MASTER'S DEGREE THESIS

Master of Science in Advanced Mathematics and Mathematical Engineering

Title: p-adic L-functions and Euler systems

Author: Oriol Velasco Falguera

Advisor: Víctor Rotger Cerdà

Departament de Matemàtiques

Academic year: 2021-2022

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Contents

1 Motivation

Many arithmetic objects of interest in number theory can be attached L-functions. These are meromorphic functions on the complex plane, and it is conjectured that special values of L-functions (that is, the values of the L-function at negative integers) encode relevant arithmetic information about the objects that they're defined from.

For instance, if E is an elliptic curve over $\mathbb{Q}$, then we can attach to it an L-function $L(E,s)$, given by analytic continuation of the following product:

$$L(E,s) = \prod_{p \nmid 2\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Where Δ is the conductor of the elliptic curve, $a_p = N_p - p$ and N_p is the number of solutions of the reduction of the elliptic curve modulo p. On the other side, the $\mathbb{Q}$-rational points of E form an abelian group, and the Birch and Swinnerton-Dyer conjecture states that

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$$

A generalization of this conjecture to the case of an L-functions attached to a Galois representation is the *Bloch-Kato conjecture*. We will say something more about it in Section 7.

Much of the current progress for the proof of the Birch and Swinnerton-Dyer conjecture, or the Bloch-Kato conjecture has been done using Euler systems and p-adic L-functions. p-adic L-functions are variants of the classical L-functions: They're analytic functions, but their domain are the p-adic numbers $\mathbb{Z}_p$, instead of the complex plane. There are 2 ways to construct p-adic L-functions. The first one is purely analytic, by interpolation of the special values of the L-function. The second way uses Fontaine's theory of (φ, Γ)-modules, the arithmetic of cyclotomic fields and Iwasawa theory, and is closely connected with Euler systems.

One way to think about the role the different objects play is the following: We want to study the connection between values of L-functions and arithmetic properties of a Galois representation. But this is too difficult, so we study Euler systems, which are connected to both the L-function (via the p-adic L-function) and the arithmetic of the representation. A diagram explains it better

$$\begin{array}{ccc} \text{Galois representation} & \longrightarrow & \text{L-function} \\ \downarrow & & \downarrow \text{p-adic interpolation} \\ \text{Euler system} & \xrightarrow{\text{Explicit reciprocity law}} & \text{p-adic L-function} \end{array}$$

The purpose of this work is to study this circle of ideas in two situations, following [10]: For the case of the p-adic Zeta function of Kubota-Leopoldt, which is the p-adic analogous of the Riemann Zeta function, we construct with full detail the whole diagram: We define the p-adic L-function by means of p-adic interpolation in Section 3, and we prove the explicit reciprocity law in Section 6. For the case of L-functions attached to modular forms, we give the construction of the p-adic L-function in Section 4, and in Section 7 we outline some details about the Euler system and the explicit reciprocity law.

Section 2 and Section 5 can be seen as the introduction of enabling tools: p-adic analysis, which we need mostly for the construction of p-adic L-functions via interpolation, and the theory of (φ, Γ)-modules, which is needed for the explicit reciprocity law.

2 p-adic analysis

This section contains an introduction to p-adic analysis. We introduce some important p-adic concepts that we will need in the following chapters. We assume a certain familiarity with the most basic concepts about p-adic numbers, like the first 2 chapters of [18]. We work with spaces of p-adic functions, whose properties can be formalized in the notion of a p-adic Banach space.

Definition 2.1. A *p-adic Banach space* B is a $\mathbb{Q}_p$ vector space with a lattice B^0 that is separated and complete for the p-adic topology, $B^0 \cong \varprojlim_n B^0/p^n B^0$.

We define a valuation on B by $v_B(x) = \sup_{n\in\mathbb{Z}}\{n \text{ such that } x \in p^n B^0\}$. This integer always exists because the fact that B^0 is a lattice means in particular that $B = B^0[\frac{1}{p}]$.

Observation 2.1. We have the following properties:

i) $v_B(x+y) \geq \min(v_B(x), v_B(y))$
ii) $v_B(\lambda x) = v_p(\lambda) + v_B(x)$, for $\lambda \in \mathbb{Q}_p$.

The examples of p-adic Banach spaces that we will deal with are those of functions over $\mathbb{Z}_p$. For instance, $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ is a p-adic Banach space with lattice $B^0 = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Z}_p)$ and valuation $v_B(f) = \inf_{x\in\mathbb{Z}_p} v_p(f(x))$.

Definition 2.2. A *Banach basis* of a p-adic Banach space B is a family $(e_i)_{i\in I}$ of elements of B satisfying the following two conditions.

i) For every $x \in B$, $x = \sum_{i\in I} x_i e_i$ in a unique way, with $x_i \in \mathbb{Q}_p$, $x_i \to 0$.
ii) $v_B(x) = \inf_{i\in I} v_p(x_i)$

Before dealing with the classical structure of an analysis course (continuous functions, differenciability, measures...), we introduce the p-adic version of the exponential and the logarithm, and also the closely-related Teichmüller character.

2.1 Teichmüller character and p-adic exponential

Lemma 2.1. $\mathbb{Z}_p$ contains exactly $p-1$ $(p-1)$-th roots of unity, and all of them are distinct modulo p.

Proof. This is a corollary of Hensel's Lemma. As $\mathbb{Q}_p$ is a field, the equation $f(x) = x^{p-1} - 1 = 0$ has at most $p-1$ solutions. Moreover, given $1 \leq a \leq p-1$, we have $a^{p-1} - 1 \equiv 0 \mod p$ by Fermat's Little Theorem. Therefore by Hensel's Lemma, for every $1 \leq a \leq p-1$ there is a root $z_a \in \mathbb{Z}_p$ of $x^{p-1} - 1$ such that $z_a \equiv a \mod p$. □

Definition 2.3. The *Teichmüller lift* is the map $\tau : \mathbb{F}_p^* \to \mathbb{Z}_p^*$ that maps every $1 \leq a \leq p-1$ to the only $(p-1)$-th root of unity in $\mathbb{Z}_p$, z_a satisfying that $z_a \equiv a \mod p$. The previous lemma guarantees that it is well defined.

We define the *Teichmüller character* as the map $\omega : \mathbb{Z}_p^* \to \mu_{p-1}$ given by reducing modulo p and then taking the Teichmüller lift.

Notation. In some places they use the term "Teichmüller character" for both τ and ω.

Definition 2.4. We denote by $\langle x \rangle$ the character $\langle \bullet \rangle : \mathbb{Z}_p^* \to 1 + p\mathbb{Z}_p$ defined by $x \mapsto \frac{x}{\omega(x)}$.

It turns out that these characters are closely related with the p-adic exponential function, as we will see next.

Definition 2.5. Let's define $\exp : D \to \mathbb{C}_p$ by $\exp(x) = \sum_{n \geq 0} \frac{s^n}{n!}$. This is called the *$p$-adic exponential*, as it's given by the Taylor series of the usual exponential map in $\mathbb{R}$. However, it can't be defined on the whole $\mathbb{C}_p$, as for it to converge we need s to be small enough to kill the p powers that appear in $n!$ as $n \to \infty$. Therefore, the domain is restricted to $D = \{s \in \mathbb{C}_p | v_p(s) \geq \frac{1}{p-1}\}$.

Analogously, we define the p-adic logarithm in terms of power series.

Definition 2.6. Let $\log : R \to \mathbb{C}_p$ be the map defined by $\log(s+1) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{s^n}{n}$. The domain of convergence is $R = \{s \in \mathbb{C}_p | |s-1|_p < 1\}$.

The domain of the p-adic logarithm is not the whole $\mathbb{C}_p$, but, unlike the case of the exponential, it can be extended by the whole $\mathbb{C}_p$, using the following lemma:

Lemma 2.2. ([9], Proposition 4.4.44) $\mathbb{C}_p = p^{\mathbb{Q}} \times \mu \times R$, where μ denotes the set of roots of unity of degree prime to p and R is the set in the definition of the logarithm.

Then, we can write every $s \in \mathbb{C}_p$ as $s = p^r w u$ and define $\log(s) := \log(u)$. In addition, note that if we restrict to $\mathbb{Z}_p$, $\log(s) \in p\mathbb{Z}_p$ (this is given by the power series expression). Similarly, $\exp(s) \in 1 + p\mathbb{Z}_p$ for $s \in p\mathbb{Z}_p$. Moreover, the maps $\exp : p\mathbb{Z}_p \to 1 + p\mathbb{Z}_p$ and $\log : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$ are inverses (c.f [11] for more details).

Proposition 2.1. i) $\omega(x) = \lim_{n \to \infty} x^{p^n}$
ii) $\langle x \rangle = \exp(\log(x))$

Proof. i) By Fermat's Little theorem, $x^{p^n} \equiv x \mod p$. Moreover, $(\lim_{n\to\infty} x^{p^n})^p = \lim_{n\to\infty} x^{p^n}$ and so $\lim_{n\to\infty} x^{p^n}$ is a $p-1$ root of unity such that is congruent to x modulo p, and by Lemma 2.1 it is $\omega(x)$.
ii) Let's write $x = \omega(x)\langle x \rangle$. Then, by definition of logarithm, we have $\log(x) = \log(\langle x \rangle)$. So, taking exponentials, $\exp(\log(x)) = \exp\log(\langle x \rangle) = \langle x \rangle$.

□

2.2 Continuous functions on $\mathbb{Z}_p$

We want to study continuous functions in the p-adic setting. What we will see is that this p-adic Banach space has a basis, consisting of the binomial functions (Theorem 2.1). We will explode this property, that simplifies a lot dealing with these functions, as every $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ is completely characterized by a sequence of coefficients.

Definition 2.7. We define the binomial function $\binom{x}{n}$ (for $x \in \mathbb{Z}_p$) as

$$\binom{x}{n} = \begin{cases} 1 & \text{if } n = 0 \\ \frac{x(x-1)\ldots(x-n+1)}{n!} & \text{if } n \geq 1 \end{cases}$$

Lemma 2.3. $v_{\mathcal{C}^0}\left(\binom{x}{n}\right) = 0$

Proof. Since $\binom{n}{n} = 1$, we have $v_{\mathcal{C}^0}(\binom{x}{n}) = \inf_{x\in\mathbb{Z}_p} v_p(\binom{x}{n}) \leq v_p(\binom{n}{n}) = 0$. On the other side, if $x \in \mathbb{N}$, then $\binom{x}{n} \in \mathbb{N}$ and so $v_p(\binom{x}{n}) \geq 0$. Therefore $v_p(\binom{x}{n}) \geq 0$ for every $x \in \mathbb{Z}_p$, as $\mathbb{N}$ is dense in $\mathbb{Z}_p$. □

Definition 2.8. Given $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ we define $f^{[k]}$ by

$$\begin{cases} f^{[k]}(x) = f(x) & \text{if } k = 0 \\ f^{[k]}(x) = f^{[k-1]}(x+1) - f^{[k-1]}(x) & \text{if } n \geq 1 \end{cases}$$

We denote $a_n(f) := f^{[n]}(0)$, and we call them the *Mahler coefficients of f.*

Proposition 2.2.

$$f^{[n]}(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(x+n-k)$$

Proof. We proceed by induction on n. The base case is simply the definition of $f^{[1]} = f(x+1) - f(x)$. Assume true the statement for n, and let's prove it for $n+1$. By definition we have

$$f^{[n+1]}(x) = f^{[n]}(x+1) - f^{[n]}(x)$$

Now applying the induction hypothesis, we have

$$f^{[n+1]}(x) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(x+1+n-k) - \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(x+n-k) =$$
$$= \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(x+(n+1)-k) + \sum_{k'=1}^{n+1} (-1)^{k'} \binom{n}{k} f(x+(n+1)-k')$$

where we have let $k' = k+1$ in the second summatory. Then we can group the terms that are different from $0, n+1$ and we obtain

$$f^{[n+1]}(x) = f(x+n+1) + \sum_{k=1}^{n} (-1)^k f(x+(n+1)-k) \left(\binom{n}{k} + \binom{n}{k-1} \right) + (-1)^{n+1} f(x)$$

Now note that we have $f(x+n+1) = (-1)^0 \binom{n}{0} f(x+n+1-0)$ and $(-1)^{n+1} f(x) = (-1)^{n+1} \binom{n+1}{n+1} f(x+(n+1)-(n+1))$ and $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$. In conclusion, we have the desired expression

$$f^{[n+1]}(x) = \sum_{k=0}^{n+1} (-1)^k \binom{n+1}{k} f(x+(n+1)-k)$$

□

Observation 2.2. In particular, this proposition gives an expression for the Mahler coefficients:

$$a_n(f) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(n-i)$$

Lemma 2.4. Let $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$. Then, there exists $k \in \mathbb{N}$ such that

$$v_{\mathcal{C}^0}(f^{[p^k]}) \geq v_{\mathcal{C}^0}(f) + 1$$

Proof. Using the result of Proposition 2.2, we have that

$$f^{[p^k]}(x) = f(x+p^k) - f(x) + \sum_{i=1}^{p^k-1} (-1)^i \binom{p^k}{i} f(x+p^k-i) + (1+(-1)^{p^k}) f(x)$$

Where the last term is just a correction of the sign of $f(x)$. Now note that $v_p\binom{p^k}{i} \geq 1$ if $1 \leq i \leq p^k - 1$ and $v_p(1+(-1)^{p^k}) \geq 1$ (if $p \neq 2$ this is 0 which has valuation ∞ and if $p = 2$ this is 2 which has valuation 1). On the other side, since $\mathbb{Z}_p$ is compact, and f is continuous, f is then automatically uniformly continuous, and so for every $c \in \mathbb{R}$, there exists an $N \in \mathbb{N}$ such that, when $v_p(x-y) \geq N$ we have $v_p(f(x) - f(y)) \geq c$. Therefore, making k greater, we can make $v_p(f(x+p^k) - f(x))$ arbitrarily big, and so in conclusion, $v_p(f^{[p^k]}(x)) = \min\{v_p(f(x+p^k) - f(x)), v_p(\sum_{i=1}^{p^k-1}(-1)^i\binom{p^k}{i} f(x+p^k-i) + (1+(-1)^{p^k}) f(x))\}$ and so

$$v_{\mathcal{C}^0}(f^{[p^k]}) \geq v_{\mathcal{C}^0}(f) + 1$$

□

Theorem 2.1. *Let $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$. Then, we have*

i) $\lim_{n\to\infty} v_p(a_n(f)) = +\infty$
ii) For every $x \in \mathbb{Z}_p$, $f(x) = \sum_{n=0}^{\infty} a_n(f)\binom{x}{n}$
iii) $v_{\mathcal{C}^0}(f) = \inf_n v_p(a_n(f))$

Proof. First of all, we define $l_\infty = \{a = (a_n)_{n\in\mathbb{N}}$ such that $a_n \in \mathbb{Q}_p$ is bounded $\}$, with valuation $v_{l_\infty}(a) = \inf_{n\in\mathbb{N}} v_p(a_n)$.

We claim that the map $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p) \to l_\infty$ defined by $f \mapsto a(f) = (a_n(f))_{n\in\mathbb{N}}$ is continuous, as given $f, g \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, $v_{\mathcal{C}^0}(f-g) = \inf_{x\in\mathbb{Z}_p} v_p((f-g)(x))$. On the other side, we have $v_{l_\infty}(a(f) - a(g)) = \inf_{n\in\mathbb{N}} v_p(a_n(f-g))$. But as $a_n(f-g) = \sum_{i=0}^{n}(-1)^i\binom{n}{i} f(n-i)$ using the properties of the valuation of the sum and Lemma 2.3, we have $v_p(a_n(f) - a_n(g)) = \min_{i\in\{0,\dots,n\}} f(n-i)$, and so $v_{l_\infty}(a(f) - a(g)) = \inf_{n\in\mathbb{N}} f(n)$.

Therefore

$$\|f-g\|_p = p^{-v_{\mathcal{C}^0}(f-g)} = p^{-\inf_{x\in\mathbb{Z}_p} v_p(f-g)(x)} \geq p^{-\inf_{n\in\mathbb{N}} v_p(f-g)(n)} = p^{-v_{l_\infty} a(f)-a(g)} = \|a(f)-a(g)\|_{l_\infty}$$

Therefore $\forall \epsilon > 0, \exists \delta = \epsilon$ such that $\|f-g\|_p < \delta$ implies $\|a(f) - a(g)\|\epsilon$, so the map $f \mapsto a(f)$ is continuous and

$$v_{l_\infty}(a(f)) \geq v_{\mathcal{C}^0}(f) \tag{1}$$

Now we define $l^0_\infty := \{(a_n)_{n\in N} \in l_\infty \text{ such that } \lim_{n\to\infty} a_n = 0\}$. It is a closed subspace of l_∞, as the map $T : l_\infty \to \mathbb{R}$ defined by $(a_n) \mapsto \limsup_n \|a_n\|_p$ is continuous, and $l^0_\infty = T^{-1}(\{0\})$, so it is closed in l_∞. By the same argument, $B := \{f \text{ such that } a(f) \in l^0_\infty\}$ is closed in $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$.

Now we define the morphism $l^0_\infty \to \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ given by $a \mapsto f_a = \sum_{n=0}^\infty a_n \binom{x}{n}$. This is a well defined map, as $a_n \to 0$. Moreover

$$v_{\mathcal{C}^0}(f_a) \geq \inf_n (a_n \binom{x}{n}) = \inf_n v_p a_n = v_{l_\infty}(a) \tag{2}$$

where the first equality is given by Lemma 2.3.

On the other hand, $f_a^{[k]} = \sum_{n=0}^\infty a_{n+k} \binom{x}{n}$. This can be shown by induction on k: The case $k = 0$ is just the definition of f_a. Assume that the statement holds for k and let's show it for $k+1$. Indeed, $f_a^{[k+1]} = f_a^{[k]}(x+1) - f_a^{[k]}(x) = \sum_{n=0}^\infty (a_{n+k}\binom{x+1}{n} - \binom{x}{n})$. The term $n = 0$ vanishes and so we have (letting $n' = n - 1$)

$$f_a^{[k+1]} = \sum_{n'=0}^\infty a_{n'+1+k} \left(\binom{x+1}{n'+1} - \binom{x}{n'+1} \right) = \sum_{n=0}^\infty a_{n+k+1} \binom{x}{n}$$

where in the last equality we have used that $\binom{x+1}{n+1} - \binom{x}{n+1} = \binom{x}{n}$.

For every n we have $a_n(f) = f^{[n]}(0) = a_n$, and so $a(f_a) = a$. Moreover, $f \mapsto a(f)$ is injective, as $a(f) = 0$ implies that $f(n) = 0$ for every n, but therefore $f(x) = 0$ as $\mathbb{N}$ is dense in $\mathbb{Z}_p$.

Now let $f \in B$. $a(f) \in l^0_\infty$ implies that $f - f_{a(f)} = 0$ because $a(f - f_{a(f)}) = a(f) - a(f) = 0$, and a is injective. So if $f \in B$ (i) and (ii) are immediately satisfied. We claim that $B = \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$. Using Lemma 2.4 repeatedly, we have that, for every $c = v_{\mathcal{C}^0}(f) + k$, $v_{\mathcal{C}^0}(f^{[N]}) \geq c$. Therefore, $a_n(f) \to \infty$, or, equivalently, $f \in B$. This finishes the proof of (i) and (ii).

Finally, using Equation (1) and Equation (2), we have that $v_{l_\infty}(a(f)) = v_{\mathcal{C}^0}(f)$, which proves (iii). □

Now let's define the power functions on $\mathbb{Z}_p$, which will be needed to construct p-adic L-functions.

Definition 2.9. Let $z \in \mathbb{C}_p$ such that $v_p(z-1) > 0$. Then, we define $z^x \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$ by

$$z^x := \sum_{n=0}^\infty \binom{x}{n} (z-1)^n$$

The function is well defined as it converges because $v_p(z-1) > 0$. The notation is chosen because it agrees with the usual power function with basis z, if $x \in \mathbb{N}$.

2.3 $\mathcal{C}^k$ functions

Let's introduce the notion of differentiability in the p-adics. The usual notion of differenciability in this setting fails to have some good properties (we will see this in Example 2.1). The most natural notion in this setting is the one that we introduce below, sometimes called *strict differentiation*.

Definition 2.10. Given $f : \mathbb{Z}_p \to \mathbb{Q}_p$, we define $f^{\{i\}}(x)$ recursively as $f^{\{0\}}(x) = f(x)$ and $f^{\{i\}}(x, h_1, h_2, \ldots, h_i) = \frac{1}{h_i}\left(f^{\{i-1\}}(x + h_i, h_1, h_2, \ldots, h_{i-1}) - f^{\{i-1\}}(x, h_1, h_2, \ldots, h_{i-1})\right)$

Observation 2.3. $f^{\{i\}}$ is an analogue of the derivation in $\mathcal{C}(\mathbb{R}, \mathbb{C})$. In fact, if $f : \mathbb{R} \to \mathbb{C}$ is $\mathcal{C}^k$, we have

$$f^{\{i\}}(x, h_1, h_2, \ldots, h_i) = \int_{[0,1]^i} f^{(i)}(x + t_1 h_1, \ldots, t_i h_i) dt_1 \cdots dt_i$$

Therefore, if f is $\mathcal{C}^k$, $f^{\{i\}}$ is continuous and $f^{\{i\}}(x, 0, \ldots, 0) = f^{(i)}(x)$. We use this fact to give a definition of $\mathcal{C}^k$ functions for $f : \mathbb{Z}_p \to \mathbb{Q}_p$.

Definition 2.11. We say that $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is $\mathcal{C}^k$ if $f^{\{i\}}$ can be extended to a continuous function in $(\mathbb{Z}_p)^{i+1} \to \mathbb{Q}_p$, for every $i \leq k$.

By induction on i, it is immediate to prove that, if $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, then $v_p(f^{\{i\}}(x, h_1, h_2, \ldots, h_i)) \geq v_{\mathcal{C}^0}(f) - \sum_{j=1}^{i} v_p(h_j)$.

Example 2.1. We show that the definition of $\mathcal{C}^k$ functions that we have given is not equivalent to the usual one, and moreover, we show that the usual definition is not as good as the one provided, as, for instance, there can be nonconstant functions with derivative 0. Indeed, take $f : \mathbb{Z}_p \to \mathbb{Q}_p$ given by $\sum_{n=0}^{\infty} p^n a_n \mapsto \sum_{n=0}^{\infty} p^{2n} a_n$. Then, we have $v_p(f(x) - f(y)) = 2v_p(x - y)$ and so the function is continuous, and $f'(x) = 0$ for every x. In consequence, $f^{(k)} = 0$, and the function would be $\mathcal{C}^k$ with the usual definition.

