Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Magistrale in Matematica

The Iwasawa Main Conjecture for Elliptic Curves and its applications to the Birch and Swinnerton-Dyer Conjecture

Candidato:
Francesco Zerman
Matricola 1206685

Relatore:
Ch.mo Prof. Matteo Longo

17/07/2020
A.A. 2019/2020

God made the integers, all else is the work of man.
— L. Kronecker

Aknowledgements

First of all, I want to express my sincere gratitude to my advisor Prof. Matteo Longo for his tireless and patient answers, notwithstanding the communication difficulties due to the health emergency. Although from far, he made me understand and love the topic. A great thankyou goes to my collegue and friend Lorenzo Stefanello, with whom I shared doubts and discoveries during the work for this thesis. Without our correspondence, it would probably have taken me twice as long to understand many mathematical questions. Also, I would like to thank Riccardo Gilblas for being a selfless friend and collegue.

Last but not least, a big thankyou goes to Ginevra, my friends and my family, who have always been close to me, specially in times of difficulty and discouragement.

Contents

Introduction

The aim of this work is to present the cyclotomic Iwasawa main conjecture for elliptic curves and give some applications to the Birch and Swinnerton-Dyer conjecture. The branch of mathematics called *Iwasawa theory* is named after the japanese mathematician Kenkichi Iwasawa (1917-1998), who developed the theory of cyclotomic $\mathbb{Z}_p$-extensions in the '50s and '60s, initiating the systematic investigation of the field $\mathbb{Q}(\zeta_{p^\infty})$, that is the extension of $\mathbb{Q}$ obtained by adding every p^n-th root of unity. The subfield $\mathbb{Q}_\infty$ of $\mathbb{Q}(\zeta_{p^\infty})$ with Galois group over $\mathbb{Q}$ isomorphic to $\mathbb{Z}_p$ is called the *cyclotomic $\mathbb{Z}_p$-extension of* $\mathbb{Q}$. Similarly, if K is a number field, the product field $K_\infty := K\mathbb{Q}_\infty$ is called the *cyclotomic $\mathbb{Z}_p$-extension of* K. Iwasawa studied in detail the behaviour of these extensions and in particular proved a formula that bounds the p-part of the class number of the intermediate extensions between K and K_∞. His work was then extended to elliptic curves by Barry Mazur and Ralph Greenberg during the '70s and the '80s, where the role of the p-part of the ideal class group was replaced by another group associated to any elliptic curve, namely the Pontryagin dual of the p-primary Selmer group. During the last decades there have been many other generalizations of Iwasawa theory, mainly to abelian varieties and motives.

The general idea of Iwasawa theory for elliptic curves is to study the arithmetic of an elliptic curve E/K over K_∞ and then deduce consequences on the arithmetic of E over the base field K. On one hand, using cohomological and algebraic methods, one builds algebraic invariants linked to the arithmetic of E over K_∞. In particular, we are able to build $\mathrm{Sel}_E(K_\infty)_p$, the p-primary Selmer group associated to E and to the extension K_∞ (see Chapter 3 and Section 5.1). Using the isomorphism (see Proposition 2.4.2) between $\Lambda := \mathbb{Z}_p[[T]]$ and $\mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]$, that is the group ring of $\mathrm{Gal}(K_\infty/K)$ with coefficients in $\mathbb{Z}_p$, one is able to prove that $\mathrm{Sel}_E(K_\infty)_p$ is a discrete Λ-module. Then its Pontryagin dual is a compact Λ-module, and it is finitely generated. Using a structure theorem for finitely generated Λ-modules (see Theorem 2.2.8), we are able to associate to the dual of $\mathrm{Sel}_E(K_\infty)_p$ a particular ideal of Λ, namely $\xi_E(K_\infty)$, called the *characteristic ideal* of E over K_∞.

On the other hand, using p-adic analytic methods, one constructs some analytic invariants associated to the elliptic curve E. In Chapter 4 we per-

form this work for some special cusp forms and then, using the modularity theorem, we adapt the same construction for elliptic curves E defined over $\mathbb{Q}$. While a great part of the algebraic Iwasawa theory can be done for a generic number field, here we must restrict to elliptic curves defined over $\mathbb{Q}$, since we have to use the modularity theorem. We start defining particular measures on $\mathbb{Z}_p^\times$, the group of invertible elements of $\mathbb{Z}_p$, associated to E. Using a correspondence between measures on $\mathbb{Z}_p^\times$ and elements of Λ (see Section 4.9), one is able to construct the *p-adic L-series*, namely $\mathcal{L}_E$, that is a particular element of Λ associated to E. The p-adic L-series has the fundamental property that it interpolates the special values of the classical complex L-series twisted by cyclotomic characters (see Theorem 4.9.3). The Iwasawa main conjecture naively states that $\mathcal{L}_E$ generates the ideal $\xi_E(\mathbb{Q})$. From the fact that it relates a p-adic L-function and an algebraic invariant associated to E, one can think of the Iwasawa main conjecture as an analogue of the Birch and Swinnerton-Dyer conjecture for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

In recent years, an important step has been made with the paper [25] of Skinner-Urban, in which they prove the Iwasawa main conjecture for elliptic curves with good ordinary reduction at p, under some other technical hypotheses on E and on p. In this thesis we are going to deal with this result (Theorem 5.3.3), but I must warn the reader that progress has been made in the last few yers also for elliptic curves with supersingular and multiplicative reduction at p.

Not only Iwasawa theory for elliptic curves is interesting in itself, still being an open research field, but in the last years it came out that it can also be remarkably applied to study other open problems, such that a particular case of the Birch and Swinnerton-Dyer conjecture. This last conjecture, that is one of the seven famous Millennium Problems, says that the order of vanishing in $s = 1$ of the complex L-function $L(E, s)$ associated to an elliptic curve $E/\mathbb{Q}$ is equal to the algebraic rank r of $E(\mathbb{Q})$, the subgroup of rational points of E. This last group is known to be finitely generated (this is a theorem due to Mordell and Weil), but there is no known algorithm that allows us to compute its rank. There is also a more expanded formulation of the Birch and Swinnerton-Dyer conjecture, that predicts the precise value of the first nonzero term of the Taylor expansion of $L(E, s)$ centered in $s = 1$ in terms of algebraic invariants of E. This conjecture, first formulated in the '60s, is still an open problem. Despite hard work of many mathematicians, satisfactory results have been obtained only for the case $r \leq 1$. The main approach to study the expanded formulation of the conjecture is to look at its p-part, that is to try to solve the equality between the p-adic norms of the two terms, for every prime p. Clearly, if we prove the p-part of the Birch and Swinnerton-Dyer conjecture for every p, then the conjecture holds. The Iwasawa main conjecture can be used to prove the p-part of the expanded Birch and Swinnerton-Dyer conjecture when $r = 0$, under some hypotheses on E and on p. We are going to present this result in the last chapter.

Guide for the reader

In Chapter 1 we present some results about elliptic curves, from basic definitions to more advanced topics. The main goal of this chapter is to define and see the first properties of the multiplication-by-m map, the Tate module and the L-series associated to an elliptic curve. We also study the reduction types of an elliptic curve E at a prime of its base field, defining the conductor of E.

In Chapter 2 we look at the properties of $\Lambda_{\mathcal{O}_F}$, the power series ring in one variable with coefficients in the ring of integers of a finite extension F of $\mathbb{Q}_p$. We study its structure as a ring and the structure of its prime ideals. We give a characterization of finitely generated $\Lambda_{\mathcal{O}_F}$-modules up to pseudo-isomorphism, defining the characteristic ideal associated to such modules. Then, we define and look at the fundamental properties of Pontryagin duality. Finally, we study $\mathbb{Z}_p$-extensions of number fields, proving also an important isomorphism theorem for Λ.

In Chapter 3 we define cohomological invariants attached to elliptic curves E defined over a number field K. We define the Shafarevich-Tate and Selmer groups, in all their forms. We also present the Mordell-Weil theorem.

Chapter 4 is devoted to the construction of the p-adic L-series. We begin with some general definitions and properties of cusp forms and Hecke operators. Introducing the theory of modular symbols, we define two measures on $\mathbb{Z}_p^\times$ associated to particular cusp forms. Integrating p-adic characters with respect to this measures, we construct the p-adic L-function. We state the modularity theorem, that serves us to define the p-adic L-series associated to an elliptic curve $E/\mathbb{Q}$ with good ordinary reduction at an odd prime p. Twisting modular forms and L-functions, we are able to present a result that gives a relation between the value of the p-adic L-series associated to E and the special values of the complex L-fuction twisted by the same character.

In Chapter 5 we give the statement of the Iwasawa main conjecture for elliptic curves $E/\mathbb{Q}$ with good ordinary reduction at an odd prime p. With this goal, we study in detail the structure of the p-primary Selmer group of an elliptic curve E, defined over a number field K, over the cyclotomic $\mathbb{Z}_p$-extension of K. We also prove Mazur's control theorem, that is a fundamental result in Iwasawa theory for elliptic curves. Finally, we present the statement of the main result proved in [25], that solves partially the main conjecture.

We begin Chapter 6 with the presentation of the Birch and Swinnerton-Dyer conjecture. Then we prove a result due to Ralph Greenberg, that together with the Iwasawa main conjecture leads to the proof of a particular case of the p-part of the Birch and Swinnerton-Dyer conjecture for $r = 0$.

Notation

We fix some notation that will be used throughout the thesis.

$A \subseteq B$	if A is a subset of B;
$A \subset B$	if A is a proper subset of B;
$R^\times$	the group of invertible elements of the ring R;
$\mathbb{N}$	the natural numbers;
$\mathbb{Z}$	the integers;
$\mathbb{Q}$	the rational numbers;
$\mathbb{R}$	the real numbers;
$\mathbb{R}_{\geq 0}$	the nonnegative real numbers;
$\mathbb{C}$	the complex numbers;
$\mathbb{F}_q$	a field with q elements;
$\mathbb{Z}_p$	the p-adic integers with p prime;
$\mathbb{Q}_p$	the field of fractions of $\mathbb{Z}_p$;
$\mathbb{C}_p$	the Cauchy completion of an algebraic closure of $\mathbb{Q}_p$;
K	a perfect field;
$\bar{K}$	a fixed algebraic closure of K;
$\mathrm{Gal}(L/K) = G_{L/K}$	the Galois group of a separable field extension;
$\Lambda = \mathbb{Z}_p[[T]]$	the power series ring in the variable T with coefficients in $\mathbb{Z}_p$;
$\mathrm{GL}_2(K)$	the group of 2×2 invertible matrices with coefficients in K;
$\mathrm{GL}_2^+(\mathbb{R})$	the subgroup of $\mathrm{GL}_2(\mathbb{R})$ consisting of matrices with positive determinant;
$\mathrm{SL}_2(K)$	the subgroup of $\mathrm{GL}_2(K)$ consisting of matrices with determinant equal to 1.

Chapter 1

Elliptic Curves

In this chapter we give a general introduction to elliptic curves, mainly following [22]. We fix

K	a perfect field;
$\bar{K}$	an algebraic closure of K;
$G_{\bar{K}/K}$	the Galois group of the extension $\bar{K}/K$;
$\mathbb{P}^n = \mathbb{P}^n(\bar{K})$	the n-dimensional projective space over $\bar{K}$.

1.1 Basic results

Definition. An *elliptic curve* is a pair (E, O) with E a smooth projective curve of genus 1 and O a point on E.

An elliptic curve is *defined over* K, written E/K, if the ideal of E (remember that E is a projective variety) can be generated by polynomials with coefficients on the field K and O can be represented with coordinates in K. If E/K is defined over K, we call $E(K)$ the set of points of E that can be represented with homogeneous coordinates in K.

The first fundamental result is that every elliptic curve is isomorphic to a certain plane curve.

Proposition 1.1.1. *Let E/K be an elliptic curve defined over K. Then there exists a morphism*

$$\phi : E \longrightarrow \mathbb{P}^2$$

that gives an isomorphism of E/K onto a curve C given by an (affine) equation of the type

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.1}$$

with $a_1, \ldots, a_6 \in K$ and satisfying $\phi(O) = [0, 1, 0]$.

Proof. See [22, III.3.1]. □

Definition. An equation of the type of (1.1) for an elliptic curve E is called a *Weierstrass equation* for E.

Thanks to the above proposition, we can always think of an elliptic curve E/K defined over K as a smooth plane curve defined by a Weierstrass equation with coefficients in K and $O = [0,1,0]$.

We see now that every elliptic curve given by a Weierstrass equation can be endowed with a natural structure of abelian group.

Construction 1.1.2. Let E be an elliptic curve given by a Weierstrass equation, $P, Q \in E$. Let l be the line through P and Q (if $P = Q$, let l be the tangent line to E at P), and let R be the third point of intersection of l with E. Let l' be the line through R and O. Then l' intersects E at R, O and a third point. We denote the third point by $P + Q$.

Remark 1.1.3. The existence and the uniqueness of the points R and $P+Q$ in the above construction are granted by Bezout's theorem.

Proposition 1.1.4. *Let E/K be an elliptic curve given by a Weierstrass equation.*

(a) The operation defined in construction 1.1.2 defines an abelian group structure on $E(\bar{K})$, with identity element $O = [0,1,0]$.

(b) The set of K-rational points $E(K)$ is a subgroup of $E(\bar{K})$.

Proof. See [22, III.2]. □

Now we see that the algebraic structure we defined on an elliptic curve E is somehow compatible with the geometric structure of E.

Theorem 1.1.5. *Let E/K be an elliptic curve defined over K. Then the functions*

$$\begin{array}{ll} +: E \times E \longrightarrow E, & \text{and} \quad -: E \longrightarrow E \\ (P_1, P_2) \mapsto P_1 + P_2 & P \longmapsto -P \end{array}$$

are morphisms of varieties.

Proof. See [22, III.3.6]. □

Remark 1.1.6. Let $G_{\bar{K}/K}$ be the Galois group of the Galois extension $\bar{K}/K$ (remember that K is a perfect field, hence $\bar{K}/K$ is separable). Let E/K be an elliptic curve defined over K. Then the action of $G_{\bar{K}/K}$ on the coordinates of each point $P \in E(\bar{K})$ defines an action of $G_{\bar{K}/K}$ on $E(\bar{K})$. For every $P \in E(\bar{K})$, $\sigma \in G_{\bar{K}/K}$, we denote by $\sigma(P)$ the transformed of the point P by the action of σ.
Since the algorithm that gives us the sum of two points $P, Q \in E(\bar{K})$ is rational in the coordinates of P and Q (see [22, III.2.3]), we have that

$$\sigma(P + Q) = \sigma(P) + \sigma(Q)$$

for every $P, Q \in E$ and $\sigma \in G_{\bar{K}/K}$.

1.2 Isogenies

We turn now to study maps between elliptic curves. Since elliptic curves are both geometric and algebraic objects, it's natural to introduce maps that preserve both structures. These maps are called *isogenies*. We first start with some preliminary results.

Definition. Let C_1/K and C_2/K be projective curves defined over K. A morphism $\phi : C_1 \to C_2$ is said to be *defined over* K if

$$\sigma(\phi(P)) = \phi(\sigma(P))$$

for every $P \in C_1$ and $\sigma \in G_{\bar{K}/K}$.

Theorem 1.2.1. *Let $\phi : C_1 \to C_2$ be a morphism of projective curves. Then ϕ is either constant or surjective.*

Proof. Since C_1 is a projective variety, its image inside C_2 must be a projective variety, and the only projective varieties contained inside a projective curve are each single point of the curve or the curve itself. □

Definition. Let $\phi : C_1 \to C_2$ be a morphism of curves defined over K. If ϕ is constant, we define the *degree of* ϕ to be 0. Otherwise, we define the *degree* of ϕ to be

$$\deg \phi := [K(C_1) : \phi^*(K(C_2))],$$

with $K(C_i)$ the field of rational functions on C_i and ϕ^* the pullback of ϕ.

Theorem 1.2.2. *Let C_1/K and C_2/K be projective curves defined over K, let $\phi : C_1 \to C_2$ be a nonconstant morphism defined over K. Then $K(C_1)$ is a finite extension of $\phi^*(K(C_2))$.*

Proof. See [22, II.2.4]. □

Definition. Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism of varieties

$$\phi : E_1 \longrightarrow E_2 \quad \text{satisfying} \quad \phi(O) = O.$$

Remark 1.2.3. Applying Theorem 1.2.1 it's clear that an isogeny satisfies either $\phi(E_1) = O$ or $\phi(E_1) = E_2$.

A remarkable fact, stated in the next theorem, says that any isogeny is a group homomorphism.

Theorem 1.2.4. *Let $\phi : E_1 \to E_2$ be an isogeny. Then for every $P, Q \in E_1$ we have*

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Proof. See [22, III.4.8]. □

Corollary 1.2.5. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny. Then*

$$\ker \phi = \phi^{\leftarrow}(O)$$

is a finite group.

Proof. From the theorem above we have that ϕ is a group morphism, hence $\ker \phi$ is a subgroup of E_1, and it is finite since its cardinality is at most $\deg \phi$. □

Example 1.2.6. Let E/K be an elliptic curve and let $Q \in E(\bar{K})$. Then we can define a *translation-by-Q map*

$$\begin{aligned} \tau_Q : E(\bar{K}) &\longrightarrow E(\bar{K}) \\ P &\longmapsto P + Q. \end{aligned}$$

The map τ_Q is an isomorphism since τ_{-Q} provides an inverse. Of course, it is not an isogeny unless $Q = O$.

Definition. The set of all isogenies from E_1 to E_2 is denoted by $\mathrm{Hom}(E_1, E_2)$. If $E_1 = E_2 = E$, we usually set $\mathrm{Hom}(E, E) =: \mathrm{End}(E)$.

For any $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ we define the addition pointwise:

$$(\phi + \psi)(P) := \phi(P) + \psi(P)$$

for every $P \in E_1$. Theorem 1.1.5 grants us that $\phi + \psi$ is a morphism, hence an isogeny. Therefore $\mathrm{Hom}(E_1, E_2)$ is a group. The set $\mathrm{End}(E)$ is endowed with a structure of ring: addition is defined as above, multiplication is defined by composition of mappings.

Definition. If E_1, E_2 and E are defined over K, then we can define the subgroup of the isogenies from E_1 to E_2 defined over K as $\mathrm{Hom}_K(E_1, E_2)$. Similarly, we define $\mathrm{End}_K(E)$ to be the subring of $\mathrm{End}(E)$ consisting of all isogenies defined over K.

1.3 The multiplication-by-m isogeny

In this section we present one of the most important types of isogenies, that will play a fundamental role in the next chapters.

Definition. For each $m \in \mathbb{Z}$ we define the *multiplication-by-m isogeny*

$$[m] : E(\bar{K}) \longrightarrow E(\bar{K}),$$

which sends

$$P \longmapsto \underbrace{P + P + \cdots + P}_{m \text{ terms}}$$

if $m > 0$. If $m < 0$ just set $[m]P := [-m](-P)$. If $m = 0$ we simply have $[0]P := O$.

Using theorem 1.1.5, an easy induction shows that $[m]$ is a morphism, hence an isogeny, since it clearly sends O to O. Using Remark 1.1.6 we also have that if E is defined over K then $[m]$ is defined over K.

Proposition 1.3.1. *Let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$. Then the multiplication-by-m isogeny $[m] : E(\bar{K}) \to E(\bar{K})$ is nonconstant, i.e. surjective.*

Proof. See [22, III.4.2]. □

Definition. Let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The *m-torsion subgroup of E*, denoted by $E[m]$ or $E(\bar{K})[m]$, is the set of points of $E(\bar{K})$ of order dividing m, i.e $E[m] := \ker[m]$.

Definition. The *torsion subgroup of E*, denoted by E_{tors} or $E(\bar{K})_{tors}$, is the set of points of $E(\bar{K})$ with finite order, i.e.

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

If E is defined over K, then $E(K)_{tors}$ denotes the points of finite order in $E(K)$.

Definition. Let p be a prime. The *p-primary subgroup of E*, denoted by $E[p^\infty]$ or $E(\bar{K})[p^\infty]$ is the subgroup of $E(\bar{K})$ consisting of all elements with order p^n for some $n \in \mathbb{N}$. Namely:

$$E[p^\infty] = \bigcup_{n=1}^{\infty} E[p^n] = \varinjlim_{n} E[p^n].$$

Defining and studying the behaviour of the dual isogenies, it comes out this fundamental result related to the multiplication-by-m function and the m-torsion groups.

Theorem 1.3.2. *Let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m > 0$. Then*

(a) $\deg[m] = m^2$.

(b) If $m \neq 0$ in K, i.e. if $\mathrm{char}(K)$ *does not divide m, then*

$$E(\bar{K})[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(c) If $\mathrm{char}(K) = p > 0$, *then either* $E(\bar{K})[p^e] = \{O\}$ *or* $E(\bar{K})[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ *for every* $e \geq 1$.

Proof. See [22, III.6.4]. □

Let E/K be an elliptic curve defined over K, $m \in \mathbb{Z}$. It's easy to see that both $E(\bar{K})$ and $E(\bar{K})[m]$ are $G_{\bar{K}/K}$-modules (see Appendix A) and since $[m] : E(\bar{K}) \to E(\bar{K})$ is defined over K, we have that $[m]$ is a $G_{\bar{K}/K}$-module homomorphism. Hence, thanks to Proposition 1.3.1, we have the following exact sequence of $G_{\bar{K}/K}$-modules:

$$0 \longrightarrow E(\bar{K})[m] \longrightarrow E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \longrightarrow 0.$$

1.4 Reduction at a prime

In this section we let K be a number field and we study the behaviour of an elliptic curve E/K when we reduce its equation at a prime of the ring of integers of K. Call $\mathfrak{p}$ such a prime and v its associated valuation. Let K_v be the completion of K with respect to the valuation v and let k_v be the residue field. Fix an elliptic curve E/K with Weierstrass equation

$$Y^2 + a_1XY + a_3 = X^3 + a_2X^2 + a_4X + a_6$$

with $a_1, \ldots, a_6 \in K$.

Definition. A Weierstrass equation for E/K is called a *minimal Weierstrass equation for* E *at* v if $v(\Delta)$ is minimized under the condition that $v(a_i) \geq 0$ for $i = 1, \ldots, 6$.

Here $\Delta \in K$ is the discriminant of the Weierstrass equation (for a precise definition see [22, III.1]). A curve given by a Weierstrass equation is an elliptic curve if and only if $\Delta \neq 0$, otherwise it has a node or a cusp.

Proposition 1.4.1. *Every elliptic curve* E/K *has a minimal Weierstrass equation at* v.

Proof. See [22, VII.1.3]. □

Consider now a minimal Weierstrass equation at v for E/K, and call $\tilde{a}_i$ the reduction of a_i modulo $\mathfrak{p}$. The curve $\tilde{E}_v$ (or $\tilde{E}$ when v is clear from the context) defined by the equation

$$\tilde{E} \ : \ Y^2 + \tilde{a}_1XY + \tilde{a}_3Y = X^3 + \tilde{a}_2X^2 + \tilde{a}_4X + \tilde{a}_6$$

is defined over the residue field k_v and it is usually called the *reduction of* E *modulo* $\mathfrak{p}$ (or *modulo* v).

Definition. Let E/K be an elliptic curve and let $\tilde{E}$ be the reduction modulo $\mathfrak{p}$. We say that

(a) E has *good reduction* at $\mathfrak{p}$ if $\tilde{E}$ is nonsingular.

(b) E has *multiplicative reduction* at $\mathfrak{p}$ if $\tilde{E}$ has a node.

(c) E has *additive reduction* at $\mathfrak{p}$ if $\tilde{E}$ has a cusp.

If E has multiplicative reduction at $\mathfrak{p}$, then the reduction is said to be *split* if the slopes of the tangent lines at the node are in k_v, and otherwise it is said to be *nonsplit*.

Lemma 1.4.2. *Let E/K be an elliptic curve. Then E has good reduction at all but finitely many primes.*

Proof. Take any Weierstrass equation for E/K

$$E:\ Y^2 + a_1Y + a_3 = X^3 + a_2X^2 + a_4X + a_6$$

and call its discriminant Δ. Let S be the set of all primes of $\mathcal{O}_K$ that appear in the factorization of every a_i with negative exponent and in the factorization of Δ with any exponent $\neq 0$. Then S is a finite set, and we see that for any prime $\mathfrak{p}$ outide S the given equation is a minimal Weierstrass equation and the reduced curve is nonsingular since the reduction of Δ modulo $\mathfrak{p}$ is nonzero. □

Remark 1.4.3. The reduction type of the curve does not depend on the minimal Weierstrass equation chosen.

Definition. Let E/K be an elliptic curve and $\tilde{E}$ the reduction of E modulo $\mathfrak{p}$. We say that E has *good ordinary reduction* at v if E has good reduction at $\mathfrak{p}$ and $\tilde{E}(\bar{k}_\mathfrak{p})[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for every $r \geq 1$.
We say that E has *good supersingular* reduction at $\mathfrak{p}$ if E has good reduction at $\mathfrak{p}$ and $\tilde{E}(\bar{k}_\mathfrak{p})[p^r] = \{O\}$ for every $r \geq 1$.

Definition. Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ and p a prime integer. Call $\tilde{E}$ the reduction of E modulo p. We define the integer $a_p(E)$ by the formula

$$a_p(E) = p + 1 - |\tilde{E}(\mathbb{F}_p)|$$

where $|\tilde{E}(\mathbb{F}_p)|$ denotes the number of the points of $\tilde{E}(\mathbb{F}_p)$.

Lemma 1.4.4. *Let p be a prime of $\mathbb{Z}$. Then an elliptic curve $E/\mathbb{Q}$ has good ordinary reduction at p if and only if $E/\mathbb{Q}$ has good reduction at p and $p \nmid a_p(E)$.*

Proof. See [22, Proof of V.4.1]. □

Definition. Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. For any prime $p > 3$ we define

$$m_p(E) := \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

For $p = 2, 3$ there's a more complicated formulation for $m_p(E)$ that can be found in [23, IV.10]. In any case $m_3(E) \leq 5$ and $m_2(E) \leq 8$.

Definition. The *conductor of* $E/\mathbb{Q}$ is defined by

$$N_E := \prod_p p^{m_p(E)}$$

where p runs over the primes of $\mathbb{Z}$.

1.5 The Tate module

Let K be a perfect field and $l \in \mathbb{Z}$ a prime. In this section we give a brief summary of the construction of the l-adic Tate module of an elliptic curve E/K and we study some properties of the Weil pairing. For more details see [22, III.7-III.8].

Definition. Let E/K be an elliptic curve and $l \in \mathbb{Z}$ be a prime. The *l-adic Tate module of E* is the group

$$T_l(E) := \varprojlim_{n \in \mathbb{N}} E(\bar{K})[l^n],$$

where the inverse limit is taken with respect to the natural maps

$$E(\bar{K})[l^{n+1}] \xrightarrow{[l]} E(\bar{K})[l^n].$$

Since each $E(\bar{K})[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}_l$-module. Moreover, the inverse limit topology is equivalent to the topology it gains by being a $\mathbb{Z}_l$-module.

Proposition 1.5.1. *The Tate module has the following structure:*

(a) $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ *as a* $\mathbb{Z}_l$*-module, if* $l \neq \mathrm{char}(K)$.

(b) $T_l(E) \cong \mathbb{Z}_l$ *or* $\{0\}$ *as a* $\mathbb{Z}_l$*-module, if* $l = \mathrm{char}(K) > 0$.

Proof. It follows immediately from Theorem 1.3.2. □

Example 1.5.2. Let E/K be an elliptic curve defined over a number field K, let v be a valuation of K and call k_v the residue field. If E has good reduction at v, then the reduction of E modulo v, namely $\tilde{E}_v$, is an elliptic curve defined over k_v. Let $l := \mathrm{char}(k_v)$. If E has good ordinary reduction at v, we have that $T_l(\tilde{E}_v) \cong \mathbb{Z}_l$. Otherwise, $T_l(\tilde{E}_v) = \{0\}$.

We now present some properties of the Weil pairing. For the precise construction we refer to [22, III.8].

Proposition 1.5.3. *Let $m \geq 2$ and let $\mu_m \subseteq \bar{K}$ denote the group of m-th roots of unity. There exists a pairing (the* Weil e_m-pairing*)*

$$e_m : E(\bar{K})[m] \times E(\bar{K})[m] \longrightarrow \mu_m$$

that satisfies the following properties:

(a) It is bilinear.

(b) It is alternating:

$$e_m(T,T) = 1 \quad \textit{and hence} \quad e_m(S,T) = e_m(T,S)^{-1}$$

for every $T, S \in E(\bar{K})[m]$.

(c) It is nondegenerate, i.e. if $e_m(S,T) = 1$ for every $S \in E(\bar{K})[m]$, then $T = O$.

(d) It is Galois invariant:

$$\sigma(e_m(S,T)) = e_m(\sigma(S), \sigma(T))$$

for every $\sigma \in G_{\bar{K}/K}$ and $T, S \in E(\bar{K})[m]$.

(e) It is compatible:

$$e_{mm'}(S,T) = e_m([m']S, T)$$

for every $S \in E(\bar{K})[mm']$ and $T \in E[m]$.

Proof. See [22, III.8.1]. □

Let l be a prime number different from $\mathrm{char}(K)$. Using the properties of the above Proposition it's easy to see that

$$e_{l^{n+1}}(S,T)^l = e_{l^n}([l]S, [l]T)$$

for every $S, T \in E[l^{n+1}]$. This property allows us to pass to inverse limits and prove the following proposition.

Proposition 1.5.4. *There exists a bilinear, alternating, nondegenerate, Galois invariant pairing*

$$e : T_l(E) \times T_l(E) \longrightarrow T_l(\mu),$$

where $T_l(\mu) := \varprojlim_{n\in\mathbb{N}} \mu_{l^n}$.

Let l be a prime different from $\mathrm{char}(K)$. We are now going to study some properties of the action of $G_{\bar{K},K}$ on $T_l(E)$.

Definition. The l-adic cyclotomic character is a group homomorphism

$$\chi : G_{\bar{K}/K} \longrightarrow \mathbb{Z}_l^\times$$

such that for any l^n-th root of unit $\zeta \in \bar{K}$ we have that

$$\sigma(\zeta) = \zeta^{\chi(\sigma)}$$

for every $\sigma \in G_{\bar{K}/K}$.

Lemma 1.5.5. *Let E/K be an elliptic curve, $l \neq \mathrm{char}(K)$ a prime of $\mathbb{Z}$. The determinant representation of $G_{\bar{K}/K}$ on $T_l(E)$ is the cyclotomic character χ.*

Proof. First, consider the representation ρ_{l^n} of $G_{\bar{K}/K}$ on $E(\bar{K})[l^n]$. Fix a basis P, Q for ρ_{l^n}. We have the Weil pairing $e_{l^n}(P,Q) = \zeta$ where ζ is necessarily a primitive l^n-th root of unity, since e_{l^n} is non degenerate. Let now $\sigma \in G_{\bar{K}/K}$ act as the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on $E(\bar{K})[l^n]$, i.e. $\sigma(P) = aP + cQ$ and $\sigma(Q) = bP + dQ$, with $a, b, c, d \in \mathbb{Z}/l^n\mathbb{Z}$. Then, using the properites of Proposition 1.5.3 we have that

$$\begin{aligned}\sigma(\zeta) = \sigma(e_{l^n}(P,Q)) = e_{l^n}(\sigma(P), \sigma(Q)) = e_{l^n}(aP + cQ, bP + dQ) = \\ = e_{l^n}(P,Q)^{ad-bc} = \zeta^{ad-bc}.\end{aligned}$$

By definition of the cyclotomic character χ we have that the projection of $\chi(\sigma)$ onto $\mathbb{Z}/l^n\mathbb{Z}$ coincides with $ad - bc$, which is exactly the determinant of ρ_{l^n}. Taking the inverse limit on $n \in \mathbb{N}$, we conclude. □

1.6 L-series

Let $E/\mathbb{Q}$ be an elliptic curve. In this section we introduce the first properties of the L-series associated to E. We will develop its study in the next chapters.

