UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

Departamento de Álgebra

TESIS DOCTORAL

Contributions to the theory of *P*-adic *L*-functions

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Iván Blanco Chacón

Directora

Pilar Bayer Isant

Madrid, 2012

UNIVERSIDAD COMPLUTENSE DE MADRID

DEPARTAMENTO DE ÁLGEBRA

CONTRIBUTIONS TO THE THEORY OF P-ADIC L-FUNCTIONS

Iván Blanco Chacón

CONTRIBUTIONS TO THE THEORY OF P-ADIC L-FUNCTIONS

Memoria presentada para optar al grado de Doctor en Matemáticas por

Iván Blanco Chacón

Universidad Complutense de Madrid, 2012

Departamento de Álgebra
Programa de Doctorado en Investigación Matemática
Doctorando: Iván Blanco Chacón
Tutora y Directora de Tesis: Pilar Bayer Isant

Pilar Bayer Isant, Catedrática de Álgebra
de la Facultad de Matemáticas de la Universidad de Barcelona,
HAGO CONSTAR
que D. Iván Blanco Chacón ha realizado esta memoria
para optar al grado de Doctor en Matemáticas bajo mi dirección.

Madrid, mayo de 2012,

Firmado: Pilar Bayer Isant

Esta tesis ha sido parcialmente financiada por
MICINN MTM2006-04895, MTM2010-17389.

2000 MSC: 11F67,11G18,11S40,14G10.

Para Jacoba Chacón Blanco, mi madre

Introduction

In the present monograph we deal with three kinds of questions concerning p-adic L-functions. The first one is the study of their set of zeros. The second, in the case of p-adic L-functions attached to elliptic curves, is their relation with the production of algebraic points. The third one, also in the case of modular forms or more in general, of automorphic forms is their relation with the geometry; more precisely, with the homology of the corresponding Shimura curve. In particular, we propose a definition of a p-adic L-function for automorphic forms attached to the Shimura curve $X(D,N)$ attached to the Eichler order $\mathcal{O}(D,N)$ of level N of the indefinite quaternion $\mathbb{Q}$-algebra of discriminant D for $p\|N$ but $p \nmid D$.

The question of when a p-adic L-function vanishes is in general very difficult and is of major arithmetical importance, but, in general, the p-adic analogues of classical conjectures, such as the conjecture of Birch and Swinnerton-Dyer, are expected to be more tractable than their classical counterpart. For instance, it has been shown by Kato, Kurihara and Tsuji ([36]) that $\mathrm{ord}_{s=1}L_p(E,\chi_{s-1}) \geq \mathrm{rk}\,(E(\mathbb{Q}))$ for any elliptic curve $E/\mathbb{Q}$, but little is known about the opposite inequality; it is not even known if the order of vanishing is finite or not in the case that $\mathrm{rk}\,(E(\mathbb{Q})) > 1$. The difficulty is that the p-adic topology is totally disconnected and, in the supersingular case, $L_p(E,\chi_s)$ is locally analytic but not analytic (equivalently, it is not an Iwasawa function). In this direction, we prove in Theorem 3.1.16, that for any cusp form $f \in S_k\,(\Gamma_0(N))$, if $L_p(f,\chi_s)$ is not identically zero, then, for any $s_0 \in \mathbb{Z}_p$, $\mathrm{ord}_{s=s_0}L(f,\chi_s)$ is finite.

Moreover, additional problems arise in the p-adic setting, like the appearance of exceptional zeros of the p-adic L-functions. These zeros come from certain Euler factors which are not present in the classical constructions.

The study of the non-vanishing of p-adic L-functions arises at the very beginning of the theory in the modular form setting: in [47], the conjecture

was formulated that $L_p(f,\chi)$ is not identically zero on the set of finite order characters. This conjecture was proved by Rohrlich in [61], and generalized in [62] for cusp forms of arbitrary weight. We also study the non-vanishing on the set of infinite order characters. In the ordinary case, we give a proof (Theorem 3.1.12) of the fact that $L_p(f,\chi_n)$ is not identically zero, where $\chi_n(x)=x^n$, for $n\in\mathbb{N}$.

As a matter of fact, the non-vanishing of p-adic analogues of complex L-series emerged as a highly difficult question in the earliest construction of p-adic L-functions for Dirichlet characters by Kubota-Leopoldt. The Leopoldt conjecture about the non-vanishing of the p-adic regulator (hence of none of the values $L_p(\chi,1)$ for any Dirichlet character χ) was proved by Brumer in [19] for abelian number fields and, recently, Mihailescu ([50]) has announced a proof for arbitrary number fields.

As we said above, we also explore here the relation of the p-adic L-functions of elliptic curves $E/\mathbb{Q}$ with the construction of algebraic points on them, but this relation occurs (at least, the relation we have studied) with a new kind of p-adic L-function which we introduce in the present work: the quadratic p-adic L-function, which is the Mazur-Mellin transform of a p-adic distribution defined through geodesics connecting quadratic imaginary points, rather than cusps. We have generalized this construction to the Shimura curves $X(D,N)$ as a way to overcome the lack of cusps.

There does not seem to be a systematic study of the theory of p-adic L-functions. Although there exists a vast amount of research on the topic, there are no surveys studying the topic from a historical and comparative point of view, starting with the construction by Kubota-Leopoldt and going on to the anti-cyclotomic setting, presenting the problems each construction faces, the conjectures it gives rise to, the meaning of each conjecture and the relations between each construction. In this regard, we should mention the excellent survey [14] in the modular setting.

We also include an account of the different definitions of p-adic L-functions in each setting from an analytical point of view. We explain, for instance, the early construction of the p-adic L-function in terms of the χ-average by Kubota and Leopoldt and relate it with the alternative approaches. There are, even in the same setting, several apparently different definitions of p-adic L-functions, and we explain how, in most cases, the interpolation properties characterize them and they are equivalent. The organization of the present work is as follows:

Chapter 1 introduces the p-adic L-function of an abelian extension of

$\mathbb{Q}$. We present a historical approach to this topic, pointing out the reasons which led Kubota and Leopold to introduce a p-adic analogue of the complex L-function of a Dirichlet character. This reason is essentially the study of the class numbers of the cyclotomic extensions, and in particular of their asymptotic behaviour. We discuss Kubota-Leopoldt's and Leopoldt's original papers [43] and [40], and introduce the p-adic L-function as limit of what Kubota and Leopold called χ-*Mittel*, which we have translated as χ-*averages* (in most of the thesis χ will denote a Dirichlet character). Later on, in the same chapter, p-adic L-functions will be presented as limits of Stickelberger elements and as Mazur-Mellin transforms and we will show how the three constructions are equivalent. In this chapter, in Theorem 1.1.15, we provide a proof of a formula of Leopoldt, which appears unproven in [43]. We give a generalization of the p-adic regulator modulo p and we use it to estimate the p-adic norm of the Dedekind ζ-function of a real abelian extension of $\mathbb{Q}$ at certain integers (Propositions 1.1.28 and 1.1.29) and, by taking a limit, we obtain a formula for $s = 1$ (Proposition 1.1.31).

Chapter 2 continues the study of the p-adic L-functions for number fields and explains the next step in the history of p-adic L-functions: the case of real abelian extensions of totally real number fields. We explain the work of Cassou-Nogues [22], since it is very explicit and contains some results on the estimation of the p-adic norm at special values.

Chapter 3 deals with Mazur and Swinnerton-Dyer ([47]) and Mazur-Tate-Teitelbaum ([49]) p-adic L-functions. These functions are usually referred to in the literature as cyclotomic p-adic L-functions. In addition, we give a proof of the fact that, in the ordinary case, the cyclotomic p-adic L-function is not identically zero on the set of infinite order characters (Theorem 3.1.12). The main tools are the approximation by polynomials of the characteristic functions of compact open discs of $\mathbb{Z}_p$ and the results by Rohrlich ([61], [62]) on the non-vanishing of the complex L-function twisted by Dirichlet characters, which is equivalent, by the interpolation formula, to the non-vanishing of the p-adic L-function on the set of finite order p-adic characters. We also prove (Theorem 3.1.16) that, in the supersingular case, the order of vanishing of the cyclotomic p-adic L-function at any point (in particular at the critical values) is finite provided that the function is not identically zero. Our results of non-vanishing are published in [17]. Here we use the injectivity property of a certain continuous linear endomorphism of the space $c_0(\mathbb{C}_p)$. We continue the chapter by showing that the Mazur-Tate-Teitelbaum and the Mazur and Swinnerton-Dyer p-adic L-functions are the same although

the p-adic distributions from which they are defined are different. We finish the chapter by examining some conjectures on the order of vanishing.

Chapter 4 is a bridge which, to some extent, justifies our study of quadratic p-adic distributions in chapter 5, since our construction is partly inspired in the anticyclotomic p-adic L-function, which will be explained here. We study in this chapter an alternative construction of the p-adic L-function due to Schneider and point out how it was related with the exceptional zero conjecture, as well as introducing a conjecture by Klingenberg which relates the Schneider p-adic L-function with the cyclotomic one. This construction was revisited by Bertolini and Darmon, who proposed some definitions of p-adic L-functions related with the classical complex L-function $L(E, K, s)$ if $E/\mathbb{Q}$ is an elliptic curve and $K/\mathbb{Q}$ a quadratic real extension. These p-adic L-functions are related with heights of generalized Heegner points and under certain conditions satisfy an interpolation property.

Chapter 5 explains our construction of quadratic p-adic L-functions attached to elliptic curves $E/\mathbb{Q}$, which produce algebraic points on the curve defined over certain abelian extensions of $\mathbb{Q}$. An important difference with regard to the cyclotomic p-adic distribution is that our p-adic distribution takes values in a countably infinite-dimensional $\mathbb{Q}_p(\alpha_p)$-vector space (α_p is a root of the Hecke polynomial for f at p). In further research, we hope to find a way of controlling the degree of the extensions we obtain. Our construction has been published in [7].

In Chapter 6 we propose a definition of a p-adic L-function for automorphic forms associated to Shimura curves arising from indefinite quaternion $\mathbb{Q}$-algebras. The method follows our construction in the modular case: we consider integrals along paths connecting quadratic imaginary points. These ideas led to the study of the homology of these Shimura curves, in the spirit of [1], which have resulted in the concept of quadratic modular symbols. This device is, to some extent, a generalization of the classical modular symbols, and we give a cohomological presentation of this construction as well as some explicit calculations in the homology of these cocompact Shimura curves via an explicit algorithm for arithmetic Fuchsian groups of signature $(1, e)$.

Acknowledgements. I am deeply indebted to my thesis advisor Pilar Bayer Isant for her help and patience. These four years in Barcelona have been vital to my mathematical training. In this training, the expertise and guidance of my thesis advisor have played an essential role. Likewise, I express my gratitude to my partners at the Department of Algebra, especially to Artur Travesa (always willing to answer a question and to find a bug in an argu-

ment), to Luis Victor Dieulefait, Ricardo García, Isabel Figueras, Federico Cantero, Ignasi Mundet, Alberto Fernández Boix (who introduced me in the world of spectral sequences) as well as to the members of the Grup de Teoria de Nombres de Barcelona. And of course, I have to thank Henri Darmon for drawing my attention to this fascinating topic and for his valuable comments and suggestions. I had the luck to attend his lectures on modular forms in McGill in 2008, and this was my first contact with p-adic L-functions. Also to the organizers of Park City Mathematics Institute-Institute for Advanced Study for giving to me the opportunity of attending these lectures and to be a teaching assistant. And I must also express my gratitude to Vinayak Vatsal for encouraging me to continue my study of p-adic L-functions from the point of view of the p-adic functional analysis, after pointing out a mistake in a problem I was trying to solve. I do not think I will ever learn (or I will be exposed to) such an amount of high level Maths as in those two years. But I should also thank all the non-number theoretical people, without whose help this thesis could not have been finished (maybe not even begun). After my mother, to whom I owe everything, I have to mention first my friend Ignacio Sols, who introduced me to what Hardy called *Real Mathematics* (and in the philosophy of Kant), and with whom I have shared so many afternoons of classical literature and so many evenings at Cascorro and Puerta de Toledo in front of a well-cooked dish of callos. My fiancée Alba Benedicto for her continuous and unconditional support, and for being always there, when the rest are gone. The help of María Nofuente has been decisive for me to be able to present my thesis on time, and to keep the faith in the sincere virtue of Christian Charity. And to the rest of my friends, who, sometimes, have endured my bad temper with a joke and a beer, and who have helped so much, even without being conscious of it: Jesús Moreno, José Vicente Alguacil, Tomás Gómez, José Antonio Sánchez and Javier Valin. These first category men serve as an illustration (the first one would possibly occupy all of it, such is the extension of our friendship, specially his) of the following adagio:

Amicus certus in re incerta cernitur.

Cicero, *Laelius, De amicitia, 17, 64*

Contents

Chapter 0

Prolegomena

0.1 Non archimedean norms and p-adic integers

From now onwards, p will denote an odd prime number (unless we say the contrary). We will denote by $|\ |_p$ the p-adic norm of $\mathbb{Q}$ normalized so that $|p|_p = p^{-1}$. If the p-adic valuation of $r \in \mathbb{Q}$ is denoted by $v_p(r)$, then, $|r|_p = p^{-v_p(r)}$. Notice that $|\ |_p$ takes values of the form p^n, with $n \in \mathbb{Z}$. By $\mathbb{Q}_p$ we mean the completion of $\mathbb{Q}$ with respect to $|\ |_p$. For any $a \in \mathbb{Q}_p$ and any $r \in \mathbb{Z}$, the open disc of radius p^r centered at a is

$$D(a, p^r) = \{z \in \mathbb{Q}_p : \ |z - a|_p < p^{-r}\}.$$

Notice that this notation for p-adic discs is not the classical one for discs in metric spaces, but we have chosen it since it is in accordance with [49]. The discs $D(a, p^r)$ form a basis of the p-adic topology as a runs through $\mathbb{Q}_p$ and r runs through $\mathbb{Z}$. The p-adic norm satisfies the following property (see Koblitz [39], ch.1).

$$|a + b|_p \leq \max\{|a|_p, |b|_p\}; \ a, b \in \mathbb{Q}. \tag{0.1.1}$$

A direct consequence of (0.1.1) is the fact that the open discs $D(a, p^r)$ are also closed. This means that the p-adic topology is totally disconnected. For any $a \in \mathbb{Q}_p$, $a \neq 0$, there exists a unique $n_0 \in \mathbb{Z}$ and a unique sequence $\{a_n\}_{n \geq n_0}$ of rational integers with $a_n \in \{0, 1, ..., p-1\}$ such that $a_{n_0} \neq 0$ and

$$a = \sum_{k=n_0}^{\infty} a_n p^n. \tag{0.1.2}$$

The integer n_0 will be denoted by $v_p(a)$. In this way, the p-adic valuation and, hence, the p-adic norm extend to $\mathbb{Q}_p$ in a unique way so that (0.1.1) also holds in $\mathbb{Q}_p$. The ring of p-adic integers is

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : \ |a|_p \leq 1\}.$$

The fact of being a ring is due to (0.1.1). In fact, $\mathbb{Z}_p$ is the discrete valuation ring of $\mathbb{Q}_p$. The maximal ideal of $\mathbb{Z}_p$ is $p\mathbb{Z}_p$. The equality (0.1.2) means that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ in the p-adic topology. In fact, the following result will be useful in our study.

Proposition 0.1.1. *For any integer $j \in \{0, ..., p-2\}$, the set*

$$\{n \in \mathbb{Z} : \ n \equiv j \pmod{p-1}\}$$

is dense in $\mathbb{Z}_p$.

Proof. Fix j with $0 \leq j \leq p-2$. For any $x \in \mathbb{Z}_p$ and for any $n \geq 1$, let x_n be the truncation of x modulo p^{n+1}. The Chinese remainder theorem grants the existence of a positive integer N_n such that $N_n \equiv j \pmod{p-1}$ and $|N_n - x_n|_p \leq p^{-(n+1)}$. □

Proposition 0.1.2 (Hensel's Lemma, cf. Koblitz [39], ch. 1)**.** *Let $p(X) \in \mathbb{Z}_p[X]$ be a polynomial and denote by $p'(X)$ its formal derivative. Let $a \in \mathbb{Z}/p\mathbb{Z}$ be a congruence class $\pmod p$ such that $p(a) \equiv 0 \pmod p$ and $p'(a) \not\equiv 0 \pmod p$. Then, there exists a unique $\alpha \in \mathbb{Z}_p$ congruent to $a \pmod p$ such that $p(\alpha) = 0$.*

Corollary 0.1.3. *The ring $\mathbb{Z}_p$ contains all the $(p-1)$-th roots of unity.*

Proof. Apply Hensel's lemma and the little theorem of Fermat to the polynomial $X^{p-1} - 1$. □

Remark 0.1.4. From Corollary 0.1.3, it follows that for any $\alpha \in \mathbb{Z}_p$, there is an expansion

$$\alpha = \sum_{n=0}^{\infty} \omega_n p^n.$$

with $\omega_n \in \mathbb{Z}_p$ and $\omega_n^p = \omega_n$. The digits ω_n are called the Teichmüller digits of α.

For any $a \in \mathbb{Q}_p$, $r \in \mathbb{Z}$, denote

$$D\left(a, p^r\right)^+ = a + p^r \mathbb{Z}_p = \left\{a + p^r z : \ |z|_p \leq 1\right\}.$$

These sets are simultaneously open and compact in the p-adic topology.

Let now L be a finite extension of $\mathbb{Q}_p$. There is a unique norm $|\ |'_p$ on L extending $|\ |_p$. This norm is given by

$$|\alpha|'_p = \left|N_{L/\mathbb{Q}_p}(\alpha)\right|_p^{\frac{1}{[L:\mathbb{Q}_p]}}, \tag{0.1.3}$$

where $N_{L/\mathbb{Q}_p}$ is the algebraic norm from L to $\mathbb{Q}_p$ and $[L : \mathbb{Q}_p]$ is the degree of the extension (see Koblitz [39]). Denote by $\mathcal{O}_L$ the integral closure of $\mathbb{Z}_p$ in L. One has the following characterization

$$\mathcal{O}_L = \left\{\alpha \in L : \ |\alpha|'_p \leq 1\right\}.$$

As with $\mathbb{Z}_p$, $\mathcal{O}_L$ is a local ring with maximal ideal

$$D(0,1) = \left\{\alpha \in L : \ |\alpha|'_p < 1\right\}.$$

The residue field of $\mathcal{O}_L$ is a finite extension of $\mathbb{F}_p$ of certain degree f. It turns out (cf. Koblitz [39], ch. 3) that f divides $[L : \mathbb{Q}_p]$. The quotient $[L : \mathbb{Q}_p]/f$ is called index of ramification of the extension. Denote this quotient by e. Let $\pi \in L$ be a uniformizer (i.e., $|\pi|'_p = p^{-\frac{1}{e}}$). We have

Proposition 0.1.5. *For any $\alpha \in L \setminus \{0\}$, there is a unique representation*

$$\alpha = \sum_{n=n_0}^{\infty} \omega_n \pi^n,$$

with $\omega_n^{p^f} = \omega_n$ for any $n \geq n_0$, and $|\alpha|'_p = p^{\frac{-n_0}{e}}$.

□

Since the norms are compatible, from now on, we will denote the norm $|\ |'_p$ by $|\ |_p$. Denote by $\mathcal{O}_L^*$ the multiplicative group of the units in $\mathcal{O}_L$. One has that $\mathcal{O}_L^* = \{\alpha \in \mathcal{O}_L : \ |\alpha|_p = 1\}$.

Let $\mathbb{Q}^{alg}$ be an algebraic closure of $\mathbb{Q}$ and $\mathbb{Q}_p^{alg}$ an algebraic closure of $\mathbb{Q}_p$. Fix an embedding $\mathbb{Q}^{alg} \subset \mathbb{Q}_p^{alg}$. According to (0.1.3), it is possible to extend the p-adic norm to $\mathbb{Q}_p^{alg}$. It can be shown that $\mathbb{Q}_p^{alg}$ is not complete.

Denote its completion by $\mathbb{C}_p$. This field is algebraically closed (cf. Koblitz [39], Ch. 3).

Let ζ_{p^n} be a primitive p^n-th root of unity contained in $\mathbb{Q}^{alg}$. Given $\sigma \in \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p^n}\right)/\mathbb{Q}\right)$, there is a unique unit a modulo p^n such that $\sigma(\zeta_{p^n}) = \zeta_{p^n}^a$. This fact defines a group monomorphism

$$\phi_n : \mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}\right) \to \left(\mathbb{Z}/p^n\mathbb{Z}\right)^* .$$

In fact, ϕ_n is an isomorphism compatible with the projections on both sides. Notice that

$$\mathbb{Z}_p^* = \varprojlim_n \left(\mathbb{Z}/p^n\mathbb{Z}\right)^* .$$

The maximal abelian extension of $\mathbb{Q}$ which is unramified outside p, which is denoted by $\mathbb{Q}(\zeta_{p^\infty})$, is the inductive limit of the cyclotomic extensions $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$. By functoriality of the inverse limit together with the isomorphisms ϕ_n, one has

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p^\infty}\right)/\mathbb{Q}\right) \simeq \mathbb{Z}_p^*. \tag{0.1.4}$$

Let us observe that the closed unit disc $1 + p\mathbb{Z}_p$ is topologically cyclic, with $1 + p$ as a topological generator. On the other hand, $\mathbb{Z}_p^*$ is also topologically cyclic. To see this fact, fix g a primitive root mod p. If the multiplicative order of g mod p^2 is $p - 1$, we can choose $g = g_0 + p$ as a primitive root mod p^n for any $n \geq 2$, otherwise, $g = g_0$ serves as a primitive root mod p^n for any $n \geq 2$.

0.2 p-adic functions

A character of $\mathbb{Z}_p^*$ is a group homomorphism $\chi : \mathbb{Z}_p^* \to \mathbb{C}_p^*$. Denote by $\mathcal{X}$ the group of continuous characters of $\mathbb{Z}_p^*$.

For any $x \in \mathbb{Z}_p^*$, there exists a unique $(p-1)$-th root of unity in $\mathbb{Z}_p$ congruent to x modulo p (apply Hensel's lemma). Denote it by $\omega(x)$. The map ω is clearly a p-adic character of order $p-1$. Since ω is locally constant, it belongs to $\mathcal{X}$. Define $\langle x \rangle = \dfrac{x}{\omega(x)}$. This is also a continuous character, but has infinite order. One has the following

Proposition 0.2.1. *The map*

$$\begin{array}{rcl} \mathbb{Z}_p^* & \to & (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}_p \\ x & \mapsto & \left(\omega(x) \pmod p, \dfrac{\langle x\rangle - 1}{p}\right) \end{array}$$

is an isomorphism. □

Corollary 0.2.2. $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p^\infty}\right)/\mathbb{Q}\left(\zeta_p\right)\right) \simeq \mathbb{Z}_p$.

Proof. This is a direct consequence of Proposition 0.2.1, the isomorphism 0.1.4 and the fact that

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_p\right)/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^*.$$

□

For any $x \in \mathbb{Z}_p$ and $n \geq 0$, define

$$\binom{x}{n} = \frac{(x-n+1)(x-n+2)\cdots x}{n!}.$$

Proposition 0.2.3 (Mahler, [60])**.** *Let $K/\mathbb{Q}_p$ be a finite extension. Then, for any continuous function $f : \mathbb{Z}_p \to K$, there exists a sequence $\{c_n\} \in K^{\mathbb{N}}$ such that $\lim_{n\to\infty} |c_n|_p = 0$ and, uniformly,*

$$f(x) = \sum_{n=0}^{\infty} c_n \binom{x}{n}.$$

□

Let $x \in \mathbb{Z}_p \setminus D(1,p)$. The function

$$\begin{array}{rcl} \mathbb{Z} & \to & \mathbb{Z}_p \\ n & \mapsto & x^n \end{array}$$

is not continuous with the p-adic topology (this is easy to see by considering $x \in p\mathbb{Z}_p$). But if we impose that $x \in \mathbb{Z}_p^*$ and restrict the domain to a fixed class of congruence modulo $p-1$, we obtain a continuous function, which can

be extended to $\mathbb{Z}_p$ by a density argument. Thus, we have $p-1$ determinations of the function $f(s) = x^s$, all of which agree over $\mathbb{Z}$.

The p-adic exponential map is

$$\begin{aligned} \exp_p : \quad D(0, p^{\frac{1}{p-1}}) \quad &\to \quad D(1,1) \\ x \qquad\quad &\mapsto \quad \sum_{n=0}^{\infty} \frac{x^n}{n!}, \end{aligned}$$

where $D(0, p^{\frac{1}{p-1}}), D(1,1) \subseteq \mathbb{Q}_p$. The key to prove that the radius of convergence is $p^{\frac{1}{p-1}}$ is the fact that $|n!|_p = p^{-\frac{n-\sigma(n)}{p-1}}$, where $\sigma(n)$ denotes the sum of the p-adic digits of n. The function $\exp_p$ is continuous on $D(0, p^{\frac{1}{p-1}})$ and has an inverse

$$\begin{aligned} \log_p \quad : D(1, p^{\frac{1}{p-1}}) \quad &\to \qquad D(0, p^{\frac{1}{p-1}}) \\ x \qquad\quad &\mapsto \quad \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}. \end{aligned}$$

The p-adic exponential map is an isomorphism between the additive group $D\left(0, p^{\frac{1}{p-1}}\right)$ and the multiplicative group $D\left(1, p^{\frac{1}{p-1}}\right)$. We will frequently use the following definition.

Definition 0.2.4 (cf. Robert, [60])**.** Given $z \in D(1,p) \in \mathbb{Z}_p$ and $s \in \mathbb{Z}_p$, define $z^s := \exp_p(s \log_p(z))$.

Let L be a finite extension of $\mathbb{Q}_p$ and let K be a compact subset of L. Denote by $\mathcal{C}(K, L)$ the L-vector space of continuous L-valued functions on K. Given $f \in \mathcal{C}(K, L)$, define the norm

$$||f||_{p,\infty} = \max_{x \in K} |f(x)|_p.$$

Denote by $L[X](K, L)$ the L-vector space of L-valued functions on K defined by polynomials with coefficients in L.

Theorem 0.2.5 (Kaplansky, cf. [2])**.** *$L[X](K, L)$ is dense in $\mathcal{C}(K, L)$ with the topology given by the norm $||\ ||_{p,\infty}$.*

Definition 0.2.6. A p-adic function given by a power series in a disc is called *analytic* in that disc. A p-adic function defined in a set $X \subseteq L$ such that for any $z \in X$ there exists $r > 0$ such that f is analytic in $D(z, r) \subseteq X$ is called *locally analytic*.

Analytic functions share most of the classical theorems of complex analytic functions, but not all of them. For instance, analytic continuation fails. This failure, and other particularities of these functions are due to the total disconnectedness of the p-adic topology. In chapter 4, we will use another kind of function, which behaves more rigidly than analytic ones: the rigid analytic functions. Prior to defining them, it is necessary to define a class of distinguished p-adic sets.

Define the Drinfeld upper half-plane to be the set $\mathcal{H}_p := \mathbb{P}^1(\mathbb{C}_p) \setminus \mathbb{P}^1(\mathbb{Q}_p)$. We can think of $\mathcal{H}_p$ as a p-adic analogue of $\mathbb{P}^1(\mathbb{C}) \setminus \mathbb{P}^1(\mathbb{R})$. But $\mathcal{H}_p$ does not split in a natural way into two disjoint components, hence it is more natural to see $\mathcal{H}_p$ as the analogue of $\mathcal{H}$. It is possible to identify $\mathcal{H}_p$ with $\mathbb{C}_p \setminus \mathbb{Q}_p$ by means of the map $(z_0 : z_1) \mapsto z_0/z_1$ (cf. [18]). Denote $\mathcal{O}(\mathbb{C}_p) := \{z \in \mathbb{C}_p \,|\, |z|_p \leq 1\}$, i.e., the valuation ring of $\mathbb{C}_p$. It is a local ring with maximal ideal $M_p = \{z \in \mathbb{C}_p \,|\, |z|_p < 1\}$ and residue field $\overline{\mathbb{F}}_p$, an algebraic closure of $\mathbb{F}_p$ (cf. [54]).

Definition 0.2.7. (cf. [64]) The reduction map is defined by

$$\begin{array}{rcl} \mathrm{red} : \mathbb{C}_p & \to & \overline{\mathbb{F}}_p \cup \{\infty\} \\ z & \mapsto & \begin{cases} z \pmod{M_p} \text{ if } z \in \mathcal{O}(\mathbb{C}_p), \\ \infty \text{ otherwise.} \end{cases} \end{array}$$

Definition 0.2.8. (cf. [64],[25]) The standard affinoid in $\mathcal{H}_p$ is the set

$$A = \mathrm{red}^{-1}\left(\overline{\mathbb{F}}_p \setminus \mathbb{F}_p\right).$$

The group $\mathrm{PGL}(2, \mathbb{Q}_p)$ acts on $\mathcal{H}_p$ by Möbius transformations. An affinoid is a translate of the standard affinoid by a transform $\gamma \in \mathrm{PGL}(2, \mathbb{Q}_p)$. Notice that the affinoids cover $\mathcal{H}_p$ and they have a hierarchical structure, which is related with the Bruhat-Tits tree of $\mathrm{PGL}(2, \mathbb{Q}_p)$. We will return to this fact in chapter 4. The standard affinoid is compact and so are the rest of affinoids, hence any continuous function on an affinoid attains its maximum and minimum in it.

Definition 0.2.9. Let $f : \mathcal{H}_p \to \mathbb{C}_p$. The function f is rigid analytic if the restriction of f to any affinoid A is the uniform limit of a sequence of rational functions with poles outside A.

In the study of p-adic L-functions it is convenient to extend the p-adic logarithm continuously to $\mathbb{C}_p^*$. By density, it suffices to extend it to $\left(\mathbb{Q}_p^{alg}\right)^*$. Denote $\mathbb{U} = \{z \in \mathbb{Q}_p^{alg} : \ |z|_p = 1\}$, and by $\mathbb{P} \subseteq \mathbb{R}_+$ the image of $|\ |_p$ on $\mathbb{Q}_p^{alg}$. One has an isomorphism as multiplicative groups

$$\begin{aligned} T: \ \left(\mathbb{Q}_p^{alg}\right)^* &\rightarrow \qquad \mathbb{U} \times \mathbb{P} \\ z \qquad &\mapsto \ \left(\frac{z}{|z|_p}, |z|_p\right). \end{aligned}$$

Set $\mathbb{D} = D(1,1) = 1 + D(0,1) \subseteq \mathbb{Q}_p^{alg}$ and $\mathbb{V}$ the group of all roots of unity in $\left(\mathbb{Q}_p^{alg}\right)^*$ of order prime to p. One has an isomorphism

$$\begin{aligned} R: \ \mathbb{U} \ &\rightarrow \qquad \mathbb{V} \times \mathbb{D} \\ z \ &\mapsto \ \left(\omega(z), \frac{z}{\omega(z)}\right). \end{aligned}$$

Hence,

$$\left(\mathbb{Q}_p^{alg}\right)^* \simeq \mathbb{V} \times \mathbb{D} \times \mathbb{P}.$$

Denote $\kappa : \left(\mathbb{Q}_p^{alg}\right)^* \rightarrow \mathbb{D}$ the projection onto $\mathbb{D}$. The power series defining the p-adic logarithm converges in $D(1,p) \subseteq \mathbb{Q}_p^{alg}$. Denote by $\log_p$ the extension of the logarithm to $\mathbb{D}$.

Definition 0.2.10. The Iwasawa logarithm is the extension to $\mathbb{C}_p^*$ of $\log_p \circ \kappa$. It is denoted by Log_p.

Proposition 0.2.11 (cf. [60])**.** *The Iwasawa logarithm is the unique continuous extension to $\mathbb{C}_p^*$ of the p-adic logarithm which vanishes at p and such that for any $\sigma \in \mathrm{Gal}\left(\mathbb{Q}_p^{alg}/\mathbb{Q}_p\right)$,*

$$\mathrm{Log}_p \circ \sigma = \sigma \circ \mathrm{Log}_p,$$

in $\mathbb{Q}_p^{alg}$.

In addition, the Iwasawa logarithm is continuous and locally analytic (cf. [60], ch. 5).

Definition 0.2.12. A polynomial $P(T) = T^n + a_{n-1}T^{n-1} + ... + a_0 \in \mathcal{O}_L[T]$ is called *distinguished* if $a_k \in \pi\mathcal{O}_L$, where π is a uniformizer of $\mathcal{O}_L$ over p.

The following result, besides being of interest by itself, is crucial in the classical study of p-adic L-functions (see Koblitz [39], ch. 5).

Theorem 0.2.13 (Weierstrass preparation theorem)**.** *Let* $f(T) = \sum_{k\geq 0} a_k T^k \in \mathcal{O}_L[[T]]$ *with* $a_k \in \pi\mathcal{O}_L$ *for* $0 \leq k \leq \lambda - 1$ *but* $a_\lambda \notin \pi\mathcal{O}_L$*. Then, there exists a unique distinguished polynomial* $p(T)$ *of degree* λ*, a unique* $u(T) \in \mathcal{O}_L[[T]]^*$ *and a unique* $\mu \in \mathbb{N} \cup \{0\}$*, such that*

$$f(T) = \pi^\mu p(T) u(T).$$

As an immediate corollary, a function given by a power series in the conditions of theorem 0.2.13 has a finite number of zeros in its domain.

0.3 Dirichlet characters and Bernoulli numbers

A Dirichlet character modulo n is a group homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$. The conjugate character $\overline{\chi} : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ is defined by setting $\overline{\chi}(a) = \overline{\chi(a)}$. If $n|m$, the character χ can be lifted to another character $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$. If a Dirichlet character modulo f is not the lift of any character, it is said to be primitive of conductor f. A Dirichlet character modulo n can be lifted to $\mathbb{Z}/n\mathbb{Z}$ by setting $\chi(a) = 0$ for $(a, n) > 1$. This way, any character modulo n can be lifted to $\mathbb{Z}$. Denote by 1_n the trivial character modulo n.

Definition 0.3.1. Let χ be a Dirichlet character modulo n. The Dirichlet L-function of χ is

$$L(s;\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},\ \mathrm{Re}(s) > 1.$$

We denote by $L(s;1)$ the Riemann zeta function. Since χ takes values on the unit circle, $L(s;\chi)$ is well defined and it is analytic in the half-plane $\mathrm{Re}(s) > 1$.

Proposition 0.3.2. *The function* $L(s;\chi)$ *admits the Euler factorization*

$$L(s;\chi) = \prod_p \left(1 - \chi(p)p^{-s}\right)^{-1},\ \mathrm{Re}(s) > 1,$$

where p *runs over the prime numbers.*

In particular, Dirichlet L-functions do not vanish at any point of the half-plane $\mathrm{Re}(s) > 1$.

A Dirichlet character is said to be even if $\chi(-1) = 1$, and odd otherwise. Let χ be a primitive Dirichlet character of conductor f. The Gauss sum for χ is defined by

$$\tau(\chi) = \sum_{a=1}^{f} \chi(a) e^{\frac{2\pi i a}{f}}.$$

Path integration of the function $G_\chi(z) = \sum_{a=1}^{f} \frac{\chi(a)e^{-az}}{1-e^{-fz}}$ and an application of the residue theorem allow us to prove the following result.

Proposition 0.3.3 (cf. Iwasawa [34], appendix)**.** *The Riemann zeta function extends to a meromorphic function on $\mathbb{C} \setminus \{1\}$. It has a simple pole at $z = 1$ with residue 1. If $\chi \neq 1$, the function $L(s;\chi)$ extends to an entire function. In addition, the following functional equation holds:*

$$L(s;\chi) = \frac{\tau(\chi)}{2i^{\delta(\chi)}} \left(\frac{2\pi}{f}\right)^s \frac{L(1-s;\overline{\chi})}{\Gamma(s)\cos\frac{\pi(s-\delta(\chi))}{2}},$$

where $\delta(\chi) = 0$ if χ is even, and 1 otherwise.

□

Let χ be a Dirichlet character of conductor f. Define

$$F_\chi(t) = \sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1},$$

$$F_\chi(t, X) = F_\chi(t) e^{Xt},$$

where X is an indeterminate. These functions are analytic in t, with series expansions of the form

$$F_\chi(t) = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!},$$

$$F_\chi(t, X) = \sum_{n=0}^{\infty} B_{n,\chi}(X) \frac{t^n}{n!}.$$

Definition 0.3.4. The numbers $B_{n,\chi}$ are called Bernoulli numbers for the character χ. The polynomials $B_{n,\chi}(X)$ are called Bernoulli polynomials for the character χ.

Remark 0.3.5. Notice that

$$B_{n,\chi}(X) = \sum_{i=0}^{n} \binom{n}{i} B_{i,\chi} X^{n-i}.$$

In particular, $B_{n,\chi}(0) = B_{n,\chi}$ for any $n \geq 0$.

Path integration leads to the equality $-\dfrac{L(1-n;\chi)}{\Gamma(n)} = \mathrm{Res}_{z=0}(F_\chi(z)z^{-n-1})$ which, in conjunction with the fact that $\Gamma(n) = (n-1)!$, leads to the following result.

Proposition 0.3.6 (cf. Iwasawa, [34])**.** *For any primitive Dirichlet character χ and for any integer $n \geq 1$,*

$$L(1-n;\chi) = -\frac{B_{n,\chi}}{n}.$$

0.4 Quaternion algebras and quaternion orders

We present here some classical notions on quaternion algebras. We mainly follow [1]. The reader is also referred to [72]. Let $a, b \in \mathbb{Z}$, $a, b \neq 0$ and let $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ be the quaternion $\mathbb{Q}$-algebra generated by I and J with the standard relations $I^2 = a, J^2 = b, IJ = -JI$. Denote $K = IJ$. The reduced trace and the reduced norm of a quaternion $\omega = x + yI + zJ + tK \in H$ are defined by

$$\mathrm{Tr}(\omega) = \omega + \overline{\omega} = 2x, \quad \mathrm{N}(\omega) = \omega\overline{\omega} = x^2 - ay^2 - bz^2 + abt^2,$$

where $\overline{\omega} = x - yI - zJ - tK$ denotes the conjugate of ω. The following map is a monomorphism of $\mathbb{Q}$-algebras

$$\begin{array}{rcl} \psi : \left(\dfrac{a,\ b}{\mathbb{Q}}\right) & \to & \mathrm{M}\left(2, \mathbb{Q}(\sqrt{a})\right) \\ x + yI + zJ + tK & \mapsto & \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix}. \end{array}$$

Notice that for any $\omega \in H$, $\mathrm{N}(\omega) = \det(\psi(\omega))$, and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\psi(\omega))$.

For any place p of $\mathbb{Q}$ (possibly including $p = \infty$), $H_p := H \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a quaternion $\mathbb{Q}_p$-algebra. If H_p is a division algebra, it is said that H is ramified at p. Otherwise, H is said to split at p. As is well known, the quaternion algebra H is ramified at a finite even number of places. The discriminant D_H is defined as the product of the primes at which H ramifies. Moreover, two quaternion $\mathbb{Q}$-algebras are isomorphic if and only if they have the same discriminant.

Definition 0.4.1. Let H be a quaternion $\mathbb{Q}$-algebra. If $D_H = 1$, H is said to be non-ramified; in this case, it is isomorphic to $M(2, \mathbb{Q})$. If H is ramified at $p = \infty$, it is said to be definite, and indefinite otherwise. An indefinite quaternion algebra is said to be small ramified if D_H is equal to the product of two distinct primes.

The following result gives a useful presentation of non-ramified and small ramified quaternion $\mathbb{Q}$-algebras.

Theorem 0.4.2 (Alsina-Bayer, [1])**.** *Let* $H = \left(\frac{a, b}{\mathbb{Q}}\right)$ *be a quaternion* $\mathbb{Q}$*-algebra.*

(i) If $D_H = 1$*, then* $H \simeq \mathrm{M}(2, \mathbb{Q}) \simeq \left(\frac{1, -1}{\mathbb{Q}}\right)$.

(ii) If $D_H = 2p$*,* p *prime,* $p \equiv 3 \pmod 4$*, then* $H \simeq \left(\frac{p, -1}{\mathbb{Q}}\right)$.

(iii) If $D_H = pq$*,* p, q *primes,* $q \equiv 1 \pmod 4$ *and* $\left(\frac{p}{q}\right) = -1$*, then* $H \simeq \left(\frac{p, q}{\mathbb{Q}}\right)$.

If a *and* b *are prime numbers, then* H *satisfies one, and only one, of these three statements.*

Let H be a quaternion $\mathbb{Q}$-algebra. An element $\alpha \in H$ is said to be integral if $\mathrm{N}(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$. A $\mathbb{Z}$-lattice Λ of H is a finitely generated torsion free $\mathbb{Z}$-module contained in H. A $\mathbb{Z}$-ideal of H is a $\mathbb{Z}$-lattice Λ such that $\mathbb{Q} \otimes \Lambda \simeq H$. A $\mathbb{Z}$-ideal is not in general a ring. An order $\mathcal{O}$ of H is a $\mathbb{Z}$-ideal which is a ring. Each order of a quaternion algebra is contained in a maximal order.

In an indefinite quaternion $\mathbb{Q}$-algebra, all the maximal orders are conjugate (cf. [72]). An Eichler order is the intersection of two maximal orders.

Let $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ be an indefinite quaternion $\mathbb{Q}$-algebra. Given a maximal order $\mathcal{O}_H$, denote by $\mathcal{O}_H^1$ the multiplicative group of elements of $\mathcal{O}_H$ of reduced norm equal to 1, and let Γ_H^1 be its image under ψ. A Fuchsian group of the first kind $\Gamma \subseteq \mathrm{GL}(2,\mathbb{R})$ is called arithmetic if it is commensurable with Γ_H^1 for some quaternion algebra H.

Proposition 0.4.3 (cf. [72])**.** *Let $\mathcal{O}$ be an Eichler order of H. Then $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$ is a $\mathbb{Z}_p$-order of H_p. Moreover, there exists a unique $n \geq 0$ such that $\mathcal{O}_p$ is conjugated to the Eichler order*

$$\mathcal{O}_n = \left\{ \begin{pmatrix} a & b \\ cp^n & d \end{pmatrix};\ a,b,c,d \in \mathbb{Z}_p \right\}.$$

The level of the local Eichler order is defined as p^n.

To define the global level of $\mathcal{O}$, write $\mathcal{O} = \mathcal{O}' \cap \mathcal{O}''$ with $\mathcal{O}', \mathcal{O}''$ maximal orders and tensor by $\mathbb{Z}_p$. The global level is then the product of all local levels.

Proposition 0.4.4 (Alsina-Bayer, [1])**.** *Let $N \geq 1$ and p, q be different primes as in Theorem 0.4.2.*

(i) $\mathcal{O}_0(1,N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix};\ a,b,c,d \in \mathbb{Z} \right\}$ *is an Eichler order of level N in* $\mathrm{M}(2,\mathbb{Q})$.

(ii) $\mathcal{O}_M(1,N) = \mathbb{Z} + \mathbb{Z}(J+K)/2 + \mathbb{Z}N(-J+K)/2 + \mathbb{Z}(1-I)/2$ *is an Eichler order of level N in $M = \left(\frac{1,-1}{\mathbb{Q}}\right)$, the matrix algebra.*

(iii) If $D = 2p$, $N|(p-1)/2$ and N is square free, then $\mathcal{O}(2p,N) = \mathbb{Z} + \mathbb{Z}I + \mathbb{Z}NJ + \mathbb{Z}\left(\frac{1+I+J+K}{2}\right)$ is an Eichler order of level N in $\left(\frac{p,-1}{\mathbb{Q}}\right)$, for $N|(p-1)/2$, N square free.

(iv) If $D = pq$, $N|(q-1)/4$, $(N,p) = 1$ and N is square free, then $\mathbb{Z} + \mathbb{Z}NI + \mathbb{Z}(1+J)/2 + \mathbb{Z}(I+K)/2$ is an Eichler order of level N in $\left(\frac{p,q}{\mathbb{Q}}\right)$, for $N|(p-1)/4$, $p \nmid N$, N square free.

Remark 0.4.5. For $D = 1, 2p, pq$, with p, q primes as in 0.4.2, and $N \geq 1$, denote by $\Gamma(D, N)$ the image under ψ of the group of units of reduced norm 1 in the Eichler orders given in Proposition 0.4.4. The groups $\Gamma(D, N)$ are arithmetic Fuchsian groups of the first kind. In particular, $\Gamma(1, N) = \Gamma_0(N)$.

Chapter 1

p-adic L-functions of abelian $\mathbb{Q}$-extensions

Introduction

In this chapter we explain four alternative constructions of the p-adic L-function attached to a real abelian extension of $\mathbb{Q}$, namely, the Kubota-Leopoldt original construction as character averages, the Iwasawa constructions as power series which interpolate special values of Dirichlet L-series and as limits of Stickelberger elements, and the construction as Mazur-Mellin transforms explained in [39]. All of them are equivalent. Special attention has been paid to the original ideas and motivations which led to the introduction of the Kubota-Leopoldt p-adic L-functions, such as the p-adic special values $\mathcal{L}_p(\chi)$ and the p-divisibility of the class numbers. We present some ideas and results from Leopoldt [43] and Kubota-Leopoldt [40] which are not present in the modern expositions on p-adic L-functions, such as the concept of χ-average, which is the main tool in the first definition of p-adic L-function. In Theorem 1.1.15, we prove a formula of Leopoldt which is stated without proof in [43]. In propositions 1.1.28 and 1.1.29, we generalize this theorem, and, finally, we apply this result to give a proof of the non-vanishing of the p-adic Dedekind zeta-function of a real abelian extension $K/\mathbb{Q}$ at $s = 1$ under certain conditions (Corollary 1.1.31).

1.1 p-adic L-functions as character averages

1.1.1 Values of Dirichlet L-functions at $s = 1$.

Let $K/\mathbb{Q}$ be an abelian extension of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings and r_2 the number of complex non-real embeddings of K up to complex conjugation. Let d and h respectively denote the discriminant and the class number of K. Let R be the regulator of K. Since K is contained in a cyclotomic extension, the Galois group $G = \mathrm{Gal}\,(K/\mathbb{Q})$ is isomorphic to a quotient of $(\mathbb{Z}/f\mathbb{Z})^*$ for some $f \in \mathbb{N}$. Let w be the order of the group of roots of unity contained in K, which is well known to be finite. The class number formula in this case is

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|d|}} = \prod L(1;\chi), \tag{1.1.1}$$

the product taken as χ runs through the non-trivial characters of G. Since $R \neq 0$, it follows that $L(1;\chi) \neq 0$ for any character $\chi : G \to \mathbb{C}^*$. A natural question is to study the special values $L(1;\chi)$. For instance, for characters of large enough conductor, knowing the behaviour of $L(1;\chi)$ allows us to describe the asymptotic behaviour of the quantity hR. If all the $L(1;\chi)$ were algebraic up to multiplication by powers of π, one could think of computing the p-adic valuation of hR up to a power of π, and this valuation would equal the sum of the valuations of the factors $L(1;\chi)$ apart from well determined factors coming from (1.1.1). Unfortunately, this is not the case in general. For any Dirichlet character χ denote by $\tau(\chi)$ its Gauss sum. Following Leopoldt [43], denote by $\mathcal{L}_\infty(\chi)$ the value $L(1;\chi)$. One has the following result.

Proposition 1.1.1 (Hasse, [32])**.** *For any primitive Dirichlet character χ of conductor f_χ and for any primitive f_χ-th root of unity,*

$$\mathcal{L}_\infty(\chi) = \frac{-\tau(\chi)}{f_\chi}\sum_{a=1}^{f_\chi}\overline{\chi}(a)\log(1-\zeta^{-a}). \tag{1.1.2}$$

We can work out (1.1.2) to obtain

$$\mathcal{L}_\infty(\chi) = \begin{cases} \frac{\pi i}{f_\chi}\tau(\chi)B_{1,\overline{\chi}}, & \text{if } \chi \text{ is odd,} \\ \\ \frac{-\tau(\chi)}{f_\chi}\displaystyle\sum_{a=1}^{f_\chi}\overline{\chi}(a)\log|1-\zeta^a|, & \text{if } \chi \text{ is even, } \chi \neq 1, \end{cases} \tag{1.1.3}$$

where $B_{j,\chi}$ denotes the j-th generalized Bernoulli number attached to χ.

If χ is odd, (1.1.3) shows that $\mathcal{L}_\infty(\chi)$ is algebraic up to multiplication by π. If χ is even, $\mathcal{L}_\infty(\chi)$ is also transcendent (Baker, [6]) but it is not a product of a power of π by an algebraic number.

Let ζ be an f_χ-th root of unity, which we consider as a p-adic number. In [43], for an even character χ, Leopoldt replaced $\mathcal{L}_\infty(\chi)$ by a p-adic analogue $\mathcal{L}_p(\chi)$ defined as

$$\mathcal{L}_p(\chi) = -\frac{\tau(\chi)}{f_\chi}\sum_{a=1}^{f_\chi}\overline{\chi}(a)\log_p(1-\zeta^a) \tag{1.1.4}$$

and established a p-adic version of the class number formula with a view to extracting some information about the class number. Two natural questions arise: what is the relation between $\mathcal{L}_p(\chi)$ and $\mathcal{L}_\infty(\chi)$? and for which pairs (χ, p) does $\mathcal{L}_p(\chi)$ vanish? The following result provides a partial answer to the second question.

Proposition 1.1.2 (Leopoldt, [43], 1.8)**.** *Suppose that $p \nmid 2f_\chi$ and that $\chi(-1) = 1$. Then*

$$\mathcal{L}_p(\chi) \equiv \overline{\chi(p)}\frac{B_{p-1,\chi}}{p-1}p \pmod{p^2}.$$

Remark 1.1.3. We point out that the p-adic value of $\tau(\chi)$ depends on the embedding $\mathbb{Q}^{alg} \hookrightarrow \mathbb{Q}_p^{alg}$, which we fix once and from now on.

1.1.2 The p-adic class number formula for a real abelian extension of $\mathbb{Q}$.

In the rest of this chapter, we suppose that $K/\mathbb{Q}$ is a real abelian extension. This implies that all the characters of G are even. Let g denote the degree of $K/\mathbb{Q}$.

Definition 1.1.4. (The p-adic regulator) Let $\{\varepsilon_1, ..., \varepsilon_{g-1}\}$ be a fundamental system of units of $\mathcal{O}_K$. Let $\{\sigma_1, ..., \sigma_g\}$ be the embeddings of K into $\mathbb{Q}^{alg}$. The p-adic regulator of K is

$$R_p(K) = \det\left(\log_p\left(\sigma_j\left(\varepsilon_k\right)\right)\right)_{j,k=1}^{g-1}.$$

Remark 1.1.5. Note that one σ_k is missing. Since $\prod_{j=1}^{g} \sigma_j(\varepsilon_k) = 1$ for any k, the p-adic regulator is well defined up to a sign.

The fact that a change of fundamental system of units is given by a unimodular matrix implies that, up to a sign, $R_p(K)$ does not depend on the choice of the units. More in general, let $\{\varepsilon'_1, ..., \varepsilon'_{g-1}\}$ be a system of independent units. This means that the subgroup H generated by $\{\varepsilon'_1, ..., \varepsilon'_{g-1}\}$ and by the roots of unity in K has finite index in $\mathcal{O}_K^*$. The p-adic regulator of H is defined, up to a sign, as

$$R_p(H) = \det\left(\log_p(\sigma_j(\varepsilon'_k))\right)_{j,k=1}^{g-1}.$$

Proposition 1.1.6. $R_p(H) = [\mathcal{O}_K^* : H] R_p(K)$.