However,

$$f^{\{2\}}(x, h_1, h_2) = \frac{1}{h_2}\left(\frac{f(x + h_1 + h_2) - f(x + h_1)}{h_1} - \frac{f(x + h_1) - f(x)}{h_1}\right)$$

And, therefore,

$$f^{\{2\}}(0, p^n, p^n) = \frac{1}{p}\left(\frac{2p^{2n} - p^{2n}}{p^n} - \frac{p^{2n}}{p^n}\right) = 0$$

$$f^{\{2\}}((p-1)p^n, p^n, p^n) = \frac{1}{p^n}\left(\frac{p^{2n+1} + p^{2n} - p^{2n+1}}{p^n} - \frac{p^{2n+1} - (p-1)p^{2n}}{p^n}\right) = \frac{p^{2n+1}}{p^{2n}} = p$$

Therefore, as $n \to \infty$, $|(p-1)p^n| \to 0$, but $f^{\{2\}}((p-1)p^n, p^n, p^n) \not\to f^{\{2\}}(0, p^n, p^n)$, and so it's impossible to extend this function continuously, and f is not $\mathcal{C}^2$ in the strict differentiable case.

Definition 2.12. On the set of $\mathcal{C}^k$ functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$, we define a valuation as $v_{\mathcal{C}^k}(f) = \min_{0 \leq i \leq k} \inf_{(x, h_1, \ldots, h_i) \in \mathbb{Z}_p^{i+1}} v_p(f^{\{i\}}(x, h_1, \ldots, h_i))$. This gives $\mathcal{C}^k$ the structure of a Banach space.

Theorem 2.2. *(Barsky) Let* $L(n, k) = \max\{\sum_{j=1}^{i} v_p(n_j), i \leq k, \sum n_j = n, n_j \geq 1\}$. *Then,* $p^{L(n,k)}\binom{x}{n}$ *is a Banach basis of* $\mathcal{C}^k$.

To prove Barsky's theorem, we need a Lemma (which we don't prove, it is essentially Mahler's theorem in n variables).

Lemma 2.5. (Mahler's Theorem in several variables, c.f. [10], Theorem 1.6.6) Let $g(x_0,\dots,x_i):\mathbb{Z}_p^i\to\mathbb{Q}_p$. We define the action $\alpha_j^{[k]}$ on g by $\alpha_j^{\lceil}1]g(x_0,\dots,x_i)=g(x_0,\dots,x_j+1,\dots,x_i)-g(x_0,\dots,x_i)$, and $\alpha_j^{[k]}=\alpha_j^{[1]}\circ\cdots\circ\alpha_j^{[1]}$ (the composition k times of $\alpha_j^{[1]}$).Define also $\alpha_{k_0,\dots,k_i}(g)=(\alpha_0^{[k_0]}\dots\alpha_0^{[k_0]}g)(0,\dots,0)$.
Then, $g:\mathbb{Z}_p^{i+1}\to\mathbb{C}_p$ is continuous if and only if $a_{k_0,\dots,k_i}(g)\to 0$ for all $(k_0,\dots,k_i)\to\infty$, and we have

$$g(x_0,\dots,x_i)=\sum_{k_0,\dots,k_i\in\mathbb{N}}a_{k_0,\dots,k_i}(g)\binom{x_0}{k_0}\cdots\binom{x_i}{k_i}$$

Reciprocally, if $a_{k_0,\dots,k_i}\to\infty$, then g defined by the expression above is continuous.

Proof. (of Barsky's theorem) Denote by $P_n=\binom{x}{n}$. We claim that

$$P_n^{\{i\}}(x_0,h_1,\dots,h_i)=\sum_{n_0+\cdots+n_i=n,n_k\geq 1}\frac{1}{n_1\cdots n_i}\binom{x_0}{n_0}\binom{h_1-1}{n_1-1}\cdots\binom{h_i-1}{n_i-1}$$

To prove the claim, let $g_T(x)=(1+T)^x$. Then,

$$g_T^{\{i\}}(x,h_1,\dots,h_i)=\frac{1}{h_1\dots h_i}\left(\sum_{I\subset\{1,\dots,i\}}(-1)^{i-|I|}g_T(x+\sum_{j\in I}h_j)\right)=$$
$$=(1+T)^x\prod_{j=1}^{i}\frac{(1+T)^{h_j}-1}{h_j}$$

On the other side, $g_T(x)=\sum_{n\geq 0}\binom{x}{n}T^n$, so $g_T^{\{i\}}(x)=\sum_{n\geq 0}P_n^{\{i\}}T^n$. Therefore, equating the same powers of T in both expressions, we obtain the equality claimed.

After proving this claim, take a general $f\in\mathcal{C}^0(\mathbb{Z}_p,\mathbb{Q}_p)$, $f=\sum_{n\geq 0}a_n(f)\binom{x}{n}$ by Mahler's theorem. Then, we have by the claim, $f^{\{i\}}(x_0,\dots,x_i)=\sum_{n=0}^{\infty}a_n(f)P_n^{\{i\}}(x_0,\dots,x_i)$. Now we define $Q_{n,i}(x_0,\dots,x_i):=P_n^{\{i\}}(x_0,x_1+1,\dots,x_i+1)$ and $g_i(x_0,\dots,x_i)=\sum_{n=0}^{\infty}a_n(f)Q_{n,i}$. It's clear that $f\in\mathcal{C}^k$ if and only if g_i is continuous for every $i\leq k$.

We have that $a_{n_0,n_1-1,\dots,n_i-1}(g_i)=\sum_n a_n(f)a_{n_0,n_1-1,\dots n_i-1}(Q_{n,i})$, with

$$a_{n_0,n_1-1,\dots n_i-1}(Q_{n,i})=\begin{cases}0 & \text{if } n\neq\sum_{j=0}^{i}n_j\\ \frac{1}{n_1\cdots n_i} & \text{if } n=\sum_{j=0}^{i}n_j\end{cases}$$

Therefore, by Mahler's theorem in several variables g_i is continuous if and only if $a_{n_0,n_1-1,\dots n_i-1}(g_i)=\frac{a_{n_0,n_1-1,\dots n_i-1}(Q_{n,i})}{n_1\cdots n_i}\to 0$ as $n\to\infty$, and this must hold for every $n_1,\dots,n_i$ such that $\sum_{j=1}^{i}n_j=n$, $i\leq k$. This is true if and only if $v_p(a_n(f))\geq L(n,k)$, so $p^{L(n,k)}$ is a Banach basis for $\mathcal{C}^k$. □

There's also an easy characterisation of a function belonging to $\mathcal{C}^k$ in terms of its Mahler coefficients, taking into account the fact that the asimptotics of $L(n,k)$ is the same of $k\frac{\log n}{\log k}$.

Proposition 2.3. The following are equivalent, for $f=\sum_{n=0}^{\infty}a_n(f)\binom{x}{n}$.

i) $\sum_{n=0}^{\infty} a_n \binom{x}{n} \in \mathcal{C}^k$.
ii) $\lim_{n\to\infty} v_p(a_n) - k\frac{\log n}{\log p} = \infty$.
iii) $\lim_{n\to\infty} n^k |a_n|_p = 0$.

In particular, $C^k(\mathbb{Z}_p, \mathbb{Q}_p)$ becomes a Banach space with the valuation

$$v_{\mathcal{C}^k}(f) = \inf_{n\in\mathbb{N}} \left\{ v_p(a_n) - r\frac{\log(1+n)}{\log p} \right\}$$

2.4 Analytic and locally analytic functions

Lemma 2.6. Let $(a_n)_{n\in\mathbb{N}}$, with $a_n \in \mathbb{C}_p$ such that $v_p(a_n) \to \infty$. Let $f = \sum_{n=0}^{\infty} a_n T^n$. Then, we have

i) If $x_0 \in \mathcal{O}_{\mathbb{C}_p}$, $f^{(k)}(x_0)$ converges for every k, and $\lim_{k\to\infty} v_p(f^{(k)}(x_0)/k!) = \infty$.
ii) Given $x_0, x_1 \in \mathcal{O}_{\mathbb{C}_p}$, $f(x_1) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!}(x_1 - x_0)^n$, and $\inf_n v_p\left(\frac{f^{(n)}(x_0)}{n!}\right) = \inf_n v_p(a_n)$.
iii) $\inf v_p(a_n) = \inf_{x\in\mathcal{O}_{\mathbb{C}_p}} v_p(f(x))$ and $v_p(f(x)) = \inf v_p(a_n)$ almost everywhere (outside a finite number of $x_i + \mathfrak{m}_{\mathbb{C}_p}$).

Proof. i) $\frac{f^{(k)}}{k!} = \sum_{n=0}^{\infty} a_{n+k}\binom{n+k}{k}T^n$. For $T = x_0$, $v_p(\binom{n+k}{k}) = 0$, $v_p(x_0^n) \geq 0$, and so $|a_{n+k}\binom{n+k}{k}x_0^n| \to 0$ and the sequence converges. Moreover, as $v_p(x_0) \geq 0$, we have

$$v_p\left(\frac{f^{(k)}(x_0)}{k!}\right) \geq \inf v_p(a_n) = \inf v_p\left(\frac{f^{(n)}}{n!}\right)$$

ii) Write $x_1 = (x_1 - x_0) + x_1$, and so we have

$$f(x_1) = \sum_{n=0}^{\infty} a_n x_1^n = \sum_{n=0}^{\infty} a_n \sum_{k=0}^{n} \binom{n}{k}(x_1 - x_0)^k x_0^{n-k} = \sum_{k=0}^{\infty}\left(\sum_{n=0}^{\infty} a_n \binom{n}{k} x_0^{n-k}\right)(x_1 - x_0)^k$$

But we know that $\sum_{n=0}^{\infty} a_n\binom{n}{k}x_0^{n-k} = \frac{f^n(x_0)}{n!}$, hence the result. Moreover, exchanging 0 and x_0 we have $\inf_n v_p\left(\frac{f^{(n)}(x_0)}{n!}\right) = \inf_n v_p(a_n)$.

iii) For every $x \in \mathcal{O}_{\mathbb{C}_p}$, $v_p(x) \geq 0$, so we have $\inf v_p(a_n) \leq \inf_{x\in\mathcal{O}_{\mathbb{C}_p}} v_p(f(x))$. Therefore it's enough to find an x satisfying the equality. As $\lim_{n\to\infty} v_p(a_n) = \infty$, there exists an a_{n_0} such that $\inf v_p(a_n) = v_p(a_{n_0})$. Therefore we can divide everything by a_{n_0} and assume that $\inf v_p(a_n) = 0$.

Let $\overline{f}(T)$ be the reduction of f modulo $\mathfrak{m}_{\mathbb{C}_p}$. If $x \in \mathcal{O}_{\mathbb{C}_p}$ doesn't reduce to a root of $\overline{f}$, then $\overline{(f)}(x) \neq 0$, which happens if and only if $v_p(f(x)) = 0$.

Therefore the equality $\inf v_p(a_n) = \inf_{x\in\mathcal{O}_{\mathbb{C}_p}} v_p(f(x))$ holds for x, so it holds for all but a finite number of $x + \mathfrak{m}_{\mathbb{C}_p}$, and in particular $\inf v_p(a_n) = \inf_{x\in\mathcal{O}_{\mathbb{C}_p}} v_p(f(x))$.

□

After this introductory result about power series and convergence in the p-adics, we introduce the notion of analytic p-adic function, which is completely analogous to the usual one.

Definition 2.13. Denote $D(x_0, r) = \{x \in \mathbb{C}_p | v_p(x - x_0) \geq r\}$. We say that a function $f : D(x_0, r) \to \mathbb{C}_p$ is *analytic* if $f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n$.

Observation 2.4. $\sum_{n=0}^{\infty} \frac{f^n(x_0)}{n!}(x-x_0)^n$ converges if and only if $v_p\left(\frac{f^n(x_0)}{n!}\right) + nv_p(x-x_0) \to \infty$. But in $D(x_0, r)$ we have $v_p(x - x_0) > r$, so the formal sum converges in $D(x_0, r)$ if and only if

$$v_p\left(\frac{f^{(n)}(x_0)}{n!}\right) + nr \to \infty$$

This motivates the following definition.

Definition 2.14. The set of analytic functions $f : D(x_0, r) \to \mathbb{C}_p$ forms a Banach space with valuation

$$v_{x_0}^{\{r\}}(f) = \inf_n \left\{ \left(\frac{f^{(n)}(x_0)}{n!} \right) + nr \right\}$$

Now we introduce the notion of locally analytic function.

Definition 2.15. Let $h \in \mathbb{N}$. The space $LA_h(\mathbb{Z}_p, \mathbb{Q}_p)$ is the space of functions whose restriction to $x_0 + p^h\mathbb{Z}_p$ is the restriction of an analytic function f_{x_0} on $D(x_0, h)$, for every $x_0 \in \mathbb{Z}_p$. This is a Banach space with the valuation

$$v_{LA_h}(f) = \inf_{x_0} v_{x_0}^{\{h\}}(f_{x_0})$$

It is immediate from the definition that every function in LA_h can be written as

$$f(x) = \sum_{j=0}^{p^h-1} 1_{j+p^h\mathbb{Z}_p}(x) \sum_{k=0}^{\infty} a_{k,j} \left(\frac{x-j}{p^h} \right)^k$$

In consequence, a Banach basis of LA_h is

$$e_n = 1_{j+p^h\mathbb{Z}_p} \left(\frac{x-j}{p^h} \right)^{m-1}$$

For $n = mp^h - i$, and $1 \leq i \leq p^h$.

The following result gives another Banach basis of LA_h that is more manageable.

Theorem 2.3. *The functions* $\lfloor \frac{n}{p^h} \binom{x}{n} \rfloor$ *are a Banach basis of* LA_h.

The proof is quite long and is essentially managing the expressions of e_n and $\lfloor \frac{n}{p^h} \binom{x}{n} \rfloor$. See [10], Theorem 1.7.8.

Definition 2.16. Let $LA = \{\text{locally analytic functions on } \mathbb{Z}_p\} = \cup_h LA_h$, be the set of locally analytic functions. It's not a Banach space, but an inductive limit of Banach spaces.

In particular, we observe that a sequence $f_n \to f$ is in LA if and only if there exists an h such that for every n, $f_n \in LA_h$ and $f_n \to f$ in LA_h. As a corollary of Theorem 2.3, and using the fact that $\frac{1}{n} v_p(\lfloor \frac{n}{p^h} \binom{x}{n} \rfloor) \sim \frac{1}{(p-1)p^h}$, we have the following result

Theorem 2.4. *The function* $f = \sum_{n=0}^{\infty} a_n \binom{x}{n}$ *is in* LA *if an only if there exists* $r > 0$ *such that* $v_p(a_n) - rn \to \infty$.

2.5 Measures and distributions

Definition 2.17. A *distribution* on $\mathbb{Z}_p$ with values in a p-adic Banach space B is a continuous linear map

$$\mu : LA(\mathbb{Z}_p, \mathbb{Q}_p) \longrightarrow B \tag{3}$$

$$f \longmapsto \mu(f) =: \int_{\mathbb{Z}_p} f(x)\mu(x) \tag{4}$$

We denote by $\mathcal{D}(\mathbb{Z}_p, B)$ the set of distributions on $\mathbb{Z}_p$ with values in B.

Definition 2.18. A *measure* on $\mathbb{Z}_p$ with values in a p-adic Banach space B is a continuous linear map

$$\mu : \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p) \longrightarrow B \tag{5}$$

$$f \longmapsto \mu(f) =: \int_{\mathbb{Z}_p} f(x)\mu(x) \tag{6}$$

We denote by $\mathcal{D}_0(\mathbb{Z}_p, B)$ the set of measures on $\mathbb{Z}_p$ with values in B. It is a p-adic Banach space with valuation

$$v_{\mathcal{D}_0}(\mu) = \inf_{f \neq 0} \left(v_p \left(\int_{\mathbb{Z}_p} f\mu \right) - v_{\mathcal{C}^0}(f) \right)$$

Observation 2.5. The definition of measure that we have just given is equivalent to the one given usually in calculus courses, i.e, as an additive function on the set of compact open sets of $\mathbb{Z}_p$. See for instance [16].

Definition 2.19. A distribution μ is a *distribution of order* r on $\mathbb{Z}_p$ with values in a p-adic Banach space B if it extends to a continuous linear map

$$\mu : \mathcal{C}^r(\mathbb{Z}_p, \mathbb{Q}_p) \longrightarrow B \tag{7}$$

$$f \longmapsto \mu(f) =: \int_{\mathbb{Z}_p} f(x)\mu(x) \tag{8}$$

We denote by $\mathcal{D}_r(\mathbb{Z}_p, B)$ the set of measures on $\mathbb{Z}_p$ with values in B. It is a p-adic Banach space with valuation

$$v'_{\mathcal{D}_r}(\mu) = \inf_{f \in \mathcal{C}^r} \left(v_p \left(\int_{\mathbb{Z}_p} f\mu \right) - v_{\mathcal{C}^r}(f) \right)$$

Moreover, denote by $LP^{[0,N]}$ the set of locally polynomial functions on $\mathbb{Z}_p$, of degree no more than N. We have the following result, that will be needed in Section 4. The proof is skipped, because it's tedious and not very enlightening, but can be found in [10], Theorem 1.9.7.

Theorem 2.5. *Let $r \geq 0$, $N \geq r$. If $f \mapsto \int_{\mathbb{Z}_p} f\mu$ is a linear function from $LP^{[0,N]}$ to a Banach space B, such that $\exists C$*

$$v_p\left(\int_{a+p^n\mathbb{Z}_p} (x-a)^j \mu\right) \geq C + (j-r)n$$

for every $a \in \mathbb{Z}_p$, $n, j \in \mathbb{N}$, then μ extends uniquely to a distribution of order r.

3 p-adic zeta functions of Kubota-Leopoldt

The aim of this chapter is to construct a p-adic zeta function: An analogous of the Riemann Zeta function but with p-adic domain instead of $\mathbb{C}$. We will do this by interpolating the Riemann Zeta function at its special values. However, this can't be done with whole generality, and we will have to make some slight modifications to ζ in order to be able to interpolate it p-adically. All the construction is explained in detail in [10].

We will also construct p-adic L-functions attached to Dirichlet characters, which are a generalization of the case of the Riemann's zeta function. The reference we follow for this second method is [22].

3.1 Introduction: The Riemann Zeta function

Let

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \qquad \text{if } \mathrm{Re}(s) > 1$$

The second expression of ζ as a product is called an *Euler product*.

Recall that the gamma function Γ is the analytic continuation to $\mathbb{C}$ of $\Gamma(s) = \int_0^{+\infty} e^{-t} t^s \frac{dt}{t}$. We also have $n^{-s} = \frac{1}{\Gamma(s)} \int_0^{+\infty} e^{-nt} t^s \frac{dt}{t}$, and therefore

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} \sum_{n=1}^{+\infty} e^{-nt} t^s \frac{dt}{t} = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{1}{e^t - 1} t^s \frac{dt}{t}$$

The following lemma guarantees that ζ can be analytically continued to $\mathbb{C}$.

Lemma 3.1. Let $f : \mathbb{R}_+ \to \mathbb{C}$ be a $\mathcal{C}^\infty$ function on $\mathbb{R}_+$, such that $\lim_{t \to +\infty} t^n f(t) = 0$ for every $n \in \mathbb{N}$. Then, $L(f, s)$ defined for $\mathrm{Re}(s) > 0$ as

$$L(f, s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} f(t) t^s \frac{dt}{t}$$

has an analytic continuation to $\mathbb{C}$, and we have

$$L(f, -n) = (-1)^n f^n(0)$$

Proof. First note that, to prove that $L(f, s)$ converges for $Re(s) > 0$, it's enough to show that $\int_0^{+\infty} f(t) t^s \frac{dt}{t}$ converges, as $\Gamma(s)$ given by an expression of this kind, for $f(t) = e^{-t}$. Indeed,

$$\int_0^{+\infty} f(t) t^s \frac{dt}{t} = \int_0^1 f(t) t^s \frac{dt}{t} + \int_1^{+\infty} f(t) t^s \frac{dt}{t}$$

The first integral is over a compact set, so we can bound $f(t)$ on it, and the result is finite. The second integral converges by the condition $\lim_{t \to +\infty} t^n f(t) = 0$.

Now, to show that $L(f,s)$ defines an holomorphic function for $Re(s) > 0$, we can use Morera's theorem. It states that a continuous, complex-valued function on an open set D such that $\oint_\gamma f(z)dz = 0$ for every piecewise closed path γ on D is holomorphic on D.

Then, if we consider the function $s \mapsto \int_0^{+\infty} f(t)t^s \frac{dt}{t}$, we need to show that $\oint_\gamma \int_0^{+\infty} f(t)t^s \frac{dt}{t} = 0$. But by Fubini's theorem we can exchange the order of integration, and using that t^s is holomorphic, the equality holds. In conclusion, $L(f,s)$ defines an analytic function on $Re(s) > 0$.

Now, using integration by parts, we get

$$\int_0^{+\infty} f(t)t^s \frac{dt}{t} = \left[f(t)\frac{t^s}{s} \right]_0^{\infty} - \frac{1}{s}\int_0^{+\infty} f'(t)t^{s+1}\frac{dt}{t}$$

Now, multiplying by $1/\Gamma(s)$, we get

$$L(f,s) = \frac{1}{\Gamma(s)}\int_0^{+\infty} f(t)t^s \frac{dt}{t} = \frac{-1}{s\Gamma(s)}\int_0^{+\infty} f'(t)t^{s+1}\frac{dt}{t} = -L(f', s+1)$$

This equation allows us to extend $L(f,s)$ to $Re(s) > -1$, by setting $L(f,s) = -L(f', s+1)$. Repeating this argument recursively, we can extend $L(f,s)$ by analytic continuation to the whole complex plane, and we have

$$L(f,s) = (-1)^n L(f^{(n)}, s+n)$$

And so, to prove that $L(f,-n) = (-1)^n f^n(0)$ we only need to show that $L(f,0) = f(0)$. But

$$L(f,0) = -L(f',1) = \int_0^{\infty} f'(t)dt = f(0)$$

□

Now let $f(t) = \frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$, which satisfies the conditions of the lemma above. The coefficients B_n are called the *Bernoulli numbers*.

Theorem 3.1. *$\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$, which is holomorphic except for a simple pole at $s = 1$ with residue $L(f,0) = 1$. Moreover, $\zeta(-n) = \frac{-B_{n+1}}{n+1} \in \mathbb{Q}$.*

Proof. We just have to use Lemma 3.1 applied to $f(t)$, and note that $\zeta(s) = \frac{1}{s-1}L(f, s-1)$. □

Definition 3.1. The analytic continuation of $\zeta(s)$ is the *Riemann Zeta function.*

Observation 3.1. The fact that $\zeta(-n) \in \mathbb{Q}$ implies that it makes sense to try to interpolate p-adically the ζ function using its special values. However, note that it won't be possible to interpolate it straight away, and we'll have to introduce some modifications. The most obvious one is due to the fact that

$$\sum_{n=1}^{\infty} n^{-s}$$

is p-adically divergent: For arbitrarily big n, we can find a power of p that is greater than n, so the terms of the sum don't go to zero, and the sum diverges. To address that, we will interpolate ζ with the Euler factor at p removed, that is, $(1 - p^s)\zeta(s)$ instead of ζ.

The result by Kubota and Leopoldt that we want to prove is the following theorem.

