \mu_n),$$

where $S = \cup_{v \in |U|} I(v)$. Therefore,

$$\mathrm{Hom}\left(\pi_1(U, \overline{x}), \mu_n\right) = \left\{\phi \in \mathrm{Hom}(G_K, \mu_n) : \rho_v(\phi) = 0 \in \mathrm{H}^1(I(v), \mu_n), \forall v \in U\right\}, \tag{4.3.9}$$

where $\rho_v : \mathrm{Hom}(G_K, \mu_n) \to \mathrm{Hom}(I(v), \mu_n)$ is the restriction morphism coming from the inclusion of $I(v)$ in G_K given by a fixed field embedding $K \hookrightarrow K_v$. It follows from Hilbert's Theorem 90 that $\mathrm{H}^1(G_K, \mu_n) \simeq K^\times / K^{\times n}$ and $\mathrm{H}^1(G_{K_v}, \mu_n) \simeq K_v^\times / K_v^{\times n}$ for each place v of K [33, p.344, Chapter VI]. Using the valuation map $\mathrm{ord}_v : K_v^\times \to \mathbb{Z}$ we deduce an isomorphism

$$\mathrm{ord}_v \bmod n : K_v^\times / K_v^{\times n} \xrightarrow{\simeq} \mathbb{Z}/n\mathbb{Z}.$$

Since k is algebraically closed, $G_{K_v} = I(v)$ and so for each $v \in U$ we have a commutative diagram

$$\begin{array}{ccccc}
\mathrm{H}^1(G_K, \mu_n) & \xrightarrow{\simeq} & K^\times / K^{\times n} & & \\
\downarrow{\scriptstyle \rho_v} & & \downarrow{\scriptstyle \rho_v} & \searrow & \\
\mathrm{H}^1(I(v), \mu_n) & \xrightarrow[\simeq]{} & K_v^\times / K_v^{\times n} & \xrightarrow[\mathrm{ord}_v \bmod n]{} & \mathbb{Z}/n\mathbb{Z}.
\end{array}$$

This identifies the restriction map $\rho_v : \mathrm{Hom}(G_K, \mu_n) \to \mathrm{Hom}(I(v), \mu_n)$ with the map $(\mathrm{ord}_v \bmod n) \circ \rho_v : K^\times / K^{\times n} \to \mathbb{Z}/n\mathbb{Z}$. Finally, the commutativity of the previous diagram implies that the right-hand side of Equation (4.3.9) is identified with

$$\{fK^{\times n} : \mathrm{ord}_v(f) \equiv 0 \bmod n, \forall v \in U\}.$$

□

Proof of Corollary 4.3.14. Since the sheaf μ_n on $C_{\text{ét}}$ is a middle extension sheaf, it follows from Proposition 2.2.58, Proposition 4.3.15, Proposition 4.3.8 and the computations of section 4.3.1, that we have the following exact sequence

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \mathrm{H}^1(C_{\text{ét}}, \mu_n) & \longrightarrow & \mathrm{H}^1(U_{\text{ét}}, j^*\mu_n) & \longrightarrow & H^2_Z(C_{\text{ét}}, \mu_n) & \longrightarrow & \mathrm{H}^2(C_{\text{ét}}, \mu_n) & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \| & & \\
0 & \longrightarrow & \mathrm{Jac}(C)(k)[n] & \longrightarrow & K(Z, n) & \xrightarrow{(\mathrm{ord}_v(f))_{v \in Z}} & (\mathbb{Z}/n\mathbb{Z})^{\oplus \# Z} & \xrightarrow{\sum_{v \in Z} \mathrm{proj}_v} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0.
\end{array}$$

where proj_v is the projection map of $(\mathbb{Z}/n\mathbb{Z})^{\oplus \# Z}$ onto its factor indexed by v. Therefore,

$$\mathrm{Jac}(C)(k)[n] = \ker\left((\mathrm{ord}_v(f))_{v \in Z} : K(Z, n) \to (\mathbb{Z}/n\mathbb{Z})^{\# Z}\right). \tag{4.3.10}$$

Since the sheaf μ_n on $C_{\text{ét}}$ is a middle extension and its pullback $j^*\mu_n$ is a lisse sheaf on $U_{\text{ét}}$, then by Theorem 4.3.10 we have the short exact sequence

$$1 \to \mathrm{Jac}(C)(k)[n] \to (\mathrm{Jac}(C')(k)[n])^G \to \bigoplus_{v\in Z} \mathrm{H}^1\left(I(w_v|v), \mu_n\right) \to 1.$$

If for each $v \in Z$ the order of $I(w_v|v)$ is coprime to n, then $\mathrm{Jac}(C)(k)[n] = (\mathrm{Jac}(C')(k)[n])^G$. Therefore, $\ker(\gamma) = 0$ and so

$$\mathrm{H}^1(C_{\text{ét}}, \mathcal{F}) \simeq \mathrm{H}^1({C'}_{\text{ét}}, \mathcal{F}')^G \simeq \left(\mathrm{Jac}(C')(k)[n]^G\right)^{\oplus r_A} = (\mathrm{Jac}(C)(k)[n])^{\oplus r_A}.$$

□

4.4 Néron Models of Elliptic Curves

4.4.1 Summary

The goal of this section is to provide the necessary background for the application of the results on middle extension sheaves to the setting of Néron models of elliptic curves. We introduce the Néron model $\mathcal{E} \to C_0$ of an elliptic curve E/K_0, its identity component $\mathcal{E}^0$ and its group of components Φ and relate them by a short exact sequence. Given a positive integer coprime with the characteristics of all residue fields of places of K_0 (for a perfect field k_0), we obtain a short exact sequence relating the n-torsion subgroups of the previous objects. The theory of middle extension sheaves allows us to compute the étale cohomology groups of $\mathcal{E}[n]$. We can then express the cohomology groups with coefficients in $\mathcal{E}^0[n]$ in terms of the cohomology groups with coefficients in $\mathcal{E}[n]$ and in $\Phi[n]$.

4.4.2 The n-torsions of $\mathcal{E}, \mathcal{E}^0$ and Φ

Let n be an integer that is not divisible by the characteristic of the residue field $k_{v,0}$ for any $v \in C_0$. The multiplication-by-n map $\times n : \mathcal{E} \to \mathcal{E}$ is étale [5, p.179, 7.3/2 (b)]. Therefore, the kernel $\mathcal{E}[n]$ of this morphism is an étale group scheme on C_0.

Hypothesis 4.4.1. From now on, we will suppose that the elliptic curve E/K_0 is nonconstant. Its locus of good reduction U_0 is an open affine subset of the projective curve C_0.

Proposition 4.4.2. *The sheaf $\mathcal{E}[n] \to C_0$ is a $\mathbb{Z}/n\mathbb{Z}$-middle extension sheaf.*

Proof. The sheaf $\mathcal{E}[n] \to C_0$ is a sheaf of $\mathbb{Z}/n\mathbb{Z}$-modules by construction. We will verify the assumptions of Lemma 4.3.5. Let $j : U_0 \to C_0$ be the inclusion of the dense Zariski open subset of C_0 which is the locus of good reduction of E/K_0. The sheaf $j^*\mathcal{E}[n] \to U_0$ is lisse. Indeed, it is constructible, has finite geometric stalks all equal to $E[n]$ and therefore, for any point v of U_0, the sheaf $j^*\mathcal{E}[n]$ is constant equal to $E[n]$ in some étale neighbourhood of v. The sheaf $j^*\mathcal{E}[n]$ is therefore locally constant.

We now verify that the adjunction morphism $\mathcal{E}[n] \to j_*j^*\mathcal{E}[n]$ is an isomorphism. To do this, it suffices to verify the statement on the geometric stalks.

Let $v \in U_0$. Then $(\mathcal{E}[n])_{\overline{v}} \simeq E[n]$ and by [26, p.71, II.3.5(b)], we have

$$(j_* j^* \mathcal{E}[n])_{\overline{v}} = (j^* \mathcal{E}[n])_{\overline{v}} \simeq E[n].$$

Now, let $v \in C_0 - U_0$. By [26, p.70, II.3.2(b)], we have

$$(j_* j^* \mathcal{E}[n])_{\overline{v}} = \mathrm{H}^0\left((U_0 \times_{C_0} \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}}))_{\text{ét}}, f'^* j^* \mathcal{E}[n]\right),$$

where $f : \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}}) \to C_0$ is the canonical morphism and $f' : U_0 \times_{C_0} \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}}) \to U_0$ is the base change of f. Now let $\widetilde{j} : U_0 \times_{C_0} \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}}) \to \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}})$ be the base change of j. This map is an open immersion on $\mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}})$. The fiber of the point $\overline{v}$ of $\widetilde{j}$ is empty. Indeed, if there were a point w in it, then $\widetilde{j}(w) = \overline{v}$ would need to coincide, by the property of fiber product of $U_0 \times_{C_0} \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}})$, with $f'(w) \in U_0$. Since v is not in U_0, there is no such point w. So the image of $\widetilde{j}$ is the generic geometric point $\overline{\eta}$. Hence,

$$U_0 \times_{C_0} \mathrm{Spec}(\mathcal{O}^{\mathrm{sh}}_{C_0,\overline{v}}) = j^{-1}(\overline{\eta}) = \mathrm{Spec}(K^{\mathrm{sh}}_{\overline{v},0}).$$

Therefore,

$$(j_* j^* \mathcal{E}[n])_{\overline{v}} = \mathrm{H}^0\left(G_{K^{\mathrm{sh}}_{\overline{v},0}}, (\mathcal{E}[n])_{\overline{\eta}}\right) = \mathrm{H}^0\left(I(v), E[n]\right) = E[n]^{I(v)}.$$

This is also $(\mathcal{E}[n])_{\overline{v}}$. □

Since the integer n is different from $\mathrm{char}(k_{v,0})$ for any $v \in C_0$, then the group scheme $\mathcal{E}^0[n]$ is flat and quasi-finite [27, p.267, Corollary C.9]. From [18, p.144, Lemma 17], we have a short exact sequence of étale sheaves on C_0:

$$0 \to \mathcal{E}^0[n] \to \mathcal{E}[n] \to \Phi[n] \to 0. \tag{4.4.1}$$

This is also a short exact sequence of étale sheaves on C.

4.5 Cohomology of n-torsion Sheaves

In this section, we compute the terms arising from the long exact sequence in étale cohomology associated to the short exact sequence (4.4.1) of étale sheaves on C.

Since $\Phi[n]$ is a skyscraper sheaf supported on a subset of the finite set Z, then $\mathrm{H}^i(C_{\text{ét}}, \Phi[n]) = 0$ for $i \geq 1$ by [47, p.159, (10.1.2) Lemma] and, if for each closed point v of Z, we write i_v for the closed embedding $\mathrm{Spec}(k_v) \hookrightarrow Z$ corresponding of the choice of the closed point v in Z, then

$$\mathrm{H}^0(C_{\text{ét}}, \Phi[n]) = \mathrm{H}^0(Z_{\text{ét}}, \Phi[n]) = \bigoplus_{v \in Z} i_{v,*} \Phi_v(k_v)[n].$$

By Proposition 4.4.2, the sheaf $\mathcal{E}[n]$ is a $\mathbb{Z}/n\mathbb{Z}$-middle extension sheaf over the smooth, proper, and geometrically connected curve C_0/k_0. The generic geometric fiber of $\mathcal{E}[n]$ is $E(K)[n]$. By Proposition 4.3.8 we have

$$\mathrm{H}^i(C_{\text{ét}}, \mathcal{E}[n]) \simeq \begin{cases} E(K)[n]^{\pi_1(U,\overline{x})} & \text{if } i = 0 \\ E(K)[n](-1)_{\pi_1(U,\overline{x})} & \text{if } i = 2, \\ 0 & \text{if } i \geq 3. \end{cases}$$

Now Shioda [41, p.25, Proposition 1.6] proved that $\mathcal{E}^0(C)$ was a torsion-free subgroup of finite index in $\mathcal{E}(C)$. Therefore, $H^0(C_{\text{ét}}, \mathcal{E}^0[n]) = 0$.