Proof. Denote $A = \left(\log_p(\sigma_j(\varepsilon_k))\right)_{j,k=1}^{g-1}$ and $B = \left(\log_p(\sigma_j(\varepsilon'_k))\right)_{j,k=1}^{g-1}$. For any $1 \leq k \leq g-1$, set

$$\varepsilon'_k = \omega_k \prod_{j=1}^{g-1} \varepsilon_1^{n_{1,k}} ... \varepsilon_{g-1}^{n_{g-1,k}},$$

with $\omega_k = \pm 1$. Set $N = (n_{j,k})_{j,k=1}^{g-1}$. Then,

$$B = AN^t.$$

But $\det(N) = [\mathcal{O}_K^* : H]$. □

In [43], Leopoldt finds a p-adic class number formula, namely:

$$\frac{2^{g-1} h R_p(K)}{\sqrt{d}} = \prod \mathcal{L}_p(\chi), \tag{1.1.5}$$

where χ runs through the nontrivial characters of G. We illustrate the proof of (1.1.5) for the maximal real subfield of the cyclotomic extension $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$. Denote by $F_{p^n}^+$ this maximal real subfield. The general argument to prove (1.1.5) is essentially the same as the one presented here, apart from the fact that the general fundamental system of units is not the naive generalization

of the system we present in this easier case. We refer the reader to Washington, [74], ch. 8. Denote by $h^+_{p^n}$ and $d_{F^+_{p^n}}$, respectively, the class number and the discriminant of $F^+_{p^n}$. For any integer $1 < a \leq \frac{p^{n-1}(p-1)}{2}$, denote

$$\xi_a = \zeta_{p^n}^{\frac{1-a}{2}} \frac{1-\zeta_{p^n}^a}{1-\zeta_{p^n}}.$$

This element is a unit of the ring of integers of $F^+_{p^n}$. Denote by C^+_n the subgroup generated by these elements. The explicit form of the eigenvalues of the matrix defining the p-adic regulator plays an important role in the p-adic class number formula. In [43] and in [34], they are computed by using properties of circular matrices. We follow the approach of [74]. The following lemma will help us to identify these eigenvalues.

Lemma 1.1.7 (cf. Washington, [74], ch. 5)**.** *Let G be a finite abelian group and f be a function on G with values in an algebraically closed field k of characteristic 0. Then,*

(i) the eigenvalues of the matrix $\left(f\left(\sigma\tau^{-1}\right)\right)_{\sigma,\tau\in G}$ are

$$\left\{\sum_{\sigma\in G}\chi(\sigma)f(\sigma)\right\},$$

as χ runs through the k-valued characters of G.

(ii) $\det\left(f\left(\sigma\tau^{-1}\right)-f(\sigma)\right)_{\sigma,\tau\neq 1} = \prod_{\chi\neq 1}\sum_{\sigma\in G}\chi(\sigma)f(\sigma).$

Proof. (i) Consider the finite-dimensional k-vector space V of k-valued functions on G. Then, G acts on V, via the action $\sigma\cdot h(x) := h(\sigma x)$, with $\sigma, x \in G$ and $h \in V$. Define the k-linear endomorphism $T : V \to V$ by the rule $T(\phi) = \sum_{\sigma\in G} f(\sigma)\left(\sigma\cdot\phi\right)$. Let us denote by ϕ_τ the characteristic function of $\tau \in G$, i.e., $\phi_\tau(\sigma) = 1$ if $\tau = \sigma$ and 0 otherwise. It is easy to see that the characteristic functions form a basis of V. For any $\tau, \tau_0 \in G$, we have that $T(\phi_\tau)(\tau_0) = \sum_{\sigma\in G} f(\sigma)\phi_\tau(\sigma\tau_0)$. Setting $\alpha = \sigma^{-1}\tau$, we obtain that $T(\phi_\tau)(\tau_0) = \sum_{\alpha\in G} f(\tau\alpha^{-1})\phi_\alpha(\tau_0)$. This means that the matrix of T with respect to the basis of V given by the characteristic functions is $\left(f(\sigma\tau^{-1})\right)_{\sigma,\tau\in G}$. On the other hand, since the characters χ of G are linearly independent, they

also form a basis for V. But $T(\chi)(\tau) = \sum_{\sigma\in G} f(\sigma)\chi(\sigma)\chi(\tau)$, which implies that χ is an eigenfunction for T with eigenvalue $\sum_{\sigma\in G} f(\sigma)\chi(\sigma)$.

(ii) Set $W = \left\{ h \in V : \sum_{\sigma\in G} h(\sigma) = 0 \right\}$, and for any $\tau \in G$, denote $\psi_\tau(\sigma) = \phi_\tau(\sigma) - |G|^{-1}$. Then, the set $\{\psi_\tau : \tau \neq 1\}$ is a basis of W. The matrix of the statement is the matrix of the endomorphism T restricted to W in this base. The result follows from the fact that the non-trivial characters of G form a diagonal basis of W. □

We need two more technical lemmas. The following one is known in the literature as the *Führer-Diskriminant Produktformel*.

Lemma 1.1.8 (Washington, [74], ch. 3)**.** *Let K be a number field of degree $n = r_1 + 2r_2$ and discriminant d_K associated to a group of Dirichlet characters. Then,*

(i) $(-1)^{r_2} \prod_{\chi\neq 1} f_\chi = d_K$, *and*

(ii) $$\prod_{\chi\neq 1} \tau(\chi) = \begin{cases} \sqrt{|d_K|} \text{ if } K \text{ is totally real,} \\ \\ i^{r_2}\sqrt{|d_K|} \text{ if } K \text{ is complex.} \end{cases}.$$

□

Lemma 1.1.9. $h^+_{p^n} = \left[\mathcal{O}^*_{F^+_{p^n}} : C^+_n \right]$.

Proof. By using Lemma 1.1.7 with $G = \mathrm{Gal}\left(F^+_{p^n}/\mathbb{Q}\right)$ and $f(\sigma) = \log|1-\zeta^\sigma_{p^n}|$, we have that

$$R\left(C^+_n\right) = \pm \prod_{\chi\neq 1} \frac{1}{2} \sum_{a=1}^{p^n} \chi(a) \log\left|1 - \zeta^a_{p^n}\right|.$$

Since $\sum_{a=1}^{p^n} \chi(a)\log\left|1-\zeta^a_{p^n}\right| = -\dfrac{f_\chi}{\tau(\chi)}\mathcal{L}_\infty(\overline{\chi})$, and χ runs through the characters of $\mathrm{Gal}\left(F^+_{p^n}/\mathbb{Q}\right)$ if and only if $\overline{\chi}$ runs through the characters of $\mathrm{Gal}\left(F^+_{p^n}/\mathbb{Q}\right)$, by using Lemma 1.1.8, we obtain

$$R\left(C^+_n\right) = \pm \frac{\sqrt{d_{F^+_{p^n}}}}{2^{g-1}} \prod_{\chi\neq 1} \mathcal{L}_\infty(\chi).$$

The result follows from the classical class number formula. □

Theorem 1.1.10. *There exists a fundamental system of units such that*

$$\frac{2^{g-1}h_{p^n}^{+}R_p\left(F_{p^n}^{+}\right)}{\sqrt{d_{F_{p^n}^{+}}}}=\prod_{\chi\neq 1}\mathcal{L}_p(\chi).$$

Proof. By Lemma 1.1.8 and Lemma 1.1.7 with $G=\mathrm{Gal}\left(F_{p^n}^{+}/\mathbb{Q}\right)$ and $f(\sigma)=\log_p(1-\zeta_{p^n}^{\sigma})$, we have that

$$R_p\left(C_n^{+}\right)=\pm\prod_{\chi\neq 1}\frac{1}{2}\sum_{a=1}^{p^n}\chi(a)\log_p\left(1-\zeta_p^a\right)=\pm\frac{\sqrt{d_{F_{p^n}^{+}}}}{2^{g-1}}\prod_{\chi\neq 1}\mathcal{L}_p(\chi).$$

Now, use Lemma 1.1.9 and Proposition 1.1.6 and the result follows. □

The following result is interesting in itself.

Proposition 1.1.11. *The $\mathbb{Z}_p$-rank of $\mathcal{O}_{F_{p^n}^{+}}^{*}\otimes\mathbb{Z}_p$ equals the number of characters χ such that $\mathcal{L}_p(\chi)\neq 0$.*

Proof. The $\mathbb{Z}_p$-rank of $\mathcal{O}_{F_{p^n}^{+}}^{*}\otimes\mathbb{Z}_p$ equals the $\mathbb{Z}_p$-rank of the additive group generated by $\{\xi_a\}_{a=2}^{g-1}$, which equals the $\mathbb{Q}_p$-rank of the matrix

$$\left(\log_p\left(\sigma_k\left(\xi_a\right)\right)\right)_{k,a-1=1}^{g-1}.$$

But the eigenvalues of this matrix, by Lemma 1.1.7, are precisely

$$\sum_{a=1}^{g-1}\chi(a)\log_p(1-\zeta_{p^n}^a)=-\frac{f_\chi}{\tau\left(\chi\right)}\mathcal{L}_p(\overline{\chi}).$$

□

1.1.3 Applications.

Let $K/\mathbb{Q}$ be a real abelian extension of degree g, class number h and discriminant d. Let ζ_K be the Dedekind zeta function of K and ζ the Riemann zeta function.

Definition 1.1.12 (cf. Leopoldt, [43])**.** For any $z \in \mathbb{Z}_p^*$, the Fermat quotient of $z \pmod p$, denoted by $Q_p(z)$, is the reminder of $(z^{p-1}-1)/p \pmod p$.

Proposition 1.1.13. *For any $z \in \mathbb{Z}_p^*$,*

$$\log_p(z) \equiv -pQ_p(z) \pmod{p^2}.$$

Proof. Write $z = \omega(z)\langle z\rangle$ and $\langle z\rangle = 1 + p\tilde{z}$. Then,

$$\log_p(z) = \log_p(\langle z\rangle) \equiv p\tilde{z} \pmod{p^2}.$$

Since $Q_p(z) = (p-1)\tilde{z} + \frac{p(p-2)(p-1)}{2}\tilde{z}^2 + O(p^2)$, the result holds. □

Definition 1.1.14 (Leopoldt, [43])**.** Given a fundamental system of units $\{\varepsilon_j\}_{j=1}^{g-1}$, the p-adic regulator mod p attached to this system of units is

$$R^{(p)}(K) = \det\left(Q_p\left(\sigma_j\left(\varepsilon_k\right)\right)\right)_{j,k=1}^{g-1}.$$

Theorem 1.1.15. *Let $K/\mathbb{Q}$ be a real abelian extension and let p be a prime such that for any character χ of $\mathrm{Gal}\,(K/\mathbb{Q})$ of conductor f_χ, $p \nmid 2f_\chi$. Then, with the above notations, there exists a fundamental system of units, a choice of the square root and an ordering of the Galois embeddings of K into $\mathbb{Q}^{alg}$ such that*

$$\frac{2^{g-1}hR^{(p)}(K)}{\sqrt{d}} \equiv \frac{\zeta_K(2-p)}{\zeta(2-p)} \pmod p.$$

Proof. From the very definition of p-adic regulator mod p, for any fundamental system of units we have that $R_p(K) \equiv (-p)^{g-1}R^{(p)}(K) \pmod{p^g}$. From the p-adic class number formula, there exists a fundamental system of units such that

$$\frac{2^{g-1}hR_p(K)}{\sqrt{d}} = \prod \mathcal{L}_p(\chi).$$

Using Proposition 1.1.2, we obtain that

$$\prod_{\chi\neq 1} \mathcal{L}_p\left(\chi\right) \equiv (-p)^{g-1} \prod_{\chi\neq 1} L\left(2-p;\chi\right) \bmod (p^g). \tag{1.1.6}$$

But the left hand side of (1.1.6) is congruent to $\dfrac{(-p)^{g-1}2^{g-1}hR^{(p)}(K)}{\sqrt{d}}$ (mod p^g). □

Remark 1.1.16. In Leopoldt's formula (3.8) in [43], the right hand side of the congruence is multiplied by $\left(\frac{d}{p}\right)$, the Legendre symbol of d over p. Notice that Theorem 1.1.15 does not contradict Leopoldt's original formula, since the regulator is defined up to a sign.

Corollary 1.1.17 (Leopoldt, [43])**.** *Let p be an odd prime. Then, $p \nmid \frac{\zeta_K(2-p)}{\zeta(2-p)}$ if and only if it satisfies the following conditions:*

(i) K does not ramify at p,

(ii) p is coprime to h, and

(iii) for any $a \in \mathcal{O}_K$ such that $a \equiv 1 \pmod{p}$ and $N_{K/\mathbb{Q}}(a) \equiv 1 \pmod{p^2}$, there exists $u \in \mathcal{O}_K^*$ such that that $a \equiv u \pmod{p^2}$.

□

1.1.4 The Kubota-Leopoldt p-adic L-function

In view of the p-adic class number formula, it seems natural to see the p-adic quantities $\mathcal{L}_p(\chi)$ as $L_p(1;\chi)$ for suitable functions $L_p(s;\chi)$ which could be seen as p-adic analogues of $L(s;\chi)$. This task was fulfilled by Kubota and Leopoldt in [40] and [41]. In this section we present the construction of $L_p(s;\chi)$ and in section 2.2 we will explain the proof that $L_p(1;\chi) = \mathcal{L}_p(\chi)$.

Denote

$$\mathbb{Q}_p[[X]]_b = \left\{ A = \sum_{n_0}^{\infty} a_n (X-1)^n \mid \lim_{n\to\infty} |a_n q^n|_p = 0 \text{ for any } q \in p\mathbb{Z}_p \right\}.$$

For $A \in \mathbb{Q}_p[[X]]_b$, the assignment $||A||_p = \sup_{n\geq 0} |a_n q^n|_p$ is a norm. The $\mathbb{Q}_p$-vector space $\mathbb{Q}_p[[X]]_b$ endowed with this norm is a Banach $\mathbb{Q}_p$-algebra.

Definition 1.1.18. Given $A \in \mathbb{Q}_p[[X]]_b$ and χ a Dirichlet character of conductor f_χ, set $\overline{f}_\chi = \operatorname{lcm}(f_\chi, q)$ where $q = 4$ if $p = 2$ and $q = p$ otherwise. Let $n \geq 1$ an integer. The n-th character average for χ is

$$M_\chi^n(A) = \frac{1}{\overline{f}_\chi q^n} \sum_{a=1}^{\overline{f}_\chi q^n} \chi(a) A(\langle a \rangle).$$

For any Dirichlet character χ, let us denote by $\mathbb{Q}_p(\chi)$ the finite extension of $\mathbb{Q}_p$ obtained by adjoining to $\mathbb{Q}_p$ the finite set $\{\chi(a) : a \in \mathbb{Z}\}$. Notice that $M_\chi^n(A) \in \mathbb{Q}_p(\chi)$.

Proposition 1.1.19. *For any $A \in \mathbb{Q}_p[[X]]_b$, there exists $\lim_{n\to\infty} M_\chi^n(A)$.*

Proof. It is consequence of the following identity:

$$\overline{f_\chi} q^{n+1}\left(M_\chi^{n+1}(A) - M_\chi^n(A)\right) = \sum_{k=1}^{\overline{f}_\chi q^n} \chi(k) \sum_{j=0}^{q-1} A(\langle k + \overline{f}_\chi q^n j\rangle) - qA(\langle k\rangle).$$

□

Denote this limit by $M_\chi(A)$. Since $\mathbb{Q}_p$ is complete, $M_\chi(A) \in \mathbb{Q}_p(\chi)$. For any Dirichlet character χ, there exists $C_\chi \geq 0$ such that for any power series $A \in \mathbb{Q}_p[[X]]_b$,

$$|M_\chi(A)|_p \leq C_\chi ||A||_p.$$

Let $s \in \mathbb{Z}_p$ be a fixed p-adic integer. Define $P_s(u) = \sum_{n\geq 0} \binom{s}{n}(u-1)^n$. By taking p-adic valuations of the combinatorial numbers we see that $P_s \in \mathbb{Q}_p[[X]]_b$.

Definition 1.1.20. (Kubota-Leopoldt, [40]) The p-adic L-function is

$$L_p(s;\chi) = \frac{1}{s-1} M_\chi(P_{1-s}).$$

For any integer $n \geq 1$ and for any Dirichlet character χ, denote by χ_n the character $\chi\omega^{-n}$ (the product of characters defined as usual).

Theorem 1.1.21 (Kubota-Leopoldt, [40])**.** *There exists $r > 1$ such that $L_p(s;\chi)$ is holomorphic (meromorphic if $\chi = 1$) on $D(1,r) \subseteq \mathbb{Q}_p$. Moreover, for any $n \geq 1$, we have*

$$L_p(1-n;\chi) = -(1 - \chi_n(p)p^{n-1})\frac{B_{n,\chi_n}}{n}.$$

Remark 1.1.22. As we will see in next section, property 1.1.21 characterizes the p-adic L-function. In particular, for any $n \equiv 0 \bmod (p-1)$, we have

$$L_p(1-n;\chi) = -(1-\chi(p)p^{n-1})\frac{B_{n,\chi}}{n}.$$

Next, we show how the continuity of the p-adic L-function can be used to approximate the values $L_p(1;\chi)$ and to control the error term. Since

$$L_p(1;\chi) = \lim_{|s|_p \to 0} L_p(1-s;\chi),$$

the values $\left(1-\chi(p)p^{p^m(p-1)-1}\right)\dfrac{B_{p^m(p-1),\chi}}{p^m(p-1)}$ approximate $L_p(1;\chi)$ for large enough m. The natural question is how to control the error term.

Lemma 1.1.23 (Kubota-Leopoldt, [40])**.** *Let $G \in \mathbb{Q}_p[[X]]_b$ be a power series and denote by G' its formal derivative. Let $n_0 \geq 0$ be such that $\left|M^{n_0}_{\chi\omega^{-1}}(G')\right|_p \leq \left|\frac{1}{6}\right|_p$. Then,*

$$\left|M_\chi(G) - M^n_\chi(G)\right|_p \leq \left|\frac{\overline{f}_\chi q^n}{12}\right|_p.$$

Proposition 1.1.24. *Suppose that $pq \nmid f_\chi$ and that $p > 3$. Then, for any $s \in \mathbb{Z}_p$,*

$$|L_p(1;\chi) - L_p(1-s;\chi)|_p \leq |ps|_p.$$

Proof. Let us denote by $I(u) = 1$ the identity of the ring $\mathbb{Q}[[u]]_b$. Define

$$L(u) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(u-1)^n.$$

A simple calculation shows that

$$\frac{1}{s}(P_s(u) - I(u)) = \sum_{n=1}^{\infty} \frac{1}{n}\binom{s-1}{n-1}(u-1)^n.$$

Denote this power series by $H_s(u)$. Clearly, $H_s(u) \in \mathbb{Q}_p[[u]]_b$. Denote

$$G_s(u) = \frac{1}{s}\left(H_s(u) - L(u)\right).$$

One can show that

$$G_s(u) = \sum_{n=0}^{\infty} \frac{L(u)^{n+2}}{(n+2)!} s^n,$$

hence, by ultrametricity, one has that, for any $u \in D(1,p)^+$, and $s \in \mathbb{Z}_p$,

$$|G_s(u)|_p \leq \max_{m\geq 2} \left|\frac{q^m}{m!}\right|_p \leq \left|\frac{q^2}{2}\right|_p < 1.$$

In particular, we have

$$\left|M^0_\chi(G_s)\right|_p \leq p^{-1}.$$

On the other hand, it is easy to see that

$$\left|M^0_{\chi\omega^{-1}}(G'_s)\right|_p \leq \left|\frac{q}{2}\right|_p.$$

Hence, by using Lemma 1.1.23, one has, in particular, that for $n \geq 0$,

$$\left|M_\chi(G_s) - M^n_\chi(G_s)\right|_p \leq p^{-1}.$$

Since

$$\left|M^n_\chi(G_s)\right|_p \leq \max\left(\left|M^n_\chi(G_s) - M_\chi(G_s)\right|_p, \left|M^0_\chi(G_s) - M_\chi(G_s)\right|_p, \left|M^0_\chi(G_s)\right|_p\right),$$

we conclude that

$$\left|M^n_\chi(G_s)\right|_p \leq p^{-1}.$$

Now, by taking limit in n, we have

$$\left|M_\chi(G_s)\right|_p \leq p^{-1}.$$

To finish, observe that $M_\chi(H_s) = -L_p(1-s;\chi)$ and $M_\chi(L_s) = L_p(1;\chi)$. Hence,

$$\left|\frac{1}{s}\left(L_p(1;\chi) - L_p(1-s;\chi)\right)\right|_p = |M_\chi(G_s)|_p < p^{-1}.$$

□

As an application of Proposition 1.1.24, to close this section, we generalize the results of section 1.3.

For $z \in \mathbb{Z}_p^*$, write $z = \omega(z)\langle z\rangle$, where $\langle z\rangle = (1+p\tilde{z})$. Denote by $Q_{p,n}(z)$ the truncation of the series $\frac{-1}{p}\log_p(1+p\tilde{z}) \pmod{p^{n+1}}$.

Definition 1.1.25. Let $\{\varepsilon_1, ..., \varepsilon_{g-1}\}$ be a fundamental system of units of K. The p-adic regulator modulo p^n attached to this system is

$$R^{(p,n)}(K) = \det\left(Q_{p,n}\left(\sigma_j(\varepsilon_k)\right)\right)_{1\leq j,k\leq g-1}.$$

The following lemma is obvious from the definition of $Q_{p,n}$.

Lemma 1.1.26. *For any integer $n \geq 1$, $-pQ_{p,n}(z) \equiv \log_p(z) \pmod{p^{n+2}}$.*

As a direct consequence of this lemma, we have the following result.

Proposition 1.1.27. *For any integer $n \geq 1$, there exists a fundamental system of units such that $R_p(K) \equiv (-p)^{g-1}R^{(p,n)}(K) \pmod{p^{n+g}}$.*

□

We will see in the next section that $L_p(1;\chi) = \mathcal{L}_p(\chi)$, but for the moment, we take it for granted. Under this assumption, we can prove the following generalization of Proposition 1.1.15, which can be used as a means to approximate p-adically the quotient of the Dedekind zeta function of K at the values $1-(p-1)p^n$ over the Riemann zeta function at the same values.

Proposition 1.1.28. *Let $K/\mathbb{Q}$ be a real abelian extension of degree g and $p > 3$ an unramified prime for K such that for any character χ of $\mathrm{Gal}(K/\mathbb{Q})$, $p \nmid f_\chi$. Then, there exists a fundamental system of units of $\mathcal{O}_K^*$, a choice of the square root and an ordering of the Galois embeddings of K into $\mathbb{Q}^{alg}$ such that for any $n \geq 1$,*

$$\frac{2^{g-1}hR^{(p,n)}(K)}{\sqrt{d}} \equiv (-1)^{g-1}\,\frac{\zeta_K(1-p^n(p-1))}{\zeta(1-p^n(p-1))} \pmod{p^{n+1}}.$$

Proof. Given an integer $n \geq 1$, by using Lemma 1.1.26 we have that $R_p(K) \equiv (-p)^{g-1}R^{(p,n)}(K) \pmod{p^{n+g}}$. By using Proposition 1.1.24 and Theorem 1.1.21, we obtain

$$\prod_{\chi\neq 1}\mathcal{L}_p(\chi) \equiv p^{g-1}\prod_{\chi\neq 1}L\left(1-p^n(p-1);\chi\right) \pmod{p^{n+g}}. \tag{1.1.7}$$

By formula 1.1.5, the left hand side of (1.1.7) equals $\dfrac{2^{g-1}hR_p(K)}{\sqrt{d}}$, which is congruent to $\dfrac{(-p)^{g-1}2^{g-1}hR^{(p,n)}(K)}{\sqrt{d}} \pmod{p^{n+g}}$. Dividing by p^{g-1}, the result follows. □

With Proposition 1.1.28, we can formulate the following result on the non-vanishing mod p of the classical Dedekind zeta function

Corollary 1.1.29. *Let $K/\mathbb{Q}$ be a real abelian extension. Let $p > 3$ be an unramified prime such that $(p, h_k) = 1$ and $R_p(K) \in p^{g-1}\mathbb{Z}_p^*$. Then, for any $n \geq 1$,*

$$p \nmid \frac{\zeta_K\left(1 - p^n(p-1)\right)}{\zeta(1 - p^n(p-1))}.$$

Proof. If $R_p(K) \in p^{g-1}\mathbb{Z}_p^*$, then, for any $n \geq 1$, $R^{(p,n)}(K) \in \mathbb{Z}_p^*$. Since p is unramified at K, $(p, d_K) = 1$. Since $(p, h_K) = 1$, the right hand side of the equality of Proposition 1.1.28 is a p-adic unit. Hence, the result follows. □

Definition 1.1.30. (Iwasawa, [34]) Let $K/\mathbb{Q}$ be a real abelian extension of $\mathbb{Q}$. The p-adic Dedekind zeta function of K is $\zeta_{K,p}(s) = \prod L_p(1 - s; \chi)$, where the product runs through the group of characters of $\mathrm{Gal}(K/\mathbb{Q})$.

The function $\zeta_{K,p}$ is meromorphic with a simple pole at $s = 0$, which can be cancelled out dividing by $L_p(1-s; 1)$. The quotient is, hence, an analytic function which we denote by $\zeta_{K/\mathbb{Q},p}$. By passing to the limit in Corollary 1.1.29, we can easily prove the following result.

Corollary 1.1.31. *Let $K/\mathbb{Q}$ be a real abelian extension. Let p be an unramified prime such that $(p, h_k) = 1$ and $R_p(K) \in p^{g-1}\mathbb{Z}_p^*$. Then,*

$$\left|\zeta_{K/\mathbb{Q},p}(1)\right|_p = 1.$$

1.2 p-adic L-functions as power series

1.2.1 Iwasawa construction of p-adic L-functions

Notice that $\mathbb{Q}_p[[X]]_b$ contains $\mathbb{Q}_p[X]$ as a dense subset. We will use the following

Lemma 1.2.1. *Let $\{b_n\}_{n\geq 0}$ be a sequence of elements of $\mathbb{Q}_p$, and define*

$$c_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k, \quad n \geq 0.$$

Then,

$$b_n = \sum_{k=0}^{n} \binom{n}{k} c_k.$$

Proof. It is straightforward after the following observation:

$$e^t \sum_{n=0}^{\infty} c_n \frac{t^n}{n!} = \sum_{n=0}^{\infty} b_n \frac{t^n}{n!}.$$

□

As we have seen in Theorem 1.1.21, $L_p(s;\chi)$ is holomorphic (meromorphic if $\chi = 1$) on a certain disc. We present here an alternative construction of $L_p(s;\chi)$.

Theorem 1.2.2 (Iwasawa, [34])**.** *There exists a unique meromorphic p-adic L-function $L_p(s;\chi)$ with the following properties:*

(i) $L_p(s;\chi) = \sum_{n=-1}^{\infty} a_n (s-1)^n$ *with* $a_n \in \mathbb{Q}_p(\chi)$.

(ii) If $\chi = 1$, then $a_{-1} = 1 - \frac{1}{p}$. Otherwise, $L_p(s;\chi)$ is holomorphic in $D\left(1, p^{\frac{1}{p-1}} q\right) \subseteq \mathbb{Q}_p^{alg}$, where $q = p$ if $p > 2$, and $q = 4$ for $p = 2$.

(iii) For any $n \in \mathbb{Z}$ with $n \geq 1$,

$$L_p(1-n;\chi) = \left(1 - \chi_n(p) p^{n-1}\right) L(1-n;\chi_n).$$

Proof. Set

$$b_n = \left(1 - \chi_n(p) p^{n-1}\right) B_{n,\chi_n},$$

and

$$c_n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} b_i.$$

Now consider the polynomials

$$A_n(x) = \sum_{k=0}^{n} c_k \binom{x}{k}.$$

According to Lemma 1.2.1, $A_n(n) = b_n$ for any $n \geq 0$. Next, observe that there exists $0 < r < p^{\frac{-1}{p-1}}$ such that

$$|c_n|_p \leq r^n.$$

In fact, we can consider $r = q^{2-n}|f^{-1}|_p$, where f is the conductor of χ. This is quite a technical calculation; it is not essential for the construction we are considering, and its proof can be found in [34]. Set $r_1 = p^{-\frac{1}{p-1}}r$. Given two integers $k < l$,

$$||A_l - A_k||_p \leq \max_{k \leq j \leq l} \left|\left| c_j \binom{x}{j} \right|\right|_p \leq r_1^{k+1}.$$

Since $\mathbb{Q}_p[[X]]_b$ is complete, the sequence $\{A_n\}_{n\geq 1}$ has a limit $A_\chi \in \mathbb{Q}_p[[X]]_b$. Now define

$$L_p(s;\chi) = (s-1)^{-1}A_\chi(1-s).$$

This function satisfies the hypotheses of the theorem. For the uniqueness, notice that A_χ is continuous on its domain and that the positive integers are dense in $\mathbb{Z}_p$. □

Remark 1.2.3. Notice that, in particular, the function $L_p(s;\chi)$ is defined in $\mathbb{Z}_p$, which is contained in $D\left(1, p^{-\frac{1}{p-1}}q\right)$.

Remark 1.2.4. By uniqueness, the p-adic L-functions constructed in Theorem 1.2.2 agree with those defined in 1.1.20.

1.2.2 The Γ-transform and the calculation of $L_p(1;\chi)$

The aim here is to explain a proof of the fact that $L_p(1;\chi) = \mathcal{L}_p(\chi)$. Throughout this subsection, we extend to $\mathbb{Z}_p$ the character $x \mapsto \langle x \rangle$ by setting $\langle px \rangle = 0$ for $x \in \mathbb{Z}_p$. Denote

$$\mathbb{Q}_p[[X]]_m = \left\{ \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[x]] : \ |a_n n!| \to 0 \text{ as } n \to \infty \right\}.$$

Obviously, $\mathbb{Q}_p[X]$ is dense in $\mathbb{Q}_p[[X]]_m$. Now, for any integer $n \geq 0$ and for any $s \in \mathbb{Z}_p$, let us consider

$$\gamma_n(s) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \langle i \rangle^s.$$

As a function of s, $\gamma_n \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$. We will use the following

Lemma 1.2.5. *For any $s \in \mathbb{Z}_p$, $|\gamma_n(s)|_p \leq p^{-\frac{n-\sigma(n)}{p-1}}$.*

Proof. By density, it suffices to prove that for any $m \in \mathbb{N}$ with $(p-1)|m$ and $p^{-m} \leq |n!|_p$,

$$|\gamma_n(m)|_p \leq |n!|_p.$$

Notice that

$$\gamma_n(m) = \sum_{p \nmid k, k=0}^{n} (-1)^{n-k} \binom{n}{k} \langle k \rangle^m,$$

hence

$$\gamma_n(m) \equiv \sum_{k=0}^{n} (-1)^{k-n} \binom{n}{k} \pmod{p^m}.$$

It is not difficult to establish that $n!$ divides the right hand side of the congruence. □

For any $s \in \mathbb{Z}_p$, some algebraic manipulation leads to

$$\langle x \rangle^s = \sum_{n=0}^{\infty} \gamma_n(s) \binom{s}{n}. \tag{1.2.1}$$

Definition 1.2.6. The Γ transform is defined on $\mathbb{Q}_p[X](\mathbb{Z}_p, \mathbb{Q}_p)$ by setting

$$\Gamma(X^n)(s) = \gamma_n(s).$$

The image of Γ lies in $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$, and by Lemma 1.2.5, Γ can be extended to $\mathbb{Q}_p[[X]]_m$ in a unique way. Denote $\Gamma(A)(s) = \Gamma_A(s)$. It is easy to check (by doing so on polynomials) that for any $A \in \mathbb{Q}_p[[X]]_m$,

$$\|\Gamma(A)\|_p \leq \|A\|_p.$$

Definition 1.2.7. Given $A(X) = \sum_{n=0}^{\infty} a_n X^n \in K[[X]]$, define

$$DA(X) = (1+X)\mathrm{Log}_p(1+X)A'(X),$$

where $A'(X)$ is the formal derivative of A.

Notice that $\mathrm{Log}_p(1+X) \in \mathbb{Q}_p[[X]]_m$, and hence, $DA \in \mathbb{Q}_p[[X]]_m$. Next, we list some properties of the Γ transform which allow to compute $L_p(1;\chi)$.

Lemma 1.2.8. *If $A(X) = (1+X)^n$, then, $\Gamma_A(s) = \langle n \rangle^s$.*

Proof. It follows directly by the very definition of Γ and by (1.2.1). □

The formal power series $e^T - 1 = \sum_{n=1}^{\infty} \frac{T^k}{k!}$ has a zero of order 1 at $T = 0$, hence, we can write

$$\left(e^T - 1\right)^n = \sum_{k=n}^{\infty} d_{n,k} \frac{T^k}{k!}, \quad d_{n,k} \in \mathbb{Z}$$

so that for any power series $A(T) = \sum_{n=0}^{\infty} a_n T^n \in \mathbb{Q}_p[[X]]_m$, we have

$$A(e^T - 1) = \sum_{n=0}^{\infty} \delta_n(A) \frac{T^n}{n!},$$

with $\delta_n(A) = \sum_{k=0}^{n} a_k d_{n,k}$ (notice that $d_{1,k} = 1$ for any $k \geq 0$). The following result gives a more tractable way to compute the Γ transform of a power series. We omit the proof, which can be found at [34].

Lemma 1.2.9. *For any $A \in \mathbb{Q}_p[[X]]_m$, for any $s \in \mathbb{Z}_p$ and for any sequence $\{n_k\}_{k\geq 1}$ such that $(p-1)|n_k$ and $\lim_{k\to\infty} n_k = s$ (p-adically), we have*

$$\Gamma_A(s) = \lim_{k\to\infty} \delta_{n_k}(A).$$

□

Lemma 1.2.10. *For any $A \in \mathbb{Q}_p[[X]]_m$ and for any $s \in \mathbb{Z}_p$, $s\Gamma_A(s) = \Gamma_{DA}(s)$.*

Proof. It suffices to note that $\delta_n(DA) = n\delta_n(A)$, which is a straightforward calculation. Now take p-adic limit on both sides. □

Lemma 1.2.11. *For any $A \in \mathbb{Q}_p[[X]]_m$,*

$$\Gamma_A(0) = A(0) - \frac{1}{p}\sum_{\zeta^p=1} A(\zeta - 1).$$

Proof. Since $|\zeta - 1| = p^{-\frac{1}{p-1}}$, it follows that $A(\zeta - 1)$ is well defined. By continuity, it suffices to prove the lemma for $A(X) = (1+X)^m$ for $m \geq 0$. We consider separately the cases where $p \nmid m$ and $p|m$. By Lemma 1.2.8, we see that if $p|m$, then, $\Gamma_A(0) = 0$. Otherwise, $\Gamma_A(0) = 1$. But

$$A(0) - \frac{1}{p}\sum_{\zeta^p=1} A(\zeta - 1) = 1 - \frac{1}{p}\sum_{\zeta^p=1} \zeta^m,$$

and the result holds. □

Now, we can compute $L_p(1, \chi)$. For $\chi = 1$, L_p has a single pole at $s = 1$ and there is nothing to prove. So, let us suppose that $\chi \neq 1$. The key idea is to express $L_p(1; \chi)$ as the Γ-transform of a certain power series at $s = 0$ and use Lemma 1.2.11. We will consider, for simplicity, that $p > 2$.

Proposition 1.2.12. *Let χ be a primitive Dirichlet character of conductor f and N an integer coprime to pf. Denote by Λ_N the group of all N-th roots of unity. Let ξ be an f-th root of unity. Consider the following power series*

$$A(x) := \frac{\tau(\chi)}{f}\sum_{a=1}^{f}\sum_{\lambda\in\Lambda_N\setminus\{1\}} \overline{\chi(a)}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}\frac{x^n}{(1-\lambda\xi^a)^n}.$$

This series belongs to $\mathbb{Q}_p[[X]]_m$ and

$$\Gamma_A(s) = (1 - \chi(N)\langle N\rangle^s)L_p(1 - s; \chi).$$

Proof. For any $n \equiv 0 \pmod{(p-1)}$ we have

$$L_p(1-n;\chi) = -(1-\chi(p)p^{n-1})\frac{B_{n,\chi}}{n}.$$

Since the congruence class of 0 modulo $p-1$ is dense in $\mathbb{Z}_p$, for any $s \in \mathbb{Z}_p$, there exists a sequence of positive integers n_k which tends to s p-adically, such that $(p-1)|n_k$ for any $k \geq 1$. Thus,

$$\lim_{k\to\infty} B_{n_k,\chi} = -sL_p(1-s;\chi).$$

A striking idea of Leopoldt was to express the limit of the Bernoulli numbers as a Γ transform of a suitable power series in $\mathbb{Q}_p[[X]]_m$. To bring to light the Bernoulli numbers, it would be desirable to find a power series related to F_χ, the generator function of the $B_{n,\chi}$. The series in the statement of the proposition in fact satisfies

$$DA(e^T-1) = \chi(N)F_\chi(NT) - F_\chi(T),$$

which implies that for any $n \geq 1$, $\delta_n(DA) = (\chi(N)N^n - 1)B_{n,\chi}$. Now, by letting k tend to infinity, we have

$$\Gamma_{DA}(s) = \lim_{k\to\infty} \delta_{n_k}(DA) = (\chi(N)\langle N\rangle^s - 1)\lim_{k\to\infty} B_{n_k,\chi}.$$

Since $\Gamma_{DA}(s) = s\Gamma_A(s)$, the result holds for $s \neq 0$. Since both sides of the equality are continuous functions, the same holds at $s = 0$. □

Notice that $A(0) = 0$, what implies, by using Lemma 1.2.11, that

$$-\frac{1}{p}\sum_{\zeta^p=1} A(\zeta-1) = (1-\chi(N))\,L_p(1;\chi).$$

Let ξ be an f-th root of unity. A simple computation yields

$$A(\zeta-1) = \frac{\tau(\chi)}{f}\sum_{a=1}^{f}\sum_{\lambda\in\Lambda_N\setminus\{1\}} \overline{\chi}(a)\log_p\left(1+\frac{\xi-1}{1-\lambda\xi^a}\right),$$

which, due to the fact that $\overline{\chi}(a) = \chi(N)\overline{\chi}(aN)$ for a coprime to N, leads to

$$\Gamma_A(0) = \frac{-\tau(\chi)}{pf}\,(\chi(p)-p)\,(\chi(N)-1)\sum_{a=1}^{f}\overline{\chi}(a)\log_p\left(1-\xi^{-a}\right). \qquad (1.2.2)$$

To finish, by comparing (1.2.2) with Proposition 1.2.12, we can conclude that the proof of the following result is complete.

Theorem 1.2.13. *Let χ be an even Dirichlet character of conductor f, p a prime and N a natural number coprime to fp. Then,*

$$L_p(1;\chi) = \frac{-\tau(\chi)}{f}\left(1-\frac{\chi(p)}{p}\right)\sum_{a=1}^{f}\overline{\chi}(a)\log_p\left(1-\xi^{-a}\right).$$

Remark 1.2.14. The study of the Γ transform and its application to the proof that $L_p(1;\chi) = \mathcal{L}_p(\chi)$ appears first in [34]. It seems, nevertheless, that the construction dates back to an unpublished work of Leopoldt, who, in 1964, gave a series of lectures on this topic in Baltimore. In the words of Leopoldt, he postponed the publication *in the wrong hope of giving a proof of the nonvanishing of* $\mathcal{L}_p(\chi)$ (cf. [41], p. 29).

1.3 p-adic L-functions via Stickelberger

We present here an alternative construction of the p-adic L-function due to Iwasawa (see [34], ch. 6). This construction is of a more algebraic nature than the previous ones, and this feature allows us to prove some classical results on class numbers.

1.3.1 The Iwasawa algebra of a finite extension of $\mathbb{Q}_p$.

Let F be a finite extension of $\mathbb{Q}_p$ and Γ a multiplicative topological group which is isomorphic to the additive group $\mathbb{Z}_p$. Let γ be a topological generator of Γ. Denote

$$\Gamma_n = \Gamma/\Gamma^{p^n}.$$

Consider the group ring $\mathcal{O}_F[\Gamma_n]$. If $m \geq n$, we have a natural projection

$$\phi_{m,n} : \mathcal{O}_F[\Gamma_m] \to \mathcal{O}_F[\Gamma_n].$$

The map

$$\mathcal{O}_F[\Gamma_n] \quad \longrightarrow \quad \mathcal{O}_F[T]/((1+T)^{p^n}-1)$$

given by $\gamma \pmod{\Gamma_n} \mapsto 1+T \pmod{((1+T)^{p^n}-1)}$ is an isomorphism compatible with $\phi_{m,n}$.

Definition 1.3.1. (Iwasawa, [34]) The Iwasawa algebra of F is the inverse limit $\mathcal{O}_F[[\Gamma]] = \varprojlim \mathcal{O}_F[\Gamma_n]$.

We have the following

Theorem 1.3.2. $\mathcal{O}_F[[\Gamma]] \simeq \mathcal{O}_F[[T]]$.

Set $F_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and denote $F_\infty = \varinjlim F_n$. Consider $\Gamma = \mathrm{Gal}(F_\infty/F_0)$, which is isomorphic to $\mathbb{Z}_p$ and $\Delta = \mathrm{Gal}(F_0/\mathbb{Q})$, which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$. Notice that

$$\mathrm{Gal}\,(F_n/\mathbb{Q}) \simeq \Delta \times \Gamma_n.$$

Let χ be a Dirichlet character of conductor dp^j (with d coprime to p). We can write $\chi = \theta\psi$, with θ a character of Δ of conductor dp^a, $a = 0, 1$ and ψ a character of Γ_n of conductor p^k for some k. We say that θ is a character of first order and that ψ is a character of second order. For any $\sigma_a \in \mathrm{Gal}(F_n/\mathbb{Q})$ with $\sigma_a(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^a$, write $\sigma_a = \delta(a)\gamma_n(a)$ with $\delta(a) \in \Delta$ and $\gamma_n(a) \in \Gamma_n$. Notice that $\gamma_n(a) = \gamma_n(b)$ if and only if $\langle a\rangle \equiv \langle b\rangle \mod (p^{n+1})$.

Definition 1.3.3. Let $\chi = \theta\psi$ be the decomposition of an even Dirichlet character. The n-th Stickelberger element attached to χ is

$$\xi_n(\theta) = -\frac{1}{p^{n+1}} \sum_{a=0}^{p^{n+1}} \langle a\rangle \theta\gamma_n(a)^{-1} \in F_\theta[\Gamma_n].$$

Where F_θ denotes the field $\mathbb{Q}_p\,(\{\theta(n); n \in \mathbb{Z}\})$. Denote

$$\eta_n(\theta) = (1 - (1+p)\gamma_n(1+p)^{-1})\xi_n(\theta) \in \mathcal{O}_{F_\theta}[\Gamma_n].$$

Lemma 1.3.4 (cf. Washington, [74])**.** *For any non trivial character $\theta \neq 1$ of second order, we have*

(i) $\frac{1}{2}\eta_n(\theta) \in \mathcal{O}_{F_\theta}[\Gamma_n]$.

(ii) $\frac{1}{2}\xi_n(\theta) \in \mathcal{O}_{F_\theta}[\Gamma_n]$.

(iii) If $m \geq n$, then,

$$\eta_m(\theta) \mapsto \eta_n(\theta)$$

and

$$\xi_m(\theta) \mapsto \xi_n(\theta)$$

under the projection $F_\theta\,[\Gamma_m] \to F_\theta\,[\Gamma_n]$.

□

By Lemma 1.3.4, $(\xi_n(\theta))_{n\geq 1}, (\eta_n(\theta))_{n\geq 1} \in \mathcal{O}_{F_\theta}[\Gamma]$. Let $f(T,\theta), g(T,\theta) \in \mathcal{O}_{F_\theta}[[T]]$ the power series corresponding respectively to $(\xi_n(\theta))_{n\geq 1}$ and $(\eta_n(\theta))_{n\geq 1}$ by Theorem 1.3.2. Denote

$$h(T,\theta) = \frac{g(T,\theta)}{f(T,\theta)}.$$

Observe that $h(T,\theta) = 1 - \frac{1+p}{1+T}$. If θ is the trivial character, we can take $\dfrac{g(T,1)}{h(T,1)}$ as definition of $f(T,1)$.

Theorem 1.3.5. *Let $\chi = \theta\psi$ be the decomposition of a Dirichlet character. Write $\zeta_\psi = \psi(1+p)^{-1} = \chi(1+p)^{-1}$. Then*

$$L_p(s;\chi) = f(\zeta_\psi(1+p)^s - 1, \theta).$$

Proof. Notice that for any $s \in D\left(1, p^{\frac{p-2}{p-1}}\right)^+$, we have that $|(1+p)^s - 1|_p < 1$. Since ζ_ψ has p-power order, $\log_p(\zeta_\psi) = 0$. Therefore, $|\zeta_\psi(1+p)^s - 1|_p < 1$ and the right hand side is an analytic function of s. So, it suffices to check the equality for $s = 1-m$ with m an even natural number. Some calculation leads to

$$g(\zeta_\psi(1+p)^{1-m} - 1, \theta) =$$
$$\frac{-1}{m} h(\zeta_\psi(1+p)^{1-m} - 1, \theta) \lim_{n\to\infty} \frac{1}{p^{n+1}} \sum_{p\nmid j, j=1}^{p^{n+1}} \chi\omega^{-m}(j) j^m.$$

It suffices to prove the equality

$$\left(1 - \chi\omega^{-m}(p)p^{m+1}\right) B_{m,\chi_m} = \lim_{n\to\infty} \frac{1}{p^{n+1}} \sum_{p\nmid j, j=1}^{p^{n+1}} \chi\omega^{-m}(j) j^m.$$

To do so, notice that

$$B_{m,\chi_m} = \lim_{n\to\infty} \frac{1}{p^{n+1}} \sum_{j=1}^{p^{n+1}} \chi\omega^{-m}(j) j^m,$$

hence

$$(1-\chi\omega^{-m}(p)p^{m+1})\,B_{m,\chi_m} =$$
$$\lim_{n\to\infty}\frac{1}{p^{n+1}}\sum_{j=1}^{p^{n+1}}\chi\omega^{-m}(j)j^m - \lim_{n\to\infty}\frac{1}{p^{n+1}}\sum_{j=1}^{p^n}\chi\omega^{-m}(pj)(pj)^m =$$
$$\lim_{n\to\infty}\frac{1}{p^{n+1}}\sum_{p\nmid j,j=1}^{p^{n+1}}\chi\omega^{-m}(j)j^m.$$

□

1.3.2 Application to class number formulas.

Let $(d,p)=1$. Let h_n be the class number of the (dp^{n+1})-th cyclotomic extension and h_n^+ the class number of its maximal real subfield. Denote $h_n^- = \frac{h_n}{h_n^+}$. As an application of Theorem 1.3.5, one can study the numbers h_n^- for n large enough.

Remark 1.3.6. Notice that $f(0,1) = -B_{1,\omega^{-1}}$. Since $pB_{1,\omega^{-1}} \in \mathbb{Z}_p$ and $h(0,1) = -p$, it follows that $\frac{1}{2}g(T,1) \in \mathbb{Z}_p[[T]]^*$.

Denote by E_d, the group of even characters of second order whose conductor is a divisor of dp.

Proposition 1.3.7 (cf. Washington, [74], ch. 7)**.** *Let $(d,p)=1$ and $q_n = dp^{n+1}$. Assume $d \not\equiv 2 \pmod 4$. Then*

$$h_n^- = h_0^- \prod_{\theta\in E_d\setminus\{1\}}\prod_{\zeta\in\Lambda_{p^n}\setminus\{1\}}\frac{1}{2}f(\zeta-1,\theta)u_n,$$

for some $u_n \in \mathbb{Z}_p^*$.

As an application of the previous proposition, we have the following result due to Iwasawa, which describes the asymptotic behaviour of h_n^-.

Theorem 1.3.8. *Let $p^{e_n^-}$ be the exact power of p dividing h_n^-. Then, there exist $C>0$, λ,μ nonnegative integers and $\nu\in\mathbb{Z}$, such that for any $n \geq C$*

$$e_n^- = \lambda n + \mu p^n + \nu.$$

Proof. Write

$$A(T) = \prod_{\theta \in E_d \setminus \{1\}} \frac{1}{2} f(T, \theta).$$

Since the different θ run over the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_{dp})/\mathbb{Q})$ and the coefficients of $A(T)$ are symmetric polynomials, it follows that $A(T) \in \mathbb{Z}_p[[T]]$. Using Proposition 1.3.7, we have that

$$\frac{h_n^-}{h_0^-} = u^{p^n - 1} \prod_{\zeta \in \Lambda_{p^n} \setminus \{1\}} A(\zeta - 1),$$

with $u \in \mathbb{Z}_p^*$. Hence, by the p-adic Weierstrass preparation theorem, we can decompose $A(T) = p^\mu P(T) U(T)$, with $\mu \geq 0$, $P(T)$ a distinguished polynomial and $U(T) \in \mathbb{Z}_p[[T]]^*$. Hence, since the number of non-trivial roots of $X^{p^n} - 1$ in $\mathbb{Q}^{alg}$ is $p^n - 1$, we can write

$$v_p(h_n^-) = v_p(h_0^-) + (p^n - 1)\mu + \sum_{\zeta \in \Lambda_{p^n} \setminus \{1\}} v_p(P(\zeta - 1)).$$

Set $\lambda = \deg P(T)$. Since $P(T)$ is a distinguished polynomial, it has the form

$$P(T) = T^\lambda + a_{\lambda - 1} T^{\lambda - 1} + ... + a_0$$

with $p | a_i$ for $0 \leq i \leq \lambda - 1$. On the other hand, one has that

$$v_p((\zeta - 1)) = \frac{1}{\phi(p^n)}.$$

Now, if n is large enough, certainly

$$v_p((\zeta - 1)^\lambda) < 1,$$

and we will have $v_p(P(\zeta - 1)) = \frac{\lambda}{\phi(p^n)}$. Thus

$$e_n^- = \mu p^n + \lambda n + v_p(h_0^-) - \mu + C$$

with C independent of n. □

Remark 1.3.9. In fact, for any finite abelian extension $F/\mathbb{Q}$, and for any prime p, the invariant μ attached to the extension $F_\infty/\mathbb{Q}$ vanishes (see [74], [28]).

1.4 p-adic L-functions as Mazur-Mellin transforms

Let X, Y be topological spaces. Denote by $\mathrm{Loc}(X, Y)$ the set of Y-valued locally constant functions on X. Every algebraic extension F of $\mathbb{Q}_p$ is totally disconnected and linear combinations of characteristic functions of compact-open subsets of F (step functions) are locally constant. Moreover, a standard compactness argument shows that every locally constant function is a step function.

Definition 1.4.1. Let F be a finite extension of $\mathbb{Q}_p$, G an abelian group and X a compact open subset of F. A *G-valued p-adic distribution* μ on X is an additive map from the set of compact-open subsets of X to G, i.e., for any finite family $\{U_i\}_{i=1}^n$ of disjoint compact open subsets of X,

$$\mu\left(\bigcup_{i=1}^{n} U_i\right) = \sum_{i=1}^{n} \mu(U_i).$$

By an interval of X we mean a set of the form $a + \pi^n \mathcal{O}_F$, where $a \in \mathcal{O}_F$ and π is a uniformizer. Let p^f denote the number of elements of the residual field $\mathcal{O}_F/\pi\mathcal{O}_F$.

Proposition 1.4.2. *Let μ be a function on the set of intervals of X such that for any interval $a + \pi^n \mathcal{O}_F \subseteq X$,*

$$\mu(a + \pi^n \mathcal{O}_F) = \sum_{j=0}^{p^f - 1} \mu(a + j\pi^n + \pi^{n+1}\mathcal{O}_F).$$

Then, μ extends uniquely to a p-adic distribution.

Proof. Since every compact-open subset $U \subseteq X$ is a finite disjoint union of intervals, it is possible to extend μ to the compact-open subsets. To check that the extension does not depend on the choice of the intervals, notice that for any two partitions we can take a refinement of both. □

Examples 1.4.3. Let F be a Galois extension of $\mathbb{Q}_p$ of degree n. The Haar distribution on $\mathcal{O}_F$ is defined by setting

$$\mu_H(a + \pi^r \mathcal{O}_F) = p^{-\frac{r}{n}}.$$

Examples 1.4.4. Let $F = \mathbb{Q}_p$. For a non-negative integer k, and a Dirichlet character χ, the k-th Bernoulli distribution attached to χ is defined by setting

$$\mu_{B,k,\chi}(a + p^n\mathbb{Z}_p) = p^{n(k-1)}B_{k,\chi}\left(\frac{a}{p^n}\right), \quad 0 \leq a \leq p^n - 1.$$

For $\chi = 1$, we will write simply $\mu_{B,k}$.

Definition 1.4.5. A p-adic measure is a p-adic distribution which is uniformly bounded on the compact-open intervals.

The point of this definition is that, in general, p-adic distributions do not allow Riemann integration of continuous functions against them, the obstruction being the unboundedness. Let $f : X \to F$ be a continuous function and μ a F-valued p-adic distribution on X.