Theorem 3.2. *Let p be a prime and $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ (or $i \in \mathbb{Z}/2Z$ if $p = 2$). Then there exists a unique $\zeta_{p,i} : \mathbb{Z}_p \to \mathbb{C}_p$, analytic on $\mathbb{Z}_p$ such that $\zeta_{p,i}(-n) = (1 - p^n)\zeta(-n)$ if $n \equiv -i \mod p - 1$.*

This result might be confusing at the beginning, as it doesn't seem to be what was expected as an interpolation of the Riemann's zeta function. It claims the existence of several several p-adic functions, and each one interpolates the special values of some congruence class modulo $p - 1$. This is necessary, as it is not possible to construct a single p-adic function that interpolates all the special values of $(1 - p^s)\zeta(s)$ at the same time. The reason behind this is explained in Section 3.4.

3.2 L-functions attached to Dirichlet characters

In fact, the construction that we have outlined of the Riemann Zeta Function can be generalized to the case of L-functions attached to a Dirichlet character.

Definition 3.2. A *Dirichlet character* is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$$

Definition 3.3. If $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ is a Dirichlet character, and $n \mid m$, then χ induces a character $\mod m$ via the composition with the projection $(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$, so χ can be thought as defined on any multiple of n. Reciprocally, a character $\mod m$ satisfying $\chi(a+n) = \chi(a)$ for every $a \in (\mathbb{Z}/m\mathbb{Z})^*$ is induced from a character $\mod n$. Therefore, for every character there is a minimal integer f_χ such that χ is defined $\mod f_\chi$. We call it the *conductor* of χ, and we say that ϕ is *primitive* when we think of it as defined $\mod f_\chi$.

We can define the product of characters

$$\chi\phi : (\mathbb{Z}/lcm(f_\chi, f_\psi)\mathbb{Z})^* \to \mathbb{C}^*$$

by $\chi\phi(a) = \chi(a)\phi(a)$.

Observation 3.2. Via the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, we can identify Dirichlet characters with Galois characters. This identification allows to use Dirichlet characters to prove important results in the arithmetic of number fields. See for instance chapter 3 in [22].

Now let's construct the L-function associated to a Dirichlet character. Let χ be a Dirichlet character of conductor f_χ, and define the L-series associated to the character as

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(s)}{n^s}$$

which converges for $\Re(s) > 1$. Notice that if we set χ to be the trivial character, we recover the definition of the Riemann zeta function. We can use the same strategy as we've done for the Riemann's zeta function to prove that it can be analytically continued to the whole $\mathbb{C}$.

Proof. Let

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

Now, we have

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty t^s \left(\sum_{n=1}^{\infty} \chi(n) e^{-nt} \right) \frac{dt}{t}$$

But as χ has conductor f_χ, we have $\chi(a + n f_\chi) = \chi(a)$, and therefore we have

$$\sum_{n=1}^{\infty} \chi(n) e^{-nt} = \sum_{a=1}^{f_\chi} \chi(a) e^{at} \sum_{n=1}^{\infty} e^{-f_\chi nt} = \sum_{a=1}^{f_\chi} \chi(a) e^{at} \frac{1}{e^{f_\chi t} - 1}$$

Then, we have that $L(s, \chi) = \frac{1}{s-1} L(f, s-1)$, and so $L(s, \chi)$ has an analytic continuation to $\mathbb{C}$ by Lemma 3.1. □

Definition 3.4. The *generalized Bernoulli numbers* are the values defined by

$$\sum_{a=1}^{f_\chi} \frac{\chi(a) t e^{at}}{e^{f_\chi t} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}$$

Notice that $L(-n, \chi) = \frac{-B_{n+1,\chi}}{n+1} \in \mathbb{Q}(\chi)$, that is, $\mathbb{Q}$ adjoining the values of χ. But as χ is a Dirichlet character, then its values are algebraic. Therefore we have that $L(-n, \chi) \in \overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}_p}$, so it makes sense to try to interpolate p-adically $L(s, \chi)$ using its special values.

Observation 3.3. $L(s, \chi)$ also has an Euler product, given by

$$L(s, \chi) = \prod_p \frac{1}{1 - \chi(p) p^{-s}}$$

The result that we will prove is the following one:

Theorem 3.3. *Fix a prime p and let $q = p$ if $p \neq 2$ and $q = 4$ if $p = 2$. Let χ be a Dirichlet character of conductor f, and let F be a multiple of q and F. Then, there exists a p-adic meromorphic function $L_p(s, \chi)$ defined on $\{s \in \mathbb{C}_p | |s| < q p^{-1/(p-1)}\}$ such that*

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

Where ω denotes the Teichmüller character. Moreover, L_p is analytic except for $\chi = 1$, when L_p has a simple pole at $s = 1$.

3.3 Measures and the Amice Transform

Definition 3.5. The *Amice transform* is defined as the map

$$A : \mathcal{D}_0(\mathbb{Z}_p, B) \longrightarrow B[[T]] \tag{9}$$

$$\mu \longmapsto A_\mu(T) := \sum_{n=0}^{\infty} T^n \int_{\mathbb{Z}_p} \binom{x}{n} \mu \tag{10}$$

Lemma 3.2. If $v_p(z-1) > 0$, then $A_\mu(z-1) = \int_{\mathbb{Z}_p} z^x \mu(x)$.

Proof. $z^x = \sum_{n=0}^{\infty} (z-1)^n \binom{x}{n}$ converges normally in $\mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, and we can interchange sum and integral. □

Theorem 3.4. *The map $\mu \mapsto A_\mu$ is an isometry (distance preserving isomorphism between metric spaces) from $\mathcal{D}_0(\mathbb{Z}_p, \mathbb{Q}_p)$ to the space*

$$\{\sum_{n=0}^{\infty} b_n T^n,\ b_n \text{ bounded and } b_n \in \mathbb{Q}_n\}$$

where the valuation in this last space is given by $v\left(\sum_{n=0}^{\infty} b_n T^n\right) = \inf_{n\in\mathbb{N}} v_p(b_n)$.

Proof. First of all, if $b = (b_n)_{n\in\mathbb{N}}$ is bounded, the measure μ_b given by $f \mapsto \sum_{n=0}^{\infty} a_n(f) b_n$ is well defined (by Mahler's Theorem, as $a_n(f) \to 0$, $\sum_{n=0}^{\infty} a_n(f) b_n$ converges). Then we have, as $a_n\left(\binom{x}{i}\right) = \delta_{n,i}$

$$A_{\mu_b}(T) = \sum_{n=0}^{\infty} T^n \int_{\mathbb{Z}_p} \binom{x}{n} \mu_b = \sum_{n=0}^{\infty} T^n \left(b_i a_i \left(\binom{x}{n} \right) \right) = \sum_{n=0}^{\infty} b_n T^n$$

This proves that $\mu \mapsto A_\mu$ is surjective.

On the other hand, given a measure μ, we have $A_\mu = \sum_{n=0}^{\infty} T^n b_n$ with $b_n = \int_{\mathbb{Z}_p} \binom{x}{n} \mu$. Now μ_b is defined by

$$f \mapsto \sum_{n=0}^{\infty} a_n(f) \int_{\mathbb{Z}_p} \binom{x}{n} \mu = \int_{\mathbb{Z}_p} \sum_{n=0}^{\infty} a_n(f) \binom{x}{n} \mu = \int_{\mathbb{Z}_p} f\mu$$

And we can exchange sum and integral in the last equality as we know that $\sum a_n(f) \binom{x}{n}$ converges. Therefore, the map $\mu \mapsto A_\mu$ is injective, and its inverse is $b \mapsto \mu_b$.

Now let's see that the map preserves distances. Let $A_\mu = \sum_{n=0}^{\infty} b_n(\mu) T^n$, with $b_n(\mu) = \int_{\mathbb{Z}_p} \binom{x}{n} \mu$. Then, we have, using the definition of the valuation $v_{\mathcal{D}_0}$,

$$v_p(b_n(\mu)) \geq v_{\mathcal{D}_0}(\mu) + v_{\mathcal{C}^0}\binom{x}{n} = v_{\mathcal{D}_0}(\mu)$$

Therefore we have the first inequality $v(A_\mu) \geq v_{\mathcal{D}_0}(\mu)$.

On the other side, we have

$$v_p\left(\sum_{n=0}^{\infty} b_n a_n(f)\right) \geq \inf_{n\in\mathbb{N}} v_p(b_n) + v_p(a_n(f)) \geq$$
$$\geq \inf_{n\in\mathbb{N}}(v_p(b_n)) + \inf_{n\in\mathbb{N}} v_p(a_n(f)) = v(A_\mu) + v_{\mathcal{C}^0}(f)$$

Therefore $v_{\mathcal{D}_0}(\mu_b) = \inf_{f\neq 0} v_p\left(\int_{\mathbb{Z}_p} f\mu_b\right) - v_{\mathcal{C}^0}(f) \geq v(A_\mu)$, if we let $b = (b_n)$ given by $\sum_{n=0}^{\infty} b_n T^n = A_\mu$. Therefore $\mu_b = \mu$ and we have shown the other inequality. In conclusion,

$$v_{A_\mu} = v_{\mathcal{D}_0}(\mu)$$

□

Now we proceed to define some operations that we can do in the space of measures. The most important ones, which play a key role in the theory of p-adic L-functions, are the actions of the operators φ and ψ.

Definition 3.6. $\varphi : \mathcal{D}_0 \to \mathcal{D}_0$ is the operator defined by

$$\begin{aligned} \varphi : \mathcal{D}_0 &\longrightarrow \mathcal{D}_0 \\ \mu &\longmapsto \varphi(\mu) \\ f &\longmapsto \int_{\mathbb{Z}_p} f(px)\mu \end{aligned}$$

$\psi : \mathcal{D}_0 \to \mathcal{D}_0$ is the operator defined by

$$\begin{aligned} \psi : \mathcal{D}_0 &\longrightarrow \mathcal{D}_0 \\ \mu &\longmapsto \varphi(\mu) \\ f &\longmapsto \int_{p\mathbb{Z}_p} f(x/p)\mu \end{aligned}$$

Analogously, we define the operators φ, ψ in the space $\{\sum_{n=0}^{\infty} b_n T^n\}$ as

$$\varphi(F)(T) := F((1+T)^p - 1)$$

and

$$\psi(F)((1+T)^p - 1) := \frac{1}{p}\sum_{z^p=1} F((1+T)z - 1)$$

The following result gives the basic properties of these operators.

Proposition 3.1. i) $A_{\varphi(\mu)} = \varphi(A_\mu)$ and $A_{\psi(\mu)} = \psi(A_\mu)$.
ii) $\psi \circ \varphi = Id$
iii) $\psi(\mu) = 0 \iff \mu$ has support in $\mathbb{Z}_p^*$.
iv) $Res_{\mathbb{Z}_p^*}(\mu) = (1 - \varphi\psi)\mu$

Proof. The only nontrivial statement is the first one. Indeed, $A_{\varphi(\mu)}(T) = \sum_{n=0}^{\infty} T^n \int_{\mathbb{Z}_p} \binom{px}{n} \mu = \int_{\mathbb{Z}_p} \sum_{n=0}^{\infty} T^n \binom{px}{n} \mu = \int_{\mathbb{Z}_p} (1+T)^{px} \mu = A_\mu((1+T)^p - 1)$.

On the other side, $A_{\psi(\mu)}(T) = \sum_{n=0}^{\infty} T^n \int_{p\mathbb{Z}_p} \binom{x/p}{n} \mu = \int_{\mathbb{Z}_p} \frac{1}{p} \sum_{z^p=1} z^x (1+T)^{x/p}$. Therefore, $A_{\psi(\mu)}((1+T)^p - 1) = \int_{\mathbb{Z}_p} \frac{1}{p} \sum_{z^p=1} z^x (1+T)^x = \frac{1}{p} \sum_{z^p=1} A_\mu((1+T)z - 1)$. □

There are some other operations that can be made on measures and it's worth defining them.

i) **Multiplication by a function**: Given $f \in \mathcal{C}^0(\mathbb{Z}_p, \mathbb{Q}_p)$, and $\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Q}_p)$ we can define $f\mu \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Q}_p)$ by

$$\int_{\mathbb{Z}_p} g(x)(f\mu) = \int_{\mathbb{Z}_p} g(x) f(x) \mu$$

For instance, if we let $f(x) = z^x$ such that $v_p(z-1) > 0$, and y such that $v_p(y-1) > 0$. Then, $\int_{\mathbb{Z}_p} y^x (z^x \mu) = \int_{\mathbb{Z}_p} (yz)^x \mu = A_\mu(yz - 1)$.

ii) **Action of** Γ: Let $\Gamma = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p))$. Let $\chi : \Gamma \to \mathbb{Z}_p^*$ be the cyclotomic character. Given $\gamma \in \Gamma$ and $\mu \in \mathcal{D}_0$ we define $\gamma\mu$ by its action on each $f \in \mathcal{C}^0$

$$\int_{\mathbb{Z}_p} f(x)(\gamma\mu) = \int_{\mathbb{Z}_p} f(\chi(\gamma)x)\mu$$

iii) **Convolution**: Given λ, μ two measures, we can define its convolution as

$$\int_{\mathbb{Z}_p} f(x) \lambda * \mu = \int_{\mathbb{Z}_p} \left(\int_{\mathbb{Z}_p} f(x+y)\mu(x) \right) \lambda(y)$$

This gives a product in the space of measures. In fact, it can be seen that the Amice transform gives not only an isomorphism of vector spaces, but also of $\mathbb{Z}_p$ algebras when we take the usual product in $\{\sum_{n=0}^{\infty} b_n T^n\}$ and the convolution in $\mathcal{D}_0$. (See [19], Theorem 2.11).

3.4 The p-adic zeta function

After introducing the basic concepts, this section is dedicated to proof Theorem 3.2.

Lemma 3.3. Let $a \in \mathbb{Z}_p^*$. Then, there exists a measure $\lambda_a \in \mathcal{D}_0$ such that

$$A_{\lambda_a}(T) = \frac{1}{T} - \frac{a}{(1+T)^a - 1}$$

Proof. Note that, as a consequence of Theorem 3.4, it's enough to show that $\frac{1}{T} - \frac{a}{(1+T)^a - 1}$ belongs to $\mathbb{Z}_p[[T]]$, with bounded coefficients. Indeed, using that $(1+T)^a - 1 = \sum_{n=1}^{\infty} \binom{a}{n} T^n$, we have

$$\frac{1}{T} - \frac{a}{(1+T)^a - 1} = \frac{1}{T} - \frac{1}{T \sum_{n=1}^{\infty} a^{-1} \binom{a}{n} T^{n-1}} = \frac{T \sum_{n=1}^{\infty} a^{-1} \binom{a}{n} T^{n-1} - T}{T^2 \sum_{n=1}^{\infty} a^{-1} \binom{a}{n} T^{n-1}} = \frac{\sum_{n=2}^{\infty} a^{-1} \binom{a}{n} T^{n-2}}{\sum_{n=1}^{\infty} a^{-1} \binom{a}{n} T^{n-1}} \tag{11}$$

But, as $\binom{a}{1} = a$, then the expression in the denominator has constant term 1, so it is invertible in $\mathbb{Z}_p[[T]]$ (see [3], Exercise 1.5), and its valuation is 0. Therefore, $\frac{1}{T} - \frac{a}{(1+T)^a - 1} \in \mathbb{Z}_p[[T]]$, and the coefficients are bounded (as the coefficients of the numerator have valuation 0 and in particular are bounded, and the denominator is a unit). This proves the existence of the measure λ_a. □

Proposition 3.2. For every $n \in \mathbb{N}$, we have

$$\int_{\mathbb{Z}_p} x^n \lambda_a = (-1)^n (1 - a^{1+n}) \zeta(-n)$$

Proof. Choose $a \in \mathbb{R}_+^*$, and let $T = e^t - 1$. Then, we define $f_a(t) = A_{\lambda_a}(T) = \frac{1}{e^t - 1} - \frac{a}{e^{at} - 1}$. Then $f_a(t)$ is $\mathcal{C}^\infty$ on $\mathbb{R}_+$ and exponentially decreasing, so, using Lemma 3.1, we have that

$$\begin{aligned} L(f_a, s) &= \frac{1}{\Gamma(s)} \int_0^\infty f_a(t) t^s \frac{dt}{t} = (1 - a^{1-s}) \zeta(s) \\ f_a^n(0) &= (-1)^n L(f_a, -n) = (-1)^n (1 - a^{n+1}) \zeta(-n) \end{aligned} \tag{12}$$

As the last equation is true for all naturals, it is also true if we take $a \in \mathbb{Z}_p^*$, and therefore to conclude the proof of the proposition it's enough to show that we have $\int_{\mathbb{Z}_p} x^n \lambda_a = f_a^n(0)$. Indeed,

$$\int_{\mathbb{Z}_p} x^n \lambda_a = \left(\frac{d}{dt} \right)^n \left(\int_{\mathbb{Z}_p} e^{tx} \lambda_a \right) |_{t=0} = \left(\frac{d}{dt} \right)^n A_{\lambda_a}(e^t - 1)|_{t=0} = f_a^n(0)$$

□

Observation 3.4. The result of this last preposition is a step towards our result: We have related a p-adic expression with the special values of the Riemann zeta function. We would like to extend the map $n \mapsto \int_{\mathbb{Z}_p} x^n \lambda_a$ to a continuous function in $\mathbb{Z}_p$. However, this is not possible in general, as $n \mapsto \int_{\mathbb{Z}_p} x^n \lambda_a$ is not p-adically continuous, unless we restrict to a single class modulo $p - 1$. This is proved in the following theorem.

Theorem 3.5. *(Kummer's Congruences) Let $a \in \mathbb{Z}_p^*$ and $k \geq 1$ ($k \geq 2$ if $p = 2$). Let $n_1, n_2 \geq k$ such that $n_1 \equiv n_2 \mod (p-1)p^{k-1}$. Then,*

$$(1 - a^{1+n_1}) \zeta(-n_1) \equiv (1 - a^{1+n_2}) \zeta(-n_2) \mod p^k$$

Proof. From the last proposition, and the fact that $n_1 \equiv n_2 \mod (p-1)p^k$ (and so in particular they're congruent modulo 2) we have that

$$(1 - a^{1+n_1}) \zeta(-n_1) - (1 - a^{1+n_2}) \zeta(-n_2) = (-1)^{n_1} \int_{\mathbb{Z}_p} (x^{n_1} - x^{n_2}) \lambda_a$$

Moreover, from the definition of the valuation in $\mathcal{D}_0$, we get the following inequality

$$v_p \left(\int_{\mathbb{Z}_p} x^{n_1} - x^{n_2} \right) \geq v_{\mathcal{D}_0(\lambda_a)} + v_{\mathcal{C}^0}(x^{n_1} - x^{n_2})$$

We know from Lemma 3.3 that $v_{\mathcal{D}_0(\lambda_a)} = 0$. Therefore, as $v_p((-1)^n) = 0$, we have $v_p(1 - a^{1+n_1})\zeta(-n_1) - (1 - a^{1+n_2})\zeta(-n_2) \geq v_{\mathcal{C}^0}(x^{n_1} - x^{n_2})$. Therefore it's enough to show that for an arbitrary x, we have $v_p(x^{n_1} - x^{n_2}) \geq k$. Indeed, there are 2 possibilities: If $x \in p\mathbb{Z}_p$, then $v_p(x_1^n), v_p(x^{n_2}) \geq k$, as $n_1, n_2 \geq k$, and so we have $v_p(x^{n_1} - x^{n_2}) \geq k$. On the other side, if $x \in \mathbb{Z}_p^*$, then using that $\mathbb{Z}/p^k\mathbb{Z}$ has order $(p-1)p^k$ and $n_1 - n_2$ is a multiple of $(p-1)p^k$ we have that $x^{n_1} - x^{n_2} = x^{n_2}(x^{n_1-n_2} - 1)$. But modulo p^k, $x^{n_1-n_2} \equiv 1$ so $x^{n_1} - x^{n_2}$ is 0 modulo p^k, i.e $v_p(x^{n_1} - x^{n_2}) \geq k$. □

However, we want to build a function that interpolates $\zeta(-n)$, instead of $(-1)^n(1-a^{1+n})\zeta(-n)$, so we need to remove the dependency on $a \in \mathbb{Z}_p^*$. It turns out that this can't be done preserving continuity, unless we remove the Euler factor of ζ at p, which we can do by restricting the integral to $\mathbb{Z}_p^*$. This is in agreement with the discussion in the introduction of this chapter, where we already pointed out the need to remove the Euler factor at p to be able to interpolate ζ. We'll first study the restriction to $\mathbb{Z}_p^*$ and then justify in Observation 3.5 that this grants p-adic continuity.

Proposition 3.3. $\psi(\lambda_a) = \lambda_a$.

Proof. We only need to show the same on the Amice transform of λ_a. Let $\gamma_a \in \Gamma$ be the inverse of a by the cyclotomic character $\chi : \Gamma \to \mathbb{Z}_p^*$, that is, $\chi(\gamma_a) = a$. Then, we have

$$A_{\lambda_a} = \frac{1}{T} - a(1+T)^a - 1 = \frac{1}{T} - a\gamma_a\left(\frac{1}{T}\right)$$

Moreover, we claim that $\psi(\frac{1}{T}) = \frac{1}{T}$. Indeed, let $F(T) = \psi(\frac{1}{T})$. Then,

$$F((1+T)^p - 1) = \frac{1}{p}\sum_{z^p=1}\frac{1}{(1+T)z - 1} = \frac{-1}{p}\sum_{z^p=1}\sum_{n=0}^{\infty}((1+T)z)^n =$$
$$= -\sum_{n=0}^{\infty}(1+T)^p n = \frac{1}{(1+T)^p - 1}$$

In conclusion, $\psi(\frac{1}{T}) = F(T) = \frac{1}{T}$ as claimed.

Therefore, as Γ and ψ commute,

$$\psi(A_{\lambda_a}) = \psi\left(\frac{1}{T}\right) - \psi\left(a\gamma_a\left(\frac{1}{T}\right)\right) = \frac{1}{T} - a\gamma_a\left(\frac{1}{T}\right) = A_{\lambda_a}$$

□

Corollary 3.1. *i)* $\mathrm{Res}_{\mathbb{Z}_p^*}(\lambda_a) = (1 - \varphi\psi)\lambda_a = (1-\varphi)\lambda_a$
ii) $\int_{\mathbb{Z}_p^*} x^n \lambda_a = \int_{\mathbb{Z}_p} x^n(1-\varphi)\lambda_a = (-1)^n(1-a^{n+1})(1-p^n)\zeta(-n)$

Observation 3.5. ([16], pg 44, Theorem 7) If $p - 1 \nmid n_1$ and n_1, n_2 are such that $n_1 \equiv n_2 \mod (p-1)p^k$, then

$$(1 - p^{n_1})\zeta(-n_1) \equiv (1 - p^{n_2})\zeta(-n_2) \mod p^{k+1}$$

In other words, for natural numbers that are congruent modulo $p-1$, the map

$$n \mapsto (1-p^n)\zeta(-n) = \frac{1}{1-a^{n+1}} \int_{\mathbb{Z}_p^*} x^n \lambda_a$$

is continuous.