Putting all this together, the long exact sequence associated to (4.4.1) becomes

$$0 \to E(K)[n]^{\pi_1(U,\overline{x})} \to \bigoplus_{v \in Z} \Phi_v(k_v)[n] \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}^0[n]) \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[n]) \to 0$$

and

$$\mathrm{H}^2(C_{\text{ét}}, \mathcal{E}^0[n]) = \mathrm{H}^2(C_{\text{ét}}, \mathcal{E}[n]) \simeq E(K)[n](-1)_{\pi_1(U,\overline{x})}.$$

In fact, $E(K)[n]^{\pi_1(U,\overline{x})} = E(K_0)[n]$ since $\pi_1(U, \overline{x})$ is the Galois group of the maximal extension of K which is unramified outside of Z [26, p.41, I.5 Example (b)].

If $E(K_0)[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{\oplus 2}$, then $\mathcal{E}[n]$ is the constant sheaf $(\mathbb{Z}/n\mathbb{Z})^{\oplus 2}$. Fixing an isomorphism of étale sheaves $\mu_n \xrightarrow{\simeq} \mathbb{Z}/n\mathbb{Z}$ on C and using the facts that $\mathrm{H}^1(C_{\text{ét}}, \mu_n) \simeq \mathrm{Jac}(C)(k)[n]$, $\mathrm{H}^2(C_{\text{ét}}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$, we have

$$\mathrm{H}^2(C_{\text{ét}}, \mathcal{E}^0[n]) = \mathrm{H}^2(C_{\text{ét}}, \mathcal{E}[n]) \simeq (\mathbb{Z}/n\mathbb{Z})^{\oplus 2} \text{ and } \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[n]) \simeq \mathrm{Jac}(C)(k)[n]^{\oplus 2}.$$

Now suppose that $E(K)[n] = \{O\}$. Then,

$$\mathrm{H}^2(C_{\text{ét}}, \mathcal{E}^0[n]) = \mathrm{H}^2(C_{\text{ét}}, \mathcal{E}[n]) = 0$$

and if C_n is the curve corresponding to the nth-division field $K_n := K(E[n])$ of K, then by Theorem 4.3.10 we have the short exact sequence of groups

$$0 \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[n]) \to \left(\mathrm{Jac}(C_n)(k)[n]^{G_n}\right)^{\oplus 2} \to \bigoplus_{v \in Z} \mathrm{H}^1(I(w_v|v), E(K)[n]) \to 0$$

and the short exact sequence

$$0 \to \bigoplus_{v \in Z} i_{v,*}\Phi_v(k_v)[n] \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}^0[n]) \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[n]) \to 0, \tag{4.5.1}$$

Hypothesis 4.5.1. For the remainder of this text we assume that the integer n is a prime ℓ different from $\mathrm{char}(k_0)$.

The assumption on n simplifies the exposition. Moreover, it suffices to compute the reduction of the polynomial $L(T, E/K_0) \in 1 + T \cdot \mathbb{Z}[T]$ modulo prime integers in order to determine $L(T, E/K_0)$. Suppose that k_0 is a finite field with q elements, that $\mu_\ell \subset k_0$, with ℓ different from $\mathrm{char}(k_0)$ and that $E(K_0)[\ell] = \{O\}$. In Theorem 4.10.1, we show that

$$L(T, E/K_0) \equiv \det(1 - \mathrm{Frob}_q T \,|\, \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}^0[\ell])) \bmod \ell.$$

In this situation, ℓ divides $q - 1$ and the group Galois group $\mathrm{Gal}(K_0(E[\ell])/K_0)$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$. The short exact sequence (4.5.1) of finite-dimensional $\mathbb{F}_\ell$-vector spaces splits. Therefore, to compute the characteristic polynomial of Frob_q on $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}^0[\ell])$ is equal to the product of the characteristic polynomials of Frob_q on $\Phi(Z)[\ell]$ and on $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell])$. We compute the characteristic polynomial of Frob_q on $\Phi(Z)[\ell]$ in Theorem 4.6.1. To compute the characteristic polynomial of Frob_q on $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell])$ we use the short exact sequence provided by Theorem 4.3.10 which is Frob_q-equivariant by Corollary 4.3.13.

4.6 Action of Frob_q on the ℓ-Torsion Subgroup of $\Phi(Z)$

As we have just seen, it is important to understand how the geometric Frobenius endomorphism Frob_q acts on the global sections $\Phi(Z)[\ell]$. In order to do this, we need to understand the action of Frob_q on Z and the induced action of the local geometric Frobenii $\mathrm{Frob}_q{}^{d_v}$ on the k_v-rational points of each local group of components $\Phi_v(k_v)$ where, for a closed point v of Z_0, $\bar{v}$ is a fixed closed point of C lying over v in the Galois orbit of v under the action of G_{k_0}.

Unless specifically mentioned, we work from now on under the assumption that the field of constants k_0 of K_0 is a finite field of order q, where q is a power of a prime $p \geq 5$. In the statement and the proof of the result below, we use the notation $\prod_{v\in Z_0 S}$ to mean that the product is over the places $v \in Z_0$ which have Kodaira symbol S.

Theorem 4.6.1. *Let E/K_0 be a nonconstant elliptic curve. The characteristic polynomial of Frob_q acting on $\Phi(Z)[\ell]$ is*

$$\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[\ell]\right) = \prod_{v\in Z_0} \det\left(1 - \mathrm{Frob}_q^{d_v}\, T^{d_v}|\Phi_v(k_v)[\ell]\right).$$

More precisely,

(i) if $\ell \geq 5$, then

$$\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[\ell]\right) = \prod_{\substack{v\in Z_0\\ I_{\ell n}, n\geq 1}} (1 - T^{d_v}) \times \prod_{\substack{v\in Z_0\\ I_{\ell n,2}, n\geq 1}} (1 + T^{d_v}).$$

(ii) if $\ell = 3$, then

$$\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[3]\right) = \prod_{\substack{v\in Z_0\\ I_{3n}, n\geq 1, IV, IV^*}} (1 - T^{d_v}) \times \prod_{\substack{v\in Z_0\\ I_{3n,2}, n\geq 1}} (1 + T^{d_v}) \times \prod_{\substack{v\in Z_0\\ IV_2, IV_2^*}} (1 + T^{d_v}).$$

(iii) if then $\ell = 2$, then

$$\begin{aligned}\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[2]\right) = &\prod_{\substack{v\in Z_0\\ S_1}} (1 - T^{d_v}) \times \prod_{\substack{v\in Z_0\\ I_{2n}^*, n\geq 0}} (1 - T^{d_v})^2\\ &\times \prod_{\substack{v\in Z_0\\ I_{2n-2,2}, n\geq 1}} (1 - T^{2d_v}) \times \prod_{\substack{v\in Z_0\\ I_{n-2}^*, n\geq 2 \text{ even}}} (1 - 2T + T^{2d_v})\\ &\times \prod_{\substack{v\in Z_0\\ I_{0,3}^*}} (1 + T^{d_v} + T^{2d_v}),\end{aligned}$$

where $S_1 := \{I_{2n}, n \geq 1, III, III^*, I_{2n+1}^*, n \geq 0, I_{2n-1,2}, n \geq 1, I_{n-2,2}^*, n \geq 3 \text{ odd}\}$.

Proof. For each closed point $v \in Z_0$, the absolute Galois group $G_{k_{v,0}} = \mathrm{Gal}(k_v/k_{v,0})$, is topologically generated by the geometric Frobenius

$$\mathrm{Frob}_q^{d_v} : k_v \to k_v : \alpha \mapsto \alpha^{1/q^{d_v}}.$$

The element $\mathrm{Frob}_q^{d_v}$ acts naturally on the local group of components $\Phi_v(k_v)$ via its action on the k_v-points of the special fiber $\mathcal{X}_{k_v} \to \mathrm{Spec}(k_v)$ of the proper minimal regular model of E/K_v. If $\det\left(1 - \mathrm{Frob}_q^{d_v} T|\Phi_v(k_v)[\ell]\right)$ is the characteristic polynomial of $\mathrm{Frob}_q^{d_v}$ action on $\Phi_v(k_v)[\ell]$, then the contribution of the place v to the characteristic polynomial $\det\left(1 - \mathrm{Frob}_q T|\Phi(Z)[\ell]\right)$ is $\det\left(1 - \mathrm{Frob}_q^{d_v} T^{d_v}|\Phi_v(k_v)[\ell]\right)$. If $\Phi_v(k_v)[\ell] = \{0\}$, then the characteristic polynomial of $\mathrm{Frob}_q^{d_v}$ equals 1, and so does not contribute $\det\left(1 - \mathrm{Frob}_q T|\Phi(Z)[\ell]\right)$. We now therefore only focus on the places v with respect to which the elliptic curve has Kodaira symbols such that $\Phi_v(k_v)[\ell] \neq \{0\}$.

Label the $n \geq 1$ irreducible components of the special fiber of $\mathcal{X}_{k_{v,0}} \to \mathrm{Spec}(k_{v,0})$ as $\Gamma_i, 1 \leq i \leq n$, where Γ_1 is the irreducible component intersecting the closure $\overline{\{O\}}$ over the distinguished rational point $O \in E(K_0)$.

We first assume that $\mathrm{Frob}_q^{d_v}$ acts as the identity on $\Phi_v(k_v)$, so that $\Phi_v(k_v) = \Phi_v(k_{v,0})$. If $\Phi_v(k_v)[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}$, then

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T|\Phi_v(k_v)[\ell]\right) = 1 - T.$$

Now, suppose that $\ell = 2$. If $\Phi_v(k_v)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$, then

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T|\Phi_v(k_v)[2]\right) = (1 - T)^2,$$

while if $\Phi_v(k_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, then

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T|\Phi_v(k_v)[2]\right) = 1 - T.$$

From the first table of [25, p.497, Remark 10.2.24] we obtain the following table.

Action of $\mathrm{Frob}_q^{d_v}$ on $\Phi_v(k_v)[\ell]$ when $\Phi_v(k_{v,0}) = \Phi_v(k_v)$ and $\ell \geq 2$		
Kodaira Symbol over $k_{v,0}$	$\Phi_v(k_v)[\ell]$	$\det\left(1 - \mathrm{Frob}_q^{d_v} T^{d_v}\|\Phi_v(k_v)[\ell]\right)$
$I_{\ell n}, n \geq 1$	$\mathbb{Z}/\ell\mathbb{Z}$	$1 - T^{d_v}$
Action of $\mathrm{Frob}_q^{d_v}$ on $\Phi_v(k_v)[\ell]$ when $\Phi_v(k_{v,0}) = \Phi_v(k_v)$ and $\ell = 2$		
Kodaira Symbol over $k_{v,0}$	$\Phi_v(k_v)[2]$	$\det\left(1 - \mathrm{Frob}_q^{d_v} T^{d_v}\|\Phi_v(k_v)[2]\right)$
$III, III^*, I^*_{2n+1}, n \geq 0$	$\mathbb{Z}/2\mathbb{Z}$	$1 - T^{d_v}$
$I^*_{2n}, n \geq 0$	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	$(1 - T^{d_v})^2$
Action of $\mathrm{Frob}_q^{d_v}$ on $\Phi_v(k_v)[\ell]$ when $\Phi_v(k_{v,0}) = \Phi_v(k_v)$ and $\ell = 3$		
Kodaira Symbol over $k_{v,0}$	$\Phi_v(k_v)[3]$	$\det\left(1 - \mathrm{Frob}_q^{d_v} T^{d_v}\|\Phi_v(k_v)[3]\right)$
IV, IV^*	$\mathbb{Z}/3\mathbb{Z}$	$1 - T^{d_v}$

We now assume that the action of $\mathrm{Frob}_q^{d_v}$ on $\Phi_v(k_v)[\ell] \neq \{0\}$ is nontrivial, which is precisely when $\Phi_v(k_v) \neq \Phi_v(k_{v,0})$. The set $\Phi_v(k_{v,0})$ corresponds to the irreducible components that are geometrically integral and of multiplicity 1 in $\mathcal{X}_{v,0}$ and the set $\Phi_v(k_v)$ to the irreducible components of $\mathcal{X}_v$ [25, p.497, Remark 2.24].