Definition 1.4.6. For any partition $X = \bigcup_{i=1}^{n} I_n$, with $\mathcal{P} = \{I_i\}_{i=1}^n$ a family of compact-open disjoint intervals contained in X, and for any choice of points $\mathcal{J} = \{x_i\}_{i=1}^n$ with $x_i \in I_i$, the associated Riemann sum is

$$S(f, \mathcal{P}, \mathcal{J}) = \sum_{i=1}^{n} f(x_i)\mu(I_i).$$

A continuous function is Riemann integrable if $\lim S(f, \mathcal{P}, \mathcal{J})$ exists when $\mathcal{P}$ runs over the set of partitions and $\mathcal{J}$ runs over the set of choices of intermediate points. This limit is denoted by $\int_C f d\mu$. Notice that locally constant functions are Riemann integrable.

Examples 1.4.7. Let $F = \mathbb{Q}_p$, $X = \mathbb{Z}_p$, f the identity and μ the Haar distribution on X. Take a partition by intervals $I_i = i + p^n\mathbb{Z}_p$ with $0 \leq i \leq p^n - 1$. As intermediate point in I_i take i. The Riemann sum equals $\frac{p^n-1}{2}$, which tends to $-\frac{1}{2}$. But, for any fixed integer k, if we choose as intermediate point $i + kp^n$, the Riemann sum is $\frac{p^n-1}{2} - k$, which tends to $-k - \frac{1}{2}$.

As pointed out above, p-adic measures do not have this problem:

Proposition 1.4.8. *Let μ be a p-adic measure on a compact subset $C \subseteq F$. Any continuous function $f : C \to F$ is Riemann integrable.*

Proof. Since X is compact, f is uniformly continuous. Since μ is bounded, say, by M, for two partitions $\mathcal{P}$ and $\mathcal{Q}$ and for any two choices of intermediate points $\mathcal{J}_{\mathcal{P}} = \{x_i\}$ and $\mathcal{J}_{\mathcal{Q}} = \{y_j\}$, by ultrametricity, we have

$$\left|S(f,\mathcal{P},\mathcal{J}_{\mathcal{P}}) - S(f,\mathcal{Q},\mathcal{J}_{\mathcal{Q}})\right|_p \leq \sup_{x_i,y_j} \left|f(x_i) - f(y_j)\right|_p M.$$

□

The following generalization of a well known result in real analysis is a direct corollary of Proposition 1.4.8.

Corollary 1.4.9. *If $\left|f(x)\right|_p \leq A$ for any $x \in X$, and $\left|\mu\left(U\right)\right|_p \leq B$ for any compact open subset $U \subseteq X$, then*

$$\left|\int_X f d\mu\right|_p \leq AB.$$

Given the Bernoulli distributions $\mu_{B,k,\chi}$, the following process gives rise to a p-adic measure: Consider $\alpha \in \mathbb{Z}^*$, $\alpha \not\equiv 1 \bmod (p)$. Let $U \subset \mathbb{Z}_p^*$ a compact open subset. Define

$$\mu_{k,\chi,\alpha}\left(U\right) = \mu_{B,k,\chi}\left(U\right) - \alpha^{-k}\mu_{B,k,\chi}\left(\alpha U\right).$$

For $\chi = 1$, we will simply write $\mu_{k,\alpha}$. One easily sees that for any $n \geq 1$ and for any $0 \leq a \leq p^n - 1$

$$\left|\mu_{1,\chi,\alpha}\left(a + p^n\mathbb{Z}_p\right)\right|_p \leq 1.$$

For $k > 1$, one has the following result:

Proposition 1.4.10 (cf. Koblitz, [39], ch. 2)**.** *Let d_k be the least common denominator of the coefficients of k-th Bernoulli polynomial. Then*

$$d_k\mu_{k,\alpha}(a + p^n\mathbb{Z}_p) \equiv d_k k a^{k-1}\mu_{1,\alpha}(a + p^n\mathbb{Z}_p) \pmod{p^n}.$$

Corollary 1.4.11. *For any $k \geq 1$, and for any $\alpha \in \mathbb{Z}_p^* \setminus D\left(1, p^{-1}\right)$, $\mu_{k,\alpha}$ is a p-adic measure.*

Proof. For any $a \in \mathbb{Z}_p$, and $n \geq 1$, by Proposition 1.4.10, we have

$$|\mu_{k,\alpha}(a + p^n\mathbb{Z}_p)|_p \leq \max\left\{\left|d_k k a^{k-1}\mu_{1,\alpha}(a + p^n\mathbb{Z}_p)\right|_p, p^{-n}\right\},$$

hence, $\max\{|d_k|_p, 1\}$ is a uniform bound for $\mu_{k,\alpha}$. □

The measure $\mu_{k,\alpha}$ is called the α-regularization of the distribution μ_k.

Remark 1.4.12. Proposition 1.4.10 can be thought of as a p-adic analogue of the fact that $d(x^k) = kx^{k-1}dx$. Indeed, it is not difficult to check that for any compact-open subset $X \subset \mathbb{Z}_p$, and $k \geq 1$,

$$\int_X d\mu_{k,\alpha} = k\int_X x^{k-1}d\mu_{1,\alpha}.$$

One can use p-adic measures to give a proof of the following classical result.

Corollary 1.4.13 (Kummer, Clausen-von Staudt)**.** *The following congruences hold:*

(i) If $k \not\equiv 0 \pmod{(p-1)}$*, then* $\left|\frac{B_k}{k}\right|_p \leq 1$.

(ii) If $k_1, k_2 \not\equiv 0 \pmod{(p-1)}$ *and if* $k_1 \equiv k_2 \pmod{(p-1)p^n}$*, then*

$$(1 - p^{k_1-1})\frac{B_{k_1}}{k_1} \equiv (1 - p^{k_2-1})\frac{B_{k_2}}{k_2} \pmod{p^{n+1}}.$$

(iii) If $(p-1)|k$*, then*

$$pB_k \equiv -1 \pmod{p}.$$

Proof. We assume $p > 2$. To prove the first result, notice that

$$\frac{B_k}{k} = \frac{-1}{(1 - \alpha^{-k})(1 - p^{k-1})}\int_{\mathbb{Z}_p^*} x^{k-1}d\mu_{1,\alpha}.$$

Taking norms on both sides, and using Proposition 1.4.9, the result holds. For the second result, notice that the congruence we have to prove can be written in the form

$$\frac{1}{\alpha^{-k_1} - 1}\int_{\mathbb{Z}_p^*} x^{k_1-1}d\mu_{1,\alpha} \equiv \frac{1}{\alpha^{-k_2} - 1}\int_{\mathbb{Z}_p^*} x^{k_2-1}d\mu_{1,\alpha} \pmod{p^{n+1}}.$$

But, to prove this, due to Proposition 1.4.9, it suffices to see that if $k_1 \equiv k_2 \pmod{(p-1)p^n}$, then, for any $x \in \mathbb{Z}_p^*$, $x^{k_1} \equiv x^{k_2} \pmod{p^n}$. For the Clausen-von Staudt congruence, take $\alpha = 1 + p$ and write

$$pB_k = -kp\left(-\frac{B_k}{k}\right) = \frac{-kp}{\alpha^{-k}-1}(1-p^{k-1})^{-1}\int_{\mathbb{Z}_p^*} x^{k-1}d\mu_{1,\alpha}.$$

Since $\alpha^{-k} - 1 \equiv -kp \pmod{p^{v_p(k)+2}}$, it amounts to check that

$$\int_{\mathbb{Z}_p^*} x^{k-1}d\mu_{1,\alpha} \equiv -1 \pmod{p}.$$

For this, observe that

$$\int_{\mathbb{Z}_p^*} x^{k-1}d\mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^*} x^{-1}d\mu_{1,\alpha} \pmod{p}.$$

Denote by $D(x)$ the first p-adic digit of x, which is a locally constant function. One has

$$\int_{\mathbb{Z}_p^*} x^{-1}d\mu_{1,\alpha} \equiv \int_{\mathbb{Z}_p^*} D(x)^{-1}d\mu_{1,\alpha} = \sum_{j=1}^{p-1}\frac{1}{j}\mu_{1,\alpha}\left(j+p\mathbb{Z}_p\right) \pmod{p}.$$

But

$$\mu_{1,\alpha}(k+p\mathbb{Z}_p) = \frac{2k-p}{2(1+p)} \equiv k \pmod{p}.$$

Thus the left sum is congruent to $-1 \pmod{p}$. □

There are a number of generalizations of these congruences. For instance, we have the following result.

Proposition 1.4.14. *If $k_1, k_2 \not\equiv 0 \pmod{(p-1)}$ and if $k_1 \equiv k_2 \pmod{(p-1)p^n}$, then*

$$\left(1-\chi(p)p^{k_1-1}\right)\frac{B_{k_1,\chi_{k_1}}}{k_1} \equiv (1-\chi(p)p^{k_2-1})\frac{B_{k_2,\chi_{k_2}}}{k_2} \pmod{p^{n+1}}.$$

For generalizations of (i) and (iii) we refer the reader to [37]. These congruences are the main tool for an alternative construction of p-adic L-functions.

Proposition 1.4.15 (Lang, [42]). *Let χ be a primitive Dirichlet character. Then, for any $\alpha \in \mathbb{Z}_p^* \setminus D(1,p)$ and for any integer $k \geq 1$, we have that*

$$\frac{-1}{1-\chi(\alpha)\langle\alpha\rangle^k}\int_{\mathbb{Z}_p^*}\chi(x)\langle x\rangle^k x^{-1}d\mu_{1,\alpha} = -(1-\chi_k(p)p^{k-1})\frac{B_{k,\chi_k}}{k}.$$

□

Notice that χ can be extended to $\mathbb{Z}_p$, since it is locally constant. The congruence given in Proposition 1.4.14 ensures that the left hand side of 1.4.15 defines a continuous function with respect to the p-adic topology. Hence, there is a unique extension to $\mathbb{Z}_p$. In fact, the extension is holomorphic if $\chi \neq 1$ (otherwise, the extension will have a simple pole at $s = 0$ when $\chi = 1$ (cf. [42], [39] for details). According to 1.4.15 and to the fact that the Kubota-Leopoldt p-adic L-function is unique, the following result holds.

Proposition 1.4.16 (Lang, [42]). *For any $s \in \mathbb{Z}_p$, one has*

$$L_p(1-s;\chi) = \frac{-1}{1-\chi(\alpha)\langle\alpha\rangle^s}\int_{\mathbb{Z}_p^*}\chi(x)\langle x\rangle^s x^{-1}d\mu_{1,\alpha}.$$

□

Remark 1.4.17. This definition of p-adic distribution is consistent with the classical definition of Borel measurability in measure theory, although this is not pointed out in the literature. Recall that the Borel σ-algebra over a topological space X is the family of $\mathcal{P}(X)$ whose sets are built up by taking unions, intersections and complements of open (equivalently closed) subsets of X. Due to the ultrametric property, any two discs either are disjoint or one is contained in the other. Thus, the Borel sets in $\mathbb{Z}_p$ are precisely the unions of open subsets. On the other hand, $\mathbb{Z}_p$ is Hausdorff and compact, thus, any arbitrary union of discs is in fact a finite union. Hence, the Borel σ-algebra over $\mathbb{Z}_p$ is precisely the family of open subsets.

Another fact to take into account is that in measure theory, a measure is defined to be σ-additive. Again, the union of any family of open subsets is just the union of a finite subfamily. Thus there are no countable infinite sequences of disjoint open sets.

One could ask why integration of continuous functions again p-adic distributions does not work if everything agrees with classical measure theory. The point is that Borel measurability requires the measure to take values in $\mathbb{R}$ and this is not the case in our setting. The p-adic distributions behave like classical measures, apart from the fact that they are $\mathbb{C}_p$-valued.

Chapter 2

p-adic L-functions of relative real abelian extensions

Introduction

Let K be a totally real number field and $\mathfrak{f}$ an integral ideal of K. Denote $K_{\mathfrak{f},1} := \{\alpha \in K |\ \alpha \text{ totally positive}, \alpha \equiv 1 \pmod{\mathfrak{f}}\}$. The congruence means that for any prime ideal $\mathfrak{p}$ dividing $\mathfrak{f}$, $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{f})$. Denote by $I_{\mathfrak{f}}$ the group of fractional ideals of K which are coprime to $\mathfrak{f}$ and by $P_{\mathfrak{f}}$ the subgroup of $I_{\mathfrak{f}}$ whose elements are principal fractional ideals generated by elements of $K_{\mathfrak{f},1}$. The group $I_{\mathfrak{f}}/P_{\mathfrak{f}}$ is finite and is called the *ray class group* of K modulo $\mathfrak{f}$. Let us denote this group by $\mathcal{C}_{\mathfrak{f}}$. The Artin reciprocity map induces an isomorphism between $\mathcal{C}_{\mathfrak{f}}$ and $\mathrm{Gal}(K^{\mathfrak{f}}/K)$, where $K^{\mathfrak{f}}$ is the *ray class field* of K modulo $\mathfrak{f}$.

Let M be a real abelian extension of K of conductor $\mathfrak{f}$. Since $K \subset M \subset K^{\mathfrak{f}}$, the Artin reciprocity map induces a surjection $\phi : \mathcal{C}_{\mathfrak{f}} \to \mathrm{Gal}(M/K)$. Let $\mathcal{X}$ denote the group of characters of $\mathrm{Gal}(M/K)$. The L function of M/K is defined over $\mathcal{X}$ as

$$L(\chi; s) = \sum \chi(\phi(\mathfrak{a}))N\mathfrak{a}^{-s},\ \chi \in \mathcal{X},\ \mathrm{Re}(s) > 1,$$

with $\mathfrak{a}$ running over the integral ideals of $\mathcal{O}_K$ which are coprime to $\mathfrak{f}$. In this chapter, we present the construction of a holomorphic p-adic function $L_p(\chi; s)$ carried out in [22]. This p-adic L-function interpolates the values of $L(\chi; s)$ at the negative integers where $\chi \in \mathcal{X}$, and satisfies congruences analogous to those by Kummer and Clausen von Staudt.

2.1 Partial zeta-functions and Shintani decomposition

Let M/K be a real abelian extension of conductor $\mathfrak{f}$ with K a totally real field of degree n. Let N denote the norm of $K/\mathbb{Q}$. For any $\sigma \in \mathrm{Gal}(M/K)$, define $I_\sigma = \{\mathfrak{a} \in \mathcal{C}_\mathfrak{f} |\, \phi(\mathfrak{a}) = \sigma\}$ and denote

$$\zeta_M(\sigma, s) = \sum_{\mathfrak{a} \in I_\sigma} N\mathfrak{a}^{-s},\ \mathrm{Re}(s) > 1.$$

It is not difficult to prove that, for any $\chi \in \mathcal{X}$,

$$L(\chi, s) = \sum_{\sigma \in \mathrm{Gal}_{(M/K)}} \chi(\sigma)\zeta_M(\sigma, s).$$

The values $\zeta_M(\sigma, 1-k)$ are rational for non-negative integers $k \geq 2$ (see [68]). Given an integral ideal $\mathfrak{a}$ of K coprime to $\mathfrak{f}$, set

$$\zeta(\mathfrak{a}^{-1}, s) = \sum N(\mathfrak{g})^{-s},$$

where $\mathfrak{g}$ runs over the integral ideals belonging to the ideal class of $\mathfrak{a}$ in $\mathcal{C}_\mathfrak{f}$.

Let p be a prime number. Throughout this chapter, we assume that $\mathfrak{f}$ is divisible by all the prime ideals of $\mathcal{O}_K$ above p. Let $r \geq 0$ be an integer and $\nu = (\nu_1, ..., \nu_r)$ an r-tuple of totally positive elements of K and $x \in K$ totally positive too. Consider the affine linear form

$$L_{x,\nu}(y_1, ..., y_r) = x + \sum_{k=1}^{r} y_k \nu_k.$$

Definition 2.1.1. Given an r-tuple of roots of unity $\xi = (\xi_1, ..., \xi_r)$, the partial zeta function for $L_{x,\nu}$ and ξ is

$$\zeta(L_{x,\nu}, \xi, s) = \sum_{m \in \mathbb{N}^r} N(L_{x,\nu}(m))^{-s} \xi^m,\ \mathrm{Re}(s) > \frac{r}{n},$$

where $\xi^m = \prod_{i=1}^r \xi_i^{m_i}$, $m = (m_1, ..., m_r)$.

Theorem 2.1.2 (Shintani, [67])**.** *There exist*

(i) a finite set J of indices,

(ii) a finite collection of totally positive elements $\{x_k\}_{k=1}^m$ *congruent to* 1 (mod $\mathfrak{f}$) *and*

(iii) for any $j \in J$*, a finite number* r_j *of totally positive elements* $\{\nu_{j,i}\}_{i=1}^{r_j}$ *with* $\nu_{j,i} \in \mathfrak{a}\mathfrak{f}$

such that

$$\zeta(\mathfrak{a}^{-1}, s) = N\mathfrak{a}^s \sum_{(j,k)\in J\times\{1,...,m\}} \zeta(L_{x_k,\nu_j}, 1, s),$$

where 1 *means* $(1, ..., 1) \in K^r$.

□

To be in a position to construct p-adic L-functions in this setting, a natural question is to find analogues of the Bernoulli numbers. Shintani's decompositions give rise to them.

Let $\nu = (\nu_1, ..., \nu_r) \in K^r$ and $t = (t_1, ..., t_n) \in K^n$. For any $j \in \{1, ..., r\}$, denote $T_j^\nu(t) = \sum_{k=1}^n \nu_j^{(k)} t_k$ where the upper scripts mean conjugation by the elements of $\mathrm{Gal}(K/\mathbb{Q})$. Let $\xi = (\xi_j)_{j=1}^r$ be an r-tuple of roots of unity, $u \in \mathbb{R}$ and $x = (x_1, ..., x_r) \in [0, 1]^r$. The function

$$P_{\nu,u,\xi,x}(t) = \prod_{j=1}^r \frac{\exp(u(1 - x_j)T_j^\nu(t))}{\exp(uT_j^\nu(t)) - \xi_j}$$

plays the role of the generating function of Bernoulli numbers attached to the data ν, ξ, u, x.

Definition 2.1.3. (Shintani, [67]) Denote by $\tilde{B}_{k+1}(L, \xi)^{(i)}$ the coefficient of $u^{kn}(t_1...t_{i-1}t_{i+1}...t_n)^k$ in the expansion of $P_{\nu,u,\xi,x}|_{t_i=1}$ around the origin. The k-th Bernoulli number for L and ξ is $B_{k+1}(L, \xi)^{(i)} = (k + 1)!\tilde{B}_{k+1}(L, \xi)^{(i)}$.

Attached to the data ν, u, ξ, x, we have the following

Definition 2.1.4. (Shintani, [67]).

$$\zeta(L, \xi, s) = \sum_{m\in\mathbb{N}^r} \frac{\xi^m}{N(L(m))^s}, \quad \mathrm{Re}(s) > \frac{r}{n}.$$

Theorem 2.1.5 (Shintani, [67]). *The function $\zeta(L,\xi,s)$ extends to a meromorphic function on $\mathbb{C}$ and satisfies:*

$$\zeta(L,\xi,-k)=(-1)^{nk}(k+1)^{-n}\sum_{i=1}^{n}\frac{B_{k+1}(L,\xi)^{(i)}}{n},\quad k\geq 0.$$

As a corollary, for any integral ideal $\mathfrak{a}$ of K coprime to $\mathfrak{f}$, the function $\zeta(\mathfrak{a}^{-1},s)$ extends to a meromorphic function on $\mathbb{C}$.

2.2 Interpolation of the partial zeta functions

Although it does not seem easy to interpolate $\zeta(L,1,-k)$, interpolation of its twists by roots of unity, i.e., interpolation of $\zeta(L,\xi,-k)$ is possible, as we see in the following result.

Theorem 2.2.1 (Cassou-Nogués, [22]). *For $y=(y_1,...,y_r)\in K^r$, set $L(y)=\sum_{i=1}^{r}(y_i+x_i)\nu_i$, with $\nu_i\in\mathfrak{f}$, $\sum_{i=1}^{r}x_i\nu_i\equiv 1 \pmod{\mathfrak{f}}$ and $c\in\mathbb{Z}$ coprime to p. Let $\xi=\{\xi_i\}_{i=1}^{r}$ be a collection of c-th roots of unity not all of them equal to 1. Then, there exists a unique function $\zeta_p(L,\xi,s)$ for $s\in\mathbb{Z}_p$, such that*

a) $\zeta_p(L,\xi,s)$ is analytic in $D(1,\rho)$ for some $\rho>1$.

b) $\zeta_p(L,\xi;k)=\zeta(L,\xi,-k)$.

Proof. (Sketch) Denote

$$\left\{ \begin{array}{c} k \\ l \end{array} \right\}=\begin{cases}(-1)^{l-1}\binom{k-1}{l-1}, & \text{if } k,l\geq 1,\\ 1, & \text{if } k=0,\\ 0, & \text{if } l=0,k\geq 1,\end{cases}$$

and setting $k=(k_1,...,k_r)$, define, for $s\in\mathbb{Z}_p$,

$$\lambda_k(s)=\sum_{l_1=0}^{k_1}...\sum_{l_r=0}^{k_r}\left\{ \begin{array}{c} k_1 \\ l_1 \end{array} \right\}...\left\{ \begin{array}{c} k_r \\ l_r \end{array} \right\}N(L_{j,x}(-l))^s,$$

where $x=(x_1,...,x_r)$ and $l=(l_1,...l_r)$. Let $\mathfrak{p}$ be a prime ideal over p and π a uniformizer of $\mathcal{O}_{M,p}$. It can be proved that if $k\neq(0,...,0)$, then

$$|\lambda_k(s)|\leq|\pi|_{\mathfrak{p}}^{k_1+...+k_r-r},$$

where r_1 is the number of non-zero $k_i's$. Define

$$\zeta_p(L,\xi,-s)=\sum_{k=(k_1,...,k_r)}\frac{\lambda_k(s)}{(1-\xi_1)^{k_1}...(1-\xi_r)^{k_r}},$$

where the k_i's runs over the non-negative integers. By taking $k_i >> 1$, it is easy to see that the terms in the sum go to zero, hence, $\zeta_p(L,\xi,-s)$ is a power series converging at a certain disc $D(1,\rho)$; thus, it is holomorphic. □

2.2.1 The p-adic L-function

Let us consider c a non-negative integer, $\mathfrak{d}$ the different ideal of K over $\mathbb{Q}$, and $\mathfrak{c}$ and $\mathfrak{f}$ integral ideals of $\mathcal{O}_K$ satisfying

- $(\mathfrak{f},\mathfrak{c})=1$ and $(\mathfrak{c},\mathfrak{d})=1$,
- $(c,\nu_{i,j})=1$ for any $j\in J$ and $i\in\{1,...,r_j\}$ (J and $\nu_{i,j}$ are those which appear in Theorem 2.1.2).
- $\mathcal{O}_K/\mathfrak{c}\simeq\mathbb{Z}/c\mathbb{Z}$.

These conditions will be referred to as *CN conditions*.

Define $\zeta(\mathfrak{a}^{-1},\mathfrak{c},s)=N(\mathfrak{c})^{1-s}\zeta(\mathfrak{a}^{-1}\mathfrak{c}^{-1},s)-\zeta(\mathfrak{a}^{-1},s)$. Let $\epsilon:\mathcal{C}_\mathfrak{f}\to\left(\mathbb{Q}_p^{alg}\right)^*$ be a ray class character. Define

$$L(\epsilon^{-1},\mathfrak{c},s)=\sum_{[\mathfrak{a}]\in\mathcal{C}_\mathfrak{f}}\epsilon([\mathfrak{a}])\zeta(\mathfrak{a}^{-1},\mathfrak{c},s).$$

Denote by ω the Teichmüller character: $\omega(z)=\lim_{n\to\infty}z^{p^n}$ for $z\in\mathbb{Z}_p^*$. The map $\theta([\mathfrak{a}]):=\omega(N(\mathfrak{a}))$ is a ray class character. From Theorem 2.1.2, one can show that if $\mathfrak{c}$ satisfies the *CN conditions*, then

$$\zeta(\mathfrak{a}^{-1},\mathfrak{c},s)=N(\mathfrak{a})^s\sum_{\mu=1}^{c-1}\sum_{L_{j,x}}\xi_x^\mu\zeta(L_{j,x},\xi^\mu,s).$$

Define now:

$$\zeta_\mathfrak{p}(\mathfrak{a}^{-1},\mathfrak{c},s)=\left(\frac{N(\mathfrak{a})}{\theta([\mathfrak{a}])}\right)^s\sum_{\mu=1}^{c-1}\sum_{L_{j,x}}\xi_x^\mu\zeta_p(L_{j,x},\xi^\mu,s).$$

For a positive integer m, denote by μ_m the group of m-th roots of unity. Define

$$\omega_m(M) = \max\{m | \operatorname{Gal}(M(\mu_m)/M) \text{ has an exponent dividing } n\}.$$

The p-adic partial zeta function $\zeta_{\mathfrak{p}}(\mathfrak{a}^{-1}, \mathfrak{c}, s)$ satisfies the following congruences.

Theorem 2.2.2 (Cassou-Nogués, [22]). *Let n be the degree of $K/\mathbb{Q}$ and suppose that $\mathfrak{c}$ satisfies the CN conditions. Then, for any $m \geq 0$,*

$$\frac{\zeta_{\mathfrak{p}}(\mathfrak{a}^{-1}, \mathfrak{c}, -m)}{N(\mathfrak{c})^{m+1}} \equiv \frac{\zeta(\mathfrak{a}^{-1}, \mathfrak{c}, 0)}{N(\mathfrak{c})^{m+1} N(\mathfrak{a}^m)} \pmod{\omega(M_{\mathfrak{f}})\mathbb{Z}_p}.$$

Theorem 2.2.3 (Cassou-Nogués, [22]). *For any real abelian extension M/K, for any $m \geq 0$ and for any $\sigma \in Gal(M/K)$, $\omega_m(M)\zeta_M(\sigma, -m)$ is an integer.*

Definition 2.2.4. (Cassou-Nogués, [22]). Let $\mathfrak{g}$ denote $\operatorname{lcm}(\mathfrak{f}, p\mathcal{O}_K)$. Given $\chi \in \operatorname{Gal}(M/K)$, the p-adic L-function of χ is

$$\zeta_p(\chi; s) = \frac{1}{(\chi(\mathfrak{c}) \left(\frac{N(\mathfrak{c})}{\theta(\mathfrak{c})}\right)^{1-s} - 1)} \sum_{\mathfrak{a}} \chi\theta^{-1}(\mathfrak{a}^{-1}) \zeta_{\mathfrak{p}}(\mathfrak{a}^{-1}, \mathfrak{c}, s).$$

This p-adic L-function satisfies the following interpolation property:

$$\zeta_p(\chi, 1-m) = L(\chi\theta^{-m}, 1-m),$$

for any integer $m \geq 1$.

Chapter 3

p-adic L-functions of modular forms

Introduction

In the previous chapters we have discussed the motivations which led to the definitions of p-adic L-functions for finite real abelian extensions of totally real number fields and we have explained their equivalence through the interpolation property. In the 1980s, there appeared definitions of p-adic L-functions for elliptic curves and modular forms. These p-adic L-functions can be intuitively seen as coherent (in a certain way) collections of integrals of differential forms of the modular curve against certain homology classes; thus, they encode partial geometric information which can be transferred into at least conjectural arithmetical information about the modular curves and the modular elliptic curves. A recurrent topic in this theory is the study of non-vanishing questions of special values of the classical complex L-functions and the relation with the non-vanishing of the corresponding p-adic analogues. A more difficult question is the non-vanishing mod p of these values.

In this chapter we explain two constructions of p-adic L-functions for modular elliptic curves, namely, those which appear in Mazur-Tate-Teitelbaum [49] and in Mazur and Swinnerton-Dyer [47]. We show that both definitions coincide in the elliptic curve setting; this fact is essentially motivated by the interpolation property of special values. We explore some questions on the non-vanishing of this p-adic L-function.

In Theorem 3.1.12, we give a proof of the fact that the p-adic L-function

of a newform of arbitrary even weight which is ordinary at the prime p is not identically zero on the set of infinite order p-adic characters. Our proof uses the results on the nonvanishing of the classical complex L-function twisted by Dirichlet characters by Rohrlich [62] together with a theorem by Kaplansky on approximation of p-adic continuous functions by polynomials applied to characteristic functions. We discuss the situation of the supersingular case, which is much more difficult, and prove in Theorem 3.1.16 that if the p-adic L-function is not identically zero at the set of infinite order p-adic characters, then, in fact, the p-adic L-function has finite order of vanishing at any p-adic integer, in particular at the critical values. This fact is non-trivial, since the p-adic topology is totally disconnected and in the supersingular case, the p-adic L-function is locally analytic, but non-analytic, since it is not an Iwasawa function; for such a function, there could perfectly well exist a point at which all the derivatives vanished, but still being non-zero at some neighbourhood of the point. To prove this result, we need to study some properties (Propositions 3.1.18 and 3.1.20) of a kind of continuous operators on the p-adic Banach space $c_0(\mathbb{C}_p)$, which we have called upper triangular operators. These results have been published in the paper [17].

3.1 Mazur-Tate-Teitelbaum p-adic L-functions

Let $\mathrm{GL}(2,\mathbb{R})^+$ denote the multiplicative group of real matrices with positive determinant and let $\mathcal{H}$ be the complex upper half-plane. Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{R})^+$ and a function $f : \mathcal{H} \to \mathbb{C}$, define $\rho(\gamma, z) := \dfrac{\det(\gamma)^{1/2}}{cz+d}$ and for any non-negative integer k, set

$$f|_k\gamma(z) = \rho(\gamma, z)^k f(\gamma(z)).$$

With this notation, we have that $f \in S_k(\Gamma_0(N))$ if and only if $f|_k\gamma = f$ for any $\gamma \in \Gamma_0(N)$, and f vanishes at the cusps.

To any eigenform $f \in S_k(\Gamma_0(N))$ of the Hecke operator T_p, and to a suitable root of the Hecke polynomial of f at p (this will be defined later) Mazur, Tate and Teitelbaum attached a p-adic L-function $L_p(f, \alpha; \chi)$ whose domain is $\mathcal{X} = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p^*, \mathbb{C}_p)$, the group of p-adic continuous characters (see [49]). From a theorem of Rohrlich ([62, Theorem 1]), it follows that if f is a normalized newform, $L_p(f, \alpha; \chi)$ does not vanish identically over $\mathcal{X}$, a conjecture stated for $k = 2$ by Mazur and Swinnerton-Dyer ([47, Conjecture

1]). A natural question is whether $L_p(f,\alpha;\chi)$ does not vanish identically over given subgroups of characters of infinite order. In the ordinary case, the identification of $\mathcal{X}$ with $p-1$ copies of the p-adic unit disc allows to conclude that $L_p(f,\alpha;\chi)$ has a finite number of zeros. This is a consequence of the p-adic Weierstrass preparation theorem. In the supersingular case, in contrast, there exist infinitely many zeros. In [56] it is shown that if the p-th Fourier coefficient of f vanishes, $L_p(f,\alpha)$ has infinitely many zeros but all of these have finite order. We give a proof of this fact removing the condition of the vanishing of the Fourier coefficient.

3.1.1 Modular integrals

We fix p a prime number and embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. We consider the p-adic norm $|\ |_p$ on $\mathbb{C}_p$ normalized so that $|p|_p = p^{-1}$. Let $S_k(\Gamma_0(N))$ be the $\mathbb{C}$-vector space of cusp forms of positive even weight k for $\Gamma_0(N)$. Let $\mathbb{T}$ be the $\mathbb{Z}$-algebra spanned by the Hecke operators $\{T_n\}_{n\geq 1}$ acting on it. Set $q = e^{2\pi i z}$. We will suppose that $f = \sum_{n\geq 1} a_n(f) q^n$ is a normalized newform and $p \nmid N$. In this case, the number field $K_f = \mathbb{Q}(\{a_n(f)\})$ is totally real. Its ring of integers will be denoted by $\mathcal{O}_f$.

For the complex L-function $L(f,s)$, the following identity holds:

$$\Lambda(f,s) := N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(f,s) = N^{\frac{s}{2}}\int_0^\infty f(it)t^{s-1}dt, \tag{3.1.1}$$

for $s \in \mathbb{C}, \mathrm{Re}(s) > \frac{k}{2}+1$. The right hand side of the equality defines an entire function which satisfies the following functional equation:

$$\Lambda(f,s) = \pm\Lambda(f,k-s), \quad s \in \mathbb{C}. \tag{3.1.2}$$

If χ is a primitive Dirichlet character of conductor n, $(n,N)=1$, and $\tau(\chi)$ its attached Gauss sum, the complex L-function of f twisted by χ is defined by

$$L(f,\chi,s) = \sum_{n=1}^{\infty} \frac{\chi(n)a_n(f)}{n^s}, \quad \mathrm{Re}(s) > \frac{k}{2}+1.$$

Let $\Lambda(f,\chi,s) = N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(f,\chi,s)$. By using orthogonality properties of the Dirichlet characters, we have that

$$\Lambda(f,\chi,s) = N^{\frac{s}{2}}\frac{\tau(\chi)}{n}\sum_{a=0}^{n-1}\overline{\chi(a)}\int_0^\infty f\left(\frac{a}{n}+it\right)t^{s-1}dt, \quad \mathrm{Re}(s) > \frac{k}{2}+1. \tag{3.1.3}$$

The function $\Lambda(f,\chi,s)$ extends to an entire function and satisfies a functional equation similar to (3.1.2).

For $r \in \mathbb{Q}$, let us denote by $\mathrm{den}(r)$ the denominator of r, written in its reduced form. The quantities

$$\lambda(f,r,j) = 2\pi \mathrm{den}\,(r)^{j+1-\frac{k}{2}} \int_0^\infty f(r+it)t^j dt, \quad r \in \mathbb{Q}, \;\; 0 \leq j \leq k-2,$$

are known in the literature as modular integrals. They satisfy the following

Theorem 3.1.1 ([49]). *There exists a $\mathbb{Z}$-lattice $\Sigma_f \subset \mathbb{C}$ of finite rank such that $\lambda(f,r,j) \in \Sigma_f$.*

It is an interesting question to study when the twisted L-function of a modular form vanishes. The following theorem is a result in this direction.

Theorem 3.1.2 (Rohrlich [62]). *Let $f \in S_k(\Gamma_0(N))$ be a normalized newform. Let P be a finite set of primes and X_P the set of primitive Dirichlet characters unramified outside $P \cup \{\infty\}$. Then, for all but finitely many $\chi \in X_P$, $L\left(f,\chi,\frac{k}{2}\right) \neq 0$.*

Since the Dirichlet characters of conductor p^m, $m \geq 1$, are those which are unramified outside p, we have the following

Corollary 3.1.3. *For $m \in \mathbb{N}$ large enough and $p \nmid N$, there exist integers a_m, $p \nmid a_m$, such that*

$$\lambda\left(f, \frac{a_m}{p^m}, \frac{k}{2}-1\right) \neq 0.$$

3.1.2 The p-adic measure attached to a newform

Let $f \in S_k(\Gamma_0(N))$ be an eigenform for T_p, $p \nmid N$, with eigenvalue $a_p(f)$. If $(p,N)=1$, the Hecke polynomial attached to f at p is $X^2 - a_p(f)X + p^{k-1}$. If $p \| N$, the Hecke polynomial is $X - a_p(f)$. For a non-zero root α of the Hecke polynomial and for $0 \leq j \leq k-2$, the following $\mathcal{O}_f[\frac{1}{\alpha}] \otimes \Sigma_f$-valued p-adic distribution is defined (a is an integer coprime to p such that $1 \leq a \leq p^n - 1$):

(i) If $(p,N)=1$, define

$$\mu_{\alpha,j}(D(a,p^n)) = \frac{1}{\alpha^n}\left(\lambda\left(f,\frac{a}{p^n},j\right) - \frac{1}{\alpha}p^{k-2}\lambda\left(f,\frac{a}{p^{n-1}},j\right)\right). \quad (3.1.4)$$

(ii) If $p \| N$, define

$$\mu_{\alpha,j}(D(a,p^n)) = \frac{1}{a_p(f)^n}\lambda\left(f, \frac{a}{p^n}, j\right). \tag{3.1.5}$$

If $|a_p(f)|_p = 1$, it is said that f is ordinary at p. Otherwise, f is said to be supersingular at p. A root α is admissible (cf. [49]) if $p^{1-k} < |\alpha|_p \leq 1$. In the ordinary case, there is only one admissible root, α; it is a p-adic unit and $\mu_{\alpha,j}$ is then a p-adic measure. In the supersingular case, both roots are admissible, but the p-adic distributions are unbounded on the compact-open sets of $\mathbb{Z}_p^*$.

Definition 3.1.4. The Mazur-Tate-Teitelbaum distributions attached to f and p are defined as

a) If f is ordinary at p: $\mu_{\alpha,j}$, where α is the unique root of the Hecke polynomial for f at p which is a p-adic unit.

b) If f is supersingular at p: $\mu_{\alpha_i,j}$, $i = 1, 2$, where α_i denote the roots of the Hecke polynomial.

For an ordinary prime p, it is possible to integrate continuous $\mathbb{Q}_p$-valued functions by using uniform approximation by locally constant functions (see for example [39, Chapter 2]). The definition of an integral in the supersingular case requires some more work. First of all, we need to restrict the class of functions to be integrated.

Definition 3.1.5. A function $F : \mathbb{Z}_p^* \to \mathbb{Q}_p$ is said to be locally analytic if there is a covering of $\mathbb{Z}_p^*$ by compact-open sets $D(a,\, p^m)^+$ such that

$$F|_{D(a,\,p^m)^+}(x) = \sum_{n=0}^{\infty} c_n(x-a)^n, \quad c_n \in \mathbb{Q}_p.$$

Let us denote by $V_{f,p}$ the $\mathbb{C}_p$-vector space $\mathcal{O}_f\left[\frac{1}{\alpha}\right] \otimes \Sigma_f \otimes \mathbb{C}_p$. The following theorem provides a $V_{f,p}$-valued integral operator attached to any admissible root.

Theorem 3.1.6. (Mazur-Tate-Teitelbaum, [49]) *Let $f \in S_k(\Gamma_0(N))$ be a normalized eigenform of the Hecke operator T_p, $p \nmid N$. For a compact-open subset $K \subseteq \mathbb{Z}_p^*$, there exists a unique $V_{f,p}$-valued $\mathbb{Q}_p$-linear operator on the space of locally analytic functions, denoted by $\int_K F(x)d\mu_\alpha(x)$, with the following properties:*

1. *Interpolation property:* $\int_K x^j d\mu_\alpha(x) = \mu_{\alpha,j}(K)$, *for* $0 \leq j \leq k-2$.

2. *Divisibility property: for any* $n \geq 0$

$$\int_{D(a,\, p^m)^+} (x-a)^n d\mu_\alpha(x) \in \left(\frac{p^n}{\alpha}\right)^m \alpha^{-1}\Sigma_f \otimes \mathbb{Z}_p.$$

3. *Continuity property: if* $F(x) = \sum_{n\geq 0} c_n (x-a)^n$ *in* $D(a,\, p^m)^+$, *then*

$$\int_{D(a,\, p^m)^+} F(x) d\mu_\alpha(x) = \sum_{n\geq 0} c_n \int_{D(a,\, p^m)^+} (x-a)^n d\mu_\alpha(x).$$

4. *For a fixed* F, *the assignment* $K \mapsto \int_K F(x) d\mu_\alpha(x)$ *yields a finitely additive function on the set of compact-open subsets of* $\mathbb{Z}_p^*$.

Since continuous characters are locally analytic, one can formulate the following

Definition 3.1.7. (The Mazur-Tate-Teitelbaum p-adic L-function) Assume that $p \nmid N$. Let $f \in S_k(\Gamma_0(N))$ be an eigenform of the Hecke operator T_p and α an admissible root of the Hecke polynomial of f at p. For $\chi \in \mathcal{X}$, we define

$$L_p(f, \alpha; \chi) = \int_{\mathbb{Z}_p^*} \chi(x) d\mu_\alpha(x).$$

Remark 3.1.8. These Mazur-Tate-Teitelbaum p-adic L-functions are known in the literature as cyclotomic p-adic distributions. The reason is that these p-adic L-functions are obtained as Mazur-Mellin transforms of the Mazur-Tate-Teitelbaum p-adic distributions, the domain of integration being $\mathbb{Z}_p^*$, which is the Galois group of the maximal abelian extension of $\mathbb{Q}$ unramified outside p.

For $x \in \mathbb{Z}_p^*$, we can write $x = \omega(x)\langle x \rangle$ where $\omega(x)$ is the unique $(p-1)$-th root of unity in $\mathbb{Z}_p^*$ congruent to x mod p and $\langle x \rangle \in D(1,p)^+$. Since $\langle x \rangle \in D\,(1,p)^+$, one can define $\langle x \rangle^s = \mathrm{Exp}_p\left(s\mathrm{Log}_p\left(\langle x \rangle\right)\right)$, where Exp_p is the p-adic exponential and Log_p the Iwasawa logarithm. For $s \in \mathbb{Z}_p$, the function $\chi_s(x) = \langle x \rangle^s$ belongs to $\mathcal{X}$. Let us denote $\Delta = \{\chi_s : s \in \mathbb{Z}_p\}$. To define x^s for $x \notin D(1,p)^+$, one has to fix a congruence class mod $p-1$, choose a sequence $\{s_n\} \in \mathbb{Z}^{\mathbb{N}}$ in this congruence class which tends to s in the

p-adic norm and set $x^s = \lim x^{s_n}$ (see [39] for details). Thus, having fixed an integer $0 \leq a \leq p-1$, one can define by density the continuous characters $\tilde{\chi}_s(x) = x^s$. Let us define $\Delta_{1,a} = \{\tilde{\chi}_s : s \in \mathbb{Z}_p\}$, once a is fixed. This way we can embed $\mathbb{Z}$ in Δ and in $\Delta_{1,a}$ for any a. We will prove that the restriction of $L_p(f,\alpha)$ to $\Delta_{1,a} \cap \mathbb{Z}$ is not identically zero for any a. Hence, we will ignore the congruence class and we will write Δ_1 for $\Delta_{1,a}$.

Denote:

$$L_p(f,\alpha)_1(s) = L_p(f,\alpha;\chi_{s-1}) = \int_{\mathbb{Z}_p^*} x^{s-1} d\mu_\alpha(x), \quad s \in \mathbb{Z}_p.$$

$$L_p\left(f,\alpha\right)_2(s) = L_p(f,\alpha;\tilde{\chi}_{s-1}) = \int_{\mathbb{Z}_p^*} \langle x \rangle^{s-1} d\mu_\alpha(x), \quad s \in \mathbb{Z}_p.$$

The following interpolation property holds (cf. [49]):

$$L_p(f,\alpha)_1(j) = \left(1 - \frac{p^j}{\alpha}\right)\left(1 - \frac{p^{k-2-j}}{\alpha}\right)\frac{j!}{(2\pi i)^j} L(f, j+1), 0 \leq j \leq k-2.$$

As in the complex analytic setting, a functional equation holds for the function $L_p(f,\alpha)_i$, $i = 1, 2$. Here we recall its proof for $L_p(f,\alpha)_1$ (cf. [49] for details). Let us introduce some notation.

Let $K \subseteq \mathbb{Z}_p^*$ be a compact-open set and F a locally analytic function over $\mathbb{Z}_p^*$. Let us define the map $g(x) = -\frac{1}{Nx}$, $x \in \mathbb{Z}_p^*$. We set

$$\tilde{F}(x) = N^{\frac{k-2}{2}} x^{k-2}(F \circ g)(x), \quad \tilde{K} = g(K), \quad \tilde{f} = w_N(f),$$

where w_N stands for the Atkin-Lehner involution on $S_k(\Gamma_0(N))$.

Proposition 3.1.9 (cf. [49], Theorem 17.1)**.** *If α is an admissible root for f, then,*

$$\int_K F(x) d\mu_\alpha(x) = \int_{\tilde{K}} \tilde{F}(x) d\mu_\alpha(x).$$

Corollary 3.1.10. *Suppose that f is a newform. For any $s \in \mathbb{Z}_p$,*

$$L_p(f,\alpha)_1(s) = \pm N^{1-s} L_p(f,\alpha)_1(k-s).$$

In particular, if $k = 2$, $L_p(f,\alpha)_1(s) = 0$ if and only if $L_p(f,\alpha)_1(2-s) = 0$.

Proof. Since f is a normalized newform, it is also an eigenfunction for the Atkin-Lehner involution; hence, $\tilde{f} = \pm f$, and we have

$$L_p(f,\alpha)_1(s) = \int_{\mathbb{Z}_p^*} x^{s-1} d\mu_\alpha(x) = \pm \int_{\mathbb{Z}_p^*} x^{k-2} \left(\frac{-1}{Nx}\right)^{s-1} d\mu_\alpha(x).$$

□

3.1.3 Non-vanishing results

As pointed out in the prolegomena, $\mathbb{Z}_p^*$ is topologically cyclic. The disc $D(1,p)^+$ is also topologically cyclic. Hence, let us fix topological generators α and β for $\mathbb{Z}_p^*$ and $D(1,p)^+$, respectively. Since any $\chi \in \mathcal{X}$ is defined by the value at α, we can identify $\mathcal{X}$ with $D(0,1)^* \subset \mathcal{O}_p^*$. One can alternatively define χ by specifying the value at β and at a generator of the group of $(p-1)$-th roots of unity, thus identifying $\mathcal{X}$ with $(p-1)$ copies of a contraction (or dilatation) of $\mathbb{Z}_p$ by an element of $\mathbb{Z}_p$.

Set $D(0,1)^* = D(0,1) \setminus \{0\}$. Under any of these identifications, $L_p(f,\alpha)$ is defined over $D(0,1)^* \subset \mathbb{C}_p^*$ and has a Taylor expansion with coefficients in $\mathcal{O}_f \otimes \mathbb{Z}_p$ provided that f is ordinary at p, i.e., it is an Iwasawa function (cf. [47] for details). Since by Theorem 3.1.2, $L_p(f,\alpha)$ is not identically zero at an infinite set of finite order characters, the series is not identically zero, and by the p-adic Weierstrass preparation theorem (cf. [39]) it has a finite number of zeros.

This argument relies on the above identification of $\mathcal{X}$ with $D(0,1)^*$. We give an alternative proof of the non vanishing of $L_p(f,\alpha)_1$. First we need some facts about p-adic norms and p-adic approximation theory.

Let us denote by χ_G the characteristic function of a set $G \subseteq \mathbb{Q}_p$. From now on, K will denote a compact-open subset of $\mathbb{Q}_p$. The p-adic ∞-norm of a continuous function $F : K \to \mathbb{Q}_p$ is defined by

$$||F||_{\infty,K,p} = \max_{x \in K} |F(x)|_p .$$

Let us denote by $\mathcal{C}^{(n)}(K,\mathbb{Q}_p)$ the $\mathbb{Q}_p$-vector space of $\mathbb{Q}_p$-valued n times continuously differentiable functions on K, and by $\mathbb{Q}_p[X](K,\mathbb{Q}_p)$ the $\mathbb{Q}_p$-vector space of $\mathbb{Q}_p$-valued functions on K defined by polynomials with coefficients in $\mathbb{Q}_p$. We will use the following p-adic analogue of the Stone-Weierstrass approximation theorem:

Theorem 3.1.11. *For any $n \geq 0$, $\mathbb{Q}_p[X](K,\mathbb{Q}_p)$ is dense in $\mathcal{C}^{(n)}(K,\mathbb{Q}_p)$ with the p-adic ∞-norm attached to this space.*

We will content ourselves with the case $n = 0$, which is a well known result published by Kaplansky. Theorem 3.1.11 is a generalization of this classical result. For a precise definition of the norm in $\mathcal{C}^{(n)}(K,\mathbb{Q}_p)$, and a proof of the statement, we refer the reader to [2].

3.1.4 The non-vanishing on $\mathbb{Z}_p$

Our aim is to prove the following result.

Theorem 3.1.12 ([17]). *Let $p > 2$ and let $f \in S_k(\Gamma_0(N))$ be a normalized newform ordinary at p and let α be the admissible root of the Hecke polynomial of f at p. Then $L_p(f,\alpha)_1$ does not vanish identically over $\mathbb{Z}_p$. Furthermore, if $k = 2$, $L_p(f,\alpha)_1$ does not vanish identically over $\mathbb{Z}_p^*$.*

Proof. Let us prove first that $L_p(f,\alpha)_1$ does not vanish identically over $\mathbb{Z}_p$. If this were not the case, we would have

$$\int_{\mathbb{Z}_p^*} x^m d\mu_\alpha(x) = 0, \quad \text{for all } m \geq 0, m \in \mathbb{Z}.$$

Let us fix $a \in \mathbb{Z}_p^* \cap \mathbb{Z}$, $n \in \mathbb{N}$ and $0 \leq j \leq k-2$. Denote by $\chi_{D(a,p^n)^+}$ the characteristic function of the compact open set $D(a,p^n)^+$ and set $F_{a,n,j}(x) = x^j \chi_{D(a,p^n)^+}(x)$. Since $F_{a,n,j}$ is a locally polynomial function on $\mathbb{Z}_p$ and since $\mathbb{Z}_p$ is totally disconnected, it is continuous. Thus, by Theorem 3.1.11, for any $m \geq 0$ one can choose a polynomial $P_m \in \mathbb{Q}_p[X]$ such that

$$||F_{a,n,j} - P_m||_{\infty,\mathbb{Z}_p^*,p} \leq p^{-m}.$$

By hypothesis

$$\int_{\mathbb{Z}_p^*} P_m(x) d\mu_\alpha(x) = 0.$$

Set $j = \frac{k}{2}$. Theorem 3.1.6 implies that $\mu_{a,\frac{k}{2}}\left(D\left(a,\, p^n\right)^+\right) = \displaystyle\int_{\mathbb{Z}_p^*} F_{a,n,\frac{k}{2}}(x) d\mu_a(x)$.

Thus,

$$\mu_{a,\frac{k}{2}}\left(D\left(a,\, p^n\right)^+\right) = \int_{\mathbb{Z}_p^*} \left(F_{a,n,\frac{k}{2}}(x) - P_m(x)\right) d\mu_a(x).$$

Now, since f is ordinary at p and $\mu_{\alpha,\frac{k}{2}}$ is a p-adic measure, we have:

$$\left|\mu_{a,\frac{k}{2}}\left(D\left(a,\, p^n\right)^+\right)\right|_p \leq M||F_{a,n,\frac{k}{2}} - P_m||_{\infty,\mathbb{Z}_p^*,p} \leq Mp^{-m}.$$

The constant M depends only on f; thus, by letting m tend to infinity we would obtain

$$\int_0^\infty f\left(\frac{a}{p^n} + it\right) t^{\frac{k}{2}-1} dt - \frac{p^{k-2}}{\alpha} \int_0^\infty f\left(\frac{a}{p^{n-1}} + it\right) t^{\frac{k}{2}-1} dt = 0. \qquad (3.1.6)$$

Iterating 3.1.6 and taking into account that, in particular, f is periodic of period 1, we would obtain

$$\int_0^\infty f\left(\frac{a}{p^n}+it\right)t^{\frac{k}{2}-1}dt=\left(\frac{p^{k-2}}{\alpha}\right)^n\int_0^\infty f(it)t^{\frac{k}{2}-1}dt. \tag{3.1.7}$$

Hence, if χ is Dirichlet character of conductor p^n, we would have

$$\Lambda\left(f,\chi,\frac{k}{2}\right)=N^{\frac{k}{4}}\frac{\tau(\chi)}{p^n}\sum_{a=0}^{p^n-1}\overline{\chi(a)}\left(\frac{p^{k-2}}{\alpha}\right)^n\int_0^\infty f(it)t^{\frac{k}{2}-1}dt.$$

Since $\sum_{a=1}^{p^n-1}\overline{\chi(a)}=0$, we would obtain that $\Lambda\left(f,\chi,\frac{k}{2}\right)=0$, and since n is arbitrary, we would reach a contradiction with Theorem 3.1.2.