Finally, we extend the function $n \mapsto \frac{1}{1-a^{n+1}} \int_{\mathbb{Z}_p^*} x^n \lambda_a$ to the whole $\mathbb{Z}_p$. It turns out that there isn't a unique way to construct this extension. This is a consequence of the following: To extend $\int_{\mathbb{Z}_p^*} x^n \lambda_a$, it seems natural to try to do it by exchanging x^n by x^s, for every $s \in \mathbb{Z}_p$. However, this won't work, as the definition that we have for x^s (see Definition 2.9) only works if $v_p(x-1) > 0$. In a second attempt, we can try to extend x^n as $\exp(s\log(x))$, which is well defined as $\log(x) \in p\mathbb{Z}_p$, but this doesn't exactly give x^s, but $\langle x \rangle^s$ (see Section 2.1, this is explained). This gives an intuition of why are there $p-1$ different ways to extend this function. Moreover, Observation 3.5 also points in this direction, as we have only showed that $n \mapsto \frac{1}{1-a^{n+1}} \int_{\mathbb{Z}_p^*} x^n \lambda_a$ is continuous for $n \in \mathbb{N}$ that are congruent modulo $(p-1)$.

As we see next, the existence of these extensions is a consequence of *Leopoldt's* Γ *Transform.*

Proposition 3.4. If λ is a function on $\mathbb{Z}_p^*$, let

- $\mu = \mu_{p-1}$ be the set of $p-1$ roots of unity in $\mathbb{Z}_p$, and $q = p$, if $p \neq 2$.
- $\mu = \{\pm 1\}$ and $q = 4$ if $p = 2$.

Then, there exists a measure $\Gamma_\lambda^{(i)}$ on $\mathbb{Z}_p$, the *Leopoldt's Transform* of λ, such that

$$\int_{\mathbb{Z}_p^*} \omega(x)^i \langle x \rangle^s \lambda(x) = \int_{\mathbb{Z}_p} u^{sy} \Gamma_\lambda^{(i)}(y) = A_{\Gamma_\lambda^{(i)}}(u^s - 1)$$

Where $u = 1+q$, $\omega(x)$ is the Teichmüller character, and $\langle x \rangle = \frac{x}{\omega(x)}$.

Proof. By additivity of the integral, we have

$$\int_{\mathbb{Z}_p^*} \omega(x)^i \langle x \rangle^s \lambda(x) = \sum_{\epsilon \in \mu} \omega(\epsilon)^i \int_{\epsilon + q\mathbb{Z}_p} \langle x \rangle^s \lambda(x) =$$
$$= \sum_{\epsilon \in \mu} \omega(\epsilon)^i \int_{1+q\mathbb{Z}_p} \langle x\epsilon \rangle^s \gamma_{\epsilon^{-1}} \lambda(x)$$

Where $\gamma_{\epsilon^{-1}} \in \Gamma$ is such that $\chi(\gamma_{\epsilon^{-1}}) = \epsilon$. Now observe that we have an isomorphism $\alpha : 1 + q\mathbb{Z}_p \to \mathbb{Z}_p$ defined by $x \mapsto y = \frac{\log(x)}{\log(u)}$ (c.f Section 2.1), and so for an arbitrary f, we have

$$\int_{\mathbb{Z}_p} f(y) \alpha_*(\gamma_{\epsilon^{-1}} \lambda) = \int_{1+q\mathbb{Z}_p} f(\alpha(x)) \gamma_{\epsilon^{-1}} \lambda$$

Now note that $\langle x \rangle^s = \exp(s\log(x)) = \exp(sy\log(u)) = u^{sy}$. Therefore, setting $f(x) = \langle x\epsilon \rangle^s$, and noting that $\log(\epsilon) = 0$, and therefore $f(x) = \langle x \rangle^s$, we have

$$\sum_{\epsilon \in \mu} \omega(\epsilon)^i \int_{1+q\mathbb{Z}_p} \langle x\epsilon \rangle^s \gamma_{\epsilon^{-1}} \lambda(x) = \sum_{\epsilon \in \mu} \omega(\epsilon)^i \int_{\mathbb{Z}_p} u^{sy} \alpha_*(\gamma_{\epsilon^{-1}} \lambda(x))$$

In conclusion, we can set $\Gamma_\lambda^{(i)} = \sum_{\epsilon\in\mu} \omega(\epsilon)^i \alpha_*(\gamma_{\epsilon^{-1}}\lambda(x))$. □

As a Corollary, we can finally prove the main Theorem for this chapter.

Definition 3.7. (p-adic zeta function) We define the p-adic zeta function as

$$\zeta_{p,i} = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}} \int_{\mathbb{Z}_p^*} \omega(x)^{-i}\langle x\rangle^{-s}\lambda_a(x)$$

Corollary 3.2. *(Theorem 3.2) Let p be a prime and $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ (or $i \in \mathbb{Z}/2Z$ if $p=2$). Then there exists a unique $\zeta_{p,i} : \mathbb{Z}_p \to \mathbb{C}_p$, analytic on $\mathbb{Z}_p$ such that $\zeta_{p,i}(-n) = (1-p^n)\zeta(-n)$ if $n \equiv -i \mod p-1$.*

Proof. Indeed, $\zeta_{p,i} = \frac{A_{\Gamma_\lambda^{(i)}}(u^{-s}-1)}{1-\omega^{1-i}\langle a\rangle^{1-s}}$ by Proposition 3.4. Therefore, $\zeta_{p,i}$ is continuous where the denominator doesn't vanish, because $A_{\Gamma_\lambda^{(i)}}(u^{-s}-1)$ is continuous. This is ensured when $\omega(a)^{1-i} \neq 1$, i.e $i \neq 1$. For $i=1$, there is a simple pole at $s=1$.
Moreover, if $n \equiv i \mod (p-1)$, then

$$\zeta_{p,i}(-n) = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1+n}} \int_{\mathbb{Z}_p^*} \omega(x)^{-i}\langle x\rangle^{n}\lambda_a(x) =$$
$$= \frac{1}{1-\omega(a)^{1+n}\langle a\rangle^{1+n}} \int_{\mathbb{Z}_p^*} \omega(x)^{n}\langle x\rangle^{n}\lambda_a(x) = (1-p^n)\zeta(-n)$$

This proves the existence of $\zeta_{i,p}$. Uniqueness is trivial, as the set $n \in \mathbb{N}$ such that $n \equiv i \mod (p-1)$ is a dense subset of $\mathbb{Z}_p$. Finally, to show analycity, recall that $u = 1+q$ and so $v_p(A_{\Gamma_\lambda^{(i)}}(u^{-s}-1)) \geq n$. In particular, using Theorem 2.4, we get that $\zeta_{p,i}$ is analytic on neighbourhoods small enough. However, it's not true that $\zeta_{p,i}$ admits a power series expansion that converges in the whole $\mathbb{Z}_p$. □

3.5 p-adic L-functions attached to Dirichlet characters

We could generalize the whole last section to the case of the L-function associated to a Dirichlet character. Indeed, one can show that for $\chi \neq 1$, taking μ_{f_χ} a primitive f_χ-th root of unity, and defining

$$f(t) = \frac{1}{\sum_{a=0}^{f_\chi-1}\chi^{-1}(a)\mu_{f_\chi}^{-a}} \sum_{a=0}^{f_\chi-1} \frac{\chi^{-1}(a)}{\mu_{f_\chi}^{-a}e^t - 1}$$

We have $L(s,\chi) = L(f,s)$, and so we can define

$$F_\chi(T) = \frac{-1}{\sum_{a=0}^{f_\chi-1}\chi^{-1}(a)\mu_{f_\chi}^{-a}} \sum_{a=0}^{f_\chi-1} \frac{\chi^{-1}(a)}{\mu_{f_\chi}^{-a}(T+1) - 1}$$

Then, we can repeat the same arguments, find that $\exists \mu_\chi \in \mathcal{D}_0(\mathbb{Z}_p, \mathbb{Q}_p)$ such that

$$A_{\mu_\chi}(T) = F_\chi(T)$$

And so we have that

$$\int_{\mathbb{Z}_p} x^n \mu_\chi = L(-n, \chi)$$

Following the same arguments of the last section, we can then build $L_p(s, \chi)$ such that $L_p(-n, \chi) = (1 - \chi(p)p^n)L(-n, \chi)$. A detailed explanation of this can be found in [12]. Note that, in this situation, if we assume $\chi \neq 1$, we have that $F_\chi(T)$ doesn't depend on any choice (in contrast with $\frac{1}{T} - \frac{a}{(1+T)^a - 1}$, which depended on the choice of $a \in \mathbb{Z}_p^*$). This is because the natural choice of power series for the case of Riemann's zeta function would have been $\frac{1}{T}$, but we had to adapt it as this doesn't belong to $\mathbb{Z}_p[[T]]$.

However, instead of proceeding this way, we will now follow a different approach, explained in [22]. Our goal is to prove Theorem 3.3.

Definition 3.8. The *Bernoulli polynomials* are the polynomials $B_n(X)$ defined by

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=1}^{\infty} B_n(X) \frac{t^n}{n!}$$

From the definition, it's immediate that $B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}$.

Proposition 3.5. Let χ be a character of conductor f, and let F be any multiple of f. Then,

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(a/F)$$

Proof.

$$\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \frac{t^n}{n!} = \frac{1}{F} \sum_{n=0}^{\infty} \sum_{a=1}^{F} \chi(a) B_n\left(\frac{a}{F}\right) \frac{(Ft)^n}{n!} =$$
$$\sum_{a=1}^{F} \chi(a) \frac{1}{F} \frac{Fte^{(a/F)Ft}}{e^{Ft} - 1} = \sum_{a=1}^{F} \chi(a) \frac{te^{(a/F)Ft}}{e^{Ft} - 1}$$

If we let $g = F/f$ and $a = b + cf$, we can rewrite the last expression as

$$\sum_{b=1}^{f} \sum_{c=0}^{g-1} \chi(b) \frac{te^{(b+cf)t}}{e^{fgt} - 1} = \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{ft-1}}$$

Then, comparing the equal powers of t in the first and last expressions, we get

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(a/F)$$

□

Definition 3.9. We define the *Hurwitz zeta function* as the analytic continuation of

$$\zeta(s,b) = \sum_{n=0}^{\infty} \frac{1}{(b+n)^s} \qquad \Re(s) > 1; 0 < b \leq 1$$

Note that we can express the L-function of a character χ in terms of Hurwitz zeta functions:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{a=1}^{f} \chi(a) \sum_{n=0}^{\infty} \frac{1}{a+nf} = \sum_{a=1}^{f} \chi(a) f^{-s} \zeta\left(s, a/f\right)$$

The same argument is used in the following definition.

Definition 3.10. Given F a positive integer, $0 < a < F$ and s a complex variable, we define

$$H(s,a,F) = \sum_{m \equiv a \mod F} m^{-s} = \sum_{n=0}^{\infty} \frac{1}{(a+nF)^s} = F^{-s} \zeta\left(s, \frac{a}{F}\right)$$

H satisfies that

$$H(-n, aF) = -\frac{F^n B_{n+1}(a/F)}{n+1} \in \mathbb{Q}$$

This is a consequence of the special values of the Hurwitz zeta function, $\zeta(-n,b) = -\frac{B_{n+1}(b)}{n+1}$. See for instance [2], Theorem 12.13 for a proof of this fact.

Now our first objective is to construct a p-adic analogue of the function H. To do so, we will need a lemma first.

Lemma 3.4. (von Staudt-Clausen theorem) Let n be an even positive integer. Then,

$$B_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z}$$

Proof. We claim that, for every prime p, either $B_n \equiv \frac{-1}{p} \mod \mathbb{Z}_p$, if $(p-1) \mid n$ or $B_n \equiv 0 \mod \mathbb{Z}_p$, if $(p-1) \nmid n$. We prove the claim by induction. The case $n = 0$ is trivial. Let's assume that the claim holds for $m < n$ and prove it for n. We have, by Proposition 3.5, that

$$B_n = B_{n,1} = p^{n-1} \sum_{a=1}^{p} B_n(a/p)$$

Using the expression of Bernoulli polynomials in terms of the Bernoulli numbers, we have

$$B_n = p^{n-1} \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} B_j (a/p)^{n-j} = \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} (pB_j) a^{n-j} p^{j-2}$$

By induction, we have that $pB_j \in \mathbb{Z}_p$, so the sum modulo $\mathbb{Z}_p$ results as

$$B_n = \sum_{a=1}^{p} pB_0 a^n p^{-2} + npB_1 a^{n-1} p^{-1} + pB_n p^{n-2}$$

Note that $B_0 = 1$ and $B_1 = -1/2$. Then $B_1 \in \mathbb{Z}_p$ if $p \neq 2$, and if $p = 1$, as n is even, $nB_1 \in \mathbb{Z}_2$. Therefore the second term is zero $\mod \mathbb{Z}_p$, and we have that

$$(1 - p^{n-1})B_n \equiv \frac{1}{p}\sum_{a=1}^{p} a^n \equiv \begin{cases} \frac{p-1}{p} & \text{if } (p-1) \mid n \\ 0 & \text{if } (p-1) \nmid n \end{cases}$$

Since $1 - p^{n-1} \equiv 1 \mod p$, the claim follows.

Now $B_n + \sum_{(p-1)|n} \frac{1}{p}$ is in $\mathbb{Z}_p$ for every p, so prime p, so there are no primes in the denominator, and so it must be an integer. □

In particular, this lemma tells us that the denominators of the Bernoulli numbers do not contain repeated powers of any prime. Now we can construct the p-adic analogue of H.

Theorem 3.6. *Let $q \mid F$ and $p \nmid a$. Then, there exists a p-adic meromorphic function $H_p(s, a, F)$ defined on $\{s \in \mathbb{C}_p || s| qp^{-1/(p-1)}\}$ such that*

$$H_p(-n, a, F) = w^{-1-n}(a)H(-n, a, F)$$

In particular, if $n \equiv 0 \mod (p-1)$, or $\mod 2$ if $p = 2$, then $H_p(-n, a, F) = H(-n, a, F)$. Moreover, H is analytic except for a simple pole at $s = 1$ with residue $1/F$.

Proof. Let

$$H_p(s, a, F) = \frac{1}{s-1}\frac{1}{F}\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}B_j\left(\frac{F}{a}\right)^j$$

Note that we only have to prove that the infinite sum converges p-adically, as the rest of the statement is immediate. Indeed, we have

$$H_p(1-n, a, F) = \frac{-1}{nF}\langle a\rangle^{n}\sum_{j=0}^{n}\binom{n}{j}B_j\left(\frac{F}{a}\right)^j$$

Multiplying and dividing by $\left(\frac{a}{F}\right)^n$ and rearranging the terms, we get

$$H_p(1-n, a, F) = -\frac{F^{n-1}\omega^{-n}(a)}{n}B_n\left(\frac{a}{F}\right)$$

Moreover, at $s = 1$ we have residue

$$\frac{1}{F}\langle a\rangle^{0}\sum_{j=0}^{\infty}\binom{0}{j}B_j\left(\frac{F}{a}\right)^j = \frac{1}{F}$$

Now let's prove the converge. By Lemma 3.4, the Bernoulli numbers have at most 1 factor p at the denominator. Moreover, as $q \mid F$ and $p \nmid a$, we have that $|B_n(F/a)^j| \leq \frac{p}{q^n}$. So, taking $r < 1/q$, $\sum_{j=0}^{\infty}\binom{s}{j}B_j(F/a)^j$ is a Mahler series satisfying the conditions of Theorem 2.4, and so it

is locally analytic. Moreover, we can say more about the radius of convergence, and ensure that this Mahler series will be analytic on

$$\{s \in \mathbb{C}_p \text{ such that } |s| < qp^{-1/(p-1)}\}$$

As $qp^{-1/(p-1)} > 1$, this is the same set as

$$\{s \in \mathbb{C}_p \text{ such that } |1-s| < qp^{-1/(p-1)}\}$$

Therefore, the series

$$\sum_{j=0}^{\infty} \binom{1-s}{j} B_j (F/a)^j$$

converges, and so does $H_p(s, a, F)$. □

As a consequence, we can prove the desired result.

Theorem 3.7. *Let χ be a Dirichlet character of conductor f and let F be any multiple of f and q. Then, there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function, $L_p(s, \chi)$ on $\{s \in \mathbb{C}_p$ such that $|s| < qp^{-1/(p-1)}\}$ such that*

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

If $\chi = 1$, then $L_p(s, 1)$ is analytic except for a pole at $s = 1$, with residue $(1 - 1/p)$. In fact, we have the formula

$$L_p(s, \chi) = \frac{1}{F}\frac{1}{s-1}\sum_{a=1, p\nmid a}^{F} \chi(a)\langle a\rangle^{1-s} \sum_{j=0}^{\infty} \binom{1-s}{j} B_j \left(\frac{F}{a}\right)^j$$

Proof. We just have to show that the formula provided for $L_p(s, \chi)$ satisfies the requirements. Note that

$$L_p(s, \chi) = \sum_{a=1, p\nmid a}^{F} \chi(a) H_p(s, a, F)$$

Therefore the convergence and analycity statements are automatically satisfied by Theorem 3.6. At $s = 1$, it has residue

$$\frac{1}{F}\sum_{a=1, p\nmid a}^{F} \chi(a)$$

which is $(1 - 1/p)$ for $\chi = 1$. In the case $\chi \neq 1$, the value of the sum can be rewritten (summing over all a and removing the multiples of p) as

$$\frac{1}{F}\sum_{a=1}^{F} \chi(a) - \frac{1}{F}\sum_{b=1}^{F/p} \chi(pb)$$

Both sums are zero, so $L_p(s,\chi)$ doesn't have a pole at $s=1$ if $\chi \neq 1$. Now it only remains to compute the values of $L_p(s,\chi)$ at negative integers. Indeed,

$$L_p(-n,\chi) = \sum_{a=1,p\nmid a}^{F} \chi(a) H_p(-n,a,F) = -\frac{1}{n}F^{n-1} \sum_{a=1,p\nmid a}^{F} \chi\omega^{-n-1}(a) B_{n+1}\left(\frac{a}{F}\right) =$$
$$-\frac{1}{n}F^{n-1}\sum_{a=1}^{F} \chi\omega^{-n-1}(a)B_{n+1}\left(\frac{a}{F}\right) + \frac{1}{n}F^{n-1}\sum_{b=1}^{F/p} \chi\omega^{-n-1}(pb)B_{n+1}\left(\frac{b}{F/p}\right)$$

But the second sum is zero, as either $p \mid f_{\chi\omega^{-n-1}}$ and then $\chi\omega^{-n-1}(pb) = 0$ for every b, or $f_{\chi\omega^{-n-1}} \mid (F/p)$, and then we can apply Proposition 3.5 on both sums and we have

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

Note that the case $p \mid f_{\chi\omega^{-n-1}}$ is also accounted in this formula, as then $\chi\omega^{-n-1}(p) = 0$. □

Observation 3.6. Note that $L_p(s,\chi)$ doesn't interpolate all the special values of $L(s,\chi)$ (with the Euler factor removed) at once. In particular, we have

$$L_p(-n,\chi) = (1-\chi(p)p^n)L(-n,\chi) \quad \text{if } n \equiv 0 \mod p-1$$

In any other case, $L_p(s,\chi)$ is a combination of $L(s,\chi\omega^j)$, for j in the different classes modulo $p-1$. In particular, if we set $\chi = 1$ we get

$$L_p(s,1) = \zeta_{p,0}(s)$$

It's interesting to compare the two results that we obtained using different approaches: Theorem 3.2 and Theorem 3.3. Both of them are consistent with the fact that we're allowed to interpolate $(1-p^s)\zeta(s)$ only at its special values congruent modulo $p-1$.

Colmez's result gives a more complete construction, as we get a different p-adic function that interpolates the special values for each class modulo $p-1$. The resulting functions are defined on $\mathbb{Z}_p$. On the other side, Washington's approach results only in a function, defined in a disk of $\mathbb{C}_p$, which interpolates the elements in $0 \mod p-1$. In addiction, this construction is not only valid for the Riemann zeta function, but for all L-functions attached to Dirichlet characters.

4 p-adic L-functions of modular forms

We will now construct p-adic L-functions attached to modular forms. We begin by introducing the classical L-functions of modular forms, and we see the analogies with Riemann's zeta function. Then we follow the same strategy as we did in the previous chapter for the Riemann Zeta function: We prove that the special values of the L-functions attached to modular forms are algebraic (i.e. $\in \overline{\mathbb{Q}}$), and so they can be p-adically interpolated. Via this p-adic interpolation, we construct the p-adic L-functions. We assume that the reader has some basic notions of the theory of modular forms, for instance the contents that can be found in [20] or chapter 2 of [10].

4.1 Introduction: L-functions attached to modular forms

Lemma 4.1. (Estimates for the Fourier coefficients) Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a subgroup of finite index. Let $f = \sum_{n \in \frac{1}{M}\mathbb{N}} a_n(f) q^n \in M_k(\Gamma, \mathbb{C})$. Then, we have

$$a_n(f) = \begin{cases} O(n^{k-1}) & \text{if } k \geq 3 \\ O(n \log n) & \text{if } k = 2 \\ O(\sqrt{(}n)) & \text{if } k = 1 \end{cases}$$

Moreover, if $f \in S_k(\Gamma)$, then $a_n(f) = O(n^{k/2})$.

Proof. It is long and tedious, so we don't include it here. It can be found in [10], Proposition 3.1.1. □

Definition 4.1. Given a sequence $\{a_n\}_{n \in \mathbb{N}}$, one defines its *Dirichlet Series* as

$$D(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Note that for $a_n = 1$ for every n, we get the Riemann Zeta function, so Dirichlet Series may be seen as a generalization of the zeta function. In particular, we can define a Dirichlet series using the coefficients of the q-expansion of a modular form.

Definition 4.2. Given $f \in M_k(1)$, we define

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s} \qquad \Lambda(f, s) = \frac{\Gamma(s)}{(2\pi)^s} L(f, s)$$

Example 4.1. If $f = G_k$, we get

$$L(G_k, s) = \sum_{n=1}^{\infty} \frac{\sigma_{k-1}(n)}{n^s} = \sum_{n=1}^{\infty} \left(\sum_{ad=n} d^{k-1} \right) (ad)^{-s} =$$
$$= \left(\sum_{a=1}^{\infty} a^{-s} \right) \left(\sum_{d=1}^{\infty} d^{k-1-s} \right) = \zeta(s)\zeta(s-k+1)$$

Observe that Lemma 4.1 guarantees that $L(f,s)$ converges for $\Re(s)$ big enough (in particular, for $\Re(s) > k$), so there is a semiplane of absolute convergence. This is completely analogous to the situation of Riemann's zeta function. Moreover, we will see that $\Lambda(f,s)$ can also be meromorphically continued to the whole $\mathbb{C}$.