We are going to refer to [25, pp.486-489] for the configurations of the irreducible components of the special fibers in what follows. We sketch the relevant content for our purposes and redirect the reader to the above source for details.

Remark 4.6.2. If v is a place of split multiplicative reduction with Kodaira symbol I_n, then $\Phi_v(k_v)[\ell]$ is a zero-dimensional (resp. one-dimensional) $\mathbb{F}_\ell$-vector space if and only if $\gcd(\ell, n) = 1$ (resp. ℓ divides n). Therefore, the characteristic polynomial of $\mathrm{Frob}_q^{d_v}$ acting on $\Phi_v(k_v)[\ell]$ has degree at most one. A similar reasoning applies to the other Kodaira symbols.

Suppose that $E/k_{v,0}$ has nonsplit multiplicative reduction at v. The irreducible components $\Gamma_i, 2 \leq i \neq n-1$ have intersection points p_{i-1} with Γ_{i-1} and p_i with Γ_{i+1}. The residue fields of these points are all isomorphic to a quadratic extension $k_{v,0}(p)$ of $k_{v,0}$ and moreover $\Gamma_i \simeq \mathbb{P}^1_{k_{v,0}(p)}$. The irreducible component Γ_n is a conic over $k_{v,0}$. If this conic is singular, then the Kodaira symbol attached to v is $I_{2n-1,2}$, while if Γ_n is smooth, then the corresponding Kodaira symbol is $I_{2n-2,2}$. The group $G_{k_{v,0}} =< \mathrm{Frob}_q^{d_v} >$ has the subgroup $G_{k_{v,0}(p)} =< \mathrm{Frob}_q^{2d_v} >$ which acts as the identity on $\Phi_v(k_v)[\ell]$. Therefore, there is an induced action of $< \mathrm{Frob}_q^{d_v} > / < \mathrm{Frob}_q^{2d_v} >$ on $\Phi_v(k_v)[\ell]$.

Suppose that $\ell \geq 3$. Then, we are only interested in places of nonsplit multiplicative reduction of the form $I_{\ell m,2}$ for some integer $m \geq 1$. Since $\Phi_v(k_{v,0})[\ell] = \{0\}$ and $\Phi_v(k_v)[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}$, then Frob_q acts by negation on $\Phi_v(k_v)[\ell]$ in this case, and we have

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T | \Phi_v(k_v)[\ell]\right) = 1 + T.$$

Now, suppose that $\ell = 2$. If Γ_n is smooth, then this quotient group can permute the components Γ_1 and Γ_n and exchange the points p_1 and p_{n-1}.

So for the Kodaira symbol $I_{2n-2,2}$, we have

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T | \Phi_v(k_v)[2]\right) = 1 + T.$$

If Γ_n is singular, then it does not correspond to a $k_{v,0}$-rational point of $\Phi_v(k_{v,0})$. Therefore, for the Kodaira symbol $I^*_{2n-1,2}$, the group $< \mathrm{Frob}_q^{d_v} > / < \mathrm{Frob}_q^{2d_v} >$ acts as the identity on $\Phi_v(k_v)[2]$ and in this case

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T | \Phi_v(k_v)[2]\right) = 1 - T.$$

Now, consider the Kodaira symbol IV_2. The special fiber has two irreducible components Γ_1 and Γ_2. The intersection point is $k_{v,0}$-rational. The irreducible component Γ_2 has multiplicity 1 but is a singular conic over $k_{v,0}$ and is in fact not geometrically irreducible: it splits into two Galois conjugate irreducible components over k_v. Since $\mathrm{Frob}_q^{d_v}$ fixes the irreducible component Γ_1, we have

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T | \Phi_v(k_v)[3]\right) = 1 + T.$$

For the Kodaira symbol IV_2^*, there are 5 irreducible components (without multiplicity). The only irreducible component besides Γ_1 which is of multiplicity 1 is Γ_5. The intersection point of Γ_4 and Γ_5 has residue is a quadratic extension $k_{v,0}(p)$ of $k_{v,0}$ and Γ_5 is isomorphic to $\mathbb{P}^1_{k_{v,0}(p)}$. Again, the subgroup $< \mathrm{Frob}_q^{2d_v} >$ of $< \mathrm{Frob}_q^{d_v} >$ acts as the identity on $\Phi_v(k_v)[3]$. Their quotient therefore permutes the two irreducible components of Γ_5 over k_v and fixes Γ_1. Thus,

$$\det\left(1 - \mathrm{Frob}_q^{d_v} T | \Phi_v(k_v)[3]\right) = 1 + T.$$

Now, suppose that the Kodaira symbol associated to v is $I^*_{0,2}$ (resp. $I_{0,3}$). Then, the special fiber has 4 (resp. 3) irreducible components and the component Γ_2 has multiplicity 2. For $I^*_{0,2}$, the irreducible components Γ_1 and $\Gamma_3 \simeq \mathbb{P}^1_{k_{v,0}}$ are $k_{v,0}$-rational, hence fixed by the action of $\mathrm{Frob}_q^{d_v}$ and $\Gamma_4 \simeq \mathbb{P}^1_{k_{v,0}(p_2)}$, where p_2 is the point of intersection of Γ_4 and Γ_2 and its residue field $k_{v,0}(p_2)$ is a quadratic extension of $k_{v,0}$. A similar reasoning as with the previous case shows that

$$\det\left(1 - \mathrm{Frob}_q^{d_v}\, T | \Phi_v(k_v)[2]\right) = 1 - 2T + T^2.$$

For the Kodaira symbol $I^*_{0,3}$, the intersection of Γ_2 and Γ_3 is a point p_3 whose residue field is a cubic extension $k_{v,0}(p_3)$ of $k_{v,0}$ and $\Gamma_3 \simeq \mathbb{P}^1_{k_{v,0}(p_3)}$. The subgroup $< \mathrm{Frob}_q^{3d_v} >$ of $< \mathrm{Frob}_q^{d_v} >$ acts as the identity on $\Phi_v(k_v)[3]$ and its quotient permutes the three irreducible components of Γ_3 which are defined over $k_{v,0}(p_3)$. Since it acts as the identity on Γ_1, we find

$$\det\left(1 - \mathrm{Frob}_q^{d_v}\, T | \Phi_v(k_v)[2]\right) = 1 + T + T^2.$$

The Kodaira symbols $I^*_{0,2}$ and $I^*_{0,3}$ become I^*_0 over k_v. Finally, we consider the Kodaira symbol $I^*_{n-2,2}$ with $n \geq 3$, which becomes I^*_{n-2} over k_v. In this configuration, Γ_1 and Γ_2 both have multiplicity 1 and are defined over $k_{v,0}$ and Γ_2 is intersected by another irreducible component which has multiplicity 2. All the irreducible components Γ_i with $3 \leq i \leq n-1$ have multiplicity 2 and are isomorphic to $\mathbb{P}^1_{k_{v,0}}$. Then irreducible component Γ_n is isomorphic to $\mathbb{P}^1_{k_{v,0}(p_2)}$ for some point p_2 with residue field a quadratic extension $k_{v,0}(p_2)$ of $k_{v,0}$. If $n-2$ odd, then $\Phi_v(k_{v,0})[2] = \Phi_v(k_v)[2] \simeq \mathbb{Z}/2\mathbb{Z}$ and so

$$\det\left(1 - \mathrm{Frob}_q^{d_v}\, T | \Phi_v(k_v)[2]\right) = 1 - T.$$

If $n-2$ is even, then $< \mathrm{Frob}_q^{d_v} > / < \mathrm{Frob}_q^{2d_v} >$ acts nontrivially on $\Phi_v(k_v)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ by permuting the irreducible components of Γ_n and fixes Γ_1 and Γ_2. This gives

$$\det\left(1 - \mathrm{Frob}_q^{d_v}\, T | \Phi_v(k_v)[2]\right) = 1 - T^2.$$

We have the following.

Action of $\mathrm{Frob}_q^{d_v}$ on $\Phi_v(k_v)[\ell]$ when $\Phi_v(k_{v,0}) = \Phi_v(k_v)$ and $\ell \geq 5$		
Kodaira Symbol over $k_{v,0}$	$\Phi_v(k_v)[3]$	$\det\left(1 - \mathrm{Frob}_q^{d_v} T^{d_v} \vert \Phi_v(k_v)[\ell]\right)$
$I_{\ell n,2}, n \geq 1$	$\mathbb{Z}/\ell\mathbb{Z}$	$1 + T^{d_v}$
Action of $\mathrm{Frob}_q^{d_v}$ on $\Phi_v(k_v)[\ell]$ when $\Phi_v(k_{v,0}) = \Phi_v(k_v)$ and $\ell = 3$		
Kodaira Symbol over $k_{v,0}$	$\Phi_v(k_v)[3]$	$\det\left(1 - \mathrm{Frob}_q^{d_v} T^{d_v} \vert \Phi_v(k_v)[3]\right)$
$I_{3n,2}, n \geq 1$	$\mathbb{Z}/3\mathbb{Z}$	$1 + T^{d_v}$
IV_2, IV_2^*	$\mathbb{Z}/3\mathbb{Z}$	$1 + T^{d_v}$
Action of $\mathrm{Frob}_q^{d_v}$ on $\Phi_v(k_v)[\ell]$ when $\Phi_v(k_{v,0}) \neq \Phi_v(k_v)$ and $\ell = 2$		
Kodaira Symbol over $k_{v,0}$	$\Phi_v(k_v)[2]$	$\det\left(1 - \mathrm{Frob}_q^{d_v} T^{d_v} \vert \Phi_v(k_v)[2]\right)$
$I_{2n-2,2}, n \geq 1$	$\mathbb{Z}/2\mathbb{Z}$	$1 + T^{2d_v}$
$I_{2n-1,2}, n \geq 1$	$\mathbb{Z}/2\mathbb{Z}$	$1 - T^{d_v}$
$I_{0,2}^*$	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	$1 - 2T^{d_v} + T^{2d_v}$
$I_{0,3}^*$	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	$1 + T^{d_v} + T^{2d_v}$
$I_{n-2,2}^*, n \geq 3$ and n odd	$\mathbb{Z}/4\mathbb{Z}$	$1 - T^{d_v}$
$I_{n-2,2}^*, n \geq 3$ and n even	$(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$	$1 - 2T_v^d + T^{2d_v}$

Combining Table 4.6 and Table 4.6 we obtain that

(i) if $\ell \geq 5$, then

$$\det\left(1 - \mathrm{Frob}_q T \vert \Phi(Z)[\ell]\right) = \prod_{\substack{v \in Z_0 \\ I_{\ell n}, n \geq 1}} (1 - T^{d_v}) \times \prod_{\substack{v \in Z_0 \\ I_{\ell n,2}, n \geq 1}} (1 + T^{d_v}).$$

(ii) if $\ell = 3$, then

$$\det\left(1 - \mathrm{Frob}_q T \vert \Phi(Z)[3]\right) = \prod_{\substack{v \in Z_0 \\ I_{3n}, n \geq 1, IV, IV^*}} (1 - T^{d_v}) \times \prod_{\substack{v \in Z_0 \\ I_{3n,2}, n \geq 1}} (1 + T^{d_v}) \times \prod_{\substack{v \in Z_0 \\ IV_2, IV_2^*}} (1 + T^{d_v}).$$

(iii) if then $\ell = 2$, then

$$\begin{aligned}\det\left(1 - \mathrm{Frob}_q T \vert \Phi(Z)[2]\right) = &\prod_{\substack{v \in Z_0 \\ S_1}} (1 - T^{d_v}) \times \prod_{\substack{v \in Z_0 \\ I_{2n}^*, n \geq 0}} (1 - T^{d_v})^2 \\ &\times \prod_{\substack{v \in Z_0 \\ I_{2n-2,2}, n \geq 1}} (1 - T^{2d_v}) \times \prod_{\substack{v \in Z_0 \\ I_{n-2}^*, n \geq 2 \text{ even}}} (1 - 2T_v^d \\ &\times \prod_{\substack{v \in Z_0 \\ I_{0,3}^*}} (1 + T^{d_v} + T^{2d_v}),\end{aligned} + T^{2d_v})$$

where $S_1 := \{I_{2n}, n \geq 1, III, III^*, I_{2n+1}^*, n \geq 0, I_{2n-1,2}, n \geq 1, I_{n-2,2}^*, n \geq 3 \text{ odd }\}$.