Let us observe that if $k=2$, the functional equation in Corollary 3.1.10 and the observation that if $|s|_p<1$, then $2-s$ is a p-adic unit imply that $L_p\left(f,\alpha\right)_1$ is not identically zero over $\mathbb{Z}_p^*$. □

3.1.5 Results on the order of the p-adic L-function

Let us recall that

$$\langle x\rangle^s=\mathrm{Exp}_p\left(s\mathrm{Log}_p\left(\langle x\rangle\right)\right)=\sum_{n=0}^\infty\frac{s^n}{n!}\left(\mathrm{Log}_p\left(\langle x\rangle\right)\right)^n,\quad s\in\mathbb{Z}_p.$$

In the ordinary case, we can interchange the infinite sum with the integral over $\mathbb{Z}_p^*$ to express the restriction of $L_p\left(f,\alpha\right)$ to Δ as the following power series:

$$\int_{\mathbb{Z}_p^*}\langle x\rangle^s d\mu_\alpha(x)=\sum_{n=0}^\infty\frac{s^n}{n!}\int_{\mathbb{Z}_p^*}\left(\mathrm{Log}_p\left(\langle x\rangle\right)\right)^n d\mu_\alpha(x).$$

It is easy to see that this power series has its coefficients in $\mathcal{O}_f\otimes\mathbb{Q}_p$. On the other hand, we have

$$\int_{\mathbb{Z}_p^*}x^s d\mu_\alpha(x)=\sum_{a=1}^{p-1}\int_{D(a,p)^+}\omega(x)^s\langle x\rangle^s d\mu_\alpha(x). \tag{3.1.8}$$

Since $\omega(x)=a$ for any $x\in D\left(a,p\right)^+$, the right hand side of 3.1.8 equals

$$\sum_{a=1}^{p-1}\omega(a)^s\int_{D(a,p)^+}\langle x\rangle^s d\mu_\alpha(x),$$

which leads to

$$L_p\left(f,\alpha\right)_1\left(s\right)=\sum_{n=0}^{\infty}\frac{s^n}{n!}\sum_{a=1}^{p-1}\omega(a)^s\int_{D(a,p)^+}\left(\mathrm{Log}_p\left(\langle x\rangle\right)\right)^n d\mu_\alpha(x),$$

which, due to the fact of f being ordinary at p, again has coefficients in $\mathcal{O}_f\otimes\mathbb{Q}_p$. Thus, we can apply the p-adic Weierstrass preparation theorem to conclude that $L_p\left(f,\alpha\right)_i$ $(i=1,2)$ has a finite number of zeros in $\mathbb{Z}_p$.

The following results show that the supersingular case is different.

Theorem 3.1.13 (Mazur, [46])**.** *Let f be supersingular at the prime p and let α_1,α_2 be the roots of the Hecke polynomial. If $|\alpha_1|_p\neq|\alpha_2|_p$, at least one of $L_p(f,\alpha_1)_2$ and $L_p(f,\alpha_2)_2$ has infinitely many zeros in $\mathbb{Z}_p$.*

Theorem 3.1.14 (Perrin-Riou, [55])**.** *Let f be supersingular at the prime p. Denote by $a_p(f)$ the p-th Fourier coefficient of f and let α_1,α_2 be the roots of the Hecke polynomial. If $a_p(f)=0$, at least one of $L_p(f,\alpha_1)_2$ and $L_p(f,\alpha_2)_2$ has infinitely many zeros in $\mathbb{Z}_p$. If $\alpha_1\notin K_f(\alpha_2)$, both functions have infinitely many zeros.*

Remark 3.1.15. The proofs are non constructive and they do not specify which function has infinitely many zeros, nor whether the orders of vanishing are finite or not. Since the p-adic topology is totally disconnected, and an identity principle does not hold, it could well be that a non zero locally analytic function had infinite order of vanishing at a point of the domain. The results of this section show that this is not the case for $L_p(f,\alpha)_i$, $i=1,2$.

For any locally analytic function $g:\mathbb{Z}_p\to\mathbb{C}_p$ and for any $s_0\in\mathbb{Z}_p$, let us denote by $\mathrm{ord}_{s=s_0}(g)$ the first natural number n such that $g^{(n)}(s_0)\neq 0$. We will prove the following

Theorem 3.1.16 ([17])**.** *Let $f\in S_k(\Gamma_0(N))$ be a normalized newform, supersingular at $p\geq 5$, and α an admissible root of the Hecke polynomial for f at p. Suppose that $L_p(f,\alpha)_1\not\equiv 0$. Then, for any $s_0\in\mathbb{Z}_p$,*

$$\mathrm{ord}_{s=s_0}L_p(f,\alpha)_i(s)<\infty\text{ for }i=1,2.$$

Before we give the proof, we need to introduce some preparatory tools. We recall the following standard notations

$$l_\infty(\mathbb{C}_p)=\{(x_n)_{n\geq 1}\in\mathbb{C}_p^{\mathbb{N}}:\ \sup_{n\geq 1}|x_n|_p<\infty\},$$

$$c_0(\mathbb{C}_p) = \{(x_n)_{n\geq 1} \in \mathbb{C}_p^{\mathbb{N}} : \lim_{n\to\infty} |x_n|_p = 0\}.$$

Both linear spaces are complete with respect to the norm

$$||(x_n)_{n\geq 1}||_{\infty,p} = \sup_{n\geq 1} |x_n|_p.$$

Let $D_i = D(i,p)^+$, $1 \leq i \leq p-1$. Given $x \in D_i$ and by setting ω_i for the unique $(p-1)$-th root of unity congruent to i mod p, we may write $x = \omega_i\langle x\rangle$, with $\langle x\rangle = 1 + p\tilde{x}$, with $\tilde{x} \in \mathbb{Z}_p$. Then

$$\tilde{x} = \frac{1}{p}\left(\frac{x}{\omega_i} - 1\right) = \frac{1}{p}\left(\frac{1}{\omega_i}(x-i) + \frac{i}{\omega_i} - 1\right).$$

We set $a_{1,i} = p^{-1}\omega_i^{-1} \in p^{-1}\mathbb{Z}_p$ and $a_{0,i} = p^{-1}\left(i{\omega_i}^{-1} - 1\right) \in \mathbb{Z}_p$.

For an admissible root α, let us write

$$L_p(f,\alpha)_2(s) = \int_{\mathbb{Z}_p^*} (1+p\tilde{x})^{s-1}\, d\mu_\alpha(x) = \int_{\mathbb{Z}_p^*} \sum_{n=0}^{\infty} \binom{s-1}{n} p^n \tilde{x}^n d\mu_\alpha(x),$$

and likewise

$$L_p(f,\alpha)_1(s) = \sum_{a=1}^{p-1} \omega(a)^{s-1} \int_{D(a,p)^+} (1+p\tilde{x})^{s-1}\, d\mu_\alpha(x) =$$

$$= \sum_{a=1}^{p-1} \omega(a)^{s-1} \int_{D(a,p)^+} \sum_{n=0}^{\infty} \binom{s-1}{n} p^n \tilde{x}^n d\mu_\alpha(x).$$

Since $n! = p^{\frac{n-\sigma_n}{p-1}} u_n$, with $u_n \in \mathbb{Z}_p^*$ and σ_n being equal to the sum of the p-adic digits of n, we shall have

$$\binom{s-1}{n} p^n = p^{\frac{(p-2)n+\sigma_n}{p-1}} u_n q_n(s),$$

where $q_n(s) = (s-1)(s-2)...(s-n) \in \mathbb{Z}_p[s]$ is a polynomial of degree n.

Proposition 3.1.17. *Let $p \geq 5$ be a prime number and a be a p-adic unit. Both for $U = D(a,p)^+$ or $U = \mathbb{Z}_p^*$ and for any sequence $(u_n)_{n\geq 1}$ of p-adic units, the sequence*

$$\left(p^{\frac{(p-2)n+\sigma_n}{p-1}} u_n \int_U \tilde{x}^n d\mu_\alpha(x)\right)_{n\geq 1}$$

is in $c_0(\mathbb{C}_p)$.

Proof. Let $g_n(x) = \tilde{x}^n$, $n \geq 1$. With the above notations, in each disc D_i we shall have

$$g_1|_{D_i}(x) = a_{1,i}(x-i) + a_{0,i},$$

with $a_{1,i} \in p^{-1}\mathbb{Z}_p$ and $a_{0,i} \in \mathbb{Z}_p$. Thus,

$$g_n|_{D(i,p)^+}(x) = \sum_{r=0}^{n} \binom{n}{r} a_{1,i}^r a_{0,i}^{n-r} (x-i)^r.$$

Furthermore, by Theorem 3.1.6 we may write

$$\int_{D(i,p)^+} (x-i)^r d\mu_\alpha(x) = \alpha^{-2} p^r \gamma_{i,r}, \text{ with } \gamma_{i,r} \in \Sigma_f \otimes \mathbb{Z}_p.$$

Thus, there exists a constant $R \geq 0$ such that

$$\left| \int_{D(i,p)^+} g_n(x) d\mu_\alpha(x) \right|_p \leq R \left|\alpha^{-2}\right|_p \max_{0 \leq r \leq n} \left| \binom{n}{r} \right|_p \leq R \left|\alpha^{-2}\right|_p p^{\frac{n-\sigma_n}{p-1}}.$$

Combining this with the strong triangle inequality, we obtain

$$\left| \int_{\mathbb{Z}_p^*} \tilde{x}^n d\mu_\alpha(x) \right|_p \leq R \left|\alpha^{-2}\right|_p p^{\frac{n-\sigma_n}{p-1}},$$

so that

$$\left| p^{\frac{(p-2)n+\sigma_n}{p-1}} u_n \int_U \tilde{x}^n d\mu_\alpha(x) \right|_p \leq p^{\frac{(2-p)n-\sigma_n}{p-1}} \left| \int_U \tilde{x}^n d\mu_\alpha(x) \right|_p \leq R \left|\alpha^{-2}\right|_p p^{\frac{(3-p)n-2\sigma_n}{p-1}}.$$

□

Proposition 3.1.17 together with the fact that $\frac{p^n}{n!} = p^{\frac{(p-2)n+\sigma_n}{p-1}} u_n$, with $u_n \in \mathbb{Z}_p^*$, implies

$$L_p(f,\alpha)_1(s) = \sum_{n=0}^{\infty} \sum_{a=1}^{p-1} \omega(a)^{s-1} \binom{s-1}{n} p^n \int_{D(a,p)^+} \tilde{x}^n d\mu_\alpha(x), \tag{3.1.9}$$

and

$$L_p(f,\alpha)_2(s) = \sum_{n=0}^{\infty} \int_{\mathbb{Z}_p^*} \binom{s-1}{n} p^n \tilde{x}^n d\mu_\alpha(x). \tag{3.1.10}$$

We will prove the statement of the theorem only for $L_p(f,\alpha)_2$, since the proof for $L_p(f,\alpha)_1$ is completely analogous.

Set $h_n(s) = n!\binom{s-1}{n}$, the n-th Pochhammer symbol. The following result will allow us to differentiate the series $L_p(f,\alpha)_2(s)$ term by term.

Proposition 3.1.18. *For any* $(\lambda_n)_{n\geq 0} \in c_0(\mathbb{C}_p)$, *the series* $\sum_{n=0}^{\infty} \lambda_n h_n(s)$ *converges uniformly in* $\mathbb{Z}_p$ *to a function* $f \in \mathcal{C}^{(j)}(\mathbb{Z}_p, \mathbb{C}_p)$ *for any* $j \geq 0$. *Moreover,*

$$f^{(j)}(s) = \sum_{n=0}^{\infty} \lambda_n h_n^{(j)}(s), \quad \text{for } j \geq 0.$$

Proof. Let us first observe that, since $(\lambda_n)_n \in c_0(\mathbb{C}_p)$, the sum $\sum_{n=0}^{\infty} \lambda_n h_n^{(j)}(s)$ converges for any $s \in \mathbb{Z}_p^*$. Next, we have to prove that, for any $j \geq 0$,

$$\lim_{m\to\infty} \left| \frac{\sum_{n=0}^{\infty} \lambda_n \left(h_n^{(j)}(s+p^m) - h_n^{(j)}(s) - p^m h_n^{(j+1)}(s) \right)}{p^m} \right|_p = 0, \text{ for any } s \in \mathbb{Z}_p^*. \tag{3.1.11}$$

We remark that the mean-value theorem does not hold in general in the p-adic setting (cf. [60]). We distinguish the cases $j = 1$ and $j > 1$.

a) For $j = 1$, let us denote by $e_k(a_1, ..., a_n)$ the k-th symmetric elementary polynomial in the indeterminates $\{a_1, ..., a_n\}$. For $n, m \geq 1$ and $x \in \mathbb{Z}_p^*$, we have that

$$h_n(s) = e_n(s-1, ..., s-n),$$

$$h_n(s+p^m) = \sum_{j=0}^{n} p^{jm} e_{n-j}(s-1, ..., s-n),$$

and $h_n'(s) = e_{n-1}(s-1, s-2, ..., s-n)$. Thus,

$$h_n(s+p^m) - h_n(s) - p^m h_n'(s) = \sum_{j=2}^{n} p^{jm} e_{n-j}(s-1, ..., s-n)$$

and

$$\left| \frac{h_n(s+p^m) - h_n(s) - p^m h_n'(s)}{p^m} \right|_p \leq p^{-m}.$$

Since $(\lambda_n)_n$ is bounded, the result follows in this case.

b) Suppose $j > 1$. A straightforward computation shows that

$$h_n^{(j)}(s) = j! e_{n-j}(s-1, s-2, ..., s-n).$$

Thus,

$$h_n^{(j)}(s+p^m) = j! \sum_{r=0}^{n-j} c_r p^{rm} e_{n-j-r}(s-1, s-2, ..., s-n),$$

for suitable integers $c_r \geq 1$. Notice that $c_0 = 1$.

Lemma 3.1.19. $c_1 = j+1$. □

Proof. Let us introduce the notation $D(s) := 1$. We have

$$e_{n-j}(s_1+p^m, s_2+p^m, ..., s_n+p^m) = \sum_{\{i_1,i_2,...,i_{n-j}\}\subset\{1,...,n\}} (s_{i_1}+p^m)(s_{i_2}+p^m)...(s_{i_{n-j}}+p^m) =$$

$$= e_{n-j}(s_1, s_2, ..., s_n) + \sum_{\{i_1,i_2,...,i_{n-j}\}\subset\{1,...,n\}} \sum_{r=1}^{n-j} p^m s_{i_1}...D(s_{i_r})...s_{i_{n-j}} + ...$$

where the dots stand for the sum of the symmetric polynomials of degree less than $n-j-1$ in the variables $s_1, s_2, ..., s_n$ multiplied by p^{rm} with $r \geq 2$. Now, c_1 is the number of times that any monomial $s_{i_1}...D(s_{i_r})...s_{i_{n-j}}$ appears repeated in the sum, that is to say, the number of possible choices for the index i_r among the variables $\{s_1, ..., s_n\} - \{s_{i_1}, ..., s_{i_{r-1}}, s_{i_{r+1}}, ..., s_{i_{n-j}}\}$, which is $j+1$. □

Let us note that

$$h_n^{(j+1)}(s) = (j+1)! e_{n-j-1}(s-1, s-2, ..., s-n).$$

Hence, using Lemma 3.1.19, we have

$$h_n^{(j)}(s+p^m) - h_n^{(j)}(s) - p^m h_n^{(j+1)}(s) = j! \sum_{r=2}^{n-j} c_r p^{rm} e_{n-j-r}(s-1, s-2, ..., s-n)$$

and the result holds. □

We proceed now with the proof of Theorem 3.1.16.

Proof. The non-vanishing of $L_p(f, \alpha)$ at the finite order characters and the growth behaviour of $\mu_{f,\alpha}$, imply that $L_p(f, \alpha)_2$ is not identically zero (cf. [56]), thus, there exists an integer $n \geq 0$ such that

$$\int_{\mathbb{Z}_p^*} \tilde{x}^n d\mu_\alpha(x) \neq 0.$$

Let us define the (non-empty) set

$$\Sigma = \{n \geq 0 : \int_{\mathbb{Z}_p^*} \tilde{x}^n d\mu_{f,\alpha} \neq 0\}.$$

Fix now $s_0 \in \mathbb{Z}_p$. If Σ is finite, we consider its maximal integer n and, by taking the n-th derivative of $L_p(f,\alpha)_2$ at $s = s_0$, we obtain

$$\frac{d^n}{ds^n} L_p(f,\alpha)_2(s)|_{s=s_0} = p^n \int_{\mathbb{Z}_p^*} \tilde{x}^n d\mu_{f,\alpha} \neq 0.$$

Now we suppose that Σ is an infinite set. For any $n_r \in \Sigma$, the n_r-th term in the expansion of $L_p(f,\alpha)_2$ has the form

$$p^{n_r} \binom{s-1}{n_r} \int_{\mathbb{Z}_p^*} \tilde{x}^{n_r} d\mu_{f,\alpha} = p^{\frac{(p-2)n_r + \sigma_{n_r}}{p-1}} u_{n_r} q_{n_r}(s) \int_{\mathbb{Z}_p^*} \tilde{x}^{n_r} d\mu_{f,\alpha}\,,$$

with $q_{n_r}(s) = (s-1)(s-2)...(s-n_r)$. If we denote by $a_{i,j}$ the n_i-th derivative of $q_{n_j}(s)$ at $s = s_0$, we may define the linear endomorphism

$$\psi : c_0(\mathbb{C}_p) \longrightarrow c_0(\mathbb{C}_p), \quad x = (x_n)_{n\geq 1} \mapsto \left(\sum_{r=n}^{\infty} a_{r,n} x_r \right)_{n \geq 1}.$$

Since $a_{i,j} \in \mathbb{Z}_p$, ψ is well defined and $||\psi(x)||_{\infty,p} \leq ||x||_{\infty,p}$. Hence, ψ is continuous. We can see this endomorphism as being represented by an infinite matrix $(a_{i,j})_{i,j\geq 1}$ which is upper triangular.

Proposition 3.1.20. *The endomorphism ψ is injective.*

Proof. For $x = (x_{n_r})_{r\geq 1} \in c_0(\mathbb{C}_p)$, we have $\psi(x) = (D \circ \phi)(x)$ where $D : c_0(\mathbb{C}_p) \longrightarrow c_0(\mathbb{C}_p)$, $x = (x_r) \mapsto (n_r! x_r)$, and $\phi : c_0(\mathbb{C}_p) \longrightarrow c_0(\mathbb{C}_p)$ is given by left natural multiplication with the infinite matrix

$$M_\phi = \begin{pmatrix} 1 & \frac{a_{1,2}}{n_1!} & \frac{a_{1,3}}{n_1!} & \frac{a_{1,4}}{n_1!} & \dots \\ 0 & 1 & \frac{a_{2,3}}{n_2!} & \frac{a_{2,4}}{n_2!} & \dots \\ 0 & 0 & 1 & \frac{a_{3,4}}{n_3!} & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Let us check that $\phi(c_0(\mathbb{C}_p)) \subseteq c_0(\mathbb{C}_p)$. Note that $q_{n_j}(s) = s^{n_j} - e_1^{n_j} s^{n_j-1} + ... + (-1)^{n_j} e_{n_j}^{n_j}$, with $e_r^{n_j}$ the r-th elementary symmetrical polynomial in the roots $\{1, 2, ..., n_j\}$. Thus,

$$\frac{1}{n_i!}\frac{d^{n_i}}{ds^{n_i}} q_{n_j}(s) = \quad \tbinom{n_j}{n_j-n_i} s^{n_j-n_i} - \tbinom{n_j-1}{n_j-1-n_i} e_1^{n_j} s^{n_j-n_i-1} + ... + (-1)^{n_j} \tbinom{n_i}{0} e_{n_i}^{n_j}.$$

Since

$$\binom{n_j - r}{n_j - n_i - r} = p^{\frac{-\sigma_{n_j-r} + \sigma_{n_j-n_i-r} + \sigma_{n_i}}{p-1}} \theta_r,$$

with $\theta_r \in \mathbb{Z}_p^*$, for $1 \leq r \leq n_j - n_i$, and

$$-\sigma_{n_j-r} + \sigma_{n_j-n_i-r} + \sigma_{n_i} = (p-1)\mathrm{ord}_p \binom{n_j + n_i - r}{n_i}$$

(cf. [39]), it follows that

$$\left| \frac{1}{n_i!}\frac{d^{n_i}}{ds^{n_i}} q_{n_j}(s)|_{s=s_0} \right|_p \leq 1.$$

Hence, ϕ is well defined and its associated matrix M_ϕ is upper triangular with ones on the diagonal. To prove the injectivity, we proceed by steps:

Step 1. We consider the adjoint matrix of the element $a_{i,j}$:

$$M_\phi^{i,j} = \begin{pmatrix} \frac{a_{1,1}}{n_1!} & \dots & \frac{a_{1,j-1}}{n_1!} & \frac{a_{1,j+1}}{n_1!} & \dots \\ 0 & \dots & \frac{a_{2,j-1}}{n_2!} & \frac{a_{2,j+1}}{n_2!} & \dots \\ \vdots & \dots & \vdots & \vdots & \vdots \\ 0 & \dots & \frac{a_{i-1,j-1}}{n_{i-1}!} & \frac{a_{i-1,j+1}}{n_{i-1}!} & \dots \\ 0 & \dots & \frac{a_{i+1,j-1}}{n_{i+1}!} & \frac{a_{i+1,j+1}}{n_{i+1}!} & \dots \\ \vdots & \dots & \vdots & \vdots & \ddots \end{pmatrix}.$$

From a particular row onwards, this matrix becomes upper triangular, with ones on the diagonal, hence we can formally compute the determinant $\det(M_\phi^{i,j})$ expanding along the first row. The result is a finite sum of finite products of the terms $\frac{a_{i,j}}{n_i!} \in \mathbb{Z}_p$; therefore, it is a p-adic integer.

Step 2. We write together all the determinants $\det(M_\phi^{i,j})$, forming the adjoint matrix and take the transpose, obtaining an upper-triangular matrix with entries in $\mathbb{Z}_p$ and ones on the diagonal. We write a few terms of this matrix:

$$M'_\phi = \begin{pmatrix} 1 & -\frac{a_{1,2}}{n_1!} & -\frac{a_{1,3}}{n_1!} + \frac{a_{1,2}a_{2,3}}{n_1!n_2!} & -\frac{a_{1,2}a_{2,3}a_{3,4}}{n_1!n_2!n_3!} + \frac{a_{1,3}a_{3,4}}{n_1!n_3!} + \frac{a_{1,2}a_{3,4}}{n_1!n_3!} - \frac{a_{1,4}}{n_1!} & \cdots \\ 0 & 1 & -\frac{a_{2,3}}{n_2!} & \frac{a_{2,4}a_{3,4}}{n_2!n_3!} - \frac{a_{2,4}}{n_2!} & \cdots \\ 0 & 0 & 1 & -\frac{a_{3,4}}{n_3!} & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Now, M'_ϕ defines again a continuous linear endomorphism of $c_0(\mathbb{C}_p)$, which we call ϕ'.

Step 3. By construction, to compute $\phi(x)$ it suffices to multiply the matrix M_ϕ by x, seen as a column vector, obtaining $M_\phi x$. Analogously, $\phi' \circ \phi(x)$ can be obtained by multiplication of $M_{\phi'}$ by the column vector $M_\phi x$. Since by construction $M_{\phi'} \circ M_\phi = I$ it follows that $(\phi' \circ \phi)(x) = x$ for all $x \in c_0(\mathbb{C}_p)$, i.e., ϕ' is a right inverse of ϕ.

Since D is trivially injective, so is ψ, completing the proof of Proposition 3.1.20 and Theorem 3.1.16. □

Remark 3.1.21. To any elliptic curve $E/\mathbb{Q}$ of conductor N, we can attach its complex analytic L-series $L(E, s)$. By modularity, there exists a weight 2 normalized newform f for $\Gamma_0(N)$ such that $L(E, s) = L(f_E, s)$. For an admissible root α of the Hecke polynomial of f_E at p, the corresponding p-adic L-functions of E are defined by setting

$$L_p(E, \alpha)_i(s) = L_p(f_E, \alpha)_i(s), \quad s \in \mathbb{Z}_p \quad i = 1, 2.$$

Corollary 3.1.22. *Let $p \geq 5$ and α an admissible root of the Hecke polynomial of f_E at p for which f_E is supersingular. If $L_p(E, \alpha)_1 \not\equiv 0$ then*

$$\mathrm{ord}_{s=s_0} L_p(E, \alpha)_i(s) < \infty, \ i = 1, 2$$

for any $s_0 \in \mathbb{Z}_p$.

3.2 Mazur and Swinnerton-Dyer p-adic L- functions

Here we present another construction of a p-adic L-function for a modular elliptic curve, namely, that carried out in [47], which is slightly different from

the one presented in the preceding section when $k = 2$. We show that both constructions are equivalent and explain a p-adic analogue of the Birch and Swinnerton-Dyer conjecture, involving this construction.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let $f_E \in S(\Gamma_0(N))$ its associated newform. Suppose that E has integer coefficients. Denote by $H_1(E,\mathbb{Z})$ the subgroup of classes of closed paths in $H_1(E,\mathbb{R})$ and set $H_1(E,\mathbb{Q}) = H_1(E,\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Take a prime p such that $(p, a_p) = 1$ where $a_p = a_p(f)$ is the p-th Fourier coefficient of f_E. Then, $p+1-a_p(f) = N_p(E)$, where $N_p(E)$ is the number of points of E on $\mathbb{F}_p$. The Hecke polynomial of f_E at p has two roots, one of which, say α, is a p-adic unit. Given $r \in \mathbb{Q}$, we write $\lambda(f_E, r)$ instead of $\lambda(f_E, r, 0)$ (notice that for weight 2, the only critical value is $j = 0$).

Proposition 3.2.1 (Manin, [45]). *For any $r \in \mathbb{Q}$, $\lambda(f_E, r) \in H_1(E,\mathbb{Q})$.*

Since, in addition, the modular integrals belong to a finitely generated $\mathbb{Z}$-lattice, and the complex conjugation acts as an involution on $H_1(E,\mathbb{R})$, it follows that there exist two real numbers Ω^+, Ω^- such that the modular integrals belong to the $\mathbb{Z}$-lattice $\Sigma_f = \mathbb{Z}\Omega^+ + \mathbb{Z}i\Omega^-$. Let $\lambda(f,r)^+, \lambda(f,r)^- \in \mathbb{Z}$ such that $\lambda(f,r) = \lambda(f,r)^+\Omega^+ + \lambda(f,r)^- i\Omega^-$.

Given an integer a coprime to p and to integers $n, m \geq 1$, with $m \geq n$, set $S_n^m(a) = \{x \in \{1, ..., p^m - 1\}, x \equiv a \pmod{p^n}\} \cap \mathbb{Z}_p^*$.

Proposition 3.2.2 (Mazur and Swinnerton-Dyer, [47]). *Let α be a root of the Hecke polynomial of f_E which is a p-adic unit. Define*

$$\mu_{E,\alpha,m}^{\pm}(a + p^n\mathbb{Z}_p) = \alpha^{-m} \sum_{b \in S_n^m(a)} \lambda\left(f_E, \frac{b}{p^m}\right)^{\pm}.$$

Then, there exists $\mu_{E,\alpha}^{\pm}(a + p^n\mathbb{Z}_p) = \lim_{m\to\infty} \mu_{E,\alpha,m}^{\pm}(a + p^n\mathbb{Z}_p)$ (p-adically). Furthermore, $\mu_{E,\alpha}$ is a p-adic measure.

Proof. Suppose that the limits exist. Then, it suffices to check the distribution property for any m large enough. But this is immediate, for

$$\sum_{j=0}^{p-1} \mu_{E,\alpha,m}^{\pm}(a + jp^n + p^{n+1}\mathbb{Z}_p) = \alpha^{-m} \sum_{j=0}^{p-1} \sum_{b \in S_n^{m+1}(a+jp^n)} \lambda\left(f_E, \frac{b}{p^{m+1}}\right)^{\pm}.$$

To check that the limit exists, fix integers $n \geq 1$ and a coprime to p and denote $A_m^{\pm} = \alpha^{-m} \sum_{b \in S_n^m(a)} \lambda\left(f_E, \frac{b}{p^m}\right)^{\pm}$. Since f_E is an eigenform for T_p, we have

$$a_p(f)\alpha^m A_m^{\pm} = \alpha^{m+1} A_{m+1}^{\pm} + p\alpha^{m-1} A_{m-1}^{\pm} + p^{m-n} \sum_{j=0}^{p-1} \lambda(f_E, \frac{j}{p})^{\pm}.$$

Since α is a root of the Hecke polynomial, we have that

$$\alpha^{m+1}\left(A_{m+1}^{\pm} - A_m^{\pm}\right) = p\alpha^{m-1}\left(A_m^{\pm} - A_{m-1}^{\pm}\right) + p^{m-n} \sum_{j=0}^{p-1} \lambda(f_E, \frac{j}{p})^{\pm}.$$

Since $\sum_{j=0}^{p-1} \lambda(f_E, \frac{j}{p})^{\pm} \in \Sigma_f$ and α is a p-adic unit, by induction, we have that $A_{m+1}^{\pm} - A_m^{\pm} \in p^{m-n}\left(\mathbb{Z}_p \otimes_{\mathbb{Z}} \Sigma_f\right)$. □

Definition 3.2.3. (The Mazur and Swinnerton-Dyer p-adic L-function). Let $\chi \in \mathcal{X}$ a p-adic character. Define

$$L_p(E, \alpha, \chi) = c_E \int_{\mathbb{Z}_p^*} \chi d\mu_{E,\alpha}^{\mathrm{sgn}(\chi)},$$

where $\mathrm{sgn}(\chi) = +$ if χ is even and $-$ otherwise, and where c_E is the Manin constant attached to E (see [45]).

Proposition 3.2.4 (Mazur and Swinnerton-Dyer, [47])**.** *Let α_1, α_2 be the roots of the Hecke polynomial for f_E at p. Suppose that $\alpha := \alpha_1$ is the unit root. Then,*

$$L_p(E, \alpha, 1) = \frac{-N_p}{\left(\alpha_1^2 - p\right)\left(1 - \alpha_2\right)^2} \sum_{j=0}^{p-1} \lambda\left(f_E, \frac{j}{p}\right).$$

Proof. Denote $S_m = \sum_{j=1}^{p^m-1} \lambda\left(f_E, \frac{j}{p^m}\right)$. Then, $L_p(E, \alpha, 1) = \lim_{m \to \infty} \alpha^{-m} S_m$. Using that f_E is an eigenform for T_p and that α is a root of the Hecke

polynomial, one obtains that the sequence $(S_m)_{m\geq 1}$ satisfies the following difference equation:

$$a_p(f_E)S_m = pS_{m-1} + S_m - p^{m-1}(p-1)S_1,$$

with a general solution of the form $S_m = \left(A\alpha_1^m + B\alpha_2^m + \frac{p^{m-1}(p-1)}{N_p}\right) S_1$. The constants are determined by setting $m = 0, 1$ in the general solution. □

In general, for any Dirichlet character, we have the following interpolation property.

Proposition 3.2.5. *Let χ be a Dirichlet character of conductor p^r. Then,*

$$L_p(E, \alpha, \chi) = \frac{\alpha^{1-r}}{\alpha - p\alpha^{-1}} \sum_{j=1}^{p^r} \overline{\chi}(j) \int_{\frac{a}{p^r}}^{\frac{a}{p^r}+i\infty} f_E(z)dz.$$

□

Let $\phi_E : X_0(N) \to E$ denote the modular parametrization morphism attached to E renormalized so that $\phi_E(i\infty) = 0_E$. Let $\omega \in H^0(E, \Omega_E)$ be an invariant differential for E such that $\phi_E^*(\omega) = f(q)\frac{dq}{q}$, where q is the local parameter of $X_0(N)$ at $i\infty$. It is known that $\phi_E(0)$ is a torsion point and that ϕ_E brings the path $\{0, i\infty\}$ into $E(\mathbb{R})$, hence there exists $M \in \mathbb{Q}$ such that $\int_0^{i\infty} f_E(z)dz = M \int_{E(\mathbb{R})} \omega$. This M is called the winding number of ϕ_E.

Proposition 3.2.6. *Let $t = 1, 2$ respectively if $E(\mathbb{R})$ has 1 or 2 connected components. Then,*

$$L_p(E, \alpha, 1) = \frac{ctN_p^2 M}{(\alpha_1^2 - p)(1-\alpha_2)^2}.$$

Proof. By Proposition 3.2.4, we only have to check that $\sum_{j=0}^{p-1} \lambda\left(f_E, \frac{j}{p}\right) = -ctN_nM$, but this follows from the fact that $\sum_{j=0}^{p-1} \lambda_E\left(f_E, \frac{j}{p}\right) = -N_p\phi_E(0)$

(which is again a straightforward consequence of f_E being an eigenform for T_p) and from the equality

$$\int_0^{i\infty} \phi^*(\omega) = M \int_{E(\mathbb{R})} \omega = c\lambda(f_E, 0).$$

□

Since the definitions of the p-adic measures carried out in [47] and in [49] are different, it is worth justifying that they are indeed the same, provided that E has good ordinary reduction at p, which is equivalent to saying that f_E is ordinary at p.

Proposition 3.2.7. *If E has good ordinary reduction at p, the Mazur and Swinnerton Dyer measure equals the Mazur-Tate-Teitelbaum measure up to a non-zero scalar.*

Proof. Denote respectively by μ_{MSD} and μ_{MTT} the Mazur and Swinnerton-Dyer and the Mazur-Tate-Teitelbaum p-adic measures and let $L_p(E, \alpha, \chi)_{MSD}$, $L_p(E, \alpha, \chi)_{MTT}$ denote the corresponding p-adic L-functions. By Proposition 3.2.5, together with the above material, we have that

$$L_p(E, \alpha, \chi)_{MTT} = (\alpha - p\alpha^{-1}) L_p(E, \alpha, \chi)_{MSD}.$$

Since p-adic characters of finite order are dense in $\mathcal{X}$ and the Mazur-Mellin transforms of p-adic measures are continuous functions on $\mathcal{X}$, it follows that both p-adic L-functions coincide on $\mathcal{X}$, in particular on the set of characters of the form $\chi_n(x) = x^n$. Since the polynomials are dense on $\mathcal{C}\left(\mathbb{Z}_p^*, \mathbb{Q}_p\right)$, we can uniformly approximate the characteristic function of $D\left(a, p^n\right)^+$, $\chi_{D(a,p^n)^+}$, by a sequence of polynomials (P_n), and since μ_{MSD} and μ_{MTT} are bounded, we have that

$$\mu_{MSD}\left(D\left(a, p^n\right)^+\right) \int_{\mathbb{Z}_p^*} \chi_{D(a,p^n)^+} d\mu_{MSD} = \lim_{n\to\infty} \int_{\mathbb{Z}_p^*} P_n d\mu_{MSD},$$

and since up to a non-zero scalar, for any $n \geq 0$, $\int_{\mathbb{Z}_p^*} x^n d\mu_{MSD} = \int_{\mathbb{Z}_p^*} x^n d\mu_{MTT}$, the result follows. □

Conjecture (Mazur-Swinnerton-Dyer, [47]). Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at the prime p. Then, the order of vanishing at $s = 1$ of $L_p(E, s)$ equals the rank of the group $E(\mathbb{Q})$.

3.3 Refined conjectures on the order of vanishing

3.3.1 Exceptional zeros

In this section we explain refined versions of the Mazur and Swinnerton-Dyer conjecture. In particular a p-adic analogue of the Birch and Swinnerton-Dyer conjecture is expected to happen. This calls for a definition of a p-adic analogue of the regulator of an elliptic curve. The case in which E has multiplicative reduction at p and the case in which E has good supersingular reduction at p imply that there are two admissible roots. Recently, Pollack has given a construction of a p-adic L-function for the critical slope case, which means that the root of the Hecke polynomial which is chosen is not admissible (see [57]).

The fact that a p-adic L-function can be constructed in cases of multiplicative or good supersingular reduction is responsible for the eventual emergence of extra zeros.

Definition 3.3.1 (Mazur-Tate-Teitelbaum, [49])**.** Let $f \in S_k(\Gamma_0(N))$ an eigenform for T_p, α an admissible root and χ a p-adic character of the form $\chi = \chi_j\psi$, where $\chi_j(x) = x^j$ $(0 \leq j \leq k-1)$ and ψ is a character of conductor $p^\nu M$ $(p \nmid M)$. The p-adic multiplier for χ is

$$e(p, \alpha, \chi) = \alpha^{-\nu}\left(1 - \overline{\psi}(p)p^{k-2-j}\alpha^{-1}\right)\left(1 - \psi(p)p^j\alpha^{-1}\right).$$

With this notation, the interpolation property becomes

$$L_p(f, \alpha, \chi) = e(p, \alpha, \chi)L(f_{\overline{\chi}}, j+1). \tag{3.3.1}$$

Definition 3.3.2 (Mazur-Tate-Teitelbaum, [49])**.** A pair (α, j) is said to be exceptional for p if there exists a finite order character ψ such that $e(p, \alpha, \chi_j\psi) = 0$.

Lemma 3.3.3. *Let ζ be an n-th root of unity. Then, there exists a Dirichlet character ψ modulo $p^n - 1$ such that $\psi(p) = \zeta$.*

Proof. Since the multiplicative subgroup of $(\mathbb{Z}/(p^n-1)\mathbb{Z})^*$ generated by p has order n, one has that $n \mid \phi(p^n-1)$ and there is a Dirichlet character of this multiplicative subgroup with the value ζ at p. All we have to do is to compose this Dirichlet character with the projection of $(\mathbb{Z}/(p^n-1)\mathbb{Z})^*$ onto C_n. □

Lemma 3.3.4. *The pair (α, j) is exceptional if and only if one of the two following facts hold:*

(i) $p \nmid N$, $|\alpha p^{-j}|_p = 1$ *or* $|\alpha p^{-k+2+j}|_p = 1$.

(ii) $p|N$ *and* $|a_p(f)p^{-j}|_p = 1$.

Proof. By definition of the p-adic multiplier, (α, j) is exceptional if and only if there exists a Dirichlet character ψ of conductor coprime to p satisfying one of the two following properties:

(i) $\overline{\psi}(p)p^{k-2-j}\alpha^{-1} = 1$.

(ii) $\psi(p)p^{j}\alpha^{-1} = 1$.

In the first case, $|\alpha p^{2-k+j}|_p = 1$, while in the second case, $|\alpha p^{-j}|_p = 1$. The reciprocal statement follows directly from Lemma 3.3.3. □

Lemma 3.3.5 (Li, [44])**.** *For any newform $f \in S_k(\Gamma_0(N))$, if $p||N$, then $a_p(f)^2 = p^{k-2}$.*

□

Proposition 3.3.6 (Mazur-Tate-Teitelbaum, [49])**.** *The pair (α, j) is exceptional if and only if $p\|N$ and $j = \frac{k-2}{2}$.*

Proof. First, recall that the Hecke polynomial for $\Gamma_0(N)$ is only defined if $p\|N$. Suppose that (α, j) is exceptional. First, we check that $p\|N$. Otherwise, set $H_p(f;s) = \left(1 - a_p(f)p^{-s} + p^{k-1-2s}\right)^{-1}$. It can be shown that this function is the Hasse-Weil L-function of a certain motive defined over $\mathbb{F}_p$ attached to the fibre over $\overline{\mathbb{F}}_p$ of the jacobian of the modular curve. Since $H_p(f;s) = (1-\alpha_1 p^{-s})^{-1}(1-\alpha_2 p^{-s})^{-1}$ where α_1, α_2 are the roots of the Hecke polynomial at p, the proof of the Weil conjectures given by Deligne implies that $|\alpha_1| = |\alpha_2| = p^{\frac{k-1}{2}}$. By Lemma 3.3.4, it follows that either $j = \frac{k-1}{2}$ or $j = \frac{j-3}{2}$; hence k is odd, which is a contradiction. Hence, $p\|N$ and, by Lemma 3.3.5, we have that $|a_p(f)| = p^{\frac{k-2}{2}}$, and again by Lemma 3.3.4, $j = \frac{k-2}{2}$. The reciprocal statement follows as a direct consequence of Lemma 3.3.5 and Lemma 3.3.4. □

Remark 3.3.7. Notice that the p-adic L-functions of Dirichlet characters can also have exceptional zeros. Since $L_p(\chi, k) = (1 - \chi(p)p^{k-1})L(\chi, 1-k)$, an extra zero occurs if and only if $k = 1$ and $\chi(p) = 1$. These are called the trivial zeros of $L_p(\chi, s)$. Notice that the classical Dirichlet L function does not vanish at these values.

Conjecture (Mazur, Tate, Teitelbaum [49]). Let ψ, χ be p-adic characters of finite order. Denote by $\rho_\infty(f, \chi, j)$ the order of vanishing of $L(f_\chi, s)$ at $s = j + 1$ and by $\rho_p(f, \alpha, \psi, j)$ the order of vanishing of $L_p(f, \alpha; \psi\tilde{\chi}_j\chi_s)$ at $s = j$. Then,

a) If $e(p, \alpha, \tilde{\chi}_j\psi) \neq 0$, then $\rho_p(f, \alpha, \psi, j) = \rho_\infty(f, \chi, j)$.

b) If $e(p, \alpha, \tilde{\chi}_j\psi) = 0$, then $\rho_p(f, \alpha, \psi, j) = \rho_\infty(f, \chi, j) + 1$.

In particular, this conjecture states that if there are two admissible roots, the orders of vanishing of the corresponding p-adic L-functions are the same. There is an easy case in which this fact can be proved.

Proposition 3.3.8. *Let $f \in S_k(\Gamma_0(N))$ be a newform which is ordinary at the prime p. Let ψ be a Dirichlet character and let $K_{f,p}(\psi)$ denote the finite extension of $\mathbb{Q}_p$ obtained by adjoining to $\mathbb{Q}_p$ the Fourier coefficients of f and the values taken by ψ. If α_1, α_2 are admissible and $\alpha_1 \notin K_{f,p}(\psi)$, then, $\rho_p(f, \alpha_1, \psi, j) = \rho_p(f, \alpha_2, \psi, j)$.*

Proof. Let $\sigma : K_{f,p}(\psi)(\alpha_1) \to K_{f,p}(\psi)(\alpha_2)$ be the non-trivial $K_{f,p}(\psi)$-morphism given by $\sigma(a + b\alpha_1) = a + b\alpha_2$ for $a, b \in K_{f,p}(\psi)$, which is clearly a bijection. Denote by μ_{p,α_1} and μ_{p,α_2} the measures obtained by the modular symbol attached to f and the roots α_1 and α_2 respectively, and let $L_p(f, \alpha_1, s)$ and $L_p(f, \alpha_2, s)$ denote the corresponding p-adic L-functions. Since f is ordinary at p, it is easy to check that for any $K_{p,f}(\psi)(\alpha_1)$-valued locally analytic function (indeed, for any $K_{p,f}(\psi)(\alpha_1)$-valued continuous function) F, $\sigma\left(\int_{\mathbb{Z}_p^*} F d\mu_{\alpha_1}\right) = \int_{\mathbb{Z}_p^*} F d\mu_{\alpha_2}$. Hence, let us consider the power series expansions $L_p(f, \alpha_m, \psi\chi_s) = \sum_{n=0}^{\infty} \frac{a_n^{(m)}}{n!} s^n$, where $a_n^{(m)} = a_{n,1}^{(m)} + \alpha_m a_{n,2}^{(m)}$, with $a_{n,m}^{(m)} \in K_{f,p}(\psi)$ for $m = 1, 2$. Assume for simplicity that $\psi = 1$. If $\rho_p(f, \alpha_1, 1, j) = r$ then, $a_{n,m}^{(1)} = 0$ for $0 \leq n \leq r-1$ and $m = 1, 2$ and $a_r^{(1)} \neq 0$. By application of σ the result follows. □

Conjecture (Mazur, Tate, Teitelbaum [49]). Let $E/\mathbb{Q}$ be an elliptic curve, p a prime and α an admissible root of the Hecke polynomial for E at p.

a) If $\alpha \neq 1$, then, $\text{ord}_{s=1} L_p(E,s) = \text{rk}\,(E(\mathbb{Q}))$.

b) If $\alpha = 1$, then, $\text{ord}_{s=1} L_p(E,s) = \text{rk}\,(E(\mathbb{Q})) + 1$.

Remark 3.3.9. Let N be the conductor of E and $f_E \in S_2(\Gamma_0(N))$ the corresponding newform. The p-adic multiplier for p, α and the trivial character is $(1-\alpha^{-1})^2$, which vanishes if and only if $\alpha = 1$, which is equivalent to the fact that $a_p(E) = -p-1$, or equivalently, E has split multiplicative reduction at p. The case when $\alpha = 1$ corresponds to the case when E has good ordinary or non-split multiplicative reduction at p (for details see [70]).

If the p-adic multiplier vanishes, the p-adic L-function vanishes at the central points and we lose the interpolation property. Hence, it is natural to ask whether the derivative of the p-adic L-function still carries information about the values of the complex L-function at the central points. This is the purpose of the following

Definition 3.3.10 (Mazur-Tate-Teitelbaum, [49])**.** Let $f \in S_k(\Gamma_0(N))$, $j \in \{0,...,k-2\}$ and α an admissible root such that (α, j) is exceptional. It is said that (α, j) is exceptional of local type if there exists a quantity $\mathcal{L}_p(f,\alpha,j)$ such that for any Dirichlet character of conductor p^m,

$$L_p'(f,\chi,j) = \mathcal{L}_p(f,\alpha,j) \sum_{a=0}^{p^m-1} \psi(a)\lambda\left(f, j, \frac{a}{p^n}\right).$$

Conjecture (Mazur-Tate-Teitelbaum [49]). For $k=2$, if the pair $(\alpha, 0)$ is exceptional, then, it is exceptional of local type.

3.3.2 The extended Mordell-Weil group

To formulate a suitable p-adic version of the refined Birch and Swinnerton-Dyer conjecture involving the leading term of the Taylor coefficient, a necessary condition is to define a p-adic analogue of the regulator of $E(\mathbb{Q})$. Such a definition was first given in [49]. We explain here how to do this.

Let K be a number field, and E/K and elliptic curve and $p \in \mathbb{Z}$ a prime. A place ν over p is said to be of type 1 if E is split multiplicative at ν. Otherwise, ν is said to be of type 2. Denote $K_p = K \otimes \mathbb{Q}_p$. Then, $K_p = \prod_{\nu|p} K_\nu$. Define $E(K_p) = \prod_{\nu|p} E(K_\nu)$. Set $E^+(K_p) = \prod_{\nu_1|p} K_{\nu_1}^* \times \prod_{\nu_2|p} E(K_{\nu_2})$ where ν_1 runs over

the places over p of type 1 and ν_2 runs over the places of type 2. For any ν of type 1, fix a Tate uniformization $i_\nu : K_\nu^* \to E(K_\nu)$. If $q = e^{2\pi i z}$, let $j(q) = \sum_{n \geq -1} a_n q^n$ the series expansion of the j-function which can be formally reversed so that $q(j) = \sum_{n \geq 1} b_n j^{-n}$. One can show that $b_n \in \mathbb{Z}$ for any $n \geq 1$. Suppose that $j(E)$ is non integral, i.e., $|j(E)|_\nu > 1$. Then, $q(j(E))$ is defined. Denote $q_\nu = q(j(E)) \in K_\nu^*$, the multiplicative period of E. Let N be the cardinality of the set of places of type 1 and M the cardinality of the set of places of type 2. We have an exact sequence

$$0 \to \mathbb{Z}^N \xrightarrow{\phi} E^+(K_p) \xrightarrow{\psi} E(K_p) \to 0,$$

where ϕ is defined as follows: if ν is of type 1 and e_ν is the vector of $\mathbb{Z}^N$ having coordinate 1 at position ν and 0 at the rest, $\phi(e_\nu) \in E^+(K_p)$ has coordinate q_ν at position ν, 0 at the rest of positions of places of type 1 and $O \in E(K_\nu)$ at the positions given by places of type 2. The map ψ is given by the following rule: if ν_j $(1 \leq j \leq N)$ are the places of type 1 and ν_{N+l}, $(1 \leq l \leq M)$ the places of type 2, for any $z_{\nu_j} \in K_{\nu_j}^*$ and $P_{\nu_{N+l}} \in E\left(K_{\nu_{N+l}}\right)$, set

$$\psi\left(z_{\nu_1}, ..., z_{\nu_N}, P_{\nu_{N+1}}, ...P_{\nu_{N+M}}\right) = \left(i_{\nu_1}(z_{\nu_1}), ..., i_{\nu_N}(z_{\nu_N}), P_{\nu_{N+1}}, ...P_{\nu_{N+M}}\right).$$

Since $E(K)$ sits diagonally as a subgroup of $E(K_p)$, it is possible to define $E^+(K) = \psi^{-1}(E(K))$. This subgroup is called the extended Mordell-Weil group. Clearly, there is an induced exact sequence

$$0 \to \mathbb{Z}^N \xrightarrow{\phi} E^+(K) \xrightarrow{\psi} E(K) \to 0,$$

hence, the extended Mordell-Weil group has rank $\mathrm{rk}(E(K)) + N$. In particular, for a curve $E/\mathbb{Q}$, if E has good ordinary reduction at p, the extended Mordell-Weil group coincides with the Mordell-Weil group, whereas if E has split multiplicative reduction, the extended Mordell-Weil group has rank $\mathrm{rk}(E(\mathbb{Q})) + 1$. Until the end of this chapter we will suppose that E is defined over $\mathbb{Q}$.

3.3.3 σ-functions

To give a full p-adic analogue of the Birch and Swinnerton-Dyer conjecture, one has to define a p-adic version of the canonical height pairing. The earliest

definition of this pairing given by Néron ([51]) uses the Weierstrass σ function. Given an elliptic curve $E/\mathbb{Q}$, and a number field K, for any place ν of K, Néron begins by defining a local canonical height $\lambda_\nu : E(K_\nu) \to \mathbb{R}$. The global height is defined as

$$\hat{h}(P) = \sum_\nu n_\nu \lambda_\nu(P), \quad n_\nu \in \mathbb{Z}.$$

Let Λ_E be the lattice attached to E by the Weierstrass uniformization. Denote by $\Delta(\Lambda)$ the corresponding discriminant and let η, σ denote the Weierstrass functions attached to Λ. For an archimedean place ν, the local height is

$$\lambda_\nu(P) = -\log|\Delta(\Lambda)^{1/12} e^{-z\eta(z)/2}\sigma(z,\Lambda)|_\nu.$$

In [48], a p-adic analogue of the σ-function is constructed, which is used in [49] to define the canonical height pairing. This function is defined on E^f, the formal group of E (supposing that E is a canonical model defined over the ring of integers of a finite extension of $\mathbb{Q}_p$). We suppose that $E/\mathbb{Z}_p$ is the Néron model of E over $\mathbb{Z}_p$ and $E/^f\mathbb{Z}_p$ its formal completion. Suppose that E has good ordinary reduction or multiplicative reduction at p. Let ω be a fixed invariant differential attached to E.

Proposition 3.3.11 (Mazur-Tate, [48])**.** *There exists a unique holomorphic odd function σ_ω on $E/\mathbb{Z}_p^f$ such that*

$$\left.\frac{d\sigma_\omega}{\omega}\right|_{P=0} = 1.$$

3.3.4 The p-adic sparsity and the p-adic regulator

Let p be a prime such that E has good ordinary or multiplicative reduction at p and define $E_p(\mathbb{Q})$ as the set of points of $E(\mathbb{Q})$ which specialize to the connected component of $0 \in E(\mathbb{R})$ and which specialize to 0 at p. A simple geometric argument together with the fact that reduction mod p is a group homomorphism show that $E_p(\mathbb{Q})$ is a subgroup.

Denote by $\mathbb{A}_\mathbb{Q}^*$ the group of ideles of $\mathbb{Q}$. Define $U_q = \mathbb{Z}_q^*$ for any prime q and $U_\infty = \mathbb{R}$. For any prime q, consider a local parameter t_q of the formal completion $E^f/\mathbb{Z}_q$ (see [70]) and let c_q be defined by

$$\left.\frac{dt_q}{\omega}\right|_{P=0} = c_q.$$

Set $\omega_q = c_q\omega$. For any $P \in E_p(\mathbb{Q})$, define an idele $i(P)$ by setting:

(i) $i(P)_\infty = 1$.

(ii) If $q \neq p$ is a prime and P does not specialize to zero, $i(P)_q = c_q^{-2}$.

(iii) If $q \neq p$ is a prime and P specializes to zero, $i(P)_q = c_q^{-2}t_q^2(P)$.

(iv) $i(P)_p = c_p^{-2}\sigma_\omega^2(P)$.

Proposition 3.3.12 ([48])**.** *There exists a bilinear symmetric pairing*

$$\langle\ \rangle : E_p(\mathbb{Q}) \times E_p(\mathbb{Q}) \to \mathbb{Q}^* \setminus \mathbb{A}_{\mathbb{Q}}^*/\prod_{q\neq p} U_q$$

such that

$$\langle P, P\rangle = i(P),$$

for any $P \in E_p(\mathbb{Q}) \setminus \{0\}$.

□

Let $\lambda : \mathbb{Q}^* \setminus \mathbb{A}_{\mathbb{Q}}^*/\prod_{q\neq p} U_q \to \mathbb{Q}_p$ be a continuous group homomorphism. We can extend $\lambda \circ \langle\ \rangle$ to $(E(\mathbb{Q}) \otimes \mathbb{Q}_p) \times (E(\mathbb{Q}) \otimes \mathbb{Q}_p)$. We have the following result.