Definition. Let p be a prime and $E/\mathbb{Q}$ be an elliptic curve. Define the *local L-function at p* by setting $L(E/\mathbb{Q}_p, s)$ to be

$(1 - a_p(E)p^{-s} + p^{1-2s})^{-1}$	if E has good reduction at p;
$(1 - p^{-s})^{-1}$	if E has split multiplicative reduction at p;
$(1 + p^{-s})^{-1}$	if E has nonsplit multiplicative reduction at p;
1	otherwise.

Definition. The *L-series of $E/\mathbb{Q}$* is defined by the Euler product

$$L(E,s) := \prod_p L(E/\mathbb{Q}_p, s)$$

where p varies amongst all primes of $\mathbb{Z}$.

Lemma 1.6.1. *The L-series of $E/\mathbb{Q}$ converges to an analytic function for every $s \in \mathbb{C}$ such that $\Re(s) > \frac{3}{2}$.*

Proof. First notice that since E has bad reduction only modulo finitely many primes, it's enough to study the convergence of

$$g(s) = \prod_p (1 - a_p(E)p^{-s} + p^{1-2s})^{-1}$$

where p varies amongst the primes of good reduction for E. Take K any compact set contained in $\{\, \Re(s) > \frac{3}{2} \,\}$ and call $b := \min_{s\in K} \Re(s)$. Then for every prime p and $s \in K$

$$\left| \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}} - 1 \right| = \frac{|a_p(E)p^{-s} - p^{1-2s}|}{|1 - a_p(E)p^{-s} + p^{1-2s}|} \leq \frac{|a_p(E)|p^{-\Re(s)} + p^{-2}}{\left| |1 + p^{1-2s}| - |a_p(E)p^{-s}| \right|}.$$

The Hasse inequality (see [22, V.1.1]) says that $|a_p(E)| \leq 2\sqrt{p}$, hence we can proceed with the inequalities

$$\frac{|a_p(E)|p^{-\Re(s)} + p^{-2}}{\left| |1 + p^{1-2s}| - |a_p(E)p^{-s}| \right|} \leq \frac{2p^{\frac{1}{2}-\Re(s)} + p^{-2}}{\left| 1 - |2p^{\frac{1}{2}-s}| \right|} \leq \frac{2p^{\frac{1}{2}-b} + p^{-2}}{1 - 2^{\frac{3}{2}-b}}$$

since $p \geq 2$ for every prime p. Since $\frac{1}{2} - b < -1$ we have that

$$\sum_p \frac{2p^{\frac{1}{2}-b} + p^{-2}}{1 - 2^{\frac{3}{2}-b}} \leq \sum_{n\in\mathbb{N}} \frac{2n^{\frac{1}{2}-b} + n^{-2}}{1 - 2^{\frac{3}{2}-b}}$$

converges. Therefore the product that defines $g(s)$ is normally convergent in $\{\, \Re(s) > \frac{3}{2} \,\}$. □

Chapter 2

Modules over $\Lambda_{\mathcal{O}_F}$ and $\mathbb{Z}_p$-extensions

In this chapter we present some results about the so called *Iwasawa algebra* $\Lambda := \mathbb{Z}_p[[T]]$, i.e. the power series ring in the variable T with coefficients in the p-adic integers $\mathbb{Z}_p$. In particular, we prove an important structure theorem about finitely generated Λ-modules. When possible, we state and prove results that hold for a bigger class of algebras, namely the algebras of power series over the ring of integers of a finite extension of $\mathbb{Q}_p$. Then, we look at some properties of Pontryagin duality of Λ-modules. In the end, we study the behaviour of $\mathbb{Z}_p$-extensions of number fields. We mainly follow [26] and [21]. We fix some notation that will be used throughout this chapter:

p	an odd prime of $\mathbb{Z}$, that works also as a uniformizer for the local ring $\mathbb{Z}_p$;
F	a finite extension of $\mathbb{Q}_p$;
$\mathcal{O}_F$	the ring of integers of F;
π	a uniformizer for $\mathcal{O}_F$;
$\mathfrak{p}$	the maximal ideal of $\mathcal{O}_F$, generated by π;
$v_\mathfrak{p}$	the $\mathfrak{p}$-adic valuation in F;
$\Lambda_{\mathcal{O}_F} = \mathcal{O}_F[[T]]$	the power series ring in the variable T with coefficients in $\mathcal{O}_F$;
$\Lambda = \Lambda_{\mathbb{Q}_p}$	the power series ring in the variable T with coefficients in $\mathbb{Z}_p$.

2.1 The structure of $\Lambda_{\mathcal{O}_F}$

We begin with an easy result that describes the invertible elements in $\Lambda_{\mathcal{O}_F}$, which infact is valid in any power series ring.

Lemma 2.1.1. *An element $f = \sum_{i=0}^{\infty} a_i T^i \in \Lambda_{\mathcal{O}_F}$ is invertible in $\Lambda_{\mathcal{O}_F}$ if and only if $a_0 \in \mathcal{O}_F^\times$, i.e. f is invertible if and only if $v_\mathfrak{p}(a_0) = 0$.*

Proof. If f is invertible in $\Lambda_{\mathcal{O}_F}$ then there exists $g = \sum_{i=0}^{\infty} b_i T^i \in \Lambda_{\mathcal{O}_F}$ such that $f \cdot g = 1$. Ordering the terms of $f \cdot g$ with respect to the powers of T, we see that $f \cdot g = 1$ implies that the term corresponding to the zero power of T must be equal to 1, i.e. $a_0 b_0 = 1$. This means means that a_0 is invertible in $\mathcal{O}_F$.

Conversely, in order to construct an inverse $g = \sum_{i=0}^{\infty} b_i T^i \in \Lambda_{\mathcal{O}_F}$ of f, we construct each $b_i \in \mathcal{O}_F$ in such a way that $f \cdot g = 1$. Notice that $f \cdot g = 1$ if and only if $a_0 b_0 = 1$ and the coefficient of T^i is equal to 0 for every $i \geq 1$. Since $a_0 \in \mathcal{O}_F^\times$ by hypothesis, then there exists $b_0 \in \mathcal{O}_F^\times$ such that $a_0 b_0 = 1$. This way we have fixed b_0. Then we can take b_1 as the only element of $\mathcal{O}_F$ such that $a_0 b_1 + a_1 b_0 = 0$, i.e. $b_1 = \frac{a_1 b_0}{a_0}$. Proceeding with this fashion we can construct every b_i, since the equation they must satisfy depends only on the (yet constructed) b_j whith $j < i$ and the only element that must be inverted at each step is just a_0, which is invertible by hypothesis. □

From a topological point of view, we endow $\Lambda_{\mathcal{O}_F}$ with the (π, T)-adic topology, where (π, T) is the ideal of $\Lambda_{\mathcal{O}_F}$ generated by π and the variable T. We'll see later that this ideal is the only maximal ideal in $\Lambda_{\mathcal{O}_F}$. We prove now a division algorithm for the algebra $\Lambda_{\mathcal{O}_F}$.

Proposition 2.1.2. *Let $f, g \in \Lambda_{\mathcal{O}_F}$ with $f = \sum_{i=0}^{\infty} a_i T^i$ such that $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$ and $a_n \in \mathcal{O}_F^\times$, for some $n \in \mathbb{N}$. Then there exist a unique $q \in \Lambda_{\mathcal{O}_F}$ and a unique $r \in \mathcal{O}_F[T]$ with $\deg r \leq n-1$ so that*

$$g = qf + r.$$

Proof. We begin by defining a shifting operator $\tau_n : \Lambda_{\mathcal{O}_F} \to \Lambda_{\mathcal{O}_F}$ defined by

$$\tau_n\Big(\sum_{i=0}^{\infty} b_i T^i\Big) = \sum_{i=n}^{\infty} b_i T^{i-n}.$$

This operator is clearely $\mathcal{O}_F$-linear and continous for the (π, T)-adic topology. Furthermore, for every $h(T) \in \Lambda_{\mathcal{O}_F}$ one has

- $\tau_n(T^n h(T)) = h(T)$;
- $\tau_n(h(T)) = 0$ if and only if h is a polynomial of degree $\leq n-1$.

By our description of $f(T)$ we have that there exists a polynomial $P(T)$ of degree at most $n-1$ and $U(T) \in \Lambda_{\mathcal{O}_F}^\times$ such that

$$f(T) = \pi P(T) + T^n U(T). \tag{2.1}$$

Now we set

$$q(T) := \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j \pi^j \Big(\tau_n \circ \frac{P}{U}\Big)^j \circ \tau_n(g(T)).$$

This definition is quite difficult to interpret, so for example one has

$$\left(\tau_n \circ \frac{P(T)}{U(T)}\right)^3 \circ \tau_n(g(T)) = \tau_n\left(\frac{P(T)}{U(T)}\tau_n\left(\frac{P(T)}{U(T)}\tau_n\left(\frac{P(T)}{U(T)}\tau_n(g(T))\right)\right)\right).$$

Note that the partial sums whose limit defines $q(T)$ is a Cauchy sequence, thanks to the term π^j. Since $\Lambda_{\mathcal{O}_F}$ is complete with respect to the (π, T)-adic topology, we have that $q(T)$ is a well defined power series in $\Lambda_{\mathcal{O}_F}$. Using equation (2.1) we have that

$$qf = q(\pi P + T^n U) = \pi q P + T^n q U.$$

Applying τ_n we obtain

$$\tau_n(qf) = \pi\tau_n(qP) + \tau_n(T^n qU) = \pi\tau_n(qP) + qU.$$

But

$$\begin{aligned}
\pi\tau_n(qP) &= \pi\tau_n\left(\frac{P}{U}\sum_{j=0}^{\infty}(-1)^j\pi^j\left(\tau_n \circ \frac{P}{U}\right)^j \circ \tau_n(g)\right) = \\
&= \sum_{j=0}^{\infty}(-1)^j\pi^{j+1}\left(\tau_n \circ \frac{P}{U}\right)^{j+1} \circ \tau_n(g) = \\
&= \pi\left(\tau_n \circ \frac{P}{U}\right) \circ \tau_n(g) - \pi^2\left(\tau_n \circ \frac{P}{U}\right)^2 \circ \tau_n(g) + \cdots = \\
&= \tau_n(g) - \left(\tau_n(g) - \pi\left(\tau_n \circ \frac{P}{U}\right) \circ \tau_n(g) + \pi^2\left(\tau_n \circ \frac{P}{U}\right)^2 \circ \tau_n(g) - \dots\right) = \\
&= \tau_n(g) - Uq.
\end{aligned}$$

Therefore we have that

$$\tau_n(qf) = \tau_n(g),$$

hence qf and g differ only by a polynomial of degree less then n.

To see uniqueness, suppose there exist $q_1, q_2, r_1, r_2 \in \Lambda_{\mathcal{O}_F}$ with the property that $g = q_1 f + r_1 = q_2 f + r_2$. Thus we have that $(q_1 - q_2)f + (r_1 - r_2) = 0$. If $q_1 \neq q_2$ and $r_1 \neq r_2$, we may assume that π doesn't divide $(q_1 - q_2)$ or $(r_1 - r_2)$. Reducing modulo $\mathfrak{p}$ we have that $r_1 \equiv r_2 \pmod{\pi}$ since $a_i \in \mathfrak{p}$ for $1 \leq i \leq n-1$. Thus π divides $(q_1 - q_2)f$. But we know that π doesn't divide f since $a_n \in \mathcal{O}_F^\times$. Hence we must have that π divides $(q_1 - q_2)$, a contradiction. □

Definition. A polynomial $P(T) \in \mathcal{O}_F[T]$ is called *distinguished* if $P(T) = a_0 + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n$ with $a_i \in \mathfrak{p}$ for every $0 \leq i \leq n-1$.

Theorem 2.1.3 (p-adic Weierstrass Preparation Theorem)**.** *Let*

$$f(T) = \sum_{i=0}^{\infty} a_i T^i \in \Lambda_{\mathcal{O}_F},$$

and assume that for some $n \in \mathbb{N}$ we have $a_i \in \mathfrak{p}$ for every $1 \leq i \leq n-1$ while $a_n \in \mathcal{O}_F^\times$. Then f can be uniquely written in the form

$$f(T) = P(T)U(T)$$

with $U(T) \in \Lambda_{\mathcal{O}_F}^\times$ and $P(T)$ is a distinguished polynomial of degree n. More generally, if $f(T) \in \Lambda_{\mathcal{O}_F}$ is nonzero, then we may uniquely write

$$f(T) = \pi^\mu P(T)U(T)$$

with P and U as above and $\mu \in \mathbb{Z}_{\geq 0}$.

Proof. We begin by applying Proposition 2.1.2 to $g(T) = T^n$ and $f(T)$ to obtain $q(T) = \sum_{i=0}^{\infty} q_i T^i \in \Lambda_{\mathcal{O}_F}$ and $r(T) \in \mathcal{O}_F[T]$ with $\deg r(T) \leq n-1$ such that

$$T^n = f(T)q(T) + r(T).$$

If we reduce the equation modulo π we see that

$$T^n \equiv (a_n T^n + a_{n+1}T^{n+1} + \dots)q(T) + r(T) \pmod{\pi}. \tag{2.2}$$

Since $\deg r(T) \leq n-1$, we must have $r(T) \equiv 0 \pmod{\pi}$, thus $T^n - r(T)$ is a distinguished polynomial of degree n, call it $P(T)$. Looking at the coefficient of T^n in equation (2.2) we have $q_0 a_n \equiv 1 \pmod{\pi}$. Thus π doesn't divide q_0, which implies that $q_0 \in \mathcal{O}_F^\times$, i.e. $q(T) \in \Lambda_{\mathcal{O}_F}^\times$ by Lemma 2.1.1. So we have that

$$f(T) = P(T)U(T)$$

with $U(T) = q(T)^{-1}$.

The uniqueness of the decomposition descends from the uniqueness in the statement of Proposition 2.1.2 and the last statement is clear when factoring out from $f(T)$ the largest power of π possible. □

Lemma 2.1.4. *Let $P(T), g(T) \in \mathcal{O}_F[T]$ with $P(T)$ distinguished. If we have $\frac{g(T)}{P(T)} \in \Lambda_{\mathcal{O}_F}$ then $\frac{g(T)}{P(T)} \in \mathcal{O}_F[T]$.*

Proof. Let $f(T) \in \Lambda_{\mathcal{O}_F}$ so that $\frac{g(T)}{P(T)} = f(T)$, i.e. $g(T) = f(T)P(T)$. Let $z \in \bar{\mathbb{Q}}_p$ be a root of $P(T)$. Call $w_\mathfrak{p}$ the unique extension to $\bar{\mathbb{Q}}_p$ of the valuation $v_\mathfrak{p}$ on F. Then

$$0 = P(z) = z^n + (\text{multiple of } \pi)$$

since $P(T)$ is distinguished. Then π divides z^n, hence $w_\mathfrak{p}(z) > 0$. Thus we have that the series $f(T)$ converges at z and so $g(z) = 0$, i.e. $(T-z)|g(T)$. Since z is a generic root of $P(T)$, we see that $P(T)|g(T)$ as polynomials. □

2.2 The structure of $\Lambda_{\mathcal{O}_F}$-modules

In the previous section we proved that $\Lambda_{\mathcal{O}_F}$ is a UFD whose irreducibles are π and irreducible distinguished polynomials. The units are elements in $\Lambda_{\mathcal{O}_F}$ whose constant term is in $\mathcal{O}_F^\times$. In this section we study the structure of the ideals of $\Lambda_{\mathcal{O}_F}$ with the purpose of stating a theorem about the structure of finitely generated $\Lambda_{\mathcal{O}_F}$-modules. Our final goal is to define some invariants associated to these $\Lambda_{\mathcal{O}_F}$-modules.

Lemma 2.2.1. *Let $f, g \in \Lambda_{\mathcal{O}_F}$ be relatively prime. The ideal (f, g) generated by f and g has finite index in $\Lambda_{\mathcal{O}_F}$.*

Proof. Let $h \in (f, g)$ have minimal degree in (f, g). By Weierstrass preparation theorem we can assume that $h(T) = \pi^n H(T)$ for some integer n and where $H = 1$ or H is a distinguished polynomial. If $H \neq 1$ we can write $f = qH + r$ with $\deg r < \deg H$. This gives us

$$\pi^n f = q\pi^n H + \pi^n r = qh + \pi^n r.$$

This shows that $\pi^n r \in (f, g)$ and has smaller degree then h, a contradiction. Hence we must have $H = 1$ and $h = \pi^n$. Without loss of generality we may assume that π doesn't divide f, for if it does divide f we can use g instead, since f and g are relatively coprime. By Weierstrass preparation theorem we also may assume that f is distinguished. We hence have that $(\pi^n, f) \subseteq (f, g)$ and so $\Lambda_{\mathcal{O}_F}/(\pi^n, f) \supseteq \Lambda_{\mathcal{O}_F}/(f, g)$. The division algorithm in Proposition 2.1.2 shows that everything in $\Lambda_{\mathcal{O}_F}$ is congruent modulo (π^n, f) to a polynomial of degree less than the degree of f with coefficients modulo π^n. Since there are only finitely many choices for such polynomials we can conclude that (π^n, f) has finite index, hence the same holds for (f, g). □

Lemma 2.2.2. *Let $f, g \in \Lambda_{\mathcal{O}_F}$ be relatively prime. Then:*

(a) The natural morphism

$$\begin{aligned} &\Lambda_{\mathcal{O}_F}/(fg) \longrightarrow \Lambda_{\mathcal{O}_F}/(f) \oplus \Lambda_{\mathcal{O}_F}/(g) \\ &h \pmod{(fg)} \longmapsto \Big(h \pmod{(f)},\ h \pmod{(g)}\Big) \end{aligned}$$

is an injection with finite cokernel.

(b) There is an injective morphism

$$\Lambda_{\mathcal{O}_F}/(f) \oplus \Lambda_{\mathcal{O}_F}/(g) \longrightarrow \Lambda_{\mathcal{O}_F}/(fg)$$

with finite cokernel.

Proof. (a) The fact that the map is an injection follows immediately from the fact that $\Lambda_{\mathcal{O}_F}$ is a UFD. In order to show that it has finite cokernel, consider $(a \pmod f, b \pmod g) \in \Lambda_{\mathcal{O}_F}/(f) \oplus \Lambda_{\mathcal{O}_F}/(g)$ and suppose that $a - b \in (f, g)$. Then there exist $\alpha, \beta \in \Lambda_{\mathcal{O}_F}$ such that $a - b = \alpha f + \beta g$. Set $\gamma = a - \alpha f = b + g\beta$ and observe that $\gamma \equiv a \pmod f$ and $\gamma \equiv b \pmod g$, hence $(a \pmod f, b \pmod g) = (\gamma \pmod f, \gamma \pmod g)$ lies in the image of the map. This means that the elements of the cokernel are less or equal than the elements of the coset of (f, g) in $\Lambda_{\mathcal{O}_F}$, which is finite by Lemma 2.2.1.

(b) Set $M \coloneqq \Lambda_{\mathcal{O}_F}/(fg)$ and $N = \Lambda_{\mathcal{O}_F}/(f) \oplus \Lambda_{\mathcal{O}_F}/(g)$. From the point (a) we know that M is of finite index in N. Let P be a distinguished polynomial in $\Lambda_{\mathcal{O}_F}$ that is relatively prime to fg. Note that in $\Lambda_{\mathcal{O}_F}$, endowed with the (π, T)-adic topology, we have that $P^k \to 0$ for $k \to \infty$, and since $\bigcap_{i=0}^{\infty} (\pi, T)^i = 0$ we have that $P^k N \subseteq M$ for some k. Suppose that $(P^k x, P^k y) = 0$ in N for some $(x, y) \in N$. We must have that $f | P^k x$ and $g | P^k y$, and since P and fg are relatively prime, we have that $f | x$ and $g | y$, thus $(x, y) = 0$ in N. Hence the morphism

$$\begin{aligned} P^k : N &\longrightarrow M \\ (x, y) &\longmapsto P^k \cdot (x, y) \end{aligned}$$

is injective. The ideal $(P^k \cdot (1,1), P^k \cdot (0,0)) = (P^k, fg)$ of M is contained in the image of this map. This ideal is of finite index in $\Lambda_{\mathcal{O}_F}$ by Lemma 2.2.1, so the cokernel of the injection is finite. □

Now we determine the prime ideals of $\Lambda_{\mathcal{O}_F}$ and we show that $\Lambda_{\mathcal{O}_F}$ has a unique maximal ideal.

Proposition 2.2.3. *The prime ideals of $\Lambda_{\mathcal{O}_F}$ are $0, (\pi, T), (\pi)$ and the ideals $(P(T))$ for $P(T)$ irreducible and distinguished. The ideal (π, T) is the unique maximal ideal.*

Proof. It is easy to see that the given ideals are prime ideals, so we just have to prove that they are the only prime ideals. Let $\mathfrak{q} \neq 0$ be a prime ideal, let $h \in \mathfrak{q}$ be of minimal degree. By Weierstrass preparation theorem 2.1.3 we may choose $h = \pi^s H$ with $H = 1$ or H distinguished polynomial. Since $\mathfrak{q}$ is prime, we must have $\pi \in \mathfrak{q}$ or $H \in \mathfrak{q}$. If $H = 1$ we must have $\pi \in \mathfrak{q}$. If $H \neq 1$ and $H \in \mathfrak{q}$, then H must be irreducible by the minimality of the degree of h. Therefore in any case we have that $(f) \subseteq \mathfrak{q}$ where $f = \pi$ or f irreducible and distinguished. If $(f) = \mathfrak{q}$, then $\mathfrak{q}$ is in the above list and we are done. Suppose $(f) \neq \mathfrak{q}$: this means that there is a $g \in \mathfrak{q}$ coprime with f, since f is irreducible. By Lemma 2.2.1 we have that $\mathfrak{q}$ is of finite index in $\Lambda_{\mathcal{O}_F}$, hence $\Lambda_{\mathcal{O}_F}/\mathfrak{q}$ is a finite $\mathcal{O}_F$-module. This means that there exists an $N \in \mathbb{N}$ such that $\pi^N \in \mathfrak{q}$, hence $\pi \in \mathfrak{q}$ since $\mathfrak{q}$ is prime. Also, $T^i \equiv T^j \pmod{\mathfrak{q}}$ for some $i < j$. This means that $T^i(T^{j-i} - 1) \in \mathfrak{q}$. Since $T^{j-i} - 1$ is a unit, we must have $T^i \in \mathfrak{q}$, hence $T \in \mathfrak{q}$ since $\mathfrak{q}$ is prime. This means that $(\pi, T) \subseteq \mathfrak{q}$. However,

$\Lambda_{\mathcal{O}_F}/(\pi,T) \cong \mathcal{O}_F/\mathfrak{p}$ which is a field, hence (π,T) is maximal and $\mathfrak{q} = (\pi,T)$. Since every prime is contained in (π,T), this is the only maximal ideal. □

Lemma 2.2.4. *Let $f \in \Lambda_{\mathcal{O}_F} \setminus \Lambda_{\mathcal{O}_F}^{\times}$. Then $\Lambda_{\mathcal{O}_F}/(f)$ is infinite.*

Proof. We may assume $f \neq 0$. Since $\Lambda_{\mathcal{O}_F}$ is a UFD, (f) is contained in a principal ideal generated by an irreducible, hence we may assume $f = \pi$ or f distinguished. If $f = (\pi)$ then $\Lambda_{\mathcal{O}_F}/(f) \cong (\mathcal{O}_F/\mathfrak{p})[[T]]$, which is infinite. If f is distinguished, using the division algorithm we see that the cardinality of $\Lambda_{\mathcal{O}_F}/(f)$ is greater or equal than the cardinality of the set of polynomials in $\mathcal{O}_F[T]$ with degree less then $\deg f$, which is infinite. □

Lemma 2.2.5. *The ring $\Lambda_{\mathcal{O}_F}$ is a Nötherian ring.*

Proof. Since $\mathcal{O}_F$ is a Nötherian ring, then also $\mathcal{O}_F[[T]]$ is Nötherian (see [12, IV.9.4]). □

Definition. Two $\Lambda_{\mathcal{O}_F}$-modules M and N are said to be *pseudo-isomorphic*, written $M \sim N$, if there exists an exact sequence of $\Lambda_{\mathcal{O}_F}$-modules

$$0 \longrightarrow A \longrightarrow M \xrightarrow{\alpha} N \longrightarrow B \longrightarrow 0$$

with A and B finite, i.e. if there exists a morphism $\alpha : M \to N$ with finite kernel and cokernel.

Remark 2.2.6. Notice that in general $M \sim N$ does not imply $N \sim M$. For example we have that $(\pi,T) \sim \Lambda_{\mathcal{O}_F}$ but $\Lambda_{\mathcal{O}_F} \not\sim (\pi,T)$ (see [26, 13.2]). However it's true that for finitely generated $\Lambda_{\mathcal{O}_F}$-torsion $\Lambda_{\mathcal{O}_F}$-modules the relation $\sim$ is simmetric.

Remark 2.2.7. Lemma 2.2.2 tells us that if f and g are coprime then

$$\Lambda_{\mathcal{O}_F}/(fg) \sim \Lambda_{\mathcal{O}_F}/(f) \oplus \Lambda_{\mathcal{O}_F}/(g) \quad \text{and} \quad \Lambda_{\mathcal{O}_F}/(f) \oplus \Lambda_{\mathcal{O}_F}/(g) \sim \Lambda_{\mathcal{O}_F}/(fg).$$

We present now a structure theorem for finitely generated $\Lambda_{\mathcal{O}_F}$-modules.

Theorem 2.2.8. *Let M be a finitely generated $\Lambda_{\mathcal{O}_F}$-module. Then*

$$M \sim \Lambda_{\mathcal{O}_F}^r \oplus \left(\bigoplus_{i=1}^{s} \frac{\Lambda_{\mathcal{O}_F}}{(\pi^{n_i})} \right) \oplus \left(\bigoplus_{j=1}^{t} \frac{\Lambda_{\mathcal{O}_F}}{(f_j(T)^{m_j})} \right)$$

where $r, s, t, n_i, m_j \in \mathbb{Z}$ and f_j is distinguished and irreducible.

Proof. See [26, 13.12]. □

Definition. Let M be a finitely generated $\Lambda_{\mathcal{O}_F}$-module, so that it is pseudo-isomorphic to an *elementary* module as in Theorem 2.2.8. The polynomial

$$\operatorname{char}(M) := \pi^{n_1+\cdots+n_s} \prod_{j=1}^{t} f_j(T)^{m_j} \in \mathcal{O}_F[T]$$

is called the *characteristic polynomial of* M. We also call the ideal

$$\xi(M) := (\operatorname{char}(M)) \subseteq \Lambda_{\mathcal{O}_F}$$

the *characteristic ideal of* M. If M is pseudoisomorphic to a torsion-free elementary module, we set $\operatorname{char}(M) = 1$ and $\xi(M) = (1) = \Lambda$.

We are now going to prove that the characteristic ideal of a finitely generated $\Lambda_{\mathcal{O}_F}$-module is uniquely determined. We write the pseudo-isomorphism of Theorem 2.2.8 in a more compact way:

$$M \sim E := \Lambda_{\mathcal{O}_F}^r \oplus \left(\bigoplus_{i=1}^{n} \frac{\Lambda_{\mathcal{O}_F}}{f_i(T)^{m_i}} \right) \tag{2.3}$$

where f_i is either π or an irreducible distinguished polynomial, $r, n, m_i \in \mathbb{N}$.

Let $\mathfrak{q} = (f)$ be a height one prime ideal of $\Lambda_{\mathcal{O}_F}$, call $\Lambda_{\mathcal{O}_F,\mathfrak{q}}$ the localization of $\Lambda_{\mathcal{O}_F}$ at $\mathfrak{q}$.

Lemma 2.2.9. *Let M be a finitely generated $\Lambda_{\mathcal{O}_F}$-module pseudo-isomorphic to a module E as in equation (2.3). Then*

$$M \otimes_{\Lambda_{\mathcal{O}_F}} \Lambda_{\mathcal{O}_F,\mathfrak{q}} \cong \Lambda_{\mathcal{O}_F,\mathfrak{q}}^r \oplus \left(\bigoplus_{(f_i)=\mathfrak{q}} \frac{\Lambda_{\mathcal{O}_F,\mathfrak{q}}}{f_i^{m_i}\Lambda_{\mathcal{O}_F,\mathfrak{q}}} \right)$$

Proof. There is an exact sequence of $\Lambda_{\mathcal{O}_F}$-modules

$$0 \to A \to M \to E \to B \to 0$$

with A and B finite. Since localization preserves exact sequences (see [2, 3.3]), the sequence

$$0 \to A \otimes \Lambda_{\mathcal{O}_F,\mathfrak{q}} \to M \otimes \Lambda_{\mathcal{O}_F,\mathfrak{q}} \to E \otimes \Lambda_{\mathcal{O}_F,\mathfrak{q}} \to B \otimes \Lambda_{\mathcal{O}_F,\mathfrak{q}} \to 0$$

is exact. Let $g \in (\pi, T)$ with $g \notin \mathfrak{q}$. Since A is finite, $g^n A = 0$ for some $n > 0$. It follows that $A \otimes \Lambda_{\mathcal{O}_F,\mathfrak{q}} = 0$ since g^n is a unit in $\Lambda_{\mathcal{O}_F,\mathfrak{q}}$. Similarly, $B \otimes \Lambda_{\mathcal{O}_F,\mathfrak{q}} = 0$. If f is irreducible and $(f) \neq \mathfrak{q}$, then

$$f^m \frac{\Lambda_{\mathcal{O}_F}}{(f^m)} = 0.$$

Since f^m is a unit in $\Lambda_{\mathcal{O}_F,\mathfrak{q}}$, this implies that

$$\frac{\Lambda_{\mathcal{O}_F}}{(f^m)} \otimes_{\Lambda_{\mathcal{O}_F}} \Lambda_{\mathcal{O}_F,\mathfrak{q}} = 0.$$

This proves the lemma. □

Corollary 2.2.10. *Let M be a finitely generated $\Lambda_{\mathcal{O}_F}$-module. Then* $\mathrm{char}(M)$ *and $\xi(M)$ are uniquely determined.*

Proof. If E and E' are two different modules written as in equation (2.3) such that $M \sim E$ and $M \sim E'$, the lemma implies that the free part of E and E' is the same. Also, since $\Lambda_{\mathcal{O}_F,\mathfrak{q}}$ is a PID, by the lemma and by the uniquenes part of the structure theorem for finitely generated modules over PIDs we conclude that also the torsion summands must be equal. Hence

$$E = \Lambda_{\mathcal{O}_F}^r \oplus \left(\bigoplus_{i=1}^{n} \frac{\Lambda_{\mathcal{O}_F}}{f_i(T)^{m_i}} \right), \quad E' = \Lambda_{\mathcal{O}_F}^r \oplus \left(\bigoplus_{i=1}^{n} \frac{\Lambda_{\mathcal{O}_F}}{g_i(T)^{m_i}} \right)$$

with f_i and g_i differing by a unit, therefore the ideal generated by $\prod f_i^{m_i}$ is equal to the ideal generated by $\prod g_i^{m_i}$ Also, if we require the f_i's and g_i's to be irreducible and distinguished, we must have also the equality between characteristic polynomials. □

Corollary 2.2.11. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of finitely generated Λ-modules. Then*

$$\mathrm{char}(M_2) = \mathrm{char}(M_1) \cdot \mathrm{char}(M_3)$$

Proof. This follows from the lemma and the corresponding result for modules over PIDs. □

2.3 Pontryagin duality

In this section we state some general results about Pontryagin duality of abelian groups and modules. This material will be used in the sequel mainly in the particular case of Λ-modules.