□

Remark 4.6.3. We have

$$\det\left(1 - \mathrm{Frob}_q\, T|\Phi(Z)[2]\right) \equiv \prod_{\substack{v\in Z_0\\ S_1}}(1-T^{d_v})^2 \times \prod_{\substack{v\in Z_0\\ I^*_{0,3}}}(1-T^{d_v})^3 \times \prod_{\substack{v\in Z_0\\ S_2}}(1-T^{d_v})^4 \bmod 2,$$

where

$$S_1 = \{I_{2n}, n\geq 1, III, III^*, I^*_{2n+1}, n\geq 0, I_{2n-1,2}, n\geq 1, I^*_{n-2,2}, n\geq 3 \text{ odd }\},$$
$$S_2 = \{I^*_{2n}, n\geq 0, I_{2n-2}, n\geq 1, I^*_{n-2,2}, n\geq 2 \text{ even }\}.$$

4.7 The G_ℓ-Invariants

Let k_0 be a perfect field, let C_0/k_0 be a proper, smooth, geometrically connected curve and let $K_0 := k_0(C_0)$ be function field. Let E/K_0 be a nonconstant elliptic curve, let ℓ be a prime different from $\mathrm{char}(k_0)$ and let $G_\ell := \mathrm{Gal}(K_{\ell,0}/K_0)$ be the Galois group of the ℓ-th division field $K_{\ell,0} := K_0(E[\ell])$ of K_0. The field $K_{\ell,0}$ is obtained from K_0 by adjoining the coordinates of the affine points of $E[\ell]$. A choice of $\mathbb{F}_\ell$-basis for $E[\ell]$ identifies G_ℓ with a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Now assume that k_0 contains μ_ℓ. Using the properties of the Weil pairing in a similar way to the proof of [43, p.99, III.8.6], we can identify G_ℓ with a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$. Define the following constant

$$c(K_0) := 2 + \max\left\{\ell \text{ prime } : \frac{\ell - (6+3e_2+4e_3)}{12} \leq \mathrm{genus}(K_0)\right\},$$

$$\text{where } e_2 = \begin{cases} 1 & \text{if } \ell \equiv 1 \bmod 4,\\ -1 & \text{otherwise}\end{cases}, e_3 = \begin{cases} 1 & \text{if } \ell \equiv 1 \bmod 3,\\ -1 & \text{otherwise}\end{cases}.$$

Then [6, p.3066, Theorem 1.1] implies that for each nonconstant elliptic curve E/K_0 and each prime $\ell \neq \mathrm{char}(k_0)$ satisfying $\ell \geq c(K_0)$, we have $G_\ell \simeq \mathrm{SL}_2(\mathbb{F}_\ell)$.

Remark 4.7.1. This result implies, for example, that if $\mu_\ell \subset k_0$ and if K_0 has genus 0, then we can deduce from [6, First sentence of p.3072], that for any prime $\ell \geq 17$ and different from $\mathrm{char}(k_0)$, we have $G_\ell \simeq \mathrm{SL}_2(\mathbb{F}_\ell)$.

In the context of elliptic curves with nonconstant j-invariants, we now determine for which subgroups G_ℓ of $\mathrm{SL}_2(\mathbb{F}_\ell)$ Theorem 4.3.10 (and more generally Theorem 4.2.5) and Corollary 4.3.14 hold.

Suppose that $E(K_0)[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$, then $G_\ell = \{1\}$. Moreover, $\mathcal{E}[\ell]$ is the constant sheaf $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ and therefore $\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell]) \simeq \mathrm{Jac}(C)(k)[\ell]^{\oplus 2}$.

We will now work under the assumption that $E(K_0)[\ell] = \{O\}$ and in particular G_ℓ is a nontrivial subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Remark 4.7.2. The cohomological machinery that we developed until now does not address the case where $E(K_0)[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}$. We hope to develop a cohomological approach to this situation in a future work. However, see the analytic approach in Chapter 3 for partial results.

Proposition 4.7.3. *Let ℓ be a prime different from the characteristic of a finite field k_0. Let $\pi : C_{\ell,0} \to C_0$ be a geometric finite morphism of smooth, proper and geometrically connected curves defined over k_0, whose corresponding extension of function fields $K_{\ell,0}/K_0$ is Galois with Galois group G_ℓ a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$. Suppose that G_ℓ has one of the following mutually exclusive set of properties.*

(i) The order of G_ℓ is not divisible by ℓ.

(ii) If $\ell \geq 3$, the order of G_ℓ is divisible by ℓ and G_ℓ contains the center $Z = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ of $\mathrm{SL}_2(\mathbb{F}_\ell)$.

(iii) If $\ell = 2$, then $G_2 = \mathrm{SL}_2(\mathbb{F}_2)$.

Then, we have the following Frob_q-equivariant short exact sequence of Frob_q-modules

$$0 \to \mathrm{H}^1(C_{\acute{e}t}, \mathcal{E}[\ell]) \to \mathrm{H}^1\left(C_{\ell,\acute{e}t}, \pi^*\mathcal{E}[\ell]\right)^{G_\ell} \to \bigoplus_{v \in Z} \mathrm{H}^1\left(I(w_v|v), E[\ell]\right) \to 0.$$

In particular, in case (i), we have

$$\mathrm{H}^1(C_{\acute{e}t}, \mathcal{E}[\ell]) = \mathrm{H}^1\left(C_{\ell,\acute{e}t}, \pi^*\mathcal{E}[\ell]\right)^{G_\ell}.$$

Proof. We verify the assumptions of Theorem 4.3.10 in each case.

(i) Take $H_\ell := G_\ell$ for normal subgroup of G_ℓ. Then the quotient group G_ℓ/H_ℓ is trivial.

(ii) The center Z of $\mathrm{SL}_2(\mathbb{F}_\ell)$ is a normal subgroup of G_ℓ. The Z-invariants of $E[\ell]$ only contains the element O. Indeed, if P is a point of $E[\ell]^Z$, then it satisfies $P = -P$. Therefore, $2P = O$ and since ℓ is odd, it follows that $P = O$.

(iii) If $G_2 = \mathrm{SL}_2(\mathbb{F}_2) \simeq S_3$, and σ is the 3-cycle $(1, 2, 3)$, then G_2 has $A_3 =< \sigma >$ for normal subgroup. The order of A_3 is coprime to the order of $E[2]$. Let $y^2 = f(x)$ be an affine weierstrass equation for the elliptic curve E/K_0. Then $E[2] = \{O, P_1, P_2, P_3\}$, where for each $i = 1, 2, 3$, $P_i = (x_i, 0)$ with x_i one of the three roots of $f(x) = (x - x_1)(x - x_2)(x - x_3)$. We have $\sigma(O) = O$, $\sigma(P_i) = P_{\sigma(i)}$ and so $E[2]^{A_3} = \{O\}$.

Moreover, if the order of G_ℓ is not divisible by ℓ, then the same is true of all its subgroups and so in particular of the inertia subgroups $I(w_v|v)$. Therefore, $\mathrm{H}^1\left(I(w_v|v), E[\ell]\right) = 0$ for each $v \in Z$. □

Remark 4.7.4. The subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ of order divisible by $\ell \geq 3$ and which contain the center as (normal) subgroup correspond to the subgroups of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ of order divisible by ℓ. From [46, p.412, 3.6.25] these subgroups of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ are

(i) groups H of order $\ell(\ell - 1)/2$ and and the subgroups of H of order divisible by ℓ. In particular, an ℓ-Sylow subgroup H_ℓ of H is an *elementary Abelian ℓ-group*, i.e., for any $x \in H_\ell$ we have $x^\ell = 1$ [46, p.159, 2.5.22],

(ii) the groups A_4, S_4 or A_5 under some conditions (see below),

(iii) the group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ itself.

We can describe more precisely the case (ii) using [46, p.414, 2.6.26]:

(a) Since ℓ is odd, then $\mathrm{PSL}_2(\mathbb{F}_\ell)$ contains a subgroup isomorphic to A_4.

(b) The group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ contains a subgroup isomorphic to S_4 if and only if $\ell^2 \equiv 1 \bmod 16$.

(c) The group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ contains a subgroup isomorphic to A_5 if and only if $\ell(\ell^2 - 1) \equiv 0 \bmod 5$.

Remark 4.7.5. Note that Theorem 4.3.10 and by extension Proposition 4.7.3, are valid for the generic case of $G_\ell = \mathrm{SL}_2(\mathbb{F}_\ell)$ when $\ell \geq 3$.

Remark 4.7.6. Theorem 4.3.10 does not apply for the subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ which have order divisible by $\ell \geq 3$ and which do not contain the center of $\mathrm{SL}_2(\mathbb{F}_\ell)$. When $\ell = 2$, the result does not apply for the three cyclic subgroups of order 2 of $\mathrm{SL}_2(\mathbb{F}_2)$.

4.8 Some Technicalities in the Application of Theorem 4.3.10

Consider the geometric finite proper morphism $\pi : C_{\ell,0} \to C_0$ of proper, smooth and geometrically connected curves defined over a finite field k_0. Let U_0 be the locus of good reduction of E/K_0. This is a dense Zariski open subset of C_0. We denote by $j : U_0 \hookrightarrow C_0$ a chosen open immersion. Let $U_{\ell,0}$ be the inverse image $\pi^{-1}(U_0)$ of U_0 by π. Let $j_\ell : U_{\ell,0} \hookrightarrow C_{\ell,0}$ be the corresponding open immersion as Zariski open subset given by the base change by π. The finite field extension of $K_{\ell,0} = K_0(E[\ell])$ over K_0 is Galois with Galois group $G_\ell = \mathrm{Gal}(K_0(E[\ell])/K_0)$. By equivalence of categories (Remark 2.2.8) the restriction morphism $\pi : U_{\ell,0} \to U_0$ is a finite Galois covering with Galois group G_ℓ. coming the finite Galois extension of $K_{\ell,0} = K_0(E[\ell])$ over K_0, whose Galois group is G_ℓ. Let $\mathcal{E}[\ell]$ be the ℓ-torsion of the Néron model of E/K_0.