Proposition 3.3.13. *There exists a unique symmetric bilinear pairing*

$$\langle\ \rangle_\lambda : (E(\mathbb{Q}) \otimes \mathbb{Q}_p) \times (E(\mathbb{Q}) \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$$

such that

$$\langle P, P\rangle_\lambda = \lambda\left(i(P)\right).$$

Proof. Define $\langle\ \rangle_\lambda$ to be zero out of the connected component of zero. If P or Q do not specialize to 0, but they are in the connected component of zero, define $\langle P, Q\rangle_\lambda = p^{-(n+m)}\langle p^nP, p^mQ\rangle_\lambda$, with p^nP, p^mQ specializing to zero. By bilinearity, it is independent of n and m. The quadratic form $\langle P, P\rangle_\lambda = i(P)$ characterizes the pairing. □

The pairing $\langle\ \rangle_\lambda$ is called the p-adic analytic height. Denote by π_p the projection of $\mathbb{Q}^* \setminus \mathbb{A}_{\mathbb{Q}}^*/\prod_{q\neq p} U_q$ onto $\mathbb{Q}_p$. The p-adic analytic height for $\lambda = \mathrm{Log}_p \circ \pi_p$ will be denoted by $\langle\ \rangle_p$. It remains to lift the pairing to the product

of the extended Mordell-Weil group in the split multiplicative case. To do this, we construct a map

$$\begin{array}{ccc} E_p(\mathbb{Q}) & \to & E^+(\mathbb{Q}) \\ P & \mapsto & \tilde{P} = (w_p(P), P)\,, \end{array}$$

where $i_p(w_p(P)) = P$.

Proposition 3.3.14. *There is a unique bilinear symmetric pairing*

$$\langle\ \rangle_p^+ : \left(E^+(\mathbb{Q}) \otimes \mathbb{Q}_p\right) \times \left(E^+(\mathbb{Q}) \otimes \mathbb{Q}_p\right) \to \mathbb{Q}_p$$

such that $\langle \tilde{P}, \tilde{Q} \rangle_p^+ = \langle P, Q \rangle_p$ *for* $P, Q \in E_p(\mathbb{Q})$ *and, if* E *has split-multiplicative reduction at* p*, then, for any* $a, b \in \mathbb{Q}_p^*$*,*

(i) $\langle a, P \rangle_p^+ = \mathrm{Log}_p\left(\pi_p(w_p(P))/v_p(q_p)\right)$.

(ii) $\langle a, b \rangle_p^+ = \mathrm{Log}_p\left(\pi_p(q_p)/v_p(q_p)\right)$.

Set $\epsilon = 0, 1$ depending on whether E has good ordinary or split multiplicative reduction at p. Let $\{P_1, ..., P_{rk(E)+\epsilon}\}$ be a basis of $E^+(\mathbb{Q})$, and call M the index of the subgroup that it generates.

Definition 3.3.15. Denote by $E(\mathbb{Q})_{\mathrm{tors}}$ the torsion group of $E(\mathbb{Q})$. If E has good ordinary or split multiplicative reduction at p, the p-adic sparsity of E is

$$\mathcal{S}_p(E) = \det\left(\langle P_i, P_j \rangle_p^+\right) / |E(\mathbb{Q})_{\mathrm{tors}}|^2 \in \mathbb{Q}_p.$$

If E has good reduction at p, the p-adic regulator of E is

$$R_p(E) = \det\left(\langle P_i, P_j \rangle_p^+\right) \in \mathbb{Q}_p.$$

Conjecture (Refined p-adic analogue of Birch and Swinnerton-Dyer, [49]). Let $E/\mathbb{Q}$ be an elliptic curve. Let ω_E be the invariant differential associated to E and $\Omega_E^+ = \int_{E(\mathbb{R})} \omega_E$, which is one of the periods of the corresponding $\mathbb{Z}$-lattice. Let r be the Mordell-Weil rank of $E/\mathbb{Q}$. Let m_l denote the l-th Tamagawa number and $G(E)$ the Tate-Schafarefich group for E. Then, if $\alpha \neq 1$, one has

(i) $L_p^{(j)}(E, 1) = 0$ for $0 \leq j \leq r - 1$.

(ii) $L_p^{(r)}(E, 1) = n!\left(1 - \frac{1}{\alpha}\right)^b |G(E)| \mathcal{S}_p(E) \prod_l m_l \Omega_E^+$, where $b = 2$ if E has good reduction at p and 1 if E has non-split multiplicative reduction.

If $\alpha = 1$, then,

(i) $L_p^{(j)}(E,1) = 0$ for $0 \leq j \leq r$.

(ii) $L_p^{(r+1)}(E,1) = (n+1)!|G(E)|\mathcal{S}_p(E)\prod_l m_l \Omega_E^+$.

Remark 3.3.16. We have to understand these equalities after having identified Ω_E^+ with the corresponding element of the basis of the vector space over where the p-adic L-function takes values.

We finish this section by stating the exceptional zero conjecture. Before formulating it, we need some ingredients:

Recall that the modular elliptic function j has an expansion in $q = e^{2\pi iz}$:

$$j = q^{-1}\sum_{n=0}^{\infty} a_n q^n,$$

with $a_n \in \mathbb{Z}$ for any $n \geq 0$. One can formally write

$$q = \sum_{n=1}^{\infty} b_n j^{-n}, \quad b_n \in \mathbb{Z}.$$

Let $j(E)$ be the j-invariant of E. Assume that $|j(E)|_p > 1$. The multiplicative period of E is

$$q(E) = \sum_{n=1}^{\infty} b_n j(E)^{-n} \in \mathbb{Z}_p.$$

Let K be a finite extension of $\mathbb{Q}_p$. Set $\lambda_p = \mathrm{Log}_p \circ N_{K/\mathbb{Q}_p}$. Define

$$\mathcal{L}_p(E) = \frac{\lambda_p(q(E))}{\mathrm{ord}_p(q(E))} \in \mathbb{Q}_p.$$

Conjecture (Mazur-Tate-Teitelbaum, [49]). If $j(E) \in \overline{\mathbb{Q}}$ and $|j(E)|_p > 1$, then $\mathcal{L}_p(E) \neq 0$.

Let ψ be a Dirichlet character of conductor p^m. Denote

$$\Lambda_E(\psi) = \sum_{a=1}^{p^m-1} \psi(a)\lambda(f, \frac{a}{p^m}).$$

Numerical evidence led Mazur, Tate and Teitelbaum to formulate the following

Conjecture (Exceptional zero conjecture, [49]). If E has split multiplicative reduction at p, then

$$L_p'(E, \psi, 1) = \mathcal{L}_p(E)\Lambda_E(\psi).$$

This conjecture was proved by Greenberg and Stevens ([30]) (for $p \geq 5$) using a two variable p-adic L-function (the Mazur-Kitagawa p-adic L-function), and the theory of Hida families.

Chapter 4

Rigid analytic p-adic L-functions

Introduction

Quoting Klingenberg (see [38]), Schneider had the brilliant idea of substituting complex uniformization by p-adic rigid analytic uniformization and suggested the following program for the proof of the exceptional zero conjecture:

i) Define a purely p-adic L-function,

ii) prove the exceptional zero conjecture for this function, and

iii) compare this L-function with the original one

Notice that in the exceptional zero conjecture, the term $\mathcal{L}_p(E)$ arises from the Tate p-adic uniformization $\mathbb{Q}_p^*/q_E^{\mathbb{Z}} \simeq E(\mathbb{Q}_p)$, but $\Lambda_E(1)$ comes from the Wiles modular parametrization. Schneider associated to E a p-adic measure, independent of the modular uniformization, by means of the Cerednik-Drinfeld uniformization and defined an alternative p-adic L-function, $L_p^{rig}(E,s)$, as the Mazur-Mellin transform of this measure. Later on, Klingenberg proved in [38] the exceptional zero conjecture (under mild conditions) for $L_p^{rig}(E,s)$. No relation between $L_p(E,s)$ and $L_p^{rig}(E,s)$ has been worked out for the time being. However, Schneider's construction has served as the inspiration for later constructions of p-adic L-functions which are related to heights of local points on elliptic curves and which satisfy certain analogues of the Birch and

Swinnerton-Dyer conjecture: the anticyclotomic p-adic L-functions. Partly inspired by these p-adic L-functions we have recently constructed the quadratic p-adic L-functions. In this chapter we explain the construction of Schneider and the anticyclotomic p-adic L-functions. In the next chapter we introduce our construction of quadratic p-adic L-functions.

4.1 The rigid analytic structure of $\mathrm{PGL}(2,\mathbb{Q}_p)$

As pointed out in the Prolegomena, the group $\mathrm{PGL}(2,\mathbb{Q}_p)$ acts on the Drinfeld upper half-plane $\mathcal{H}_p$ by Möbius transformations. For the purposes of the present chapter, it is convenient to enlarge the set of affinoids. For any $t \in \{0,...,p-1\}$, define $W_t = \{\tau \in \mathcal{H}_p |\ p^{-1} < |\tau - t|_p < 1\}$ and $W_\infty = \{\tau \in \mathcal{H}_p |\ 1 < |\tau|_p < p\}$ and set $W = \cup_{t=0}^{p-1} W_t$. Denote by A the standard affinoid as defined in the Prolegomena, and let us call the set $A \cup W \cup W_\infty$ the thickened standard affinoid. The translates of the affinoids by $\mathrm{PGL}(2,\mathbb{Q}_p)$ have a natural order relation by containment which is translated into an order relation of homothety classes of $\mathbb{Z}_p$-lattices.

Definition 4.1.1. The Bruhat-Tits tree of $\mathrm{PGL}(2,\mathbb{Q}_p)$ is the homogeneous tree of degree $p+1$ whose vertices are homothety classes of rank 2 $\mathbb{Z}_p$-lattices contained in $\mathbb{Q}_p^2$; two vertices are joined by an edge if the homothety classes have representatives Λ_1 and Λ_2 such that $p\Lambda_2 \subset \Lambda_1 \subset \Lambda_2$, the inclusion being proper. The Bruhat-Tits tree is denoted by $\mathcal{T}_p$.

Denote by $\mathcal{V}(\mathcal{T}_p)$ and by $\mathcal{E}(\mathcal{T}_p)$, respectively, the set of vertices and edges of $\mathcal{T}_p$. Given an edge $e \in \mathcal{E}(\mathcal{T}_p)$, denote by $S(e)$ and $T(e)$ respectively the source and target of e, i.e., the vertices such that e corresponds to the inclusion $S(e) \subseteq T(e)$ (at the level of representatives). Denote by $\overline{e}$ the edge such that $S(\overline{e}) = T(e)$ and $T(\overline{e}) = S(e)$. As in the case of rank two $\mathbb{Z}$-lattices, the following lemma is easy to prove.

Lemma 4.1.2. *The $\mathbb{Z}_p$-lattices $\mathbb{Z}_p + \tau_1\mathbb{Z}_p$ and $\mathbb{Z}_p + \tau_2\mathbb{Z}_p$ are homothetic if and only if there exists a matrix $\gamma \in \mathrm{PSL}(2,\mathbb{Z}_p)$ such that $\gamma(\tau_1) = \tau_2$.*

□

Since any $\mathbb{Z}_p$-lattice Λ is homothetic to some lattice of the form $\mathbb{Z}_p + \tau\mathbb{Z}_p$, the assignment $\mathbb{Z}_p + \omega\mathbb{Z}_p \mapsto \mathbb{Z}_p + \gamma(\omega)\mathbb{Z}_p$ defines a left action of $\mathrm{PGL}(2,\mathbb{Q}_p)$ on $\mathcal{V}(\mathcal{T}_p)$, and hence on $\mathcal{E}(\mathcal{T}_p)$.

Denote by v^0 the homothety class of the lattice $\mathbb{Z}_p^2$. The edges having v_0 as an endpoint correspond to index p sublattices of $\mathbb{Z}_p^2$, and hence, they are in canonical bijection with $\mathbb{P}^1(\mathbb{F}_p)$. Label them by $\{e_0, e_1, ..., e_{p-1}, e_\infty\}$.

Proposition 4.1.3 (cf. [25])**.** *There is a unique map* $r : \mathcal{H}_p \to \mathcal{E}(\mathcal{T}_p) \cup \mathcal{V}(\mathcal{T}_p)$ *such that*

(i) $r(\tau) = v_0$ *if and only if* $\tau \in A$.

(ii) $r(\tau) = e_t$ *if and only if* $\tau \in W_t$.

(iii) r *is* $\mathrm{PGL}(2,\mathbb{Q}_p)$*-equivariant.*

Proof. First, by Lemma 4.1.2, notice that $\mathrm{PGL}(2,\mathbb{Z}_p)$ is the stabilizer of v_0 in $\mathrm{PGL}(2,\mathbb{Q}_p)$; hence we have a bijection

$$\begin{array}{rcl} \eta_1 : \mathrm{PGL}(2,\mathbb{Q}_p)/\mathrm{PSL}(2,\mathbb{Z}_p) & \to & \mathcal{V}(\mathcal{T}_p) \\ \gamma\mathrm{PSL}(2,\mathbb{Z}_p) & \mapsto & \gamma(v_0). \end{array}$$

For any $v \in \mathcal{V}(\mathcal{T}_p)$, choose a representative $\gamma \in \mathrm{PGL}(2,\mathbb{Q}_p)$ such that $\eta_1(\gamma) = v$ and define

$$F(v) = \left\{ z \in \mathbb{P}^1(\mathbb{C}_p) : \mathrm{red}\left(\gamma^{-1}(z)\right) \in \overline{\mathbb{F}}_p \setminus \mathbb{F}_p \right\}.$$

Now, if we denote by G the stabilizer of e_∞ in $\mathrm{PGL}(2,\mathbb{Q}_p)$, we have a bijection

$$\begin{array}{rcl} \eta_2 : \mathrm{PGL}(2,\mathbb{Q}_p)/G & \to & \mathcal{E}(\mathcal{T}_p) \\ b\mathrm{Stab}(e_\infty) & \mapsto & b(e_\infty). \end{array}$$

Given $e \in \mathcal{E}(\mathcal{T}_p)$, let γ be an element in $\mathrm{PGL}(2,\mathbb{Q}_p)$ such that $\eta_1(\gamma) = e$. Define the open annulus

$$W(e) = \left\{ z \in \mathbb{P}^1(\mathbb{C}_p) : \gamma^{-1}(z) \in W \right\}.$$

It is easy to see that the family of the compact open sets $W(e)$ and $F(v)$ covers $\mathcal{H}_p$ as e runs through $\mathcal{E}(\mathcal{T}_p)$ and v runs through $\mathcal{V}(\mathcal{T}_p)$. Hence, for $\tau \in W(e)$, define $r(\tau) := e$ and for $\tau \in F(v)$, define $r(\tau) := v$. To check equivariance, notice that for any $\gamma \in \mathrm{PGL}(2,\mathbb{Q}_p)$, we have that $\tau \in F(v)$ if and only if $\gamma(\tau) \in F(\gamma v)$. A $\mathrm{PGL}(2,\mathbb{Q}_p)$-equivariant map which brings W_t to e_t and $F(v_0)$ to v_0 necessarily behaves like r in the rest of affinoids, since they are $\mathrm{PGL}(2,\mathbb{Q}_p)$-translates of these basic ones. □

4.2 The Schneider distribution

Let $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Q}_p)$ be a discrete subgroup. As in the case of discrete subgroups of $\mathrm{SL}(2,\mathbb{R})$, for any function $f : \mathcal{H}_p \to \mathbb{C}_p$, any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and any non-negative integer k, recall the notation $f|_k\gamma(z) = (cz+d)^{-k} f(\gamma(z))$.

Definition 4.2.1. A rigid analytic modular form of weight 2 for Γ is a rigid analytic function $f : \mathcal{H}_p \to \mathbb{C}_p$ such that $f|_2\gamma = f$ for any $\gamma \in \Gamma$. The $\mathbb{C}_p$-vector space of rigid analytic modular forms for Γ is denoted by $S_2^{rig}(\Gamma)$.

Definition 4.2.2. Let M be a $\mathbb{Z}$-module endowed with the trivial action of Γ. An M-valued harmonic cocycle on $\mathcal{T}_p$ is a function $c : \mathcal{E}(\mathcal{T}_p) \to M$ such that

i) For any $e \in \mathcal{E}(\mathcal{T}_p)$, $c(\overline{e}) = -c(e)$.

ii) For any $v \in \mathcal{V}(\mathcal{T}_p)$, $\displaystyle\sum_{S(e)=v} c(e) = 0$.

If $M = \mathbb{C}_p$, c is said to be a weight 2 harmonic cocycle.

It can be proved that the quotient map $\phi_p : \mathcal{H}_p \to \Gamma\backslash\mathcal{H}_p$ induces an isomorphism between $S_2^{rig}(\Gamma)$ and $\Omega_{\Gamma\backslash\mathcal{H}_p}$ (see [64]). For any $e \in \mathcal{E}(\mathcal{T}_p)$ and $f \in S_2^{rig}(\Gamma)$, consider the annulus $W(e)$. The restriction of f to $W(e)$ gives rise to a meromorphic differential $\omega_f \in \Omega_{\Gamma\backslash W(e)}$. Denote by $\mathrm{Res}_e(f)$ the residue of ω_f on $W(e)$. The p-adic version of the residue theorem allows us to prove the following statement.

Proposition 4.2.3 (Schneider, [64])**.** *For any $f \in S_2^{rig}(\Gamma)$, the assignment $c_f(e) = \mathrm{Res}_e(f)$ is a weight 2 harmonic cocycle.*

Since for any $f \in S_2^{rig}(\Gamma)$, and for any $\gamma \in \Gamma$, $f(\gamma(z))d(\gamma(z)) = f(z)dz$, it follows that the harmonic cocycle c_f is Γ-invariant. The harmonic cocycle c_f can be used to define a p-adic distribution on the set of edges of $\mathcal{T}_p$. First, we explain how to give a topology to $\mathcal{T}_p$: for any edge $e \in \mathcal{E}(\mathcal{T}_p)$, denote by $\mathcal{T}_p(e)$ the largest connected subtree of $\mathcal{T}_p$ containing e and no other edge having $S(e)$ as an endpoint. Set $\Sigma_e = r^{-1}(\mathcal{T}_p(e))$. Denote by $\overline{\Sigma}_e$ the closure of Σ_e in $\mathbb{P}^1(\mathbb{C}_p)$ and define $U_e := \overline{\Sigma}_e \cap \mathbb{P}^1(\mathbb{Q}_p)$.

Proposition 4.2.4. *The assignment $e \mapsto U_e$ is a bijection from $\mathcal{E}(\mathcal{T}_p)$ to the set of compact open discs of $\mathbb{P}^1(\mathbb{Q}_p)$*

Proof. Given $e \in \mathcal{E}(\mathcal{T}_p)$, from the very definition of r, Σ_e is a union of affinoids contained one in each other. Apart from $p+1$ limit points, this union fills the affinoid $r^{-1}(e)$ by adding a sequence of sub-affinoids contained in the excised discs of $\mathcal{T}_p(e)$, so that by adding these limit points, i.e., by taking the closure, we see that $\overline{\Sigma}_e$ is the smallest disc of $\mathbb{P}^1(\mathbb{C}_p)$ which contains $r^{-1}(e)$. Since $r^{-1}(e_1)$ and $r^{-1}(e_2)$ are disjoint for different edges e_1 and e_2, the assignment is injective. Finally, given a compact open disc $U \in \mathbb{P}^1(\mathbb{Q}_p)$, consider the corresponding disc $W \in \mathbb{P}^1(\mathbb{C}_p)$ such that $W \cap \mathbb{P}^1(\mathbb{Q}_p) = U$ and the biggest affinoid $W(e)$ contained in W. This affinoid determines an edge e such that $r^{-1}(e) = W(e)$. □

Finally, the fact that the quotient graph $\Gamma\backslash\mathcal{T}_p$ is finite allows us to control the growth of $\mu_f(U(e))$, and to establish that the Schneider distribution is tempered in the sense that it is possible to integrate locally analytic $\mathbb{C}_p$-valued functions on $\mathbb{P}^1(\mathbb{Q}_p)$ against μ_f (for details see [25] and [64]).

4.3 The Schneider p-adic L-function

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let $\phi \in S_2^{new}(\Gamma_0(N))$ be the newform provided by the Wiles modular parametrization. In particular, E is a Weil curve, which means that there exists a complex uniformization $\Phi : X_0(N)(\mathbb{C}) \to E(\mathbb{C})$, defined over $\mathbb{Q}$. Assume that N is square free with an even number of prime divisors.

As an alternative to the Mazur-Tate-Teitelbaum p-adic L-function, which is defined through the modular integrals, it is possible to attach a rigid analytic modular form to ϕ, $f_\phi \in S_2^{rig}(\Gamma)$ for certain $\Gamma \in \mathrm{SL}(2, \mathbb{Z}_p)$, and to consider the Mazur-Mellin transform of the p-adic distribution attached to the weight 2 harmonic cocycle defined above for f_ϕ. This yields a construction of a p-adic L-function for E, using directly the theory of p-adic uniformizations due to Mumford, Cerednik and Drinfeld. The rigid analytic modular form f_ϕ arises from three basic ingredients: the Cerednik-Drinfeld uniformization, the Wiles modular parametrization and the Jacquet Langlands correspondence.

The method considers complex and p-adic uniformizations of E obtained from a Shimura curve attached to N and p, which provides a supply of new algebraic points on E which do not come from the Wiles uniformization evaluated on classical Heegner points on the modular curve. This way, the theory of p-adic uniformization is related with the construction of algebraic

points on E. This link provides a bridge between the Schneider construction and the problem of finding algebraic points on E, a bridge that is examined, for instance, in [25] and [14].

4.3.1 p-adic and complex uniformizations

Let N be the conductor of E. Let $\phi \in S_2(\Gamma_0(N))$ be, as above, its corresponding newform given by Wiles modular uniformization. A factorization of the form $N = N^+D$ is said to be admissible if $(N^+, D) = 1$ and if D is square-free and has an even number of prime factors. Let H be the indefinite quaternion $\mathbb{Q}$-algebra of discriminant D. Let R_0 be a maximal order of H, which is unique up to conjugation, as we saw in the Prolegomena. Since $H \otimes \mathbb{R} \simeq M(2, \mathbb{R})$, we can choose an identification $\eta : R_0 \otimes (\mathbb{Z}/N^+\mathbb{Z}) \to M_2(2, \mathbb{Z}/N^+\mathbb{Z})$. The sub-ring $R = \{x \in R_0 | \, \eta(x) \text{ is upper-triangular}\}$ is an Eichler order of level N^+. To see this, it suffices to check this statement locally. But in fact, for any $p|N$, we have that $R \otimes \mathbb{Z}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. Fix an embedding $\psi : R^* \to \mathrm{GL}(\mathbb{R})$ and define $\Gamma(D, N^+) = \psi(R^1)$, where R^1 is the group of units of reduced norm 1 in R. As a first step, we will use the following version of the Jacquet-Langlands correspondence:

Theorem 4.3.1 (Jacquet-Langlands, [35])**.** *Let ϕ be a newform for $\Gamma_0(N)$. Let $N = N^+D$ an admissible factorization. Then, there exists an automorphic form $g \in S_2(\Gamma(D, N^+))$ such that $L(\phi, s) = L(g, s)$, up to finitely many Euler factors.*

Given an algebraic or an analytic variety X, denote by $\mathrm{Jac}(X)$ its Jacobian, i.e., its group of classes of divisors of degree 0, which has structure of algebraic or analytic variety respectively. Set $\Phi^0_{D,N^+} : \mathrm{Jac}(\mathcal{H}) \to \mathbb{C}$ defined by $\Phi^0_{D,N^+}(C) = \int_x^y g(z)dz$, if $C = (y) - (x)$, and extended by linearity. By projection, this map induces an analytic morphism

$$\Phi^0_{D,N^+} : \mathrm{Jac}(\Gamma(D, N^+)\backslash\mathcal{H}) \to \mathbb{C}/\Lambda_g \ ,$$

where Λ_g is the lattice of periods of g. Denote by E_g the elliptic curve defined over $\mathbb{Q}$ isomorphic to the complex elliptic curve uniformized by $\mathbb{C}/\Lambda_g$ via the Weierstrass functions $\wp_{\Lambda_g}$ and $\wp'_{\Lambda_g}$. Since, up to finitely many Euler factors,

$$L(E_g, s) = L(g, s) = L(\phi, s) = L(E, s),$$

by Falting's Theorem, there exists an isogeny $\alpha : E_g \to E$ defined over $\mathbb{Q}$. Putting altogether all the ingredients, we obtain a complex uniformization

$$\alpha \circ \Phi^0_{D,N^+} : \mathrm{Jac}\left(\Gamma(D,N^+)\backslash\mathcal{H}\right) \to E.$$

It can be proved that this map is defined over $\mathbb{Q}$ and, hence, it takes algebraic points into algebraic points.

Recall that in the case of the modular uniformization of E by $X_0(N)$, a Heegner point is a quadratic imaginary point τ which satisfies an equation of the form $NA\tau^2 + B\tau + C = 0$ with $A, B, C \in \mathbb{Z}$. This point corresponds, by the coarse moduli interpretation of $X_0(N)$, to an elliptic curve with complex multiplication by an order associated to τ in a precise way and with an N-torsion point.

The notion of Heegner points still works in the cocompact Shimura curve setting. Recall that $\Gamma(D,N^+)$ is the image under ψ of the subgroup of elements of reduced norm 1 of the Eichler order $R \simeq \mathcal{O}(D,N^+)$ up to conjugation. Hence, the coarse moduli interpretation of $X(D,N^+)$ (see [63]) implies that this Shimura curve parametrizes abelian surfaces with quaternionic multiplication together with an N^+-torsion subgroup.

Given a quadratic imaginary point $\tau \in \mathcal{H}$, consider the order $\mathcal{O}_\tau \subseteq \mathcal{O}(D,N^+)$ which stabilizes τ. A quadratic imaginary point $\tau \in \mathcal{H}$ is called a CM point if $\mathcal{O}_\tau$ is isomorphic to an order in a quadratic imaginary field. In this case, it can be proved that the corresponding abelian surface parametrized by τ has complex multiplication by this quadratic order isomorphic to $\mathcal{O}_\tau$.

Given an order $\mathcal{O}$ in a quadratic imaginary field K, denote $CM(\mathcal{O}) = \{\tau \in \mathcal{H} |\ \mathcal{O}_\tau = \mathcal{O}\}$. It can be proved (cf. [25]) that for any $\tau \in CM(\mathcal{O})$, $\Phi_{D,N^+}(\tau) \in E\left(K^{ab}\right)$, where K^{ab} is the maximal abelian extension of K. This construction provides extra algebraic points apart from those produced via the modular parametrization.

The second ingredient is a p-adic analogue of this cocompact Shimura curve parametrization. Before explaining this, suppose that $E/\mathbb{Q}$ is an elliptic curve of conductor N and $p\|N$, which implies that E has multiplicative reduction at p. Let us consider a factorization $N = pN^+N^-$ with N^+, N^- and p coprime and N^- square-free and such that N^- is the product of an odd number of primes. This kind of decomposition is called p-admissible.

Let B be the definite quaternion $\mathbb{Q}$-algebra of discriminant $N^-\infty$. There exists a unique Eichler $\mathbb{Z}[1/p]$-order R of level N^+ (up to conjugation). Fix an identification $\iota : B \otimes \mathbb{Q}_p \to M_2(\mathbb{Q}_p)$ and define $\Gamma^p_{N^+,N^-} = \iota(R^1) \in \mathrm{SL}(2,\mathbb{Q}_p)$.

Recall that $S_2^{rig}\left(\Gamma^p_{N^+,N^-}\right)$ is endowed with a Hecke action.

Theorem 4.3.2 (Cerednik-Drinfeld, [29]). *The rigid analytic quotient space $\Gamma^p_{N^+,N^-}\backslash\mathcal{H}_p$ is isomorphic to $X\left(N^-p,N^+\right)$ as an algebraic curve over $\mathbb{C}_p$.*

4.3.2 Rigid analytic modular forms and elliptic curves. A conjecture.

In particular, Theorem 4.3.2 implies that $S_2^{rig}\left(\Gamma^p_{N^+,N^-}\right)$ gives rise to the same system of Hecke eigenvalues for the Hecke operators as $S_2\left(\Gamma\left(N^-p,N^+\right)\right)$. Hence, starting with $\phi\in S_2^{new}\left(\Gamma_0(N)\right)$, consider the automorphic form $g\in S_2\left(\Gamma\left(N^-p,N^+\right)\right)$ provided by Theorem 4.3.1. Hence, $a_l(E)=a_l(\phi)=a_l(g)$ for any l outside N. Consider the corresponding $f\in S_2^{rig}\left(\Gamma^p_{N^+,N^-}\right)$ corresponding to the Hecke eigenvalues of g. Consider μ_f the p-adic measure attached to the harmonic cocycle defined by f.

Definition 4.3.3. The Schneider p-adic distribution attached to E is the function

$$L_p^{rig}\left(E,s\right)=\int_{\mathbb{Z}_p}\langle x\rangle^{s-1}d\mu_f.$$

Recall that K_ϕ stands for the number field obtained by adjoining to $\mathbb{Q}$ the Hecke eigenvalues of ϕ. The matrices describing the coset representatives for the Hecke operators T_q with q prime, in particular, belong to $M(2,\mathbb{Z}_p)$, hence, the Hecke algebra also acts on $S_2^{rig}(\Gamma)$. In [38], it is pointed out that, while the Mazur-Tate-Teitelbaum p-adic L-function takes values in a K_ϕ-vector space of dimension at most 2, the Schneider p-adic L-function takes values in the field K_f, obtained by adjoining to $\mathbb{Q}_p$ the Hecke eigenvalues of f, and the relation between these fields is not clear. The relation between the Mazur-Tate-Teitelbaum and the Schneider p-adic L-functions is also unclear and it would be an interesting project to work on this problem as a continuation of the present thesis.

Conjecture (Klingenberg, [38]). Fix an embedding $\iota:K_\phi\to\mathbb{C}_p$. Write $\Lambda(\phi,1)=\lambda^+\Omega^++i\lambda^{-1}\Omega^-$ with $\lambda^\pm\in K_\phi$ (i.e., $\Omega^\pm$ are the transcendental periods attached to ϕ). Then, there exists a constant $C\in\iota(K_\phi)$ such that

$$\left.\frac{dL_p(E,s)}{ds}\right|_{s=1}=C\lambda^+\left.\frac{L_p^{rig}(E,s)}{ds}\right|_{s=1}.$$

4.4 Anticyclotomic p-adic L-functions

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let p be a prime such that $p\|N$. This means that E has multiplicative reduction at p. Let $\phi \in S_2(N)$ be the corresponding newform. Let K be a quadratic imaginary field of discriminant d and suppose that the following conditions are satisfied:

i) $\mathcal{O}_K^* = \{\pm 1\}$,

ii) $(N, d) = 1$, and

iii) E has multiplicative reduction at the primes dividing N which are inert in K.

Consider the factorization $N = pN^+D$, where N^+ is the product of the primes dividing N which are inert in K, and D is the product of the primes dividing N which are split in K. Let ϵ be the primitive Dirichlet character attached to K. We say that we are in the definite case if $\epsilon(D) = -1$, and we are in the indefinite case if $\epsilon(D) = 1$. Denote by K_n the ring class field of K of conductor p^n, and define $K_\infty = \cup_{n=0}^{\infty} K_n$. Set $\tilde{G}_\infty = \mathrm{Gal}(K_\infty/K)$. Let $\chi : \tilde{G}_\infty \to \mathbb{C}^*$ be a finite order character. We can exhibit $\tilde{G}_\infty$ in a more precise way. First, denote $\hat{\mathbb{Z}} = \prod_q \mathbb{Z}_q$, where q runs through the set of prime numbers and set $\hat{\mathcal{O}}_K = \mathcal{O}_K \otimes \hat{\mathbb{Z}}$ and $\hat{K} = \hat{\mathcal{O}}_K \otimes \mathbb{Q}$. Now, define $\hat{\mathcal{O}}' = \prod_{q \neq p} \mathcal{O}_q^*$.

Proposition 4.4.1 (cf. [53])**.** $\tilde{G}_\infty \simeq \hat{K}^*/\hat{\mathbb{Q}}^* \hat{\mathcal{O}}' K^*$.

Notice that if $K = \mathbb{Q}$ instead of being a quadratic extension, we recover $\tilde{G}_\infty = \mathbb{Z}_p^*$, hence, integration on $\mathbb{Z}_p^*$ is integration on the Galois group of the maximal abelian extension of $\mathbb{Q}$ which is unramified outside p. Under this point of view, it is understandable why the p-adic L-functions introduced by Mazur-Tate-Teitelbaum are called cyclotomic.

Suppose that we are in the indefinite case. If χ is ramified, the sign in the functional equation for $L(E/K, \chi, s)$ is $-\epsilon(N^-)$ (see [31]), hence, $L(E/K, \chi, s)$ vanishes at $s = 1$ with odd order. In particular, $L(E/K, \chi, 1) = 0$ for any character χ of $\mathrm{Gal}(K_\infty/K)$. This fact calls for the study of $L'(E/K, \chi, 1)$ for different characters χ. Let H be the indefinite quaternion $\mathbb{Q}$-algebra of discriminant D. Choose an embedding $\psi : H \hookrightarrow \mathrm{SL}(2, \mathbb{R})$. Fix an Eichler order R of level N^+ and define $\Gamma = \psi(R^1)$.

Consider an optimal embedding of K in H so that there is an action of K^* on $\mathcal{H}$. Let P be the image on $X(\Gamma)$ of the unique fixed point of $\mathcal{H}$ under

the action of K^*. Suppose that P can be seen as an abelian variety with quaternionic multiplication by the Eichler order R and complex multiplication by $\mathcal{O}_K$, due to the interpretation of $X(\Gamma)$ as a coarse moduli space,. By the theory of complex multiplication, P is defined over K_0, the Hilbert class field of K.

As stated above, there is a modular parametrization $\mathrm{Jac}(X) \to E$ defined over $\mathbb{Q}$. In fact, there exists a sequence of points $P_n \in X(D, N^+)$ such that they produce points $x_n \in E(K_n)$ in a compatible way by this modular parametrization. The argument is as follows: Let P correspond by the coarse moduli space interpretation of X to the triple (A, ι, C), where A is an abelian surface with quaternionic multiplication, ι is an R^{max}-action on A (R^{max} is a maximal order containing R) and C is a subgroup of N^+-torsion of A.

The tree of p-isogenies attached to P is the tree whose vertices correspond to abelian surfaces with quaternionic multiplication by R^{max} and N^+-torsion subgroups which are related to A by an isogeny of degree a power of p. There is an edge between two vertices if the corresponding abelian surfaces are isogenous via an isogeny of degree p^2 in a compatible way. Denote this tree by $\mathcal{T}_p^{(A)}$.

Choose a half line $(e_1, e_2, ..., e_n, ...)$ starting at P, where $S(e_n) = P_{n-1}$ and $T(e_n) = P_n$, setting $P_0 = P$. We can suppose that the endomorphism ring of the abelian surface attached to P_1 is exactly the order of conductor p^n of $\mathcal{O}_K$. As before, the correspondence of Jacquet-Langlands together with the modularity of E allow to map the point P_n to a point $x_n \in E(K_n)$.

Let $a_p := a_p(\phi)$ be the p-th Hecke eigenvalue of ϕ and set $x_n^* = a_p x_n \in E(K_\infty)_p$, where $E(K_\infty)_p = E(K_\infty) \otimes \mathbb{Z}_p$. The system $\{x_n^*\}_{n \geq 1}$ is norm compatible (see [14]).

Denote by $E^+(K_n)$ the extended Mordell-Weil group over K_n. Define a canonical lift $\tilde{x}_n$ of x_n^* to $E^+(K_n)_p$ by the rule

$$x_n = \lim_{m \to \infty} N_{K_m/K_n}(y_m),\ m \geq n,$$

where y_m is a lift of x_n^* to $E^+(K_m)_p$. All these elements are also norm compatible. Denote by $E^+(K_\infty)_p$ the direct limit of the groups $E^+(K_n)_p$ with respect to the inclusions. The fact that $\mathrm{Gal}\,(K_\infty/K) \simeq \mathcal{O}_{K,\mathfrak{p}}^*$ allows us to define an $E^+(K_\infty)_p$-valued p-adic measure by the rule

$$\mu_{\phi,K}([g]) = \tilde{x}_n^g,$$

where $[g]$ is the compact open $g\mathrm{Gal}\,(K_\infty/K_n)$ of $\tilde{G}_\infty$. The details of the fact that $\mu_{\phi,K}$ is a p-adic measure can be found in [13].

As we can see, it is by no means obvious that the group where $\mu_{\phi,K}$ takes values is finitely generated. In this direction, we have the following result due to Rohrlich.

Theorem 4.4.2 ([62])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. Let P be a finite set of primes at which E has good reduction and let L be the maximal abelian extension of $\mathbb{Q}$ unramified outside $P \cup \{\infty\}$. Then, $E(L)$ is finitely generated.*

Nevertheless, if $E/\mathbb{Q}$ has no complex multiplication, $\mu_{\phi,K}$ possibly takes values on a p-adic vector spaces of countably infinite dimension.

Definition 4.4.3 (Bertolini-Darmon, [14], [13])**.** The indefinite anticyclotomic p-adic L-function is the function

$$L_p(E/K,\chi) = \int_{\tilde{G}_\infty} \chi(g) d\mu_{\phi,K},$$

for characters $\chi : \tilde{G}_\infty \to \mathbb{C}^*$.

Fix an embedding of $\mathbb{Q}_p^{alg}$ in $\mathbb{C}$. The measure $\mu_{f,K}$ is expected to satisfy the following interpolation formula:

$$\langle \int_{\tilde{G}_\infty} \chi(g) d\mu_{f,K}, \int_{\tilde{G}_\infty} \chi(g) d\mu_{f,K} \rangle = \theta L(E/K,\chi,1),$$

where $\theta \neq 0$ and where χ is a finite order ramified character of $\tilde{G}_\infty$ and $\langle , \rangle$ denotes the natural extension of the (normalized) Néron-Tate height on $E(K_\infty)$ to a C-valued hermitian pairing on $E^+(K_\infty)_p$. The validity of this above formula depends on a generalization of the Gross-Zagier formula to ramified characters and to Heegner points on Shimura curves, which has not been entirely worked out so far.

Conjecture (Bertolini, Darmon, [14]). $\mathrm{ord}_{s=1} L_p'(E/K,s) \geq (\tilde{r}-1)/2$, where $\tilde{r}$ is the rank of the extended Mordell-Weil group $E^+(K)$.

The reader is referred to [14] for a detailed study of the anticyclotomic p-adic L-function and partial results concerning this conjecture.

Chapter 5

Quadratic p-adic L-functions for $X_0(N)$

Introduction

As we have seen in Chapter 3, the cyclotomic p-adic distribution attached to a newform $f \in S_k(\Gamma_0(N))$ assigns to a compact-open disc $D(a, p^n) \subseteq \mathbb{Z}_p$ the integral of f along the path connecting the cusp $\frac{a}{p^n}$ with $i\infty$ (or a correction of this integral if $p \nmid N$). In this way, as we will see in the present chapter, the p-adic L-function is defined through the modular integral, which is a map from the set $\mathrm{SL}(2,\mathbb{Z})\, i\infty$ to $\mathbb{C}$ obtained by integrating f along geodesics in the extended upper half-plane $\mathcal{H}^*$ which go from the rational numbers to the infinity cusp. This means that the infinity cusp is distinguished. An arithmetical motivation for such a definition is that the complex L function of f and its twists by Dirichlet characters take on values in an $\mathcal{O}_f$-lattice at the critical points $s = j$ with $0 \leq j \leq k-2$, where $\mathcal{O}_f$ is the ring of integers of K_f, the finite extension of $\mathbb{Q}$ obtained by adjoining the Fourier coefficients of f. These facts can be summarized by saying that on the geometric side, the p-adic L-function encodes (partial) information about the homology. But the homology of the modular curve $X_0(N)$ can be generated by loops joining two rational numbers or by loops joining any prescribed point in the extended upper half-plane with its $\Gamma_0(N)$-transforms (see [45]). Hence, a construction of a p-adic L-function depending on, say, quadratic imaginary points rather than cusps would also theoretically encode information on the homology.

In this chapter we propose a definition of a p-adic L-function for a new-

form of even weight 2 for $\Gamma_0(N)$ through modular integrals connecting $\Gamma_0(N)$-transforms of quadratic imaginary points. The main difference with regard to the p-adic L-functions made up with classical modular symbols is that the action of the Hecke operators does not preserve the set $\mathrm{SL}(2,\mathbb{Z})\tau$ for $\tau \in \mathcal{H}$ a quadratic imaginary point. This fact implies that our p-adic L-function takes values in a vector space of countably infinite dimension over a finite extension of $\mathbb{Q}_p$.

For a modular elliptic curve $E/\mathbb{Q}$, the quadratic p-adic L-function attached to E will be defined as the quadratic p-adic L-function attached to the associated normalized newform. For a quadratic imaginary point τ in the upper half-plane, the value of the associated quadratic p-adic L-function at $s = 1$, after composing with the Weierstrass uniformization, will be a point of E defined over $\mathbb{Q}(\tau)^{ab}$, the maximal abelian extension of $\mathbb{Q}(\tau)$. This chapter follows essentially our article [7].

5.1 Quadratic modular integrals

Definition 5.1.1. Let $f \in S_2(\Gamma_0(N))$ be a cusp form and let $\tau \in \mathcal{H}$ be a quadratic imaginary point. The quadratic modular integral attached to f is the assignment

$$\{\gamma_1(\tau), \gamma_2(\tau)\}_f = \int_{\gamma_1(\tau)}^{\gamma_2(\tau)} f(z)dz$$

with $\gamma_1, \gamma_2 \in \mathrm{SL}(2,\mathbb{Z})$.

Clearly, the quadratic modular integral is $\Gamma_0(N)$-invariant. Quadratic modular integrals have been defined as an extension of classical modular symbols, as introduced in [45], in order to study the homology of $X_0(N)$ from another point of view. We will deal with the theory of modular symbols in more detail in chapter 6. The following theorem describes the $\mathbb{Z}$-lattice of classes of closed paths.

Theorem 5.1.2 (Manin, [45])**.** *For any $\alpha \in \mathcal{H}^*$, the following map is surjective. In fact, it does not depend on α:*

$$\begin{array}{ccc} \psi : \Gamma_0(N) & \to & H_1\left(X_0(N)(\mathbb{C}), \mathbb{Z}\right) \\ \gamma & \mapsto & \{\alpha, \gamma(\alpha)\}_{\Gamma_0(N)}. \end{array}$$

Let E_N, P_N and $\Gamma_0(N)'$ denote, respectively, the sets of elliptic, parabolic and commutator elements of $\Gamma_0(N)$. The map ψ gives rise to an exact sequence

$$0 \to \langle \Gamma_0(N)', E_N, P_N \rangle \to \Gamma_0(N) \to H_1\left(X_0(N)(\mathbb{C}), \mathbb{Z}\right) \to 0.$$

These closed paths can be decomposed as $\mathbb{Z}$-linear combinations of elements of a certain finite family of non closed elementary paths. From now on, for any $x, y \in \mathcal{H}^*$, we will write $\{x, y\}$ instead of $\{x, y\}_{\Gamma_0(N)}$.

Definition 5.1.3 (Manin, [45])**.** Consider the map

$$\begin{array}{rcl} \xi : \Gamma_0(N)\backslash \mathrm{SL}\,(2,\mathbb{Z}) & \to & H_1\left(X_0(N)(\mathbb{C}), \mathbb{R}\right) \\ \Gamma_0(N)\gamma & \mapsto & \{\gamma(0), \gamma(i\infty)\}. \end{array}$$

This assignment does not depend on the representative γ. The classes so obtained are called distinguished classes by Manin.

The role of the distinguished classes is given in the following statement.

Theorem 5.1.4 (Manin, [45])**.** *Any class in $H_1\left(X_0(N)(\mathbb{C}), \mathbb{Z}\right)$ can be represented as a sum of distinguished classes. In particular, the distinguished classes generate $H_1\left(X_0(N)(\mathbb{C}), \mathbb{R}\right)$ as a real vector space.*

Manin distinguished classes give rise to the usual modular integrals, i.e., integrals along geodesics connecting rational numbers and infinity. Hence, the closed paths in the homology of $X_0(N)$ are just $\mathbb{Z}$-combinations of distinguished classes. The proof of Theorem 5.1.4 relies on a constructive argument that is known as the Manin continued fraction trick.

Next, we introduce another kind of classes which generate the homology.

Definition 5.1.5 (Rademacher, [58])**.** Let G be a finite set of generators of $\Gamma_0(N)$. It is said to be minimal if $G = \{\gamma_1, ..., \gamma_r, \varepsilon_1, .., \varepsilon_s\}$ with γ_l hyperbolic or parabolic for any $1 \leq l \leq r$, ε_k elliptic for any $1 \leq k \leq s$, and the only relations between the generators are $\varepsilon_k^{n_k} = 1$, with $n_k = 4$ or 6.

The group $\Gamma_0(N)$ always admits a minimal set of generators which can be computed explicitly. This fact is proved in [58] for $N = p$ prime (cf. table 5.1), and in [23] for an arbitrary $N \geq 1$.

Definition 5.1.6. Let G be a minimal set of generators of $\Gamma_0(N)$ and denote $H(G) = \{\sigma \in G | \, \sigma \notin \langle \Gamma_0(N)', E_N, P_N \rangle\}$. Let $\tau \in \mathcal{H}$ be a quadratic imaginary point. A family of quadratic distinguished classes is $\{\{\tau, \sigma(\tau)\}\}_{\sigma \in H(G)}$.

Notice that if G is a minimal set of generators of $\Gamma_0(N)$ in the sense of Rademacher, then $H(G)$ is the set of hyperbolic elements of G.

Proposition 5.1.7. *Any class in $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$ can be represented as a sum of quadratic distinguished classes. In particular, quadratic distinguished classes generate $H_1(X_0(N)(\mathbb{C}), \mathbb{R})$ as a real vector space.*

Proof. Let $\tau \in \mathcal{H}$ be a quadratic imaginary point. By Theorem 6.1.9, any class in $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$ is of the form $\{\tau, \gamma(\tau)\}$ for some $\gamma \in \Gamma_0(N)$. Fix G a minimal set of generators of $\Gamma_0(N)$. Decompose $\gamma = \eta_1 ... \eta_l$ with $\eta_k \in G$. Notice that

$$\{\tau, \gamma(\tau)\} = \{\tau, \eta_1(\tau)\} + \{\eta_1(\tau), \gamma(\tau)\} = \{\tau, \eta_1(\tau)\} + \{\tau, \eta_2\eta_3 ... \eta_l(\tau)\}.$$

Iterating, we have:

$$\{\tau, \gamma(\tau)\} = \sum_{k=1}^{l} \{\tau, \eta_k(\tau)\}.$$

Let us denote by T the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, which induces the unitary translation. Since $\{\tau, T(\tau)\} = 0$, we can suppose that $\eta_k \neq T$ for any k. In addition, if η_k is an elliptic matrix, we can consider its fixed point τ_{η_k} so that we have

$$\{\tau, \eta_k(\tau)\} = \{\tau, \tau_{\eta_k}\} + \{\tau_{\eta_k}, \eta_k(\tau)\} = \{\tau, \tau_{\eta_k}\} + \{\eta_k(\tau_{\eta_k}), \eta_k(\tau)\} = 0.$$

□

Next, we relate the set of hyperbolic elements of a minimal set of generators with the genus of the modular curve.

Theorem 5.1.8. *Let G be a minimal set of generators of $\Gamma_0(N)$ and g the genus of $X_0(N)$. Then,*

$$\operatorname{card}(H(G)) = 2g.$$

Proof. By Proposition 6.1.11, for any minimal set G of quadratic distinguished classes, $H(G)$ generates $H_1\left(X_0(N)(\mathbb{C}),\mathbb{Z}\right)$; hence $\text{card}\left(H(G)\right) \geq 2g$. Denote by K the subgroup of $\Gamma_0(N)$ generated by the commutators, parabolic and elliptic matrices. By Theorem 6.1.9, it is a normal subgroup of $\Gamma_0(N)$ and $\Gamma_0(N)/K$ is isomorphic to $H_1\left(X_0(N)(\mathbb{C}),\mathbb{Z}\right)$, as a free abelian group, and hence, as a $\mathbb{Z}$-module. Since the classes $\{\eta K\}_{\eta\in G}$ generate $\Gamma_0(N)/K$ and the system is minimal, these classes are $\mathbb{Z}$-linearly independent, otherwise there would exist an extra relation between the generators; hence, $\text{card}\left(H(G)\right) \leq 2g$. □

Let us consider the matrices

$$V_k = \begin{pmatrix} k' & 1 \\ -(k'k+1) & -k \end{pmatrix}$$

with $1 \leq k, k' \leq p-1$ and $kk' \equiv -1 \pmod{p}$. From table 5.1 we can see that the number of non elliptic and non parabolic elements in a minimal set of generators of $\Gamma_0(p)$ (p prime) equals $2g$, which illustrates numerically Theorem 5.1.8.

Inspired by Mazur, Tate and Teitelbaum ([49]), let us consider the following kind of quadratic modular integrals.

Definition 5.1.9. Let $\tau \in \mathcal{H}$ be a quadratic imaginary point. Let us define the map

$$\begin{array}{rccc} \phi_f^\tau : & \text{GL}\left(2,\mathbb{R}\right)^+ & \longrightarrow & \mathbb{C} \\ & \gamma & \mapsto & \displaystyle\int_{\gamma(\tau)}^{\tau} f(z)dz. \end{array}$$

The quadratic modular integral attached to f (with fixed end at τ) is the map ϕ_f^τ restricted to the subgroup $\text{SL}\left(2,\mathbb{Z}\right)$. We will denote by ϕ_f the quadratic modular integral ϕ_f^i, where $i^2 = -1$.

Proposition 5.1.10. *Let $A, \gamma \in \text{GL}\left(2,\mathbb{R}\right)^+$. Then*

$$\phi_f^\tau(A\gamma) = \phi_{f|A}^\tau(\gamma) + \phi_f^\tau(A).$$

Proof. First, notice that $dA(z) = \rho(A,z)^2 dz$; hence

$$\phi_{f|A}^\tau(\gamma) = \int_{\gamma(\tau)}^{\tau} \rho(A,z)^2 f(A(z))dz = \int_{A\gamma(\tau)}^{A(\tau)} f(w)dw.$$

Since f is holomorphic in the upper half-plane, the integral along the triangle with vertices $A(\tau)$, $A\gamma(\tau)$ and τ vanishes. Hence

$$\phi^{\tau}_{f|A}(\gamma) = \int_{A\gamma(\tau)}^{\tau} f(z)dz + \int_{\tau}^{A(\tau)} f(z)dz.$$

□

Proposition 5.1.11. *The $\mathbb{Z}$-submodule of $\mathbb{C}$ generated by $\phi^{\tau}_f(\gamma)$ as γ runs through $\mathrm{SL}(2,\mathbb{Z})$ is finitely generated and torsion-free.*

Proof. It is obviously torsion-free. With regard to the finite generation, let $\{A_l\}_{1\leq l\leq n}$ be a set of right coset representatives of $\Gamma_0(N)\backslash\mathrm{SL}(2,\mathbb{Z})$ and let $\{B_j\}_{1\leq j\leq m}$ be a set of generators of $\Gamma_0(N)$. Let $A \in \mathrm{SL}(2,\mathbb{Z})$. There exist $B \in \Gamma_0(N)$ and $l_0 \in \{1,...,n\}$ such that $A = BA_{l_0}$. Hence

$$\phi^{\tau}_f(BA_{l_0}) = \phi^{\tau}_{f|B}(A_{l_0}) + \phi^{\tau}_f(B) = \phi^{\tau}_f(A_{l_0}) + \phi^{\tau}_f(B).$$

Now, write $B = B_{j_1}...B_{j_r}$ with $\{j_1,...,j_r\} \subseteq \{1,...,m\}$. Hence

$$\phi^{\tau}_f(B) = \phi^{\tau}_f(B_{j_2}...B_{j_r}) + \phi^{\tau}_f(B_{j_1}),$$

and this implies that $\phi^{\tau}_f(A)$ is a $\mathbb{Z}$-linear combination of $\phi^{\tau}_f(A_l)$ and $\phi^{\tau}_f(B_j)$ with $1 \leq l \leq n$ and $1 \leq j \leq m$. □

Corollary 5.1.12. *The $\mathbb{Z}$-submodule of $\mathbb{C}$ generated by $\displaystyle\int_{\gamma_1(\tau)}^{\gamma_2(\tau)} f(z)dz$ as γ_1 and γ_2 run through $\mathrm{SL}(2,\mathbb{Z})$ is finitely generated and torsion-free.*

Proof. It follows from the fact that

$$\int_{\gamma_1(\tau)}^{\gamma_2(\tau)} f(z)dz = \phi^{\tau}_f(\gamma_1) - \phi^{\tau}_f(\gamma_2).$$

□

Remark 5.1.13. Denote by Σ_f the $\mathbb{Z}$-submodule of $\mathbb{C}$ generated by $\phi^{\tau}_f(\gamma)$ as γ runs through $\mathrm{SL}(2,\mathbb{Z})$. Propositions 5.1.10 and 6.2.4 imply that we can define an action of $\mathrm{SL}(2,\mathbb{Z})$ on Σ_f, which is given by

$$A \cdot \phi^{\tau}_f(\gamma) = \phi^{\tau}_{f|A}(\gamma), \quad \text{for } A, \gamma \in \mathrm{SL}(2,\mathbb{Z}).$$

Furthermore, Proposition 5.1.10 implies that ϕ^{τ}_f is a 1-cocycle from $\mathrm{SL}(2,\mathbb{Z})$ with values in Σ_f.