Definition. Let A be a locally compact Hausdorff topological abelian group. The *Pontryagin dual* of A is defined to be the topological group

$$A' := \mathrm{Hom}_{cont}(A, \mathbb{R}/\mathbb{Z})$$

with a topology whose basis of open sets is composed by the sets of the form

$$\mathscr{B}(K,U) = \{ f \in A' \ : \ f(K) \subseteq U \}$$

where $K \subseteq A$ is compact and $U \subseteq \mathbb{R}/\mathbb{Z}$ is open for the usual topology in $\mathbb{R}/\mathbb{Z}$.

Proposition 2.3.1. *If A is a discrete topological abelian group, then A' is a compact Hausdorff topological abelian group.*

Proof. Since A is discrete, $K \subseteq A$ is compact if and only if K is a finite set. This means that a basis' open set of A' is of the type

$$\mathscr{B}(a_1, \dots, a_r, U) = \{ f \in A' \,:\, f(a_i) \subseteq U \text{ for every } i = 1, \dots, r \},$$

i.e. the topology on A' is the one induced by the product topology on the set of functions $(\mathbb{R}/\mathbb{Z})^A$, with $A' \subset (\mathbb{R}/\mathbb{Z})^A$ in the natural way. Thanks to Tychonov theorem we have that $(\mathbb{R}/\mathbb{Z})^A$ is a compact space with respect to the product topology, and it is not difficult to show that A' is a closed subset of $(\mathbb{R}/\mathbb{Z})^A$, hence A' is compact. □

Theorem 2.3.2. *Let A be a locally compact Hausdorff abelian group. Then there is a canonical isomorphism between A and A''.*

Proof. See [16, 4]. □

If A is a torsion locally compact Hausdorff topological abelian group, then $A' = \mathrm{Hom}_{cont}(A, \mathbb{Q}/\mathbb{Z})$, whereas if A is pro-p or discrete p-torsion, then $A' = \mathrm{Hom}_{cont}(A, \mathbb{Q}_p/\mathbb{Z}_p)$. If A is a discrete abelian group, then we have $A' = \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z})$.

If A has the additional structure of (left) Λ-module, then A' has a natural structure of (right) Λ-module defined as

$$(f\lambda)(a) := f(\lambda a)$$

for every $f \in A'$, $\lambda \in \Lambda$ and $a \in A$.

2.4 $\mathbb{Z}_p$-extensions

Let K be a number field. In this section we define and study $\mathbb{Z}_p$-extensions, giving also a standard construction of the cyclotomic $\mathbb{Z}_p$-extension of K. We also prove an important isomorphism theorem for Λ.

Definition. Let L/K be a Galois extension of fields, and let H be a closed subgroup of $\mathrm{Gal}(L/K)$. We denote by L^H the field of elements of L that are fixed by the action of H.

Definition. Given a number field K, a *$\mathbb{Z}_p$-extension of K* is a field extension K_∞/K such that $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$.

Remark 2.4.1. Notice that the group structure of $\mathrm{Gal}(K_\infty/K)$ is usually written multiplicatevely, while $\mathbb{Z}_p$ has additive group structure.

We begin with a construction for a $\mathbb{Z}_p$-extension of $\mathbb{Q}$ (remember that p is an odd prime). Call ζ_{p^n} a primitive p^n-th root of unity for $n \in \mathbb{N}$, and consider $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$. Recall that one has

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z}).$$

Call $\mathbb{Q}_n := \mathbb{Q}(\zeta_{p^{n+1}})^{(\mathbb{Z}/p\mathbb{Z})^\times}$ and $\mathbb{Q}_\infty := \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n$. From Galois theory we obtain that

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p,$$

hence $\mathbb{Q}_\infty/\mathbb{Q}$ is a $\mathbb{Z}_p$-extension, called the *cyclotomic $\mathbb{Z}_p$-extension* of $\mathbb{Q}$.

Let now K be a number field and set $K_\infty := K\mathbb{Q}_\infty$. Thus we obtain that $\mathrm{Gal}(K_\infty/K) \cong \mathrm{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty)$. This means that $\mathrm{Gal}(K_\infty/K)$ is isomorphic to a nonzero closed subgroup of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$, hence it is isomorphic to some $p^n\mathbb{Z}_p \cong \mathbb{Z}_p$. This means that K_∞/K is a $\mathbb{Z}_p$-extension, called the *cyclotomic $\mathbb{Z}_p$-extension* of K. For $K \neq \mathbb{Q}$ there are usually many $\mathbb{Z}_p$-extensions of K, but we will see that for $K = \mathbb{Q}$ the cyclotomic $\mathbb{Z}_p$-extension is the only $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Let now K_∞ be any $\mathbb{Z}_p$-extension of K. From Galois theory we know that we have a tower of fields

$$K = K_1 \subset K_2 \subset \cdots \subset K_n \subset \cdots \subset K_\infty \tag{2.4}$$

with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. The K_n's are the only subfields between K and K_∞, since the only closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$. Call $\Gamma := \mathrm{Gal}(K_\infty/K)$ and $\Gamma_n := \mathrm{Gal}(K_n/K) \cong \Gamma/\Gamma^{p^n}$. Consider the group rings $\mathbb{Z}_p[\Gamma_n]$. If $m \geq n \geq 0$ we have natural morphisms induced by the projections $\Gamma_m \to \Gamma_n$. So we can define the completed group ring $\mathbb{Z}_p[[\Gamma]] := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[\Gamma_n]$, endowing it with the topology induced by the product topology.

Proposition 2.4.2. *Let $\gamma \in \Gamma$ be a topological generator of Γ. Then*

$$\begin{aligned} \alpha : \mathbb{Z}_p[[\Gamma]] &\longrightarrow \Lambda = \mathbb{Z}_p[[T]] \\ \gamma &\longmapsto 1 + T \end{aligned}$$

is a topological isomorphism.

Proof. First notice that we have an isomorphism

$$\begin{aligned} \beta : \mathbb{Z}_p[\Gamma_n] &\longrightarrow \mathbb{Z}_p[T]/((1+T)^{p^n} - 1) \\ \gamma \pmod{\Gamma^{p^n}} &\mapsto 1 + T \pmod{((1+T)^{p^n} - 1)}, \end{aligned}$$

therefore it suffices to prove that we have a topological isomorphism

$$\mathbb{Z}_p[[T]] \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[T]/((1+T)^{p^n} - 1).$$

Set $P_n(T) := (1+T)^{p^n} - 1$. Since $P_0(T) \in (p, T)$ and

$$\frac{P_{n+1}(T)}{P_n(T)} = (1+T)^{p^n(p-1)} + (1+T)^{p^n(p-2)} + \cdots + 1 \in (p, T),$$

by induction we have that $P_n \in (p,T)^{n+1}$ for every $n \in \mathbb{N}$. Thanks to Proposition 2.1.2 we can associate to any power series $f(T) \in \mathbb{Z}_p[[T]]$ an element $f_n(T) \in \mathbb{Z}_p[T] \pmod{P_n(T)}$ with $\deg f_n < p^n$, such that

$$f(T) = q_n(T)P_n(T) + f_n(T).$$

If $m \geq n$, then

$$f_m(T) - f_n(T) = \Big(q_n - \frac{P_m}{P_n}q_m\Big)P_n.$$

By Lemma 2.1.4 $\Big(q_n - \frac{P_m}{P_n}q_m\Big) \in \mathbb{Z}_p[T]$, hence $f_m \equiv f_n \pmod{P_n}$ as polynomials. By performing manually the division, it can be seen that the map $f \mapsto f_n$ is continous. Therefore the universal property of the projective limit gives us a continous morphism from Λ to $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[T]/(P_n(T))$, defined as

$$f \longmapsto (f_0, f_1, \dots).$$

If $f_n = 0$ for every n, then P_n divides f for every n, therefore we obtain that $f \in \bigcap_{n=0}^{\infty}(p,T)^{n+1} = 0$, so the map is injective.

We now show that it is surjective. Set $\Delta := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[T]/(P_n(T))$. Since Λ is compact, its image in Δ is compact, hence closed as the natural topology in Δ is Hausdorff. Since the maps

$$\begin{aligned} \Lambda &\longrightarrow \mathbb{Z}_p[T]/(P_n(T)) \\ f &\longmapsto f_n \end{aligned}$$

are surjective, by the density criterion we have that the image of Λ is dense in Δ, hence it is equal to Δ. □

We now look at some ramification properties of $\mathbb{Z}_p$-extensions. For more information about the behaviour of valuations in algebraic extensions, see Appendix B.

Definition. Let L/K be a Galois extension of valued fields, fix a valuation v on K and a valuation w on L that lies above v. We say that the extension $(L,w)/(K,v)$ is *ramified* at v if the inertia group $I_w = I_w(L/K)$ is not trivial. If an extension is not ramified, it is called *unramified*.
If $I_w = \mathrm{Gal}(L/K)$, the extension is called *totally ramified*.
We say that v is *finitely decomposed* in L if the decomposition group G_w has finite index in $\mathrm{Gal}(L/K)$.
We say that v *splits completely* in L if $G_w = 0$.

The fact that a Galois extension is ramified at v does not depend on the extension w we choose, since all the extensions are conjugate. Hence we write $G_v := G_w$ and $I_v := I_w$.

Proposition 2.4.3. *Let K be a number field, K_∞/K a $\mathbb{Z}_p$-extension and v a valuation on K. If v does not lie above p, then K_∞/K is unramified at v.*

Proof. Let I_v be the inertia group of v and $\Gamma := \mathrm{Gal}(K_\infty/K)$. We know that the inertia group is a closed subgroup, so in this case I_v is either 0 or Γ^{p^n} for some $n \in \mathbb{N}$. If $I_v = 0$ we are done, hence assume that $I_v = \Gamma^{p^n}$. If v is an archimedean valuation, $|I_v| = 1$ or 2, but Γ^{p^n} is infinite. Let now v be an archimedean valuation. For each $m \in \mathbb{N}$ choose v_m to be a valuation that lies over v_{m-1}, setting $v_0 = v$. We can complete each field K_m at v_m and obtain a tower of completed fields

$$K_v \subseteq (K_1)_{v_1} \subseteq \ldots (K_m)_{v_m} \subseteq \ldots.$$

Set $\hat{K}_\infty := \bigcup_{m\geq 0}(K_m)_{v_m}$. Observe that I_v can be seen in $\mathrm{Gal}(\hat{K}_\infty/K_v)$ as the inertia subgroup of the extension $\hat{K}_\infty/K_v$ (see Proposition B.4.3). Let now $\mathcal{O}_{K_v}^\times$ be the units of the ring of v-adic integers of K_v. From local class field theory (see for example [26, Appendix 3.10]) we know that there exists a continous surjective morphism $\alpha : \mathcal{O}_{K_v}^\times \to I_v = \Gamma^{p^n}$. The local unit theorem (see [17, II.5.7]) gives that $\mathcal{O}_{K_v}^\times \cong (\text{finite group}) \times \mathbb{Z}_l^a$ for some $a \in \mathbb{Z}$ and some prime $l \in \mathbb{Z}$ with $v|l$. Since Γ^{p^n} has no torsion elements, the restriction of α to $\mathbb{Z}_l^a$ is still surjective. Composing with the natural projection, we obtain a continous surjective morphism

$$\mathbb{Z}_l^a \longrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p.$$

This would give a closed subgroup of index p in $\mathbb{Z}_l^a$, wich cannot happen since $l \neq p$. Thus $I_v = 0$. □

Proposition 2.4.4. *Let K be a number field, K_∞/K a $\mathbb{Z}_p$-extension. At least one valuation v of K ramifies in the extension K_∞/K and there is an $m \geq 0$ such that every prime that ramifies in K_∞/K_m is totally ramified.*

Proof. The maximal abelian unramified extension of K is a finite extension (see [4, 6.4]) and K_∞/K is infinite, hence at least one prime must ramify.

From the previous proposition we know that only the valuations lying over p can possibly ramify: call $v_1, \ldots, v_r$ the valuations of K that ramify in K_∞, and denote by $I_1, \ldots, I_r$ the corresponding inertia groups. Since each I_i is a nonzero closed subgroup of $\Gamma := \mathrm{Gal}(K_\infty/K)$, we have that there is some $m \in \mathbb{N}$ such that

$$\bigcap_{i=1}^{r} I_i = \Gamma^{p^m}.$$

Since $\mathrm{Gal}(K_\infty/K_m) = \Gamma^{p^m}$, it is contained in I_i for every $i = 1, \ldots, r$. Thus, v_i must be totally ramified in K_∞/K_m for every $i = 1, \ldots, r$. □

Remark 2.4.5. When $K = \mathbb{Q}$, it can be easily proved that the cyclotomic $\mathbb{Z}_p$-extension is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. To see this, one can use the Kronecker-Weber theorem which asserts that the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is generated by all the roots of unity. Propositions 2.4.3 and 2.4.4

imply that every $\mathbb{Z}_p$-extension of $\mathbb{Q}$ must be ramified only at p and therefore it is contained in $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_n \mathbb{Q}(\zeta_{p^n})$. By Galois theory, we conclude that the cyclotomic $\mathbb{Z}_p$-extension is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{p^\infty})$.

Lemma 2.4.6. *Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. Then every prime v that lies over p ramifies in K_∞.*

Proof. From the two previous propositions we have that p must ramify in $\mathbb{Q}_\infty$, hence it ramifies in $K\mathbb{Q}_\infty$. Call w an extension of p to $K\mathbb{Q}_\infty$ and call v the corresponding valuation on K (i.e. $v := w|_K$). From the previous proposition we have that the inertia group I_p of the extension $K\mathbb{Q}_\infty/\mathbb{Q}$ is infinite. Since $\mathrm{Gal}(K\mathbb{Q}_\infty/K)$ has finite index in $\mathrm{Gal}(K\mathbb{Q}_\infty/\mathbb{Q})$, we must have that the inertia group of the extension w/v is $I_v = \mathrm{Gal}(K\mathbb{Q}_\infty/K) \cap I_p \neq 0$. This means that v ramifies in $K_\infty := K\mathbb{Q}_\infty$. □

Lemma 2.4.7. *Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension. Then every nonarchimedean valuation v of K is finitely decomposed in K_∞.*

Proof. If v lies over p, there exists an $m \in \mathbb{N}$ such that any extension v_m of v to K_m is totally ramified in K_∞, hence v is finitely decomposed.

Let $K = \mathbb{Q}$ and consider $l \neq p$ a prime. Recall that the extension $\mathbb{Q}_n$ is built as the fixed field of $(\mathbb{Z}/p\mathbb{Z})^\times$ of the extension $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$ that has Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. The Frobenius of the prime l in $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ corresponds to the element $l \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. Therefore the prime l splits completely in $\mathbb{Q}_n$ if and only if $l \pmod{p^{n+1}}$ lies in $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e. if and only if $l^{p-1} \equiv 1 \pmod{p^{n+1}}$. This may clearly happen for a finite number of $n \in \mathbb{N}$, hence l does not split completely in $\mathbb{Q}_\infty$. This means that the decomposition group of l is nonzero, hence it has finite index in Γ and so l is finitely decomposed in $\mathbb{Q}_\infty$.

For $K \neq \mathbb{Q}$, just reason as in the proof of the above lemma with the decomposition group instead of the inertia group, remembering that every nontrivial subgroup of $\mathbb{Z}_p$ is of finite index in $\mathbb{Z}_p$. □

Chapter 3

The Selmer and Shafarevich-Tate Groups

The aim of this chapter is to give a detailed introduction to Selmer and Shafarevich-Tate groups for elliptic curves. We'll use some group cohomology (see Appendix A for the basics) and some algebraic number theory (see Appendix B). In this chapter we fix:

K	a number field;
v	a valuation on K;
$G_{\bar{K}/K}$	the Galois group of the extension $\bar{K}/K$;
E/K	an elliptic curve defined over K.

3.1 The Shafarevich-Tate group

Let E/K be an elliptic curve defined over a number field K. Fix a valuation v on K and consider an extension w of v to $\bar{K}$. Define K_v to be the completion of K with respect to v. Fix an embedding of $\bar{K}$ inside the algebraic closure of the completion of K, namely $\bar{K}_v$ (see Appendix B.4). Call G_w the decomposition group of the extension w over v, and recall that $G_w \cong \mathrm{Gal}(\bar{K}_v/K_v)$ (see Corollary B.4.6). Hence we have an action of G_w on $E(\bar{K}_v)$. Since all decomposition groups of extensions of v are conjugate, we write G_v instead of G_w.

Since G_v is a subgroup of $G_{\bar{K}/K}$ we have the natural restriction map in cohomology

$$\mathrm{Res} : H^1(G_{\bar{K}/K}, E(\bar{K})) \longrightarrow H^1(G_v, E(\bar{K})).$$

The embedding $\bar{K} \subseteq \bar{K}_v$ gives a natural map

$$\alpha : H^1(G_v, E(\bar{K})) \longrightarrow H^1(G_v, E(\bar{K}_v)).$$

We call Res_v the composition of $\alpha \circ \mathrm{Res}$.

Definition. Let E/K be an elliptic curve defined over a number field K. The *Shafarevich-Tate group of E over K* is the subgroup of $H^1(G_{\bar{K}/K}, E(\bar{K}))$ defined by

$$Ш_E(K) := \ker\left\{ \prod_v \mathrm{Res}_v : H^1(G_{\bar{K}/K}, E(\bar{K})) \to \prod_v H^1(G_v, E(\bar{K}_v)) \right\}$$

where v runs over all places of K.

3.2 The m-Selmer group

Definition. Let $(A, +)$ be an abelian group, $m \in \mathbb{N}$. We denote by $A[m]$ the group of m-torsion elements of A, i.e.

$$A[m] := \{\, a \in A \;:\; ma = 0 \,\}.$$

Let E/K be an elliptic curve defined over a number field K, $m \in \mathbb{Z}$ with $m \geq 2$. From the exact sequence related to the multiplication-by-m (see equation (1.3)), looking at $E(\bar{K})$ as a $G_{\bar{K}/K}$-module, we get the long exact sequence in cohomology (see Proposition A.1.5)

$$\begin{array}{l} 0 \longrightarrow E(K)[m] \xrightarrow{\ \iota\ } E(K) \xrightarrow{\ m\ } E(K) \xrightarrow{\ \delta\ } \\ \quad H^1(G_{\bar{K}/K}, E[m]) \xrightarrow{\ \iota_*\ } H^1(G_{\bar{K}/K}, E) \xrightarrow{\ m_*\ } H^1(G_{\bar{K}/K}, E) \end{array}$$

and from this we form the fundamental exact sequence

$$0 \to E(K)/mE(K) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, E(\bar{K})[m]) \xrightarrow{\iota_*} H^1(G_{\bar{K}/K}, E(\bar{K}))[m] \to 0.$$

Let now v be a place of K. Since K is naturally embedded inside K_v, we have that the elliptic curve E/K is also defined over K_v. Since we have that $G_v \cong \mathrm{Gal}(\bar{K}_v/K_v)$, repeating the above argument we obtain the exact sequence

$$0 \to E(K_v)/mE(K_v) \xrightarrow{\delta_v} H^1(G_v, E(\bar{K}_v)[m]) \xrightarrow{\iota_{v*}} H^1(G_v, E(\bar{K}_v))[m] \to 0.$$

Putting together the local and global exact sequences, we obtain the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \xrightarrow{\delta} & H^1(G_{\bar{K}/K}, E[m]) & \xrightarrow{\iota_*} & H^1(G_{\bar{K}/K}, E)[m] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \prod_v \mathrm{Res}_v} & & \downarrow{\scriptstyle \prod_v \mathrm{Res}_v} & & \\ 0 & \longrightarrow & \prod_v E(K_v)/mE(K_v) & \xrightarrow{\delta_v} & \prod_v H^1(G_v, E[m]) & \xrightarrow{\iota_{v*}} & \prod_v H^1(G_v, E)[m] & \longrightarrow & 0 \end{array} \tag{3.1}$$

where in the first row $E = E(\bar{K})$, in the second row $E = E(\bar{K}_v)$, in the products v runs over all places of K and θ is the natural map induced by the inclusion $E(K) \subseteq E(K_v)$.

Definition. Let E/K be an elliptic curve and let $m \geq 2$ be an integer. The *m-Selmer group of E/K over K* is the subgroup of $H^1(G_{\bar{K}/K}, E(\bar{K})[m])$ defined by

$$\mathrm{Sel}_E^{(m)}(K) := \ker\left\{ \prod_v \mathrm{Res}_v \circ \iota_* : H^1\big(G_{\bar{K}/K}, E(\bar{K})[m]\big) \to \prod_v H^1(G_v, E(\bar{K}_v)) \right\}$$

with v running over all places of K.

Lemma 3.2.1. *Let $m \geq 2$ be an integer. Then there is an exact sequence*

$$0 \longrightarrow E(K)/mE(K) \xrightarrow{\delta} \mathrm{Sel}_E^{(m)}(K) \xrightarrow{\iota_*} Ш_E(K)[m] \longrightarrow 0.$$

Proof. If we apply the snake lemma to the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \xrightarrow{\delta} & H^1(G_{\bar{K}/K}, E[m]) & \xrightarrow{\iota_*} & H^1(G_{\bar{K}/K}, E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \prod_v \mathrm{Res}_v \circ \iota_*} & & \downarrow{\scriptstyle \prod_v \mathrm{Res}_v} & & \\ 0 & \longrightarrow & 0 & \longrightarrow & \prod_v H^1(G_v, E)[m] & = & \prod_v H^1(G_v, E)[m] & \longrightarrow & 0, \end{array}$$

from the first half of the snake we obtain the claim. □

Theorem 3.2.2. *Let K be a number field. The m-Selmer group over K of an elliptic curve E/K is finite.*

Proof. See [22, X.4.2]. □

Corollary 3.2.3. *Let K be a number field. The groups $E(K)/mE(K)$ and $Ш_E(K)[m]$ are finite.*

From this corollary it follows that $E(K)/mE(K)$ is a finite group: this is the so called *weak Mordell-Weil theorem*. From this result it can be proved the so called *Mordell-Weil theorem*.

Theorem 3.2.4 (Mordell-Weil)**.** *Let E/K be an elliptic curve defined over a number field K. Then the group $E(K)$ is finitely generated.*

Proof. See [22, VIII]. □

Corollary 3.2.5. *We have an isomorphism of groups*

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$$

where $E(K)_{tors}$ is finite and r is a nonnegative integer.

3.3 The Selmer group

In this section we define the Selmer group of an elliptic curve by taking the direct limit of the m-Selmer groups defined in the previous section.

Lemma 3.3.1. *Let $(A,+)$ be an abelian group, $m \geq 2$ an integer. Then*

$$\frac{A}{mA} \cong A \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Proof. See [12, XVI.2.7]. □

Remark 3.3.2. Using Lemma 3.3.1 we see that

$$\frac{E(K)}{mE(K)} \cong E(K) \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{m\mathbb{Z}}$$

and

$$\frac{E(K_v)}{mE(K_v)} \cong E(K_v) \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

We now apply the exact functor $\varinjlim_m$ (exact since $\mathbb{N}$ is a filtered set) to the diagram (3.1). Using Remark 3.3.2, the fact that $\varinjlim_m \mathbb{Z}/m\mathbb{Z} = \mathbb{Q}/\mathbb{Z}$ and Proposition A.2.7 we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)\otimes_{\mathbb{Z}} \frac{\mathbb{Q}}{\mathbb{Z}} & \xrightarrow{\vec{\delta}} & H^1(G_{\bar{K}/K}, E_{tors}) & \xrightarrow{\vec{\iota_*}} & H^1(G_{\bar{K}/K}, E)_{tors} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \vec{\theta}} & & \downarrow{\scriptstyle \prod_v \vec{\mathrm{Res}}_v} & & \downarrow{\scriptstyle \prod_v \vec{\mathrm{Res}}_v} & & \\ 0 & \longrightarrow & \prod_v E(K_v)\otimes \frac{\mathbb{Q}}{\mathbb{Z}} & \xrightarrow{\vec{\delta_v}} & \prod_v H^1(G_v, E_{tors}) & \xrightarrow{\vec{\iota_{v*}}} & \prod_v H^1(G_v, E)_{tors} & \longrightarrow & 0 \end{array} \tag{3.2}$$

where in the first row $E = E(\bar{K})$, in the second row $E = E(\bar{K}_v)$ and in the products v runs over all places of K. The maps are the natural maps given applying the direct limit. This idea leads us to the next definition.

Definition. The *Selmer group of an elliptic curve E/K over K* is

$$\mathrm{Sel}_E(K) := \varinjlim_{m\in\mathbb{N}} \mathrm{Sel}_E^{(m)}(K)$$

where the direct limit is taken with respect to the restriction of the natural maps

$$\phi_{m_1,m_2} : H^1(G_{\bar{K}/K}, E(\bar{K})[m_1]) \longrightarrow H^1(G_{\bar{K}/K}, E(\bar{K})[m_2])$$

to the m_1 and m_2-Selmer groups, with $m_1 | m_2$.

Lemma 3.3.3. *We have that*

$$\mathrm{Sel}_E(K) = \ker\left\{ \prod_v \vec{\mathrm{Res}}_v \circ \vec{\iota_*} : H^1(G_{\bar{K}/K}, E(\bar{K})_{tors}) \to \prod_v H^1(G_v, E(\bar{K}_v)) \right\}.$$

Proof. If we call $A_m := H^1(G_{\bar{K}/K}, E(\bar{K})[m])$ and $B := \prod_v H^1(G_v, E(\bar{K}_v))$, the claim follows since

$$\varinjlim_m \ker(A_m \to B) = \ker(\varinjlim_m A_m \to B)$$

and

$$\varinjlim_m H^1(G_{\bar{K}/K}, E(\bar{K})[m]) = H^1(G_{\bar{K}/K}, \varinjlim_m E(\bar{K})[m])$$

by Proposition A.2.7. □

We're now going to generalize the exact sequence of Lemma 3.2.1 to the case of the Selmer group.

Proposition 3.3.4. *Let E/K be an elliptic curve defined over a number field K. There is an exact sequence*

$$0 \longrightarrow E(K) \otimes_{\mathbb{Z}} \frac{\mathbb{Q}}{\mathbb{Z}} \xrightarrow{\vec{\delta}} \mathrm{Sel}_E(K) \xrightarrow{\vec{\iota_*}} Ш_E(K)_{tors} \longrightarrow 0.$$

Proof. Apply the exact functor $\varinjlim_m$ to the exact sequence in Lemma 3.2.1. □

Remark 3.3.5. From some properties of homogeneous spaces it follows that the Shafarevich-Tate group is a torsion group, hence we can write $Ш_E(K)_{tors} = Ш_E(K)$ in Proposition 3.3.4. See [22, X.3] for more details.

3.4 The p-primary Selmer group

Let p be a prime. In this section we mimic the procedure of the preceeding section with $m = p^n$.

We apply the exact functor $\varinjlim_n$ to the diagram (3.1) with $m = p^n$. Using Remark 3.3.2, the fact that $\varinjlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p$ and Proposition A.2.7 we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K) \otimes_{\mathbb{Z}} \frac{\mathbb{Q}_p}{\mathbb{Z}_p} & \xrightarrow{\vec{\delta}} & H^1(G_{\bar{K}/K}, E[p^\infty]) & \xrightarrow{\vec{\iota_*}} & H^1(G_{\bar{K}/K}, E)[p^\infty] & \longrightarrow & 0 \\
 & & \downarrow \vec{\theta} & & \downarrow \prod_v \vec{\mathrm{Res}}_v & & \downarrow \prod_v \vec{\mathrm{Res}}_v & & \\
0 & \longrightarrow & \prod_v E(K_v) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} & \xrightarrow{\vec{\delta_v}} & \prod_v H^1(G_v, E[p^\infty]) & \xrightarrow{\vec{\iota_{v*}}} & \prod_v H^1(G_v, E)[p^\infty] & \longrightarrow & 0
\end{array} \tag{3.3}$$

where in the first row $E = E(\bar{K})$, in the second row $E = E(\bar{K}_v)$ and in the products v runs over all places of K. The maps are the natural maps that come out applying the direct limit.

Definition. Let p be a prime. The *p-primary Selmer group of E/K over K* is

$$\mathrm{Sel}_E(K)_p := \varinjlim_n \mathrm{Sel}_E^{(p^n)}(K),$$

where the direct limit is taken with respect to the restriction of the natural maps

$$\phi_n : H^1(G_{\bar{K}/K}, E(\bar{K})[p^n]) \longrightarrow H^1(G_{\bar{K}/K}, E(\bar{K})[p^{n+1}])$$

to the p^n and p^{n+1}-Selmer groups.

Lemma 3.4.1. *We have that*

$$\mathrm{Sel}_E(K)_p = \ker\left\{\prod_v \vec{\mathrm{Res}}_v \circ \vec{\iota_*} : H^1(G_{\bar{K}/K}, E(\bar{K})[p^\infty]) \to \prod_v H^1(G_v, E(\bar{K}_v))\right\}$$

Proof. If we call $A_n := H^1(G_{\bar{K}/K}, E(\bar{K})[p^n])$ and $B := \prod_v H^1(G_v, E(\bar{K}_v))$, the claim follows since

$$\varinjlim_n \ker(A_n \to B) = \ker(\varinjlim_n A_n \to B)$$

and

$$\varinjlim_n H^1(G_{\bar{K}/K}, E(\bar{K})[p^n]) = H^1(G_{\bar{K}/K}, \varinjlim_n E(\bar{K})[p^n])$$

by Proposition A.2.7. □

We're now going to generalize the exact sequence of Lemma 3.2.1 to the case of the p-primary Selmer group.

Proposition 3.4.2. *Let E/K be an elliptic curve defined over a number field K. There is an exact sequence*

$$0 \longrightarrow E(K) \otimes_{\mathbb{Z}} \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \xrightarrow{\vec{\delta}} \mathrm{Sel}_E(K)_p \xrightarrow{\vec{\iota_*}} Ш_E(K)[p^\infty] \longrightarrow 0.$$

Proof. Apply the exact functor $\varinjlim_n$ to the exact sequence in Lemma 3.2.1 with $m = p^n$. □

Chapter 4

p-adic L-functions of Elliptic Curves

We begin this chapter by introducing some notions that deal with the world of modular forms, in order to present the theory of modular symbols. Then we study some properties of p-adic measure theory. Our aim is to build a measure on $\mathbb{Z}_p^\times$ associated to a particular modular form. Then, integrating p-adic characters with respect to this measure, we define a p-adic L-function attached to some special modular forms and a p-adic L-series attached to an elliptic curve $E/\mathbb{Q}$ with good ordinary reduction at an odd prime p. This p-adic L-series is the so called "analytic ingredient" of the Iwasawa main conjecture. We will also study the relation of this p-adic L-series with the usual complex L-series attached to any elliptic curve $E/\mathbb{Q}$. This last results will help us to prove a special case of the Birch and Swinnerton-Dyer conjecture in Chapter 6. We fix some notation that will be used throughout this chapter:

p	an odd prime of $\mathbb{Z}$;
l	a prime of $\mathbb{Z}$;
N	an integer greater that 0;
$\mathscr{H}$	the upper half plane $\{z \in \mathbb{C} \,:\, \Im(z) > 0\}$;
ε	a Dirichlet character $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$;
$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$	an element of $\mathrm{GL}_2(\mathbb{Q})$;
v	the p-adic valuation on $\mathbb{Q}_p$ and $\mathbb{C}_p$.