The pullback $\pi^*\mathcal{E}[\ell]$ is a $\mathbb{Z}/\ell\mathbb{Z}$-sheaf, but is not in general the constant sheaf $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$. Indeed, since the j-invariant of E/K_0 is nonconstant, U_0 is not C_0 [24, p.11]. In particular, there exists a finite set Z_0 of closed points where E/K_0 has bad reduction. Let $v \in Z_0$ be such a point and let $w \in Z_{\ell,0} := \pi^{-1}(Z_0)$ be a closed point of $C_{\ell,0}$ lying over v. By [26, p.69, II.3.2(a)], we have

$$(\pi^*\mathcal{E}[\ell])_{\overline{w}} = \mathcal{E}[\ell]_{\overline{v}} \simeq E[\ell]^{I(v)},$$

which is a one-dimensional $\mathbb{F}_\ell$-vector space if $v \in M$ and is the vector space 0 if $v \in A$. In particular, the étale sheaves $\pi^*\mathcal{E}[\ell]$ and $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ on $C_{\ell,0}$ can't be isomorphic since they differ by (at least) a geometric stalk.

Now, the pullback sheaf $\pi^* j^*\mathcal{E}[\ell]$ is the constant sheaf $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ on $U_{\ell,0}$, since all its geometric stalks are isomorphic to the vector space $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$. Since $U_{\ell,0}$ is dense in $C_{\ell,0}$, the

pushforward sheaf $j_{\ell,*}(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ is the constant sheaf $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ on $C_{\ell,0}$. Now, we have a Cartesian diagram as in [26, p.170, V.1.14].

$$\begin{array}{ccc} U_{\ell,0} & \xhookrightarrow{j_\ell} & C_{\ell,0} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ U_0 & \xhookrightarrow{j} & C_0 \end{array}$$

Therefore, the sheaf $j_{\ell,*}j_\ell^*\pi^*\mathcal{E}[\ell]$ is the constant sheaf $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ on $C_{\ell,0}$.

By considering geometric stalks, we see that the adjunction morphism $\pi^*\mathcal{E}[\ell] \to j_{\ell,*}j_\ell^*\pi^*\mathcal{E}[\ell]$ is injective. We therefore have a short exact sequence of étale sheaves on $C_{\ell,0}$:

$$0 \to \pi^*\mathcal{E}[\ell] \to j_{\ell,*}j_\ell^*\pi^*\mathcal{E}[\ell] \to \mathcal{Q} \to 0, \tag{4.8.1}$$

where the quotient sheaf $\mathcal{Q}$ is a skyscraper sheaf supported on $Z_{\ell,0}$. More precisely, write $i_w : \mathrm{Spec}(k_{w,0}) \hookrightarrow C_{\ell,0}$ for the closed immersion which picks up the closed point w of $C_{\ell,0}$ and let M_ℓ and A_ℓ, respectively denoting the set of places of $K_{\ell,0}$ over which the elliptic curve $E/K_{\ell,0}$ has multiplicative and additive reduction. Then we have

$$\mathcal{Q} \simeq \left(\bigoplus_{w\in M_\ell} i_{w,*}\mathbb{Z}/\ell\mathbb{Z}\right) \oplus \left(\bigoplus_{w\in A_\ell} i_{w,*}(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}\right).$$

We now base change the whole situation to the algebraic closure k of k_0. By abuse of notation, denote the morphisms π, j and j_ℓ corresponding to the base change to k of the said morphisms considered over k_0. We write $\overline{M_\ell}$ and $\overline{A_\ell}$ for the sets of places respectively lying over M and A in k.

We obtain a short exact sequence as in (4.8.1), but of étale sheaves over C_ℓ. Since $\mathcal{Q}$ is a skyscraper sheaf, we have [47, p.159, (10.1.2) Lemma]

$$\mathrm{H}^i(C_{\ell,\text{ét}}) = \begin{cases} \left(\bigoplus_{w\in\overline{M_\ell}} \mathbb{Z}/\ell\mathbb{Z}\right) \oplus \left(\bigoplus_{w\in\overline{A_\ell}} (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}\right) & \text{if } i = 0, \\ 0 & \text{if } i > 0. \end{cases}$$

Moreover, we have

$$\mathrm{H}^i\left(C_{\ell,\text{ét}}), (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}\right) \simeq \begin{cases} (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2} & \text{if } i \in \{0,2\}, \\ \mathrm{Jac}(C_\ell)(k)[\ell]^{\oplus 2} & \text{if } i = 1, \\ 0 & \text{if } i \geq 3. \end{cases}$$

Taking the long exact sequence in étale cohomology associated to the short exact sequence 4.8.1 of étale sheaves over C_ℓ, we obtain a canonical isomorphism $\mathrm{H}^2(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell]) \simeq (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ and an exact sequence, both being of finite-dimensional $\mathbb{F}_\ell$-vector spaces.

$$0 \to \mathrm{H}^0(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell]) \to (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2} \to \left(\bigoplus_{w\in\overline{M_\ell}} \mathbb{Z}/\ell\mathbb{Z}\right) \oplus \left(\bigoplus_{w\in\overline{A_\ell}} (\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}\right)$$
$$\cdots \to \mathrm{H}^1(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell]) \to \mathrm{Jac}(C_\ell)(k)[\ell]^{\oplus 2} \to 0.$$

We leave a finer investigation of this exact sequence to some of our future investigations.

4.9 The Reduction of $L(T, E/K_0)$ modulo ℓ

4.9.1 The Quadratic Twists

In this subsection, we give a "cohomological" solution to the following problem.

Problem 4.9.1 (Quadratic Twists)**.** Let E/K_0 be a nonconstant elliptic curve. Let $f \in K_0^\times \smallsetminus (K_0^{\times 2} \cup k_0^\times)$ be an element whose elements which can only have zeroes and poles over U_0. Suppose moreover that for each point $v \in |U_0|$ which is a zero or a pole of f, we have $\mathrm{ord}_v(f)$ odd. Let E_f/K_0 be the corresponding quadratic twist of E/K_0. Assume that ℓ is a prime distinct from $\mathrm{char}(k_0)$. Suppose that $E(K_0)[\ell]$ is a 2-dimensional $\mathbb{F}_\ell$-vector space. Give a formula $\mathrm{L}(T, E_f/K_0) \bmod \ell$.

Note that we already gave a solution for $\mathrm{L}(T, E_f/K_0) \bmod N$ in Theorem 3.1.5 and Corollary 3.1.11, for a positive integer N coprime with $\mathrm{char}(k_0)$.

If $\ell = 2$, then $E(K_0)[2]$ and $E_f(K_0)[2]$ both are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$. Therefore, [18, p.133, Theorem 4] gives a formula for $\mathrm{L}(T, E_f/K_0) \bmod 2$. We show the following.

Theorem 4.9.2. *Let E/K_0 be an elliptic curve with nonconstant j-invariant. Let $f \in K_0^\times \smallsetminus (K_0^{\times 2} \cup k_0^\times)$ be an element which can only have zeroes and poles over U_0, generating a quadratic extension $K_{f,0}/K_0$ of Galois group G_f. Let E_f/K_0 be the corresponding quadratic twist of E/K_0. Assume that ℓ is a prime distinct from* $\mathrm{char}(k_0)$. *Suppose that $E(K_0)[\ell]$ is a 2-dimensional $\mathbb{F}_\ell$-vector space.*

(*a*) *If $\ell = 3$, then*

$$\mathrm{L}(T, E_f/K_0) \equiv \det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^1\left(C_{f,\acute{e}t}, \pi^*\mathcal{E}_f[3]\right)^{G_f}\right) \prod_{\substack{v \in Z_0 \\ I_{3n}, n\geq 1, IV, IV^*}} (1 - T^{d_v}) \times \prod_{\substack{v \in Z_0 \\ I_{3n,2}, n\geq 1, IV_2, IV_2^*}} (1 + T^{d_v}) \bmod 3.$$

(*b*) *If $\ell \geq 5$, then*

$$\mathrm{L}(T, E_f/K_0) \equiv \det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^1\left(C_{f,\acute{e}t}, \pi^*\mathcal{E}_f[\ell]\right)^{G_f}\right) \prod_{\substack{v \in Z_0 \\ I_{\ell n}, n\geq 1}} (1 - T^{d_v}) \times \prod_{\substack{v \in Z_0 \\ I_{\ell n,2}, n\geq 1}} (1 + T^{d_v}) \bmod \ell.$$

where

$$\varepsilon_v = \begin{cases} 1 & \text{if } v \in M_{inert}, \\ -1 & \text{if } v \in M_{split}, \end{cases} \text{ and } m(T^{d_v}) = \begin{cases} 1 + T^{2d_v} & \text{if } v \in M_{inert}, \\ (1 + T^{d_v})^2 & \text{if } v \in M_{split}. \end{cases}$$

Proof. Since $\ell \geq 3$ is odd, one deduces from [43, p.360, X.10.22] that

$$E_f(K_0)[\ell] \oplus E(K_0)[\ell] = E(K_{f,0})[\ell].$$

Because $E(K_0)[\ell]$ is a 2-dimensional $\mathbb{F}_\ell$-vector, space, then $E_f(K_0)[\ell] = \{O\}$. Hence, $\mathrm{H}^2(C_{\text{ét}}, \mathcal{E}_f^0[\ell]) = 0$. The group $\mathrm{Gal}(K_{f,0}/K_0)$ has order 2, coprime to ℓ and Corollary 4.3.14 applies and so

$$\mathrm{H}^1(C_{\text{ét}}, \mathcal{E}_f[\ell]) \simeq \mathrm{H}^1\left(C_{f,\text{ét}}, \pi^*\mathcal{E}_f[\ell]\right)^{G_f}.$$

Each place of $M \cup A$ is unramified in $K_{f,0}$ and therefore has the same Kodaira symbol for E/K_0 and for E_f/K_0. Each place $v \in U_0$ for which $\mathrm{ord}_v(f) \neq 0$, will be a place of additive reduction for E_f/K_0 with Kodaira symbol I_0^*. Since $\ell \geq 3$, the places with reduction type I_0^* yield local groups of components isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ and so do not contribute to the ℓ-torsion of the global group of components $\Phi_{f,\ell}$. Therefore, $\Phi_{f,\ell}(C)$ and $\Phi_\ell(C)$ have the same support Z. The rest follows from Theorem 4.6.1. □

4.9.2 The Problem of ℓ-torsion

Theorem 4.9.3. *Let $\pi : C_0' \to C_0$ is a k_0-finite morphism of geometrically connected curves defined over k_0. Let E/K_0 be an elliptic curve with nonconstant j-invariant and let ℓ be a prime distinct from* $\mathrm{char}(k_0)$ *for which $E(K_0)[\ell] = \{O\}$ and assume that $q \equiv 1 \bmod \ell$. Let G_ℓ be the Galois group of the extension $K_0(E[\ell])/K_0$. Suppose that G_ℓ is one of the groups in Proposition 4.7.3 and let H_ℓ be the kernel of the canonical* Frob_q*-equivariant morphism*

$$\mathrm{H}^2_Z(C, \mathcal{E}[\ell]) \to \mathrm{H}^2_{Z'}(C_\ell, f^*\mathcal{E}[\ell])^G.$$

For each $v \in Z_0$, let Σ_v be its G_{k_0}-orbit inside Z. For each $\overline{v} \in \Sigma_v$, choose exactly one element $\overline{w_v}$ in $\pi^{-1}(Z)$ lying over $\overline{v}$. Then

$$\mathrm{L}(T, E/K_0) \equiv \frac{\det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C_{\ell,\acute{e}t}, \pi^*\mathcal{E}[\ell]\right)^{G_\ell}\right)}{\prod_{v\in Z_0}\prod_{\overline{v}\in\Sigma_v} \det\left(1 - T^{d_{\overline{w_v}}}\,\mathrm{Frob}_q^{d_{\overline{w_v}}} \,|\mathrm{H}^1(I(\overline{w_v}|\overline{v}), E[\ell])\right)} \times \det\left(1 - T\,\mathrm{Frob}_q\,|\Phi(Z)[\ell]\right) \bmod \ell,$$

where $\det\left(1 - T\,\mathrm{Frob}_q\,|\Phi(Z)[\ell]\right)$ *is given by Theorem 4.6.1.*