Theorem 4.1. *Let $f \in M_k(1)$, $f = \sum_{n=0}^{\infty} a_n(f)q^n$. Then, we have*

i) $\Lambda(f,s)$ *has a meromorphic continuation to* $\mathbb{C}$.
ii) $\Lambda(f,s)$ *is holomorphic, except for simple poles at* $s = 0$ *and* $s = k$, *of residue* $a_0(f)$ *and* $(-1)^k a_0(f)$.
iii) $\Lambda(f, k-s) = (-1)^k \Lambda(f,s)$
iv) $\Lambda(f,s) \to 0$ *on each vertical strip.*

Proof. Let $\varphi(t) = f(it) - a_0(f)$. Then $\varphi \in \mathcal{C}^\infty(\mathbb{R}_+)$ and $\varphi(t) = O(e^{-2\pi t})$ at ∞. As $f \in M_k(1)$, we have

$$\varphi(t^{-1}) = (-1)^k t^k \varphi(t) + (-1)^k a_0(f) t^k - a_0(k) \tag{13}$$

For $\Re(s) > 0$ we have $\int_0^\infty e^{-2\pi n t} t^s \frac{dt}{t} = \Gamma(s)/(2\pi s)$. So, for $\Re(s) > k$, we have uniform convergence, so we can interchange sum and integral and we get

$$\begin{aligned}\Lambda(f,s) = \sum_{n=1}^{\infty} a_n(f) \frac{\Gamma(s)}{(2\pi n)^s} = \sum_{n=1}^{\infty} a_n(f) \int_0^\infty e^{-2\pi n t} t^s \frac{dt}{t} = \\ = \int_0^\infty \varphi(t) t^s \frac{dt}{t} = \int_1^\infty \varphi(t) t^s \frac{dt}{t} + \int_0^1 \varphi(t) t^s \frac{dt}{t} = \\ = \int_1^\infty \varphi(t) t^s \frac{dt}{t} + \int_1^\infty \varphi(t^{-1}) t^{-s} \frac{dt}{t}\end{aligned}$$

Now using Equation (13), we obtain finally

$$\Lambda(f,s) = \int_1^\infty \varphi(t) \left(t^s + (-1)^k t^{k-s} \right) \frac{dt}{t} - a_0(f) \left(\frac{(-1)^k}{k-s} + \frac{1}{s} \right)$$

Then, as the first term is holomorphic for all $s \in \mathbb{C}$, we have proved (i) and (ii), and (iii) follows immediately by replacing s by $k - s$. As $\varphi(t) = O(e^{-2\pi t})$, the integral is absolutely convergent and uniformly on each vertical strip, so Λ is bounded on each vertical strip. □

Thanks to the results on Hecke operators we can prove the existence of an Euler product for these L-functions.

Theorem 4.2. *If $f \in S_k(1)$ is primitive, then*

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

Proof. $a_{nm}(f) = a_n(f) a_m(f)$ if n, m are coprime. Then,

$$L(f,s) = \prod_p \left(\sum_{r=0}^{\infty} a_{p^r}(f) p^{-rs} \right)$$

Moreover, we have $0 = a_{p^{r+1}}(f) - a_p(f)a_{p^r}(f) + p^{k-1}a_{p^{r-1}}(f)$. Multiplying by $p^{-(r+1)s}$, and summing over r, we get

$$\sum_{r=1}^{\infty} a_{p^{r+1}}(f)p^{-rs-s} - \sum_{r=1}^{\infty} a_p(f)a_{p^r}(f)p^{-rs-s} + \sum_{r=1}^{\infty} p^{k-1-rs-s}a_{p^{r-1}}(f) = 0$$

Rearranging the terms we get

$$\sum_{r=2}^{\infty} a_{p^r}p^{-rs} - a_p p^{-s}\sum_{r=1}^{\infty} a_{p^r}p^{-rs} + p^{k-1-2s}\sum_{r=0}^{\infty} p^{-rs}a_{p^r}$$

Now denote $L_p = \sum_{r=0}^{\infty} a_{p^r}(f)p^{-rs}$. On one side, we have $L(f,s) = \prod_p L_p$. On the other side, $\sum_{r=2}^{\infty} a_{p^r}p^{-rs} = L_p - a_p p^{-s} - 1$, and $\sum_{r=1}^{\infty} a_{p^r}(f)p^{-rs} = L_p - 1$. Therefore, substituting in the expression above, we have

$$L_p - a_p p^{-s} - 1 - a_p p^{-s}(L_p - 1) + p^{k-1-2s}L_p = 0$$

And so

$$L_p = \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}$$

Which proves the result by taking the product over p. □

In fact, this results for $M_k(1)$ can be generalized to modular forms of higher level. Below we state the generalized results, without proof. Set the following notation for congruence subgroups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | c \equiv 0 \mod N \right\}$$

We will also denote $S_k(N) = S_k(\Gamma_0(N))$. For every level N, we can distinguish two types of modular forms: Note that $\Gamma_0(N) \subseteq \Gamma_0(M)$, for $M \mid N$. Therefore we have $S_k(N) \supseteq S_k(M)$.

Definition 4.3. We say that $f \in S_k(N)$ is *old* if $f \in S_k(M)$ for some $M \mid N$. We say that $f \in S_k(N)$ is *new* if $\langle f, g \rangle = 0$ for every old g. We denote by $S_k^{new}(N)$ the set of new forms in $S_k(N)$.

Definition 4.4. For $f \in S_k(N)$, we define the action of the Hecke operator T_n, for $(N,n) = 1$ as

$$f|_k T_n = n^{k-1} \sum_{ad=n, a>1, b \mod d} d^{-k} f\left(\frac{az+b}{d}\right)$$

Definition 4.5. $f \in S_k(1)$ is called *primitive* if $f \in S_k^{new}(N)$, $a_1(f) = 1$ and $f|_k T_n = a_n(f)f$, for $(n,N) = 1$.

Now we can state the analogue of Theorem 4.1 for higher level modular forms.

Theorem 4.3. *Suppose that $f = \sum_{n=1}^{\infty} a_n q^n \in S_k(N)$ is a primitive cusp form. Now we define*

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad \Lambda(f,s) = \Gamma(s) \left(\frac{\sqrt{N}}{2\pi}\right)^s L(f,s)$$

Then we have

i)

$$L(f,s) = \prod_{p|N} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid N} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}$$

ii) $\Lambda(f,s)$ has an analytic continuation to $\mathbb{C}$ and we have

$$\Lambda(f,s) = \pm i^{-k} \Lambda(f, k-s)$$

4.2 Algebraicity of special values of L-functions

In order to be able to interpolate the special values of these L-functions, we need to proof that they satisfy some algebraic relation. However, we will see that the statement here is not as clean as it was for the case of Riemann's zeta function, as the special values are not rational, nor algebraic, but algebraic modulo a product by a complex constant that only depends on f.

Notation. We denote by $A[x]^{(d)}$ the space of polynomials with coefficients in A of degree less or equal than d.

Definition 4.6. Let $0 \leq j \leq k-2$, and $f \in S_k(N)$. Then, a *modular symbol* is an integral of the form $\int_0^{i\infty} f(z)P(z)dz$, for some $P \in A[x]^{(k-2)}$. In particular, we define

$$r_j(f) = \int_0^{i\infty} f(z) z^j dz$$

Observation 4.1. By induction and integration by parts, it's immediate that

$$r_j(f) = \frac{\Gamma(j+1)}{(-2\pi i)^{j+1}} L(f, j+1)$$

So the modular symbols are related with the special values of the L-function.

The purpose of this section is to prove the algebraic relation satisfied by the special values of L-functions (Theorem 4.5). We will prove it for the case of $N = 1$ (that is, modular forms for $SL_2(\mathbb{Z})$). However, some parts of the argument are stated in more general terms, and the result holds in general for $S_k(N)$.

Notation.

- We denote by L_f the $\mathbb{Z}$-module generated by $\{r_j(f|_k\delta)\}_{\delta \in \Gamma_0(N)\backslash SL_2(\mathbb{Z}), 0\leq j\leq k-2}$. As congruence subgroups are of finite index in $SL_2(\mathbb{Z})$, L_f is finitely generated.
- Let $N = 1$. Then we denote L_f^+ (and respectively L_f^-), the $\mathbb{Z}$-module generated by $r_j(f)$, for all odd (respectively even) j.

Definition 4.7. Let $f \in S_k(1)$, and $\phi : \mathbb{Z} \to \overline{\mathbb{Q}}$ constant $\mod M$. Then, we let

$$L(f,\phi,s) = \sum_{n=1}^{\infty} \phi(n)\frac{a_n}{n^s} \qquad \Lambda(f,\phi,s) = \frac{\Gamma(s)}{(2\pi)^s} L(f,\phi,s)$$

Lemma 4.2. Let $P \in A[x]^{(k-2)}$, and $r \in \mathbb{Q}$. Then

$$\int_r^{i\infty} f(z)P(z)dz \in A \cdot L_f$$

Proof. If $r = 0$ it follows immediately from the definition. Therefore we will reduce the general situation to the case $r = 0$. Note that, given $\gamma \in SL_2(\mathbb{Z})$, by change of variable we have

$$\int_{\gamma(0)}^{\gamma(i\infty)} f(z)P(z)dz = \int_0^{i\infty} f(\gamma z)P(\gamma z)d(\gamma z) = \int_0^{i\infty} P|_{2-k}\gamma(z)dz$$

where $P|_{2-k}\gamma(z) = (cz+d)^{k-2}P(\frac{az+b}{cz+d}) \in A[z]^{(k-2)}$. Therefore the last integral belongs to AL_f. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\gamma(0) = b/d$ and $\gamma(i\infty) = a/c$.

Now let $r = a/b$, with $(a,b) = 1$. By [10], Proposition 2.2.1, there exists $\gamma_l = \begin{pmatrix} a_{l-1} & a_l \\ b_{l-1} & b_l \end{pmatrix}$ such that $(a_0, b_0) = (1,0)$ and $(a_n, b_n) = (a,b)$.
Therefore, we have

$$\int_r^{i\infty} f(z)P(z)dz = \sum_{l=1}^{n} \int_{a_l/b_l}^{a_{l-1}/b_{l-1}} f(z)P(z)dz = \sum_{l=1}^{n} \int_0^{i\infty} f|_k\gamma_l(z)P|_{2-k}\gamma_l(z)dz \in A \cdot L_f$$

□

Lemma 4.3. Let $N = 1$, $P \in A[x]^{(k-2)}$, $r \in \mathbb{Q}$ and $\epsilon = \pm 1$. Then, we have

$$\int_r^{i\infty} f(z)P(z)dz - \epsilon \int_{-r}^{i\infty} f(z)P(-z)dz \in A \cdot L_f^{\epsilon}$$

Proof. This is just a matter of writing the expressions. For j odd, we have

$$\int_{-r}^{i\infty} f(z)(-z)^j dz = -\int_{-r}^{i\infty} f(z)z^j dz$$

Now, as in the proof of Lemma 4.2, expressing from $\int_{-r}^{i\infty}$ in terms of $\int_0^{i\infty}$ changes he polynomial involved in the integrals, but all the terms of even degree are the same in $-\int_{-r}^{i\infty} f(z)z^j dz$ and $\int_r^{i\infty} f(z)z^j dz$ so they will cancel out and the difference belongs to $A \cdot L_f^+$. The same reasoning proves the case of L_f^-. □

The first important result is the following proposition:

Proposition 4.1. For $f \in S_k(1)$ and $\phi : \mathbb{Z} \to \overline{\mathbb{Q}}$, constant modulo M, we have:

i) $\Lambda(f, \phi, j) \in \overline{\mathbb{Q}} \cdot L_f$.

ii) If moreover $\phi(-x) = \epsilon(-1)^j \phi(x)$, then $\Lambda(f, \phi, j) \in \overline{\mathbb{Q}} \cdot L_f^\epsilon$, if $1 \leq j \leq k-1$.

Proof. i) It's enough to consider $\phi(n) = e^{2\pi i \frac{nu}{m}}$, for $0 \leq u \leq M-1$, as these functions form a basis of the periodic functions mod M (by Fourier). As $\int_0^\infty e^{-2\pi n y} y^s \frac{dy}{y} = \frac{\Gamma(s)}{(2\pi n)^s}$, we have

$$\Lambda(f, \phi, s) = \int_0^\infty \sum_{n=1}^\infty a_n e^{2\pi i \frac{nu}{M}} e^{-2\pi n y} y^s \frac{dy}{y} = \int_0^\infty f(\frac{u}{M} + iy) y^s \frac{dy}{y}$$

Now, with a change of variable $\frac{u}{M} + iy = z$, $y = iy'$ we get

$$\Lambda(f, \phi, s) \int_{u/M}^{i\infty} f(z) \left(z - \frac{u}{M}\right)^{j-1} dz \in \mathbb{Q} \cdot L_f$$

ii) In this case, we can assume $\phi(n) = e^{2\pi i \frac{un}{M}} + \epsilon(-1)^j e^{-2\pi i \frac{un}{M}}$, and we have

$$\Lambda(f, \phi, j) = \int_{u/M}^{i\infty} f(z) \left(z - \frac{u}{M}\right)^{j-1} dz + \epsilon \int_{-u/M}^{i\infty} f(z) \left(-z + \frac{u}{M}\right)^{j-1} dz$$

and the result follows from Lemma 4.3.

□

Definition 4.8. Let χ be a Dirichlet character mod N. Then, we define

$$G_{j,\chi,s}(z) = \frac{1}{2} \frac{\Gamma(j)}{(-2\pi i)^j} \sum_{\substack{N|m \\ (N,n)=1}}{}' \frac{\chi(n) y^{s+1-k}}{(mz+n)^j |mz+n|^{2(s+1-k)}}$$

Note that, in particular, if we set $\chi = 1$ and $s = k-1$, then $G_{j,\chi,k-1} = G_j$, so we can see this as a generalization of the Eisenstein Series.

Definition 4.9. Let $k = l + j \in \mathbb{N}$ and let $f = \sum_{n=1}^\infty a_n q^n \in S_k(N, \chi_1^{-1})$, $g = \sum_{n=1}^\infty b_n q^n \in M_l(N, \chi_2)$.

Then, we define the *convolution L-series of f, g with respect to the characters* $\chi_1, \chi_2 : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ as

$$D(f, g, s) = L(\chi, j + 2(s+1-k)) \sum_{n=1}^\infty \frac{\overline{a_n} b_n}{n^s}$$

Lemma 4.4.

$$D(f, g, s) = \frac{(4\pi)^s}{\Gamma(s)} \frac{(-2\pi i)^j}{\Gamma(j)} \langle f, g G_{j,\chi_1\chi_2,s} \rangle [SL_2(\mathbb{Z}) : \Gamma_0(N)]$$

Proof. It is basically an analytic calculation, the proof is based in the reasoning from [1]. We start by recalling that $\Gamma(s) = \int_0^\infty u^{s-1}e^{-u}du$. With the appropriate change of variables $u = 4\pi ny$, we get

$$\Gamma(s) = (4\pi n)^s \int_0^\infty y^{s-1}e^{-4\pi ny}dy$$

Now, we multiply on both sides of this equality by $(4\pi)^{-s}\sum_{n=1}^\infty \frac{\overline{a_n}b_n}{n^s}$, and we get

$$\Gamma(s)(4\pi)^{-s}\sum_{n=1}^\infty \frac{\overline{a_n}b_n}{n^s} = \sum_{n=1}^\infty \overline{a_n}b_n \int_0^\infty y^{s-1}e^{-4\pi ny}dy$$

Therefore, we have

$$\sum_{n=1}^\infty \frac{\overline{a_n}b_n}{n^s} = \frac{\Gamma(s)}{(4\pi)^s}\int_0^\infty \sum_{n=1}^\infty \overline{a_n}b_n e^{-4\pi ny}y^{s-1}dy$$

Finally, we use Parseval's theorem, applied to $\overline{f} = \sum_{n=1}^\infty \overline{a_n}e^{-2\pi inx}$ and g and we have that

$$\int_{-1/2}^{1/2} \overline{f(z)}g(z)dx = \sum_{n=1}^\infty \overline{a_n}b_n e^{-4\pi ny}$$

On conclusion, we finally get

$$\sum_{n=1}^\infty \frac{\overline{a_n}b_n}{n^s} = \frac{\Gamma(s)}{(4\pi)^s}\int_0^\infty y^{s-1}dy\int_{-1/2}^{1/2} \overline{f(z)}g(z)dx$$

Now let $\Gamma_\infty = \langle T\rangle$. Note that the vertical strip over which we want to integrate $[-1/2,-1/2]\times[0,\infty)$ is exactly $\Gamma_\infty\backslash\mathcal{H}$. Therefore, we have

$$\sum_{n=1}^\infty \frac{\overline{a_n}b_n}{n^s} = \frac{\Gamma(s)}{(4\pi)^s}\int_{\Gamma_\infty\backslash\mathcal{H}} y^{s+1}\overline{f(z)}g(z)\frac{dxdy}{y^2} =$$

$$= \frac{\Gamma(s)}{(4\pi)^s}\int_{\Gamma_0(N)\backslash\mathcal{H}} \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(N)} \overline{f(\gamma z)}g(\gamma z)\Im(\gamma z)^{s+1}\frac{dxdy}{y^2} =$$

$$= \frac{\Gamma(s)}{(4\pi)^s}\int_{\Gamma_0(N)\backslash\mathcal{H}} \overline{f(z)}\left(g(\gamma z)\sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(N)}\frac{\chi_1\chi_2(d)}{(cz+d)^j}\Im(\gamma z)^{s+1-k}\right)y^k\frac{dxdy}{y^2}$$

Therefore, multiplying by $L(\chi_1\chi_2, j+2(s+1-k))$ on both sides we get the desired result. □

Proposition 4.2. i) $D(f,g,s)$ admits a meromorphic continuation to $\mathbb{C}$, which is holomorphic outside a simple pole at $s=k$ if $l=k$ and $\chi_1\chi_2 = 1$.

ii) If f is a primitive form, and $g \in M_l(N,\chi_2,\overline{\mathbb{Q}})$, then

$$D(f,g,k-1) \in \overline{\mathbb{Q}}\pi^{j+k-1}\langle f,f\rangle$$

Proof. As already said, we will only give the proof for $N = 1$, $\chi_1\chi_2 = 1$. Using the last lemma, (i) holds because the same statement holds for $G_{j,\chi_1\chi_2,s}$. Moreover, we have that

$$D(f, g, k-1) = \frac{(4\pi)^{k-1}}{\Gamma(k-1)} \frac{(-2\pi i)^j}{\Gamma(j)} \langle f, gG_j \rangle [SL_2(\mathbb{Z}) : \Gamma_0(N)]$$

Therefore, it will be enough to prove that

$$\langle f, gG_j \rangle \in \overline{\mathbb{Q}} \langle f, f \rangle$$

But by the fact that f is primitive, we can take f_i a basis of $S_k(1)$ of primitive forms, with $f_1 = f$. As $gG_j \in M_k(1, \overline{\mathbb{Q}})$, we have $gG_j = \lambda_0 G_k + \sum_i \lambda_i f_i$ with $\lambda_i \in \overline{\mathbb{Q}}$. But $\langle G_k, f \rangle = 0$ and $\langle f_i, k \rangle = 0$, for $i \neq 1$. Then, we have $\langle f, gG_j \rangle = \lambda_1 \langle f, f \rangle$. □

Lemma 4.5. Suppose that we have

$$\sum_{n=1}^{\infty} \frac{\overline{a_n}}{n^s} = \left(\sum_{n \in \mathbb{Z}[1/N]^*} \frac{\overline{a_n}}{n^s} \right) \prod_{p \nmid N} \frac{1}{(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})}$$

and

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \left(\sum_{n \in \mathbb{Z}[1/N]^*} \frac{b_n}{n^s} \right) \prod_{p \nmid N} \frac{1}{(1 - \gamma_p p^{-s})(1 - \delta_p p^{-s})}$$

with $\alpha_p \beta_p = \chi_1(p) p^{k-1}$ and $\gamma_p \delta_p = \chi_2(p) p^{l-1}$. Then, we have

$$D(f, g, s) = \left(\sum_{n \in \mathbb{Z}[1/N]^*} \frac{\overline{a_n} b_n}{n^s} \right) \prod_{p \nmid N} \frac{1}{(1 - \alpha_p \gamma_p p^{-s})(1 - \beta_p \gamma_p p^{-s})(1 - \alpha_p \delta_p p^{-s})(1 - \beta_p \delta_p p^{-s})}$$

Proof. First we claim that, under the hypothesis of the statement, we have

$$\overline{a_p^r} = \frac{\alpha_p^{r+1} - \beta_p^{r+1}}{\alpha_p - \beta_p} \qquad b_p^r = \frac{\gamma_p^{r+1} - \delta_p^{r+1}}{\gamma_p - \delta_p}$$

Let's prove the claim. Let's substitute the expression into the L-series factor for p.

$$\sum_{r=0}^{\infty} \overline{a_{p^r}} p^{-rs} = \sum_{r=0}^{\infty} \frac{\alpha_p^{r+1} - \beta_p^{r+1}}{\alpha_p - \beta_p} p^{-rs} = \sum_{r=0}^{\infty} \alpha^r \frac{1 - (\beta_p/\alpha_p)^{r+1}}{1 - \beta_p/\alpha_p} p^{-rs}$$

Now we can separate this into two infinite sums, and we get

$$\frac{1}{1 - \beta_p/\alpha_p} \left(\sum_{r=0}^{\infty} \alpha_p^r p^{-rs} - \frac{\beta_p}{\alpha_p} \sum_{r=0}^{\infty} \beta_p^r p^{-rs} \right)$$

Now using the formal inverse of the geometric series, we get

$$\frac{1}{1-\beta_p/\alpha_p}\left(\frac{1}{1-\alpha_p p^{-s}}-\frac{\beta_p}{\alpha_p}\frac{1}{1-\beta_p p^{-s}}\right)$$

Now we just have to sum these two fractions, and we get

$$\frac{1}{1-\beta_p/\alpha_p}\left(\frac{1-\beta_p p^{-s}-\frac{\beta_p}{\alpha_p}(1-\alpha_p p^{-s})}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}\right)=\frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}$$

So the claim is proved. Now, to complete the proof, we just have to substitute these expressions, and we obtain the result after long and tedious computations. □

Theorem 4.4. *Given f primitive we have, for l odd,*

$$r_{k-2}r_l(f)\in\overline{\mathbb{Q}}\langle f,f\rangle$$

Proof. For $N=1$, let $f\in S_k(1)$. For an even l, let $g=G_l$ and we have

$$\sum_{n=1}^{\infty}\frac{b_n}{n^s}=\prod_p\frac{1}{(1-p^{-s})(1-p^{l-1}p^{-s})}$$

Therefore, in the terms of the previous lemma, we have $\gamma_p=1$, $\delta_p=p^{l-1}$.

$$D(f,G_l,s)=\prod_p\frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})(1-\alpha_p p^{-s+l-1})(1-\beta_p p^{-s+l-1})}$$

And so

$$D(f,G_l,s)=L(f,s)L(f,s-l+1)$$

But, by Proposition 4.2, $D(f,G_l,k-1)\in\overline{\mathbb{Q}}\pi^{j+k-1}\langle f,f\rangle$. Therefore,

$$L(f,k-1)L(f,k-l)\in\overline{\mathbb{Q}}\pi^{j+k-1}\langle f,f\rangle$$

Substituting $r_j(f)=\frac{\Gamma(j+1)}{(-2\pi i)^{j+1}}L(f,j+1)$, and using that $j=k-l$ we get

$$r_{k-2}(f)r_{k-l-1}(f)\in\overline{\mathbb{Q}}\langle f,f\rangle$$

□

Finally, we have the desired result.