4.1 Holomorphic cusp forms

In this section we present some basic definitions and results about holomorphic cusp forms.

Definition. Let $N > 0$ be an integer. We define three subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N},\ a \equiv d \equiv 1 \pmod{N} \right\},$$

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv b \equiv 0 \pmod{N},\ a \equiv d \equiv 1 \pmod{N} \right\}.$$

The group $\mathrm{GL}_2^+(\mathbb{Q})$ acts on $\mathscr{H}$ by Möbius transformations, i.e. for every $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$ and $z \in \mathscr{H}$ the action of γ on z is defined as

$$\gamma(z) := \frac{az + b}{cz + d}.$$

It's easy to see that it is a well defined left action.

Let k be a nonnegative integer. The group $\mathrm{GL}_2^+(\mathbb{Q})$ acts also on holomorphic functions $f : \mathscr{H} \to \mathbb{C}$ in this way:

$$(f|_k\gamma)(z) := \frac{\det(\gamma)^{k-1} f(\gamma(z))}{(cz + d)^k} \tag{4.1}$$

for every $z \in \mathscr{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$. It can be proven that it is a well defined right action (see [6, 1.2]).

We also have an action of $\mathrm{GL}_2(\mathbb{Q})$ on $\mathbb{P}^1(\mathbb{Q})$, which is defined as

$$\gamma(r) := \frac{ar + b}{cr + d}$$

if $r \in \mathbb{Q}$ and $\gamma(\infty) := \frac{a}{c}$, with the convention that $\frac{e}{0} = \infty$ for every element $e \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0\}$. It's easy to see that it is a well defined left action.

Definition. Let $k \in \mathbb{Z}_{\geq 0}$ and $\mathrm{SL}_2(\mathbb{Z}) \supseteq \Gamma \supseteq \Gamma(N)$ for some $N > 0$. A *cusp form of weight k and level Γ* is a holomorphic function $f : \mathscr{H} \to \mathbb{C}$ such that:

1. $f|_k\gamma = f$ for every $\gamma \in \Gamma$.
2. For every $\delta \in \mathrm{SL}_2(\mathbb{Z})$ we have $(f|_k\delta)(z) = \sum_{n \geq 1} a_\delta(n) e^{\frac{2\pi i n z}{M}}$ for some integer $M \geq 1$ and some $a_\delta(n) \in \mathbb{C}$.

The group Γ is called *congruence group*. The set of all cusp forms of weight k and level Γ is denoted by $\mathcal{S}_k(\Gamma)$.

The set $\mathcal{S}_k(\Gamma)$ has a natural structure of finitely dimensional $\mathbb{C}$-vector space. If $\Gamma \supseteq \Gamma_1(N)$, the action of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ shows that every cusp form f in $\mathcal{S}_k(\Gamma)$ satisfies $f(z+1) = f(z)$ for every $z \in \mathscr{H}$. Hence in this case we have a Fourier series for f of the type

$$f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z} \tag{4.2}$$

with $a_n \in \mathbb{C}$.

Lemma 4.1.1. *We have an isomorphism*

$$\begin{aligned} \alpha : \Gamma_0(N)/\Gamma_1(N) &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto d \pmod N. \end{aligned}$$

Proof. Since $ad - bc = 1$ and $c \equiv 0 \pmod N$ we have that $(N, d) = 1$. From a straightforword computation it comes out that α is a well defined homomorphism. The kernel is $\Gamma_1(N)$ since $d \equiv 1 \pmod N$, $c \equiv 0 \pmod N$ and $ad - bc = 1$ imply that $a \equiv 1 \pmod N$. The surjectivity is trivial. □

Using this lemma we can see any Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$ as a character of $\Gamma_0(N)$ that contains $\Gamma_1(N)$ inside its kernel. Note also that the action of $\Gamma_0(N)$ on $\mathcal{S}_k(\Gamma_1(N))$, defined as in (4.1), is well defined. This is because it is a particular case of a *double coset action* (see [6, 5.1-5.2] for details).

Definition. Let $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$ be a Dirichlet character. We define $\mathcal{S}_k(\Gamma_1(N), \varepsilon)$ to be the $\mathbb{C}$-subspace of $\mathcal{S}_k(\Gamma_1(N))$ of functions f that satisfy

$$f|_k \gamma = \varepsilon(\gamma) f(z)$$

for any $\gamma \in \Gamma_0(N)$.

Lemma 4.1.2. *There is a decomposition*

$$\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\varepsilon} \mathcal{S}_k(\Gamma_1(N), \varepsilon)$$

where ε runs over the Dirichlet characters of $(\mathbb{Z}/N\mathbb{Z})^\times$.

Proof. The action of $\Gamma_0(N)$ on $\mathcal{S}_k(\Gamma_1(N))$ induces a well defined action of the finite abelian group $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. From a standard fact of linear algebra we can find a basis $f_1, \ldots, f_n$ of $\mathcal{S}_k(\Gamma_1(N))$ of eigenvectors for the action of every element of $(\mathbb{Z}/N\mathbb{Z})^\times$. The system of eigenvalues of the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on a fixed f_i defines a Dirichlet character, i.e. every f_i has the property that $f_{i|_k} \gamma = \varepsilon_i(\gamma) f_i$ for every $\gamma \in \Gamma_0(N)$ and some Dirichlet character ε_i of $(\mathbb{Z}/N\mathbb{Z})^\times$. □

Definition. We define the space of all cusp forms of weight k and level $\Gamma_1(N)$ for some N

$$\mathcal{S}_k(\Gamma_1) := \sum_N \mathcal{S}_k(\Gamma_1(N)).$$

4.2 Modular symbols

From now on we focus on cusp forms of weight 2. For the sake of simplicity, we change notation and write $f|\gamma$ instead of $f|_2\gamma$ for the action of $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ on $f \in \mathcal{S}_2(\Gamma_1(N))$. In this section we study modular symbols, mainly following [14] and [8].

Definition. Let $\mathscr{D}_0 := \mathrm{Div}^0(\mathbb{P}^1(\mathbb{Q}))$ denote the group of divisors of degree 0 supported on $\mathbb{P}^1(\mathbb{Q})$ and let Γ be a congruence group. An additive morphism

$$\lambda : \mathscr{D}_0 \longrightarrow \mathbb{C}$$

is called a *modular symbol* over Γ if $\lambda(\gamma D) = \lambda(D)$ for every $D \in \mathscr{D}_0$ and $\gamma \in \Gamma$. The $\mathbb{C}$-vector space of modular symbols over Γ will be denoted by $\mathrm{Symb}_\Gamma(\mathbb{C})$.

The group $\mathrm{GL}_2(\mathbb{Q})$ acts on $\mathrm{Symb}_\Gamma(\mathbb{C})$ by the formula

$$\lambda|\gamma : D \longmapsto \lambda(\gamma D)$$

for every $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ and $D \in \mathscr{D}_0$. The matrix $\iota := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ induces an involution $\lambda \mapsto \lambda|\iota$ on $\mathrm{Symb}_\Gamma(\mathbb{C})$, hence we can decompose any modular symbol λ in a unique way as a sum

$$\lambda = \lambda^+ + \lambda^- \tag{4.3}$$

with $\lambda^+|\iota = \lambda^+$ and $\lambda^-|\iota = -\lambda^-$. It can be easily verified that

$$\lambda^+(\{c_2\} - \{c_1\}) = \frac{\lambda(\{c_2\} - \{c_1\}) + \lambda(\{-c_2\} - \{-c_1\})}{2}$$
$$\lambda^-(\{c_2\} - \{c_1\}) = \frac{\lambda(\{c_2\} - \{c_1\}) - \lambda(\{-c_2\} - \{-c_1\})}{2}$$

for every $c_1, c_2 \in \mathbb{P}^1(\mathbb{Q})$.

Definition. Let $f \in \mathcal{S}_2(\Gamma_1(N))$ and $c_1, c_2 \in \mathbb{P}^1(\mathbb{Q})$. The *standard modular symbol* $\lambda_f \in \mathrm{Symb}_{\Gamma_1(N)}(\mathbb{C})$ associated to f is defined on divisors of type $\{c_2\} - \{c_1\} \in \mathscr{D}_0$ by

$$\lambda_f(\{c_2\} - \{c_1\}) := 2\pi i \int_{c_1}^{c_2} f(z)dz,$$

where the integral is meant to be taken on the geodesic of $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ with respect to the metric $\frac{dx^2+dy^2}{y^2}$. For more details see [15, Chapter 1].

Lemma 4.2.1. *Let $f \in \mathcal{S}_2(\Gamma_1)$ and $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$. Then*

(a) λ_f is $\mathbb{C}$-linear in f.

(b) $\lambda_{f|\gamma} = \lambda_f|\gamma$.

Proof. (a) Clear from the definition of λ_f.
(b) Since for every $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ we have that $dz = \frac{(cz+d)^2 d(\gamma(z))}{\det(\gamma)}$, we obtain the relation

$$(f|\gamma)(z)dz = f(\gamma(z))d(\gamma(z)).$$

This implies that for every $c_1, c_2 \in \mathbb{P}^1(\mathbb{Q})$ we have that

$$\begin{aligned}\lambda_{f|\gamma}(\{c_2\} - \{c_1\}) &= 2\pi i \int_{c_1}^{c_2} (f|\gamma)(z)dz = 2\pi i \int_{c_1}^{c_2} f(\gamma(z))d(\gamma(z)) \overset{y=\gamma(z)}{=} \\ &= 2\pi i \int_{\gamma(c_1)}^{\gamma(c_2)} f(y)dy = \lambda_f(\{\gamma(c_2)\} - \{\gamma(c_1)\}).\end{aligned}$$

□

4.3 Hecke operators

In this section we present the main properties of the action of Hecke operators on $\mathcal{S}_2(\Gamma_1(N))$. In order to have more details one can see [6, 5.1-5.2]. Here l will denote a prime of $\mathbb{Z}$.

Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and consider the left action of $\Gamma_1(N)$ on the double coset $\Gamma_1(N)\alpha\Gamma_1(N)$ defined as

$$\gamma \cdot \gamma_1\alpha\gamma_2 := (\gamma\gamma_1)\alpha\gamma_2$$

for any $\gamma, \gamma_1, \gamma_2 \in \Gamma_1(N)$. The orbit space is a finite disjoint union

$$\Gamma_1(N)\backslash\Gamma_1(N)\alpha\Gamma_1(N) = \bigsqcup_{j\in J} \Gamma_1(N)\beta_j$$

with $\beta_j \in \Gamma_1(N)\alpha\Gamma_1(N)$ representatives for each orbit.

Definition. Let $\alpha_l := \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}$. The l-th Hecke operator on $\mathcal{S}_2(\Gamma_1(N))$ is

$$\begin{aligned} T_l : \mathcal{S}_2(\Gamma_1(N)) &\longrightarrow \mathcal{S}_2(\Gamma_1(N)) \\ f &\longmapsto f|T_l := \sum_{j\in J} f|\beta_j \end{aligned}$$

where $\{\beta_j\}_{j\in J}$ are orbit representatives for the left action of $\Gamma_1(N)$ on $\Gamma_1(N)\alpha_l\Gamma_1(N)$ defined above.

It can be proven that it is a well defined right action on $\mathcal{S}_2(\Gamma_1(N))$. By a long but straight computation of the β_j it can be proven the next proposition.

Proposition 4.3.1. *For any $f \in \mathcal{S}_2(\Gamma_1(N))$ we have*

$$f|T_l = \begin{cases} \sum_{j=0}^{l-1} f\left|\begin{pmatrix} 1 & j \\ 0 & l \end{pmatrix}\right. & \text{if } l \mid N \\ \sum_{j=0}^{l-1} f\left|\begin{pmatrix} 1 & j \\ 0 & l \end{pmatrix}\right. + f\left|\begin{pmatrix} m & n \\ N & l \end{pmatrix}\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}\right. & \text{if } l \nmid N \end{cases}$$

where $ml - nN = 1$.

Proof. See [6, 5.2.1]. □

Let now $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$ be a Diriclet character. It can be extended to every $x \in \mathbb{Z}$ by $\varepsilon(x) := 0$ if $(x, N) \neq 1$ and $\varepsilon(x) := \varepsilon(x \pmod N)$ if $(x, N) = 1$. We have the following important corollary,

Corollary 4.3.2. *Let ε be a Dirichlet character on $(\mathbb{Z}/N\mathbb{Z})^\times$ and consider $f \in \mathcal{S}_2(\Gamma_1(N), \varepsilon)$. Then*

$$f|T_l = \sum_{j=0}^{l-1} f\left|\begin{pmatrix} 1 & j \\ 0 & l \end{pmatrix}\right. + \varepsilon(l) f\left|\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}\right..$$

The actions of T_l and $\Gamma_0(N)$ on $\mathcal{S}_2(\Gamma_1(N))$ commute (see [6, 5.2.4]), therefore the operator T_l preserves $\mathcal{S}_2(\Gamma_1(N), \varepsilon)$ for every prime l.

Proposition 4.3.3. *For every $f \in \mathcal{S}_2(\Gamma_1(N), \varepsilon)$ and $a, m \in \mathbb{Q}$ we have that*

$$\lambda_{f|T_l}\Big(\Big\{\frac{a}{m}\Big\} - \{i\infty\}\Big) = \sum_{j=0}^{l-1} \lambda_f\Big(\Big\{\frac{a+jm}{lm}\Big\} - \{i\infty\}\Big) + \varepsilon(l)\lambda_f\Big(\Big\{\frac{al}{m}\Big\} - \{i\infty\}\Big).$$

Proof. The proof is straightforword using Lemma 4.2.1 and Corollary 4.3.2. □

Definition. A *Hecke eigenform* is a cusp form $f \in \mathcal{S}_2(\Gamma_1(N))$ that is an eigenform for the action of T_l for any prime l. A Hecke eigenform is called *normalized* if the first Fourier coefficient a_1 of f is equal to 1.

Proposition 4.3.4. *Let $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z}$ be a normalized Hecke eigenform, call λ_l the eigenvalue of f for T_l. Then $a_l = \lambda_l$.*

Proof. See [6, 5.8]. □

Theorem 4.3.5. *Let $f \in \mathcal{S}_2(\Gamma_1(N), \varepsilon)$ be a normalized Hecke eigenform, call $K(f)$ the extension of $\mathbb{Q}$ made by adjoining every Fourier coefficient of f. Then $K(f)$ is a finite extension of $\mathbb{Q}$.*

Proof. See [6, 6.5]. □

4.4 L-functions

In this section we define the L-function associated to a cusp form and see that it can be holomorfically extended to the whole $\mathbb{C}$. In conclusion, we look at its connection to modular symbols.

Definition. Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in \mathcal{S}_2(\Gamma_1(N))$. The *$L$-function of f* is the formal series

$$L(f,s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Proposition 4.4.1. *Let $f \in \mathcal{S}_2(\Gamma_1(N))$. The sum that defines $L(s,f)$ converges absolutely for all $s \in \mathbb{C}$ such that $\Re(s) > 2$.*

Proof. See [6, 5.9.1]. □

Theorem 4.4.2. *Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in \mathcal{S}_2(\Gamma_1(N), \varepsilon)$ be a normalized Hecke eigenform. Then*

$$L(s,f) = \prod_p (1 - a_p p^{-s} + \varepsilon(p) p^{1-2s})^{-1}$$

where the product is taken over all primes.

Proof. See [6, 5.9.2]. □

Definition. The *Λ-function* associated to a cusp form $f \in \mathcal{S}_2(\Gamma_1(N))$ is

$$\Lambda(E,s) := (2\pi)^{-s} N^{\frac{s}{2}} \Gamma(s) L(E,s)$$

where

$$\Gamma(s) := \int_0^{\infty} t^{s-1} e^{-t} dt \quad \text{if } \Re(s) > 0$$

is the classical gamma function.

We're now going to show that $L(f,s)$ and $\Lambda(f,s)$ extend to a holomorphic functions on the whole $\mathbb{C}$ and that $\Lambda(f,s)$ satisfies a particular functional equation. Remember that the gamma function extends to a meromorphic function on $\mathbb{C}$ that never vanishes.

Definition. We define the operator

$$W_N : \mathcal{S}_2(\Gamma_1(N)) \longrightarrow \mathcal{S}_2(\Gamma_1(N))$$
$$f \longmapsto -f\left|\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}\right.$$

It's easy to see that W_N^2 is the identity operator, hence we can decompose

$$\mathcal{S}_2(\Gamma_1(N)) = \mathcal{S}_2(\Gamma_1(N))^+ \oplus \mathcal{S}_2(\Gamma_1(N))^-$$

with

$$\mathcal{S}_2(\Gamma_1(N))^\pm := \{ f \in \mathcal{S}_2(\Gamma_1(N)) : W_N f = \pm f \}.$$

Thanks to a straight computation, it can be proved that the actions of W_N and T_l commute for every prime l. This means that we can find a basis of eigenvectors for T_l for every l that are also eigenvectors for W_N. In general, if $f \in \mathcal{S}_2(\Gamma_1(N))$ is an eigenvector for W_N we write

$$f|W_N = w_f f \quad \text{with } w_f \in \{1, -1\}.$$

Theorem 4.4.3. *Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in \mathcal{S}_2(\Gamma_1(N))^\pm$. Then*

(a) $L(f,s)$ and $\Lambda(f,s)$ have analytic continuation to entire functions on $\mathbb{C}$.

(b) We have that

$$L(f,s) = (2\pi)^s \Gamma(s)^{-1} \int_0^\infty f(it) t^{s-1} dt$$

for any $s \in \mathbb{C}$.

(c) The function $\Lambda(f,s)$ satisfies the functional equation

$$\Lambda(f,s) = w_f \Lambda(f, 2-s).$$

Proof. Replacing t by $2\pi n t$ in the integral that defines the gamma function, we obtain the relation

$$n^{-s} = (2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} e^{-2\pi n t} dt$$

for $\Re(s) > 0$. Now we restrict to $\Re(s) > 2$ and consider

$$\begin{aligned} L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s} &= \sum_{n=1}^{\infty} a_n (2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} e^{-2\pi n t} dt = \\ &= (2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} \sum_{n=1}^{\infty} a_n e^{-2\pi n t} dt = \\ &= (2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} f(it) dt. \end{aligned}$$

Notice that we could reverse the order of the sum and the integral since the sum is absolutely convergent for $\Re(s) > 2$ (see Proposition 4.4.1). Now we want to prove that this last expression is converging for every $s \in \mathbb{C}$, giving an analytic continuation of L and solving both point (a) and point (b).

Computing the action of the W_N operator, we find the relation

$$f\Big(\frac{i}{t}\Big) = \frac{t^2}{N}(f|W_N)\Big(\frac{it}{N}\Big).$$

Hence we can write

$$\begin{aligned}(2\pi)^{-s}\Gamma(s)L(f,s) &= \int_0^\infty t^{s-1}f(it)dt = \\ &= \int_0^1 t^{s-1}f(it)dt + \int_1^\infty t^{s-1}f(it)dt = \\ &= \int_\infty^1 \Big(\frac{1}{t}\Big)^{s-1} f\Big(\frac{i}{t}\Big)d\Big(\frac{1}{t}\Big) + \int_1^\infty t^{s-1}f(it)dt = \\ &= \int_1^\infty \frac{t^{2-s-1}}{N}(f|W_N)\Big(\frac{it}{N}\Big)dt + \int_1^\infty t^{s-1}f(it)dt.\end{aligned}$$

Since $f \in \mathcal{S}_2(\Gamma_1(N))^\pm$ we have that $f|W_N = \pm f$. Since $f(it)$ and $f(it/N)$ go to zero exponentially as $t \to \infty$, we have that both integrals converge for every $s \in \mathbb{C}$. Moreover, the fact that $\Gamma(s)$ is never zero tells us that $L(f,s)$ can be holomorphically extended to $\mathbb{C}$. Hence we proved point (a) and point (b). With similar computations we can also recover (c) (see [6, 5.10.2]). □

In conclusion, we see a result that gives a relation between a special value of the L-function and modular symbols.

Corollary 4.4.4. *Let $f \in \mathcal{S}_2(\Gamma_1(N))$. Then we have that*

$$\lambda_f(\{0\} - \{i\infty\}) = L(f,1).$$

Proof. Use the change of variable $z = it$ in the definition of standard modular symbol and point (b) of the previous theorem with $s = 1$. □

4.5 Twists

In this section we study the behaviour of cusp forms, modular symbols and L-functions when twisted by a Dirichlet character.

Definition. Let $\chi : \mathbb{Z} \to \mathbb{C}^\times$ be a Dirichlet character of conductor $m \geq 1$. The *Gauss sum* is defined by the formula

$$\tau(n,\chi) := \sum_{a=0}^{m-1} \chi(a)e^{\frac{2\pi ina}{m}}$$

for $n \in \mathbb{Z}$. If $n = 1$ we set $\tau(\chi) := \tau(1,\chi)$.

Lemma 4.5.1. *Let χ be a Dirichlet character modulo m. Then*

(a) If χ is primitive, then

$$\tau(n,\chi) = \bar{\chi}(n)\cdot\tau(\chi)$$

for every $n \in \mathbb{Z}$.

(b) If χ is primitive modulo m then

$$|\tau(\chi)|^2 = \chi(-1)\tau(\chi)\tau(\bar{\chi}) = m.$$

Proof. See [15, 3.1.1]. □

Definition. Let χ be a Dirichlet character modulo $m \geq 1$ and consider $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ in $\mathcal{S}_2(\Gamma_1(N))$. We define the *twist of f by χ* to be

$$f_\chi(z) := \sum_{n=1}^{\infty} \chi(n) a_n e^{2\pi i n z}.$$

Lemma 4.5.2 (Birch)**.** *Let χ be a primitive Dirichlet character of conductor m and $f \in \mathcal{S}_2(\Gamma_1(N))$. Then*

$$f_{\bar{\chi}}(z) = \frac{1}{\tau(\chi)} \sum_{a=0}^{m-1} \chi(a) f\Big(z + \frac{a}{m}\Big).$$

Proof. Use point (a) of lemma 4.5.1 to replace $\bar{\chi}(n)$ by $\tau(n,\chi)/\tau(\chi)$ and rearrange the sums. □

Corollary 4.5.3. *Let $f \in \mathcal{S}_2(\Gamma_1(N))$, χ a primitive Dirichlet character of conductor m and $c \in \mathbb{Q}$. Then*

$$\lambda_{f_{\bar{\chi}}}(\{c\} - \{i\infty\}) = \frac{1}{\tau(\chi)} \sum_{a=0}^{m-1} \chi(a) \lambda_f\Big(\Big\{c + \frac{a}{m}\Big\} - \{i\infty\}\Big).$$

Proof. Just use the definitions and Birch's lemma. □

Definition. Let $f \in \mathcal{S}_2(\Gamma_1(N))$, χ be a primitive Dirichlet character modulo m. Then we write

$$L(f,\chi,s) := L(f_\chi, s).$$

Lemma 4.5.4. *Let $f \in \mathcal{S}_2(\Gamma_1(N))$, χ be a primitive Dirichlet character modulo m. Then*

$$L(f,\bar{\chi},1) = \frac{1}{\tau(\chi)} \sum_{a=0}^{m-1} \chi(a) \lambda_f\Big(\Big\{\frac{a}{m}\Big\} - \{i\infty\}\Big).$$

Proof. Use Corollary 4.4.4 and Corollary 4.5.3 with $c = 0$. □

4.6 p-adic distributions

In this section we introduce the basics of p-adic distributions over a compact open subset of $\mathbb{Z}_p$ and define two particular distributions on $\mathbb{Z}_p^\times$ that will lead us to the definition of the p-adic L-function. From now on we fix an embedding $\mathbb{Q} \to \mathbb{Q}_p$ and we consider $\mathbb{C}_p$ as the Cauchy completion of the algebraic closure of $\mathbb{Q}_p$. It is known that $\mathbb{C}_p$ is a complete and algebraically closed valued field. We also fix an embedding $\bar{\mathbb{Q}} \to \mathbb{C}_p$. We call v the canonical valuation on $\mathbb{C}_p$. Let X be a compact open subset of $\mathbb{Z}_p$.

Definition. A *$\mathbb{C}_p$-valued p-adic distribution* on X is a map μ from the collection of compact open sets of X to $\mathbb{C}_p$ such that

$$\mu\Big(\bigcup_{k=1}^{n} U_k\Big) = \sum_{k=1}^{n} \mu(U_k)$$

with $n \geq 1$ and $\{U_1, \ldots, U_k\}$ any collection of pairwise disjoint compact open sets in X. Compact open sets of type $a + p^n\mathbb{Z}_p$ are called *p-adic balls*.

Proposition 4.6.1. *Every map μ from the set of p-adic balls contained in X to $\mathbb{C}_p$ for which*

$$\mu(a + p^n\mathbb{Z}_p) = \sum_{j=0}^{p-1} \mu(a + jp^n + p^{n+1}\mathbb{Z}_p)$$

whenever $a + p^n\mathbb{Z}_p \subseteq X$, extends uniquely to a p-adic distribution on X.

Proof. See [10, II.3]. □

Definition. A $\mathbb{C}_p$-valued distribution μ on X is called a *measure* if there exists $B \in \mathbb{R}$ such that $v(\mu(U)) \geq B$ for every compact open $U \subseteq X$.

Given a $\mathbb{C}_p$-valued measure μ on X, following [10, II.5] it's possible to define a notion of integration for continous functions $f : X \to \mathbb{C}_p$. In particular we define the Riemann sums

$$S_{N,x_{a,n}} := \sum_{0 \leq a < p^N} f(x_{a,N})\mu(a + p^N\mathbb{Z}_p)$$

where the sum is taken over all a for wich $a + p^n\mathbb{Z} \subseteq X$ and $x_{a,N}$ is chosen to be any element of $a + p^N\mathbb{Z}_p$. This sums converge to a limit in $\mathbb{C}_p$ as $N \to \infty$ that does not depend on the choice of $x_{a,N}$. This limit is called

$$\int_X f d\mu.$$

Remark 4.6.2. The construction in [10, II.5] is made only for continous functions $f : \mathbb{Z}_p^\times \to \mathbb{Q}_p$, but replacing $\mathbb{Q}_p$ with $\mathbb{C}_p$ does not change the proofs.

We are now going to define two special measures on $\mathbb{Z}_p^\times$. First recall an important result due to Manin and Shimura.

Theorem 4.6.3 (Manin, Shimura)**.** *Let $f \in \mathcal{S}_2(\Gamma_1(N), \varepsilon)$ be a Hecke eigenform. There exist complex periods $\Omega_f^+, \Omega_f^- \in \mathbb{C}^\times$ such that*

$$\eta_f^\pm(\{c_2\} - \{i\infty\}) := \frac{\lambda_f^\pm(\{c_2\} - \{i\infty\})}{\Omega_f^\pm} \in \mathcal{O}_K(f)$$

for every $c_2 \in \mathbb{P}^1(\mathbb{Q})$, where $\mathcal{O}_K(f)$ is the ring of integers of the $\mathbb{Q}$-extension $K(f)$ made by adjoining the Fourier coefficients of f to $\mathbb{Q}$.

Proof. See [1, Théorème 1], [3, Proposition 1.1] or [8, Theorem 4.8]. □

Definition. Let $f \in \mathcal{S}_2(\Gamma_1(N), \varepsilon)$ be a normalized Hecke eigenform, call a_p its eigenvalue for T_p and suppose that the polynomial

$$X^2 - a_p X + \varepsilon(p)p \tag{4.4}$$

has a non-zero root with zero valuation. Choose such a root α. We define two measures on $\mathbb{Z}_p^\times$ by the formula

$$\mu_f^\pm(a + p^n\mathbb{Z}_p) := \frac{1}{\alpha^n}\eta_f^\pm\Big(\Big\{\frac{a}{p^n}\Big\} - \{i\infty\}\Big) - \frac{\varepsilon(p)}{\alpha^{n+1}}\eta_f^\pm\Big(\Big\{\frac{a}{p^{n-1}}\Big\} - \{i\infty\}\Big) \tag{4.5}$$

with $a \in \mathbb{Z}$ with $p \nmid a$ and $n > 0$. We also set

$$\mu_f^+(\mathbb{Z}_p^\times) = \Big(1 - \frac{\varepsilon(p)}{\alpha}\Big)\Big(1 - \frac{1}{\alpha}\Big)\frac{\lambda_f(\{0\} - \{i\infty\})}{\Omega_f^+} \quad \text{and} \quad \mu_f^-(\mathbb{Z}_p^\times) = 0. \tag{4.6}$$

Proposition 4.6.4. *The functions $\mu_f^\pm$ give well defined $\mathbb{C}_p$-valued measures on $\mathbb{Z}_p^\times$.*

Proof. Using Proposition 4.3.3, the fact that a_p is the eigenvalue of the action of T_p on f and that α is a root of 4.4 we obtain that $\mu_f^\pm$ satisfy the condition of Proposition 4.6.1, hence they are distributions on $\mathbb{Z}_p^\times$ (see also [14, I.10]). The values for the measure of $\mathbb{Z}_p^\times$ written in equation (4.6) are just

$$\mu_f^\pm(\mathbb{Z}_p^\times) = \sum_{a=1}^{p-1} \mu_f^\pm(a + p\mathbb{Z}_p).$$

Since $v(\alpha) = 0$ and $v(\eta^\pm(\{c_2\} - \{i\infty\})) \geq 0$ for every $c_2 \in \mathbb{P}^1(\mathbb{Q})$ thanks to Theorem 4.6.3, we have that the distributions are bounded. □

4.7 p-adic L-functions

Definition. A *p-adic character* is any continous homomorphism

$$\chi : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times.$$

Remembering that we are working with p odd we obtain the following classical lemma on the structure of $\mathbb{Z}_p^\times$.

Lemma 4.7.1. *If p is an odd prime, we have an isomorphism*

$$\alpha : \mathbb{Z}_p^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p).$$

Proof. See [17, II.5.3]. □

Let now $x \in \mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$. We denote by $\langle x \rangle$ the projection of x on $1 + p\mathbb{Z}_p$ and $\omega(x)$ as the projection of x on $(\mathbb{Z}/p\mathbb{Z})^\times$. We recall now the definition of two imporant $\mathbb{C}_p$-valued functions on $\mathbb{Z}_p$. For details, see [26, 5.1].

Definition. Let $x \in \mathbb{Z}_p$, we define

$$\exp(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

and

$$\log(1 + x) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^n}{n}.$$

The exponential function converges if and only if $v(x) > \frac{1}{p-1}$, while the logarithm converges if and only if $v(x) > 0$.

Definition. For $s \in \mathbb{Z}_p$ we define the p-adic character

$$\chi_s(x) := \langle x \rangle^s := \exp(s \log \langle x \rangle) = \sum_{n=0}^{\infty} \frac{s^n}{n!} (\log \langle x \rangle)^n.$$

Remark 4.7.2. The character χ_s is well defined for every $s \in \mathbb{Z}_p$. For details see [26, 5.1].

The set of p-adic characters $\mathrm{Hom}_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ can be viewed as the disjoint union of the set $\mathrm{Hom}^+_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ of *even* characters (i.e. characters χ such that $\chi(-1) = 1$) and the set $\mathrm{Hom}^-_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ of *odd* characters (i.e. characters χ such that $\chi(-1) = -1$).