5.2 Quadratic p-adic distributions

Let $f = \sum a_n q^n \in S_2(\Gamma_0(N))$ be a normalized eigenform for the Hecke operator T_p. The Hecke polynomial of f at p is defined as $X^2 - a_p X + p$ if $p \nmid N$ or as $X - a_p$ if $p \| N$. If $p^2 | N$, the Hecke polynomial is 1. Denote by $\mathbb{Q}^{alg}$ an algebraic closure of $\mathbb{Q}$ and fix an embedding of $\mathbb{Q}^{alg}$ in an algebraic closure $\mathbb{Q}_p^{alg}$ of the p-adic field $\mathbb{Q}_p$. Let α_p be an admissible root of the Hecke polynomial in the sense of [49]. Our aim is to construct a p-adic distribution by means of the quadratic modular symbols and to derive algebraic properties from it.

Recall that the classical p-adic distribution is defined on the compact open sets $a + p^n\mathbb{Z}_p$ through the classical modular symbols. The distribution property is established through the fact that f is an eigenform for the Hecke operator T_p and that α_p is a root of the Hecke polynomial. The coset representatives of T_p act on the set of cusps and the integrals along the resulting paths can be seen as the measures of compact open subsets covering $a+p^n\mathbb{Z}_p$. The fact that the coset representatives of T_p preserve the cusps implies that the cyclotomic p-adic measure takes values in a finite dimensional $\mathbb{C}_p$-vector space.

Although T_p acts on quadratic modular symbols, its coset representatives do not. This fact calls for an alternative definition of a p-adic measure in this setting. Our p-adic measure, in principle, takes values in a K-vector space of countable dimension (K is a certain finite extension of $\mathbb{Q}_p$). This situation comes from the fact that the integrals of f acted by the coset representatives of T_p do not belong to a lattice. Measures which take values in a group which is not a lattice are not new: in [13], the authors constructed a p-adic measure which takes values in the extended Mordell-Weil group of $E(K_\infty)$, where $E/\mathbb{Q}$ is an elliptic curve and K_∞ is a certain algebraic infinite extension of $\mathbb{Q}_p$.

If f is defined over $\mathbb{Q}$, we will prove that our p-adic L-function provides values in the group of algebraic points of the elliptic curve attached to f by the Eichler-Shimura construction.

A p-adic measure on $\mathbb{Z}_p$ is uniquely determined by its values on the closed discs $\alpha + p^n\mathbb{Z}_p$, where α runs through $\mathbb{Z}_p$ and $n \geq 0$. First, we define the measure on the closed discs contained in $\mathbb{Z}_p^*$. To this end, notice that for any closed disc $\alpha + p^n\mathbb{Z}_p$ of $\mathbb{Z}_p^*$, there exists a unique positive integer a, with $1 \leq a < p^n$, such that $\alpha + p^n\mathbb{Z}_p = a + p^n\mathbb{Z}_p$ (in fact, a is the truncation of α up to order p^n). We will define the measure of the disc by means of this

unique integer a; in this way it will be well defined. After that, we check in Proposition 5.2.3 that the distribution property is satisfied.

For any $a \in \mathbb{Z}$ with $|a| \in \{1, ..., p-1\}$, there exists a unique couple of integers $x, y \in \mathbb{Z}$ such that $ax - py = 1$ and $x \in \{0, ..., p-1\}$. Denote

$$\gamma_{a,1} = \begin{pmatrix} a & y \\ p & x \end{pmatrix}.$$

For any $u \in \mathbb{Z}$ such that $0 \leq |u| \leq p-1$, define

$$\gamma_u = \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}.$$

For any $a \in \mathbb{Z}$ with $1 \leq |a| < p^n$ and $(a,p) = 1$, write $|a| = a_0 + \sum_{k=1}^{n-1} u_k p^k$ with $0 \leq u \leq p-1$. Define

$$\gamma_{a,n} = \begin{cases} \gamma_{u_{n-1}} \gamma_{u_{n-2}} \cdots \gamma_{u_1} \gamma_{a_0,1}, & \text{if } a > 0, \\ \gamma_{-u_{n-1}} \gamma_{-u_{n-2}} \cdots \gamma_{-u_1} \gamma_{-a_0,1}, & \text{if } a < 0. \end{cases}$$

Notice that $\gamma_{a+up^n,n+1} = \gamma_u \gamma_{a,n}$. Denote

$$\gamma_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Lemma 5.2.1. *For any $f \in S_2(\Gamma_0(N))$, any integers a, u with $1 \leq |a| < p^n$ and $0 \leq |u| < p$, we have*

$$\phi_f^\tau(\gamma_p \gamma_{a+up^n,n+1}) = \phi_f^\tau(\gamma_{a,n}).$$

Proof. It follows from the facts that for $\tau \in \mathcal{H}$, $\gamma_p \gamma_{a+up^n,n+1}(\tau) = \gamma_{a,n}(\tau) + u \in \mathcal{H}$, and that the translation T^u belongs to $\Gamma_0(N)$. □

Let $f \in S_2(\Gamma_0(N))$ be an eigenform for T_p with eigenvalue a_p and let α_p be an admissible root of the Hecke polynomial. From now on, we will suppose that $p \nmid N$ or that $p \| N$. We propose the following

Definition 5.2.2. For any $a \in \mathbb{Z}$ coprime to p and any $n \geq 1$ such that $0 \leq a < p^n$, denote

$$\Delta_f^\tau(a,n) = \phi_f^\tau(\gamma_{a,n}) - \phi_f^\tau(\gamma_{-a,n}),$$
$$\Delta_f^\tau(pa,n) = \phi_f^\tau(\gamma_p\gamma_{a,n}) - \phi_f^\tau(\gamma_p\gamma_{-a,n}).$$

- If $p \| N$, we define

$$\mu_{\mathcal{Q}}\left(a + p^n\mathbb{Z}_p\right) = a_p^{-n}\Delta_f^\tau(a,n).$$

- If $p \nmid N$, we define

$$\mu_{\mathcal{Q}}\left(a + p^n\mathbb{Z}_p\right) = \alpha_p^{-n}\left(\Delta_f^\tau(a,n) - \alpha_p^{-1}\Delta_f^\tau(pa,n)\right).$$

Define

$$\mu_{\mathcal{Q}}\left(\mathbb{Z}_p^*\right) = \sum_{a=1}^{p-1}\mu_{\mathcal{Q}}\left(a + p\mathbb{Z}_p\right),$$

and for any $k \geq 1$, set

$$\mu_{\mathcal{Q}}\left(p^k\mathbb{Z}_p\right) = 0.$$

Let α_p be a root of the Hecke polynomial ($\alpha_p = a_p$ if $p \| N$). Consider the $\mathbb{Z}_p[\alpha_p^{-1}]$-lattice

$$\Sigma_{f,1} = \langle \phi_f^\tau\left(\gamma_{a,1}\right),\ 1 \leq |a| \leq p-1\rangle_{\mathbb{Z}_p\left[\alpha_p^{-1}\right]}.$$

Define by induction

$$\Sigma_{f,n+1} = \Sigma_{f,n} + \langle \phi_f^\tau\left(\gamma_{a,n+1}\right),\ 1 \leq |a| \leq p^{n+1}-1, (a,p)=1\rangle_{\mathbb{Z}_p\left[\alpha_p^{-1}\right]}.$$

We can identify $\Sigma_{f,n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p(\alpha_p)$ with $\mathbb{Q}_p\left(\alpha_p\right)^{N_n}$ for some N_n. Since we have inclusions

$$\Sigma_{f,n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p(\alpha_p) \hookrightarrow \Sigma_{f,n+1} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p(\alpha_p),$$

we can consider the infinite dimensional $\mathbb{Q}_p\left(\alpha_p\right)$-vector space $\varinjlim \Sigma_{f,n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p(\alpha_p)$, where $\mu_{\mathcal{Q}}$ takes values. In fact, for any $a \in \mathbb{Z}$ and $n \geq 1$ with $1 \leq a < p^n$, $\mu_{\mathcal{Q}}\left(a + p^n\mathbb{Z}_p\right) \in \Sigma_{f,n}$.

Let K be a non-archimedean field which is complete with respect to its ultrametric norm $|\ |_p$. Denote

$$c_{00}(K) = \left\{(x_n)_{n\geq 1} \in K^{\mathbb{N}} \,|\, \text{there exists } N_x \text{ such that } x_n = 0 \text{ for } n \geq N_x\right\}.$$

This subspace is endowed with the norm

$$|(x_n)|_{\infty,p} = \max_{n\geq 1} |x_n|_p .$$

The Banach completion of $c_{00}(K)$ with respect to its norm is the infinite dimensional Banach space

$$c_\infty(K) = \\ \left\{(x_n)_{n\geq 1} \in K^{\mathbb{N}} \,|\, \text{there exists } C_x \text{ such that } |x_n|_p \leq C_x \text{ for any } n \geq 1\right\}.$$

Given a sequence $(x_n) \in c_\infty(K)$, we write $|(x_n)|_p$ instead of $|(x_n)|_{\infty,p}$. Having fixed a basis in each $\Sigma_{f,n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p(\alpha_p)$ in a compatible way, since each compact open subset can be covered by a finite number of discs, it turns out that $\mu_{\mathcal{Q}}$ takes values on $c_{00}(\mathbb{Q}_p(\alpha_p))$.

The aim is to integrate continuous functions against this $c_{00}(\mathbb{Q}_p(\alpha_p))$-valued measure. These integrals will belong to the Banach space $c_\infty(\mathbb{Q}_p(\alpha_p))$.

Proposition 5.2.3. *The function $\mu_{\mathcal{Q}}$ extends, in a unique way, to a p-adic distribution with values in $c_{00}(\mathbb{Q}_p(\alpha_p))$.*

Proof. Define

$$\epsilon(N) = \begin{cases} 1, & \text{if } (p,N) = 1, \\ 0, & \text{if } (p,N) = p. \end{cases}$$

By definition of the Hecke operator T_p and the fact that f is an eigenform for it, one has that for any $a \in \mathbb{Z}$, and $n \geq 1$ such that $1 \leq a < p^n$ and $(a,p) = 1$,

$$a_p \phi_f^\tau(\gamma_{a,n}) = \sum_{u=0}^{p-1} \phi_{f|\gamma_u}^\tau(\gamma_{a,n}) + \epsilon(N)\phi_{f|\gamma_p}^\tau. \tag{5.2.1}$$

After changing variables and splitting the integrals, (5.2.1) becomes

$$a_p \phi_f^\tau(\gamma_{a,n}) = \sum_{u=0}^{p-1} \phi_f^\tau(\gamma_{a+up^n,n+1}) + \epsilon(N)\phi_f^\tau(\gamma_p\gamma_{a,n}) + R$$

with

$$R = \sum_{u=0}^{p-1} \phi_f^\tau(\gamma_u) - \epsilon(N)\phi_f^\tau(\gamma_p).$$

Now, taking into account that

$$\sum_{u=0}^{p-1} \phi_f^\tau(\gamma_u) = \sum_{u=0}^{p-1} \phi_f^\tau(\gamma_{p-u}),$$

we have that

$$a_p \phi_f^\tau(\gamma_{-a,n}) = \sum_{u=0}^{p-1} \phi_f^\tau(\gamma_{-a-up^n,n+1}) + \epsilon(N)\phi_f^\tau(\gamma_p\gamma_{-a,n}) + R. \tag{5.2.2}$$

Subtracting (5.2.2) from (5.2.1), we have

$$a_p \Delta_f^\tau(a,n) = \sum_{u=0}^{p-1} \Delta_f^\tau(a+up^n, n+1) + \epsilon(N)\Delta_f^\tau(pa,n).$$

If $p \| N$, we have

$$\Delta_f^\tau(a,n) = a_p^{-1} \sum_{u=0}^{p-1} \Delta_f^\tau(a+up^n, n+1),$$

which is equivalent to the distribution property in this case. If $p \nmid N$, by using Lemma 5.2.1, we can write

$$(a_p + p\alpha_p^{-1})\Delta_f^\tau(a,n) =$$
$$\textstyle\sum_{u=0}^{p-1} \Delta_f^\tau(a+up^n, n+1) - \alpha_p^{-1}\Delta_f^\tau(p(a+up^n), n+1) + \Delta_f^\tau(pa,n).$$

Since α_p is a root of the Hecke polynomial, we have

$$\alpha_p \Delta_f^\tau(a,n) - \Delta_f^\tau(pa,n) = \sum_{u=0}^{p-1} \Delta_f^\tau(a+up^n, n+1) - \alpha_p^{-1}\Delta_f^\tau(p(a+up^n), n+1),$$

which is also equivalent to the distribution property in this case. □

If α_p is a p-adic unit, then all the $\mathbb{Z}_p\left[\alpha_p^{-1}\right]$-linear combinations of the integrals $\phi_f^\tau(\gamma_{a,n})$ are uniformly bounded by 1. In this case, f is said to be ordinary at p; otherwise f is supersingular at p. We will suppose that f is ordinary at p. We will use the next proposition to show that we can integrate continuous functions against $\mu_{\mathcal{Q}}$.

Proposition 5.2.4. *Let K be a non-archimedean field which is complete with respect to its ultrametric norm. Let μ be a $c_{00}(K)$-valued p-adic distribution which is uniformly bounded. Then, for any continuous function $\chi : \mathbb{Z}_p \to K$, the Riemann sums*

$$S_n(\chi, \{x_a\}) = \sum_{(a,p)=1, a=1}^{p^n-1} \chi(x_a)\mu\left(a + p^n\mathbb{Z}_p\right)$$

converge to an element of $c_\infty(K)$ which is independent of the choice of the points $x_a \in a + p^n\mathbb{Z}_p$.

Proof. Given two partitions of $\mathbb{Z}_p$, $\mathcal{P}_n = \{a + p^n\mathbb{Z}_p\}_a$ and $\mathcal{P}_m = \{b + p^m\mathbb{Z}_p\}_b$, and two choices $\{x_a\}, \{y_b\}$ with $x_a \in a + p^n\mathbb{Z}_p$ and $y_b \in b + p^m\mathbb{Z}_p$, take a refinement of both partitions, $\mathcal{P}_r = \{c + p^r\mathbb{Z}_p\}_c$. We can write

$$S_n(\chi, \{x_a\}) - S_m(\chi, \{y_b\}) = \sum_c (\chi(x_{a,c}) - \chi(x_{b,c}))\mu\left(c + p^r\mathbb{Z}_p\right),$$

where $x_{a,c} = x_a$ if $c + p^r\mathbb{Z}_p \subset a + p^n\mathbb{Z}_p$. Since μ is uniformly bounded, say, by M, according to the ultrametric triangle inequality, we have:

$$|S_n(\chi, \{x_a\}) - S_m(\chi, \{y_b\})|_p \leq \max_c |\chi(x_{a,c}) - \chi(y_{b,c})|_p M.$$

Since χ is continuous, the Riemann sums form a Cauchy sequence. Hence, they have a limit in $c_\infty(K)$. □

5.3 Quadratic p-adic L-functions

Let $f \in S_2(\Gamma_0(N))$ be an eigenform for T_p which is ordinary at p and let $\tau \in \mathcal{H}$ be a quadratic imaginary point and $\mu_{\mathcal{Q}}$ the attached p-adic quadratic measure. Denote by $\mathcal{X}$ the topological group $\mathrm{Hom}_{\mathrm{cont}}\left(\mathbb{Z}_p^*, \mathbb{Q}_p^*\right)$. We propose the following

Definition 5.3.1. The quadratic p-adic L-function attached to f and τ is

$$L_p(f; \chi) = \int_{\mathbb{Z}_p^*} \chi(x) d\mu_{\mathcal{Q}}(x),$$

where $\chi \in \mathcal{X}$.

Recall that for any $x \in \mathbb{Z}_p^*$ we can write

$$x = \omega(x)\langle x \rangle,$$

where $\omega(x)$ is the unique $(p-1)$-th root of unity in $\mathbb{Z}_p^*$ congruent to $x \pmod{p}$. Given $s \in \mathbb{Z}_p$, let us consider the p-adic character

$$\chi_s(x) = \exp_p\left(s \log_p\left(\langle x \rangle\right)\right), \quad x \in \mathbb{Z}_p^*.$$

Here, the function $\exp_p$ is the p-adic exponential, which is holomorphic in the open disc $D\left(0, p^{\frac{1}{p-1}}\right)$, and $\log_p$ is the p-adic logarithm, which is holomorphic in the open disc $D\left(1, p^{\frac{1}{p-1}}\right)$ (for details cf. [60]).

It is not difficult to obtain the following expansion:

$$\chi_s(x) = \sum_{n=0}^{\infty} \frac{\log_p\left(\langle x \rangle\right)^n}{n!} s^n. \tag{5.3.1}$$

Given $s \in \mathbb{Z}_p$, let us denote

$$L_p(f; s) = L_p(f; \chi_s).$$

Proposition 5.3.2. *The quadratic p-adic L-function $L_p(f; s)$ is p-adically holomorphic in the open unit disc.*

Proof. For any integer $n \geq 1$, let us denote by σ_n the sum of its digits in base p. It is well known (cf. [60]) that $|n!|_p = p^{\frac{-n+\sigma_n}{p-1}}$. Thus, there exists $C > 0$ such that

$$\left| \frac{\log_p\left(\langle x \rangle\right)^n}{n!} \right|_p \leq C.$$

Since $\mu_{\mathcal{Q}}$ is uniformly bounded on the compact subsets of $\mathbb{Z}_p$, say, by M, we have that

$$\left| \int_{\mathbb{Z}_p^*} \frac{\log_p\left(\langle x \rangle\right)^n}{n!} d\mu_{\mathcal{Q}}(x) \right|_p \leq MC,$$

hence, if $|s|_p < 1$, we have

$$\int_{\mathbb{Z}_p^*} \langle x \rangle^s d\mu_{\mathcal{Q}}(x) = \sum_{n=0}^{\infty} s^n \int_{\mathbb{Z}_p^*} \frac{\log_p\left(\langle x \rangle\right)^n}{n!} d\mu_{\mathcal{Q}}(x).$$

□

Definition 5.3.3. The quadratic p-adic L-function attached to a modular elliptic curve $E/\mathbb{Q}$ and a quadratic imaginary point τ is defined as

$$L_p(E;s) = L_p(f_E; s-1),$$

where f_E is the modular newform attached to E.

If E has conductor N, then, there is a modular parametrization

$$\begin{aligned} \Psi_E : \ \Gamma_0(N)\backslash\mathcal{H} &\to \mathbb{C}/\Lambda_E \\ w &\mapsto \int_{i\infty}^{w} f_E(z)dz. \end{aligned}$$

If we denote by $\Phi_E = (\wp_E, \wp'_E)$ the Weierstrass uniformization map, the following result is well known.

Theorem 5.3.4 (Birch, [15])**.** *Let K be a quadratic imaginary field. If $\tau \in K \cap \mathcal{H}$, then*

$$\Phi_E\left(\Psi_E(\tau)\right) \in E\left(K^{ab}\right),$$

where K^{ab} denotes the maximal abelian extension of K.

As an application of the above constructions, we have the following

Theorem 5.3.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and α_p an admissible root of the Hecke polynomial at p of the corresponding newform f_E. Let a_p be the eigenvalue of T_p corresponding to f_E. Suppose that f_E is ordinary at p.*

- *If $p \nmid N$ and $\alpha_p = 1$, then, for any $a \in \mathbb{Z}$ coprime to p and for any $n \geq 0$,*

  $$\Phi_E\left(\mu_{\mathcal{Q}}\left(a + p^n\mathbb{Z}_p\right)\right) \in E\left(\mathbb{Q}(\tau)^{ab}\right).$$

  In particular,

  $$\Phi_E\left(L_p(E;1)\right) \in E\left(\mathbb{Q}(\tau)^{ab}\right).$$

- *If $p \| N$, then, for any $a \in \mathbb{Z}$ coprime to p and for any $n \geq 0$,*

  $$\Phi_E\left(a_p^n \mu_{\mathcal{Q}}\left(a + p^n\mathbb{Z}_p\right)\right) \in E\left(\mathbb{Q}(\tau)^{ab}\right).$$

  In particular,

  $$\Phi_E\left(a_p L_p(E;1)\right) \in E\left(\mathbb{Q}(\tau)^{ab}\right).$$

Proof. Suppose that $p\|N$ (the other case is analogous). We have:

$$\mu_{\mathcal{Q}}\left(a+p^n\mathbb{Z}_p\right)=a_p^{-n}\Delta_f^{\tau}\left(\gamma_{a,p^n}\right)=a_p^{-n}\left(\Psi_E\left(\gamma_{a,p^n}(\tau)\right)-\Psi_E\left(\gamma_{-a,p^n}(\tau)\right)\right).$$

In our case, the arguments of the modular parametrization belong to the quadratic imaginary field $\mathbb{Q}(\tau)$. Hence, by using Theorem 5.3.4,

$$\Phi_E\left(\Psi_E\left(\gamma_{a,p^n}(\tau)\right)\right),\Phi_E\left(\Psi_E\left(\gamma_{-a,p^n}(\tau)\right)\right)\in E\left(\mathbb{Q}(\tau)^{ab}\right).$$

Since Φ_E is an isomorphism of groups, the result follows. □

Examples 5.3.6. The elliptic curve $Y^2=4X^3-1728X+32832$ has conductor 11. Its associated newform f generates $S_2(\Gamma_0(11))$ as a $\mathbb{C}$-vector space. Take $p=11$ and $\tau=i$, the imaginary unit. The corresponding Fourier coefficient is $a_{11}(f)=1$. We find that $\wp_E(L_{11}(E,1))=x$, where the irreducible polynomial of x over $\mathbb{Q}$ is

$$\begin{aligned}&-38963-9322X+14726X^2-9706X^3+23974X^4+16790X^5-22187X^6\\&+17974X^7+13460X^8+17402X^9+11639X^{10}+13814X^{11}-5399X^{12}\\&-14060X^{13}+46589X^{14}-3031X^{15}+20654X^{16}-27210X^{17}+8188X^{18}\\&+12786X^{19}+15058X^{20}+14566X^{21}+7756X^{22}+20873X^{23}+995X^{24}\\&-4516X^{25}-15375X^{26}-1732X^{27}+16538X^{28}-13180X^{29}+7636X^{30}\\&-5915X^{31}+8989X^{32}-2532X^{33}+358X^{34}+2334X^{35}-3140X^{36}+3786X^{37}\\&+3484X^{38}-119X^{39}+X^{40}.\end{aligned}$$

We calculated this polynomial by means of the software Mathematica. First, for $1\leq a\leq 10$, we computed the integrals $\phi_f(\gamma_{a,11})$ up to a precision of 150 decimals. Second, we summed them up. This sum, seen as a complex number, belongs to the complex torus attached to E by the Weierstrass uniformization map. Alternatively, seen p-adically, the sum is $L_{11}(f,0)$ (see Definition 5.2.2). We computed $\wp_E(L_{11}(f,0))$ and $\wp'_E(L_{11}(f,0))$, also up to a precision of 150 decimals. After that, we recognized $x=\wp_E(L_{11}(f,0))$ and $y=\wp'_E(L_{11}(f,0))$ as algebraic integers by means of the command RootApproximant and we checked that the point (x,y) satisfies the Weierstrass equation of E.

Table 5.1:

p	Minimal set of generators of $\Gamma_0(p)$	Relations	$g(X_0(p))$
2	T, V_1	$V_1^2 = 1$	0
3	T, V_2	$V_2^3 = 1$	0
5	T, V_2, V_3	$V_2^2 = V_3^2 = 1$	0
7	T, V_3, V_5	$V_3^3 = V_5^3 = 1$	0
11	T, V_4, V_6		1
13	T, V_4, V_5, V_8, V_{10}	$V_5^2 = V_8^2 = V_4^3 = V_{10}^3 = 1$	0
17	T, V_4, V_7, V_9, V_{13}	$V_4^2 = V_{13}^2 = 1$	1
19	$T, V_5, V_8, V_{12}, V_{13}$	$V_8^2 = V_{12}^3 = 1$	1
23	$T, V_8, V_{10}, V_{12}, V_{14}$		2
29	$T, V_6, V_{12}, V_{13}, V_{15}, V_{17}, V_{22}$	$V_{12}^2 = V_{17}^2 = 1$	2
31	$T, V_6, V_9, V_{13}, V_{17}, V_{21}, V_{26}$	$V_6^3 = V_{26}^3 = 1$	2
37	$T, V_6, V_8, V_{11}, V_{16}, V_{20}, V_{27}, V_{28}, V_{31}$	$V_6^2 = V_{31}^2 = V_{11}^3 = V_{27}^3 = 1$	2
41	$T, V_7, V_9, V_{16}, V_{19}, V_{21}, V_{24}, V_{32}, V_{33}$	$V_9^2 = V_{32}^2 = 1$	3
43	$T, V_7, V_{13}, V_{15}, V_{18}, V_{24}, V_{27}, V_{29}, V_{37}$	$V_7^3 = V_{37}^3 = 1$	3
47	$T, V_{13}, V_{16}, V_{19}, V_{22}, V_{24}, V_{27}, V_{30}, V_{33}$		4
53	$T, V_{12}, V_{14}, V_{20}, V_{23}, V_{25}, V_{27}, V_{30}, V_{32}$ V_{38}, V_{40}	$V_{23}^2 = V_{30}^2 = 1$	4
59	$T, V_{12}, V_{15}, V_{20}, V_{26}, V_{28}, V_{30}, V_{32}, V_{38}$ V_{43}, V_{46}		5
61	$T, V_9, V_{11}, V_{14}, V_{18}, V_{25}, V_{28}, V_{32}, V_{35}$ $V_{42}, V_{48}, V_{50}, V_{51}$	$V_{11}^2 = V_{50}^2 = V_{14}^3 = V_{48}^3 = 1$	4
67	$T, V_{10}, V_{18}, V_{21}, V_{24}, V_{30}, V_{31}, V_{35}, V_{38}$ $V_{42}, V_{45}, V_{48}, V_{56}$	$V_{30}^3 = V_{28}^3 = 1$	5
71	$T, V_9, V_{13}, V_{24}, V_{26}, V_{28}, V_{34}, V_{36}, V_{42}$ $V_{44}, V_{46}, V_{57}, V_{61}$		6
73	$T, V_9, V_{11}, V_{17}, V_{22}, V_{25}, V_{27}, V_{33}, V_{39}$ $V_{46}, V_{47}, V_{50}, V_{55}, V_{61}, V_{65}$	$V_{27}^2 = V_{46}^2 = V_9^3 = V_{65}^3 = 1$	5
79	$T, V_{12}, V_{20}, V_{24}, V_{25}, V_{30}, V_{34}, V_{36}, V_{42}$ $V_{44}, V_{48}, V_{53}, V_{56}, V_{58}, V_{66}$	$V_{24}^3 = V_{56}^3 = 1$	6
83	$T, V_{14}, V_{22}, V_{28}, V_{30}, V_{32}, V_{37}, V_{40}, V_{42}$ $V_{45}, V_{50}, V_{52}, V_{54}, V_{60}, V_{68}$		7
89	$T, V_{10}, V_{18}, V_{21}, V_{31}, V_{34}, V_{36}, V_{39}, V_{43}$ $V_{45}, V_{49}, V_{52}, V_{55}, V_{57}, V_{67}, V_{70}, V_{78}$	$V_{34}^2 = V_{55}^2 = 1$	7
97	$T, V_{11}, V_{15}, V_{22}, V_{23}, V_{28}, V_{30}, V_{36}, V_{40}$ $V_{46}, V_{50}, V_{56}, V_{62}, V_{66}, V_{68}, V_{73}, V_{75}, V_{81}, V_{85}$	$V_{22}^2 = V_{75}^2 = V_{36}^3 = V_{62}^3 = 1$	7
101	$T, V_{10}, V_{19}, V_{23}, V_{27}, V_{30}, V_{35}, V_{40}, V_{43}$ $V_{49}, V_{51}, V_{57}, V_{60}, V_{65}, V_{70}, V_{73}, V_{77}, V_{81}, V_{91}$	$V_{10}^2 = V_{91}^2 = 1$	8

Chapter 6

Quadratic p-adic L-functions for $X(D, N)$

Introduction

For a cocompact arithmetic Fuchsian group of the first kind, the absence of cusps prevents the definition of p-adic L-functions via modular integrals connecting rational numbers. In this chapter, we extend the concept of quadratic modular integral introduced in chapter 5 to cover the cocompact case, and we extend the definition of the quadratic p-adic L-function given in chapter 5 for the modular curve $X_0(N)$ to a Shimura curve $X(D, N)$ with $D > 1$, $p \nmid D$ and $p \| N$. We examine the construction of the classical modular symbol by Birch and Manin and we extend it to our quadratic setting. The quadratic modular symbol will depend on a quadratic imaginary element in $\mathcal{H}$ and a prime p. After fixing a quadratic imaginary point $\tau \in \mathcal{H}$, in Proposition 6.2.15, we prove the existence of an inclusion of the $\mathbb{C}$-vector space of classical modular symbols in the space of quadratic modular symbols associated to p, if p is inert in $\mathbb{Q}(\tau)$.

There is an analogue of the Manin continued fraction trick in the cocompact case, in which the role of the Manin distinguished classes is played by closed homology classes which are loops around the prescribed quadratic imaginary point τ. Algorithm 6.1.20 finds the decomposition of any closed paths into these elementary paths in the case of an arithmetic Fuchsian group of signature $(1, e)$, and Algorithm 6.1.22 decomposes closed paths in $X_0(N)$ into open paths connecting quadratic imaginary points. This algorithm is

inspired by continuous fractions.

The last part of the chapter consists of a cohomological study of the modular symbols (classical and quadratic). We work out the details of the identification of the classical modular symbol with the compact support cohomology of the open quotient $\Gamma_0(N)\backslash\mathcal{H}$ developed in [5]. In particular, we make explicit the spectral sequences that intervene in the proof and explain how they collapse providing the isomorphisms. We adapt these ideas to give a cohomological interpretation of our quadratic modular symbols in Theorem 6.2.12. The key to prove this result is Proposition 6.2.10. This chapter follows the articles [8] and [9].

6.1 Quaternion algebras and Shimura curves

6.1.1 Arithmetic Fuchsian groups acting on $\mathcal{H}$

We introduce here some notations and general facts about quotients of the Poincaré upper half-plane $\mathcal{H}$ by arithmetic Fuchsian groups. For a closer study of these subjects, we refer the reader to [1]. Let us begin by presenting the hyperbolic metric on $\mathcal{H}$, which is defined as

$$\delta(z_1,z_2)=\left|\operatorname{arccosh}\left(1+\frac{|z_1-z_2|^2}{2\mathrm{Im}(z_1)\mathrm{Im}(z_2)}\right)\right|.$$

Under this metric, the hyperbolic lines are the semilines which are orthogonal to the real axis and the semicircles centred at real points.

The group $\mathrm{SL}(2,\mathbb{R})$ acts on $\mathcal{H}$ by Möbius transformations and its action factorizes through $\mathrm{PSL}(2,\mathbb{R})$. For any subgroup Γ of $\mathrm{SL}(2,\mathbb{R})$, denote by $\mathrm{P}\Gamma$ the image of Γ in $\mathrm{PSL}(2,\mathbb{R})$.

Definition 6.1.1. Let $\gamma\in\mathrm{SL}(2,\mathbb{R})$, $\gamma\neq\pm\mathrm{Id}$. Then,

(a) γ is elliptic if it has a fixed point $z\in\mathcal{H}$, and the other fixed point is $\overline{z}$.

(b) γ is parabolic if it has a unique fixed point in $\mathbb{R}\cup\{i\infty\}$.

(c) γ is hyperbolic if it has two distinct fixed points in $\mathbb{R}\cup\{i\infty\}$.

Proposition 6.1.2. *Let $\gamma\in\Gamma\subseteq\mathrm{SL}(2,\mathbb{R})$, $\gamma\neq\pm\mathrm{Id}$. Then, γ is elliptic if and only if $|\mathrm{Tr}(\gamma)|<2$. If $\mathrm{Tr}(\gamma)=0$, then, γ has order 2 or 4 depending on $-\mathrm{Id}\in\Gamma$ or $-\mathrm{Id}\notin\Gamma$. If $\mathrm{Tr}(\gamma)=1$, then, γ has order 3 or 4 depending*

on $-\mathrm{Id} \in \Gamma$ *or* $-\mathrm{Id} \notin \Gamma$. *These are the two only possibilities for elliptic transformations with integral traces.*

□

Definition 6.1.3. Let $\Gamma \subseteq \mathrm{SL}(2,\mathbb{R})$ be a discrete subgroup acting on $\mathcal{H}$. A point $z \in \mathcal{H}$ is said to be elliptic if its isotropy group in $\mathrm{P}\Gamma$ is generated by the class of an elliptic element of Γ. The order of z is the order of its isotropy group.

Fix $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ be an indefinite quaternion $\mathbb{Q}$-algebra and $\Gamma^1 = \phi(\mathcal{O}_H^1)$. Let Γ be an arithmetic Fuchsian group of the first kind commensurable with Γ^1. It acts on $\mathcal{H}$ by Möbius transformations and the action factors through its image in $\mathrm{PSL}(2,\mathbb{R})$. The quotient $\Gamma\backslash\mathcal{H}$ has an analytic structure of Riemann surface. If this Riemann surface is compact, then Γ is said to be cocompact. The Riemann surface $\Gamma\backslash\mathcal{H}$ is analytically isomorphic to an open subset of a smooth algebraic curve defined over $\mathbb{Q}$, which is denoted $X(\Gamma)$ (see [65]). Notice that the order of an elliptic point in $\Gamma\backslash\mathcal{H}$ can only be 2 or 3.

The following result is well known.

Theorem 6.1.4. *Let* Γ *be an arithmetic Fuchsian group of the first kind commensurable with* Γ_H^1. *Then* Γ *is cocompact if and only if* H *is a division algebra.*

□

Examples 6.1.5. The quaternion $\mathbb{Q}$-algebra with discriminant 1 is isomorphic to $\mathrm{M}(2,\mathbb{Q})$. Consider the maximal order $\mathrm{M}(2,\mathbb{Z})$. As seen in the Prolegomena, the congruence subgroup $\Gamma_0(N)$ is provided by the Eichler order $\mathcal{O}_0(1,N)$. Thus, $\Gamma_0(N)$ is not cocompact. The Riemann surface $\Gamma_0(N)\backslash\mathcal{H}$ becomes compact by adding the set of cusps, $\mathrm{SL}(2,\mathbb{Z})\, i\infty$. The compact Riemann surface corresponds to $X_0(N)(\mathbb{C})$, the set of complex points of the modular curve $X_0(N)$.

Examples 6.1.6. Let $H = \left(\frac{a,b}{\mathbb{Q}}\right)$ be a quaternion $\mathbb{Q}$-algebra of discriminant $D > 1$. The group $\Gamma(D,N)$ is cocompact because it does not have parabolic elements. The Riemann surface $\Gamma(D,N)\backslash\mathcal{H}$ is compact and analytically isomorphic to an algebraic curve $X(D,N)$ (see [65]). An explicit method for producing fundamental domains for several $\Gamma(D,N)$, as well as various examples of them, can be consulted at [1] and [73].

Let $\mathrm{GL}(2,\mathbb{R})^+$ be the multiplicative subgroup of real matrices with positive discriminant and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{R})^+$. Recall the definition of the automorphy factor given in chapter 5:

$$\rho(\gamma, z) = \frac{\det(\gamma)^{1/2}}{cz+d}.$$

Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function. As in chapter 5, for any non-negative integer k, denote

$$f|_k\gamma(z) = \rho(\gamma, z)^k f(\gamma(z)).$$

Definition 6.1.7. An automorphic form of weight k for a cocompact group Γ is a holomorphic function f on $\mathcal{H}$ such that $f|_k\gamma = f$, for any $\gamma \in \Gamma$. The $\mathbb{C}$-vector space of automorphic forms of weight k for Γ is denoted by $S_k(\Gamma)$.

Let us denote by Ω the sheaf of holomorphic differentials on $X(\Gamma)$ and let g denote the genus of $X(\Gamma)$. There is an isomorphism

$$S_2(\Gamma) \simeq H^0(X(\Gamma), \Omega).$$

Hence, in particular, the dimension of $S_2(\Gamma)$ as a $\mathbb{C}$-vector space is g. From now on, we will restrict ourselves to automorphic forms of weight 2.

6.1.2 The structure of the homology of a Shimura curve

Let Γ be an arithmetic Fuchsian group of the first kind attached to an indefinite quaternion $\mathbb{Q}$-algebra of discriminant $D > 1$. The homology group $H_1(X(\Gamma)(\mathbb{C}), \mathbb{R})$ contains the maximal lattice $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$. We will use the following result to study the structure of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{R})$.

Theorem 6.1.8 (Armstrong, [4])**.** *Let Γ be a group which acts simplicially on a simplicial complex U. Let E be the normal subgroup of Γ of elements with a fixed element in U. Given a point $\alpha \in U$ and $g \in \Gamma$, define $\phi_\alpha(g)$ as the homotopy class of an edge path joining α with $g(\alpha)$. Then, the map ϕ_α factors by a map $f_\alpha : \Gamma/E \to \pi_1(\Gamma\backslash U, \alpha)$, which is an isomorphism.*

□

Notice that Möbius transforms are conform; hence, they preserve geodesic triangles. In particular, arithmetic Fuchsian groups act simplicially on $\mathcal{H}$.

Theorem 6.1.9. *Let Γ be a cocompact arithmetic Fuchsian group of the first kind. Denote by E the set of elliptic elements of Γ. Let Γ' be the commutator subgroup of Γ. Fix $\alpha \in \mathcal{H}$. For any $g \in \Gamma$, define $\phi_\alpha(g) = \{\alpha, g(\alpha)\}_\Gamma \in H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$. Then, the following sequence of groups is exact:*

$$0 \to \Gamma' E \to \Gamma \stackrel{\phi_\alpha}{\to} H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z}) \to 0,$$

and the map ϕ_α is independent of α.

Proof. For any $z, w \in \mathcal{H}$, we will denote the homology class $\{z, w\}_\Gamma$ simply by $\{z, w\}$. First, we check that for any $\alpha \in \mathcal{H}$, ϕ_α is a group homomorphism. Thus, take $g, h \in \Gamma$. Since $\mathcal{H}$ is simply connected, we have

$$\{\alpha, gh(\alpha)\} = \{\alpha, g(\alpha)\} + \{g(\alpha), gh(\alpha)\} = \{\alpha, g(\alpha)\} + \{\alpha, h(\alpha)\},$$

hence, ϕ_α is a group homomorphism.

Next, we check the independency on α. Let $\alpha, \beta \in \mathcal{H}$. We can decompose

$$\phi_\alpha(g) = \{\alpha, \beta\} + \{\beta, g(\beta)\} + \{g(\beta), g(\alpha)\} = \{\alpha, \beta\} + \{\beta, g(\beta)\} + \{\beta, \alpha\} = \phi_\beta(g).$$

We claim that the commutator subgroup of Γ/E is $\Gamma' E/E$. To see this, let us consider the projection $p : \Gamma \to \Gamma/E$, which sends Γ' onto $\Gamma' E/E$. Hence, it induces a projection $\overline{p} : \Gamma/\Gamma' \to \Gamma/\Gamma' E$, so that $\Gamma/\Gamma' E \simeq (\Gamma/E)/(\Gamma' E/E)$ is abelian. Thus, $(\Gamma/E)' \subseteq \Gamma' E/E$. On the other hand, for any $g, h \in \Gamma$, one has, by normality of E, that $ghg^{-1}h^{-1}E = gEhE(gE)^{-1}(hE)^{-1}$. This shows the reverse inclusion. In particular, there is an isomorphism $\psi : H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z}) \to \Gamma/\Gamma' E$.

Consider the commutative diagram

$$\begin{array}{ccccc} \Gamma & \stackrel{\phi_\alpha}{\longrightarrow} & H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z}) & & \\ \downarrow & & \downarrow \psi & & \\ \Gamma/E & \longrightarrow & (\Gamma/E)/(\Gamma' E/E) & \longrightarrow & 0. \end{array}$$

It follows that $\mathrm{Ker}(\phi_\alpha) = \Gamma' E$; thus, the result follows. □

From now on, we denote by L the kernel of the map ϕ. Let G be a set of generators of Γ. Denote by $H(G)$ the set of elements of G not belonging to L.

Definition 6.1.10. Let $\tau \in \mathcal{H}$ be a quadratic imaginary point. A family of quadratic distinguished classes attached to τ is

$$\{\{\tau, \sigma(\tau)\}_\Gamma\}_{\sigma \in H(G)},$$

with G a set of generators of Γ.

Proposition 6.1.11. *Any class in $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$ can be represented as a sum of quadratic distinguished classes. In particular, quadratic distinguished classes generate $H_1(X(\Gamma)(\mathbb{C}), \mathbb{R})$ as a real vector space.*

Proof. By Theorem 6.1.9, for any class in $\omega \in H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$ there exists some $g \in \Gamma$ such that $\omega = \{\tau, g(\tau)\}_\Gamma$. Decompose $g = \eta_1 \cdots \eta_l$ where the η_k are generators of Γ. Notice that

$$\{\tau, g(\tau)\}_\Gamma = \{\tau, \eta_1(\tau)\}_\Gamma + \{\eta_1(\tau), g(\tau)\}_\Gamma = \{\tau, \eta_1(\tau)\}_\Gamma + \{\tau, \eta_2\eta_3 \cdots \eta_l(\tau)\}_\Gamma.$$

Iterating, we have

$$\{\tau, g(\tau)\}_\Gamma = \sum_{k=1}^{l} \{\tau, \eta_k(\tau)\}_\Gamma.$$

If $\eta_k \notin H(G)$, we can consider its fixed point $\tau_{\eta_k} \in \mathcal{H}$ and have

$$\{\tau, \eta_k(\tau)\}_\Gamma = \{\tau, \tau_{\eta_k}\} + \{\tau_{\eta_k}, \eta_k(\tau)\}_\Gamma = \{\tau, \tau_{\eta_k}\} + \{\eta_k(\tau_{\eta_k}), \eta_k(\tau)\}_\Gamma,$$

which vanishes, by Γ-invariance. □

Remark 6.1.12. For any arithmetic Fuchsian group of the first kind Γ, it is possible to find a set of generators of Γ of the form $\{\eta_1, ..., \eta_{2g}, \varepsilon_1, ..., \varepsilon_t\}$ with ε_j elliptic, parabolic or belonging to the commutator subgroup, and η_k hyperbolic for any j, k (see [71]). Thus, the set $\{\{\tau, \eta_1(\tau)\}, ..., \{\tau, \eta_{2g}(\tau)\}\}$ is a basis of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$. The following examples illustrate this fact numerically.

Examples 6.1.13. In chapter 5, we have showed numerically Proposition 6.1.11 for modular curves. For an example in the cocompact case, we can look at the Shimura curves $X(D,N)$: for instance, the curve $X(6,1)$, which has genus 0 and $\Gamma(6,1)$ can be generated by six elliptic matrices. The curve $X(10,1)$ has genus 0 and $\Gamma(10,1)$ can be generated by three elliptic matrices. The Shimura curve $X(15,1)$ has genus 1 and $\Gamma(15,1)$ has the following minimal set of generators:

$$\alpha = \frac{1}{2}\begin{pmatrix} 3 & 1 \\ 5 & 3 \end{pmatrix}, \; h = \begin{pmatrix} 2+\sqrt{3} & 0 \\ 0 & 2-\sqrt{3} \end{pmatrix}, \; \beta = \frac{1}{2}\begin{pmatrix} 1+2\sqrt{3} & 3-2\sqrt{3} \\ 15+10\sqrt{3} & 1-2\sqrt{3} \end{pmatrix}.$$

The matrices α, h are hyperbolic and β is elliptic of order 6. All these affirmations can be checked at [1].

Remark 6.1.14. Apart from Theorem 6.1.9, and from the fact that

$$H_1\left(X(\Gamma)(\mathbb{C}), \mathbb{Z}\right) \cong \mathbb{Z}^{2g},$$

where g is the genus of $X(\Gamma)$, saying something more precise about the structure of the homology of $X\left(\Gamma\right)\left(\mathbb{C}\right)$ seems a difficult task. In some cases, it is possible to find a presentation of the group Γ consisting of a set of matrices not belonging to L together with some relations involving certain commutators (see [71]). In [23], an algorithm is given to find a presentation for congruence groups, and in [1] and [73] an algorithm is given which produces a presentation for arithmetic Fuchsian groups and fundamental domains for the corresponding actions on $\mathcal{H}$.

Fix $\tau \in \mathcal{H}^*$ ($\tau \in \mathcal{H}$ if Γ is cocompact). By virtue of Theorem 6.1.9 and the above remark, given $\omega \in H_1\left(X\left(\Gamma\right)\left(\mathbb{C}\right), \mathbb{Z}\right)$ there exists $g \in \Gamma$ such that $\omega = \{\tau, g(\tau)\}_\Gamma$. In the modular case, in addition to Theorem 6.1.9, we can use the Manin continued fraction trick, which allows us to decompose ω as a $\mathbb{Z}$-linear combination of a family of non-closed paths, namely, the Manin distinguished classes (see [45]). We look for an algorithm which decomposes g as a product of elements in a fixed set of generators of Γ such that we can express ω as a $\mathbb{Z}$-linear combination of certain distinguished closed paths. We develop this algorithm for the finite family of all the arithmetic Fuchsian groups of signature $(1; e)$. Additionally, we give an algorithm which decomposes matrices of $\mathrm{SL}\left(2, \mathbb{Z}\right)$ as products of powers of the generators $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in cubic polynomial time. It is different from the classical one, which uses the euclidean algorithm (see [27], for instance). Our algorithm resembles the Manin continued fraction trick, but it is based on a quadratic imaginary point instead of the cusp $i\infty$.

6.1.3 Arithmetic Fuchsian group of signature $(1; e)$

Recall that all the fundamental domains for Γ have the same number of non-accidental elliptic cycles (see [1]).

Definition 6.1.15. The signature of Γ is the $(r+1)$-tuple $(g; e_1, \ldots, e_r)$, where g is the genus of $X\left(\Gamma\right)$, r is the number of non-equivalent non-

accidental elliptic cycles, and for any elliptic cycle $\mathcal{E}_k$, e_k is the integer such that the sum of angles of the vertices of $\mathcal{E}_k$ equals $\frac{2\pi}{e_k}$.

For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, if g is not a homothety then denote by $I(g)$ the isometry circle of g, namely, the set $\{z \in \mathcal{H} : |cz + d| = 1\}$. If g is a homothety of factor λ then define $I(g) = \{z \in \mathcal{H} : |\lambda z| = 1\}$. Denote by $\mathrm{Ext}(I(g))$ the exterior of $I(g)$ and by $\mathrm{Int}(I(g))$ the complement of $\mathrm{Ext}(I(g))$. For any $\lambda \in \mathbb{R}$, $\lambda > 0$, denote

$$S(\lambda) = \{z \in \mathcal{H} : \lambda^{-1} \leq |z| \leq \lambda\}.$$

If h is a homothety, notice that the isometry circles of h and h^{-1} are parallel in the hyperbolic metric. Sometimes (cf. [1]), it is possible to find a system of generators G of Γ such that one of them is a hyperbolic homothety h of factor λ and a fundamental domain of the form

$$\mathcal{F} = \bigcap_{g \in G \setminus \{h, h^{-1}\}} \mathrm{Ext}(I(g)) \cap S(\lambda).$$

We will call $S(\lambda)$ the fundamental strip of $\mathcal{F}$. We can construct such a fundamental domain, for instance, when Γ is one of the 73 arithmetic Fuchsian groups of signature $(1; e)$ which were classified by Takeuchi in [71]. These arithmetic Fuchsian groups admit a presentation of the form $\Gamma = \langle \alpha, \beta : (\alpha\beta\alpha^{-1}\beta^{-1})^e = \pm 1 \rangle$, where $\alpha, \beta \notin L$ are hyperbolic elements.

Proposition 6.1.16 (Sijsling, [69])**.** *Let Γ be a cocompact arithmetic Fuchsian group of signature $(1; e)$ generated by α and β. Then, after a change of variables, we can suppose that α is a homothety of factor λ and $\beta = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Furthermore, the hyperbolic rectangle $\mathcal{F} = S(\lambda) \cap \mathrm{Ext}(I(\beta)) \cap \mathrm{Ext}(I(\beta^{-1}))$ is a fundamental domain.*

Let Γ be a cocompact arithmetic Fuchsian group of signature $(1; e)$ generated by α, β. Given $\omega \in H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$, by Theorem 6.1.9, we know that, for any $\tau \in \mathcal{H}$, there exists $g \in \Gamma$ such that $\omega = \{\tau, g(\tau)\}_\Gamma$. Since quadratic imaginary points contained in $\mathcal{H}$ are dense in $\mathcal{H}$, we will suppose, without loss of generality, that τ is a quadratic imaginary point contained in the interior of $\mathcal{F}$. The paths $\omega_\alpha = \{\tau, \alpha(\tau)\}_\Gamma$ and $\omega_\beta = \{\tau, \beta(\tau)\}_\Gamma$ form a $\mathbb{Z}$-basis of $H_1(X(\Gamma)(\mathbb{C}), \mathbb{Z})$. Our aim is to decompose explicitly $\omega = n_\alpha\omega_\alpha + n_\beta\omega_\beta$, with

$n_\alpha, n_\beta \in \mathbb{Z}$. To do this, it is enough to express g as a product of powers of α and β. The idea is to multiply g by the left by a suitable sequence of matrices $\{g_{k_j}\}$, with g_{k_j} a power of α or β to obtain a product $g_{k_1} \cdots g_{k_n} g$, such that $g_{k_1} \cdots g_{k_n} g(\tau)$ belongs to the interior of $\mathcal{F}$. In this case, $g = (g_{k_1} g_{k_2} \cdots g_{k_n})^{-1}$. Observe that the decomposition of g as a product of generators is not unique in general.

Lemma 6.1.17. *Suppose that $\lambda \geq 1$. Then, for any $z \in \mathcal{H}$ there exists an integer N such that $\lambda^{-1} \leq |\alpha^N(z)| \leq \lambda$.*

Proof. If $|z| > \lambda$ then take

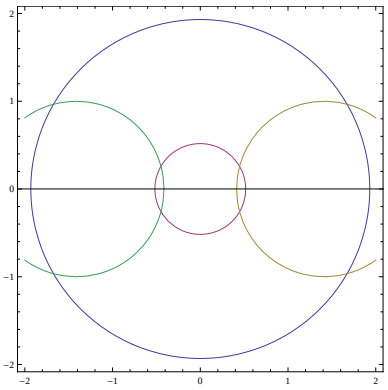
$$N := \min\{n \in \mathbb{N} \mid \quad |\lambda^{-2n} z| \leq \lambda\}.$$

Since $\alpha^{-N}(z) = \lambda^{-2N} z$, if $\lambda^{-1} \leq |\lambda^{-2n} z|$, then, we would have finished. Otherwise, if $\lambda^{-1} > |\lambda^{-2n} z|$, it would follow, multiplying by λ^2, that

$$\lambda > \lambda^2 \cdot |\lambda^{-2n} z| = |\lambda^{-2(n-1)} z|,$$

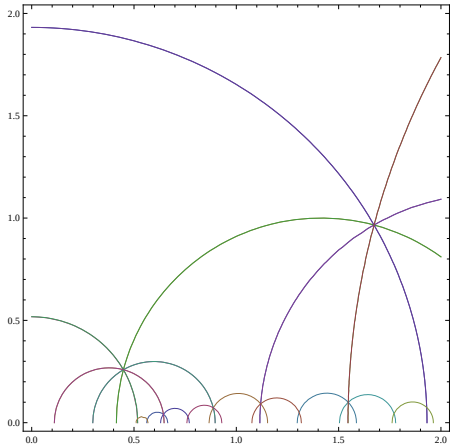
a contradiction taking into account the choice of n. The case when $|z| \leq \lambda^{-1}$ is analogue. □

The following graph shows a fundamental domain for the curve of signature $(1; 2)$, labelled $e2d1D6ii$ in [69].