Theorem 4.5. *If f is primitive, there exist Ω_f^+ and $\Omega_f^-\in\mathbb{C}$ such that, given $\phi:\mathbb{Z}\to\overline{\mathbb{Q}}$, constant* mod M*, and satisfying $\phi(x)=\epsilon(-1)^j\phi(-x)$, we have,*

$$\Lambda(f,\phi,j)\in\overline{\mathbb{Q}}\cdot\Omega_f^{\epsilon}$$

For $1\le j\le k-1$.

Proof. We prove the case of $\epsilon = 1$. By Proposition 4.1 we have that $\Lambda(f, \phi, j) \in \overline{\mathbb{Q}} \cdot L_f^+$. But by Theorem 4.4 all the $r_l(f)$ for l odd belong to $\overline{\mathbb{Q}}\langle f, f\rangle \frac{1}{r_{k-2}(f)}$. Therefore take $\Omega_f^+ = \frac{\langle f,f\rangle}{r_{k-2}(f)}$ and the result holds. □

We have reached an interesting point of the discussion. We aim to interpolate $L(f, s)$ or $\Lambda(f, s)$ p-adically. For this purpose we need the special values of the L-functions to be rational or algebraic. What we've seen in Theorem 4.5, however, is slightly different from this. It's in some sense weaker, as the special values of the L-function are not algebraic, we only have that the transcendence is "controlled". In another sense, we got an stronger result, as we also got the results for any morphism $\phi : \mathbb{Z}/M\mathbb{Z} \to \overline{\mathbb{Q}}$ and the twist of the L-function by this map: $L(f, \phi, s)$.

Observation 4.2. Suppose that $f \in S_k(N)$ is primitive. Take any $\phi : \mathbb{Z} \to \overline{\mathbb{Q}}$, and define $\phi^+(x) = \frac{1}{2}(\phi(x) + \phi(-x))$ and $\phi^-(x) = \frac{1}{2}(\phi(x) - \phi(-x))$. Then,

$$\tilde{\Lambda}(f, \phi, j) := \frac{\Lambda(f, \phi^+, j)}{\Omega_f^{(-1)^j}} + \frac{\Lambda(f, \phi^-, j)}{\Omega_f^{(-1)^{j+1}}} \in \overline{\mathbb{Q}}$$

for all $1 \leq j \leq k - 1$.

Notation. We also denote $\tilde{\Lambda}(f, j) = \tilde{\Lambda}(f, 1, j) = \tilde{\Lambda}(f, 1_{\mathbb{Z}_p}, j)$.

4.3 p-adic L-functions of modular forms

Definition 4.10. Let

$$L(f, s) = \prod_p \frac{1}{E_p(s)}$$

where $E_p(s) \in \overline{\mathbb{Q}}[p^{-s}]$ is the Euler factor at p, and has degree at most 2 in p^{-s}. (c.f Theorem 4.3) Let $E_p(s) = (1 - \alpha p^{-s})(1 - \beta p^{-s})$. Then, we define

$$f_\alpha(z) = f(z) - \beta f(pz)$$

Let $f \in S_k(N)$. Before going on we recall the relation between the operators T_p and U_p operators:

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} & \text{if } p \mid N \\ \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + p^{k-1} f(pz) & \text{if } p \nmid N \end{cases}$$

$$U_p f = \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$$

Therefore, we have

$$T_p f = \begin{cases} U_p f & \text{if } p \mid N \\ U_p f + p^{k-1} f(pz) & \text{if } p \nmid N \end{cases}$$

Lemma 4.6. For every $f \in S_k(N)$ primitive, it holds

$$f_\alpha|_k U_p = \alpha f_\alpha$$

Proof. In the case $p \mid N$ we have $E_p(s) = (1 - \alpha p^{-s})$, so $\alpha = a_p$, $\beta = 0$ and $f_\alpha = f$. Therefore we have

$$f_\alpha|_k U_p = f|_k T_p = a_p f = \alpha f = \alpha f_\alpha$$

For the case $p \nmid N$, we have $\alpha + \beta = a_p$, $\alpha\beta = p^{k-1}$ and $f|_k T_p = (\alpha + \beta)f$. Then

$$f_\alpha|_k U_p - \alpha f_\alpha = (f - \beta f)|_k U_p = \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) - \beta f(z+i) - \alpha f(z) + \alpha\beta f(z) =$$
$$U_p f - (\alpha + \beta)f + p^{k-1} f = T_p f - a_p f = 0$$

□

In the last section we defined $L(f, \phi, s)$ for ϕ a constant function $\mod M$. This definition can be extended for the case of f_α to the situation where ϕ is locally constant in $\mathbb{Q}_p$ with compact support.

Observation 4.3. Let $\phi \in LC_c(\mathbb{Q}_p, \overline{\mathbb{Q}})$ be a locally constant function in $\mathbb{Q}_p$ with compact support in $p^{-r}\mathbb{Z}_p$. Then there exists $\phi_0 : \mathbb{Z} \to \overline{\mathbb{Q}}$ constant $\mod p^m\mathbb{Z}$ for some m, such that $\phi(x) = \phi_0(p^r x)$.

On the other hand, if $f = \sum_{n>1} b_n q^n$, then we have $U_p f = \sum_{n>1} b_{np} q^n$. Therefore, *Lemma* 4.6 implies that the coefficients of the q-expansion of f_α satisfy $b_{np} = \alpha b_n$.

Definition 4.11. Let $\phi \in LC_c(\mathbb{Q}_p, \overline{\mathbb{Q}})$ be a locally constant function in $\mathbb{Q}_p$ with compact support in $p^{-r}\mathbb{Z}_p$. Then, we define $L(f_\alpha, \phi, s)$ (and analogously $\Lambda(f_\alpha, \phi, s)$) as

$$L(f_\alpha, \phi, s) = \sum_{n \in \mathbb{Z}[1/p]} \phi(n)\frac{a_n}{n^s}$$

Where we have defined $a_n := \alpha^{-r} b_{p^r n}$, for $n \in \mathbb{Z}[1/p]$. We have that $L(f_\alpha, \phi, s) = \alpha^{-r} p^{rs} L(f_\alpha, \phi_0, s)$. In particular, $\tilde{\Lambda}(f_\alpha, \phi, j) \in \overline{\mathbb{Q}}$ for every $\phi \in LC_c(\mathbb{Q}_p, \overline{\mathbb{Q}})$.

Definition 4.12. Let $\phi \in LC_c(\mathbb{Q}_p, \overline{\mathbb{Q}})$, and constant modulo $p^n\mathbb{Z}$. The *discrete Fourier transform* is

$$\widehat{\phi}(x) = p^{-m} \sum_{y \mod p^m} \phi(y) e^{-2\pi i x y}$$

for $m \geq n - v_p(x)$.

Observation 4.4. Given $a \in \mathbb{Q}_p$, let $\phi_a(x) = \phi(ax)$. Let $a = p^k\alpha$, with $\alpha \in \mathbb{Z}_p^*$. Then, we have

$$\widehat{\phi_a(x)} = p^{-m} \sum_{y \mod p^m} \phi(ya) e^{-2\pi i x y}$$

For $m \geq n - v_p(x)$. Therefore, the sum has only p^{m-k} different terms, each one p^k times, and so changing variables $ya = y'$ we get

$$\widehat{\phi_a(x)} = p^{-m}p^k \sum_{\substack{y' \\ \text{mod } p^{m-k}}} \phi(y)e^{-2\pi ixy/a} = p^{v_p(a)}\widehat{\phi(x/a)}$$

Theorem 4.6. *i) There exists a unique $\mu_{f,\alpha} : LP^{[0,k-2]}(\mathbb{Z}_p, \mathbb{Q}_p) \to \overline{\mathbb{Q}_p}$ such that, for every $\phi \in LC(\mathbb{Z}_p, \overline{\mathbb{Q}})$, we have*

$$\int_{\mathbb{Z}_p} \phi(x)x^{j-1}\mu_{f,\alpha} = \tilde{\Lambda}(f_\alpha, \widehat{\phi}, j)$$

for $1 \leq j \leq k-1$.

ii) $\psi(\mu_{f,\alpha}) = \frac{1}{\alpha}\mu_{f,\alpha}$.

iii) If $v_p(\alpha) < k-1$, then $\mu_{f,\alpha}$ extends uniquely as an element of $\mathcal{D}_{v_p(\alpha)}$.

Proof. The first statement is immediate, because we only want $\mu_{f,\alpha} : LP^{[0,k-2]}(\mathbb{Z}_p, \mathbb{Q}_p) \to \overline{\mathbb{Q}_p}$, so it's enough to define how it acts on monomials of degree less than $k-1$ and extend the definition by linearity. Indeed, we just need to define

$$\int_{\mathbb{Z}_p} \phi(x)x^{j-1}\mu_{f,\alpha} := \tilde{\Lambda}(f_\alpha, \widehat{\phi}, j)$$

And note that both $\phi \mapsto \widehat{\phi}$ and $\phi \mapsto \tilde{\Lambda}(f, \phi, j)$ are linear maps.

For the second statement, using the observation above note that

$$\int_{p\mathbb{Z}_p} \phi\left(\frac{x}{p}\right)\left(\frac{x}{p}\right)^{j-1}\mu_{f,\alpha} = \frac{1}{p^{j-1}}\int_{\mathbb{Z}_p} \phi\left(\frac{x}{p}\right)x^{j-1}\mu_{f,\alpha} = \frac{1}{p^{j-1}}\tilde{\Lambda}(f_\alpha, p^{-1}\widehat{\phi(px)}, j) = \frac{1}{p^j}\tilde{\Lambda}(f_\alpha, \widehat{\phi(px)}, j)$$

Now, as we saw on Definition 4.11, we have $\tilde{\Lambda}(f_\alpha, \widehat{\phi(px)}, j) = \frac{1}{\alpha}p^j\tilde{\Lambda}(f_\alpha, \widehat{\phi}, j)$, and so

$$\int_{p\mathbb{Z}_p} \phi\left(\frac{x}{p}\right)\left(\frac{x}{p}\right)^{j-1}\mu_{f,\alpha} = \frac{1}{\alpha}\int_{\mathbb{Z}_p} \phi(x)x^{j-1}\mu_{f,\alpha}$$

Or, in other words,

$$\psi(\mu_{f,\alpha}) = \frac{1}{\alpha}\mu_{f,\alpha}$$

Finally, the last statement is just showing that Theorem 2.5 holds here, that is, there exists a constant C such that

$$v_p\left(\int_{a+p^n\mathbb{Z}_p} (x-a)^j\mu_{f,a}\right) \geq C + (j - v_p(\alpha))n$$

Note that we have

$$\widehat{1_{a+p^n\mathbb{Z}_p}} = \begin{cases} p^{-n}e^{-2\pi iax} & \text{if } x \in p^{-n}\mathbb{Z}_p \\ 0 & \text{otherwise} \end{cases}$$

And so $\hat{(}1_{a+p^n\mathbb{Z}_p}) = p^{-n}\phi_a(p^n x)$, where $\phi_a(x) := e^{2\pi i a x/p^n}$, for $x \in \mathbb{Z}_p$. Therefore we have

$$\int_{a+p^n\mathbb{Z}_p} (x-a)^j \mu_{f,a} = \sum_{l=0}^{j} (-a)^l \binom{j}{l} p^{-n} \tilde{\Lambda}(f_\alpha, \widehat{\phi_a(p^n)}, l+1) = \alpha^{-n} \sum_{l=0}^{j} (-a)^{j-l} \binom{j}{l} p^{nl} \tilde{\Lambda}(f_\alpha, \widehat{\phi_a}, l+1)$$

Now, we have that

$$p^{nl}\tilde{\Lambda}(f_\alpha, \widehat{\phi_a}, l+1) = \int_{-a/p^n}^{i\infty} f_\alpha(z)(p^n z + a)^l dz$$

And so

$$\alpha^{-n} \sum_{l=0}^{j} (-a)^l \binom{j}{l} p^{nl}\tilde{\Lambda}(f_\alpha, \widehat{\phi_a}, l+1) = \int_{-a/p^n}^{i\infty} \sum_{l=0}^{j} \binom{j}{l} (-a)^{j-l} f_\alpha(z)(p^n z + a)^l dz = \int_{-a/p^n}^{i\infty} f_\alpha(z)(p^n z)^j dz \in \alpha^{-n} p^{nj} L_{f_\alpha}$$

Then we just have to pick $C = \min(v_p(\tilde{r}_j(f_\alpha|_k \delta)))$ and the result holds. □

As a consequence of this theorem, we can finally define the p-adic L function.

Definition 4.13. Let $\chi : \mathbb{Z}_p^* \to \mathbb{C}_p^*$ be a continuous character. Then, we define

$$L_{p,\alpha}(f \otimes \chi) = \int_{\mathbb{Z}_p^*} x^{-1}\chi(x)\mu_{f,\alpha}$$

Theorem 4.7. *For $1 \leq j \leq k-1$, we have*

$$L_{p,\alpha}(f \otimes x^j) = \left(1 - \frac{p^{j-1}}{\alpha}\right)\left(1 - \frac{\beta}{p^j}\right)\tilde{\Lambda}(f, j)$$

Proof. We have to compute $\int_{\mathbb{Z}_p^*} x^{j-1}\mu_{f,\alpha} = \tilde{\Lambda}(f_\alpha, \widehat{1_{\mathbb{Z}_p^*}}, j)$. First note that $1_{p\mathbb{Z}_p}(x) = 1_{\mathbb{Z}_p}(x/p)$, and so $\widehat{1_{\mathbb{Z}_p^*}}(x) = \widehat{1_{\mathbb{Z}_p}}(x) - p^{-1}\widehat{1_{\mathbb{Z}_p}}(xp)$. Therefore,

$$\tilde{\Lambda}(f_\alpha, \widehat{1_{\mathbb{Z}_p^*}}, j) = \tilde{\Lambda}(f_\alpha, \widehat{1_{\mathbb{Z}_p}}, j) - \frac{1}{p}\tilde{\Lambda}(f_\alpha, \widehat{1_{\mathbb{Z}_p}}(xp), j) = \tilde{\Lambda}(f_\alpha, \widehat{1_{\mathbb{Z}_p}}, j)\left(1 - \frac{p^j}{\alpha p}\right)$$

Where the last equality is provided by Definition 4.11.

On the other hand, we have $f_\alpha(z) = f(z) - \beta f(pz)$, and $\tilde{\Lambda}(f(pz), \phi, j) = \frac{1}{p^j}\tilde{\Lambda}(f, \phi, j)$. Moreover, $\widehat{1_{\mathbb{Z}_p}} = 1_{\mathbb{Z}_p}$. Putting everything together, we have

$$\int_{\mathbb{Z}_p^*} x^{j-1}\mu_{f,\alpha} = \left(1 - \frac{p^{j-1}}{\alpha}\right)\tilde{\Lambda}(f_\alpha, \widehat{1_{\mathbb{Z}_p}}, j) = \left(1 - \frac{p^{j-1}}{\alpha}\right)\left(1 - \frac{\beta}{p^j}\right)\tilde{\Lambda}(f, \widehat{1_{\mathbb{Z}_p}}, j) = \left(1 - \frac{p^{j-1}}{\alpha}\right)\left(1 - \frac{\beta}{p^j}\right)\tilde{\Lambda}(f, j)$$

□

Observation 4.5. If $p \nmid N$, using that $\alpha\beta = p^{k-1}$, we have

$$1 - \frac{p^{j-1}}{\alpha} = 1 - \frac{\beta}{p^{k-j}}$$

Therefore, the Euler factor of the p-adic L-function at p is

$$\left(1 - \frac{p^{j-1}}{\alpha}\right)\left(1 - \frac{\beta}{p^j}\right) = \left(1 - \frac{\beta}{p^j}\right)\left(1 - \frac{\beta}{p^{k-j}}\right)$$

Recall that the Euler factor of the L-function at p is $(1-\alpha p^{-s})(1-\beta p^{-s})$, so the Euler factor of the p-adic L-function at p is the product of one part of the Euler factor of $L(f,s)$ and one part of the Euler factor of $L(f,k-s)$. This is a general phenomena, which is in consonance with the functional equation $\Lambda(f,s) = \Lambda(f,k-s)$.

Observation 4.6. It's interesting to compare the result we got for the case of modular forms, and for the case of the Riemann's zeta function or Dirichlet characters that we built in Section 3. In the case of modular forms, the result obtained is much weaker: In addition to the discussion on the algebraicity of the special values, we have only obtained a distribution that can interpolate a finite number of special values. We haven't obtained a p-adic function as in the case of the Kubota-Leopoldt zeta function, but only a distribution that interpolates some of the values. This tells us that, in the general case of a Galois representation, we can't expect to get a p-adic L-function interpolating the special values of the L-function, but **the expected p-adic instance of the L-function is played by a p-adic distribution that interpolates p-adically some of the special values**.

5 Fontaine's theory of (φ, Γ)-modules

5.1 Witt vectors

Let $K/\mathbb{Q}_p$ be a finite unramified extension. Then K is a local field with p as an uniformizer, so we can write elements of $\mathcal{O}_K$ as $x = \sum_n x_n p^n$, with some representatives $x_n \in K$ of the elements of $\mathcal{O}_K/p\mathcal{O}_K = \kappa$. Usually, for $K = \mathbb{Q}_p$, we take $x_n = \{0, 1, \dots, p-1\}$, but it may be interesting to choose other representatives.

Lemma 5.1. There is a unique homomorphism $\tau : \kappa^* \to \mathcal{O}_K^*$, satisfying that $\tau(x) \equiv x \mod p$, and it is given by $x \mapsto \lim_{n\to\infty} x^{|K|^n}$.

This lemma is just a generalization of what we saw in Definition 2.3 of $\mathbb{Z}_p$. τ is called the *Teichmüller lift*, and extends to a map $\kappa \to \mathcal{O}_K$ by $\tau(0) = 0$. For every $x \in \mathcal{O}_K$ there is a unique sequence (x_n), $x_n \in \kappa$ such that $x = \sum_{n=0}^{\infty} \tau(x_n) p^n$.

Let's see how does the sum work for this expansion. Let $x = \sum_n \tau(x_n)p^n$ and $y = \sum_n \tau(y_n)p^n$. Then,

$$\sum_n \tau(x_n)p^n + \sum_n \tau(y_n)p^n = \sum_n \tau((x+y)_n)p^n$$

Reducing modulo p we get $\tau((x+y)_0) = \tau(x_0) + \tau(y_0)(mod p)$ so $(x+y)_0 = x_0 + y_0$. Reducing modulo p^2 and after some calculations we get $p\tau((x+y)_1) = \tau(x_0^{1/p})^p + \tau(y_0^{1/p})^p - (\tau(x_0)^{1/p} + \tau(y_0^{1/p}))^p + p(\tau(x_1) + \tau(y_1))$ and so

$$(x+y)_1 = x_1 + y_1 - \sum_{n=1}^{p-1} \frac{1}{p}\binom{p}{n} x_0^{n/p} y_0^{(p-n)/p}$$

This construction is generalized to an arbitrary setting (not just $\mathbb{Q}_p$) by the theory of Witt vectors, which we summarize below.

Definition 5.1. Consider the set of variables $\{X_0, X_1, \dots\}$. We define the *ghost component* of the sequence $(X_0, X_1, \dots,)$ as

$$X^{(n)} = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$$

Definition 5.2. Given a commutative ring R, a *Witt vector* over R (relative to a prime p) is a sequence $(X_0, X_1, \dots)$ with $X_i \in R$. We give a ring structure on this set by $X^{(n)} + Y^{(n)} = (X+Y)^{(n)}$ and $X^{(n)}Y^{(n)} = XY^{(n)}$. We denote this ring as $W(R)$. We denote $W_n(R)$ as the projection of $W(R)$ on the first n coordinates.

Observation 5.1. Note that $W(\mathbb{F}_p) = \mathbb{Z}_p$. In fact, the ring of Witt vectors can be seen as a certain way to construct local fields with a given residue field. The following theorem ([13], Theorem A.42) makes this observation precise.

Theorem 5.1. *For every perfect field κ of characteristic p, $W(\kappa)$ is the unique complete discrete valuation ring of characteristic 0 (up to unique isomorphism) which is absolutely unramified and has κ as its residue field.*

In general, if the field is not perfect, there is a similar construction (namely, Cohen rings).

Definition 5.3. Given a field κ of characteristic p, there is a unique complete discrete valuation ring of characteristic 0 (up to isomorphism) which is absolutely unramified and has κ as its residue field. We call it the *Cohen ring* of κ and denote it $C(\kappa)$.

5.2 p-adic Galois representations

We will introduce étale φ-modules, and later on étale (φ, Γ)-modules, which will be a tool that will help us solve problems about p-adic Galois representations. This section is a summary of the results about (φ, Γ)-modules in [10], complemented with some details from [13].

Definition 5.4. Let G be a topological group, B a topological commutative ring with a continuous action of G that preserves the ring structure. Then, a *B-representation of G* is a B-module of finite type, equipped with a semi-linear continuous action of G. In other words, X is a B-representation of G if, for every $x_i \in X$, $\lambda \in B$ and $g \in G$, we have

$$g(x_1 + x_2) = g(x_1) + g(x_2) \qquad\qquad g(\lambda x) = g(\lambda)g(x)$$

Observation 5.2. This definition is nothing else than an extension of the usual definition of continuous representations, corresponding to the case when G acts trivially on B, and B is a field.

Notation. We denote by $\boldsymbol{Rep}_B(G)$ the category of B-representations of G.

Let E be a field of characteristic p, and E^{sep} be a separable closure of E with the Galois group $G = \mathrm{Gal}(E^{sep}/E)$. Let $\boldsymbol{Rep}_{\mathbb{Q}_p}(G)$ be the category of p-adic representations of G. Let $\mathcal{O}_\mathcal{E} = C(E)$ and $\mathcal{E} = \mathrm{Frac}(\mathcal{O}_\mathcal{E})$.

We can provide $\mathcal{E}$ with a Frobenius φ, a continuous endomorphism such that $\varphi(\mathcal{O}_\mathcal{E}) = \mathcal{O}_\mathcal{E}$ and that induces the absolute Frobenius $x \mapsto x^p$ in E.

Definition 5.5. A *φ-module* M over $\mathcal{O}_\mathcal{E}$ is a pair (M, φ), where M is a $\mathcal{O}_\mathcal{E}$-module and $\varphi : M \to M$ is semilinear, i.e. if $x_i \in M$, $\lambda \in \mathcal{O}_\mathcal{E}$, then

$$\varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2) \qquad\qquad \varphi(\lambda x) = \varphi(\lambda)\varphi(x)$$

Similarly, a *φ-module* D over $\mathcal{E}$ is a pair (M, φ), where M is a $\mathcal{E}$-vector space and $\varphi : M \to M$ is semilinear.