Definition. Let f be a normalized Hecke eigenform of $\mathcal{S}_2(\Gamma_1(N), \varepsilon)$, and suppose that the polynomial in (4.4) has a root of valuation 0. Then for every p-adic character χ we define

$$L_p(f, \chi) := \int_{\mathbb{Z}_p^\times} \chi d\mu_f^+$$

if $\chi \in \mathrm{Hom}^{+}_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$, and

$$L_p(f,\chi) := \int_{\mathbb{Z}_p^\times} \chi d\mu_f^-$$

if $\chi \in \mathrm{Hom}^{-}_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$. We also set

$$L_p(f,\chi,s) := L_p(f,\chi\chi_{s-1})$$

for every $s \in \mathbb{Z}_p$. If χ is trivial, we just set

$$L_p(f,s) := L_p(f,1,s).$$

Explicitly, we have that

$$L_p(f,\chi,s) = \int_{\mathbb{Z}_p^\times} \chi(x)\langle x\rangle^{s-1}\, d\mu_f^{\pm}(x)$$

where the sign in $\mu_f^{\pm}$ is chosen to be the parity of $\chi\chi_{s-1}$, which is equal to the parity of χ since the character χ_{s-1} is always even ($\langle -1\rangle = 1$).

4.8 Modularity

Since now, in this chapter we have seen how to construct a p-adic L-function associated to a normalized Hecke eigenform. In this section we are going to present a "dictionary" that tells us how we can pass from the world of elliptic curves to the world of cusp forms. The main ingredient will be the Modularity Theorem, first conjectured in the 50's and completely proved only at the beginning of this century. This theorem has various equivalent formulations: we are going to deal only with the ones we are interested in.

Theorem 4.8.1 (Modularity)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Then there exists a normalized Hecke eigenform $f_E \in \mathcal{S}_2(\Gamma_0(N_E))$ such that*

(a) $a_p(E) = a_p(f_E) \in \mathbb{Z}$ for every prime p, where $a_p(f_E)$ is the eigenvalue for f relative to T_p and $a_p(E)$ is defined as in Section 1.4.

(b) $L(f_E,s) = L(E,s)$, and in particular $L(E,s)$ can be extended to an entire function on $\mathbb{C}$.

Thanks to this theorem, to any elliptic curve $E/\mathbb{Q}$ we can attach the modular form f_E and repeat the constructions we made in the previous sections. This means that we can define two measures $\mu_E^{\pm} := \mu_{f_E}^{\pm}$ associated to E as in equation (4.5).

Lemma 4.8.2. *Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p. Then the measures $\mu_E^{\pm}$ exist and take values in $\mathbb{Z}_p$.*

Proof. In order to show the existence, we need to prove that in this conditions there is always a root α of

$$g(X) := X^2 - a_p(f_E)X + p$$

with zero valuation (note that we put $\varepsilon = 1$ since $f_E \in \Gamma_0(N_E)$). Since E has good ordinary reduction at p we have that $v(a_p(f_E)) = 0$, hence if we call α and β the two roots of $g(X)$ we must have

$$0 = v(a_p(f_E)) = v(\alpha + \beta) \geq \min\{\, v(\alpha), v(\beta)\,\}.$$

This means that one root has zero valuation.

We now have to show that

$$\frac{1}{\alpha^n}\eta^{\pm}_{f_E}\Big(\Big\{\frac{a}{p^n}\Big\} - \{i\infty\}\Big) - \frac{1}{\alpha^{n+1}}\eta^{\pm}_{f_E}\Big(\Big\{\frac{a}{p^{n-1}}\Big\} - \{i\infty\}\Big) \in \mathbb{Z}_p$$

for any $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Thanks to the modularity theorem we know that $a_l(f_E) \in \mathbb{Z}$ for any prime l, hence by Theorem 4.6.3

$$\eta^{\pm}_{f_E}(\{c_2\} - \{i\infty\}) \in \mathbb{Z}$$

for any $c_2 \in \mathbb{P}^1(\mathbb{Q})$. We now show that $\alpha \in \mathbb{Z}_p^\times$. Consider the reduction $\bar{g}(X)$ of $g(X)$ modulo p. The polynomial $\bar{g}(X)$ has two different solutions in $\mathbb{F}_p$ since $a_p \not\equiv 0 \pmod{p}$. By Hensel's lemma, we can lift the two roots of $\bar{g}(X)$ to roots of $g(X)$ that lie in $\mathbb{Z}_p$. Moreover, α is invertible since $v(\alpha) = 0$. □

4.9 p-adic L-series

In this section we study the relations between measures on $\mathbb{Z}_p^\times$ and elements of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. We build a particular element of $\Lambda = \mathbb{Z}_p[[T]]$ related to the measures defined in equation (4.5) that will play a fundamental role in the statement of the Iwasawa main conjecture.

Proposition 4.9.1. *There is a one to one correspondence between $\mathbb{Z}_p$-valued measures μ on $\mathbb{Z}_p^\times$ and elements β of*

$$\mathbb{Z}_p[[\mathbb{Z}_p^\times]] \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times].$$

Proof. Let μ be a function from the set of open compact sets of $\mathbb{Z}_p^\times$ to $\mathbb{Z}_p$. Then we define

$$\beta_n := \sum_{\substack{0<a<p^n \\ p\nmid a}} \mu(a + p^n\mathbb{Z}_p)[a]_n \in \mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times] \tag{4.7}$$

where $[a]_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ is the group element attached to a. Then one can easily check that $\beta := (\beta_n)_{n\in\mathbb{N}}$ is an element of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ if and only if μ satisfies the properties of Proposition 4.6.1, hence if and only if μ is a measure on $\mathbb{Z}_p^\times$. Also, starting with any element $\beta = (\beta_n) \in \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[(\mathbb{Z}/p^n\mathbb{Z})^\times]$, we can always define a measure using equation (4.7). □

Let now $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p. Recall that we defined two measures $\mu_E^{\pm}$ on $\mathbb{Z}_p^\times$ that take value in $\mathbb{Z}_p$, thanks to Lemma 4.8.2. Thanks to the above proposition, we can construct an element $\beta_E^{\pm} \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ that corresponds to the measure $\mu_E^{\pm}$. Let now $\mathbb{Q}_\infty/\mathbb{Q}$ be the $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and call $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. From the isomorphism in Lemma 4.7.1 we have a natural projection

$$\pi : \mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p) \longrightarrow (1+p\mathbb{Z}_p) \cong \Gamma.$$

The map π naturally extends to a map

$$\tilde{\pi} : \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \longrightarrow \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$$

thanks to the isomorphism in Proposition 2.4.2.

Definition. The element $\mathcal{L}_E := \tilde{\pi}(\beta_E^+) \in \Lambda = \mathbb{Z}_p[[T]]$ is called the *p-adic L-series* associated to $E/\mathbb{Q}$. With a little abuse of notation, we will also call $\mathcal{L}_E$ the corresponding element of $\mathbb{Z}_p[[\Gamma]]$.

Now we try to give a connection between the p-adic L-function and the p-adic L-series. We also look at some relations with complex L-functions of elliptic curves.

Lemma 4.9.2. *Let χ be a character on $\mathbb{Z}_p^\times$ of conductor p^n for some $n \in \mathbb{N}$ and let μ be a measure on $\mathbb{Z}_p^\times$. Then*

$$\int_{\mathbb{Z}_p^\times} \chi d\mu = \sum_{\substack{0<a<p^n \\ p\nmid a}} \chi(a)\mu(a+p^n\mathbb{Z}_p).$$

Proof. By definition of integral we have that

$$\int_{\mathbb{Z}_p^\times} \chi d\mu = \lim_{N\to\infty} \sum_{\substack{0\le a<p^N \\ p\nmid a}} \chi(x_{a,N})\mu(a+p^N\mathbb{Z}_p)$$

with $x_{a,N}$ any element of $a+p^N\mathbb{Z}_p$, hence we can take $x_{a,N} = a$. Since χ has conductor p^n, using Proposotion 4.6.1 we have that

$$\begin{aligned}
\sum_{\substack{0<a<p^n \\ p\nmid a}} \chi(a)\mu(a+p^n\mathbb{Z}_p) &= \sum_{\substack{0<a<p^n \\ p\nmid a}} \sum_{j=0}^{p-1} \chi(a)\mu(a+jp^n+p^{n+1}\mathbb{Z}_p) = \\
&= \sum_{\substack{0<a<p^n \\ p\nmid a}} \sum_{j=0}^{p-1} \chi(a+jp^n)\mu(a+jp^n+p^{n+1}\mathbb{Z}_p) = \\
&= \sum_{\substack{0<b<p^{n+1} \\ p\nmid b}} \chi(b)\mu(b+p^{n+1}\mathbb{Z}_p).
\end{aligned}$$

This means that the sequence whose limit defines the integral is constant from the n-th term on. □

Definition. Let χ be a character on $\mathbb{Z}_p^\times$ and $\beta = (\beta_0, \beta_1, \dots) \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. Write

$$\beta_n := \sum_{\substack{0<a<p^n \\ p\nmid a}} \rho_{a,n}[a]_n$$

where $[a]_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ is the group element attached to a and $\rho_{a,n} \in \mathbb{Z}_p$. We define

$$\chi(\beta) := \lim_{n\to\infty} \sum_{\substack{0<a<p^n \\ p\nmid a}} \rho_{a,n}\chi(a).$$

Since every element $\beta \in \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ corresponds to a measure μ_β on $\mathbb{Z}_p^\times$ using equation 4.7, we easily see that for every character χ on $\mathbb{Z}_p^\times$ we have

$$\chi(\beta) = \int_{\mathbb{Z}_p^\times} \chi d\mu_\beta.$$

In particular, this implies that if $E/\mathbb{Q}$ is an elliptic curve with good ordinary reduction at p, then

$$\chi(\beta_E^\pm) = L_p(f_E, \chi)$$

where f_E is the cusp form corresponding to E by the modularity theorem and the sign in $\beta_E^\pm$ is chosen to be equal to the parity of χ.

Now, characters on $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)$ that are trivial on $(\mathbb{Z}/p\mathbb{Z})^\times$ correspond to characters on $\Gamma \cong 1+p\mathbb{Z}_p$. Let ψ be such a charcter. Such a ψ is always even since the projection of $-1 \in \mathbb{Z}_p^\times$ onto $1+p\mathbb{Z}_p$ is 1. By definition of $\mathcal{L}_E$, we clearly have that

$$\psi(\beta_E^+) = \psi(\mathcal{L}_E) = L_p(f_E, \psi).$$

For example, we obtain that

$$\chi_s(\mathcal{L}_E) = L_p(f, s).$$

Definition. Let $E/\mathbb{Q}$ be an elliptic curve, χ a Dirichlet character with conductor m and f_E the cusp form corresponding to E by the modularity theorem. Then

$$L(E, \chi, s) := L(f_E, \chi, s) = L(f_{E,\chi}, s).$$

Theorem 4.9.3. *Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at p and let $\chi \in \mathrm{Hom}^\pm_{cont}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ be a character of conductor p^n for some $n \geq 0$. Then*

$$\chi(\beta_E^\pm) = \begin{cases} \left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E,1)}{\Omega^+_{f_E}} & \text{if } \chi = 1 \\ \frac{\tau(\chi)}{\alpha^n} \frac{L(E,\bar{\chi},1)}{\Omega^\pm_{f_E}} & \text{if } \chi \neq 1 \end{cases}$$

where $\tau(\chi)$ is the Gauss sum defined in section 4.5 and α is a root of the polynomial in (4.4) of zero valuation.

Proof. If $\chi = 1$ then $\chi(\beta_E^+) = \mu_E^+(\mathbb{Z}_p^\times)$ and the result follows from equation (4.6) and Corollary 4.4.4.

Let $\chi \neq 1$, and suppose that χ is even. Let f_E be the cusp form corresponding to E by the modularity theorem. For the sake of simplicity, write $\lambda(\{c\}) := \lambda_{f_E}(\{c\} - \{i\infty\})$ and $\Omega^\pm := \Omega^\pm_{f_E}$. Thanks to the discussion of this section and Lemma 4.9.2 we can compute

$$\chi(\beta_E^+) = \int_{\mathbb{Z}_p^\times} \chi d\mu_E^+ = \sum_{\substack{0<a<p^n \\ p\nmid a}} \chi(a)\mu_E^+(a+p^n\mathbb{Z}_p) =$$

$$= \sum_{\substack{0<a<p^n \\ p\nmid a}} \chi(a)\left(\frac{\lambda\left(\left\{\frac{a}{p^n}\right\}\right) + \lambda\left(\left\{-\frac{a}{p^n}\right\}\right)}{2\alpha^n\Omega^+} - \frac{\lambda\left(\left\{\frac{a}{p^{n-1}}\right\}\right) + \lambda\left(\left\{-\frac{a}{p^{n-1}}\right\}\right)}{2\alpha^{n+1}\Omega^+}\right).$$

The fact that χ is even implies that $\chi(a) = \chi(p^n - a)$, and $\lambda\left(\left\{\frac{a}{m}\right\}\right)$ depends only on a modulo m, since f_E is periodic of period 1. Using this facts, we can proceed with the equalities

$$\sum_{\substack{0<a<p^n \\ p\nmid a}} \chi(a)\left(\frac{1}{\alpha^n}\frac{\lambda\left(\left\{\frac{a}{p^n}\right\}\right) + \lambda\left(\left\{-\frac{a}{p^n}\right\}\right)}{2\Omega^+} - \frac{1}{\alpha^{n+1}}\frac{\lambda\left(\left\{\frac{a}{p^{n-1}}\right\}\right) + \lambda\left(\left\{-\frac{a}{p^{n-1}}\right\}\right)}{2\Omega^+}\right) =$$

$$= \sum_{\substack{0<a<p^n \\ p\nmid a}} \frac{\chi(a)\lambda\left(\left\{\frac{a}{p^n}\right\}\right)}{\alpha^n\Omega^+} - \sum_{\substack{0<a<p^{n-1} \\ p\nmid a}} \frac{\lambda\left(\left\{\frac{a}{p^{n-1}}\right\}\right) + \lambda\left(\left\{-\frac{a}{p^{n-1}}\right\}\right)}{2\alpha^{n+1}\Omega^+}\left(\sum_{j=0}^{p-1}\chi(a+jp^{n-1})\right).$$

Since χ is a primitive character modulo p^n, we have that

$$\sum_{j=0}^{p-1}\chi(a+jp^{n-1}) = 0$$

for every $0 < a < p^{n-1}$ with $p \nmid a$. Using Lemma 4.5.4 we get the claim.

If χ is odd the proof is similar, using μ_E^- instead of μ_E^+ and the fact that $\chi(-a) = -\chi(a)$. □

Corollary 4.9.4. *With the notation of the above theorem, if the caracter χ factors through $1 + p\mathbb{Z}_p$ in the factorizarion $\mathbb{Z}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$ (and hence is even), then we have*

$$\chi(\mathcal{L}_E) = \chi(\beta_E^+) = \begin{cases} \left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E,1)}{\Omega^+_{f_E}} & \text{if } \chi = 1 \\ \frac{\tau(\chi)}{\alpha^n}\frac{L(E,\bar{\chi},1)}{\Omega^+_{f_E}} & \text{if } \chi \neq 1. \end{cases}$$

Proof. It is clear from the discussion before Theorem 4.9.3 and from Theorem 4.9.3. □

Chapter 5

The Main Conjecture

The aim of this chapter is to present the Iwasawa main conjecture for an elliptic curve $E/\mathbb{Q}$ with good ordinary reduction at an odd prime p. We also prove Mazur's control theorem for cyclotomic $\mathbb{Z}_p$-extensions, that is a fundamental result of Iwasawa theory for elliptic curves and will be useful also in the next chapter. We fix some notation that will be used throughout this chapter:

p	an odd prime of $\mathbb{Z}$;
K	a number field;
K_∞	the cyclotomic $\mathbb{Z}_p$-extension of K;
K_n	the intermediate field between K and K_∞ of degree p^n over K;
Γ	the Galois group of the extension K_∞/K;
Γ_n	the Galois group of the extension K_n/K.

5.1 The p-Selmer group of E over K_∞

Let E/K be an elliptic curve. In this section we want to study the structure of $\mathrm{Sel}_E(K_\infty)_p$ and of its Pontryagin dual. If M is any perfect field and S is a $G_{\bar{M}/M}$-module, we write $H^1(M,S) \coloneqq H^1(G_{\bar{M}/M}, S)$ in order to ease the notation.

Definition. Let E/K be an elliptic curve defined over a number field K. We define the *p-primary Selmer group of E over K_∞* to be

$$\mathrm{Sel}_E(K_\infty)_p \coloneqq \varinjlim_{n\in\mathbb{N}} \mathrm{Sel}_E(K_n)_p.$$

Reconsider the exact sequence in (3.3) with K_n in place of K. By considering the direct limit on n and applying Proposition A.2.7 we find the

following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K_\infty)\otimes_{\mathbb{Z}}\frac{\mathbb{Q}_p}{\mathbb{Z}_p} & \xrightarrow{\vec{\delta}} & H^1(K_\infty, E[p^\infty]) & \xrightarrow{\vec{\iota_*}} & H^1(K_\infty, E)[p^\infty] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \vec{\theta}} & & \downarrow{\scriptstyle \prod_\eta \vec{\mathrm{Res}}_\eta} & & \downarrow{\scriptstyle \prod_\eta \vec{\mathrm{Res}}_\eta} & & \\ 0 & \longrightarrow & \prod_\eta E((K_\infty)_\eta)\otimes\frac{\mathbb{Q}_p}{\mathbb{Z}_p} & \xrightarrow{\vec{\delta_v}} & \prod_\eta H^1(G_\eta, E[p^\infty]) & \xrightarrow{\vec{\iota_{\eta *}}} & \prod_\eta H^1(G_\eta, E)[p^\infty] & \longrightarrow & 0 \end{array} \tag{5.1}$$

where in the first row $E = E(\bar{K})$, in the second row $E = E(\overline{(K_\infty)}_\eta)$ and η runs among the valuations of K_∞. Here G_η is the decomposition group of an extension of η to $\bar{K}$ and $(K_\infty)_\eta$ denotes the union of the completions of every K_n with respect to η (see section B.4). Using the same argument of the proof of Lemma 3.4.1 we obtain the following proposition.

Proposition 5.1.1. *Let E/K be an elliptic curve. Then*

$$\mathrm{Sel}_E(K_\infty)_p = \ker\left\{\prod_\eta \vec{\mathrm{Res}}_\eta \circ \vec{\iota_*} : H^1(K_\infty, E(\bar{K})[p^\infty]) \to \prod_\eta H^1(G_\eta, E(\overline{(K_\infty)}_\eta)\right\}$$

where η varies among the valuations of K_∞.

Endow $H^1(K_n, E(\bar{K})[p^\infty])$ with the discrete topology. Since we have that $\Gamma_n \cong G_{\bar{K}/K}/G_{\bar{K}/K_n}$, the construction in Lemma A.2.4 gives us a well defined continous action of Γ_n on $H^1(K_n, E(\bar{K})[p^\infty])$, defined in the following way:

$$(\bar{\sigma}\cdot\xi)(\tau) = \sigma(\xi(\sigma^{-1}\tau\sigma))$$

for every $\tau \in G_{\bar{K}/K_n}$ and $\xi \in H^1(K_n, E(\bar{K})[p^\infty])$. Here $\bar{\sigma}$ is any element of Γ_n and σ denotes any lifting of $\bar{\sigma}$ to an element of $G_{\bar{K}/K}$.

Proposition 5.1.2. *The group $\mathrm{Sel}_E(K_\infty)_p$ is a discrete Λ-module.*

Proof. Let $E[p^\infty] := E(\bar{K})[p^\infty]$. See that $E[p^\infty]$ is a $\mathbb{Z}_p$-module, with multiplication defined as $x\cdot P = [\bar{x}]P$ where $x \in \mathbb{Z}_p$, $P \in E[p^\infty]$ of order p^m for some $m \in \mathbb{N}$ and $\bar{x}$ is the reduction of x modulo $p^m\mathbb{Z}_p$. The notation $[\bar{x}]$ stands for the multiplication by $\bar{x}$ on E. This action induces also an action of $\mathbb{Z}_p$ on $H^1(K_n, E[p^\infty])$. It is easy to see that this action is well defined. The continuity of

$$\begin{aligned} \mathbb{Z}_p \times H^1(K_n, E[p^\infty]) &\longrightarrow H^1(K_n, E[p^\infty]) \\ (x, \xi) &\longmapsto x\cdot\xi \end{aligned}$$

is clear since the preimage of 0 is the union of $(\mathrm{Ann}_{\mathbb{Z}_p}(\xi), \xi)$ for every $\xi \in H^1(K_n, E[p^\infty])$, and $\mathrm{Ann}_{\mathbb{Z}_p}(\xi) := \{\, x \in \mathbb{Z}_p \,:\, x\cdot\xi = 0 \,\}$ is open in $\mathbb{Z}_p$ since ξ assumes only a finite number of values in $E[p^\infty]$.

From the fact that the multiplication by m is an isogeny defined over K, it descends that

$$x \cdot \bar{\sigma}(\xi) = \bar{\sigma}(x \cdot \xi) \tag{5.2}$$

for every $\xi \in H^1(K_n, E[p^\infty])$, $\bar{\sigma} \in \Gamma_n$ and $x \in \mathbb{Z}_p$. Thanks to equation (5.2) we can join the two actions described above to build an action of the group ring $\mathbb{Z}_p[\Gamma_n]$ on the discrete module $H^1(K_n, E[p^\infty])$.

Now we prove that $\mathrm{Sel}_E(K_n)_p$ is a $\mathbb{Z}_p[\Gamma_n]$-submodule of $H^1(K_n, E[p^\infty])$. Take $\xi \in \mathrm{Sel}_E(K_n)_p$. By definition (remember the diagram in (3.3)) this means that $\vec{\mathrm{Res}}_v(\xi)$ lies in the image of $\vec{\delta}_v$ for any place v of K_n. Hence

$$\begin{aligned} \vec{\mathrm{Res}}_v(\xi) : G_v &\longrightarrow E(\overline{(K_n)_v})[p^\infty] \\ \tau &\longmapsto \tau(Q) - Q \end{aligned} \tag{5.3}$$

for some $Q \in E(\overline{(K_n)_v})$ such that $p^m Q \in E((K_n)_v)$ for some $m \in \mathbb{N}$ and for G_v a decomposition group for v. Fix now $\bar{\sigma} \in \Gamma_n$; we have to prove that $\bar{\sigma}(\xi) \in \mathrm{Sel}_E(K_n)_p$. This means that we have to prove that the restriction of $\bar{\sigma}(\xi)$ on G_v stays in the image of $\vec{\delta}_v$ for any place v of K_n. Let σ be a lifting of $\bar{\sigma}$ to $G_{\bar{K}/K}$. By definition of the action of $\bar{\sigma}$, using the basic properties of cocycles and equation (5.3) we obtain

$$\begin{aligned} \bar{\sigma}(\xi)(\tau) &= \sigma(\xi(\sigma^{-1}\tau\sigma)) = \sigma\xi(\sigma^{-1}) + \xi(\tau) + \tau\xi(\sigma) = \\ &= (\xi(\sigma\sigma^{-1}) - \xi(\sigma)) + \tau(Q) - Q + \tau\xi(\sigma) = \tau(Q + \xi(\sigma)) - (Q + \xi(\sigma)) \end{aligned}$$

for any $\tau \in G_v$. Since $\xi(\sigma) \in E[p^\infty]$ we have that there exists an $r \in \mathbb{N}$ such that $p^r(Q + \xi(\sigma)) \in E((K_n)_v)$, hence $\bar{\sigma}(\xi)$ lies in the image of $\vec{\delta}_v$ for any valuation v of K_n. Therefore $\bar{\sigma}(\xi) \in \mathrm{Sel}_E(K_n)_p$. This implies that $\mathrm{Sel}_E(K_n)_p$ is a $\mathbb{Z}_p[\Gamma_n]$-submodule of $H^1(K_n, E[p^\infty])$.

Using Proposition A.2.7 we can endow $\mathrm{Sel}_E(K_\infty) = \varinjlim_{n\in\mathbb{N}} \mathrm{Sel}_E(K_n)_p$ with a stucture of a discrete $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[\Gamma_n]$-module. Thanks to the isomorphism in Proposition 2.4.2 we conclude that $\mathrm{Sel}_E(K_\infty)_p$ is a discrete Λ-module. □

Definition. We denote the Pontryagin dual of $\mathrm{Sel}_E(K_\infty)_p$ as

$$X_E(K_\infty) := \Big(\mathrm{Sel}_E(K_\infty)_p\Big)' = \mathrm{Hom}\Big(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p\Big).$$

Corollary 5.1.3. *The group $X_E(K_\infty)$ is a compact Λ-module.*

Proof. From our discussion in Section 2.3 and from Proposition 5.1.2 we have that $X_E(K_\infty)$ is a compact Λ-module, since $\mathrm{Sel}_E(K_\infty)_p$ is a discrete Λ-module. □

5.2 Mazur's Control Theorem

Let K be a number field. From now on we consider an elliptic curve E/K with good ordinary reduction at every prime v of K that lie above p. Recall that we have the cyclotomic $\mathbb{Z}_p$-extension K_∞/K with Galois group $\Gamma \cong \mathbb{Z}_p$, call K_n the intermediate field of degree p^n over K. The aim of this section is to prove the following theorem, mainly following [7, Section 3].

Theorem 5.2.1 (Mazur's Control Theorem)**.** *Assume that E/K has good ordinary reduction at every prime of K that lie above p. Then the natural restriction maps*

$$s_n : \mathrm{Sel}_E(K_n)_p \longrightarrow \mathrm{Sel}_E(K_\infty)_p^{\Gamma^{p^n}}$$

have finite kernel and cokernel, of bounded order as n varies.

The natural restriction maps we refer to are the maps described in Lemma A.2.4. We will prove this theorem with a series of lemmas, but first we give some notation.

Let M denote a field that could be K, K_∞ or K_n for every $n \in \mathbb{N}$. Recalling the exact sequences (3.3) and (5.1), for every prime w of M we define

$$\mathcal{H}_E(M_w) := H^1(M_w, E(\bar{M}_w)[p^\infty])/\mathrm{Im}(\vec{\delta}_w) \cong H^1(M_w, E(\bar{M}_w))[p^\infty].$$

We also set $\mathcal{P}_E(M) := \prod_w \mathcal{H}_E(M_w)$, where w runs over all valuations of M, and

$$\mathcal{G}_E(M) := \mathrm{Im}\left\{\vec{\iota}_{w*} \circ \prod_w \vec{\mathrm{Res}}_w : H^1(M, E(\bar{K})[p^\infty]) \to \mathcal{P}_E(M)\right\}.$$

Thus,

$$\mathrm{Sel}_E(M)_p = \ker\left\{\vec{\iota}_{w*} \circ \prod_w \vec{\mathrm{Res}}_w : H^1(M, E(\bar{K})[p^\infty]) \to \mathcal{P}_E(M)\right\}.$$

A result on semilocal Galois cohomology (see [19, B.5.1]) tells us that $\mathcal{P}_E(K_n)$ and $\mathcal{G}_E(K_n)$ are naturally Γ_n-modules, and hence $\mathcal{P}_E(K_\infty)$ and $\mathcal{G}_E(K_\infty)$ are naturally Λ-modules. Using Lemma A.2.4 and Proposition A.1.5, for every $n \in \mathbb{N}$ we can construct the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}_E(K_n)_p & \longrightarrow & H^1(K_n, E(\bar{K})[p^\infty]) & \longrightarrow & \mathcal{G}_E(K_n) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle g_n} & & \\
0 & \longrightarrow & \mathrm{Sel}_E(K_\infty)_p^{\Gamma^{p^n}} & \longrightarrow & H^1(K_\infty, E(\bar{K})[p^\infty])^{\Gamma^{p^n}} & \longrightarrow & \mathcal{G}(K_\infty)^{\Gamma^{p^n}}. & &
\end{array} \tag{5.4}$$

The maps s_n, h_n and g_n are the natural restriction maps (see A.2.4). The snake lemma then gives the exact sequence

$$0 \longrightarrow \ker(s_n) \longrightarrow \ker(h_n) \longrightarrow \ker(g_n) \longrightarrow \operatorname{coker}(s_n) \longrightarrow \operatorname{coker}(h_n).$$

Therefore, in order prove Mazur's control theorem we must study the order of $\ker(h_n)$, $\ker(g_n)$ and $\operatorname{coker}(h_n)$. We first recall an important result due to Mazur.

Theorem 5.2.2 (Mazur)**.** *The group $E(K_\infty)[p^\infty]$ is finite.*

Proof. See [13, 6.12]. □

Lemma 5.2.3. *The kernel of h_n is finite and has bounded order as n varies.*

Proof. By the inflation-restriction sequence (see Proposition A.2.3) we have that $\ker(h_n) \cong H^1(\Gamma^{p^n}, E(K_\infty)[p^\infty])$. From the above theorem we have that $E(K_\infty)[p^\infty]$ is finite. Therefore, calling F the extension of K obtained by adjoining the coordinates of the points in $E(K_\infty)[p^\infty]$, we have that F/K is finite. Hence there exists an $N \in \mathbb{N}$ such that Γ^{p^n} acts trivially on F, and therefore on $E(K_\infty)[p^\infty]$, for every $n \geq N$. Now, since $\Gamma^{p^n} \cong \Gamma$ we have that $H^1(\Gamma^{p^n}, E(K_\infty)[p^\infty])$ is finite for every n (see Proposition A.3.6). For $n \geq N$ we have that

$$H^1(\Gamma^{p^n}, E(K_\infty)[p^\infty]) \cong \operatorname{Hom}_{cont}(\Gamma, E(K_\infty)[p^\infty]),$$

that is finite and independent on n. □

Lemma 5.2.4. $\operatorname{coker}(h_n) = 0$ *for every* $n \in \mathbb{N}$.

Proof. Thanks to the five-terms cohomology sequence (see Proposition A.2.5) we have the exact sequence

$$H^1(K_n, E(\bar{K})[p^\infty]) \xrightarrow{h_n} H^1(K_\infty, E(\bar{K})[p^\infty])^{\Gamma^{p^n}} \longrightarrow H^2(\Gamma^{p^n}, B)$$

where $B := H^0(K_\infty, E(\bar{K})[p^\infty]) = E(K_\infty)[p^\infty]$. But Γ^{p^n} is a free pro-p-group, hence $H^2(\Gamma_n, B) = 0$ as $\operatorname{cd}_p(\Gamma) = 1$ (see Proposition A.3.2). □

Let now v be any place of K. We will let v_n be any place of K_n lying over v. To study $\ker(g_n)$ we focus on each factor in $\mathcal{P}_E(K_n)$ by considering

$$r_{v_n} : \mathcal{H}_E((K_n)_{v_n}) \longrightarrow \mathcal{H}_E((K_\infty)_\eta) \tag{5.5}$$

to be the natural restriction map, with η a valuation that lies above v_n. Notice that the restriction map that defines g_n has factors of the type

$$\mathcal{H}_E((K_n)_{v_n}) \longrightarrow \prod_\eta \mathcal{H}_E((K_\infty)_\eta)$$

where η runs over the valuations of K_∞ that lie over v_n. But all such $(K_\infty)_\eta$ are isomorphic, hence the kernel of each such factor is equal to the kernel of r_{v_n}, for a fixed η.