Fundamental domain in the upper half-plane for Γ

Define the sets of tranformations $\Gamma^+ = \{\beta, \beta\alpha, \beta\alpha^{-1}, \beta\alpha\beta^{-1}, \beta\alpha^{-1}\beta^{-1}\}$ and $\Gamma^- = \{\beta^{-1}, \beta^{-1}\alpha, \beta^{-1}\alpha^{-1}, \beta^{-1}\alpha\beta^{-1}, \beta^{-1}\alpha^{-1}\beta^{-1}\}$. They will play an important role in our algorithm. The following graph shows a detail of the right region, in which we have depicted the translates of $\mathcal{F}$ by the elements of Γ^+.



Denote by S^+ the right region of the strip $S(\lambda)$ which excludes $\mathcal{F}$, and by S^- the left portion, which is symmetric to S^+ with respect to the vertical axis. Denote by R^+ and R^- the regions covered by the translate of $\mathcal{F}$ under iterated applications of the transformations in Γ^+ or Γ^-, respectively. Namely,

$$R^+ = \bigcup_{n\geq 1} \bigcup_{\gamma_{j_k}\in\Gamma^+} \gamma_{j_n}\gamma_{j_{n-1}}\cdots\gamma_{j_1}(\mathcal{F}).$$

The following statement is straightforward to prove and it is geometrically illustrated by the above figure.

Lemma 6.1.18. *If $R = R^+$ or $R = R^-$, then,*

$$M = \sup\{\mathrm{Im}(z) : z \in \mathrm{Fr}(R) \setminus \mathrm{Fr}(\mathcal{F})\} < \inf\{\mathrm{Im}(z) : z \in \mathrm{Fr}(\mathcal{F})\}.$$

□

The following result will also be used to prove the correctness of our algorithm.

Lemma 6.1.19. $S^+ = R^+$.

Proof. First of all, let us check that, for any $n \geq 1$, $\gamma_{j_n}\gamma_{j_{n-1}}\cdots\gamma_{j_1}(\mathcal{F}) \subseteq S^+$. For $n = 1$ it has been already checked. Suppose that it is true for certain n. To see that it is also true for $n+1$ it suffices to observe again that the five

transforms of Γ^+ preserve S^+. To see the reciprocal containment, define the sequence

$$h_n = \sup\left\{ \mathrm{Im}(z) : z \in \bigcup_{\gamma_{j_k} \in \Gamma^+} \gamma_{j_n}\gamma_{j_{n-1}}\cdots\gamma_{j_1}(\mathcal{F}) \right\}.$$

It is easy to see that, for any $\gamma \in \Gamma^+$ and for any $z \in S^+$, $\mathrm{Im}(\gamma(z)) < \mathrm{Im}(z)$. Lemma 6.1.18 implies that $h_{n+1} < h_n$ for any $n \geq 1$. Since $\{h_n\}_{n\geq 0}$ is a decreasing sequence and $h_n > 0$ for any $n \geq 1$, it is convergent. However, if the limit were nonzero, then there would exist an accumulation point in $\mathcal{H}$ of a sequence $\{\gamma_n(z)\} \subseteq \mathcal{H}$ with $\gamma_n \in \Gamma$ and $z \in \mathcal{F}$. Since Γ acts properly discontinuously on $\mathcal{H}$, this would be a contradiction. □

Algorithm 6.1.20. Let $g \in \Gamma$ such that $g(\tau) \notin S$. Define $N(g) \in \mathbb{Z}$ such that $\lambda^{-1} \leq |\alpha^{N(g)}(z)| \leq \lambda$. We propose the following algorithm:

Require: $g \in \Gamma$;
  $\gamma \leftarrow g, n_\alpha \leftarrow 0, n_\beta \leftarrow 0$;
  $flag = false$;
  while $flag == false$ **do**
    if $\gamma(\tau) \notin S$ **then**
      $n_\alpha \leftarrow n_\alpha + N(g)$;
      $g \leftarrow \alpha^{N(g)} g$;
      $\gamma \leftarrow \gamma\alpha^{-N(g)}$;
    else
      if $\gamma(\tau) \in \mathcal{F}$ **then**
        $flag \leftarrow true$;
      end if
    end if
    if $\gamma(\tau) \in S^+$ **then**
      $n_\beta \leftarrow n_\beta + 1$;
      $g \leftarrow \beta^{-1} g$;
      $\gamma \leftarrow \gamma\beta$;
    end if
    if $\gamma(\tau) \in S^-$ **then**
      $n_\beta \leftarrow n_\beta - 1$;
      $g \leftarrow \beta g$;
      $\gamma \leftarrow \gamma\beta^{-1}$;
    end if

end while
return $\{n_\alpha, n_\beta\}$ such that $\{i, g(i)\} = n_\alpha\{i, \alpha(i)\} + n_\beta\{i, \beta(i)\}$.

Proof of correctness. If $g(\tau) \notin S$, then, left multiplication by α^m, for some m, brings $g(\tau)$ to, say, S^+. Then, by Lemma 6.1.19, we can write $\alpha^m g(\tau) = \gamma_{k_n} \cdots \gamma_{k_1}(\tau)$, where $\gamma_{k_j} \in \Gamma^+$. If $\gamma_{k_n} \neq \beta\alpha\beta^{-1}, \beta\alpha^{-1}\beta^{-1}$, then, we can write

$$\alpha^v \beta^{-1} \alpha^m g(\tau) = \gamma_{k_{n-1}} \cdots \gamma_{k_1}(\tau)$$

for some $v \in \mathbb{Z}$. This point belongs to S^+. If $\gamma_{k_n} = \beta\alpha\beta^{-1}$, then, we distinguish two cases. If $\gamma_{k_j} \neq \beta\alpha\beta^{-1}, \beta\alpha^{-1}\beta^{-1}$ for some $j \in \{1, \ldots, n-1\}$, then,

$$\beta^{-1}\alpha^v\beta^{-1}\alpha^m g(\tau) = \gamma_{k_{j-1}} \cdots \gamma_{k_1}(\tau) \in S^+.$$

Otherwise, $\alpha^v\beta^{-1}\alpha^m g(\tau) = \beta^{-1}(\tau) \in S^-$. The algorithm does n operations if $g = \gamma_{k_n} \cdots \gamma_{k_1}$. □

Examples 6.1.21. For $g = \begin{pmatrix} 6+3\sqrt{3} & 2\sqrt{2} \\ 2\sqrt{2} & 6-3\sqrt{3} \end{pmatrix}$, algorithm 6.1.20 returns $n_\alpha = n_\beta = 2$. In fact, $g = \alpha\beta^2\alpha$.

6.1.4 An alternative algorithm for the modular case.

We develop a procedure which, given a matrix $g \in \mathrm{SL}(2,\mathbb{Z})$, gives a factorization of g in terms of S and T. There is an explicit method which uses the euclidean algorithm. We compare g with the elements of a sequence of products of matrices acting on the imaginary unit in such a way that this sequence can be understood as the convergents of a certain continued fraction-like expansion. We start with $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. Since $(ST)^3 = Id$ and $S(i) = i$, we can suppose that

$$g = T^{n_k} S T^{n_{k-1}} S \cdots T^{n_2} S T^{n_1},$$

with $n_1, \ldots, n_k$ to be determined. We want to express $\omega = \{i, g(i)\}_{\Gamma_0(N)}$ as a $\mathbb{Z}$-linear combination of the form

$$\omega = \{i, ST^{n_1}(i)\} + \sum_{j=1}^{k-1} \{T^{n_j} S \cdots T^{n_1}(i), T^{n_{j+1}} S T^{n_j} S \cdots T^{n_1}(i)\}.$$

Define the following finite sequence:

$$g_1(i) = n_1 + i, \quad g_{m+1}(i) = n_{m+1} - \frac{1}{g_m(i)}.$$

Write $g_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix} \in \mathrm{SL}\,(2,\mathbb{Z})$. Notice that $g_{n_k}(i) = g(i)$. At the j-th step, $g_j(i)$ admits an explicit expression as an element of $\mathbb{Q}(i)$, which we call the j-th convergent. For instance, the first four convergents are

$$\begin{aligned}
g_1(i) &= n_1 + i, \\
g_2(i) &= \frac{n_2 i + (n_1 n_2 - 1)}{n_1 + i}, \\
g_3(i) &= \frac{(n_2 n_3 - 1)i + (n_1 n_2 n_3 - n_1 - n_3)}{n_2 i + (n_1 n_2 - 1)}, \\
g_4(i) &= \frac{(n_2 n_3 n_4 - n_2 - n_4)i + (n_1 n_2 n_3 n_4 - n_1 n_4 - n_3 n_4 - n_1 n_2 + 1)}{(n_2 n_3 - 1)i + (n_1 n_2 n_3 - n_1 - n_3)}.
\end{aligned}$$

For any $j = 2, \ldots, k$, notice that if $|a_j| > |c_j|$, the quotient $f_j = a_j/c_j$ can be written as $f_j = n_j - A_j/B_j$, where $A_j = B_{j-1}$, $B_j = n_{j-1}B_{j-1} - A_{j-1}$. We set $B_1 = 0$. Hence, for any $j \geq 2$, either A_j is coprime to B_j, or $A_j = \pm B_j$.

Algorithm 6.1.22. Given $a, b \in \mathbb{Z}$ with $b \neq 0$, denote by $\mathrm{Div}(a,b)$ the quotient of the euclidean division of a by b. We propose the following algorithm:

Require: $g \in \mathrm{SL}\,(2,\mathbb{Z})$;
  $\gamma \leftarrow g$;
  $v \leftarrow \emptyset$;
  while $\gamma \neq Id, S$ **do**
    if $|\gamma[1,1]| < |\gamma[2,1]|$ **then**
      $\gamma \leftarrow S\gamma$;
      $h \leftarrow hS$;
    else
      $\gamma \leftarrow T^{-\mathrm{Div}(\gamma[1,1],\gamma[2,1])}\gamma$;
      $v \leftarrow v \cup \{\mathrm{Div}\,(\gamma[1,1], \gamma[2,1])\}$;
    end if
  end while
  return $v = \{n_k, \ldots, n_1\}$ such that $g(i) = T^{n_k} S \cdots T^{n_1}(i)$.

Proof of correctness. If $c = 0$ then g is a translation. If $|a| > |c|$, the integer part of the quotient f_k gives the exponent n_k; otherwise, the upper-left entry of Sg is larger in absolute value than the lower-left entry. □

Examples 6.1.23. For $g = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$, algorithm 6.1.22 returns the ordered vector $v = \{-2, 3, 1\}$. Indeed, $g = -ST^{-2}ST^3ST$.

6.2 Modular symbols

6.2.1 Modular integrals

In what follows, Γ will denote an arithmetic Fuchsian group commensurable with Γ_H^1 for some quaternion $\mathbb{Q}$-algebra H.

Definition 6.2.1. Let f be an automorphic form of weight 2 for Γ and $\tau \in \mathcal{H}$ a quadratic imaginary point. The modular integral attached to f and τ is the map

$$\begin{array}{rccc} \phi_f^\tau : & \Gamma_H^1 & \longrightarrow & \mathbb{C} \\ & \gamma & \mapsto & \displaystyle\int_{\gamma(\tau)}^{\tau} f. \end{array}$$

We will denote $\phi_f = \phi_f^i$ when $\tau = i$, the imaginary unit.

Remark 6.2.2. If $\Gamma = \Gamma_0(N)$ and instead of a quadratic imaginary point we consider $\tau = i\infty$, we have the classical modular integral as in [49].

Let Γ be an arithmetic Fuchsian group of the first kind commensurable with Γ_H^1 for some quaternion $\mathbb{Q}$-algebra H. In particular, there is a finite number of coset representatives of $(\Gamma_H^1 \cap \Gamma)\backslash\Gamma_H^1$.

Lemma 6.2.3. *Let $f \in S_2(\Gamma)$ and let $A, \gamma \in \mathrm{GL}(2,\mathbb{R})^+$. Then*

$$\phi_f^\tau(A\gamma) = \phi_{f|A}^\tau(\gamma) + \phi_f^\tau(A),$$

where $\phi_{f|A}^\tau(\gamma) = \int_{\gamma(\tau)}^{\tau} f|A$.

Proof. Since $dA(z) = \rho(A,z)^2 dz$, we can write

$$\phi_{f|A}^\tau(\gamma) = \int_{\gamma(\tau)}^{\tau} \rho(A,z)^2 f(A(z))dz = \int_{A\gamma(\tau)}^{A(\tau)} f(w)dw.$$

Since f is holomorphic in the upper half-plane, the integral along the triangle with vertices $A(\tau)$, $A\gamma(\tau)$ and τ vanishes. Hence

$$\phi_{f|A}^\tau(\gamma) = \int_{A\gamma(\tau)}^{\tau} f(z)dz + \int_{\tau}^{A(\tau)} f(z)dz,$$

and the result holds. □

Proposition 6.2.4. *The $\mathbb{Z}$-module Σ_f^τ spanned by the modular integrals $\phi_f^\tau(\gamma)$ as $\gamma \in \Gamma_H^1$ is finitely generated and torsion-free. Given G a minimal set of generators of Γ, then*

$$\mathrm{rk}\left(\Sigma_f^\tau\right) \leq \mathrm{card}\,(G) + \left[\Gamma_H^1 : \Gamma \cap \Gamma_H^1\right].$$

Proof. Let $\{A_l\}_{1\leq l\leq n}$ be a set of coset representatives of $(\Gamma \cap \Gamma_H^1)\backslash\Gamma_H^1$ and let $G = \{B_j\}_{1\leq j\leq m}$ be a minimal set of generators of Γ. Let $A \in \Gamma_H^1$. There exists $B \in \Gamma \cap \Gamma_H^1$ and $l_0 \in \{1, ..., n\}$ such that $A = BA_{l_0}$. Hence

$$\phi_f^\tau(BA_{l_0}) = \phi_{f|B}^\tau(A_{l_0}) + \phi_f^\tau(B) = \phi_f^\tau(A_{l_0}) + \phi_f^\tau(B).$$

Now, write $B = B_{j_1}...B_{j_r}$ with $\{j_1, ..., j_r\} \subseteq \{1, ..., m\}$. Hence

$$\phi_f^\tau(B) = \phi_f^\tau(B_{j_2}...B_{j_r}) + \phi_f^\tau(B_{j_1}),$$

and hence, $\phi_f^\tau(A)$ belongs to the $\mathbb{Z}$-module spanned by the modular integrals $\phi_f^\tau(A_l)$ and $\phi_f^\tau(B_j)$ as $1 \leq l \leq n$ and $1 \leq j \leq m$. □

6.2.2 Classical modular symbols

We begin by recalling the following

Definition 6.2.5 (Manin [45], Pollack-Stevens [56])**.** A $\mathbb{C}$-valued modular symbol is a map F from the set $\mathrm{P}^1(\mathbb{Q}) \times \mathrm{P}^1(\mathbb{Q})$ to $\mathbb{C}$ such that for any $P, Q, R \in \mathrm{P}^1(\mathbb{Q})$,

$$F(P, Q) = F(P, R) + F(R, Q).$$

Let $\mathcal{D} := \mathrm{Div}(\mathbb{P}^1(\mathbb{Q}))$ be the group of divisors supported on the rational cusps $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{i\infty\}$ or in $i\infty$, and let $\mathcal{D}_0 \subset \mathcal{D}$ be the subgroup of divisors of degree zero. Denote by $\mathrm{Symb}\,(\mathcal{D}_0, \mathbb{C})$ the $\mathbb{C}$-vector space of $\mathbb{C}$-valued modular symbols.

Equivalently, $\mathrm{Symb}\,(\mathcal{D}_0, \mathbb{C}) = \mathrm{Hom}_{\mathbb{Z}}\,(\mathcal{D}_0, \mathbb{C})$. Notice that $\Gamma_0(N)$ acts by the left on $\mathrm{Symb}\,(\mathcal{D}_0, \mathbb{C})$. The $\mathbb{C}$-vector space of $\Gamma_0(N)$-invariant modular symbols will be denoted by $\mathrm{Symb}\,(\mathcal{D}_0, \mathbb{C})^{\Gamma_0(N)}$.

Via Theorem 6.1.9 and the Manin continued fraction trick, one can constructively show (cf. [24]) that any closed path $\omega \in H_1\left(X\left(\Gamma_0(N)\right)(\mathbb{C}), \mathbb{Z}\right)$ can be expressed as a $\mathbb{Z}$-linear combination of paths of the form $\{g(0), g(i\infty)\}$,

with $g \in \mathrm{SL}(2,\mathbb{Z})$. These paths are called Manin distinguished classes and they suffice to determine a modular symbol. The $\mathbb{C}$-valued modular symbols supported on the Manin distinguished classes are normally referred to as Manin symbols.

The action of the Hecke algebra on $\mathrm{Symb}(\mathcal{D}_0,\mathbb{C})^{\Gamma_0(N)}$ is determined by the following double coset decomposition (cf. [24], Proposition 1.6):

(i) If $p \nmid N$, then

$$\Gamma_0(N)\backslash\Gamma_0(N)\begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}\Gamma_0(N) = \bigcup_{u=0}^{p-1}\Gamma_0(N)\begin{pmatrix} 1 & u \\ 0 & p\end{pmatrix}\Gamma_0(N)\bigcup\begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}\Gamma_0(N).$$

(ii) If $p|N$, then

$$\Gamma_0(N)\backslash\Gamma_0(N)\begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}\Gamma_0(N) = \bigcup_{u=0}^{p-1}\begin{pmatrix} 1 & u \\ 0 & p\end{pmatrix}\Gamma_0(N).$$

Later on, we will refer to this decomposition as the s*tandard right coset decomposition* for T_p. For $x, y \in \mathcal{H}^*$, denote by $\{x,y\}$ the class $\{x,y\}_\Gamma$. The action of T_p on classes of paths is:

(i) if $p \nmid N$, then

$$\{g(0), g(i\infty)\}|_{T_p} = \sum_{u=0}^{p-1}\{(g(0)+u)p^{-1}, (g(i\infty)+u)p^{-1}\}+\{pg(0), pg(i\infty)\}.$$

(ii) If $p|N$, then

$$\{g(0), g(i\infty)\}|_{T_p} = \sum_{u=0}^{p-1}\{(g(0)+u)p^{-1}, (g(i\infty)+u)p^{-1}\}.$$

Notice that, since T_p acts on $\mathrm{P}^1(\mathbb{Q})$, it is again possible to decompose each path in the above sum as a $\mathbb{Z}$-linear combination of Manin paths.

Remark 6.2.6. If K is a field, denote by K^{alg} an algebraic closure of K. Fix compatible embeddings of $\mathbb{Q}$ in $\mathbb{Q}^{alg}$ and in $\mathbb{Q}_p^{alg}$. By Proposition 6.2.4, given $f \in S_2(\Gamma_0(N))$, the classical modular integral attached to f can be seen as a modular symbol with values in $\mathbb{C}$ or in a finite dimensional $\mathbb{Q}_p$-vector space.

An important application of classical modular symbols is the explicit computation of spaces of modular forms. This topic is treated in detail in [24]. In particular, one has the following result:

Proposition 6.2.7 (Pollack-Stevens [56]). *There exists an injection as Hecke-modules*

$$S_2\left(\Gamma_0(N)\right) \hookrightarrow \mathrm{Symb}\left(\mathcal{D}_0, \mathbb{C}\right)^{\Gamma_0(N)}.$$

The method for computing modular forms consists in the determination of the eigenvalues of the Hecke operators acting on $\mathrm{Symb}\left(\mathcal{D}_0, \mathbb{C}\right)^{\Gamma_0(N)}$. These eigenvalues determine spaces of newforms for $\Gamma_0(N)$. The Manin continued fraction trick grants that it is easy to determine the eigenvalues by working on modular symbols. Hence, the Fourier expansion at infinity of such an eigenform has as n-th Fourier coefficient the computed eigenvalue for T_n.

6.2.3 Ash-Stevens cohomological interpretation of the modular symbols

In this and in the next section, we will use some ideas from the theory of spectral sequences and topological pairs. For general facts on the first topic, we refer the reader to [21], and for the second, to [33].

Set $\Gamma := \Gamma_0(N)$ and let R be a commutative ring such that the order of every torsion element of Γ is invertible in R and let E be an $R[\Gamma]$-module. We can identify $X(\Gamma)(\mathbb{C})$ with $\Gamma\backslash\mathcal{H}^*$. Denote $Y(\Gamma)(\mathbb{C}) := \Gamma\backslash\mathcal{H}$. Let $\widetilde{E}$ be the local coefficient system on $X(\Gamma)(\mathbb{C})$ associated to E.

Theorem 6.2.8 (Ash-Stevens, [5]). *For any $i \in \mathbb{N}$, we have the following commutative diagram with exact rows:*

$$\begin{array}{ccccc}
H^i\left(\left(X(\Gamma)(\mathbb{C}), X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C})\right), \widetilde{E}\right) & \longrightarrow & H^i\left(X(\Gamma)(\mathbb{C}), \widetilde{E}\right) & \longrightarrow & H^i\left(X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C}), \widetilde{E}\right) \\
\downarrow & & \downarrow & & \downarrow \\
H^{i-1}(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_0, E)) & \longrightarrow & H^i(\Gamma, E) & \longrightarrow & H^i(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}, E)),
\end{array}$$

where the vertical arrows are isomorphisms.

Proof. First of all, set $A := \mathcal{H}^* \setminus \mathcal{H}$. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
Q & \hookrightarrow & H^0(\mathcal{H}^*, E) & \longrightarrow & H^0(A, E) & \longrightarrow & H^1\left((\mathcal{H}^*, A), E\right) & \longrightarrow & H^1(\mathcal{H}^*, E) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_{\mathbb{Z}}(K, E) & \hookrightarrow & \mathrm{Hom}_{\mathbb{Z}}\left(H_0\left(\mathcal{H}^*\right), E\right) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}\left(H_0\left(A\right), E\right) & \longrightarrow & G_1 & \longrightarrow & G_2
\end{array}$$

where

$$\begin{aligned} Q &:= H^0\left((\mathcal{H}^*, A), E\right), \quad K := H_0\left((\mathcal{H}^*, A)\right), \\ G_1 &:= \mathrm{Hom}_{\mathbb{Z}}(H_1\left((\mathcal{H}^*, A), E\right)) \oplus \mathrm{Ext}^1_{\mathbb{Z}}\left(H_0\left((\mathcal{H}^*, A)\right), E\right), \\ G_2 &:= \mathrm{Hom}_{\mathbb{Z}}(H_1\left(\mathcal{H}^*\right), E) \oplus \mathrm{Ext}^1_{\mathbb{Z}}\left(H_0\left(\mathcal{H}^*\right), E\right). \end{aligned}$$

Moreover, the vertical arrows in the above diagram are the isomorphisms given by the universal coefficients theorem for cohomology. In addition, we must underline that the following facts hold.

(i) $Q = 0$. Indeed, observe that

$$H_0\left((\mathcal{H}^*, A)\right) = \mathrm{Coker}\left(H_0(A) \xrightarrow{i_*} H_0(\mathcal{H}^*) \right).$$

Since the boundary components of $\mathcal{H}^*$ are in one-one correspondence with $\mathbb{P}^1(\mathbb{Q})$ it follows that $H_0(A) \cong \mathcal{D}$. Moreover, $H_0(\mathcal{H}^*) \cong \mathbb{Z}$ since $\mathcal{H}^*$ is pathwise connected. With these identifications in mind, i_*, which is the map induced in homology by the inclusion $A \xhookrightarrow{i} \mathcal{H}^*$, can be identified with the degree map $\mathcal{D} \longrightarrow \mathbb{Z}$, which is clearly surjective. Hence $H_0((\mathcal{H}^*, A), E) = H_0\left((\mathcal{H}^*, A)\right) \otimes E \cong 0$.

(ii) $\mathrm{Hom}_{\mathbb{Z}}(H_0(\mathcal{H}^*), E) \cong E$. Indeed, this fact is obvious because $\mathcal{H}^*$ is pathwise connected.

(iii) $\mathrm{Ext}^1_{\mathbb{Z}}\left(H_0\left(\mathcal{H}^*\right), E\right) = 0$. Indeed, as $\mathcal{H}^*$ is pathwise connected and $\mathbb{Z}$ is projective it follows that

$$\mathrm{Ext}^1_{\mathbb{Z}}\left(H_0\left(\mathcal{H}^*\right), E\right) = \mathrm{Ext}^1_{\mathbb{Z}}\left(\mathbb{Z}, E\right) = 0.$$

(iv) $H_1\left(\mathcal{H}^*\right) = 0$. Indeed, as $\mathcal{H}^*$ is pathwise connected $H_1\left(\mathcal{H}^*\right)$ is the abelianization of the first fundamental group $\pi_1(\mathcal{H}^*)$. But $\pi_1(\mathcal{H}^*) \cong 1$ because $\mathcal{H}^*$ is simply connected.

In this way, combining all these facts, the above diagram becomes the following commutative diagram with exact rows and vertical isomorphisms.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(\mathcal{H}^*, E) & \longrightarrow & H^0(A, E) & \longrightarrow & H^1\left((\mathcal{H}^*, A), E\right) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}, E) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_0, E) & \longrightarrow & 0. \end{array}$$

Applying to the above diagram the left exact functor $(-)^{\Gamma}$ we obtain the following commutative diagram with exact rows and vertical isomorphisms.

$$\begin{array}{ccccc} H^i(\Gamma, H^0(\mathcal{H}^*, E)) & \longrightarrow & H^i(\Gamma, H^0(A, E)) & \longrightarrow & H^i\left(\Gamma, H^1\left((\mathcal{H}^*, A), E\right)\right) \\ \downarrow & & \downarrow & & \downarrow \\ H^i(\Gamma, E) & \longrightarrow & H^i(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}, E)) & \longrightarrow & H^i(\Gamma, \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_0, E)). \end{array}$$

Thus, we only need to check, for each $i \in \mathbb{N}$, that

$$H^i(\Gamma, H^0(\mathcal{H}^*, E)) \cong H^i(X(\Gamma)(\mathbb{C}), \widetilde{E}),$$
$$H^i(\Gamma, H^0(A, E)) \cong H^i(X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C}), \widetilde{E}), \text{ and}$$
$$H^i(\Gamma, H^1\left((\mathcal{H}^*, A), E\right)) \cong H^{i+1}\left(\left(X\left(\Gamma\right)(\mathbb{C}), X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C})\right), \widetilde{E}\right).$$

Now, consider the following Grothendieck spectral sequences.

$$H^i(\Gamma, H^j(\mathcal{H}^*, E)) \underset{i}{\Longrightarrow} H^{i+j}(X(\Gamma)(\mathbb{C}), \widetilde{E}),$$
$$H^i(\Gamma, H^j(A, E)) \underset{i}{\Longrightarrow} H^{i+j}(X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C}), \widetilde{E}), \text{ and}$$
$$H^i(\Gamma, H^j((\mathcal{H}^*, A)\,, E)) \underset{i}{\Longrightarrow} H^{i+j}((X(\Gamma)(\mathbb{C}), X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C})), \widetilde{E}).$$

We start by analysing the first one. The foregoing calculations show, in particular, that $H^j(\mathcal{H}^*, E) = 0$ for all $j \neq 0, 2$. This fact implies that the source or the target of any differential of the E_2-page of this spectral sequence is zero and therefore it collapses, providing an isomorphism

$$H^i(\Gamma, H^j(\mathcal{H}^*, E)) \cong H^{i+j}(X(\Gamma)(\mathbb{C}), \widetilde{E}),$$

for any $(i, j) \in \mathbb{N}^2$. Let us move on to the second spectral sequence. Again by the foregoing, $H^j(A, E) = 0$ for all $j \neq 0$. Thus, this spectral sequence has just one non-zero row; hence it collapses, yielding an isomorphism

$$H^i(\Gamma, H^j(A, E)) \cong H^{i+j}(X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C}), \widetilde{E}),$$

for each $(i, j) \in \mathbb{N}^2$. Bearing in mind that $H^j((\mathcal{H}^*, A)\,, E) = 0$ for all $j \neq 1$, a similar argument implies that, for each $(i, j) \in \mathbb{N}^2$, there is an isomorphism

$$H^i(\Gamma, H^1\left((\mathcal{H}^*, A), E\right)) \cong H^{i+1}\left(\left(X(\Gamma)(\mathbb{C}), X(\Gamma)(\mathbb{C}) \setminus Y(\Gamma)(\mathbb{C})\right), \widetilde{E}\right),$$

which is what we wanted to show. □

Notice that, in particular, $H^i(\Gamma, H^1\left((\mathcal{H}^*, A), E\right)) \cong H_c^{i+1}(Y(\Gamma)(\mathbb{C}), \widetilde{E})$.

6.2.4 Quadratic modular symbols

Let Γ be an arbitrary arithmetic Fuchsian group of the first kind which is commensurable with Γ_H^1 for some quaternion $\mathbb{Q}$-algebra H. Fix $\tau \in \mathcal{H}^*$ ($\tau \in \mathcal{H}$ if Γ is cocompact). Let p be a prime number and let $\omega_p \in \mathcal{O}_H$ be a quaternion of reduced norm p. Set $\gamma_p := \psi(\omega_p)$. We must recall (cf. [66]) that there exists $d \in \mathbb{N}$ such that

$$\left[\Gamma : \Gamma \cap \gamma_p \Gamma \gamma_p^{-1}\right] = d$$

and, therefore, there is a coset decomposition

$$\Gamma \gamma_p \Gamma = \bigcup_{a=1}^{d} \gamma_a \Gamma.$$

Set, for each $n \in \mathbb{N}$, $I_n := \{1, \ldots, d\}^n$. Moreover, for each $\mathbf{u} = (u_1, \ldots, u_n) \in I_n$ set

$$\gamma_{\mathbf{u}} := \prod_{t=1}^{n} \gamma_{u_t}.$$

Finally, we define

$$\Delta_{\tau,p} := \bigcup_{n \geq 0} \bigcup_{\mathbf{u} \in I_n} \gamma_{\mathbf{u}} \Gamma^1 \tau.$$

The reason why we define $\Delta_{\tau,p}$ is that, on one hand, we are interested in considering integrals along geodesics connecting points of $\Gamma^1 \tau$ (classical modular symbols are integrals along geodesics connecting cusps), and, on the other hand, we want the action of the coset representatives given by the matrices γ_j to respect our module of values.

Proposition 6.2.9. *If $\tau = i\infty$, we have that $\Delta_{i\infty,p} = \mathbb{P}^1(\mathbb{Q})$.*

Proof. First, notice for any $a, b \in \mathbb{Z}$ coprime, there exists $x, y \in \mathbb{Z}$ such that $ax - by = 1$. Setting $\gamma = \begin{pmatrix} a & y \\ b & x \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, we have that $\gamma(i\infty) = a/b$, hence, $\mathrm{P}^1(\mathbb{Q}) = \mathrm{SL}(2,\mathbb{Z})\, i\infty$. Obviously, for any prime p, $\mathrm{SL}(2,\mathbb{Z})\, i\infty \subseteq \Delta_{i\infty,p}$. To see the other containment, it suffices to see that for any $0 \leq u \leq p$, and for any $r \in \mathbb{Q}$, $\frac{r+u}{p}$ can be expressed as $\gamma'(i\infty)$ for some $\gamma' \in \mathrm{SL}(2,\mathbb{Q})$. This is obvious, since $\frac{r+u}{p} \in \mathbb{Q}$. □

Let us suppose that Γ is cocompact and that τ is a quadratic imaginary point.

Consider the topological pair $(\mathcal{H}, \Delta_{\tau,p})$. We are interested in finding a result analogous to Theorem 6.2.8 in the quadratic setting.

Consider the inclusion $\Delta_{\tau,p} \overset{i}{\hookrightarrow} \mathcal{H}$ and, for any abelian group G, recall that

$$H_0\left((\mathcal{H}, \Delta_{\tau,p}), G\right) = \text{Coker}\left(H_0(\Delta_{\tau,p}, G) \xrightarrow{i_*} H_0(\mathcal{H}, G) \right),$$

where i_* is the map induced in 0-th homology by the inclusion i.

Consider the beginning of the long exact sequence in homology of the pair $(\mathcal{H}, \Delta_{\tau,p})$:

$$H_1(\mathcal{H}) \longrightarrow H_1((\mathcal{H}, \Delta_{\tau,p})) \longrightarrow H_0(\Delta_{\tau,p}) \xrightarrow{i_*} H_0(\mathcal{H}) \twoheadrightarrow H_0((\mathcal{H}, \Delta_{\tau,p})).$$

As $\mathcal{H}$ is simply connected, $H_1(\mathcal{H}) = 0$. On the other hand, as $\mathcal{H}$ is pathwise connected $H_0(\mathcal{H}) \cong \mathbb{Z}$ and therefore the map i_* is the map induced in homology by the degree map

$$\begin{aligned} C_0(\Delta_{\tau,p}) &\longrightarrow \mathbb{Z} \\ \sum_i b_i \sigma_i &\longmapsto \sum_i b_i. \end{aligned}$$

Here, $C_0(\Delta_{\tau,p})$ denotes the free abelian group of 0-dimensional singular simplices of $\Delta_{\tau,p}$. In this way, it follows from this fact that i_* is surjective. Hence we have the short exact sequence of abelian groups

$$0 \longrightarrow H_1((\mathcal{H}, \Delta_{\tau,p})) \xrightarrow{\partial_{\tau,p}} H_0(\Delta_{\tau,p}) \xrightarrow{i_*} H_0(\mathcal{H}) \longrightarrow 0.$$

Set $\mathcal{D}_{\tau,p} := H_0\left(\Delta_{\tau,p}\right)$ and $\mathcal{D}^0_{\tau,p} := H_1\left((\mathcal{H}, \Delta_{\tau,p})\right)$. We underline that the above exact sequence allows us to view $\mathcal{D}^0_{\tau,p}$ as a subgroup of $\mathcal{D}_{\tau,p}$. If we interpret $\mathcal{D}_{\tau,p}$ as a group of divisors, then, the foregoing statements imply that $\mathcal{D}^0_{\tau,p}$ is the subgroup of divisors of degree zero.

We are interested in studying modular symbols of weight 2; hence, we will consider $G = \mathbb{C}$. Given a topological pair (X, A), denote

$$\begin{aligned} Q_1 &:= \text{Hom}_{\mathbb{Z}}(H_1((X, A)), \mathbb{C}) \oplus \text{Ext}^1_{\mathbb{Z}}(H_0((X, A)), \mathbb{C}), \\ Q_2 &:= \text{Hom}_{\mathbb{Z}}(H_1(X), \mathbb{C}) \oplus \text{Ext}^1_{\mathbb{Z}}(H_0(X), \mathbb{C}). \end{aligned}$$

We have the following commutative diagram with exact rows, where the vertical arrows are the isomorphisms given by the universal coefficients theorem for cohomology:

$$\begin{array}{ccccccccc} H^0((X,A),\mathbb{C}) & \hookrightarrow & H^0(X,\mathbb{C}) & \longrightarrow & H^0(A,\mathbb{C}) & \longrightarrow & H^1((X,A),\mathbb{C}) & \longrightarrow & H^1(X,\mathbb{C}) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbb{Z}}(H_0((X,A)),\mathbb{C}) & \hookrightarrow & \mathrm{Hom}_{\mathbb{Z}}(H_0(X),\mathbb{C}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(H_0(A),\mathbb{C}) & \longrightarrow & Q_1 & \longrightarrow & Q_2. \end{array} \tag{6.2.1}$$

If we particularize the sequence (6.2.1) to our pair then we obtain the following result.

Proposition 6.2.10. *There is a commutative diagram with exact rows, where the vertical arrows are the isomorphisms given by the universal coefficients theorem for cohomology:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(\mathcal{H},\mathbb{C}) & \longrightarrow & H^0(\Delta_{\tau,p},\mathbb{C}) & \longrightarrow & H^1((\mathcal{H},\Delta_{\tau,p}),\mathbb{C}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(H_0(\mathcal{H}),\mathbb{C}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_{\tau,p},\mathbb{C}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}^0_{\tau,p},\mathbb{C}) & \longrightarrow & 0. \end{array}$$

Proof. All we have to see is that the Ext terms are zero. First of all, since $H_0((\mathcal{H},\Delta_{\tau,p})) = 0$, it follows that $Q_1 = 0$. Secondly, since $\mathcal{H}$ is pathwise connected, we have that $Q_2 = \mathrm{Ext}^1_{\mathbb{Z}}(H_0(\mathcal{H}),\mathbb{C}) = 0$. Notice that the left terms in each row are isomorphic to $\mathbb{C}$. □

By passing to the long exact sequence (acting Γ on each term), we obtain the following commutative diagram with exact rows and vertical isomorphisms:

$$\begin{array}{ccccc} H^{i-1}(\Gamma,\mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}^0_{\tau,p},\mathbb{C})) & \longrightarrow & H^i(\Gamma,\mathbb{C}) & \longrightarrow & H^i(\Gamma,\mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_{\tau,p},\mathbb{C})) \\ \downarrow & & \downarrow & & \downarrow \\ H^{i-1}(\Gamma,H^1((\mathcal{H},\Delta_{\tau,p}),\mathbb{C})) & \longrightarrow & H^i(\Gamma,H^0(\mathcal{H},\mathbb{C})) & \longrightarrow & H^i(\Gamma,H^0(\Delta_{\tau,p},\mathbb{C})). \end{array} \tag{6.2.2}$$

Definition 6.2.11. Let $\tau \in \mathcal{H}$ be a quadratic imaginary point. The $\mathbb{C}$-vector space of quadratic modular symbols attached to τ is

$$H^0(\Gamma,\mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}^0_{\tau,p},\mathbb{C})).$$

We denote this space by $\mathrm{Symb}(\mathcal{D}^0_{\tau,p},\mathbb{C})^{\Gamma}$.

Now, consider the Grothendieck spectral sequences

$$H^i(\Gamma, H^j(\mathcal{H}, \mathbb{C})) \underset{i}{\Longrightarrow} H^{i+j}(X(\Gamma)(\mathbb{C}), \mathbb{C}),$$

$$H^i(\Gamma, H^j(\Delta_{\tau,p}, \mathbb{C})) \underset{i}{\Longrightarrow} H^{i+j}(\Gamma\backslash\Delta_{\tau,p}, \mathbb{C}), \text{ and}$$

$$H^i(\Gamma, H^j((\mathcal{H}, \Delta_{\tau,p}), \mathbb{C})) \underset{i}{\Longrightarrow} H^{i+j}((X(\Gamma)(\mathbb{C}), \Gamma\backslash\Delta_{\tau,p}), \mathbb{C}).$$

We start by analysing the first one. The foregoing calculations imply, in particular, that $H^j(\mathcal{H}, \mathbb{C}) = 0$ for all $j \neq 0$. This fact implies that this spectral sequence has just one non-zero row and therefore it collapses providing an isomorphism

$$H^i(\Gamma, H^j(\mathcal{H}, \mathbb{C})) \cong H^{i+j}(X(\Gamma)(\mathbb{C}), \mathbb{C}),$$

for any $(i, j) \in \mathbb{N}^2$. Now, we deal with the second spectral sequence. Again by the foregoing, $H^j(\Delta_{\tau,p}, \mathbb{C}) = 0$ for all $j \neq 0$. Thus, as in the cuspidal case, this spectral sequence has just one non-zero row; hence, it collapses, yielding an isomorphism

$$H^i(\Gamma, H^j(\Delta_{\tau,p}, \mathbb{C})) \cong H^{i+j}(\Gamma\backslash\Delta_{\tau,p}, \mathbb{C}),$$

for each $(i, j) \in \mathbb{N}^2$. Since $H^j((\mathcal{H}, \Delta_{\tau,p}), \mathbb{C}) = 0$ for all $j \neq 1$, an analogous argument allows us to conclude that there is an isomorphism

$$H^i(\Gamma, H^1((\mathcal{H}, \Delta_{\tau,p}), \mathbb{C})) \cong H^{i+1}((X(\Gamma)(\mathbb{C}), \Gamma\backslash\Delta_{\tau,p}), \mathbb{C}),$$

for each $(i, j) \in \mathbb{N}^2$. Taking into account the above isomorphisms and diagram (6.2.2), the following result is proved.

Theorem 6.2.12. *Let $\tau \in \mathcal{H}$ be a quadratic imaginary point and let p be a prime. Then,*

$$\text{Symb}\left(\mathcal{D}^0_{\tau,p}, \mathbb{C}\right)^\Gamma \cong H^1((X(\Gamma)(\mathbb{C}), \Gamma\backslash\Delta_{\tau,p}), \mathbb{C}).$$

6.2.5 A relation between quadratic and classical modular symbols

As in the classical case, it is possible to give an alternative description of quadratic modular symbols in a more down-to-earth fashion. This description

will provide, in some cases, an injection of the space of classical modular symbols into the space of quadratic modular symbols. First, observe that our arithmetic Fuchsian group Γ acts on $\mathcal{D}^0_{\tau,p}$, the action being given by $\gamma\left(\sum_{j=1}^n P_k\right) = \sum_{j=1}^n \gamma(P_j)$, with $\gamma \in \Gamma$. Set

$$\Gamma\Delta^2_{\tau,p} = \{(\gamma\sigma_1(\tau), \gamma\sigma_2(\tau));\ \gamma \in \Gamma, \sigma_1, \sigma_2 \in \Delta_{\tau,p}\}.$$

Since any divisor $D \in \mathcal{D}^0_{\tau,p}$ can be decomposed as $D = \sum_{j=1}^n m_j(P_j - Q_j)$ with $P_j, Q_j \in \Delta_{\tau,p}$, any modular symbol determines a unique map $F : \Gamma\Delta^2_{\tau,p} \to \mathbb{C}$ such that for any $P,Q,R \in \Delta_{\tau,p}, \gamma \in \Gamma$, $F(\gamma P, \gamma Q) = F(\gamma P, \gamma R) + F(\gamma R, \gamma Q)$, and reciprocally. Denote by $M(\Gamma, \tau, p)$ the $\mathbb{C}$-vector space of these maps. We will not distinguish between $M(\Gamma,\tau,p)$ and $\mathrm{Symb}\left(\mathcal{D}^0_{\tau,p}, \mathbb{C}\right)$.

Let us turn to the modular case, i.e., suppose again that $\Gamma = \Gamma_0(N)$. Let $\tau \in \mathcal{H}$ be a quadratic non-elliptic imaginary point satisfying $\tau^2 + D = 0$ with D square free. It is convenient to recall the following facts on representability of integers by binary quadratic forms.

Definition 6.2.13. An integer n is properly represented by a binary quadratic form $aX^2 + bXY + cY^2$ if there exists a pair of coprime integers α, β such that $a\alpha^2 + b\alpha\beta + c\beta^2 = n$.

The following fact is well known, and we refer the reader to [20] for a proof.

Proposition 6.2.14. *The integer n is properly represented by a binary quadratic form of discriminant d if and only if d is a square* $\pmod{4n}$.

□

Proposition 6.2.15. *Let $D > 1$ be an integer and let p be a prime number such that $\left(\frac{-D}{p}\right) = -1$. Then, there is an injection*

$$\mathrm{Symb}\left(\mathcal{D}_0, \mathbb{C}\right)^{\Gamma_0(N)} \hookrightarrow \mathrm{Symb}\left(\mathcal{D}^0_{\tau,p}, \mathbb{C}\right)^{\Gamma_0(N)}.$$

Proof. Given $0 \le u \le p^n - 1$, let us denote, as in Chapter 5, $\gamma_{u,n} = \begin{pmatrix} 1 & u \\ 0 & p^n \end{pmatrix}$. Define a map

$$\begin{array}{rccc} I : \mathrm{Symb}\left(\mathcal{D}_0, \mathbb{C}\right)^{\Gamma_0(N)} & \to & \mathrm{Symb}\left(\mathcal{D}^0_{\tau,p}, \mathbb{C}\right)^{\Gamma_0(N)} \\ F & \mapsto & I(F), \end{array}$$

where

$$I(F)(\gamma\gamma_{u,n}\gamma_1(\tau), \gamma\gamma_{v,m}\gamma_2(\tau)) = F(\gamma\gamma_{u,n}\gamma_1(i\infty), \gamma\gamma_{v,m}\gamma_2(i\infty)).$$

First, we check that the map is well defined. It suffices to check that if

$$\sigma_1\gamma_{u,n}\gamma_1(\tau) = \sigma_2\gamma_{v,m}\gamma_2(\tau), \text{ with } \sigma_1, \sigma_2 \in \Gamma_0(N), \text{ and } \gamma_1, \gamma_2 \in \mathrm{SL}(2,\mathbb{Z}),$$

then, $\sigma_1\gamma_{u,n}\gamma_1(i\infty) = \sigma_2\gamma_{v,m}\gamma_2(i\infty)$. Hence, suppose that $\sigma_1\gamma_{u,n}\gamma_1(\tau) = \sigma_2\gamma_{v,m}\gamma_2(\tau)$. Then, τ is fixed by $\gamma = \gamma_2^{-1}\gamma_{v,m}^{-1}\sigma_2^{-1}\sigma_1\gamma_{u,n}\gamma_1 \in \mathrm{GL}(2,\mathbb{Q})$. Notice that $\eta = p^m\gamma \in \mathrm{GL}(2,\mathbb{Z})$ also fixes τ and has determinant p^{n+m}. If $\eta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then, $a = d$ and $b = cD$ (since τ is quadratic imaginary). Hence, $p^{n+m} = a^2 + Dc^2$.

If a and d were coprime, we would have that p^{n+m} were properly representable by the binary quadratic form X^2+DY^2, whose discriminant is $-4D$; hence, by applying Proposition 6.2.14, we would obtain that $-4D$ would be a square $\pmod{4p^{n+m}}$. Therefore, $-D$ would be, in particular, a square $\pmod{p}$, which contradicts the assumption that $\left(\frac{-D}{p}\right) = -1$.

If $(a,b) = d$, the only choice is that $d = p^r$ for some positive r. Write $a = a_0 d$ and $b = b_0 d$. If $r < n+m$, we would have again that $-D$ is a square $\pmod{p}$. Thus, $r = n+m$. This means that $a_0^2 + Db_0^2 = 1$ and $(a_0, b_0) = (\pm 1, 0)$. Hence, the matrices η and γ are diagonal and, in particular, γ induces the identity in $\mathrm{PGL}(2,\mathbb{Q})$. Hence, $\sigma_1\gamma_{u,n}\gamma_1 = \sigma_2\gamma_{v,n}\gamma_2\gamma$, and $\sigma_1\gamma_{u,n}\gamma_1(i\infty) = \sigma_2\gamma_{v,n}\gamma_2(i\infty)$, as we wanted to prove. Linearity and injectivity are obvious. □

Remark 6.2.16. It does not seem easy to prove that the Hecke algebra acts on $\mathrm{Symb}\left(\mathcal{D}^0_{\tau,p}, \mathbb{C}\right)^{\Gamma_0(N)}$ (the operator T_p certainly does). But since

$$\mathrm{Symb}\left(\mathcal{D}_0, \mathbb{C}\right)^{\Gamma_0(N)} \hookrightarrow \bigcap_{\left(\frac{-D}{p}\right)=-1} \mathrm{Symb}\left(\mathcal{D}^0_{\tau,p}, \mathbb{C}\right)^{\Gamma_0(N)},$$

we see that the Hecke algebra acts on the image of $\mathrm{Symb}\left(\mathcal{D}_0, \mathbb{C}\right)^{\Gamma_0(N)}$ in the intersection.

6.3 p-adic L-functions for automorphic forms

Classical modular symbols are at the core of the definition of the cyclotomic p-adic L-function, since the Mazur-Tate-Teitelbaum p-adic distribution can

be seen as a device which packs together in a coherent way all the modular integrals corresponding to the paths $\left\{\frac{a}{p^n}, i\infty\right\}$ (see chapter 3). Nevertheless, the construction of this measure depends on the explicit coset representatives for the action of the Hecke algebra. Relaxing these dependence is, as we will see, a necessary condition to define p-adic L-functions attached to certain Shimura curves in the cocompact case.

6.3.1 Coset representatives

To define the classical p-adic L-function, one considers the standard right coset decomposition of the operator T_p. Indeed, one fixes a way of assigning a coset representative to any compact open subset of the form $a + p\mathbb{Z}_p$ for $1 \leq a \leq p-1$. Even if we fix the standard right coset decomposition, another assignment of right coset representatives yields a different p-adic measure. To illustrate this, let us consider a permutation $\sigma \in \mathrm{Bij}\left(\{1, ..., p-1\}\right)$. Define $\sigma(0) = 0$. Denote again by σ the bijection

$$\begin{array}{rcl} \sigma : \mathbb{Z}_p^* \cap \{1, ..., p^n - 1\} & \to & \mathbb{Z}_p^* \cap \{1, ..., p^n - 1\} \\ \displaystyle\sum_{j=0}^{n-1} a_j p^j & \mapsto & \displaystyle\sum_{j=0}^{n-1} \sigma(a_j) p^j. \end{array}$$

Let μ be a $\mathbb{Q}_p$-valued p-adic distribution. Define

$$\mu^\sigma\left(a + p^n\mathbb{Z}_p\right) = \mu\left(\sigma(a) + p^n\mathbb{Z}_p\right).$$

Proposition 6.3.1. *For any p-adic distribution μ and for any permutation $\sigma \in \mathrm{Bij}\left(\{1, ..., p-1\}\right)$, μ^σ is a p-adic distribution.*

Proof. First notice that for any $a = \displaystyle\sum_{j=0}^{n-1} a_j p^j \in \mathbb{Z}_p^*$, we have the decomposition

$$a + p^n\mathbb{Z}_p = \bigcup_{j=0}^{p-1} a + jp^n + p^{n+1}\mathbb{Z}_p.$$

Hence,

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

But since σ is a permutation of indices between 1 and $p-1$, the right hand side equals

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

□

Lemma 6.3.2. *Let σ be a bijection of the set $\{1,...,p-1\}$. Set $\sigma(0)=0$. The assignment $\sigma\left(\sum_{j=0}^{n} a_j p^j\right)$ determines a $\mathbb{Z}_p$-valued continuous function defined on $\mathbb{Z}$. Hence, it extends in a unique way to $\mathbb{Z}_p$ and, in particular, to $\mathbb{Z}_p^*$.*

Proof. Let $u,v\in\mathbb{Z}$ be a couple of integers with $|u-v|_p \leq p^{-n}$. This means that the first n digits of u and v are equal. Hence, the first n digits of $\sigma(u)$ and $\sigma(v)$ are equal, which means that $|\sigma(u)-\sigma(v)|_p \leq p^{-n}$. □

Let $\chi\in\mathcal{X}$ be a continuous p-adic character. We can define

$$\chi_\sigma(a) = \chi\left(\sigma^{-1}(a)a^{-1}\right),$$

where σ is the extension to $\mathbb{Z}_p$ of a bijection of the set $\{1,...,p\}$. By using Lemma 6.3.2, it is not difficult to see that $\chi_\sigma\in\mathcal{X}$. Let $f\in S_2\left(\Gamma_0(N)\right)$ be an eigenform for T_p. Denote by $L_p^\sigma(f;\chi)$ the Mazur-Mellin transform of μ^σ at χ. We have the following result:

Proposition 6.3.3. *For any $\chi\in\mathcal{X}$, $L_p^\sigma(f;\chi) = L_p(f;\chi\chi_\sigma)$. In particular, L_p^σ is not identically zero.*

Proof. By definition, $\int_{\mathbb{Z}_p^*}\chi(x)d\mu(x) = \lim\sum_a \chi(a)\mu^\sigma(a+p^n\mathbb{Z}_p)$ where the limit is taken as $\{a+p^n\mathbb{Z}_p\}$ runs over the partitions of $\mathbb{Z}_p^*$. Hence,

$$L_p^\sigma(f;\chi) = \lim\sum_a \chi(\sigma(a))\chi(a\sigma(a^{-1}))\mu(a^\sigma+p^n\mathbb{Z}_p),$$

which, after a straightforward manipulation equals $\lim\sum_a \chi(a)\chi_\sigma(a)\mu(a+p^n\mathbb{Z}_p)$. But this limit coincides with $L_p(f;\chi\chi_\sigma)$. As for the fact that it does not vanish, notice that the conductor of χ_σ is a power of p, and apply the main result of [62]. □

As we can see, the Mazur-Mellin transforms of μ^σ and μ are not equal. However, as an immediate consequence of Proposition 6.3.3, we have the following

Corollary 6.3.4. *For any* $\sigma \in \mathrm{Bij}\,(\{1,...,p-1\})$, $L_p(f;1) = L_p^\sigma(f;1)$.