Proof. By Proposition 4.7.3, we have a Frob_q-equivariant short exact sequence of Frob_q-modules

$$0 \to \mathrm{H}^1(C_{\text{ét}}, \mathcal{E}[\ell]) \to \mathrm{H}^1\left(C_{\ell,\text{ét}}, \pi^*\mathcal{E}[\ell]\right)^{G_\ell} \to \bigoplus_{v\in Z} \mathrm{H}^1\left(I(w_v|v), E[\ell]\right) \to 0.$$

Corollary 4.3.13 gives the characteristic polynomial of Frobenius on the right term of the exact sequence, while Theorem 4.6.1 gives the characteristic polynomial of Frobenius on $\Phi(Z)[\ell]$. □

Corollary 4.9.4. *In the context of Theorem 4.9.3, suppose for each $v \in Z_0$, the order of each group $I(\overline{w_v}|\overline{v})$ is not divisible by ℓ. Then,*

$$\mathrm{L}(T, E/K_0) \equiv \det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C_{\ell,\acute{e}t}, \pi^*\mathcal{E}[\ell]\right)^{G_\ell}\right) \det\left(1 - T\,\mathrm{Frob}_q\,|\Phi(Z)[\ell]\right) \bmod \ell.$$

where $\det\left(1 - T\,\mathrm{Frob}_q\,|\Phi(Z)[\ell]\right)$ *is given by Theorem 4.6.1.*

Proof. We have $\mathrm{H}^1\left(I(w_v|v), E[\ell]\right) = 0$ for all $I(w_v|v)$. □

4.10 Cohomological Description of an L-function Modulo ℓ

In this section, we show the following Theorem.

Theorem 4.10.1. *Let C_0 be a smooth, proper, and geometrically connected curve over a finite field k_0 of characteristic $p \geq 5$ and let K_0 be the function field of C_0. Let E/K_0 be an elliptic curve with nonconstant j-invariant. If ℓ is a prime distinct from p for which k_0 contains μ_ℓ and if $E(K)[\ell] = \{O\}$, then*

$$\mathrm{L}(T, E/K_0) \equiv \det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^1(C_{\acute{e}t}, \mathcal{E}^0[\ell])\right) \bmod \ell.$$

This result might be known, but we could not find in the literature. Hence, we provide a proof to this potentially new result in a series of lemmas.

Lemma 4.10.2. *Let E/K_0 be an elliptic curve defined over the function field of a smooth, proper and geometrically connected curve C_0/k_0. Let $\pi : \mathcal{X}_0 \to C_0$ be the proper regular model of E/K_0 and let $\mathcal{F}_0$ be the sheaf $\mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))$ on $C_{0,\acute{e}t}$. Then the L-function of E/K_0 is the rational function*

$$\mathrm{L}(T, E/K_0) = \frac{\det\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^1(C, \mathcal{F})\right)}{\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^0(C, \mathcal{F})\right)\left(1 - \mathrm{Frob}_q\, T \,|\, \mathrm{H}^2(C, \mathcal{F})\right)} \in \mathbb{Z}[[T]].$$

Proof. Since the sheaf $\mathbb{Q}_\ell(1)$ is constructible on $\mathcal{X}_{0,\text{ét}}$ and the morphism π is proper, then by [26, p.223, VI.2.1] the sheaf $\mathcal{F}_0$ is constructible on C_0. Then the pullback $\mathcal{F}$ of $\mathcal{F}_0$ via the algebraic closure k of k_0 is constructible on C.

As a consequence of the proper base change theorem [26, p.224, VI.2.5], we have, for each closed point v of C_0 and for a choice of geometric point $\overline{v}$ lying over v, that

$$\mathcal{F}_{\overline{v}} \simeq \mathrm{H}^1\left(\mathcal{X}_v, \mathbb{Q}_\ell(1)\right) \simeq \mathrm{H}^1\left(\mathcal{X}_\eta, \mathbb{Q}_\ell(1)\right)^{I(v)},$$

where, for $v \in |U|$, the inertia $I(v)$ acts trivially on $\mathrm{H}^1\left(\mathcal{X}_\eta, \mathbb{Q}_\ell(1)\right)$ and $\mathcal{X}_\eta$ is the elliptic curve E/K. Therefore, the Euler product (2.3.2) of the L-function can be written as

$$\mathrm{L}(T, E/K_0) = \prod_{v \in |C_0|} \det\left(1 - \mathrm{Frob}_q^{d_v}\, T^{d_v} \,|\, \mathrm{H}^1\left(\mathcal{X}_\eta, \mathbb{Q}_\ell(1)\right)^{I(v)}\right)^{-1}.$$

Indeed, when $v \in |U|$, then $\det\left(1 - \mathrm{Frob}_q\, T^{d_v} \,|\, \mathrm{H}^1(\mathcal{X}_v, \mathbb{Q}_\ell(1)\right)$ is the numerator of the zeta function of the elliptic curve $\mathcal{X}_v$ over the finite field with q^{d_v} elements [43, p.143, V.2.4]. If v is a place of multiplicative reduction, then $\mathcal{X}_v$ is a (split or nonsplit) 1-dimensional torus. If v is a place of additive reduction, then $\mathcal{X}_v$ is a 1-dimensional additive group $\mathbb{G}_a$ [43, p.196, VII.5.1]. Since $\ell \neq p$, then $\mathrm{H}^1(\mathcal{X}_v, \mathbb{Q}_\ell(1)) \simeq \mathbb{Q}_\ell$, when $\mathcal{X}_v$ is a 1-dimensional torus and $\mathrm{H}^1(\mathcal{X}_v, \mathbb{Q}_\ell(1)) = 0$, when $\mathcal{X}_v \simeq \mathbb{G}_a$. Therefore, in the case of multiplicative reduction, the characteristic polynomial of Frob_q on $\mathrm{H}^1(\mathcal{X}_v, \mathbb{Q}_\ell(1))$ is be $1 - T$ or $1 + T$. A finer analysis shows that when the torus is split, then the characteristic polynomial is $1 - T$ and it is $1 + T$ otherwise. In the case of additive reduction, the characteristic polynomial of Frob_q on $\mathrm{H}^1(\mathcal{X}_v, \mathbb{Q}_\ell(1))$ is 1.

Also, we have that $\mathcal{F} = \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Indeed, on the geometric stalks we have isomorphisms

$$\begin{aligned}
\mathrm{H}^1(\mathcal{X}_v, \mathbb{Q}_\ell(1)) &\simeq \mathrm{H}^1(\mathcal{X}_v, \mathbb{Q}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell(1) && \text{[26, p.185, in proof of V.2.5]} \\
&\simeq \mathrm{H}^1(\mathcal{X}_v, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \\
&\simeq \mathrm{H}^1(\mathcal{X}_v, \mathbb{Z}_\ell(1)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell && \text{[26, p.164].}
\end{aligned}$$

Now, for each positive integer n, the sheaf $(\mathbb{Z}/\ell^n\mathbb{Z})(1)$ is Abelian and torsion on $\mathcal{X}_{\text{ét}}$ and the morphism $\pi : \mathcal{X} \to C$ is proper. Therefore, the sheaf $\mathrm{R}^1\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(1))$ is Abelian and torsion on $C_{\text{ét}}$ [44, Tag 0DDD, (1)]. Moreover, the curve C is smooth, proper and connected over the algebraically closed field k. Therefore,

$$\mathrm{H}^i\left(C_{\text{ét}}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(1))\right) = 0,$$

for each $i \geq 3$ [44, Tag 03SC (1)]. By definition of ℓ-adic cohomology, it follows that for $i \geq 3$, the groups $\mathrm{H}^i\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right)$ vanish and thus the groups $\mathrm{H}^i(C, \mathcal{F})$ vanish as well. Now, the Grothendieck-Lefschetz trace formula [26, p.292, VI.13.4] allows us to conclude, as in [26, p.291, VI.13.3] or in [23, p.464, Exposé XV, 3.2 Théorème], that

$$\mathrm{L}(T, E/K_0) = \frac{\det\left(1 - \mathrm{Frob}_q T \,|\, \mathrm{H}^1(C, \mathcal{F})\right)}{\left(1 - \mathrm{Frob}_q T \,|\, \mathrm{H}^0(C, \mathcal{F})\right)\left(1 - \mathrm{Frob}_q T \,|\, \mathrm{H}^2(C, \mathcal{F})\right)} \in \mathbb{Z}[[T]].$$

□

Lemma 4.10.3. *Let E/K_0 be an elliptic curve defined over the function field of a smooth, proper and geometrically connected curve C_0/k_0. Let $\pi : \mathcal{X}_0 \to C_0$ be the proper regular model of E/K_0 and let $\mathcal{F}_0$ be the sheaf $\mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))$ on $C_{0,ét}$. If the j-invariant of E/K_0 is nonconstant, then*

$$\mathrm{L}(T, E/K_0) = \det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1(C, \mathcal{F})\right) \in \mathbb{Z}[T].$$

Proof. Since the j-invariant of E/K_0 is nonconstant, it follows from the proof [10, pp.211-212, Lemme (3.5.5.)], that the geometric monodromy group of the lisse Weil sheaf $j^*\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))$ on U_0, namely the image of the geometric fundamental group $\pi_1(U, \overline{\eta})$ in

$$\mathrm{GL}\left(\left(j^*\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right)_{\overline{\eta}}\right) = \mathrm{GL}\left(\mathrm{H}^1(E, \mathbb{Z}_\ell(1))\right),$$

is an open subgroup with finite index. Therefore the groups

$$\begin{aligned}
\mathrm{H}^0\left(U, j^*\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right) &= \left(\mathrm{H}^1(E, \mathbb{Z}_\ell(1))\right)^{\pi_1(U,\overline{\eta})}, \\
\mathrm{H}^2_c\left(U, j^*\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right) &= \left(\mathrm{H}^1(E, \mathbb{Z}_\ell(1))\right)(-1)_{\pi_1(U,\overline{\eta})}
\end{aligned}$$

are finite. Hence, the groups

$$\begin{aligned}
\mathrm{H}^0\left(U, j^*\mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))\right) &= \mathrm{H}^0\left(U, j^*\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell, \\
\mathrm{H}^2_c\left(U, j^*\mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))\right) &= \mathrm{H}^2_c\left(U, j^*\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell
\end{aligned}$$

are trivial. Since, $j : U \to C$ is the smooth completion of U, then for $i \in \{0, 2\}$ the group $\mathrm{H}^i\left(C, \mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))\right)$ is trivial. We thus find as desired that

$$\mathrm{L}(T, E/K_0) = \det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1(C, \mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))\right) \in \mathbb{Z}[T].$$

□

The kernel of the morphism $\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1)) \to \mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))$ is the torsion part of $\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))$. One can show that it follows

$$\det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right)\right) = \det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))\right)\right).$$

Definition 4.10.4. Let G be a group scheme defined over a curve C/k. Its *$\mathbb{Z}_\ell$-adic Tate module* is defined (based on [17, Exposé IX, p.330, (2.2.2.1)]) to be the $\mathbb{Z}_\ell$-sheaf :

$$T_\ell(G) := (G_{\ell^{n+1}})_{n\geq 0}\,,$$

where G_ℓ^{n+1} is the kernel of the multiplication by ℓ^{n+1} in G. *Its $\mathbb{Q}_\ell$-adic Tate module* is defined to be the following $\mathbb{Q}_\ell$-sheaf:

$$V_\ell(G) := T_\ell(G) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Remark 4.10.5. We chose to start the indexing at $n = 0$ in order to match the definition 2.2.59 of $\mathbb{Z}_\ell$-sheaves.