If v is archimedean, thanks to Proposition 2.4.3 we have that v is unramified in K_∞/K, hence $K_v = (K_\infty)_\eta$ and $\ker(r_{v_n}) = 0$. For nonarchimedean primes we consider separately the cases $v \nmid p$ and $v \mid p$. We begin recalling a general lemma about the structure of $(\mathbb{Q}_p/\mathbb{Z}_p)^2$.

Lemma 5.2.5. *Let $r \in \mathbb{N}$. The subgroups of $(\mathbb{Q}_p/\mathbb{Z}_p)^2$ are of type*

$$(\mathbb{Q}_p/\mathbb{Z}_p)^e \times U$$

where U is a finite group and $0 \le e \le 2$.

Lemma 5.2.6. *Let $l \neq p$ be a valuation of $\mathbb{Q}$, M any algebraic extension of $\mathbb{Q}$ and η an extension of l to M. Then*

$$E(M_\eta) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = 0.$$

Proof. Let first M be a finite extension of $\mathbb{Q}$ and l nonarchimedean. We have a theorem of Lutz (that follows from [22, 6.3]) that says that

$$E(M_\eta) \cong \mathbb{Z}_l^{[M_\eta:\mathbb{Q}_l]} \times U$$

as a group, where U is a finite group. Since p is a unit in $\mathbb{Z}_l$, for every $x \in \mathbb{Z}_l$ we have a factorization $x = p(p^{-1}x)$ with all coefficients in $\mathbb{Z}_l$: this means that $\mathbb{Z}_l$ is p-divisible. Since $\mathbb{Q}_p/\mathbb{Z}_p$ is p-torsion, we obtain that

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) = 0.$$

Since $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible, $U \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$, and the claim follows.

If M is a finite extension of $\mathbb{Q}$ and l is an archimedean valuation, we have that $M_\eta = \mathbb{R}$ or $\mathbb{C}$. In this case

$$E(M_\eta) \cong T^{[M_\eta:\mathbb{R}]} \times U$$

where U is finite and $T = \mathbb{R}/\mathbb{Z}$. Since T is divisible, we obtain the claim.

If M is an infinite algebraic extension of $\mathbb{Q}$, just use that $M = \bigcup L$ where L runs over all finite extensions of $\mathbb{Q}$ contained in M. □

Lemma 5.2.7. *Let v be a nonarchimedean prime of K not dividing p. Then $\ker(r_{v_n})$ is finite and has bounded order as n varies. If E has good reduction at v, then $\ker(r_{v_n}) = 0$ for every n.*

Proof. Let $B_v := H^0((K_\infty)_\eta, E(\bar{K}_v)[p^\infty])$, and call $G_{v_n} \subseteq \Gamma$ the decomposition group of the extension $(K_\infty, \eta)/(K_n, v_n)$, that is unramified since $v_n \nmid p$. From Lemma 2.4.7, we know that $G_{v_n} = 0$ is impossible. Hence

$G_{v_n} = \Gamma^{p^m} \cong \Gamma$ for some $m \in \mathbb{N}$. Since G_{v_n} is the Galois group of the extension $(K_\infty)_\eta/(K_n)_{v_n}$, this is an unramified $\mathbb{Z}_p$-extension. Remember that $E(\bar{K}_v)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$. From Lemma 5.2.5 we have that

$$B_v \cong (\mathbb{Q}_p/\mathbb{Z}_p)^e \times U$$

with $0 \leq e \leq 2$ and U a finite group. Applying Lemma 5.2.6 we have that $\mathcal{H}_E(L) = H^1(L, E(\bar{K}_v)[p^\infty])$ for every algebraic extension L of K_v. Fixing γ_{v_n} to be a topological generator for G_{v_n}, the inflation-restriction sequence gives us the following exact sequence:

$$0 \to H^1(G_{v_n}, B_v) \longrightarrow H^1\big((K_n)_{v_n}, E(\bar{K}_v)[p^\infty]\big) \xrightarrow{r_{v_n}} H^1\big((K_\infty)_\eta, E(\bar{K}_v)[p^\infty]\big).$$

This means that

$$\ker(r_{v_n}) \cong H^1(G_{v_n}, B_v) \cong B_v/(\gamma_{v_n} - 1)B_v$$

(see Proposition A.3.6). Using again Lutz's theorem (that follows from [22, 6.3]) we have that $\ker(\gamma_{v_n} - 1)$, i.e. the p-primary group $E((K_n)_{v_n})[p^\infty]$, is finite. Call $(B_v)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^e$ the p-divisible part of B_v. Applying point (d) of Proposition A.3.6 we have that

$$(B_v)_{\mathrm{div}} \cong (\gamma_{v_n} - 1)(B_v)_{\mathrm{div}} \subseteq (\gamma_{v_n} - 1)B_v.$$

Hence we obtain that

$$|\ker(r_{v_n})| = \Big|B_v/(\gamma_{v_n} - 1)B_v\Big| \leq |B_v/(B_v)_{\mathrm{div}}| = |U|.$$

The bound is finite and independent from n.

Assume now that E has good reduction at the place v. Consider the field $K_{v,n} := K_v([p^n]^{-1}E(K_v))$ obtained from K_v by adding the coordinates of the preimages of every element of $E(K_v)$ by means of the multiplication-by-p^n map. Let

$$K_{v,\infty} := \bigcup_n K_{v,n} = K_v(E(\bar{K}_v)[p^\infty]).$$

From [22, VII.1.5] we have that $K_{v,\infty}/K_v$ is unramified and that $K_{v,n}/K$ is an abelian p-extension for every n. Hence

$$\mathrm{Gal}(K_{v,\infty}/K_v) \cong \varprojlim_{n \in \mathbb{N}} \mathrm{Gal}(K_{v,n}/K_v)$$

is a pro-p-group. Since $K_{v,\infty}/K_v$ is unramified, $\mathrm{Gal}(K_{v,\infty}/K_v)$ is a quotient of $\mathrm{Gal}(\bar{k}_v/k_v) \cong \hat{\mathbb{Z}} \cong \prod_l \mathbb{Z}_l$, where k_v is the residue field of K_v and l varies amongst the primes of $\mathbb{Z}$. Since $\mathrm{Gal}(K_{v,\infty}/K_v)$ is a pro-p-group, it must be a quotient of the maximal pro-p-quotient of $\hat{\mathbb{Z}}$, i.e. $\mathbb{Z}_p$. Since $(K_\infty)_\eta$ is the only unramified $\mathbb{Z}_p$-extension of K_v, we must have that $K_{v,\infty} \subseteq (K_\infty)_\eta$. This means that $B_v = E(\bar{K}_v)[p^\infty]$ and then

$$\ker(r_{v_n}) = H^1(G_{v_n}, E(\bar{K}_v)[p^\infty]) = 0$$

using the fact that $E(\bar{K}_v)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$ and Proposition A.3.6. □

We now consider the case $v|p$. We call k_{v_n} the residue field of $(K_n)_{v_n}$ and $\tilde{E}$ the reduction of E at v. Since K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension, by Lemma 2.4.6 we have that v ramifies in K_∞, and by Proposition 2.4.4 we have that there exists an $N \in \mathbb{N}$ such that v_n is totally ramified in K_∞/K_n for every $n \geq N$. This implies that $k_{v_n} = k_\eta$ for every $n \geq N$.

Lemma 5.2.8. *Let $v|p$ be a valuation of K. Assume that E has good ordinary reduction at v. Then*

$$|\ker(r_{v_n})| = |\tilde{E}(k_{v_n})[p^\infty]|^2.$$

It is finite and bounded as n varies.

Proof. Call $E[p^\infty] := E(\bar{K}_v)[p^\infty]$ and $\tilde{E}[p^\infty] := \tilde{E}(\bar{k}_v)[p^\infty]$. We also let $C_v := \ker(E[p^\infty] \to \tilde{E}[p^\infty])$. Since E has good ordinary reduction at v, we have that $C_v \cong \mathbb{Q}_p/\mathbb{Z}_p$. For any algebraic extension M_w of K_v we have the natural map

$$\lambda_w : H^1(M_w, C_v) \longrightarrow H^1(M_w, E[p^\infty]).$$

Recall the commutative diagrams (3.3) and (5.1), and call

$$\delta_{v_n} : E((K_n)_{v_n}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow H^1((K_n)_{v_n}, E[p^\infty]) \quad \text{and}$$

$$\delta_\eta : E((K_\infty)_\eta) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow H^1((K_\infty)_\eta, E[p^\infty]).$$

Using two results of Greenberg ([7, 2.2] and [7, 2.4]) we have that

$$\mathrm{Im}(\delta_{v_n}) = \mathrm{Im}(\lambda_{v_n})_{\mathrm{div}} \quad \text{and} \quad \mathrm{Im}(\delta_\eta) = \mathrm{Im}(\lambda_\eta)$$

where $\mathrm{Im}(\lambda_{v_n})_{\mathrm{div}}$ is the divisible part of $\mathrm{Im}(\lambda_{v_n})$. These two facts hold since E has good ordinary reduction at v and since the inertia subgroup of v has finite index in $\Gamma = \mathrm{Gal}(K_\infty/K)$. Hence it can be easily seen that we can factor r_{v_n} as follows:

$$\begin{array}{ccc} H^1((K_n)_{v_n}, E[p^\infty])/\mathrm{Im}(\lambda_{v_n})_{\mathrm{div}} & \xrightarrow{a_{v_n}} & H^1((K_n)_{v_n}, E[p^\infty])/\mathrm{Im}(\lambda_{v_n}) \\ & \searrow^{r_{v_n}} & \downarrow{\scriptstyle b_{v_n}} \\ & & H^1((K_\infty)_\eta, E[p^\infty])/\mathrm{Im}(\lambda_\eta). \end{array}$$

Since a_{v_n} is surjective, we have that $|\ker(r_{v_n})| = |\ker(a_{v_n})| \cdot |\ker(b_{v_n})|$. Greenberg proved in [7, 2.5] that $|\ker(a_{v_n})| = |\tilde{E}(k_{v_n})[p^\infty]|$. Using the long exact sequence in cohomology, together with the restriction maps, we find the commutative diagram

$$\begin{array}{ccccccc} H^1((K_n)_{v_n}, C_v) & \xrightarrow{\lambda_{v_n}} & H^1((K_n)_{v_n}, E[p^\infty]) & \xrightarrow{\pi_{v_n}} & H^1((K_n)_{v_n}, \tilde{E}[p^\infty]) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle d_{v_n}} & & \\ H^1((K_\infty)_\eta, C_v) & \xrightarrow{\lambda_\eta} & H^1((K_\infty)_\eta, E[p^\infty]) & \xrightarrow{\pi_\eta} & H^1((K_\infty)_\eta, \tilde{E}[p^\infty]) & \longrightarrow & 0. \end{array}$$

The surjectivity of π_{v_n} follows from the following fact. From Poitou Tate duality (Theorem A.3.7) we have that $H^2(M, C_v)$ is the dual of the group $H^0(M, C_v^*) = \mathrm{Hom}_{G_{\bar{M}/M}}(C_v, \mu_{p^\infty})$ where M is any finite extension of K_v and μ_{p^∞} is the group of all p^n-th roots of unity for every n. The action of $G_{\bar{M}/M}$ on C_v and on $\tilde{E}[p^\infty]$ is given by two characters $G_{\bar{M}/M} \to \mathbb{Z}_p^\times$, say ψ for the action on C_v and ϕ for the action on $\tilde{E}[p^\infty]$. The Galois group also acts on the Tate module $T_p(E)$. Pick a basis P, Q for $T_p(E)$ with $P \in C_v$. Then the matrix for the action of $\sigma \in G_{\bar{M}/M}$ on $T_p(E)$ with respect to the basis P, Q must have the form

$$\begin{pmatrix} \psi(\sigma) & * \\ 0 & \phi(\sigma) \end{pmatrix}.$$

Thanks to Lemma 1.5.5 we obtain that $\psi\phi = \chi$, where χ is the cyclotomic character. Let m be the residue field of M. Since

$$\tilde{E}(m)[p^\infty] \subsetneq \tilde{E}[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p,$$

we have that $\phi \neq 1$, and so $\psi = \chi\phi^{-1} \neq \chi$. Since χ is the character related to the action of $G_{\bar{M}/M}$ on μ_{p^∞}, we obtain that C_v and μ_{p^∞} are not isomorphic as $G_{\bar{M}/M}$-modules. With a straight computation it's easy to see that this implies that there are no $G_{\bar{M}/M}$-equivariant morphisms between C_v and μ_{p^∞}, i.e. $\mathrm{Hom}_{G_{\bar{M}/M}}(C_v, \mu_{p^\infty}) = 0$. This proves the surjectivity of π_{v_n}. The surjectivity of π_η follows passing to the direct limit.

Thus we have that $\ker(b_{v_n}) = \ker(d_{v_n})$. Using the inflation-restriction sequence and Lemma A.3.6 we obtain that

$$\ker(d_{v_n}) \cong H^1\Big(\mathrm{Gal}((K_\infty)_\eta/(K_n)_{v_n}), \tilde{E}(k_\eta)[p^\infty]\Big) \cong \frac{\tilde{E}(k_\eta)[p^\infty]}{(\gamma_{v_n} - 1)\tilde{E}(k_\eta)[p^\infty]}$$

where γ_{v_n} is a topological generator of $\mathrm{Gal}((K_\infty)_\eta/(K_n)_{v_n})$. Since there exists an $N \in \mathbb{N}$ such that $k_{v_N} = k_\eta$, we have that k_η is finite, and so is $\tilde{E}(k_\eta)[p^\infty]$. Hence the kernel and the cokernel of $\gamma_{v_n} - 1$ have the same order, namely $|\tilde{E}(k_{v_n})[p^\infty]|$. This is the order of $\ker(d_{v_n})$. □

We are now able to prove Mazur's control theorem for an elliptic curve E/K with good ordinary reduction at every valuation of K lying over p and for the cyclotomic $\mathbb{Z}_p$-extension K_∞/K.

Proof of Theorem 5.2.1. Let Σ denote the set of nonarchimedean valuations of K that either lie over p or where E has bad reduction. If $v \notin \Sigma$ and v_n is a valuation of K_n lying over v, then $\ker(r_{v_n}) = 0$ thanks to Lemma 5.2.7. For every $v \in \Sigma$, Lemma 5.2.7 and Lemma 5.2.8 show that $|\ker(r_{v_n})|$ is bounded as n varies. Since Σ is finite and since the number of primes v_n lying above any nonarchimedean valuation v of K is bounded as n varies (see Lemma 2.4.7), we have that $|\ker(g_n)|$ is bounded as n varies.

Coming back to the sequence in (5.2), Lemma 5.2.3 implies that $\ker(s_n)$ is finite and has bounded order as n varies, no matter what type of reduction E has at any $v|p$. Lemma 5.2.4 and the fact that $|\ker(g_n)|$ is bounded as n varies show that $\mathrm{coker}(s_n)$ is finite and with bounded order as n varies, assuming that E has good ordinary reduction at every $v|p$. Therefore s_n has finite kernel and cokernel, with bounded order as n varies. □

5.3 The Iwasawa Main Conjecture

Let E/K be an elliptic curve with good ordinary reduction at every prime of K that lies over p. Using Mazur's Control Theorem it can be proven that $X_E(K_\infty) = \mathrm{Sel}_E(K_\infty)'_p$ is a finitely generated Λ-module, hence one can define its characteristic ideal $\xi_E(K_\infty) := \xi(X_E(K_\infty)) \subseteq \Lambda$. Let now $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Thanks to a result of Kato and Rohlrich we can say more on the structure of $X_E(\mathbb{Q}_\infty)$.

Theorem 5.3.1 (Kato-Rohlrich)**.** *Assume that $E/\mathbb{Q}$ has good ordinary reduction at p. Then $X_E(\mathbb{Q}_\infty)$ is finitely generated Λ-torsion.*

Proof. See [7, 1.5]. □

We are now ready to state the Iwasawa main conjecture for elliptic curves $E/\mathbb{Q}$ with good ordinary reduction at an odd prime p.

Conjecture 5.3.2. Let p be an odd prime and let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at p. Let $\xi_E(\mathbb{Q}_\infty) \subseteq \Lambda$ be the characteristic ideal of $X_E(\mathbb{Q}_\infty)$. Let also $\mathcal{L}_E \in \Lambda$ be the p-adic L-series associated to E defined in Section 4.9. Then

$$\xi_E(\mathbb{Q}_\infty) = (\mathcal{L}_E)$$

as ideals of Λ.

This conjecture was proved by Skinner and Urban in their article [25] under some other hypotheses. Before stating the main theorem of their paper, we introduce some notation.

We call

$$\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \longrightarrow T_p(E)$$

the action of $\mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q})$ on the p-adic Tate module of E, that is isomorphic to $\mathbb{Z}_p^2$. We also set

$$\bar{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \longrightarrow E[p]$$

the composition of $\rho_{E,p}$ with the natural projection $T_p(E) \to E[p]$. We call N_E the conductor of E (see Section 1.4). The main theorem in this setting, proved by Skinner and Urban, is the following.

Theorem 5.3.3. *Let $E/\mathbb{Q}$ be an elliptic curve. Assume that*

- *E has good ordinary reduction at p;*
- *$\bar{\rho}_{E,p}$ is irreducible;*
- *there exists a prime $q \neq p$ such that $q|N_E$, $q^2 \nmid N_E$ and $\bar{\rho}_{E,p}$ is ramified at q.*

Then $\xi_E(\mathbb{Q}_\infty) = (\mathcal{L}_E)$ in $\Lambda \otimes \mathbb{Q}_p$. If $\bar{\rho}_{E,p}$ is surjective, then this equality holds in Λ, i.e. the main conjecture holds for E.

Proof. See [25, 3.6.9]. □

An important consequence of this theorem is that when $E/\mathbb{Q}$ satisfies its hypotheses and has the property that $L(E,1) \neq 0$, then the p-adic Birch and Swinnerton-Dyer conjecture holds for E. We are going to deal with the proof of this fact in the next chapter, after a general introduction to the Birch and Swinnerton-Dyer conjecture.

Chapter 6

Applications to the Birch and Swinnerton-Dyer Conjecture

In this chapter we present the Birch and Swinnerton-Dyer conjecture for elliptic curves $E/\mathbb{Q}$ and look at an application of Theorem 5.3.3 to the proof of a particular case of this conjecture. We fix some notation that will be used throughout this chapter:

BSD	"Birch and Swinnerton-Dyer";
p	an odd prime of $\mathbb{Z}$;
K	a number field;
K_∞	the cyclotomic $\mathbb{Z}_p$-extension of K;
K_n	the intermediate field between K and K_∞ of degree p^n over K;
v	a valuation of K.

6.1 Néron-Tate height

In this section we give a summary of the theory of heights for an elliptic curve E/K. Our aim is to define the *elliptic regulator* associated to E, that is one of the invariants that appear in the formulation of the BSD conjecture.

Definition. Let $P \in \mathbb{P}^N(K)$ be a point with homogeneous coordinates

$$P = [x_0, \ldots, x_N], \quad x_0, \ldots, x_N \in K.$$

The *height of P (relative to K)* is

$$H_K(P) := \prod_v \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}$$

where v runs over the valuations of K, $n_v := [K_v : \mathbb{Q}_v]$ and $|\ |_v$ denotes the absolute value associated to the valuation v.

It can be proven that the height is well defined and satisfies $H_K(P) \geq 1$ (see [22, VII.5.4]). In order to cut the dependence on K, we define the *absolute height of* $P \in \mathbb{P}^N(K)$ to be

$$H(P) := H_K(P)^{1/[K:\mathbb{Q}]}.$$

We now use this function to define heights on elliptic curves.

Definition. Let E/K be an elliptic curve defined over a number field K and f a rational function on E, that can be seen as a morphism $E(\bar{K}) \to \mathbb{P}^1(\bar{K})$. We define the *height on E relative to f* to be

$$\begin{aligned} h_f : E(\bar{K}) &\longrightarrow \mathbb{R} \\ P &\longmapsto \log H(f(P)). \end{aligned}$$

From this quantity, that depends on the morphism f, we can define the *canonical height* for E, in order to loose the dependence on f.

Definition. Let f be a rational function on E/K. The function f is called *even* if $f \circ [-1] = f$.

Definition. The *canonical* (or *Néron-Tate*) *height on E/K*, denoted by $\hat{h}$, is the function

$$\begin{aligned} \hat{h} : E(\bar{K}) &\longrightarrow \mathbb{R} \\ P &\longmapsto \lim_{N\to\infty} \frac{4^{-N}}{\deg(f)} h_f([2^N]P) \end{aligned}$$

where f is any nonconstant rational even function on $E(\bar{K})$.

The limit that defines the canonical height exists and is independent on f (see [22, VIII.9.1]). In the next theorem we state the most important properties of $\hat{h}$.

Theorem 6.1.1 (Néron-Tate)**.** *Let E/K be an elliptic curve defined over a number field K and let $P, Q \in E(\bar{K})$.*

(a) $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.

(b) For every $m \in \mathbb{Z}$ we have $\hat{h}([m]P) = m^2\hat{h}(P)$.

(c) $\hat{h}$ is a quadratic form on E, i.e. $\hat{h}$ is an even function and the pairing

$$\begin{aligned} \langle \cdot, \cdot \rangle : E(\bar{K}) \times E(\bar{K}) &\longrightarrow \mathbb{R} \\ (P, Q) &\longmapsto \langle P, Q \rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \end{aligned}$$

is bilinear.

(d) $\hat{h}(P) \geq 0$ *and* $\hat{h}(P) = 0$ *if and only if P is a torsion point.*

Proof. See [22, VII.9.3]. □

The pairing defined in point (c) is usually called the *canonical* (or *Nèron-Tate*) *pairing on* E/K.

The Mordell-Weil theorem (see Corollary 3.2.5) implies that $E(K)$ is isomorphic as a group to

$$\mathbb{Z}^r \times E_{tors}(K)$$

with $r \geq 0$ and $E_{tors}(K)$ finite torsion group. Fix a basis $P_1, \ldots, P_r$ of the $\mathbb{Z}$-submodule of $E(K)$ isomorphic to $\mathbb{Z}^r$.

Definition. The *(elliptic) regulator* of E/K is the quantity

$$\mathrm{Reg}_E(K) := \det(\langle P_i, P_j \rangle)_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}$$

if $r > 0$. If $r = 0$ we set $\mathrm{Reg}_E(K) := 1$.

Remark 6.1.2. Point (d) of Theorem 6.1.1 implies that $\mathrm{Reg}_E(K)$ is never vanishing. We also have that $\mathrm{Reg}_E(K) > 0$.

6.2 The Birch and Swinnerton-Dyer conjecture

In this section we present the Birch and Swinnerton-Dyer conjecture for elliptic curves E defined over $\mathbb{Q}$. We give a summary of the tools we need for its statement.

1. It is possible to write a Weierstrass equation

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

   for E that is minimal with respect to any prime of $\mathbb{Z}$ (see Section 1.4 and [22, VIII.8]), and we call it a *global minimal Weierstrass equation* for E/K. We define the *real period* of E to be

   $$\Omega_E := \int_{E(\mathbb{R})} |\omega_E|$$

   where $\omega_E = dx/(2y + a_1x + a_3)$ is an invariant differential on E.

2. Let l be a prime of $\mathbb{Z}$. The *Tamagawa number* at l is defined to be

   $$c_l(E) := [E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]$$

   where $E_0(\mathbb{Q}_l)$ is the subgroup of $E(\mathbb{Q}_l)$ consisting in the points with nonsingular reduction at l. Thus, we have that $c_l(E) = 1$ if E has good reduction at l, i.e. if l does not divide the conductor N_E of E.

3. The regulator $\mathrm{Reg}_E(\mathbb{Q}) = \det(\langle P_i, P_j \rangle)_{\substack{1 \leq i \leq r \\ 1 \leq j \leq r}}$ defined in Section 6.1.

4. The *Shafarevich-Tate group* $Ш_E(\mathbb{Q})$ defined in Section 3.1.

5. The function $L(E,s)$ associated to an elliptic curve, defined in Section 1.6. Using the modularity theorem, stated in Section 4.8, we have that $L(E,s)$ is a holomorphic function defined on the whole $\mathbb{C}$.

We are now able to state the Birch and Swinnerton-Dyer conjecture. If $f:\mathbb{C}\to\mathbb{C}$ is a holomorphic function, we denote by $f^{(n)}(x)$ the n-th derivative of f computed in the point $x\in\mathbb{C}$. We also denote with $\mathrm{ord}_{X=x} f(X)$ the order of vanishing of f in $X=x$.

Conjecture 6.2.1 (Birch and Swinnerton-Dyer)**.** Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E, call r the $\mathbb{Z}$-rank of $E(\mathbb{Q})$.

1) ("Millenium problem") We have $\mathrm{ord}_{s=1} L(E,s)=r$.

2) (BSD) The group $Ш_E(\mathbb{Q})$ is finite and the following equality holds:

$$\frac{L^{(r)}(E,1)}{r!}=\frac{2^r\Omega_E\,\mathrm{Reg}_E(\mathbb{Q})|Ш_E(\mathbb{Q})|\prod_{l|N_E}c_l(E)}{|E(\mathbb{Q})_{tors}|^2}.$$

The principal way to study this conjecture is looking at its q-part for every prime q, i.e. studying the equation

$$(\mathrm{BSD})_q:\qquad \left|\frac{L^{(r)}(E,1)|E(\mathbb{Q})_{tors}|^2}{r!2^r\Omega_E\,\mathrm{Reg}_E(\mathbb{Q})\prod_{l|N_E}c_l(E)}\right|_q^{-1}=|Ш_E(\mathbb{Q})[q^\infty]|$$

where $|x|_q:=q^{-v(x)}$ for $x\in\mathbb{C}_p$ and v the q-adic valuation. It is clear that (BSD) is true if and only if $(\mathrm{BSD})_q$ is true for every prime q of $\mathbb{Z}$.

6.3 Greenberg's theorem

The aim of the following two sections is to present an application of Theorem 5.3.3 to the study of a particular case of the BSD conjecture. The main result we state is based on the following theorem, due to Greenberg, that we will prove in this section. Let E/K be an elliptic curve. If $a,b\in\mathbb{Q}_p^\times$ have the same p-adic valuation, we write $a\sim b$. We also set k_v to be the residue field of K_v and $\tilde{E}_v$ to be the reduction of E modulo v. We define $c_v^{(p)}$ to be the p-part of $c_v(E)=[E(K_v):E_0(K_v)]$, where $E_0(K_v)$ denotes the group of points defined over K_v with nonsingular reduction modulo v. Let $\Gamma:=\mathrm{Gal}(K_\infty/K)$ and γ a topological generator of Γ. Recall that $X_E(K_\infty):=\mathrm{Sel}_E(K_\infty)'_p$.

Theorem 6.3.1 (Greenberg)**.** *Let E be an elliptic curve defined over a number field K with good ordinary reduction at all primes of K lying over p. Let*

$f \in \Lambda$ be a generator of the characteristic ideal of $X_E(K_\infty)$. Assume also that $\mathrm{Sel}_E(K)_p$ is finite. Then

$$f(0) \sim \Big(\prod_{v \ bad} c_v^{(p)} \Big) \Big(\prod_{v|p} |\tilde{E}_v(k_v)[p^\infty]|^2 \Big) |\mathrm{Sel}_E(K)_p| / |E(K)[p^\infty]|^2$$

where in the first product v runs over the places of K of bad reduction for E, while in the second product v runs over the places of K that lie above p.

Definition. Let $\mathscr{P}$ be a property of Λ-modules. We say that a Λ-module S is *co-$\mathscr{P}$* if its Pontryagin dual S' satisfies the property $\mathscr{P}$.

Lemma 6.3.2. *Let S be a cofinitely generated, cotorsion discrete Λ-module. Let $f(T)$ be a generator of the characteristic ideal of $X := S' = \mathrm{Hom}(S, \mathbb{R}/\mathbb{Z})$. Then S^Γ is finite if and only if $f(0) \neq 0$. In this case, we also have that $S_\Gamma := S/TS$ is finite and $f(0) \sim |S^\Gamma|/|S_\Gamma|$.*

Proof. We have that $(S^\Gamma)' \cong X_\Gamma$ (see Lemma A.3.5) is finite if and only if S^Γ is so, using Pontryagin duality. Using Theorem 2.2.8, we obtain that X is pseudo-isomorphic to the direct sum of modules of the form

$$Y = \Lambda/(g(T))$$

with $g(T)$ a power of an irreducible distinguished polynomial in Λ. For each such Y, we have that

$$Y_\Gamma = Y/TY = \Lambda/(T, g(T)) = \mathbb{Z}_p/(g(0)).$$

Thus, Y_Γ is finite if and only if $g(0) \neq 0$. In this case, we also have that $Y^\Gamma = \ker(T : Y \to Y) = 0$, since $[h] \in \ker(T)$ if and only if $T[h] = 0$, if and only if $g(T)|Th(T)$, if and only if $g(T)|h(T)$, since $T \nmid g(T)$. From the facts that X is pseudo-isomorphic to a direct sum of elements of Y-type and that the characteristic polynomial is multiplicative (see Corollary 2.2.11), we have that X_Γ is finite if and only if $f(0) \neq 0$, and that in this case $X^\Gamma = \ker(T : X \to X)$ if finite. Since $X^\Gamma = (S_\Gamma)'$, we have also that S_Γ is finite.

Suppose now that S^Γ is finite. Using the long exact sequence in cohomology it's easy to see that the quantity

$$\frac{|S^\Gamma|}{|S_\Gamma|} = \frac{|X_\Gamma|}{|X^\Gamma|} = \frac{H^0(\Gamma, S)}{H^1(\Gamma, S)}$$

is multiplicative in exact sequences (it is the Euler characteristic). Since also the characteristic polynomial is multiplicative in exact sequences (see Corollary 2.2.11), it is enough to verify the statement when X is finite and when $X = \Lambda/(g(T))$. In the first case, since X is pseudo-isomorphic to 0, we

have that $f(T) = 1$ and $|X_\Gamma|/|X^\Gamma| = |X|/|X| = 1$. In the second case, we have that

$$\frac{|S^\Gamma|}{|S_\Gamma|} = \frac{|X_\Gamma|}{|X^\Gamma|} = |X_\Gamma| = p^{v_p(f(0))}$$

from the above remarks on Y, where v_p is the p-adic valuation. □

Corollary 6.3.3. *Let $K = \mathbb{Q}$ and $S = \mathrm{Sel}_E(\mathbb{Q}_\infty)_p$. Then $\mathrm{Sel}_E(\mathbb{Q})_p$ is finite if and only if $f(0) \neq 0$.*

Proof. From Theorem 5.3.1 we have that $X := X_E(\mathbb{Q}_\infty)$ is a finitely generated torsion Λ-module. From the previous lemma we have that $f(0) \neq 0$ if and only if $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p^\Gamma$ is finite. Using Mazur's Control Theorem (Theorem 5.2.1) we obtain that $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p^\Gamma$ is finite if and only if $\mathrm{Sel}_E(\mathbb{Q})_p$ is so. □

Referring to the diagram in (5.4), we will denote s_0, h_0 and g_0 simply by s, h and g.