6.3.2 p-adic L-functions for certain Shimura curves

Let H be an indefinite quaternion $\mathbb{Q}$-algebra of discriminant $D > 1$; consider the Eichler order $\mathcal{O} = \mathcal{O}(D,N)$ of level $N \geq 1$ and denote by $\mathcal{O}_1^*$ the group of units of reduced norm 1 in $\mathcal{O}$. Let $\Gamma = \Gamma(D,N)$ be the group $\psi(\mathcal{O}_1^*)$. Let p be a prime. The Hecke operator T_p is defined as the double coset $\Gamma\eta_p\Gamma$ acting on $S_2(\Gamma)$, where $\eta_p = \psi(\omega_p)$ with ω_p a quaternion of reduced norm p (see [66]). We thank Professor Y. Yang for showing us the following fact.

Proposition 6.3.5. *Let p be a prime.*

(i) If $p \nmid ND$, then $[\Gamma : \Gamma \cap \eta_p^{-1}\Gamma\eta_p] = p+1$.

(ii) If $p|N$ and $p \nmid D$, then $[\Gamma : \Gamma \cap \eta_p^{-1}\Gamma\eta_p] = p$.

(iii) If $p|D$, then $[\Gamma : \Gamma \cap \eta_p^{-1}\Gamma\eta_p] = 1$.

Proof. The number of coset representatives is finite in any case (see [66]) and it is enough to count it locally, since H splits at infinity. On the other hand, there is a bijection between the orbit spaces $\Gamma\backslash\Gamma\eta_p\Gamma$ and $\Gamma\cap\eta_p^{-1}\Gamma\eta_p\backslash\Gamma$. Denote $\mathcal{O}_p = \mathcal{O}\otimes\mathbb{Z}_p$. If $p \nmid ND$, the Eichler order $\mathcal{O}_p$ is conjugated to the local Eichler order $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. The matrices $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$ with $0 \leq j \leq p-1$ are a family of coset representatives of $\Gamma\backslash\Gamma\eta_p\Gamma$. If $p|N$ but $p \nmid D$, the Eichler order $\mathcal{O}_p$ is conjugated to the local Eichler order $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ N\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. The matrices $\gamma_j = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$ with $0 \leq j \leq p-1$ are a family of coset representatives of $\Gamma\backslash\Gamma\eta_p\Gamma$ in this case. Finally, if $p|D$, the Eichler order $\mathcal{O}_p$ is a discrete valuation ring and we can take as element of norm p any uniformizer of the Eichler order, and any element of norm p of this Eichler order is a uniformizer, which differs from the first in a unit; hence, there is only one class. □

Next we propose a definition of a p-adic L-function for the Shimura curve $X(D,N)$ provided that $p|N$ but $p \nmid D$. Prior to doing this, we point out that the decomposition in coset representatives is not unique. In the non-cocompact case, having fixed the standard decomposition of the Hecke double coset operator, as we have seen above, one has to assign a coset representative to any compact-open subset $D(j,p)$, $1 \leq j \leq p-1$, and for different assignments, the corresponding p-adic L-functions are different.

Fix a family of coset representatives $\{\gamma_j\}$ for the orbit space $\Gamma\backslash\Gamma\eta_p\Gamma$. Let $f \in S_2(\Gamma)$ be a weight 2 automorphic form which is an eigenform for the operator T_p, which is defined as

$$T_p(f) = \sum_{j=1}^{p} f|_2\gamma_j.$$

A standard argument analogous to the modular case shows that the definition of T_p does not depend on the choice of the coset representatives. Let a be a natural number less than p^n. Write $a = \sum_{i=0}^{n-1} a_i p^i$ with $0 \leq a_i \leq p-1$. Fix a permutation σ of the set $\{1, ...p-1\}$ and set $\sigma(0) = 0$. Denote

$$\delta(f,\tau,\sigma,a) = \phi_f^\tau\left(\gamma_{\sigma(a_{n-1})}\cdots\gamma_{\sigma(a_0)}(\tau)\right) - \phi_f^\tau\left(\gamma_{\sigma(p-a_{n-1})}\cdots\gamma_{\sigma(p-a_0)}(\tau)\right).$$

Definition 6.3.6. Let σ be a bijection of the set $\{0, ..., p-1\}$ with $\sigma(0) = 0$ and let $f \in S_2(\Gamma)$ be an eigenform for T_p with eigenvalue a_p. Let $\tau \in \mathcal{H}$ be a quadratic imaginary point. The quadratic p-adic distribution attached to f, τ and σ is defined by

$$\mu_{\mathcal{Q}}^\sigma(D(a,p^n)) = a_p^{-n}\delta(f,\tau,\sigma,a),$$

$$\mu_{\mathcal{Q}}^\sigma\left(\mathbb{Z}_p^*\right) = \sum_{a=1}^{p-1}\mu_{\mathcal{Q}}^\sigma(D(a,p^n)),$$

$$\mu_{\mathcal{Q}}^\sigma(p^n\mathbb{Z}_p) = 0, \text{ for any } n \geq 1.$$

Proposition 6.3.7. *The function $\mu_{\mathcal{Q}}$ extends, in a unique way, to a p-adic distribution with values in $c_{00}(\mathbb{Q}_p(a_p))$.*

Proof. Notice that $\mu_{\mathcal{Q}}(a+p^n\mathbb{Z}_p) \in \Sigma_{f,n} \otimes \mathbb{Z}_p[a_p^{-1}]$. Since each compact open subset can be covered by a finite number of discs, $\mu_{\mathcal{Q}}$ takes values on $c_{00}(\mathbb{Q}_p(a_p))$.

To prove the distribution property, suppose that $\gamma_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}$. Since f is an eigenform for T_p, and $\det(\gamma_j) = p$, we have

$$a_p \phi_f^\tau \left(\gamma_{\sigma(j_{n-1})} \cdots \gamma_{\sigma(j_0)}(\tau)\right) = \sum_{j=1}^{p} \int_{\gamma_{\sigma(j_{n-1})} \cdots \gamma_{\sigma(j_0)}(\tau)}^{\tau} p(c_j z + d_j)^{-2} f\left(\gamma_j(z)\right) dz.$$

Since $d(\gamma_j(z)) = p(c_j z + d_j)^{-2} dz$, after changing variables ($\gamma_j(z)$ by w), and taking into account that j is a mute index, we have

$$a_p \phi_f^\tau \left(\gamma_{\sigma(j_{n-1})} \cdots \gamma_{\sigma(j_0)}(\tau)\right) = \sum_{j=1}^{p} \phi_f^\tau \left(\gamma_{\sigma(j)} \gamma_{\sigma(j_{n-1})} \cdots \gamma_{\sigma(j_0)}(\tau)\right) + K, \quad (6.3.1)$$

where

$$K = -\sum_{j=1}^{p} \int_{\gamma_j(\tau)}^{\tau} f(z) dz.$$

In addition

$$a_p \phi_f^\tau \left(\gamma_{\sigma(p-j_{n-1})} \cdots \gamma_{\sigma(p-j_0)}(\tau)\right) = \sum_{j=1}^{p} \phi_f^\tau \left(\gamma_{\sigma(p-j)} \gamma_{\sigma(p-j_{n-1})} \cdots \gamma_{\sigma(p-j_0)}(\tau)\right) + K. \quad (6.3.2)$$

Now, by subtracting equation 6.3.1 from 6.3.2, the result follows. □

To distinguish between ordinary and supersingular forms, we need the following result on algebraicity:

Theorem 6.3.8 (Shimura [66])**.** *Let H be a quaternion $\mathbb{Q}$-algebra of discriminant D and let $\mathcal{O}$ be an Eichler order of level N. Let p be a prime. Then the eigenvalue of the Hecke operator T_p acting on $S_2(\Gamma)$ is an algebraic integer.*

Let a_p be the eigenvalue of T_p attached to f. By Theorem 6.3.8, a_p is an algebraic integer. We say that f is ordinary at p if $|a_p|_p = 1$; otherwise we say that f is supersingular at p.

Definition 6.3.9. Denote by Σ_{p-1} the symmetric group of order $p-1$. Let $f \in S_2\left(\Gamma(D,N)\right)$ be an eigenform for the Hecke operator T_p, for $p \nmid D$, $p|N$. Let $\tau \in \mathcal{H}$ be a quadratic imaginary point. If f is ordinary at p, the p-adic L-function attached to f and τ is

$$L_p(f; \sigma, \chi) = \int_{\mathbb{Z}_p^*} \chi(x) d\mu_{\mathcal{Q}}^{\sigma}(x).$$

Chapter 7

Resumen en castellano

7.1 Extensiones abelianas reales

7.1.1 Introducción

La teoría de funciones L p-ádicas surge en la década de los 60 en la escuela de Erlangen, de la mano de H.W. Leopoldt. A finales de esa década es exportada y reformulada por K. Iwasawa. El contexto original en el que surge es el estudio del número de clases de ideales de una extensión abeliana finita de $\mathbb{Q}$. Como es bien sabido, el teorema de Kronecker-Weber establece que una tal extensión está contenida en una extensión ciclotómica. El estudio del número de clases de ideales de las extensiones ciclotómicas es de primera importancia, ya que para primos regulares el conocido argumento de Kummer establece la validez del último teorema de Fermat (cf. [74]). Este hecho hace pertinente un estudio asintótico de los numeros de clases de ideales de las extensiones ciclotómicas. No obstante, la fórmula del número de clases de Dedekind proporciona información sobre el producto $h_K R(K)$, donde h_K es el número de clases y $R(K)$ el regulador. No parece fácil, por otro lado, el cálculo del regulador, toda vez que para ello es necesario encontrar un sistema maximal de unidades fundamentales.

Si $K/\mathbb{Q}$ es una extensión abeliana finita, se sabe que para todo carácter no trivial $\chi \in \mathrm{Gal}(K/\mathbb{Q})$, si χ es impar, se tiene que $L(1;\chi)$ es esencialmente el producto de π por un entero algebraico, mientras que si es par, se trata de una suma de logaritmos de números algebraicos, que, como es sabido (cf. [6]), es trascendente. En concreto, se tiene el siguiente resultado.

Proposición 7.1.1 (Hasse, [32]). *Dada una extensión abeliana real $K/\mathbb{Q}$, para todo carácter de Dirichlet χ de conductor f_χ y para toda raíz primitiva f_χ-ésima de la unidad, se tiene:*

$$L(1;\chi) = \begin{cases} \frac{\pi i}{f_\chi}\tau(\chi)B_{1,\overline{\chi}}, & \text{si } \chi \text{ es impar,} \\ \\ \frac{-\tau(\chi)}{f_\chi}\sum_{a=1}^{f_\chi}\overline{\chi}(a)\log|1-\zeta^a|, & \text{si } \chi \text{ es par, } \chi \neq 1. \end{cases}$$

Por lo tanto, parece pertinente el estudio de la p-divisibilidad de los números de Bernoulli. A este objeto, Leopoldt ([43]) sustituyó los valores $L(1;\chi)$ para χ par por un análogo p-ádico $\mathcal{L}_p(\chi)$ obtenido al sustituir el logaritmo usual por el logaritmo p-ádico:

Definición 7.1.2. (Leopoldt, [43]) Dado un carácter de Dirichlet χ de conductor f_χ, se define

$$\mathcal{L}_p(\chi) := -\frac{\tau(\chi)}{f_\chi}\sum_{a=1}^{f_\chi}\overline{\chi}(a)\log_p(1-\zeta^a).$$

Definiendo un análogo p-ádico del regulador a través del logaritmo p-ádico, al que se denota por $R_p(K)$, se llega a la siguiente fórmula, conocida como fórmula p-ádica del número de clases:

Teorema 7.1.3 (Leopoldt, [43]). *Dada una extensión abeliana real $K/\mathbb{Q}$ de grado g, discriminante d y número de clases h, se tiene la siguiente igualdad*

$$\frac{2^{g-1}hR_p(K)}{\sqrt{d}} = \prod \mathcal{L}_p(\chi), \tag{7.1.1}$$

donde χ recorre los caracteres no triviales del grupo de Galois asociados a la extensión.

Posteriormente, la cantidad $\mathcal{L}_p(\chi)$ resultará ser, como parece natural, el valor en $s=1$ de una función meromorfa p-ádica $L_p(s;\chi)$ caracterizada por el valor que toma en los enteros impares negativos, que coincide con el que toma cierta torcida de la función $L(s;\chi)$ en esos valores, corregido por un factor de Euler asociado a χ y al entero en cuestión. Se dice que $L_p(s;\chi)$ interpola a $L(s;\chi)$ en estos valores.

Tres son las posibles construcciones de $L_p(s;\chi)$, que analizamos en el capítulo 1: la construcción original de Kubota-Leopoldt ([40]) en términos de lo que hemos traducido por χ-medias, las construcciones de Iwasawa ([34]) en términos de series de potencias y de elementos de Stickelberger, y la construcción en términos de transformadas de Mazur-Mellin de medidas p-ádicas asociadas a los polinomios de Bernoulli (cf. [39]). Todas ellas son equivalentes, siendo la última la que permite una generalización inmediata al contexto de las extensiones abelianas reales de un cuerpo totalmente real ([22]), lo que se expone en el capítulo segundo.

7.1.2 Objetivos, aportaciones fundamentales y conclusiones

A continuación presentamos nuestras contribuciones a la teoría en este contexto. Antes de ello, conviene introducir las siguientes nociones.

Definición 7.1.4 (cf. Leopoldt, [43])**.** Dado $z \in \mathbb{Z}_p^*$, el cociente de Fermat de z módulo p, denotado por $Q_p(z)$, es el resto $(z^{p-1}-1)/p \pmod p$.

Dada $K/\mathbb{Q}$ una extensión abeliana real de grado g, denotemos por $\{\sigma_j\}_{j=1}^{g}$ al conjunto de inmersiones de K en $\mathbb{Q}^{alg}$.

Definición 7.1.5 (Leopoldt, [43])**.** El regulador p-ádico módulo p es

$$R^{(p)}(K) = \det\left(Q_p\left(\sigma_j\left(\varepsilon_k\right)\right)\right)_{j,k=1}^{g-1},$$

donde $\{\varepsilon_j\}_{j=1}^{g-1}$ es un sistema fundamental de unidades.

Nuestro primer resultado es la prueba del Teorema 1.1.15, que si bien se presenta enunciado en [43], no se da la demostración, ni una referencia donde encontrarla. Además, el regulador p-ádico está definido salvo un signo, a menos que se fije un sistema fundamental de unidades, por lo que nosotros precisamos el enunciado de este resultado. En concreto, probamos la siguiente afirmación:

Teorema 7.1.6. *Sea $K/\mathbb{Q}$ una extensión abeliana real y sea $p > 3$ un primo tal que para todo carácter χ de $\mathrm{Gal}\,(K/\mathbb{Q})$ de conductor f_χ, se tiene que $p \nmid f_\chi$. Entonces, existen un sistema fundamental de unidades de $\mathcal{O}_K$, una*

determinación de la raíz cuadrada y una ordenación de las inmersiones de K *en* $\mathbb{Q}^{alg}$ *tales que*

$$\frac{2^{g-1}hR^{(p)}(K)}{\sqrt{d}} \equiv \frac{\zeta_K(2-p)}{\zeta(2-p)} \pmod{p},$$

donde ζ_K *denota la función zeta de Dedekind y* ζ *es la función zeta de Riemann.*

Para explicar nuestra segunda contribución en este contexto, definimos primero la siguiente generalización del regulador p-ádico módulo p^n (con $n \geq 1$).

Definición 7.1.7. Denotemos por $\{\varepsilon_1, ..., \varepsilon_{g-1}\}$ un sistema fundamental de unidades de K. Denotemos por $Q_{p,n}(z)$ el truncamiento de la serie $\frac{-1}{p}\log_p(1+p\tilde{z}) \pmod{p^{n+1}}$. El regulador p-ádico módulo p^n es

$$R^{(p,n)}(K) = \det\left(Q_{p,n}\left(\sigma_j(\varepsilon_k)\right)\right)_{1\leq j,k\leq g-1}.$$

El hecho de que esta construcción generaliza al regulador p-ádico módulo p es implicado por la Proposición 1.1.13. Demostramos los siguientes resultados (enumerados en el capítulo 1 como Proposiciones 1.1.28 y 1.1.29, respectivamente) que, además de ser interesantes en si mismos, son herramientas técnicas para nuestro resultado principal en esta sección, enumerado en el capítulo 1 como Proposición 1.1.31.

Proposición 7.1.8. *Sea* $K/\mathbb{Q}$ *una extensión abeliana real de* $\mathbb{Q}$ *de grado* g *y* $p > 3$ *un primo no ramificado para* K *tal que para todo carácter* χ *de* $\mathrm{Gal}(K/\mathbb{Q})$ *se tiene que* $p \nmid f_\chi$. *Entonces, existen un sistema fundamental de unidades, una determinación de la raíz cuadrada y una ordenación de las inmersiones de* K *en* $\mathbb{Q}^{alg}$ *tales que para todo* $n \geq 1$,

$$\frac{2^{g-1}hR^{(p,n)}(K)}{\sqrt{d}} \equiv (-1)^{g-1}\frac{\zeta_K(1-p^n(p-1))}{\zeta(1-p^n(p-1))} \pmod{p^{n+1}}.$$

Proposición 7.1.9. *Sea* $K/\mathbb{Q}$ *una extensión abeliana real. Sea* p *un primo no ramificado para* K *tal que* $(p, h_k) = 1$ *y* $R_p(K) \in p^{g-1}\mathbb{Z}_p^*$. *Entonces, para todo* $n \geq 1$ *se tiene que*

$$p \nmid \frac{\zeta_K\left(1-p^n(p-1)\right)}{\zeta(1-p^n(p-1))}.$$

Mediante estos resultados estimamos la p-divisibilidad de la función zeta de Dedekind p-ádica relativa a la extensión evaluada en ciertos enteros y obtenemos una fórmula para $s = 1$, a través de un argumento de aproximación p-ádica. Nuestra contribución principal es el siguiente enunciado.

Proposición 7.1.10. *Sea $K/\mathbb{Q}$ una extensión abeliana real. Sea p un primo no ramificado para K tal que $(p, h_k) = 1$ y $R_p(K) \in p^{g-1}\mathbb{Z}_p^*$. Entonces,*

$$\left|\zeta_{K/\mathbb{Q},p}(1)\right|_p = 1.$$

Nuestras contribuciones originales en el contexto de las extensiones abelianas están siendo redactadas para ser enviadas a publicación ([16]). Asimismo, hemos procurado exponer en el capítulo 1 los trabajos de Leopoldt ([43]) y de Kubota-Leopoldt ([40]) en su contexto original. En esencia, todo su contenido está presente en los libros [34] y [74]. Sin embargo, resulta interesante (y justo) recuperar las ideas y motivaciones originales que impulsaron la teoría. Por ejemplo, nuestros resultados son aplicaciones más o menos sencillas de ligeras variaciones de la teoría original, y probarlo desde el punto de vista de las distribuciones p-ádicas parece más complicado. Además, conviene apuntar que si bien es cierto que en [34] se da la prueba de que $\mathcal{L}_p(\chi) = L_p(1;\chi)$, la transformada Γ había sido introducida anteriormente por Leopoldt, o al menos eso es lo que se indica en [41].

7.2 Formas modulares

7.2.1 Introducción

En los capítulos 3, 4 y 5 investigamos diversas construcciones de funciones L p-ádicas asociadas a formas modulares para $\Gamma_0(N)$ y proponemos una definición que permite generalizarse al caso de una curva de Shimura $X(D, N)$ con $p \nmid D$ y $p \| N$, lo que se hace en el capítulo 6. En concreto, exponemos las definiciones de Mazur-Tate-Teitelbaum ([49]) y Mazur y Swinnerton-Dyer ([47]).

Siguiendo con nuestra exposición histórica, apuntamos que la década de los 70 fue el turno de las funciones L p-ádicas asociadas a curvas elípticas modulares o, más en general, a formas modulares. Mediante el empleo de las funciones L p-ádicas se pueden tratar muy cómodamente problemas como el de la estimación de la p-divisibilidad de la parte negativa del número de

clases y se puede dar información sobre la distribución de los primos irregulares. Mediante el uso de distribuciones p-ádicas se obtienen pruebas cortas y elegantes de las congruencias de Kummer y Clausen-Von Staudt, que se generalizan fácilmente a un carácter χ no trivial. Aparecen resultados análogos de p-divisibilidad e interpolación en el caso de extensiones abelianas reales de cuerpos totalmente reales ([67],[22],[26]) y se obtienen fórmulas p-ádicas del número de clases sorprendentemente análogas a las clásicas complejas. Por otro lado, la conjetura de Birch y Swinnerton-Dyer se acababa de formular. Todo ello propició la definición de una función L p-ádica para curvas elípticas $E/\mathbb{Q}$, que se supone que debería arrojar algo de luz sobre determinados problemas, como el cómputo de la constante de Manin y la estimación de la p-divisibilidad de valores de la función L-clásica o de sus torcidas por caracteres de Dirichlet y, sobre todo, de su anulación o no anulación en el punto crítico $s = 1$.

Se formula por ello la conjetura p-ádica de Birch y Swinnerton-Dyer ([47]) y otras relacionadas, como el problema de la anulación de las funciones L p-ádicas en distintos tipos de caracteres. En estas conjeturas, la transformada de Mellin de la forma modular es sustituída por la transformada de Mazur-Mellin.

7.2.2 Objetivos, aportaciones fundamentales y conclusiones

Dada una forma cuspidal $f \in S_k(\Gamma_0(N))$ que sea autofunción para el operador de Hecke T_p, cabe considerar el polinomio de Hecke en el primo p, definido como $X^2 - a_p(f)X + p^{k-1}$, si p es primo con N, y como $X - a_p(f)$ si $p \| N$ ($a_p(f)$ denota el p-ésimo coeficiente de Fourier de f). Denotemos por Σ_f al $\mathbb{Z}$-módulo generado por los coeficientes de Fourier de f, del que se demuestra que es finito-generado. Dada una raíz $\alpha \neq 0$ de este polinomio y dado un entero $0 \leq j \leq k-2$, se define en [49] la siguiente distribución p-ádica con valores en $\mathcal{O}_f[\frac{1}{\alpha}] \otimes \Sigma_f$ sobre los conjuntos $D(a, p^n) := a + p^n\mathbb{Z}_p$, con $a \in \mathbb{Z}_p^*$ y $n \geq 1$. Estos conjuntos recubren $\mathbb{Z}_p^*$ cuando a recorre $\mathbb{Z}_p^*$ y $n \geq 1$. Son además compactos y abiertos.

(i) Si $(p, N) = 1$, se define

$$\mu_{\alpha,j}(D(a, p^n)) = \frac{1}{\alpha^n}\left(\lambda\left(f, \frac{a}{p^n}, j\right) - \frac{1}{\alpha}p^{k-2}\lambda\left(f, \frac{a}{p^{n-1}}, j\right)\right).$$

(ii) Si $p \| N$, se define

$$\mu_{\alpha,j}(D(a,p^n)) = \frac{1}{a_p(f)^n}\lambda\left(f, \frac{a}{p^n}, j\right).$$

Aqu, dado $r \in \mathbb{Q}$, $\lambda(f,r,j)$ denota la integral modular (cf. [27]). Si $|a_p(f)|_p = 1$, se dice que f es ordinaria en p. En otro caso, se dice que f es supersingular en p. Una raíz α es llamada admisible (cf. [49]) si su valoración p-ádica es inferior a $k-1$. En el caso ordinario, sólo hay una raíz admisible, α, que es una unidad p-ádica y en tal caso, $\mu_{\alpha,j}$ es una medida p-ádica.

Definición 7.2.1. Las distribuciones de Mazur-Tate-Teitelbaum asociadas a f y p son

a) Si f es ordinaria en p: $\mu_{\alpha,j}$, donde α es la única raíz del polinomio de Hecke de f en p que es una unidad p-ádica.

b) Si f es supersingular en p: $\mu_{\alpha_i,j}$, $i = 1,2$, donde α_i denotan las raíces del polinomio de Hecke.

Finalmente, la función L p-ádica asociada a f se define en el grupo de caracteres p-ádicos continuos a través de la integral asociada a la distribución p-ádica (cf. [49] para el caso supersingular):

Definición 7.2.2. Dada una raíz admisible α y dado un carácter p-ádico continuo $\chi \in \mathrm{Hom}_{\mathrm{cont}}\left(\mathbb{Z}_p^*, \mathbb{C}_p^*\right)$, se define

$$L_p(f,\alpha,\chi) := \int_{\mathbb{Z}_p^*} \chi(x) d\mu_\alpha(x).$$

La función L p-ádica interpola valores especiales de la función L compleja torcida por caracteres de Dirichlet. En concreto, dado un entero $j \in \{0,...,k-2\}$, consideremos el carácter p-ádico definido como $\chi_j(x) := x^j$ y dado ψ un carácter de Dirichlet de conductor p^r, definamos el factor

$$e(p,\alpha,\chi) = \alpha^{-\nu}\left(1 - \overline{\psi}(p)p^{k-2-j}\alpha^{-1}\right)\left(1 - \psi(p)p^j\alpha^{-1}\right).$$

Se tiene la siguiente igualdad:

$$L_p(f,\alpha,\chi) = e(p,\alpha,\chi)L(f_{\overline{\chi}}, j+1).$$

Es fácil ver que factor $e(p, \alpha, \chi)$ no es nulo salvo en el caso en que $p \| N$, en que eventualmente puede anularse.

Dado $x \in \mathbb{Z}_p^*$, el lema de Hensel permite probar que existe una única raíz $(p-1)$-ésima de 1 perteneciente a $\mathbb{Z}_p^*$ y congruente con x módulo p, que se denota por $\omega(x)$. Denotando asimismo $\langle x \rangle := x/\omega(x)$, se define la transformada de Mazur-Mellin de $\mu_{f,\alpha}$ como la restricción de $L_p(f, \alpha)$ a caracteres de la forma $\chi_s(x) = \langle x \rangle^s$, donde $s \in \mathbb{Z}_p$, es decir, $L_p(f, \alpha, s) := \int_{\mathbb{Z}_p^*} \langle x \rangle^{s-1} d\mu_\alpha(x)$.

Dada una curva elíptica $E/\mathbb{Q}$ de conductor N, y dada su forma cuspidal $f \in S_2^{new}(\Gamma_0(N))$ asociada a la parametrización modular de Wiles, para todo primo p de buena reducción ordinaria de E, se puede definir su función L p-ádica a través de f, como $L_p(E, s) := L_p(f, \alpha, s)$, donde α es la única raíz admisible del polinomio de Hecke. El análogo p-ádico de la conjetura de Birch y Swinnerton-Dyer establece que el orden de anulación de $L_p(E, s)$ en $s = 1$ coincide con el rango del grupo $E(\mathbb{Q})$ (cf. [47]). En [49] se ofrece la definición de $L_p(E, s)$ para primos supersingulares y de reducción multiplicativa.

Las funciones L p-ádicas tienen una dificultad no presente en el caso clásico: la aparición de determinados factores de Euler puede producir ceros adicionales, como ocurre en el caso de reducción multiplicativa. De hecho no está claro a priori que no sean idénticamente zero. En el caso de extensiones abelianas esto es ya así; fijémonos, por ejemplo, en la conjetura de Leopoldt.

En el capítulo 3 comentamos la conjetura del cero excepcional y otras relacionadas. Además, exponemos los artículos [47] y [49] elaborando las pruebas de varios resultados que allí se dan, en muchos casos, en bosquejo, lo que puede suponer una dificultad adicional a quien esté interesado en este tipo de resultados. Particularizamos a $\mathbb{Q}$ la exposición del grupo de Mordell-Weil extendido y del apareamiento p-ádico, ya que resulta así más comprensible. Mostramos, además la equivalencia de las definiciones de Mazur y Swinnerton-Dyer y de Mazur-Tate-Teitelbaum de la función L p-ádica asociada a una curva elíptica racional (por tanto modular, según sabemos hoy). En principio la definición es distinta y la igualdad es consecuencia de una propiedad de interpolación.

El primer resultado de no anulación de funciones L p-ádicas de formas modulares se debe a Rohrlich ([61], [62]). Y es el siguiente:

Teorema 7.2.3 (Rohrlich, [61]). *Dada una forma cuspidal $f \in S_2(\Gamma_0(N))$, para todo carácter de Dirichlet de conductor potencia de p salvo a lo sumo una cantidad finita se tiene que $L(f, \chi, 1) \neq 0$.*

Obsérvese que este resultado, debido a la propiedad de interpolación de la función L p-ádica implica que ésta no es idénticamente nula sobre el grupo de caracteres p-ádicos de orden finito. Posteriormente, este resultado se generalizó en [62] a formas cuspidales de peso arbitrario. Nuestra contribución a este problema establece la no anulación de la función L p-ádica en el conjunto de caracteres de orden infinito y conlleva un estudio de los órdenes de anulación en el caso supersingular. A continuación exponemos nuestros resultados principales (enumerados en el capítulo 3 como Teoremas 3.1.12 y 3.1.16), las principales ideas de las pruebas y las consecuencias de ellos en el seno de la teoría general. En primer lugar, denotemos $L_p(f,\alpha)_1(s) := L_p(f,\alpha,\tilde{\chi}_s)$, donde $\tilde{\chi}_s(x) = x^s$. Nótese que es necesario fijar una clase de congruencia módulo $p-1$ para definir la exponencial p-ádica fuera del disco unitario, y que distintas clases de congruencia dan lugar a distintas definiciones de la exponencial, que, eso sí, coinciden sobre los enteros. Denotemos asimismo $L_p(f,\alpha)_2(s) = L_p(f,\alpha,\chi_s)$, donde $\chi_s(x) = \langle x\rangle^s$. Con estas definiciones, tenemos:

Teorema 7.2.4 ([17])**.** *Sea $p > 2$ un número primo y sea $f \in S_k(\Gamma_0(N))$ una forma nueva cuspidal normalizada y ordinaria en p. Sea α la única raíz admisible del polinomio de Hecke de f en p. Entonces, $L_p(f,\alpha)_1$ no es idénticamente nula sobre $\mathbb{Z}_p$. Además, si $k = 2$, $L_p(f,\alpha)_1$ no es idénticamente nula sobre $\mathbb{Z}_p^*$.*

La prueba de este resultado es por reducción al absurdo. Suponer que $L_p(f,\alpha,n) = 0$ para todo $n \geq 1$ implica, mediante un uso del teorema de Kaplansky de aproximación de funciones continuas p-ádicas por polinomios, que las medidas $\mu_{\alpha,j}$ se anulan en todos los discos compacto-abiertos recubridores de $\mathbb{Z}_p^*$ (observemos que la topología p-ádica es totalmente disconexa). Y este resultado, a su vez, mediante un argumento sobre límites bajo el signo integral, para el que se usa la cuspidalidad de f, implica la negación del anterior resultado de Rohrlich.

Nuestro segundo resultado establece que, en el caso supersingular, el orden de anulación de la función L p-ádica en cualquier entero p-ádico es finito:

Teorema 7.2.5 ([17])**.** *Sea $f \in S_k(\Gamma_0(N))$ una forma nueva cuspidal normalizada, supersingular en un primo $p \geq 5$, y α una raíz admisible del polinomio de Hecke de f en p. Si $L_p(f,\alpha)_1$ no es idénticamente nula, se tiene que para todo $s_0 \in \mathbb{Z}_p$, se da la siguiente desigualdad:*

$$\mathrm{ord}_{s=s_0} L_p(f,\alpha)_i(s) < \infty \text{ for } i = 1, 2.$$

Para la prueba de este resultado utilizamos herramientas de análisis p-ádico infinito-dimensional. En concreto, definimos un tipo de operadores llamados triangulares superiores y establecemos que el operador asociado a una forma modular a través de su función L p-ádica es inyectivo (Proposición 3.1.20). Conviene observar que [36] establece que $\mathrm{ord}_{s=1} L_p(E,s) \geq \mathrm{rk}(\mathrm{E}(\mathbb{Q}))$, pero no se sabe gran cosa sobre la desigualdad en el otro sentido para rango superior a 1. Ni siquiera se sabía si el orden era finito, por lo que nuestro resultado constituye una evidencia a la conjetura principal de Mazur, Tate y Teitelbaum. Obsérvese que en el caso supersingular, la función L p-ádica es localmente analítica pero no analítica.

En el capítulo 5, cuyo contenido es completamente original, se exponen nuestros resultados publicados en [7]. Nuestra aportación en este artículo es la construcción de una medida p-ádica basada en integración sobre ciclos cuadráticos que permite obtener puntos algebraicos en la curva elíptica $E/\mathbb{Q}$, ya que esta medida se define a través de integrales de la forma modular correspondiente a lo largo de caminos que conectan la cúspide del infinito con el punto cuadrático, y por tanto, se pueden ver como el morfismo de parametrización modular evaluado en esos puntos cuadráticos. En concreto, representamos en primer lugar los discos p-ádicos a través de matrices de $\mathrm{GL}\,(2,\mathbb{Q})$ de la siguiente manera:

Dado $a \in \mathbb{Z}$ con $|a| \in \{1,...,p-1\}$, existe una única pareja de enteros $x, y \in \mathbb{Z}$ tales que $ax - py = 1$ y $x \in \{0,...,p-1\}$. Denotemos

$$\gamma_{a,1} = \begin{pmatrix} a & y \\ p & x \end{pmatrix}.$$

Para todo $u \in \mathbb{Z}$ con $0 \leq |u| \leq p-1$, definamos

$$\gamma_u = \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}.$$

Para todo $a \in \mathbb{Z}$ con $1 \leq |a| < p^n$ y $(a,p) = 1$, escribamos $|a| = a_0 + \sum_{k=1}^{n-1} u_k p^k$ with $0 \leq u \leq p-1$. Definamos también

$$\gamma_{a,n} = \begin{cases} \gamma_{u_{n-1}} \gamma_{u_{n-2}} \cdots \gamma_{u_1} \gamma_{a_0,1}, & \text{si } a > 0, \\ \gamma_{-u_{n-1}} \gamma_{-u_{n-2}} \cdots \gamma_{-u_1} \gamma_{-a_0,1}, & \text{si } a < 0. \end{cases}$$

Sea a_p el autovalor de T_p asociado a f y sea α_p una raíz admisible del polinomio de Hecke. Supongamos que $p \nmid N$ o que $p \| N$. Fijemos un

punto cuadrático imaginario τ en el semiplano superior y, dada una matriz $g \in \mathrm{GL}(2,\mathbb{Z})$ con determinante positivo, denotamos $\phi_f^\tau := \int_\tau^{g(\tau)} f(z)dz$. Proponemos la siguiente definición

Definición 7.2.6. Para todo $a \in \mathbb{Z}$ primo con p y para todo $n \geq 1$ tal que $0 \leq a < p^n$, denotemos

$$\Delta_f^\tau(a,n) = \phi_f^\tau(\gamma_{a,n}) - \phi_f^\tau(\gamma_{-a,n}),$$
$$\Delta_f^\tau(pa,n) = \phi_f^\tau(\gamma_p\gamma_{a,n}) - \phi_f^\tau(\gamma_p\gamma_{-a,n}).$$

- Si $p \| N$, definimos

$$\mu_{\mathcal{Q}}\left(a + p^n\mathbb{Z}_p\right) = a_p^{-n}\Delta_f^\tau(a,n).$$

- Si $p \nmid N$, definimos

$$\mu_{\mathcal{Q}}\left(a + p^n\mathbb{Z}_p\right) = \alpha_p^{-n}\left(\Delta_f^\tau(a,n) - \alpha_p^{-1}\Delta_f^\tau(pa,n)\right).$$

Definamos finalmente

$$\mu_{\mathcal{Q}}\left(\mathbb{Z}_p^*\right) = \sum_{a=1}^{p-1}\mu_{\mathcal{Q}}\left(a + p\mathbb{Z}_p\right),$$

y para cada $k \geq 1$, definimos

$$\mu_{\mathcal{Q}}\left(p^k\mathbb{Z}_p\right) = 0.$$

Demostramos en la Proposición 5.2.3 que nuestra medida cuadrática toma valores en un $\mathbb{Q}_p(\alpha_p)$-espacio vectorial de dimensión infinita numerable (α_p es una raíz admisible no nula del polinomio de Hecke). No obstante, sorprendentemente, el $\mathbb{Z}$-módulo donde toma valores la integral modular cuadrática (que resulta ser un 1-cociclo) es finitamente generado.

Exploramos asimismo la relación de las funciones L p-ádicas con la homología de $X_0(N)$ y relacionamos nuestras medidas cuadráticas con la producción de puntos algebraicos en curvas elípticas definidos sobre la extensión abeliana maximal de $\mathbb{Q}(\tau)$, donde τ es el punto cuadrático imaginario de partida. Usamos para ello herramientas de la teoría de puntos de Heegner. Nuestro Teorema 5.3.5 es un resultado en este sentido.

7.3 Formas automorfas

7.3.1 Introducción

El capítulo 6, por un lado, aporta una de las principales construcciones originales de nuestra tesis, a saber, la función L p-ádica asociada a una forma automorfa de peso 2 respecto a un grupo aritmético Fuchsiano indefinido, y por otro, explica los detalles del resultado principal de [5], que asimismo hemos adaptado nosotros a nuestro contexto. Nos centramos por tanto en este capítulo en las curvas de Shimura $X(D,N)$ con $D > 1$. Estas curvas se obtienen como el modelo canónico asociado a los cocientes analíticos $\Gamma(D,N)\backslash\mathcal{H}$, donde $\Gamma(D,N)$ es la imagen en $\mathrm{GL}(2,\mathbb{R})$ del grupo multiplicativo de los elementos de norma reducida 1 del orden de Eichler $\mathcal{O}(D,N)$ asociado al álgebra de cuaterniones sobre $\mathbb{Q}$ de discriminante D (cf. [1]). En concreto, nos ocupamos de la relación entre la homología y nuestra teoría de integración sobre ciclos con base un punto cuadrático, sobre la que construiremos nuestra función L p-ádica cuadrática para estas curvas.

7.3.2 Objetivos, aportaciones fundamentales y conclusiones

Probamos la siguiente generalización del conocido teorema de Manin sobre la homología de $X_0(N)$:

Teorema 7.3.1. *Sea Γ un grupo aritmético fuchsiano de primer tipo. Denotemos por E al conjunto de elementos elípticos de Γ. Sea Γ' el subgrupo conmutador de Γ. Fijemos $\alpha \in \mathcal{H}$. Dado $g \in \Gamma$, definamos $\phi_\alpha(g) = \{\alpha, g(\alpha)\}_\Gamma \in H_1(X(\Gamma)(\mathbb{C}),\mathbb{Z})$. Entonces, la siguiente sucesión de grupos es exacta:*

$$0 \to \Gamma' E \to \Gamma \xrightarrow{\phi_\alpha} H_1(X(\Gamma)(\mathbb{C}),\mathbb{Z}) \to 0,$$

y la aplicación ϕ_α es independiente de α.

Damos un algoritmo de descomposición de ciclos cerrados en curvas de Shimura de signatura $(1,e)$ (algoritmo 6.1.20) en elementos de una base de homología y un planteamiento alternativo al caso modular, con cierto parecido al desarrollo de Manin en fracciones continuas (algoritmo 6.1.22). En definitiva, nos percatamos de que si sustituimos las clases distinguidas de Manin por ciclos cerrados con base un punto cuadrático, podemos definir

un análogo de los símbolos modulares clásicos que denominamos símbolos modulares cuadráticos.

Este símbolo modular cuadrático depende del primo p considerado (es de hecho, en cierto modo, un objeto p-ádico). Asimismo, este símbolo cuadrático da lugar a una distribución p-ádica en el caso en que $p \nmid D$ y $p \| N$ (esta condición se debe a la forma particularmente sencilla en que actúa el operador de Hecke T_p en este caso, aunque en ulteriores investigaciones trataremos de afrontar el caso general). Por último, describimos nuestro espacio de símbolos modulares cuadráticos en términos cohomológicos, inspirándonos en el isomorfismo de Ash-Stevens entre los símbolos modulares clásicos y la cohomología de soporte compacto.

Asimismo, probamos que el espacio de símbolos modulares clásicos tiene una copia isomorfa en la intersección de los espacios de símbolos cuadráticos asociados a cierta familia infinita de primos descrita de manera precisa en función del punto cuadrático. Estos resultados han dado lugar a los preprints [8] y [9], que han sido enviados a publicación. Recientemente, hemos observado que la teoría de puntos CM en curvas de Shimura $X(D, N)$ podría implicar que nuestras distribuciones p-ádicas quadráticas también produjesen puntos algebraicos, ya que la correspondencia de Jacquet-Langlands permite asociar a una forma automorfa, una forma modular cuyos autovalores de Hecke coinciden con los de la forma automorfa de partida, salvo una cantidad finita. Esto supone que las dos funciones L complejas coinciden salvo una cantidad finita de factores de Euler. Controlar estos factores de Euler, no obstante, parece una tarea en absoluto trivial.

Producir explícitamente puntos algebraicos en curvas de Shimura, encontrar ecuaciones para sus modelos canónicos o funciones uniformizantes es una tarea extremadamente delicada. En el Grupo de Teoría de Números de Barcelona se ha trabajado extensivamente en ella, destacándose los trabajos de P. Bayer y A. Travesa ([11], [12]) y de P. Bayer y J. Guàrdia ([10]). Nosotros, en suma, ofrecemos en esta tesis, una relación del problema de producción de puntos algebraicos con el estudio de valores especiales de nuestras funciones L p-ádicas.

Bibliography

[1] M. Alsina, P. Bayer: *Quaternion orders, quadratic forms and Shimura curves*. CRM Monograph Series, 22. American Mathematical Society, Providence, RI 2004.

[2] J. Araujo, W.H. Schikhof: The Weierstrass-Stone approximation theorem for p-adic C^n-functions. *Ann. Math. Blaise Pascal* 1, 1 (1994), 61–74.

[3] A. Arenas, J.C. Lario: Sistema minimal de generadors de $\Gamma_0(N)$. In: *Corbes modulars: taules*. P. Bayer, A. Travesa (eds.). Notes del Seminari de Teoria de Nombres (UB-UAB-UPC) 1 (1992), 165–168.

[4] M.A. Armstrong: On the fundamental group of an orbit space. *Proc. Cambridge Philos. Soc.* 61 (1965), 639–646.

[5] A. Ash, G. Stevens: Modular forms in characteristic ℓ and special values of their L-functions. *Duke Math. J.* 53, 3 (1986), 849–868.

[6] A. Baker: Linear forms in the logarithms of algebraic numbers. *Mathematika* 13 (1966), 204–216.

[7] P. Bayer, I. Blanco-Chacón: Quadratic modular symbols. *RACSAM*, To appear.

[8] P. Bayer, I. Blanco-Chacón: Quadratic modular symbols on Shimura curves (submitted).

[9] P. Bayer, I. Blanco-Chacón, A. F. Boix: Computing quadratic modular symbols (submitted).

[10] P. Bayer, J. Guàrdia: On equations defining fake elliptic curves. *J. Théor. Nombres Bordeaux* 17 no 1 (2005) 57–67.

[11] P. Bayer, A. Travesa: Uniformizing functions for certain Shimura curves, in the case $D = 6$. *Acta Arithmetica* 126 (2007) 315–339.

[12] P. Bayer, A. Travesa: Uniformization of triangle modular curves. *Publ. Mat.* (2007) 43–106.

[13] M. Bertolini, H. Darmon: Heegner points on Mumford-Tate curves. *Invent. Math.* 126 (1996), 413–456.

[14] M. Bertolini, H. Darmon: *The p-adic L-functions of modular elliptic curves.* Springer-Verlag (2001).

[15] B. Birch: Heegner points: the beginnings. In: *Heegner points and Rankin L-series*. H. Darmon, S. W. Zhang (eds.). Math. Sci. Res. Inst. Publ. 49, Cambridge Univ. Press, 2004, 1–10.

[16] I. Blanco-Chacón: A note on the Kubota-Leopoldt p-adic L-function (in process).

[17] I. Blanco-Chacón: Upper triangular operators and p-adic L-functions. *p-adic numbers, ultrametric analysis and applications* 3, 2 (2011), 1–14.

[18] J.F. Boutot, F. Carayol: Uniformisation p-adique des courbes de Shimura: les théorèmes de Cerednik et de Drinfeld. Courbes modulaires et courbes de Shimura. *Astérisque* 196/197, 7, (1991).

[19] A. Brumer: On the units of algebraic number fields. *Mathematika* 14, 2 (1967), 121–124.

[20] D.A. Buell: *Binary quadratic forms. Classical theory and modern computations.* Springer, 1989.

[21] H. Cartan, S. Eilenberg: *Homological algebra.* Princeton University Press (1956).

[22] P. Cassou-Nogués: Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Invent. Math.* 51 (1979), 1, 29–59.

[23] Y. Chuman: Generators and relations of $\Gamma_0(N)$. *J. Math. Kyoto Univ.* 13 (1973), 381–390.

[24] J.E. Cremona: *Algorithms for modular elliptic curves.* Cambridge University Press, 1997.

[25] H. Darmon: *Rational points on modular elliptic curves.* CBMS, Regional Conference Series in Mathematics 101, 2004.

[26] P. Deligne, K. Ribet: Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.* 59 (1980), 227–286.

[27] F. Diamond, J. Shurman: *A first course in modular forms.* Graduate Texts in Mathematics 228. Springer, 2000.

[28] B. Ferrero, L. Washington: The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. Math.* 109 (1979), 377–395.

[29] L. Gerritzen, M. Van der Put: *Schottky groups and Mumford curves.* Lecture notes in Math. 817. Springer, 1980.

[30] R. Greenberg, G. Stevens: p-adic L-functions and p-adic periods of modular forms. *Invent. Math.* 111, 2 (1993), 407-447.

[31] B.H. Gross, D.B. Zagier: Heegner points and derivatives of L-series. *Invent. Math.* 84, 2 (1986), 225-320.

[32] H. Hasse: Über die Klassenzahl abelscher Zahlkörper. Akademie Verlag, Berlin, 1952.

[33] A. Hatcher: *Algebraic topology.* Cambridge University Press, 2002.

[34] K. Iwasawa: Lectures on p-adic L-functions. *Annals of Mathematics Studies* 74, 1972.

[35] H. Jacquet, R. P. Langlands: *Automorphic forms on $GL(2)$.* Lecture Notes in Math. 114. Springer, 1970.

[36] K. Kato: Iwasawa theory and p-adic Hodge theory. *Kodai Math. J.* 16, 1 (1993), 1–31.

[37] M. S. Kim: On Bernouilli Numbers. *J. Korean Math. Soc.,* 37, 3 (2000), 391–410.

[38] C. Klingenberg: On p-adic L-functions of Mumford curves, in: *p-adic Monodromy and the Birch and Swinnerton-Dyer conjecture.* Contemp. Math. 165 (1994), 277-315.

[39] N. Koblitz: *p-adic numbers, p-adic analysis, and zeta-functions.* Second edition. Graduate Texts in Mathematics 58. Springer, 1984.

[40] T. Kubota, H.W. Leopoldt: Eine p-adische Theorie der Zetawerte I. *J. Reine und Angew. Math.* 214/215 (1964), 328–339.

[41] H.W. Leopoldt: Eine p-adische Theorie der Zetawerte II. *J. Reine und Angew. Math.* 274/275 (1975), 328–339.

[42] S. Lang: *Cyclotomic Fields II.* Graduate Texts in Mathematics. Springer, 1980.

[43] H.W. Leopoldt: Zur Arithmetik in abelschen Zahlkörpern. *J. Reine und Angew. Math.* 209 (1962), 54–71.

[44] W. Li: Newforms and functional equations. *Math. Ann.* 212 (1975), 285–315.

[45] Ju. Y. Manin: Parabolic points and zeta functions of modular curves. *Mat. Sbornik* 6 (1972), 19–64.

[46] B. Mazur: Rational isogenies of prime degree. *Invent. Math.* 44 (1978), 129–162.

[47] B. Mazur, P. Swinnerton-Dyer: Arithmetic of Weil curves. *Invent. Math.* 25 (1974), 1–61.

[48] B. Mazur, J. Tate: The p-adic σ-function. *Duke Math.* 62, 3 (1991), 663–688.

[49] B. Mazur, J. Tate, J. Teitelbaum: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.* 84, 1 (1986), 1–48.

[50] P. Mihailescu: The T and T^* components for Λ-modules and Leopoldt's conjecture. Preprint: arXiv:0905.1274 .

[51] A. Néron: Quasi-fonctions et hauteurs sur les variétés abéliennes. *Ann. of Math.* 82 (1965), 249–331.

[52] J. Neukirch: *Algebraische Zahlentheorie*. Grundlehren der mathematischen Wissenschaften. Springer, 1992.

[53] J. Neukirch: *Class field theory*. Springer, 1986.

[54] C. Pérez-García, W.H. Schikhof: *Locally convex spaces over non-Archimedean valued fields.* Cambridge Studies in Advanced Mathematics 119. Cambridge University Press, 2010.

[55] B. Perrin-Riou: Fonctions L p-adiques d'une courbe elliptique et points rationnels. *Ann. Inst. Fourier* 43 (1993), 945–995.

[56] R. Pollack: On the p-adic L-function of a modular form at a supersingular prime. *Duke Math. J.* 118, 3 (2003), 523–558.

[57] R. Pollack, G. Stevens: Critical slope p-adic L-functions. Available at http://math.bu.edu/people/rpollack/Papers.

[58] H. Rademacher: Über die Erzeugende von Kongruenzuntergruppen der Modulgruppe. *Abh. Math. Seminar Hamburg* 7 (1929), 134–138.

[59] K. Ribet: Sur les variétés abéliennes à multiplications réelles. *C.R. Acad Sc. Paris* 291 (1980), 121–123.

[60] A. M. Robert: *A course in p-adic analysis*. Graduate Texts in Mathematics, 198. Springer, 2000.

[61] D. E. Rohrlich: On L-functions of elliptic curves and cyclotomic towers. *Invent. Math.* 75 (1984), 409–423.

[62] D. E. Rohrlich: L-functions and division towers. *Math. Ann.* 281 (1988), 611–632.

[63] V. Rotger: Modular Shimura varieties and forgetful maps. *Trans. Amer. Math. Soc.* 356 (2004), no. 4, 1535–1550.

[64] P. Schneider: *Rigid analytic L-transforms*. Lecture Notes in Math. 1068. Springer, 1984.

[65] G. Shimura: Construction of class fields and zeta functions of algebraic curves. *Ann. of Math.* 85, 2 (1967), 58–159.

[66] G. Shimura: *Introduction to the arithmetic theory of automorphic forms.* Kano Memorial Lectures, 1. Publications of the Mathematical Society of Japan, 11. Iwanami Shoten, Publishers, Tokyo. Princeton University Press, Princeton, N.J., 1971.

[67] T. Shintani: On evaluation of zeta functions of totally real number fields at non-positive integers. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 23, 2 (1976), 393–417.

[68] C. L. Siegel: Über die Fourierschen Koeffizienten von Modulformen. *Nachr. Akad. Wiss. Göttingen, Math.-Phys.* K1, 2 (1968), 7–38.

[69] J. Sijsling: *Equations for arithmetic pointed tori.* Ph.D. Thesis, Universiteit Utrecht, 2010.

[70] J. H Silverman: *The arithmetic of elliptic curves.* Springer, 1986.

[71] K. Takeuchi: Arithmetic Fuchsian groups with signature $(1; e)$. *J. Math. Soc. Japan* 35, 3 (1983). 381–407.

[72] M. F. Vignéras: *Arithmétique des algèbres de quaternions.* Lecture Notes in Mathematics 800. Springer, 1980.

[73] J. Voight: Computing fundamental domains for Fuchsian groups. *J. Théorie des Nombres de Bordeaux* 21 (2009), 467–489.

[74] L. Washington: *Introduction to cyclotomic fields.* Springer, 1982.

[75] Y. Yang: Schwarzian differential equations and Hecke eigenforms on Shimura curves. arXiv: 1110.6284v1 (2011).