Let $(\mathcal{O}_\mathcal{E})_\varphi$ denote $\mathcal{O}_\mathcal{E}$, viewed as an $\mathcal{O}_\mathcal{E}$-module via the Frobenius φ. Let $M_\varphi = (\mathcal{O}_\mathcal{E})_\varphi \otimes_{\mathcal{O}_\mathcal{E}} M$. Then, giving a semi-linear map $\varphi : M \to M$ is equivalent to give a linear map $\Phi : M_\varphi \to M$.

Indeed, given $\phi : M \to M$ semilinear, $\Phi(\lambda \otimes x) = \lambda\varphi(x)$ defines a linear map $M_\varphi \to M$ and, reciprocally, given a linear map $\Phi : M_\varphi \to M$, $\varphi(x) = \Phi(1 \otimes x)$ defines the corresponding semilinear map $M \to M$. The same construction holds for φ-modules over $\mathcal{E}$.

Definition 5.6. We say that a φ-module M is étale if the corresponding map $\Phi : M_\varphi \to M$ is an isomorphism.

Notation. $\mathcal{M}_\varphi^{ét}(\mathcal{O}_\mathcal{E})$ denotes the category of étale φ-modules over $\mathcal{O}_\mathcal{E}$. Respectively, $\mathcal{M}_\varphi^{ét}(\mathcal{E})$ denotes the category of étale φ-modules over $\mathcal{E}$.

Let's construct an equivalence of categories from the category of $\mathbb{Z}_p$ (or $\mathbb{Q}_p$)- representations of G to the category of étale φ modules over $\mathbb{Z}_p$ (or $\mathbb{Q}_p$). The following key lemma is a consequence of the functoriality of Cohen rings, see [13], A.45.

Lemma 5.2. Let F be a finite separable extension of E.

i) There is a unique unramified extension $\mathcal{E}_F$ of $\mathcal{E}$ whose residue field is F.
ii) There is a unique endomorphism $\varphi' : \mathcal{E}_F \to \mathcal{E}_F$ such that $\varphi'|_\mathcal{E} = \varphi$ and φ' induces the Frobenius on F.
iii) If F/E is Galois, then $\mathcal{E}_F/\mathcal{E}$ is also Galois, and

$$\mathrm{Gal}(\mathcal{E}_F/\mathcal{E}) = \mathrm{Gal}(F/E)$$

Definition 5.7. $\mathcal{E}^{ur} := \bigcup_{F/E \text{ finite unramified}} \mathcal{E}_F$. Let $\widehat{\mathcal{E}^{ur}}$ be its completion. Then $\mathcal{O}_{\widehat{\mathcal{E}^{ur}}} = \varprojlim_n \mathcal{O}_{\widehat{\mathcal{E}^{ur}}}/p^n\mathcal{O}_{\widehat{\mathcal{E}^{ur}}}$. φ extends by continuity to an action on $\mathcal{O}_{\widehat{\mathcal{E}^{ur}}}$ and $\widehat{\mathcal{E}^{ur}}$, which commutes with the action of G.

Theorem 5.2. *i) The functor*

$$\begin{aligned} D : \boldsymbol{Rep}_{\mathbb{Z}_p}(G) &\longrightarrow \mathcal{M}_\varphi^{ét}(\mathcal{O}_\mathcal{E}) \\ T &\longmapsto (\mathcal{O}_{\widehat{\mathcal{E}^{ur}}} \otimes_{\mathbb{Z}_p} T)^G \end{aligned}$$

is an equivalence of Tannakian categories, with inverse functor given by

$$\begin{aligned} V : \mathcal{M}_\varphi^{ét}(\mathcal{O}_\mathcal{E}) &\longrightarrow \boldsymbol{Rep}_{\mathbb{Z}_p}(G) \\ D &\longmapsto (\mathcal{O}_{\widehat{\mathcal{E}^{ur}}} \otimes_{\mathcal{O}_\mathcal{E}} D)_{\varphi=1} \end{aligned}$$

ii) The functor

$$\begin{aligned} D : \boldsymbol{Rep}_{\mathbb{Q}_p}(G) &\longrightarrow \mathcal{M}_\varphi^{ét}(\mathcal{E}) \\ T &\longmapsto (\widehat{\mathcal{E}^{ur}} \otimes_{\mathbb{Q}_p} T)^G \end{aligned}$$

is an equivalence of Tannakian categories, with inverse functor given by

$$\begin{aligned} V : \mathcal{M}_\varphi^{ét}(\mathcal{E}) &\longrightarrow \boldsymbol{Rep}_{\mathbb{Q}_p}(G) \\ D &\longmapsto (\widehat{\mathcal{E}^{ur}} \otimes_{\mathcal{E}} D)_{\varphi=1} \end{aligned}$$

5.3 Fontaine's rings

Definition 5.8. Let A be a ring of characteristic p, and φ the absolute Frobenius. We define $R(A) := \varprojlim_n A_n$, with $A_n = A$ and transition maps φ.

$$R(A) = \{x = (x_n)_{n\in\mathbb{N}} \text{ such that } x_{n+1}^p = x_n\}$$

Proposition 5.1. If A is a separated and complete ring for the p-adic topology, there is a bijection between $R(A/pA)$ and the set $S = \{(x^{(n)})_{n\in\mathbb{N}}$ such that $x^{(n)} \in A$, $(x^{(n+1)})^p = x^{(n)}\}$.

Proof. Given an element $x = (x_n) \in R(A/pA)$, choose for each x_n a lifting $\widehat{x_n} \in A$. We have $\widehat{x_{n+1}}^p = \widehat{x_n} \mod pA$, and so $\widehat{x_{n+m+1}}^{p^{m+1}} = \widehat{x_{n+m}}^{p^m} \mod p^{m+1}A$. Therefore the limit $x^{(n)} := \lim_{m\to\infty} \widehat{x_{n+m}}^{p^m}$ exists in A, and is independent of the choice of the liftings.
This defines a map $R(A/pA) \to S$, whose inverse is the reduction modulo p. □

Observation 5.3. As a consequence of this result, there are 2 ways of writing elements of $R(A/pA)$. One is as a sequence $\{(x_n)\}$, $x_n \in A/pA$. The other one is as a sequence $\{x^{(n)}\}$, $x^{(n)} \in A$.

Definition 5.9. $\tilde{E}^+ := R(\mathcal{O}_{\mathbb{C}_p}/p\mathcal{O}_{\mathbb{C}_p})$, is a ring of characteristic p with valuation given by $v_E(x) = v_p(x^{(0)})$.

Observation 5.4. Let's fix an element $\epsilon = (1, \epsilon^{(1)}, \dots) \in \tilde{E}^+$, such that $\epsilon^{(1)} \neq 1$. Then, each $\epsilon^{(n)}$ is a primitive p^n-th root of unity. Let $\overline{\pi} = \epsilon - 1 \in \tilde{E}^+$. We have $\overline{\pi}^{(0)} = \lim_{k\to\infty}(\epsilon^{(k)} - 1)^{p^k}$. As $\epsilon^{(k)}$ is a primitive p^k-th root of unity, then for every k we have $v_p(\epsilon^{(k)} - 1)^{p^k} = p^k \frac{1}{(p-1)p^{k-1}} = \frac{p}{p-1}$, and so $v_E(\overline{\pi}) = \frac{p}{p-1}$.

Definition 5.10. We define an action of $G_{\mathbb{Q}_p}$ on ϵ by

$$g(\epsilon) = \epsilon^{\chi(g)}$$

Where $\chi : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^*$ is the cyclotomic character.

Notation. Now let $K/\mathbb{Q}_p$ be a finite extension, and let k be its residue field. We denote

- $K_n := K(\epsilon^{(n)})$
- $K_\infty = \bigcup_n K_n$
- F' the maximal unramified extension of $\mathbb{Q}_p$ inside K_∞
- $G_K = \mathrm{Gal}(\overline{\mathbb{Q}_p}/K)$, $H_K = \mathrm{Gal}(\overline{\mathbb{Q}_p}/K_\infty)$ and $\Gamma_K = G_K/H_K = \mathrm{Gal}(K_\infty/K)$.
- $E_K^+ := \{x = (x_n) \in \tilde{E}^+, x_n \in \mathcal{O}_{K_n}/p\mathcal{O}_{K_n}, \forall n \geq n(K)\}$
- $E_K := E_K^+[\overline{\pi}^{-1}]$.

Theorem 5.3.
- *E_K is a local field of characteristic p, and ring of integers E_K^+. If $K/\mathbb{Q}_p$ is unramified, then $E_K = k((\overline{\pi}))$.*
- *$E = E^s = \bigcup_{[K:\mathbb{Q}_p]<\infty} E_K$ is a separable closure of $E_{\mathbb{Q}_p}$, and $\mathrm{Gal}(E^s/E_K) = H_K$.*
- *$\tilde{E} = \tilde{E}^+[\overline{\pi}^{-1}]$ is the completion of the radical closure of E.*

This theorem is proved in a course by Fontaine, and we will use this result several times. Let's introduce some other rings that will be useful.

Definition 5.11. We denote

- $A_{\mathbb{Q}_p} = \mathcal{O}_{\mathcal{E}} = C(E_{\mathbb{Q}_p})$ and $B_{\mathbb{Q}_p} = \mathcal{E}$. Similarly, $A_K = \mathcal{O}_{\mathcal{E}_K} = C(E_K)$, and $B_K = \mathcal{E}_K$.
- $B = \widehat{\mathcal{E}^{ur}}$ and $A = \mathcal{O}_{\widehat{\mathcal{E}^{ur}}}$. Therefore $B^{H_K} = B_K$ and $A^{H_K} = A_K$.
- $\tilde{A}^+ = W(\tilde{E}^+)$, $\tilde{A} = W(\tilde{E})$ and $\tilde{B} = \tilde{A}[1/p]$.

Definition 5.12. We denote by $[\epsilon] \in \tilde{A}^+$ the Teichmüller lift of ϵ, and $\pi := [\epsilon] - 1$. We also define the actions of φ and $G_{\mathbb{Q}_p}$ as

$$\varphi([\epsilon]) = [\epsilon]^p \qquad g([\epsilon]) = [\epsilon]^{\chi(g)}$$

Where $\chi : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^*$ is the cyclotomic character.

All this new definitions (and some more that we still have to introduce) seem very difficult to handle with at the beginning. However, while it's true that working with these rings is sometimes intangible, one should focus in the properties that these rings inherit from the constructions of Cohen or Witt rings. Moreover, the following result shows that some of these rings turn out to have nice expressions after all.

Proposition 5.2. $A_{\mathbb{Q}_p} = \mathbb{Z}_p\widehat{[[\pi]][\pi^{-1}]}$, so we have

$$A_{\mathbb{Q}_p} = \left\{ \sum_{k\in\mathbb{Z}}^{\infty} a_k \pi^k | a_k \in \mathbb{Z}_p, \lim_{k\to-\infty} v_p(a_k) = +\infty \right\}$$

Similarly,

$$A_K = \left\{ \sum_{k\in\mathbb{Z}}^{\infty} a_k \pi^k | a_k \in \mathcal{O}_{F'}, \lim_{k\to-\infty} v_p(a_k) = +\infty \right\}$$

Observation 5.5. The above characterization of $A_{\mathbb{Q}_p}$ and A_K shows that these rings have 2 topologies (and therefore they also induce 2 different topologies in A and B).

- **Strong topology:** The p-adic topology given by the valuation $v_p(\sum_{k=-N}^{\infty} a_k\pi^k) = \inf_k\{v_p(a_k)\}$. It is the same as the topology of the inverse limit $A = \varprojlim A_{\mathbb{Q}_p}/p^n A_{\mathbb{Q}_p}$ when we give the discrete topology on each $A_{\mathbb{Q}_p}/p^n A_{\mathbb{Q}_p}$. A basis of neighbourhoods of 0 is $\{p^k A_{\mathbb{Q}_p}\}_k$. (respectively, the same for A_K and A).
- **Weak topology:** The (p,π)-adic topology, given by the valuation $v_E(\sum_{k=-N}^{\infty} a_k\pi^k) = \inf_k\{v_p(a_k)+kv_p(\pi)\}$. It is the same as the topology of the inverse limit $A = \varprojlim A_{\mathbb{Q}_p}/p^n A_{\mathbb{Q}_p}$ when we give each $A_{\mathbb{Q}_p}/p^n A_{\mathbb{Q}_p}$ the topology induced by the valuation v_E. A basis of neighbourhoods of 0 is $\{p^k A_{\mathbb{Q}_p} + \pi^n A_{\mathbb{Q}_p}\}_{k,n}$. (respectively, the same for A_K and A).

We will also introduce the rings B_{dR}, B_{dR}^+ which play an important role in p-adic Hodge theory. Take $a \in \tilde{A}^+ = W(\tilde{E}^+)$. Then we can write $a = (a_0, a_1, \dots)$, with each $a_i \in \tilde{E^+}$, so at its turn, each a_i can be written as $a_i = (a_{i,r})_r$, with $a_{i,r} \in \mathcal{O}_{\mathbb{C}_p}/p$, $a_{i,r+1}^p = a_{i,r}$. Therefore, we have a

natural map $\tilde{A}^+ \to W_n(\mathcal{O}_{\mathbb{C}_p}/p)$ given by $a \mapsto (a_{0,n}, a_{1,n}, \dots, a_{n-1,n})$. For every n, we have a commutative diagram

$$\begin{array}{ccc} \tilde{A}^+ & \longrightarrow & W_{n+1}(\mathcal{O}_{\mathbb{C}_p}/p) \\ & \searrow & \downarrow f_n \\ & & W_n(\mathcal{O}_{\mathbb{C}_p}/p) \end{array}$$

where we have defined $f_n(x_0, \dots, x_n) = (x_0^p, \dots, x_{n-1}^p)$. It's not difficult to see that we indeed have

$$\tilde{A}^+ = \varprojlim_{f_n} W_n(\mathcal{O}_{\mathbb{C}_p}/p) \tag{14}$$

On the other hand, we have a map

$$\begin{aligned} \psi_n : W_{n+1}(\mathcal{O}_{\mathbb{C}_p}) &\to W_n(\mathcal{O}_{\mathbb{C}_p}/p) \\ (a_0, \dots, a_n) &\mapsto (\overline{a_0}, \dots, \overline{a_{n-1}}) \end{aligned}$$

which has kernel $I = (pa_0, pa_1, \dots, pa_{n-1}, a_n)$. We can define a map

$$\begin{aligned} w_{n+1} : W_{n+1}(\mathcal{O}_{\mathbb{C}_p}) &\to \mathcal{O}_{\mathbb{C}_p} \\ (a_0, \dots, a_n) &\mapsto \sum_{i=0}^{n} a_i^{p^{n-i}} p^{n-i} \end{aligned}$$

If we let $\overline{w_{n+1}}$ be the composition of w_{n+1} and quotient $\mod p^n$, we get that $I \subseteq \ker \overline{w_{n+1}}$, and so $\overline{w_{n+1}}$ factors through $W_n(\mathcal{O}_{\mathbb{C}_p}/p)$. We denote by θ_n this morphism

$$\theta_n : W_n(\mathcal{O}_{\mathbb{C}_p}/p) \to \mathcal{O}_{\mathbb{C}_p}/p^n$$

Moreover, we have a commutative diagram

$$\begin{array}{ccc} W_{n+1}(\mathcal{O}_{\mathbb{C}_p}) & \xrightarrow{\theta_{n+1}} & \mathcal{O}_{\mathbb{C}_p}/p^{n+1} \\ \downarrow f_n & & \downarrow \\ W_n(\mathcal{O}_{\mathbb{C}_p}/p) & \xrightarrow{\theta_n} & \mathcal{O}_{\mathbb{C}_p}/p^n \end{array}$$

and so we can induce a morphism

$$\theta : \tilde{A}^+ \cong \varprojlim_{f_n} W_n(\mathcal{O}_{\mathbb{C}_p}/p)$$

Proposition 5.3. Let $x \in \tilde{A}^+$. Then,

i) If $x = (x_0, x_1, \dots)$, with $x_i = (x_i^{(m)})_m \in \tilde{E}^+$, we have

$$\theta(x) = \sum_m p^m x_m^{(m)}$$

ii) If $x = \sum_n p^n[x_n]$, then

$$\theta(x) = \sum_m p^m x_m^{(0)}$$

Proof. i) The image of x in $W_n(\mathcal{O}_{\mathbb{C}_p}/p)$ is $(x_{0,n}, x_{1,n}, \dots, x_{n-1,n})$. Take $x_i^{(n)}$ the lifting of $x_{i,n}$ and we have

$$\theta_n(x_{0,n}, x_{1,n}, \dots, x_{n-1,n}) = \sum_{i=0}^{n-1} p^i (x_i^{(n)})^{p^{n-i}} = \sum_{i=0}^{n-1} p^i x_i^{(i)}$$

where we have used $(x_i^{(n)})^{p^r} = x_i^{(n-r)}$. Then we just have to take limits and we get the desired result.

ii) We just have to relate the expression of x as Teichmüller lift and the expression as a Witt vector, noting that $p^n[x] = (0, \dots, 0, x, 0, \dots)$ and that the ghost components of $p^n[x_n]^{(i)} = p^n x_n^{p^{i-n}}$.

□

Moreover, we can extend θ to $\tilde{A}^+[1/p]$. Now let $\omega \in \tilde{E}^+$ such that $\omega^{(0)} = -p$. Then, $\xi = [\omega] + p \in \tilde{A}^+$, $\xi = (\omega, 1, 0, \dots)$, and we have $\theta(\xi) = 0$.

Proposition 5.4. (c.f. [13], Prop. 5.12) $\ker\theta$ is the principal ideal generated by ξ, and moreover, $\cap_n (\ker\theta)^n = 0$.

Definition 5.13. B_{dR}^+ is the completion of $\tilde{A}^+[1/p]$ with respect to $\ker\theta$.

$$B_{dR}^+ := \varprojlim_n \tilde{A}^+[1/p]/(\ker\theta)^n$$

B_{dR} is the fraction field of B_{dR}^+.

$$B_{dR} := Frac(B_{dR}^+) = B_{dR}^+\left[\frac{1}{\xi}\right]$$

Observation 5.6. As $\epsilon^{(0)} = 1$, using Proposition 5.3 we have $\theta(\pi) = \theta([\epsilon] - 1) = \epsilon^{(0)} - 1 = 0$.

Observation 5.7. We have just defined the rings B_{dR}^+, B_{dR} because they play a role in the proof on a result that we need (Lemma 6.4). However, in this study we won't go further enough to realise the key role that these rings play. It turns out that B_{dR} and the whole p-adic Hodge theory provide a very useful tool to study Galois representations. In particular, there is an important type of representations, namely *de Rham representations*, which are defined using B_{dR} (c.f. [6] for a more detailed introduction to p-adic Hodge theory).

Definition 5.14. Let V be a $\mathbb{Q}_p$ representation of G_K. Then, we say that it is *de Rham* if

$$\dim_K (B_{dR} \otimes_{\mathbb{Q}_p} V)^{G_K} = \dim_{\mathbb{Q}_p} V$$

5.4 (φ, Γ)-modules

We finally introduce (φ, Γ)-modules and see their connection with Galois representations.

Definition 5.15. An étale (φ, Γ_K)-*module* over A_K (or B_K) is an étale A_K (or B_K) φ-module with a continuous action of Γ_K commuting with φ.

Then, Theorem 5.2, is in this situation:

Theorem 5.4. *The correspondence*

$$V \mapsto D(V) := (A \otimes_{\mathbb{Z}_p} V)^{H_K}$$

(respectively B and $\mathbb{Q}_p$) is an equivalence of Tannakian categories from $\boldsymbol{Rep}_{\mathbb{Z}_p}(G_K)$ (respectively $\boldsymbol{Rep}_{\mathbb{Q}_p}(G_K)$) to the category $\mathcal{M}^{ét}_{(\varphi,\Gamma_K)}(A_K)$ (respectively $\mathcal{M}^{ét}_{(\varphi,\Gamma_K)}(B_K)$), and the inverse functor is

$$D \mapsto V(D) = (A \otimes_{A_K} D)^{\varphi=1}$$

The rest of the chapter will be dedicated to study (φ, Γ)-modules. Assume from now on that Γ_K is procyclic, so it has a topological generator γ. We start by defining an operator ψ, which is analogue as the ones defined for measures and distributions. Let $[\epsilon] \in A$ denote the Teichmüller representative of $\epsilon \in E_{\mathbb{Q}_p}$, and $\pi = [\epsilon] - 1$. Then, we have the following lemma.

Lemma 5.3. i) $\{1, \epsilon, \dots, \epsilon^{p-1}\}$ is a basis of $E_{\mathbb{Q}_p}$ over $\varphi(E_{\mathbb{Q}_p})$.
ii) $\{1, \epsilon, \dots, \epsilon^{p-1}\}$ is a basis of E_K over $\varphi(E_K)$, for every finite extension $K/\mathbb{Q}_p$.
iii) $\{1, [\epsilon], \dots, [\epsilon^{p-1}]\}$ is a basis of A over $\varphi(A)$.

Proof. i) $E_{\mathbb{Q}_p} = \mathbb{F}_p((\pi))$, and therefore $\varphi(E_{\mathbb{Q}_p}) = \mathbb{F}_p((\pi^p))$. As we're in characteristic p, $\pi^p = \epsilon^p - 1$ and the result is immediate.
ii) The polynomial $X^p - \pi^p \in \mathbb{F}_p((\pi^p))[X]$ is purely inseparable. In the other side, $E_K/E_{\mathbb{Q}_p}$ is a separable extension, and therefore so is $\varphi(E_K)/\varphi(E_{\mathbb{Q}_p})$. Therefore, we must have $E_K/\varphi(E_K)$ purely inseparable (by multiplicativity of separable and inseparable degrees) and the result follows.
iii) True using that $E^s = \bigcup_{[K:\mathbb{Q}_p]<\infty} E_K$.
iv) As A is p-adically complete, then we have $\varprojlim A/p^n A = A$ and so every element has a unique expression in the form $\sum_n p^n [x_n]$ with $[x_n]$ a representative of $x_n \in A/p$. Then, as $1, \epsilon \dots, \epsilon^{p-1}$ is a basis of E over $\varphi(E)$, $\{1, [\epsilon], \dots, [\epsilon^{p-1}]\}$ is a basis of A over $\varphi(A)$.

□

Definition 5.16. We define the operator $\psi : A \to A$ by

$$\psi\left(\sum_{i=0}^{p} [\epsilon]^i \varphi(x_i)\right) = x_0$$

Proposition 5.5. (Properties of ψ)
i) $\psi \circ \varphi = \mathrm{Id}$
ii) ψ commutes with $G_{\mathbb{Q}_p}$.