Lemma 4.10.6. *(i) There is a canonical isomorphism between the $\mathbb{Z}_\ell$-sheaves $\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))$ and $T_\ell\left(\mathcal{E}^0\right)$. In particular, we have a canonical isomorphism between the $\mathbb{Q}_\ell$-sheaves $\mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))$ and $V_\ell\left(\mathcal{E}^0\right)$.*

(ii) If $j : U_0 \to C_0$ is the inclusion of the locus of good reduction for the elliptic curve E/K_0, then we also have a canonical isomorphism between the $\mathbb{Z}_\ell$-sheaves $j_*j^*\left(\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))\right)$ and $T_\ell(\mathcal{E})$. In particular, we have a canonical isomorphism between the $\mathbb{Q}_\ell$-sheaves $j_*j^*\mathrm{R}^1\pi_*(\mathbb{Q}_\ell(1))$ and $V_\ell(\mathcal{E})$.

Proof. (i) We verify the statement on the geometric stalks. From the proper base change theorem [26, p.224, VI.2.5], the definition of ℓ-adic cohomology and Hilbert's theorem 90 [26, p.134, III.4.9], we have

$$\begin{aligned}
\left(\mathrm{R}^1\pi_*\left(\mathbb{Z}_\ell(1)\right)\right)_{\overline{v}} &= \mathrm{H}^1\left(\mathcal{X}_{v,\text{ét}}, \mathbb{Z}_\ell(1)\right) \\
&:= \varprojlim_{n\geq 0} \mathrm{H}^1\left(\mathcal{X}_{v,\text{ét}}, \mu_{\ell^{n+1}}\right) \\
&= \varprojlim_{n\geq 0} \mathrm{H}^1\left(\mathcal{X}_{v,\text{ét}}, \mathbb{G}_m\right)[\ell^{n+1}] \\
&= \varprojlim_{n\geq 0} \mathrm{Pic}\left(\mathcal{X}_{v,\text{ét}}\right)[\ell^{n+1}] \\
&= \varprojlim_{n\geq 0} \mathrm{Pic}^0\left(\mathcal{X}_{v,\text{ét}}\right)[\ell^{n+1}].
\end{aligned}$$

The last equality holds because the quotient group $\mathrm{Pic}\,(\mathcal{X}_v)\,/\,\mathrm{Pic}^0\,(\mathcal{X}_v)$ is isomorphic via the degree map to the (torsion)-free Abelian group $\mathbb{Z}$.

Since the greatest common divisor of the geometric multiplicities of the irreducible components of the special fiber of $\mathcal{X}_v$ equals 1, then there is a canonical isomorphism from the relative picard functor $\mathrm{Pic}^0_{\mathcal{X}_v/\,\mathrm{Spec}(\mathcal{O}_{C,v})}$ to the identity component of the local Néron model $\mathcal{E}^0_v$ by [5, p.267, 9.5/4(b)]. In particular, there is a bijection

$$\mathrm{Pic}^0\,(\mathcal{X}_v) = \mathrm{Pic}^0_{\mathcal{X}_v/\,\mathrm{Spec}(\mathcal{O}_{C,v})}\,(\mathrm{Spec}(\mathcal{O}_{C,v})) \xrightarrow{\simeq} \mathcal{E}^0_v\,(\mathrm{Spec}(\mathcal{O}_{C,v}))\,.$$

Thus, the geometric stalk of $\mathrm{R}^1\,(\pi_*\mathbb{Z}_\ell(1))$ at v is canonically isomorphic to

$$\varprojlim_{n\geq 0} \mathcal{E}^0_v\,(\mathrm{Spec}(\mathcal{O}_{C,v}))\,[\ell^{n+1}],$$

which is by definition the geometric stalk of $T_\ell\left(\mathcal{E}^0\right)$ at v. The second part of the statement is obtained by tensoring by $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$.

(ii) The proof is similar: we consider the geometric stalks of the two $\mathbb{Z}_\ell$-sheaves (compare with the proof of Proposition 4.4.2) and then we tensor by $\mathbb{Q}_\ell$ over $\mathbb{Z}_\ell$.

□

Remark 4.10.7. This lemma implies that

$$\mathrm{L}(T, E/K_0) = \det\left(1 - T\,\mathrm{Frob}_q\,|V_\ell(\mathcal{E}^0)\right).$$

Remark 4.10.8. For any integer $j \in \mathbb{Z}$, the $\mathbb{Z}_\ell$-sheaves $\mathrm{R}^1\pi_*\,(\mathbb{Z}_\ell(1))\otimes_{\mathbb{Z}_\ell}\mathbb{Z}/\ell\mathbb{Z}$ and $\mathrm{R}^1\pi_*\,(\mathbb{Z}/\ell\mathbb{Z})(1))$ have canonically isomorphic geometric stalks. Therefore, the previous lemma also implies that

$$\mathrm{R}^1\pi_*\,(\mathbb{Z}/\ell\mathbb{Z}(1)) \simeq \mathcal{E}^0[\ell]$$

Observe also the following.

Lemma 4.10.9. *The $\mathbb{Q}_\ell$-adic sheaves $V_\ell(\mathcal{E}^0)$ and $V_\ell(\mathcal{E})$ are canonically isomorphic.*

Proof. By [18, p.144, Lemma 17], for each positive integer n, the sequence

$$0 \to \mathcal{E}^0_{\ell^n} \to \mathcal{E}_{\ell^n} \to \Phi_{\ell^n} \to 0$$

is exact. Therefore, we have a short exact sequence of $\mathbb{Z}_\ell$-sheaves

$$0 \to T_\ell(\mathcal{E}^0) \to T_\ell(\mathcal{E}) \to T_\ell(\Phi) \to 0.$$

By definition of Φ, each of the finitely many direct summands Φ_v is a finite étale group scheme of $\mathrm{Spec}(k_v)$. Therefore, Φ_v can be identified with its set of k_v-rational points $\Phi_v(k_v)$. In particular, none of them is infinitely ℓ-divisible. Therefore, $V_\ell(\Phi) = T_\ell(\Phi)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell = 0$ and therefore $V_\ell(\mathcal{E}^0)$ and $V_\ell(\mathcal{E})$ are canonically isomorphic. □

Taking into account what we proved, our main objective is to show that

$$\begin{aligned}\det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C, V_\ell\left(\mathcal{E}\right)\right)\right) &= \det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C, V_\ell\left(\mathcal{E}^0\right)\right)\right) \\ &\equiv \det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C, \mathcal{E}^0[\ell]\right)\right) \bmod \ell.\end{aligned}$$

Since we assumed that $E(K_0)[\ell] = \{O\}$, then $\mathrm{H}^0(C_{\text{ét}}, \mathcal{E}[\ell]) = 0$ and by the duality of Poincaré we have

$$\mathrm{H}^2(C_{\text{ét}}, \mathcal{E}^0[\ell]) = \mathrm{H}^2(C_{\text{ét}}, \mathcal{E}[\ell]) = 0.$$

In other words, we are in a situation where $\mathrm{H}^i(C_{\text{ét}}, \mathbb{Z}/\ell(1)) = 0$ for $i \neq 1$. We consider consequences of these assumptions. First, without the assumption on the vanishing to the zeroth and second cohomology groups, we have

Lemma 4.10.10. *For each nonnegative integers i and n, and each integer j the group* $\mathrm{H}^i\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right)$ *is a finitely generated* $\mathbb{Z}_\ell$*-module and there is a canonical exact sequence*

$$0 \to \mathrm{H}^i\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^n\mathbb{Z} \to \mathrm{H}^i\left(C_{ét}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(j))\right) \to \mathrm{H}^{i+1}\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right)[\ell^n] \to 0.$$

Proof. It suffices to verify that the conditions of [26, p.165, V.1.11] are satisfied for the $\mathbb{Z}_\ell$-adic sheaf $\mathrm{R}^1\pi_*(\mathbb{Z}_\ell(1))$, namely that

(i) all the cohomology groups $\mathrm{H}^i\left(C_{\text{ét}}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(j))\right)$ are all finite, and

(ii) the sheaf $\mathrm{R}^1\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(j))$ is a flat $(\mathbb{Z}/\ell^n\mathbb{Z})$-module.

We start by showing condition (i). We already explained why $\mathrm{R}^i\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(j))$ is a constructible, Abelian, torsion sheaf on $C_{\text{ét}}$. These properties, together with the facts that C is a smooth, proper curve over the algebraically closed field k whose characteristic is coprime to ℓ imply that the cohomology groups $\mathrm{H}^i\left(C_{\text{ét}}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(j))\right)$ are all finite by [44, 03SC, (4)]. To show condition (ii) it suffices to verify the statement on geometric stalks by [44, Tag 05NE]. For each point v of C we have

$$\left(\mathrm{R}^1\pi_*(\mathbb{Z}/\ell^n\mathbb{Z}(j))\right)_{\overline{v}} = \mathrm{H}^i(\mathcal{X}_{v,\text{ét}}, (\mathbb{Z}/\ell^n\mathbb{Z})(j))$$

which is a free, thus flat $\mathbb{Z}/\ell^n\mathbb{Z}$-module. □

We now use the assumption that the cohomology groups H^i vanish for $i \neq 1$.

Lemma 4.10.11. *Suppose that* $H^i\left(C_{ét}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell\mathbb{Z})\right) = 0$ *for* $i \in \{0, 2\}$. *Then for each integer* $j \in \mathbb{Z}$

(i) $\mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right)$ *is a free* $\mathbb{Z}_\ell$*-module.*

(ii) $\mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell\mathbb{Z} = \mathrm{H}^1\left(C_{ét}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell\mathbb{Z}(j))\right)$.

Proof. Tensoring the cohomology groups of in the assumption by $\mathbb{Z}/\ell\mathbb{Z}(j)$ over $\mathbb{Z}/\ell\mathbb{Z}$ for some $j \in \mathbb{Z}$ shows that equivalently we could assume that $H^i\left(C_{\text{ét}}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell\mathbb{Z}(j))\right) = 0$ for $i \in \{0, 2\}$ for any such integer j.

(i) Since $H^0\left(C_{\text{ét}}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell\mathbb{Z}(j))\right) = 0$, then Lemma 4.10.10 for $n = 1$ and $i = 0$ implies that

$$\mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right)[\ell] = 0.$$

Also from Lemma 4.10.10, $\mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right)$ is a finitely generate module over the principal ideal domain $\mathbb{Z}_\ell$. Now, a nonzero proper ideal of $\mathbb{Z}_\ell$ is of the form $\ell^r\mathbb{Z}_\ell$ for some positive integer r. Thus, it follows from the structure theorem for finitely generated modules over principal ideal domains that having no nonzero element of order ℓ is equivalent to to be torsion-free and thus free as $\mathbb{Z}_\ell$-module.

(ii) Since $\mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right)$ is a free $\mathbb{Z}_\ell$-module, then tensoring by $\mathbb{Z}/\ell\mathbb{Z}$ over $\mathbb{Z}_\ell$ commutes with cohomology and the result follows from Remark 4.10.8.

□

Lemma 4.10.12. *Suppose that $\pi : \mathcal{X} \to C$ is defined over k_0 and that $H^i(C, \mathrm{R}^1\pi_*\mathbb{Z}/\ell\mathbb{Z}) = 0$, for $i \in \{0, 2\}$. Then*

(1) The group G_{k_0} acts on $\mathrm{H}^1\left(C, \mathrm{R}^1\pi_*(\mathbb{Z}_\ell(j))\right)$ and on $\mathrm{H}^1\left(C_{ét}, \mathrm{R}^1\pi_*(\mathbb{Z}/\ell\mathbb{Z}(j))\right)$ continuously and functorially.