Lemma 6.3.4. *Under the assumption of Theorem 6.3.1, we have*

$$|\mathrm{Sel}_E(K_\infty)_p^\Gamma| = |\mathrm{Sel}_E(K)_p||\ker(g)|/|E(K)[p^\infty]|$$

Proof. Using the finiteness of $\mathrm{Sel}_E(K)_p$, diagram (5.4) and Theorem 5.2.1, we find that

$$\frac{|\mathrm{Sel}_E(K_\infty)_p^\Gamma|}{|\mathrm{Sel}_E(K)_p|} = \frac{|\mathrm{coker}(s)|}{|\ker(s)|},$$

where all the groups occurring are finite. By Lemma 5.2.4, $\mathrm{coker}(h) = 0$. Thus, we have an exact sequence

$$0 \longrightarrow \ker(s) \longrightarrow \ker(h) \longrightarrow \ker(g) \longrightarrow \mathrm{coker}(s) \longrightarrow 0.$$

It follows that

$$\frac{|\mathrm{coker}(s)|}{|\ker(s)|} = \frac{|\ker(g)|}{|\ker(h)|}.$$

Using inflation-restriction and Proposition A.3.6 we find that

$$\ker(h) = H^1(\Gamma, E(K_\infty)[p^\infty]) = (E(K_\infty)[p^\infty])_\Gamma.$$

Using Theorem 5.2.2, we know that $E(K_\infty)[p^\infty]$ is finite, therefore the group $(E(K_\infty)[p^\infty])_\Gamma$ is finite and has the same cardinality of the group $(E(K_\infty)[p^\infty])^\Gamma = E(K)[p^\infty]$. □

We now skip to the study of $|\ker(g)|$. In Section 5.2 we saw that the behaviour of $\ker(g)$ can be studied by means of the maps

$$r_v : \mathcal{H}_E(K_v) \longrightarrow \mathcal{H}_E((K_\infty)_\eta)$$

where η is any valuation of K_∞ that lies over v. We also define the natural map

$$r : \mathcal{P}_E(K) \longrightarrow \mathcal{P}_E(K_\infty).$$

It will be necessary to replace $\mathcal{P}_E(*)$ with a much smaller group.

Definition. We call Σ the set of primes of K where E has bad reduction or which divide p or ∞.

By Lemma 5.2.7 we have that $\ker(r_v) = 0$ if $v \notin \Sigma$. We call

$$\mathcal{P}_E^{\Sigma}(K) := \prod_{v \in \Sigma} \mathcal{H}_E(K_v).$$

Clearly, $\ker(r) \subseteq \mathcal{P}_E^{\Sigma}(K)$ and $|\ker(r)| = \prod_v |\ker(r_v)|$ where again v runs over the primes of K in Σ.

Let $v \in \Sigma$. If $v|p$, then by Lemma 5.2.8 we have that

$$|\ker(r_v)| = |\tilde{E}_v(k_v)[p^{\infty}]|^2.$$

If v is archimedean, we saw in Section 5.2 that $\ker r_v = 0$. For $v \nmid p$ nonarchimedean, by analizing every possible type of reduction of E at v, it can be proven (see [7, pag. 24]) that $|\ker(r_v)| = c_v^{(p)}$. Therefore we obtain the following result.

Lemma 6.3.5. *Assume that E/K has good ordinary reduction at every prime $v|p$. Then*

$$|\ker(r)| \sim \Big(\prod_{v \ bad} c_v^{(p)} \Big) \Big(\prod_{v|p} |\tilde{E}_v(k_v)[p^{\infty}]|^2 \Big).$$

We clearly have that

$$\ker(g) = \ker(r) \cap \mathcal{G}_E(K).$$

Now, we want to define a subgroup of $\mathcal{G}_E(K)$ that still makes the above relation hold.

Definition. We define $\mathcal{G}_E^{\Sigma}(K) := \mathcal{G}_E(K) \cap \mathcal{P}_E^{\Sigma}(K)$. We define also

$$S_E^{\Sigma}(K) := \ker\Big(H^1(K, E(\bar{K})[p^{\infty}]) \to \prod_{v \notin \Sigma} \mathcal{H}_E(K_v) \Big)$$

Lemma 6.3.6. *With the above notation, we have that*

(a) $S_E^{\Sigma}(K) \cong H^1\Big(G_{K,\Sigma}, E(\bar{K})[p^{\infty}]\Big)$ *where* $G_{K,\Sigma} := \mathrm{Gal}(K_{\Sigma}, K)$, *with* K_{Σ} *the maximal extension of* K *unramified outside* Σ.

(b) $\mathcal{G}_E^{\Sigma}(K) = \mathrm{Im}\Big(S_E^{\Sigma}(K) \longrightarrow \mathcal{P}_E^{\Sigma}(K)\Big)$.

(c) $\mathrm{Sel}_E(K)_p = \ker\Big(S_E^{\Sigma}(K) \longrightarrow \mathcal{P}_E^{\Sigma}(K)\Big)$.

(d) $\ker(g) = \ker(r) \cap \mathcal{G}_E^{\Sigma}(K)$.

Proof. (a) Using Lemma 5.2.6, we have that $\mathcal{H}_E(K_v) = H^1(K_v, E(\bar{K}_v)[p^\infty])$ for every $v \notin \Sigma$. Fix $v \notin \Sigma$. Call $I_v \subseteq \mathrm{Gal}(\bar{K}/K)$ the inertia subgroup relative to v. Using the inflation-restriction sequence we have that the kernel of the restriction map $H^1(K_v, E(\bar{K}_v)[p^\infty]) \to H^1(I_v, E(\bar{K}_v)[p^\infty])$ is

$$B_v := H^1\Big(G_{\bar{K}_v/K_v}/I_v, (E(\bar{K}_v)[p^\infty])^{I_v}\Big).$$

Since $v \nmid p$, the reduction map $E \to \tilde{E}_v$ is an isomorphism on the p^n-torsion points for every n (see [22, VII.3.1]), hence

$$E(\bar{K}_v)[p^\infty] \cong \tilde{E}_v(\bar{k}_v)[p^\infty].$$

Let $P \in E(\bar{K}_v)[p^\infty]$ and $\sigma \in I_v$. Since σ acts trivially on $\tilde{E}_v$, we have that $\sigma(P)$ and P have the same image in $\tilde{E}_v$. It follows from the injectivity of the reduction map on $E(\bar{K}_v)[p^\infty]$ that $\sigma(P) = P$. This means that I_v acts trivially on $E(\bar{K}_v)[p^\infty]$, and so

$$(E(\bar{K}_v)[p^\infty])^{I_v} = E(\bar{K}_v)[p^\infty].$$

The group $G_{\bar{K}_v/K_v}/I_v$ is procyclic, since it is the Galois group of an extension of finite fields, and generated by the Frobenius ϕ. Since $v \nmid p$, from Proposition 2.4.3 and Lemma 2.4.7 we have that $G_{\bar{K}_v/K_v}/I_v$ contains a subgroup isomorphic to $\mathbb{Z}_p$. Since $E(\bar{K}_v)[p^\infty]$ is p-torsion, we obtain that

$$B_v = H^1\Big(G_{\bar{K}_v/K_v}/I_v, E(\bar{K}_v)[p^\infty]\Big) = \frac{E(\bar{K}_v)[p^\infty]}{(1-\phi)E(\bar{K}_v)[p^\infty]}.$$

Since $\ker(1-\phi) \cong \tilde{E}_v(k_v)[p^\infty]$ is finite and $E(\bar{K}_v)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$, applying Proposition A.3.6 we have that $B_v = 0$.

This fact means that, for such v, vanishing in $H^1(K_v, E(\bar{K}_v)[p^\infty])$ is equivalent to vanishing in $H^1(I_v, E(\bar{K}_v)[p^\infty])$, i.e. we have that

$$S_E^\Sigma(K) = \ker\Big(H^1(K, E(\bar{K})[p^\infty]) \to \prod_{v \notin \Sigma} H^1(I_v, E(\bar{K}_v)[p^\infty])\Big).$$

Therefore, $\xi \in S_E^\Sigma(K)$ if and only if its restriction to I_v is a coboundary for every $v \notin \Sigma$. Since I_v acts trivially on $E(\bar{K}_v)[p^\infty]$, this is the same as asking that ξ is zero on the closure H of the subgroup of $G_{\bar{K}/K}$ generated by every inertia I_v, with v varying outside Σ. The field corresponding to H is exactly K_Σ, that is a normal extension of K since it is the maximal extension unramified outside Σ. Hence, using the inflation-restriction sequence, we have that

$$\begin{aligned} S_E^\Sigma(K) &= \ker\Big(H^1(K, E(\bar{K})[p^\infty]) \to H^1(K_\Sigma, E(\bar{K})[p^\infty])\Big) \cong \\ &\cong H^1(G_{K,\Sigma}, E(\bar{K})[p^\infty]). \end{aligned}$$

(b) By definition, we have that

$$\begin{aligned}\mathcal{G}_E^\Sigma(K) &= \mathrm{Im}\left(H^1(K, E(\bar{K})[p^\infty]) \longrightarrow \mathcal{P}_E(K)\right) \cap \mathcal{P}_E^\Sigma(K) = \\ &= \mathrm{Im}\left(\ker\left(H^1(K, E(\bar{K})[p^\infty]) \to \prod_{v\notin\Sigma} \mathcal{H}_E(K_v)\right) \longrightarrow \mathcal{P}_E^\Sigma(K)\right) = \\ &= \mathrm{Im}\left(S_E^\Sigma(K) \longrightarrow \mathcal{P}_E^\Sigma(K)\right).\end{aligned}$$

(c) By definition, we have that

$$\begin{aligned}\mathrm{Sel}_E(K)_p &= \ker\left(H^1(K, E(\bar{K})[p^\infty]) \longrightarrow \mathcal{P}_E(K)\right) = \\ &= \ker\left(\ker\left(H^1(K, E(\bar{K})[p^\infty]) \to \prod_{v\notin\Sigma} \mathcal{H}_E(K_v)\right) \longrightarrow \mathcal{P}_E^\Sigma(K)\right) = \\ &= \ker\left(S_E^\Sigma(K) \longrightarrow \mathcal{P}_E^\Sigma(K)\right).\end{aligned}$$

(d) Since $\ker(r) \subseteq \mathcal{P}_E^\Sigma(K)$, we have that

$$\ker(g) = \ker(r) \cap \mathcal{G}_E(K) = \ker(r) \cap \mathcal{G}_E(K) \cap \mathcal{P}_E^\Sigma(K) = \ker(r) \cap \mathcal{G}_E^\Sigma(K).$$

□

With the same argument one can also define $\mathcal{G}_E^\Sigma(K_n)$ and $S_E^\Sigma(K_n)$ for every $n \in \mathbb{N}$ and prove the same lemma with K_n in place of K, *mutatis mutandis*. We state now a theorem of Cassels that will be useful in the sequel.

Theorem 6.3.7 (Cassels)**.** *With the above notation, if* $\mathrm{Sel}_E(K_n)_p$ *is finite we have a group isomorphism*

$$\mathcal{P}_E^\Sigma(K_n)/\mathcal{G}_E^\Sigma(K_n) \cong E(K_n)[p^\infty]$$

for every $n \in \mathbb{N}$.

Proof. See [7, 4.13]. □

We can now define $\mathcal{P}_E^\Sigma(K_\infty)$. Take $v \in \Sigma$. For any $v \in \Sigma$ we define

$$\mathcal{P}_E^{(v)}(K_\infty) = \varinjlim_{n\in\mathbb{N}} \mathcal{P}_E^{(v)}(K_n)$$

where $\mathcal{P}_E^{(v)}(K_n) = \prod_{v_n|v} \mathcal{H}((K_n)_{v_n})$. If v is archimedean, for every $v_n|v$ we know from Lemma 5.2.6 that $\mathcal{H}_E((K_n)_{v_n}) = H^1((K_n)_{v_n}, E[p^\infty])$. Since $p \neq 2$, it is clear that $H^1((K_n)_{v_n}, E[p^\infty]) = 0$, hence $\mathcal{P}_E^{(v)}(K_\infty) = 0$. If v is nonarchimedean, it is finitely decomposed in K_∞ (see Lemma 2.4.7) and so

$$\mathcal{P}_E^{(v)}(K_\infty) = \prod_{\eta|v} \mathcal{H}_E((K_\infty)_\eta)$$

where η runs over the places of K_∞ lying over v. Finally, we define

$$\mathcal{P}_E^\Sigma(K_\infty) := \prod_{v\in\Sigma} \mathcal{P}_E^{(v)}(K_\infty).$$

Taking the direct limit on $n \in \mathbb{N}$ of the maps that characterize $\mathcal{G}_E^\Sigma(K_n)$ and $S_E^\Sigma(K_n)$ in points (b) and (c) of Lemma 6.3.6 (with K_n in place of K), we are able to define a morphism

$$\psi : H^1(\mathrm{Gal}(K_\Sigma, K_\infty), E(\bar{K})[p^\infty]) \longrightarrow \mathcal{P}_E^\Sigma(K_\infty).$$

Lemma 6.3.8. *Assume that* $\mathrm{Sel}_E(K_\infty)_p$ *is* Λ*-cotorsion. Then we have an exact sequence*

$$0 \longrightarrow \mathrm{Sel}_E(K_\infty)_p \longrightarrow H^1\big(\mathrm{Gal}(K_\Sigma/K_\infty), E(\bar{K})[p^\infty]\big) \xrightarrow{\psi} \mathcal{P}_E^\Sigma(K_\infty) \longrightarrow 0.$$

Proof. The fact that $\mathrm{Sel}_E(K_\infty)_p$ is the kernel of ψ follows from point (c) of Lemma 6.3.6, taking the direct limit on K_n.

In order to show that ψ is surjective, the idea is to prove that $\mathrm{Im}(\psi)$ is a Λ-submodule of $\mathcal{P}_E^\Sigma(K_\infty)$ with finite index and that any such Λ-submodule must be the whole $\mathcal{P}_E^\Sigma(K_\infty)$. We will explain the last point first. Let $v \in \Sigma$ be a nonarchimedean valuation. From Lemma 2.4.7 we know that the decomposition group of v in K_∞ has finite index in Γ. This means that, chosen an extension η of v on K_∞, we have that $\mathrm{Gal}((K_\infty)_\eta/K_v) \cong \mathbb{Z}_p$. From a result in Galois cohomology (see Theorem A.3.4) we have that $\mathrm{Gal}(\bar{K}_v/(K_\infty)_\eta)$ has p-cohomological dimension 1. This means (see Lemma A.3.3) that $H^1\big((K_\infty)_\eta, E(\bar{K}_v)[p^\infty]\big)$ is divisible. This implies that every factor of $\mathcal{P}_E^\Sigma(K_\infty)$ is divisible, and hence $\mathcal{P}_E^\Sigma(K_\infty)$ itself is divisible. Therefore it has not proper subgroups of finite index (otherwise the quotient would be finite and divisible).

The proof of the fact that $\mathrm{Im}\,\psi$ has finite index in $\mathcal{P}_E^\Sigma(K_\infty)$ involves the theory of Selmer groups for twisted modules, hence we just give an idea of it with the simplifying assumption that $\mathrm{Sel}_E(K_n)_p$ is finite for every $n \geq 0$. For the complete proof see [7, 4.6]. By Cassels theorem (Theorem 6.3.7) we have that the cokernel of the map

$$\psi_n : H^1\big(\mathrm{Gal}(K_\Sigma/K_n), E(\bar{K})[p^\infty]\big) \longrightarrow \mathcal{P}_E^\Sigma(K_n)$$

is isomorphic to $E(K_n)[p^\infty]$. But we know that $|E(K_n)[p^\infty]|$ is bounded since $E(K_\infty)[p^\infty]$ is finite by Mazur's theorem (Theorem 5.2.2). Since clearly $\psi = \varinjlim_n \psi_n$, we have that $\mathrm{coker}\,\psi$ is finite. □

Lemma 6.3.9. *Under the assumptions of Theorem 6.3.1, we have that*

$$|\ker(g)| = |\ker(r)||(\mathrm{Sel}_E(K_\infty)_p)_\Gamma|/|E(K)[p^\infty]|.$$

Proof. Call $G^{\Sigma}_{K_\infty} := \mathrm{Gal}(K_\Sigma/K_\infty)$ and $G^{\Sigma}_{K} := \mathrm{Gal}(K_\Sigma/K)$. Set also $E[p^\infty] := E(\bar{K})[p^\infty]$. From the exact sequence of Lemma 6.3.8, we obtain the long exact sequence

$$H^1\big(G^{\Sigma}_{K_\infty}, E[p^\infty]\big)^\Gamma \longrightarrow \mathcal{P}^{\Sigma}_E(K_\infty)^\Gamma \longrightarrow (\mathrm{Sel}_E(K_\infty)_p)_\Gamma \longrightarrow H^1\big(G^{\Sigma}_{K_\infty}, E[p^\infty]\big)_\Gamma.$$

It can be proven that the last term is zero (see [7, Appendix to Section 4]). Thus, we get the following commutative diagram with exact rows and columns.

$$\begin{array}{ccccccc}
H^1(G^{\Sigma}_{K}, E[p^\infty]) & \xrightarrow{\psi_0} & \mathcal{P}^{\Sigma}_E(K) & \longrightarrow & \mathcal{P}^{\Sigma}_E(K)/\mathcal{G}^{\Sigma}_E(K) & \longrightarrow & 0 \\
\downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle r} & & \downarrow & & \\
H^1(G^{\Sigma}_{K_\infty}, E[p^\infty])^\Gamma & \xrightarrow{\tilde{\psi}} & \mathcal{P}^{\Sigma}_E(K_\infty)^\Gamma & \longrightarrow & (\mathrm{Sel}_E(K_\infty)_p)_\Gamma & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & &
\end{array}$$

The first row is exact by definition of $\mathcal{G}^{\Sigma}_E(K)$, the second is exact from the remark above. The first and the second vertical arrows are the natural restriction maps, the last vertical arrow is defined by diagram chasing. Using the five terms cohomology sequence and the fact that Γ has p-cohomological dimension 1, we obtain the surjectivity of the first vertical arrow. In order to show the surjectivity of r, we must consider each $v \in \Sigma$ separately, showing that $\mathcal{P}^{(v)}_E(K) \longrightarrow \mathcal{P}^{(v)}_E(K_\infty)^\Gamma$ is surjective. In order to do this, we consider K_n to be the greatest subfield of K_∞ on which v splits completely. It is easy to see that we have an isomorphism $\mathcal{P}^{(v)}_E(K) \longrightarrow \mathcal{P}^{(v)}_E(K_n)^{\Gamma_n}$, since $K_v = (K_n)_{v_n}$ for every extension v_n of v on K_n. Then, since clearly v_n does not split in K_∞, we consider the maps r_{v_n} defined is equation (5.5) if $v \nmid p$ and the maps d_{v_n} defined in the proof of Lemma 5.2.8. Since $\mathrm{Gal}((K_\infty)_\eta, (K_n)_{v_n}) \cong \Gamma$ has p-cohomological dimension 1, using the five terms cohomology sequence we have that r_{v_n} and d_{v_n} are surjective onto the Γ-invariants of their codomain, hence r is surjective. The surjectivity of the third vertical arrow follows by diagram chasing. It is also clear that $\mathrm{Im}(\psi_0)$ is mapped surjectively to $\mathrm{Im}(\tilde{\psi})$. We then obtain the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{G}^{\Sigma}_E(K) & \xrightarrow{\psi_0} & \mathcal{P}^{\Sigma}_E(K) & \longrightarrow & \mathcal{P}^{\Sigma}_E(K)/\mathcal{G}^{\Sigma}_E(K) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle t} & & \\
0 & \longrightarrow & \mathrm{Im}(\tilde{\psi}) & \longrightarrow & \mathcal{P}^{\Sigma}_E(K_\infty)^\Gamma & \longrightarrow & (\mathrm{Sel}_E(K_\infty)_p)_\Gamma & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

From the snake lemma, we then obtain $0 \to \ker(g) \to \ker(r) \to \ker(t) \to 0$. Thus, $|\ker(g)| = |\ker(r)|/|\ker(t)|$. We also have that

$$|\ker(t)| = \frac{|\mathcal{P}_E^\Sigma(K)/\mathcal{G}_E^\Sigma(K)|}{|(\mathrm{Sel}_E(K_\infty)_p)_\Gamma|}.$$

Applying Cassels theorem (Theorem 6.3.7) we obtain that

$$|\ker(g)| = \frac{|\ker(r)||(\mathrm{Sel}_E(K_\infty)_p)_\Gamma|}{|E(K)[p^\infty]|}.$$

□

Proof of Theorem 6.3.1. Let $S := \mathrm{Sel}_E(K_\infty)_p$. Since $\mathrm{Sel}_E(K)_p$ if finite, using Mazur's control theorem we see that S^Γ is finite. Using Pontryagin duality, we have that $X := S'$ has the property that

$$(S^\Gamma)' = X_\Gamma = X/TX$$

is finite. Using a version of Nakayama's lemma for Λ-modules (see [26, 13.16]), this implies that X is a finitely generated Λ-module. It is also easy to see that if X/TX is finite, the torsion-free part of the elementary module (described in Theorem 2.2.8) pseudo-isomorphic to X is zero. Therefore X is a torsion Λ-module. Hence we can apply Lemma 6.3.2 to find that

$$f(0) \sim \frac{|\mathrm{Sel}_E(K_\infty)_p^\Gamma|}{|(\mathrm{Sel}_E(K_\infty)_p)_\Gamma|}.$$

Using Lemma 6.3.4, Lemma 6.3.5 and Lemma 6.3.9 we obtain the claim. □

6.4 An application of the Iwasawa main conjecture to the BSD

Greenberg's theorem was first published (in [7]) in 1998, before the proof of Theorem 5.3.3, that was presented in the article [25] by Skinner and Urban. In this article they point out that, combining Greenberg's theorem with their result about the Iwasawa main conjecture, they are able to give an easy proof of a particular case of the p-part of the BSD. We prove now the main result. Recall that, if E is defined over $\mathbb{Q}$, we have the representations $\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \to T_p(E)$ and $\bar{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \to E[p]$ defined in Section 5.3. We call $|\ |_p$ the p-adic absolute value on $\mathbb{C}_p$.

Theorem 6.4.1. *Let $E/\mathbb{Q}$ an elliptic curve with conductor N_E. Assume that*

- *E has good ordinary reduction at p;*

- $\bar{\rho}_{E,p}$ *is surjective;*
- *there exists a prime* $q \neq p$ *such that* $q|N_E$, $q^2 \nmid N_E$ *and* $\bar{\rho}_{E,p}$ *is ramified at* q.

If $L(E,1) \neq 0$, *then*

$$\left|\frac{L(E,1)}{\Omega_E}\right|_p^{-1} = |Ш_E(\mathbb{Q})[p^\infty]| \cdot \prod_{l|N_E} c_l^{(p)},$$

i.e. the $(BSD)_p$ *holds.*

Proof. From Theorem 5.3.3 we have that, under these hypotheses, the characteristic ideal of the dual of $\mathrm{Sel}_E(\mathbb{Q}_\infty)_p$ is generated by the p-adic L-series $\mathcal{L}_E$. Let α and β be the roots of $X^2 - a_p X + p$, where $a_p = p + 1 - |\tilde{E}(\mathbb{F}_p)|$, such that α has valuation 0 and β has valuation 1. From Corollary 4.9.4 we obtain that

$$1(\mathcal{L}_E) = \mathcal{L}_E(0) = \left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E,1)}{\Omega^+_{f_E}}, \tag{6.1}$$

where f_E is the normalized Hecke eigenform corresponding to E by modularity theorem. Remember that the invariant $\Omega^+_{f_E}$ was well defined up to multiplication by an element of $\mathbb{Z}_p^\times$. A deep result about periods of elliptic curves (see [9, Section 3]) tells us that in our case we can choose $\Omega^+_{f_E}$ to be equal to Ω_E.

Since by hypothesis $L(E,1) \neq 0$, we have that $\mathcal{L}_E(0) \neq 0$. We can hence use Corollary 6.3.3 to obtain that $\mathrm{Sel}_E(\mathbb{Q})_p$ is finite, therefore we can apply Greenberg's theorem 6.3.1 with $f = \mathcal{L}_E$. We have that

$$\left|\left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E,1)}{\Omega_E}\right|_p^{-1} = \left(\prod_{l|N_E} c_v^{(p)}\right) |\mathrm{Sel}_E(\mathbb{Q})_p| \left|\frac{|\tilde{E}(\mathbb{F}_p)|^2}{|E(\mathbb{Q})[p^\infty]|^2}\right|_p^{-1}.$$

Since $|\tilde{E}(\mathbb{F}_p)| = (1-\alpha)(1-\beta)$, we have that the term

$$\left(1 - \frac{1}{\alpha}\right)^{-2} (1-\alpha)^2 (1-\beta)^2 = \alpha^2 (1-\beta)^2$$

has p-adic norm equal to 1, hence equation (6.4) simplifies in

$$\left|\frac{L(E,1)}{\Omega_E}\right|_p^{-1} = \left(\prod_{l|N_E} c_v^{(p)}\right) |\mathrm{Sel}_E(\mathbb{Q})_p| \left|\frac{1}{|E(\mathbb{Q})[p^\infty]|^2}\right|_p^{-1}.$$

From Proposition 3.4.2 we have the exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes_{\mathbb{Z}} \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow \mathrm{Sel}_E(\mathbb{Q})_p \longrightarrow Ш_E(\mathbb{Q})[p^\infty] \longrightarrow 0.$$

The fact that $\mathrm{Sel}_E(\mathbb{Q})_p$ is finite implies that the divisible group $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$ is finite, hence it is 0. Therefore $|\mathrm{Sel}_E(\mathbb{Q})_p| = |Ш_E(\mathbb{Q})[p^\infty]|$.

We also have that $E(\mathbb{Q})$ does not have any nontrivial p-torsion elements. Indeed, if there exists a point $P \in E(\mathbb{Q}) \setminus \{O\}$ such that $pP = O$, then we could take a basis for the $\mathbb{Z}/p\mathbb{Z}$-module $E(\bar{\mathbb{Q}})[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ made by P, Q for some $Q \in E(\bar{\mathbb{Q}})[p]$. Since $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts surjectively on $E(\bar{\mathbb{Q}})[p]$, there must be a $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(P) = Q$, but this is impossible since $\sigma(P) = P$ for every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. This means that there are no nontrivial p-torsion points in $E(\mathbb{Q})$, hence the theorem follows. □

Appendix A

Group cohomology

In this appendix we discuss the basic properties of profinite group cohomology that are used throughout this thesis. We mainly follow [22, Appendix B], [27, 9-10] and [18, 1].

A.1 Profinite group cohomology (H^0 and H^1)

In this secton we present naively the first cohomology groups defined by a continous action of a profinite group on an abelian group. We will denote by G the profinite group and by M the abelian group on which G acts.

Definition. Let G be a group and M be an abelian group. A *(left) action* of G on M is a map $\phi : G \times M \to M$ such that

1. $\phi(\sigma, m + m') = \phi(\sigma, m) + \phi(\sigma, m')$ for every $\sigma \in G$ and $m, m' \in M$.
2. $\phi(\sigma\tau, m) = \phi(\sigma, \phi(\tau, m))$ for every $\sigma, \tau \in G$ and $m \in M$.
3. $\phi(1_G, m) = m$ for every $m \in M$.

We will always denote $\phi(\sigma, m)$ as $\sigma(m)$.

Definition. Let G be a profinite group. A *(discrete) G-module* is an abelian group M on which G acts such that the action is continous for the profinite topology on G and the discrete topology on M. This means that the map

$$\begin{aligned} G \times M &\longrightarrow M \\ (\sigma, m) &\longmapsto \sigma(m) \end{aligned}$$

is continous, or equivalently that for every $m \in M$ the *stabilizer* of m

$$\mathrm{Stab}_G(m) := \{ \sigma \in G \ : \ \sigma(m) = m \}$$

is an open normal subgroup of G.

Example A.1.1. Here we give two important examples of discrete G-modules.

(a) Let K be a perfect field and $\bar{K}$ an algebraic closure of K. Then the Galois group $G_{\bar{K}/K}$ is a profinite group, and it acts continously for example on $(\bar{K},+)$ and $(\bar{K}^\times,\cdot)$, since for any $x \in \bar{K}$ the extension $K(x)/K$ is finite, so the stabilizer of x is closed and of finite index in $G_{\bar{K}/K}$, hence it is open. Therefore we have that $\bar{K}$ and $\bar{K}^\times$ are discrete $G_{\bar{K}/K}$-modules.

(b) Let E/K be an elliptic curve. In Remark 1.1.6 we have seen that $G_{\bar{K}/K}$ acts on $E(\bar{K})$, and the action is continous since the coordinates of any fixed point of $E(\bar{K})$ generate a finite extension of K.

Definition. Let M and N be G-modules. A *G-module homomorphism* is a homomorphism of abelian groups $\phi : M \to N$ commuting with the action of G, i.e.

$$\phi(\sigma(m)) = \sigma(\phi(m))$$

for every $m \in M$ and for every $\sigma \in G$.

We define now the 0^{th} and the 1^{st} cohomology group for a G-module, with G profinite group.

Definition. The *0^{th} cohomology group of the G-module M* is the subgroup of M made of the G-invariant elements, i.e.

$$H^0(G,M) := M^G = \{m \in M \ : \ \sigma(m) = m \text{ for every } \sigma \in G\}.$$

Example A.1.2. Coming back to the above examples, we obtain that $H^0(G_{\bar{K}/K},\bar{K}) = K$, $H^0(G_{\bar{K}/K},\bar{K}^\times) = K^\times$ and $H^0(G_{\bar{K}/K},E(\bar{K})) = E(K)$.

Definition. Let M be a discrete G-module. The *group of continous cocycles from G to M* (or *continous crossed homomorphisms*), denoted by $Z^1(G,M)$, is the group of continous maps $\xi : G \to M$ satisfying the cocycle condition

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

for every $\sigma,\tau \in G$.

Definition. Let M be a G-module. The *group of coboundaries*, denoted $B^1(G,M)$ is the group of maps $\xi : G \to M$ that are of the type

$$\sigma \longmapsto \sigma(m) - m$$

for some $m \in M$.

Remark A.1.3. One can easily check that $B^1(G,M) \subseteq Z^1(G,M)$ and that every map in $B^1(G,M)$ is automatically continous with respect to the profinite topology on G and the discrete topology on M.

Definition. We define the 1^{st} *cohomology group of the G-module M* as the quotient group

$$H^1(G,M) := \frac{Z^1(G,M)}{B^1(G,M)}.$$

Remark A.1.4. Notice that if G acts trivially on M we have $H^0(G,M) = M$ and

$$H^1(G,M) = \mathrm{Hom}_{cont}(G,M).$$

This last equality is true since in the case G acts trivially on M then $B_1(G,M) = 0$ and crossed homomorphism are homomorphisms.

Proposition A.1.5. *For any exact sequence of G-modules*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0,$$

with f, g two G-module homomorphisms, there exists a canonical long exact sequence

$$\begin{array}{l} 0 \longrightarrow H^0(G,M) \xrightarrow{f} H^0(G,N) \xrightarrow{g} H^0(G,P) \xrightarrow{\delta} \\ \quad H^1(G,M) \xrightarrow{f_*} H^1(G,N) \xrightarrow{g_*} H^1(G,P) \end{array}$$

where the connecting morphism *δ is defined as follows: consider any element $p \in H^0(G,P) = P^G$, choose an $n \in N$ such that $g(n) = p$ and define a function $\xi : G \to N$ such that*

$$\xi(\sigma) = \sigma(n) - n.$$

The values of ξ are in $\ker g = \mathrm{Im}\, f$*, hence there exist $\zeta : G \to M$ such that $f \circ \zeta = \xi$. We have that $\zeta \in Z^1(G,M)$, so we can define $\delta(p)$ to be the cohomology class in $H^1(G,P)$ of ζ.*

Proof. See [27, 9.3.3]. □

A.2 Profinite group cohomology (H^n)

The specific construction of the previous section for H^0 and H^1 can be generalized in order to construct cohomology groups H^n for $n > 1$. For this section we fix G a profinite group and M a discrete G-module.