(2) Modulo ℓ, the characteristic polynomials of Frob_q on $\mathrm{H}^1\left(C, \mathrm{R}^1\pi_*\mathbb{Z}_\ell(j)) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell\mathbb{Z}\right)$ and on $\mathrm{H}^1\left(C_{ét}, \mathrm{R}^1\pi_*\mathbb{Z}/\ell\mathbb{Z}(j))\right)$ coincide.

Proof. Since the map π is defined over k_0, G_{k_0} has a canonical action on C by acting on k. This induces a functorial continuous action of G_{k_0} on $\mathrm{H}^1(C_{\text{ét}}, (R^1\pi_*\mathbb{Z}/\ell\mathbb{Z})(j))$ for any $n \geq 1$ and any $j \in \mathbb{Z}$, since this an étale cohomology group of an étale sheaf defined on C. This action is compatible with taking projective limit of these groups over $\mathbb{Z}_{\geq 1}$. It thus give a functorial continuous action of G_{k_0} on $\mathrm{H}^1(C, (R^1\pi_*\mathbb{Z}_\ell)(j)$.

Now, Lemma 4.10.11 (2), shows that the $\mathbb{F}_\ell$-vector spaces $\mathrm{H}^1(C, (\mathrm{R}^1\pi_*\mathbb{Z}_\ell(j)) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell\mathbb{Z}$ and $\mathrm{H}^1(C_{\text{ét}}, (\mathrm{R}^1\pi_*\mathbb{Z}/\ell\mathbb{Z}(j)))$ were canonically isomorphic. Therefore, the induced endomorphisms of $\mathbb{F}_\ell$-vector spaces are equal. □

In particular we have

$$\det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C, T_\ell\left(\mathcal{E}^0\right)\right)\right) \equiv \det\left(1 - T\,\mathrm{Frob}_q \,|\, \mathrm{H}^1\left(C_{\text{ét}}, \mathcal{E}^0[\ell]\right)\right) \bmod \ell,$$

which concludes the proof of Theorem 4.10.1.

Bibliography

[1] Emil Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. I & II*, Math. Z. **19** (1924), 153–206,207–246, DOI 10.1007/BF01181074, 10.1007/BF01181075. MR1544651, MR1544652

[2] Michael Artin and Pierre Deligne, *Théorie des topos et cohomologie étale des schémas. Séminaire de géométrie algébrique du Bois-Marie 1963-1964 (SGA 4)*: *Tome 3*, Lecture Notes in Mathematics, vol. 305, Springer Berlin, Heidelberg, 1973.

[3] Salman Baig and Chris Hall, *Experimental data for Goldfeld's conjecture over function fields*, Exp. Math. **21** (2012), no. 4, 362-374, DOI 10.1080/10586458.2012.671638. MR3004252

[4] Jose E. Bertin, Michel Demazure, and Pierre Gabriel, *Schémas en groupes. Séminaire de géometrie algébrique du Bois Marie 1962/64 (SGA 3)*: *I: Propriétés générales des schémas en groupes*, Lecture Notes in Mathematics, vol. 151, Springer Berlin, Heidelberg, 1970. MR0274458 (43 #223a)

[5] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, vol. 21, Springer Berlin, Heidelberg, 1990. MR1045822 (91i:14034)

[6] Alina Carmen Cojocaru and Chris Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Math. Res. Not. **2005** (2005), 3065–3080, DOI 10.1155/IMRN.2005.3065. MR2189500 (2006g:11107)

[7] Edgar Costa, David Harvey, and Kiran S. Kedlaya, *Zeta functions of nondegenerate hypersurfaces in toric varieties via controlled reduction in p-adic cohomology*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., Math. Sci. Publ. **2** (2019), 221–238, DOI 10.2140/obs.2019.2.221. MR3952014

[8] Pierre Deligne, *Cohomologie étale*: *Séminaire de géométrie algébrique du Bois-Marie SGA 4 1/2*, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, Berlin, 1977. MR0463174 (57 #3132)

[9] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273-307, DOI 10.1007/BF02684373. MR0340258 (49 #5013)

[10] Pierre Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252, DOI 10.1007/BF02684780. MR0601520 (83c:14017)

[11] Jean Dieudonné and Alexandre Grothendieck, *Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes*, Publications Mathématiques de l'Institut des Hautes Scientifiques, 1961. MR0217084 (36 #177b)

[12] David S Dummit and Richard M Foote, *Abstract algebra. Third edition*, John Wiley & Sons, Inc., Hoboken, N, 2004. MR2286236 (2007h:00003)

[13] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631-648, DOI 10.2140/10.2307/2372974. MR0140494 (25 #3914

[14] Lei Fu, *Etale cohomology theory*, Revised edition, Nankai Tracts in Mathematics, vol. 14, Scientific Publishing Co. Pte. Ltd., 2015. MR3380806

[15] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki: années 1964/65 1965/66, exposés 277-312, Séminaire Bourbaki **9** (1966, Exposé no. 279), 15 p. MR3202554

[16] Alexandre Grothendieck and Michèle Raynaud, *Revêtements étales et groupe fondamental*: *Séminaire de Géométrie Algébrique du Bois Marie 1960/61 (SGA 1)*, Édition recomposée SMF, Paris (2003), Lecture Notes in Mathematics, vol. 224, Springer, Berlin Heidelberg New York, 1971. MR0217088 (36 #179b)

[17] Pierre Deligne, Alexandre Grothendieck, Michèle Raynaud, Michel Raynaud, and D. S. Rim, *Groupes de monodromie en géométrie algébrique*: *Séminaire de géométrie algébrique du Bois-Marie 1967-1969. (SGA 7 I)*, Lecture Notes in Mathematics, vol. 288, Springer Berlin, Heidelberg, 1972. MR0217088 (36 #179b)

[18] Chris Hall, *L-functions of twisted Legendre curves*, J. Number Theory **119** (2006), no. 1, 128-147, DOI 10.1016/j.jnt.2005.10.004. MR2228953 (2007b:11091)

[19] Chris Hall, Jonathan P. Keating, and Edva Roditty-Gershon, *Variance of arithmetic sums and L-functions in* $\mathbb{F}_q[t]$, Algebra Number Theory **13** (2019), no. 1, 19-92, DOI 10.2140/ant.2019.13.19. MR3917915

[20] Helmut Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufie Mitteilung*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1933** (1933), 252-262.

[21] Kunihiko Kodaira, *On the structure of compact complex analytic surfaces. I*, Amer. J. Math **86** (1964), 751-798, DOI 10.2307/2373157. MR0187255 (32 #4708)

[22] Kunihiko Kodaira, *On the structure of compact complex analytic surfaces. II*, Amer. J. Math **88** (1966), 682-721, DOI 10.2307/2373150. MR0205280 (34 #5112)

[23] Luc Illusie (ed.), *Cohomologie l-adique et Fonctions L*: *Séminaire de géométrie algébrique du Bois-Marie 1965-66, SGA 5*, Lecture Notes in Mathematics, vol. 589, Springer Berlin, Heidelberg, 1977. MR0491704 (58 #10907)

[24] Nicholas M. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, N.J., 2002. MR1875130 (2003i:11087)

[25] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. MR1917232 (2003g:14001)

[26] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR0559531 (81j:14002)

[27] James S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Inc., 1986. MR0881804 (88e:14028)

[28] James S. Milne, *Abelian Varieties*, In: Cornell, G., Silverman, J.H. (eds) Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, NY, 1986. MR0861974

[29] David Mumford, *Abelian varieties*, Second Edition, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, London, 1974. MR0282985 (44 #219)

[30] Jacob P. Murre, *Lectures on an introduction to Grothendieck's theory of the fundamental group*, Notes by S. Anantharaman. Tata Institute of Fundamental Research Lectures on Mathematics, vol. 40, Tata Institute of Fundamental Research, Bombay, 1967. http://www.math.tifr.res.in/ publ/ln/tifr40.pdf. MR0302650 (46 #1794)

[31] André Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publications Mathématiques de L'Institut des Hautes Scientifiques **21** (1964), 5-125, DOI 10.1007/BF02684271. MR0179172 (31 #3423)

[32] Jürgen Neukirch, *Algebraic number theory*, Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences, vol. 322, Springer-Verlag, Berlin, 1999. MR3-540-65399-6

[33] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of Number Fields*, Second Edition, Grundlehren der mathematischen Wissenschaften, vol. 323, Springer Berlin, Heidelberg, 2008. MR2392026 (2008m:11223)

[34] Jonathan S. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763, DOI 10.1090/S0025-5718-1990-1035941-X. MR1035941 (91a:11071)

[35] Michael O. Rabin, *Probabilistic Algorithms in Finite Fields*, SIAM J. Comput. **9** (1980), no. 2, 273-280, DOI 10.1137/0209024. MR0568814 (81g:12002)

[36] Friedrich Karl Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math Z **33** (1931), 1-32, DOI 10.1007/BF01174341. MR1545199

[37] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p.*, Math. Comp. **44** (1985), no. 170, 483-494, DOI 10.1090/S0025-5718-1985-0777280-6. MR0777280 (86e:11122)

[38] René Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux **7** (1995), no. 1, 219–254. MR1413578 (97i:11070)

[39] Jean-Pierre Serre, *Groupes algébriques et corps de classes*: *cours au Collège de France*, Actualités scientifiques et industrielles, 1264; Publications de l'Institut de Mathématique de l'Université de Nancago, VII, Hermann Paris, 1959. MR0103191 (21 #1973)

[40] Romyar Sharifi, *Algebraic Number Theory*, `https://www.math.ucla.edu/~sharifi/algnum.pdf`. Consulted on May 11, 2022.

[41] Tetsuji Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), no. 1, 20-59, DOI 10.2969/jmsj/02410020. MR0429918 (55 #2927)

[42] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer New York, NY, 1994. MR1312368 (96b:11074)

[43] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer New York, NY, 2009. MR2849819

[44] The Stacks Project authors, *The Stacks Project* (2022), `https://stacks.math.columbia.edu`.

[45] Henning Stichtenoth, *Algebraic Function Fields and Codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer Berlin, Heidelberg, 2009. MR2464941 (2010d:14034)

[46] Michio Suzuki, *Group theory I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin-New York, 1982. MR0648772 (82k:20001c)

[47] Günter Tamme, *Introduction to étale cohomology*, Universitext, Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster. MR1317816 (95k:14033)

[48] Douglas Ulmer, *Elliptic curves over function fields*: *In: Arithmetic of L-functions*, Amer. Math. Soc., Providence, RI, posted on 2011, 211-280, DOI 10.1090/pcms/018. MR2882692

[49] André Weil, *Variétés abéliennes et courbes algébriques*, Publ. Inst. Math. Univ. Strasbourg, 8 (1946). Actualités Scientifiques et Industrielles, vol. 1064, Hermann & Cie, Paris, 1948. MR0029522 (10,621d)

[50] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497-508, DOI 10.1090/S0002-9904-1949-09219-4. MR0029393 (10,592e)

Curriculum Vitae

Name:	Félix Baril Boudreau
Post-Secondary Education and Degrees:	Western University London, Ontario, Canada Ph.D. Mathematics, 2022
	Western University London, Ontario, Canada M.Sc. Mathematics, 2017
	Université de Sherbrooke Sherbrooke, Québec, Canada B.Sc. Mathematics, 2013
Honours and Awards:	NSERC Postgraduate Scholarship-Doctoral program (PGS D) 2019-2021
	Western Graduate Research Scholarship Western University 2016-2021
	NSERC Undergraduate Student Research Award Summer 2011, Fall 2012
Related Work Experience:	Teaching Assistant Western University 2016 - 2022

Publications:

Baril Boudreau, Félix, *Reduction of an L-function Modulo an Integer*, `https://arxiv.org/abs/2110.12156`, 2021.