Definition. We define the abelian group of *n-cochains* $C^n(G,M)$ to be the group of continous functions from G^n to M. For $n > 1$ we define homomorphisms $\partial_n : C^{n-1}(G,M) \to C^n(G,M)$ by

$$\begin{aligned}(\partial_n f)(\sigma_1,\ldots,\sigma_n) :=& \sigma_1(f(\sigma_2,\ldots,\sigma_n)) + \sum_{i=1}^{n-1}(-1)^i f(\sigma_1,\ldots,\sigma_i\sigma_{i+1},\ldots,\sigma_n) + \\ &+ (-1)^n f(\sigma_1,\ldots,\sigma_{n-1}).\end{aligned}$$

When $n = 0$ we have $G^0 = 1$ and we define $C^0(G, M) := M$. For $n = 1$ we define $\partial_1 : C^0(G, M) \to C^1(G, M)$ by

$$(\partial_1 m)(\sigma) := \sigma(m) - m$$

for $m \in M$. We also define ∂_0 to be the zero map from 0 to $C^0(G, M)$.

Lemma A.2.1. *$\partial_{n+1} \circ \partial_n : C^{n-1}(G, M) \to C^{n+1}(G, M)$ is the zero map for every $n > 0$.*

Definition. The groups of *n-coboundaries* and *n-cocycles* are defined respectively to be $B^n(G, M) := \operatorname{Im} \partial_n$ and $Z^n(G, M) := \ker \partial_{n+1}$.

Definition. The n-th cohomology group of the G-module M is

$$H^n(G, M) := \frac{Z^n(G, M)}{B^n(G, M)}.$$

Definition. Let K be a perfect field, $\bar{K}$ an algebraic closure of K and M a $G_{\bar{K}/K}$-module. In this case, we set $H^n(K, M) := H^n(G_{\bar{K}/K}, M)$.

Definition. Let G_1 and G_2 be profinite groups, let M_1 be a G_1-module and M_2 be a G_2-module. Consider $\theta : G_1 \to G_2$ and $\phi : M_2 \to M_1$ be continous homomorphisms. The pair (θ, ϕ) is called *compatible* if we have $\phi(\theta(\sigma_1)(m_2)) = \sigma_1(\phi(m_2))$ for every $\sigma_1 \in G_1$ and $m_2 \in M_2$.

Lemma A.2.2. *Let $\theta : G_1 \to G_2$ and $\phi : M_2 \to M_1$ be a compatible pair. Then for every $n \geq 0$ there is an induced morphism*

$$\begin{aligned} H^n(G_2, M_2) &\longrightarrow H^n(G_1, M_1) \\ \xi + B^n(G_2, M_2) &\longmapsto (\theta, \phi)^* \xi + B^n(G_1, M_1) \end{aligned}$$

where $((\theta, \phi)^* \xi)(\sigma_1, \ldots, \sigma_n) := \phi(\xi(\theta\sigma_1, \ldots, \theta\sigma_n))$ for every $\sigma_1, \ldots, \sigma_n \in G_1$.

Proof. See [27, 9.2.1]. □

Now we present two important morphisms induced by compatible pairs, and we study some exact sequences related to them.

Definition. Let G be a profinite group, M a G-module and H a closed subgroup of G. Then M is also an H-module. Consider the inclusion map $j : H \to G$. Then the pair of maps (j, id_M) is compatible, and so there are induced maps, called *restriction maps*, defined by

$$\begin{aligned} \mathrm{Res} : H^n(G, M) &\longrightarrow H^n(H, M) \\ [\xi] &\longmapsto [\xi|_{H^n}]. \end{aligned}$$

Definition. Let G be a profinite group, M a G-module and H a normal closed subgroup of G. Then the module M^H has a natural structure as a G/H-module. Denote by $q : G \to G/H$ the quotient map, and $j : M^H \to M$ the inclusion map. Then the pair (q, j) is compatible and so there are induced maps, called *inflation maps*, defined by

$$\begin{aligned} \mathrm{Inf} : H^n(G/H, M^H) &\longrightarrow H^n(G, M) \\ [\xi] &\longmapsto [j\xi\tilde{q}] \end{aligned}$$

where $\tilde{q} : G^n \to (G/H)^n$ is induced by q.

Proposition A.2.3 (Inflation-Restriction sequence)**.** *Let M be a G-module and let H be a closed normal subgroup of G. Then the following sequence is exact:*

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

Proof. See [22, B.1.3] or [27, 10.2.3]. □

Let now M be a discrete G-module, with G profinite group, and let H be a normal closed subgroup of G. Fix $\sigma \in G$. Define

$$\begin{aligned} \theta_\sigma : H &\longrightarrow H \\ \tau &\longmapsto \sigma^{-1}\tau\sigma. \end{aligned}$$

and

$$\begin{aligned} \phi_\sigma : M &\longrightarrow M \\ m &\longmapsto \sigma(m). \end{aligned}$$

It can be easily checked that the pair $(\theta_\sigma, \phi_\sigma)$ is a compatible pair. Call $\bar{\sigma} := (\theta_\sigma, \phi_\sigma)^* + B^n(H, M)$ the induced morphism between n-th cohomology groups.

Lemma A.2.4. *(a) For any $\sigma_1, \sigma_2 \in G$ we have $\overline{\sigma_1\sigma_2} = \bar{\sigma}_1\bar{\sigma}_2$ and $\bar{1}$ is the identity map.*

(b) For any $\sigma \in G$ and $n \geq 0$ the morphism

$$\begin{aligned} G \times H^n(H, M) &\longrightarrow H^n(H, M) \\ (\sigma, \xi) &\longmapsto \bar{\sigma}(\xi) \end{aligned}$$

is continous, hence $H^n(H, M)$ is a discrete G-module.

(c) If $\sigma \in H$ then $\bar{\sigma}$ is the identity map, hence $H^n(H, M)$ is a discrete G/H-module.

(d) The image of $\mathrm{Res} : H^n(G, M) \to H^n(H, M)$ is in $H^n(H, M)^{G/H}$.

Proof. See [27, 10.2.4]. □

The exact sequence in A.2.3 can be extended to a longer exact sequence with five terms.

Proposition A.2.5. *Let M be a G-module and H a closed normal subgroup of G. There is an exact sequence*

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)^{G/H} \hookrightarrow H^2(G/H, M^H) \xrightarrow{\text{Inf}} H^2(G, M).$$

Proof. See [27, 10.3.1]. □

The long exact sequence in cohomology of Proposition A.1.5 can be extended in order to involve the higher degree cohomology groups.

Proposition A.2.6. *For any exact sequence of G-modules*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0,$$

with f, g two G-module homomorphisms, there exists a canonical long exact sequence that extends the exact sequence of Proposition A.1.5

$$\ldots \longrightarrow H^n(G, M) \longrightarrow H^n(G, N) \longrightarrow H^n(G, P) \hookrightarrow H^{n+1}(G, M) \longrightarrow H^{n+1}(G, N) \longrightarrow H^{n+1}(G, P) \longrightarrow \ldots$$

for every $n \in \mathbb{N}$.

We end this section with an important result about the behaviour of cohomology groups with direct and inverse limits.

Proposition A.2.7. *Let $\{G_i\}_{i\in I}$ be an inverse system of profinite groups, $\{M_i\}_{i\in I}$ be a direct system with M_i a discrete G_i-module for each $i \in I$. Then*

(a) $\varinjlim_{i\in I} M_i$ *has a natural structure of discrete* $(\varprojlim_{i\in I} G_i)$*-module.*

(b) $\{H^n(G_i, M_i)\}_{i\in I}$ *is a direct system of abelian groups for every* $n \geq 0$ *and*

$$\varinjlim_{i\in I} H^n(G_i, M_i) = H^n(\varprojlim_{i\in I} G_i, \varinjlim_{i\in I} M_i).$$

Proof. See [27, 9.7.2]. □

A.3 Cohomological dimension and duality

Definition. Let G be a profinite group. We write

$$\mathrm{cd}_p(G) := \sup\{n \in \mathbb{N} : \text{there is a } p\text{-torsion } G\text{-module } M \text{ with } H^n(G, M) \neq 0\}$$

and we define the *cohomological dimension of* G to be

$$\mathrm{cd}(G) := \sup\{\mathrm{cd}_p(G) : p \text{ prime}\}.$$

Proposition A.3.1. *Let G be a profinite group. Then*

$$\mathrm{cd}(G) := \sup\{n \in \mathbb{N} : \textit{there is a } \mathbb{Z}\textit{-torsion } G\textit{-module } M \textit{ with } H^n(G, M) \neq 0\}.$$

Proof. See [27, 11.1.2]. □

Proposition A.3.2. *If G is a free profinite group then* $\mathrm{cd}(G) \leq 1$.

Proof. See [27, 11.2.3]. □

Lemma A.3.3. *Let G be a profinite group with* $\mathrm{cd}_p(G) \geq 1$ *and let M be a discrete p-primary G-module that is also a divisible group. Then the group $H^{\mathrm{cd}_p(G)}(G, M)$ is divisible.*

Proof. Consider the exact sequence $0 \longrightarrow M[p] \longrightarrow M \xrightarrow{p} M \longrightarrow 0$, where the map $M \xrightarrow{p} M$ is the multiplication by p. From the long exact sequence in cohomology we obtain the exact sequence

$$H^{\mathrm{cd}_p(G)}(G, M) \xrightarrow{p} H^{\mathrm{cd}_p(G)}(G, M) \longrightarrow H^{\mathrm{cd}_p(G)+1}(G, M[p]).$$

Since the last group is zero, $H^{\mathrm{cd}_p(G)}(G, M)$ is p-divisible. Since we also have that $H^{\mathrm{cd}_p(G)}(G, M)$ is p-primary group, the lemma follows. □

Theorem A.3.4. *Let l be a prime and K be a local field with* $\mathrm{char}(K) = 0$. *Then we have that* $\mathrm{cd}_l(G_{\bar{K}/K}) = 2$ *and* $\mathrm{cd}_l(G_{\bar{K}/M}) \leq 1$ *for every extension M/K of degree divisible by p^∞.*

Proof. See [18, 7.1.8]. □

Now we study in detail the particular case when the profinite group G is procyclic. Let S be a set of prime numbers, and consider Γ a procyclic group of the form $\Gamma := \prod_{p \in S} \mathbb{Z}_p$. We say that an abelian group M is *S-torsion* if for every $m \in M$ we have that $(p_1^{i_1} \cdot \cdots \cdot p_r^{i_r})m = 0$ for some $p_1, \ldots, p_r \in S$ and $i_1, \ldots, i_r \in \mathbb{N}$.

Lemma A.3.5. *Let G be a procyclic group with topological generator γ, M a discrete G-module and call $M_G := M/(\gamma - 1)M$. Then $(M')_G \cong (M^G)'$ and $(M')^G \cong (M_G)'$.*

Proof. Since the group $\mathbb{R}/\mathbb{Z}$ is divisible, we have that it is an injective abelian group, hence the functor $\mathrm{Hom}(-, \mathbb{R}/\mathbb{Z})$ is exact. Dualizing the exact sequence

$$0 \longrightarrow M^G \longrightarrow M \xrightarrow{\gamma-1} M \longrightarrow M_G \longrightarrow 0$$

we obtain the exact sequence

$$0 \longrightarrow (M_G)' \longrightarrow M' \xrightarrow{(\gamma-1)^*} M' \longrightarrow (M^G)' \longrightarrow 0.$$

Since $(\gamma - 1)^*$ is exactly the multiplication by $\gamma - 1$ on M' (see Section 2.3), the claim follows by definition of $(M')_G$ and $(M')^G$. □

Proposition A.3.6. *Let S be a set of prime numbers and $\Gamma := \prod_{p \in S} \mathbb{Z}_p$ with topological generator γ. Let M be a discrete S-torsion Γ-module. Then*

(a) There is an isomorphism

$$H^1(\Gamma, M) \longrightarrow M_\Gamma := M/(\gamma - 1)M$$
$$[\xi] \longmapsto [\xi(\gamma)].$$

(b) If M is finite, then $H^1(\Gamma, M)$ is finite.

(c) $\mathrm{cd}(\Gamma) = 1$.

(d) Let $M \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ and $p \in S$. If M^Γ is finite then $H^1(\Gamma, M) = 0$.

Proof. See [18, 1.7.7] for the proof of (a). The point (b) is a direct consequences of (a). The point (c) is true since Γ is a free profinite group and $\mathrm{cd}(\Gamma) = 0$ if and only if $\Gamma = 1$ (see [27, 11.1.4]).
(d) Dualizing the exact sequence

$$0 \longrightarrow M^\Gamma \longrightarrow M \xrightarrow{\gamma-1} M \longrightarrow M_\Gamma \longrightarrow 0$$

we obtain the exact sequence

$$0 \longrightarrow (M_\Gamma)' \longrightarrow \mathbb{Z}_p^r \xrightarrow{(\gamma-1)^*} \mathbb{Z}_p^r \longrightarrow (M^\Gamma)' \longrightarrow 0.$$

Since $(M^\Gamma)'$ is finite, we must have that $(M_\Gamma)'$ is finite, and since $\mathbb{Z}_p^r$ has no nontrivial subgroups of finite order, we have that $(M_\Gamma)' = 0$. □

We now give one of the main results of Poitou-Tate duality.

Theorem A.3.7. *Let p be a prime of $\mathbb{Z}$, K be a finite extension of $\mathbb{Q}_p$ and $G_{\bar{K}/K} := \mathrm{Gal}(\bar{K}/K)$. Let M be a direct limit of finite $G_{\bar{K}/K}$-modules and set $M^* := \mathrm{Hom}(M, \mu)$, where μ is the group of roots of unity in $\bar{K}$. Then for every $0 \le i \le 2$ there is an isomorphism of finite abelian groups*

$$H^i(K, M) \xrightarrow{\sim} H^{2-i}(K, M^*)',$$

where $H^{2-i}(K, M^*)'$ denotes the Pontryagin dual of $H^{2-i}(K, M^*)$.

Proof. See [18, 7.2.6]. □

Appendix B

Theory of Valuations on Number Fields

In this appendix we sum up some notions of the theory of valuations that are used throughout this thesis. In order to have a more detailed presentation of this subject, one can read [17, Chapter II], [5] and also [11, Chapters I and II].

B.1 Absolute Values and Valuations

Definition. Let K be a field. An *absolute value* of K is a map $|\ |: K \to \mathbb{R}_{\geq 0}$ satisfying the properties

1. $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x||y|$.
3. $|x + y| \leq |x| + |y|$ "triangle inequality".

We tacitly exclude the case where $|\ |$ is the trivial absolute value of K which satisfies $|x| = 1$ for every $x \neq 0$.

Defining the distance between two points $x, y \in K$ by

$$d(x, y) = |x - y|$$

makes K into a metric space, and hence in particular a topological space.

Definition. Two absolute values are called *equivalent* if they define the same topology on K.

Proposition B.1.1. *The following statements are equivalent for two absolute values* $|\ |_1$ *and* $|\ |_2$ *on a field* K*:*

(a) $|\ |_1$ *and* $|\ |_2$ *are equivalent.*

(b) There exists a real number $s > 0$ such that $|x|_1 = |x|_2^s$ for every $x \in K$.

(c) $|x|_1 < 1$ if and only if $|x|_2 < 1$.

Proof. See [17, II.3.3]. □

Definition. Let K be a field and $\phi : \mathbb{Z} \to K$ the natural morphism. An absolute value $|\ |$ on a field K is called *nonarchimedean* if $|\phi(n)|$ stays bounded for every $n \in \mathbb{N}$. Otherwise it is called archimedean.

Proposition B.1.2. *An absolute value $|\ |$ on a field K is nonarchimedean if and only if it satisfies the* strong triangle inequality

$$|x + y| \leq \max\{\, |x|, |y| \,\}$$

for every $x, y \in K$.

Proof. See [17, III.3.6]. □

Let $|\ |$ be a nonarchimedean valuation on the field K. Setting

$$v(x) := -\log|x| \text{ for } x \neq 0, \text{ and } v(0) := \infty,$$

we obtain a function

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

verifying the following properties:

1. $v(x) = \infty$ if and only if $x = 0$.
2. $v(xy) = v(x) + v(y)$.
3. $v(x + y) \geq \min\{\, v(x), v(y) \,\}$.

with the usual conventions for operations with infinity.

A function v on K with these properties is called a *(real) valuation* of K. We exclude the case of the trivial function $v(x) = 0$ for every $x \neq 0$. From the properties of absolute values it descends that two valuations v_1 and v_2 are equivalent if and only if $v_1 = sv_2$ for some $s > 0$, or equivalently they must satisfy $v_1(x) > 0$ if and only if $v_2(x) > 0$. From a valuation v on K we can always obtain a non archimedean absolute value on K by putting

$$|x| = q^{-v(x)}$$

for every $x \in K$, for some fixed real number $q > 1$.

B.2 Places of a Number Field

In this section we characterize all valuations on a number field K modulo equivalence.

Definition. Equivalence classes of absolute values on a number field K are called *places* of K. The set of archimedean places is denoted by M_K^∞, the set of nonarchimedean places is called M_K^0.

Let K be a number field, $\mathcal{O}_K$ its ring of integers and $\mathfrak{p}$ a prime of $\mathcal{O}_K$. There is always a nonarchimedean (real) valuation on K associated to the prime $\mathfrak{p}$ defined as

$$v_\mathfrak{p}(x) = \mathrm{ord}_\mathfrak{p}(x)$$

for every $x \in K$, where $\mathrm{ord}_\mathfrak{p}(x)$ is the exact power of $\mathfrak{p}$ that appears in the primary decomposition of the fractional ideal (x). This valuation is called the $\mathfrak{p}$-adic valuation. Since it takes values in $\mathbb{Z} \subset \mathbb{R}$, it is a *discrete valuation.*

Moreover, if $\mathfrak{p}$ and $\mathfrak{q}$ are two distinct primes in $\mathcal{O}_K$, their valuations are inequivalent, since by the Chinese remainder theorem it can be found an $x \in \mathcal{O}_K$ satisfying $x \equiv 0 \pmod{\mathfrak{p}}$ and $x \equiv 1 \pmod{\mathfrak{q}}$, so that $v_\mathfrak{p}(x) > 0$ and $v_\mathfrak{q}(x) = 0$.

Let K be a number field. Every embedding of K in $\mathbb{C}$ gives us an archimedean absolute value for K descending from the usual archimedean absolute value of $\mathbb{C}$. Two different embeddings give equivalent absolute values on K if and only if the two embeddings are conjugate (see [11, II.1]).

What's amazing is that for a number field K these are the only absolute values possible (modulo equivalence).

Theorem B.2.1 (Ostrowski)**.** *Let K be a number field. Any nontrivial place of K is represented by a $\mathfrak{p}$-adic absolute value for a unique prime $\mathfrak{p} \in \mathcal{O}_K$ or it is represented by an absolute value coming from a complex embedding of K.*

Proof. For a very clear proof, look at the article of Conrad [5]. □

Corollary B.2.2. *Any nonarchimedean place of a number field K is discrete and we can always choose a* normalized valuation *(i.e. a valuation that takes values in $\mathbb{Z}$) that represents it.*

When $K = \mathbb{Q}$ and v_l is the valuation associated to the prime $l \in \mathbb{Z}$, the corresponding absolute value is usually defined as $|x|_l := l^{-v_l(x)}$ for every $x \in \mathbb{Q}$.

B.3 Completions

Definition. A valued field $(K, |\ |)$ is called *complete* if every Caucy sequence $\{a_n\}_{n\in\mathbb{N}}$ in K converges to an element of K.

Construction B.3.1. From any valued field $(K, |\ |)$ (or (K, v) with v valuation associated to $|\ |$) we can always get a complete valued field $(K_v, |\ |)$ by the process of *completion*, exactly in the same way as the field of the real numbers is constructed from the field of rational numbers with respect to the usual absolute value.

Take the ring R of all Cauchy sequences of $(K, |\ |)$, consider therein the maximal ideal $\mathfrak{m}$ of all sequences converging to zero with respect to $|\ |$ and define

$$K_v := R/\mathfrak{m}.$$

One embeds K into K_v by sending every $x \in K$ to the class of the constant sequence $(x, x, x, \dots)$. The absolute value $|\ |$ is canonically extended from K to K_v by giving the element $x \in K_v$, which is represented by the Cauchy sequence $\{x_n\}_{n\in\mathbb{N}}$, the absolute value

$$|x| := \lim_{n\to\infty} |x_n|.$$

We have another beautiful result due to Ostrowski that classifies every completion with respect to an archimedean valuation.

Theorem B.3.2 (Ostrowski)**.** *Let K be a field which is complete with respect to an archimedean absolute value $|\cdot|$. Then there is an isomorphism σ from K onto $\mathbb{R}$ or $\mathbb{C}$ satisfying*

$$|x| = |\sigma(x)|^s$$

for every $x \in K$ and for some fixed $s \in (0, 1]$.

Proof. See [17, II.4.2]. □

This result allows us to focus on fields with nonarchimedean valuations. We state now an important theorem about algebraic extensions of complete valued fields.

Theorem B.3.3. *Let K be a field complete with respect to a nonarchimedean valuation v of K. Let L be an algebraic extension of K. Then there exists a unique valuation v' on L which extends v.*

Proof. See [17, II.4.8]. □

Remark B.3.4. If the valuation v in Theorem B.3.3 is discrete and the extension L/K is not finite, then the extension v' may not be a discrete valuation in general. On the other hand, if L/K is finite then v' is always discrete.

B.4 Extensions of Valuations

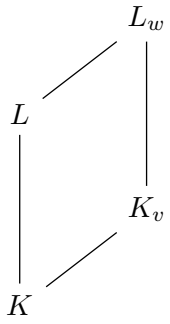
As stated in [17, II.8] there's a problem of notation, because archimedean absolute values doesn't manifest themselves as a valuation in the way we defined them. In spite of this, we define somehow "abstractly" a valuation v also in the nonarchimedean case, but in practice we will always use the absolute value that we denote $|\ |_v$, and we denote the completion of a field K with respect to a (archimedean or nonarchimedean) valuation by K_v.

For every (archimedean or nonarchimedean) valuation v on a field K we consider the completion K_v and an algebraic closure $\bar{K}_v$ of K_v. The canonical extension of v to K_v is again denoted by v and the unique (Theorem B.3.3) extension of this latter valuation to $\bar{K}_v$ is denoted by $\bar{v}$.

Let L/K be an algebraic extension. Choosing an embedding $\tau : L \to \bar{K}_v$ that fixes K we obtain by restriction of $\bar{v}$ to $\tau(L)$ an extension $w = \bar{v} \circ \tau$ of the valuation v to L. The mapping τ is continous with respect to this valuation (it is an isometric embedding). Then τ can be extended in a unique way to a continous embedding

$$\tau : L_w \longrightarrow \bar{K}_v,$$

where in case of an infinite extension L/K, L_w does not mean the completion of L with respect to w, but the union of the completions of all finite subextensions of L/K. Then we obtain the fundamental diagram



that is of central importance when dealing with the so-called "local-to-global" principle.

Definition. Let K be a valued field, L/K an algebraic extension, τ and τ' two embeddings $L \to \bar{K}_v$ that fix K. If there exist $\sigma \in \mathrm{Gal}(\bar{K}_v/K_v)$ such that $\tau' = \sigma \circ \tau$ we say that τ and τ' are *conjugate over* K_v.

Theorem B.4.1 (Extension)**.** *Let K be a valued field, L/K be an algebraic field extension and v a valuation of K. Then one has that*

(a) Every extension w of the valuation v arises as the composite $w = \bar{v} \circ \tau$ for some embedding $\tau : L \to \bar{K}_v$.

(b) Two extensions $\bar{v} \circ \tau$ and $\bar{v} \circ \tau'$ are equal if and only if τ and τ' are conjugate over K_v

Proof. See [17, II.8.1]. □

We now consider the case when L/K is a Galois extension of a valued field K. We define an important subgroup of $\mathrm{Gal}(L/K)$.

Definition. Let K be a field, v a valuation on K, L/K a Galois extension and w an extension of v on L. The *decomposition group* of the extension w of v to L is defined by

$$G_w = G_w(L/K) := \{\, \sigma \in \mathrm{Gal}(L/K) \;:\; w \circ \sigma = w \,\}.$$

If the valuation v is nonarchimedean, the decomposition group contains another canonical group.

Definition. Let K be a field, v a nonarchimedean valuation on K, L/K a Galois extension and w an extension of v on L. The *inertia group* of the extension w of v is defined by

$$I_w = I_w(L/K) := \{\, \sigma \in G_w \;:\; w(\sigma(x) - x) > 0 \quad \text{for every } x \in \mathcal{O}_L \,\}.$$

If the valuation v is archimedean, we simply set $I_w := G_w$. It's easy to verify that G_w and I_w are always closed subgroups.

Proposition B.4.2. *Let K be a field, v a valuation on K, L/K a Galois extension. Then $\mathrm{Gal}(L/K)$ acts transitively on the set of valuations of L that extend v, and the decomposition (resp. inertia) groups of any two such extensions are conjugate.*

Proof. See [17, II.9.1 and II.9.4]. □

We state now a fundamental result that tells us how to pass from global to local information whenever we have a Galois extension.

Proposition B.4.3. *Let (K, v) be a valued field, L a Galois extension of K, w a valuation on L that extends v. Then*

$$G_w(L/K) \cong \mathrm{Gal}(L_w/K_v);$$
$$I_w(L/K) \cong I_w(L_w/K_v).$$

Proof. See [17, II.9.6]. □

When K is a number field and the valuation v is archimedean, the situation is pretty easy, since thanks to Theorem B.3.2 the cardinality of the decomposition (and inertia) group is 1 or 2.

We now focus on the Galois extension $\bar{K}/K$ with K a number field. In this case Proposition B.4.3 tells us that, given v a valuation on K and w an extension of v to $\bar{K}$, then

$$G_w(\bar{K}/K) \cong \mathrm{Gal}((\bar{K})_w/K_v)$$

where $(\bar{K})_w$ is the union of the completions of all finite subextensions of $\bar{K}/K$, as stated at the beginning of this section.

We're now going to prove that if K is a number field then $(\bar{K})_w = \bar{K}_v$, following the proof of [18, Proposition 8.1.5]. If v is an archimedean valuation, this is trivial since in both cases we get $\mathbb{C}$. Hence we focus on the case v is a nonarchimedean valuation. For the proof we will use the following lemma.

Lemma B.4.4 (Krasner)**.** *Let F be a complete field with respect to a nonarchimedean valuation v and let $\bar{F}$ be an algebraic closure of F. Let $\alpha \in \bar{F}$ be separable over F and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over F. Suppose that there exists $\beta \in \bar{F}$ such that*

$$w(\alpha - \beta) > w(\alpha - \alpha_i) \quad \text{for every } i = 2, \ldots, n,$$

where w is the unique extension of v to $\bar{F}$. Then $F(\alpha) \subseteq F(\beta)$.

Proof. See [18, Proposition 8.1.6]. □

Proposition B.4.5. *Let K be a number field and v a nonarchimedean valuation of K. Let w be an extension of v on $\bar{K}$. Then*

$$(\bar{K})_w = \bar{K}_v,$$

where $(\bar{K})_w$ is the union of the completions of all intermediate fields of $\bar{K}/K$ with finite degree on K and $\bar{K}_v$ is the algebraic closure of the completion of K with respect to v.

Proof. Since K is naturally included in K_v, for any $\alpha \in \bar{K}$ we have that the completion of $K(\alpha)$ is contained in $K(\alpha)K_v = K_v(\alpha)$. Hence we have a natural inclusion of $(\bar{K})_w$ inside $\bar{K}_v$.

Conversely, let now $\alpha \in \bar{K}_v$ and let $f \in K_v[X]$ be its minimal polynomial over K_v. Since K is dense in K_v, for every $M \in \mathbb{N}$ we can choose a polynomial $g(X) \in K[X]$ of the same degree of f such that $v(g(X) - f(X)) \geq M$. Then we have that $v(g(\alpha)) = v(g(\alpha) - f(\alpha))$ grows as M grows, by the properties of the valuation. Writing $g(X) = \prod_{j=1}^{r}(X - \beta_j)$ with $\beta_j \in \bar{K}$, we see that $v(\alpha - \beta)$ is arbitrarily big for some root β of $g(X)$. In particular, if we choose $g(X)$ and β such that $v(\beta - \alpha) > v(\alpha_i - \alpha)$ for all conjugates $\alpha_i \in \bar{K}_v$ of α different from α. By Lemma B.4.4 we obtain that $\alpha \in K_v(\beta) = (K(\beta))_w$, hence α is inside a completion of a finite extension of K, hence $(\bar{K})_w \supseteq \bar{K}_v$. □

Joining the results of Proposition B.4.5 and of Proposition B.4.3 we obtain this fundamental corollary.

Corollary B.4.6. *Let K be a number field, v valuation on K and w an extension of v on $\bar{K}$. Then*

$$G_w(\bar{K}/K) \cong \mathrm{Gal}(\bar{K}_v/K_v).$$

Bibliography

[1] Yvette Amice, Jacques Vélu, *Distributions p-adiques associées aux séries de Hecke*, Astérisque, tome 24-25, pp.119-131, 1975.

[2] Michael F. Atiyah, Ian G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[3] Massimo Bertolini, Henri Darmon, *Hida families and rational points on elliptic curves*, Invent. math., 2007.

[4] Nancy Childress, *Class Field Theory*, Springer-Verlag, 2009.

[5] Keith Conrad, *Ostrowski for Number Fields.*

[6] Fred Diamond, Jerry Shurman, *A First Course in Modular Forms*, Springer-Verlag, 2005.

[7] Ralph Greenberg, *Iwasawa Theory for Elliptic Curves*, 1998.

[8] Ralph Greenberg, Glenn Stevens, *p-adic L-functions and p-adic periods of modular forms*, Inventiones mathematicae, vol. 111, pp. 407-448, 1993.

[9] Ralph Greenberg, Vinayak Vatsal, *On the Iwasawa Invariants of Elliptic Curves.*

[10] Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, 2nd edition, Springer-Verlag, 1984.

[11] Serge Lang, *Algebraic Number Theory*, Springer-Verlag, 1994.

[12] Serge Lang, *Algebra*, 3rd edition, Springer-Verlag, 2002.

[13] Barry Mazur, *Rational Points of Abelian Varieties with Values in Towers of Number Fields*, Invent. Math. 18, 183-266.

[14] Barry Mazur, John Tate, Jeremy Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. math. 84, 1-48, 1986.

[15] Toshitsune Miyake, *Modular Forms*, Springer-Verlag, 1989.

[16] Sidney A. Morris, *Pontryagin Duality and the Structure of Locally Compact Abelian Groups*, Cambridge University Press, 1977.

[17] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.

[18] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg, *Cohomology of Number Fields*, 2nd edition, Springer-Verlag, 2008.

[19] Karl Rubin, *Euler systems*, Princeton University Press, 2000.

[20] Jean Pierre Serre, *Galois Cohomology*, Springer-Verlag, 1997.

[21] Romyar Sharifi, *Iwasawa Theory*, lecture notes.

[22] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Springer-Verlag, 2009.

[23] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[24] Christof Skinner, *Lectures on the Iwasawa theory of elliptic curves.*

[25] Christofer Skinner, Eric Urban, *The Iwasawa Main Conjecture for GL_2*, Inventiones mathematicae 195.1, pp.1-277, 2014.

[26] Lawrence C. Washington, *Introduction to Cyclotomic fields*, 2nd edition, Springer-Verlag, 1997.

[27] John S. Wilson, *Profinite groups*, Clarendon Press, 1998.