Proof. i) Is clear.

ii) By definition of the action of $G_{\mathbb{Q}_p}$ on $[\epsilon]$ (Definition 5.12), we have

$$g\left(\sum_{i=0}^{p-1}[\epsilon]^i\varphi(x_i)\right)=\sum_{i=0}^{p-1}[\epsilon]^{i\chi(g)}\varphi(g(x_i))$$

If we write $i\chi(g)=i_g+pj_g$, for $1\leq i_g\leq p-1$, then we have

$$\psi(g(x))=\psi\left(\varphi(g(x_0)+\sum_{i=1}^{p-1}[\epsilon]^{i_g}\varphi([\epsilon]^{j_g}g(x_i))\right)=g(x_0)=g(\psi(x))$$

□

The following result generalizes this operator ψ to any étale (φ,Γ)-module.

Proposition 5.6. If D is an étale (φ,Γ)-module over A_K (or B_K), there is a unique operator $\psi: D\to D$ satisfying that, for every $a\in A_K$, $x\in D$, $\psi(\varphi(a)x)=a\psi(x)$ and $\psi(a\varphi(x))=\psi(a)x$.

Proof. By Theorem 5.4, it is enough to prove it for an étale (φ,Γ)-module of the form $D(V)$, for some representation V. In this situation, we have $D(V)=(A\otimes_{\mathbb{Z}_p}V)^{H_K}$. Therefore, we can define ψ on $(A\otimes_{\mathbb{Z}_p}V)$ via the operator ψ on A that we have already defined, $\psi(a\otimes x)=\psi(a)\otimes x$. By the previous proposition, ψ commutes with $G_{\mathbb{Q}_p}$, and therefore, if $\sigma\in H_K$, $\sigma(\psi(a\otimes x))=\psi(\sigma(a\otimes x))=\psi(a\otimes x)$. Therefore $\psi(a\otimes x)\in D(V)$ if $a\otimes x\in D(V)$, and, in conclusion, ψ is well defined as an operator $D(V)\to D(V)$.

Now let's check that the properties are satisfied. Let $a\in A_K$, $x=b\otimes v\in D(V)$. Then, $\psi(\varphi(a)x)=\psi(\varphi(a)b\otimes x)=a\psi(b)\otimes x=a\psi(b\otimes x)$. The same argument shows that $\psi(a\varphi(x))=\psi(a)x$.

The uniqueness of the operator ψ follows from the fact that $D(V)$ is étale, and so $\varphi(D(V))$ generates $D(V)$ as an A_K-module, and so $D(V)=A_K\otimes_{\varphi(D(V))}\varphi(D(V))$, and ψ is completely determined by $\psi(a\varphi(x))=\psi(a)x$ and the definition of $\psi: A\to A$. □

Example 5.1. Consider the trivial (φ,Γ)-module $D=A_{\mathbb{Q}_p}\cong\mathbb{Z}_p\widehat{[[\pi]][\pi^{-1}]}$, and its submodule $\mathbb{Z}_p[[\pi]]$, that we'll denote $A^+_{\mathbb{Q}_p}$. φ acts on $A_{\mathbb{Q}_p}$ in a way that it induces the Frobenius in $E_{\mathbb{Q}_p}$. Therefore it is enough to define its action on π. But, as $\pi=[\epsilon]-1$, then $\varphi(\pi)=\varphi([\epsilon]-1)=[\epsilon]^p-1=(\pi+1)^p-1$.

Therefore, for every $F(\pi)\in A_{\mathbb{Q}_p}$, we can write $F(\pi)=\sum_{i=0}^{p-1}(1+\pi)^iF_i((1+\pi)^p-1)$, and $\psi(F(\pi))=F_0(\pi)$.

Moreover, we have

$$\varphi(\psi(F))=\frac{1}{p}\sum_{z^p=1}F(z(1+\pi)-1)$$

This is because $F_0((1+\pi)^p-1)$ can be written as $\frac{1}{p}\sum_{i=0}^{p-1}\sum_{z^p=1}(z(1+\pi))^iF((z(1+\pi))^p-1)$, as the i-th term of the sum for i is just $pF_0((1+\pi)^p-1)$ for $i=0$ and for $i>0$ it is equal to $(\sum_{z^p=1}z^i)((1+\pi))^iF(((1+\pi))^p-1))=0$ as $(\sum_{z^p=1}z^i)=0$.

We will now prove that given an étale φ module, the submodule $D^{\psi=1} = \{x \in D \text{ such that } \psi(x) = x\}$ is compact. We need a lemma first.

Lemma 5.4. If D is an étale (φ, Γ)-module, then the weak topology on A_K induces a topology on D, and ψ is continuous for this topology.

Proof. As A_K is a finite extension of $A_{\mathbb{Q}_p}$ we can consider every A_K-module as an $A_{\mathbb{Q}_p}$-module and reduce to the case $K = \mathbb{Q}_p$. The structure theorem of modules over a PID ensures that we can write every $A_{\mathbb{Q}_p}$-module as a direct sum $D \cong \bigoplus(A_{\mathbb{Q}_p}/p^{n_i})$, for $n_i \in \mathbb{N} \cup \infty$. Thus, via this identification, we can induce a topology on D via the weak topology on $A_{\mathbb{Q}_p}$, and it's enough to check that ψ is continuous in $A_{\mathbb{Q}_p}$.

To prove this, it's enough to show that $\psi(A^+_{\mathbb{Q}_p}) \subseteq A^+_{\mathbb{Q}_p}$ (i.e. ψ doesn't increase distances). As these rings are complete for the p-adic topology, it's enough to show the statement modulo p, that is, $\psi(E^+_{\mathbb{Q}_p}) \subseteq E^+_{\mathbb{Q}_p}$ (though we didn't give a definition of ψ in $E_{\mathbb{Q}_p}$, its completely analogous: Replace $[\epsilon]$ by ϵ in Definition 5.16).

Indeed, with the notation of Example 5.1, let $F(\pi) = \sum_{i=0}^{p-1}(1+\pi)^i F_i((1+\pi)^p - 1) \in A^+_{\mathbb{Q}_p}$, so F doesn't have denominators in π. Modulo p, the expression transforms to $\overline{F}(\overline{\pi}) = \sum_{i=0}^{p-1}(1+\overline{\pi})^i \overline{F_i}(\overline{\pi}^p)$. Suppose that we have

$$\overline{F_i} = \frac{\sum_{j=0}^{\infty} a_j \overline{\pi}^j}{\sum_{j=0}^{\infty} b_j \overline{\pi}^j}$$

Note that $b_0 = 0$, as otherwise the denominator is invertible in $\mathbb{F}_p[[\overline{\pi}]]$. But then $(1+\overline{\pi})^i\overline{F_i}(\overline{\pi}^p) = \frac{1}{\overline{\pi}^p} G_i$, with G_i with lowest $\overline{\pi}$ exponent i. Therefore the $\overline{\pi}^p$ in the denominator can't be killed, and we have a contradiction with $\overline{F} \in \mathbb{F}_p[[\overline{\pi}]]$. In consequence, if $F(\pi) \in A^+_{\mathbb{Q}_p}$, then $F_0(\pi) = \psi(F(\pi)) \in A^+_{\mathbb{Q}_p}$, and so ψ is continuous for the week topology. □

Proposition 5.7. If D is an étale φ-module over A_K (respectively, over B_K), then $D^{\psi=1}$ is compact (respectively, locally compact).

Proof. Note that we can reduce to prove the same result over $E_{\mathbb{Q}_p}$. Indeed, first we can reduce to $K = \mathbb{Q}_p$. Moreover, the case B_K follows from the case of A_K by tensor product with $\mathbb{Q}_p$. Moreover, $D^{\psi=1} = \varprojlim_n (D/p^n D)^{\psi=1}$. Therefore it is enough to show that $(D/p^n D)^{\psi=1}$ is compact. This follows from induction if we prove that $(D/pD)^{\psi=1}$, which is an étale φ-module over $E_{\mathbb{Q}_p}$, is compact.

So, let $\{e_1, \dots, e_d\}$ be a basis of D over $E_{\mathbb{Q}_p}$. As D is étale, then $\{\varphi(e_1), \dots, \varphi(e_d)\}$ is still a basis. Now let $x = \sum x_i \varphi(e_i)$, and we have, by definition of valuation in D, $v_E(x) = \inf_i v_E(x_i)$. Now let $\psi(x) = \sum \psi(x_i) e_i$, $e_i = \sum_{j=1}^d a_{i,j}\varphi(e_j)$ and set $c = \inf_{i,j} v_E(a_{i,j})$. Then, we have

$$v_E(\psi(x)) \geq c + \inf_i v_E(\psi(x_i))$$

On the other hand, write $x = \sum_{i=0}^{p-1}(1+\overline{\pi})^i F_i(\overline{\pi}^p)$, as we're in characteristic p. Then we have $v_E(x) = \min v_E(F_i(\overline{\pi}^p)) \leq v_E(F_0(\overline{\pi}^p)) = p v_E(\psi(x))$. In conclusion,

$$v_E(\psi(x)) \geq \lfloor \frac{v_E(x)}{p} \rfloor$$

Therefore, the inequality above yields

$$v_E(\psi(x)) \geq c + \inf \lfloor \frac{v_E(x_i)}{p} \rfloor \geq c + \lfloor \frac{v_E(x)}{p} \rfloor$$

Therefore, if $v_E(x) < \frac{p(c-1)}{p-1}$, then $v_E(\psi(x)) \geq c + \lfloor \frac{c-1}{p-1} \rfloor \geq \frac{p(c-1)}{p-1}$, and so $x \notin D^{\psi=1}$.
In particular,

$$D^{\psi=1} \subseteq M := \left\{ x \text{ such that } v_E(x) \geq \frac{p(c-1)}{p-1} \right\}$$

But M is compact (it is a closed disk), and $D^{\psi=1}$ is closed in D since ψ is continuous (by Lemma 5.4), and so $D^{\psi=1}$ is a closed subset of a compact set, and therefore compact. □

Finally, we state two more results about the structure of (φ, Γ)-modules that will be needed in the following sections.

Proposition 5.8. ([10], Proposition 5.3.8 (ii)) If D is an étale φ-module over A_K (respectively, over B_K), then $D/(\psi - 1)$ is finitely generated over $\mathbb{Z}_p$ (respectively $\mathbb{Q}_p$)

Proposition 5.9. ([10], Proposition 5.3.13) If D is an étale (φ, Γ)-module over A_K or B_K, then $\gamma - 1$ has a continuous inverse on $D^{\psi=0}$.

5.5 Galois Cohomology

Now we will relate the theory of (φ, Γ)-modules with Galois cohomology. First of all we give a brief introduction on the basics of this cohomology theory.

Definition 5.17. Let G be a profinite group, and A an abelian group. We say that A is a G-module if it has an action $G \times A \to A$ that is continuous when we give A the discrete topology.

Lemma 5.5. The action of a profinite group G on a set E with the discrete topology is continuous $\iff$ $\forall e \in E$ the stabilizer $G_e = \{\sigma \in G : \sigma e = e\}$ is open in G.

Proof. Let $A : G \times E \to E$ denote the action. Let $e \in E$. If the action is continuous, the set $U = A^{-1}(\{e\}) = \{(\sigma, g) \text{ such that } \sigma g = e\}$ is open. Then, $U \cap (G \times \{e\}) = G_e$ is also open.
Reciprocally, let Ge denote the orbit of $e \in E$. Let $e' \in Ge$, and $\tau_{e'} \in G$ such that $\tau_{e'} e = e'$. Then, $m^{-1}_{\tau_{e'}}(G_e) = \{\sigma : \sigma e' = e\}$ is open. Then, $A^{-1}(\{e\}) = \bigcup_{e' \in Ge} (m^{-1}_{\tau_{e'}}(G_e) \times \{e'\})$ is open, and so the action is continuous. □

Definition 5.18. Let G be a group, A a G-module. Denote $C^i(G, A)$ the set of continuous maps $G^n \to A$ (note that $C^0(G, A)$ is just A). We define the coboundary maps

$$\partial_n : C^n(G, A) \to C^{n+1}(G, A)$$

by $\partial f(g_1, \ldots, g_n) = g_1 f(g_2, \ldots, g_n) + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_n) + (-1)^{n+1} f(g_1, \ldots, g_n)$
This gives a cohomological complex

$$0 \to C^0(G,A) \underset{\partial}{\to} C^1(G,A) \underset{\partial}{\to} \dots$$

whose cohomology groups $H^i(G,A)$ are called *the cohomology groups of G with coefficients in A.*

Definition 5.19. Given A a G-module, A^G is the submodule of elements fixed by G, $A^G = \{x \in A \text{ such that } \sigma x = x \ \forall \sigma \in G\}$.

One has the following result (which we won't prove), that gives an alternative definition for the cohomology groups of G.

Lemma 5.6. The functors $A \mapsto H^i(G,A)$ are the right derived functors of the left exact functor $A \mapsto A^G$.

Definition 5.20. Let K be a field, and G_K its absolute Galois group, which is a profinite group. If A is a G_K-module, we define $H^i(G_K, A)$ the *Galois cohomology.*

Definition 5.21. Let $\phi : G' \to G$ be a morphism of groups. This induces a morphism of complexes

$$\begin{array}{ccccccc} 0 & \longrightarrow & C^0(G,A) & \longrightarrow & C^1(G,A) & \longrightarrow & \dots \\ & & \downarrow \phi & & \downarrow \phi & & \\ 0 & \longrightarrow & C^0(G',A) & \longrightarrow & C^1(G',A) & \longrightarrow & \dots \end{array}$$

by sending $C^i(G,A) \ni f \mapsto (f \circ \phi) \in C^i(G',A)$. This induces a morphism in cohomology. There are two main examples of this situation.

- When H is a subgroup of G, and $\phi : H \to G$ is simply the inclusion. The induced morphism on cohomology is called the *restriction*:

  $$Res_{G/H} : H^i(G,A) \to H^i(H,A)$$

  On dimension 0 it's simply the inclusion $A^G \to A^H$.

- If H is a normal subgroup of G, then $\phi : G \to G/H$ induces a morphism on cohomology called the *inflation*

  $$Inf_{G/H} : H^i(G/H,A) \to H^i(G,A)$$

Theorem 5.5. *(Inflation-restriction)([23]) The following sequence is exact*

$$0 \to H^1(G/H, A^H) \xrightarrow{inf} H^1(G,A) \xrightarrow{res} H^1(H,A)^{G/H} \to H^2(G/H, A^H) \xrightarrow{inf} H^2(G,A)$$

Observation 5.8. ([21]) If H is an open subgroup of G of index n, there is also a *corestriction* map

$$Cor : H^q(H,A) \to H^q(G,A)$$

which in dimension 0 is the norm map $N_{G/H} : A^H \to G^H$, $a \mapsto \sum_{G/H} \sigma(a)$. Moreover, the composition with the restriction is the multiplication-by-n map.

$$Cor \circ Res = |G/H|$$

The following examples and results are a little motivation for the introduction of Galois cohomology.

Example 5.2. We consider the problem of lifting fixed points: Suppose that we have $A \subset B$ two G-modules and we consider the G-modules B/A and $(B/A)^G$. Is it possible to lift elements of $(B/A)^G$ to B^G?

Let $b \in B$ be such that $\bar{b} \in (B/A)^G$. Define the map $f_b : G \to A$ given by $g \mapsto gb - b$. Note that $f_b(gg') = gf_b(g') + f_b(g)$, so f_b gives rise to a 1-cocycle, and, moreover, f_b measures the obstruction of lifting $\bar{b}$ to a fixed point in B. In particular, f_b is a coboundary if and only if $f_b(g) = ga - a$ for every g, that is, if and only if $b - a$ is a fixed point over B.

Example 5.3. (Cohomology of cyclic groups) If the group G is a finite cyclic group, any cocycle is determined by $f(\gamma)$, where γ is a generator of G.

Note that $f(\gamma) \in \ker Tr_G$, where $Tr_G : A \to A$ is the map $a \mapsto \sum_{\sigma \in G} \sigma(a)$. This is clear, as $Tr_G = \sum_k \gamma^k f(\gamma) = \sum_k f(\gamma^{k+1}) - f(\gamma^k) = 0$, as it's a telescopic sum. Reciprocally, if $f(\gamma) = a$, with $a \in \ker(Tr_G)$, we have $f(\gamma^k\gamma^m = f(\gamma^k) + \gamma^k f(\gamma^m)$, as $f(\gamma^m) = 0 = Tr_G(a)$ and $f(\gamma^k) = \sum_{i=0}^{n-1} \gamma^i a$. Therefore it's enough to show the result for $k + m < n$, which is an easy computation. Therefore, this shows that

$$H^1(G, A) \cong \frac{\ker Tr_G}{(1-\gamma)A}$$

As a direct consequence, we have shown the additive form of Hilbert's Theorem 90: Let $a \in k$, $\mathrm{Gal}(K/k)$ be cyclic of degree n. Then, $Tr_{\mathrm{Gal}(K/k)}(a) = 0$ if and only if $a = \alpha - \gamma\alpha$, for a certain $\alpha \in K$. In conclusion,

$$H^1(G, K) = 0$$

After this introduction on Galois Cohomology, let's consider our problem. Suppose that we have V a $\mathbb{Z}_p$ or a $\mathbb{Q}_p$ representation of G_K, and we want to compute its Galois Cohomology groups. We may do so using the theory of (φ, Γ)-modules. Recall that we've defined $D(V) = (A \otimes_{\mathbb{Z}_p} V)^{H_K}$.

Definition 5.22. The complex $C_{\varphi,\gamma}(K, V)^\bullet$ is the following one

$$0 \to D(V) \xrightarrow{(\varphi-1,\gamma-1)} D(V) \oplus D(V) \xrightarrow{(\gamma-1)pr_1-(\varphi-1)pr_2} D(V) \to 0$$

The complex is well defined, as γ and φ commute.

Theorem 5.6. *For every $i \in \mathbb{N}$, we have*

$$H^i(C_{\varphi,\gamma}(K, V)) \cong H^i(G_K, V)$$

This result was originally proved by Herr in [14]. However, here we give another proof, which is more explicit, following [7].

Proof. $\boxed{i = 0}$ Note that

$$H^0(C^\bullet_{\varphi,\gamma}(K, V)) = \{x \in D(V) | \gamma(x) = x, \varphi(x) = x\} = D(V)^{\varphi=1,\gamma=1}$$

But we know that $D(V) = (A \otimes_{\mathbb{Z}_p} V)^{H_K}$, so $D(V)^{\varphi=1} = (A^{\varphi=1} \otimes_{\mathbb{Z}_p} V)^{H_K}$ and $A^{\varphi=1} = \mathbb{Z}_p$ so $D(V)^{\varphi=1} = V^{H_K}$. In consequence, $D(V)^{\varphi=1,\gamma=1} = V^{G_K} = H^0(G_K, V)$.

$\boxed{i=1}$ In this case we have

$$H^1(C^\bullet_{\varphi,\gamma}(K,V)) = \frac{\{(x,y) \in D(V) \oplus D(V) | (\gamma-1)x = (\varphi-1)y\}}{\{((\varphi-1)z, (\gamma-1)z) | z \in D(V)\}}$$

First we claim that that the following sequence is exact.

$$0 \to \mathbb{Z}_p \to A \xrightarrow{\varphi-1} A \to 0 \tag{15}$$

To show this, it's enough to prove it modulo p, as all the rings are complete w.r.t the p-adic topology. Modulo p, the sequence is

$$0 \to \mathbb{F}_p \to E \xrightarrow{\varphi-1} E \to 0$$

The only non-trivial think to check is the surjectivity of $\varphi - 1$. But this is clear since E is the separable closure of $E_{\mathbb{Q}_p}$, so every separable polynomial has roots. In particular, as $f_a(x) = X^p - X - a$ is separable for every $a \in E$, for every $a \in E$ we can find $b \in E$ such that $b^p - b = a$, so $\varphi - 1$ is surjective.

Moreover, as V is a free $\mathbb{Z}_p$-module, it is flat and so tensoring Equation (15) with V we get an exact sequence

$$0 \to V \to A \otimes_{\mathbb{Z}_p} V \xrightarrow{\varphi-1} A \otimes_{\mathbb{Z}_p} V \to 0 \tag{16}$$

Now let $(x,y) \in H^1(C^\bullet_{\varphi,\gamma}(K,V))$, so we have $(\gamma-1)x = (\varphi-1)y$. By Equation (16), we know we can choose $b \in A \otimes_{\mathbb{Z}_p} V$ such that $(\varphi-1)b = x$. This allows us to define a cocycle with values in V:

$$g \in G_K \mapsto c_{x,y}(g) = \frac{g-1}{\gamma-1} y - (g-1)b$$

Where $\frac{g-1}{\gamma-1}y := \lim_{i\to\infty}(1+\gamma+\cdots+\gamma^{n_i-1})y$, with $\chi(g) = \lim_{i\to\infty}\chi(\gamma)^{n_i}$. It's immediate that the map we have defined is a cocycle, and moreover we have $(\varphi-1)c_{x,y}(g) = (g-1)x - (\varphi-1)(g-1)b = 0$, so $c_{x,y}(g) \in (A \otimes_{\mathbb{Z}_p} V)^{\varphi=1} = V$.

In addition, note that $c_{(\varphi-1)z,(\gamma-1)z}(g) = (g-1)(z-z) = 0$. Therefore the map $(x,y) \mapsto c_{x,y}$ induces a morphism

$$H^1(C^\bullet_{\varphi,\gamma}(K,V)) \to H^1(G_K, V)$$

We will prove that it is an isomorphism. To prove injectivity, suppose that we have $c_{x,y} = 0$ in $H^1(G_K, V)$, that is, we have that $\exists z \in V$ such that $c_{x,y}(g) = (g-1)z$. Therefore we have

$$\frac{g-1}{\gamma-1} y = (g+1)(b+z)$$

Then we have that $b+z \in D(V)$, because it's fixed by H_K, and so we have that $y = (\gamma-1)(b+z)$ and $x = (\varphi-1)(b+z)$ so $(x,y) = 0$ in $H^1(C^\bullet_{\varphi,\gamma}(K,V))$.

To prove surjectivity, to every 1-cocycle c we can associate a G_K-module E_c, which is isomorphic to $\mathbb{Z}_p \times V$ as a $\mathbb{Z}_p$-module, and G_K acts on E_c by $g(a,m) = (a, gm + c_g)$. We have the exact sequence

$$0 \to V \to E_c \to \mathbb{Z}_p \to 0$$

Let $e \in E_c$ such that $e \mapsto 1 \in \mathbb{Z}_p$, we have $ge = e + c_g$, so $(g-1)e = c_g$. As the functor D is an equivalence of categories, we have

$$0 \to D(V) \to D(E_c) \to A_K \to 0$$

Let $\tilde{e} \in D(E_c) \mapsto 1 \in \mathbb{Z}_p$, and let $x = (\varphi - 1)\tilde{e}$ and $y = (\gamma - 1)\tilde{e}$, which satisfy $(\gamma - 1)x = (\varphi - 1)y$. Let $b = \tilde{e} - e \in A \otimes_{\mathbb{Z}_p} E_c$. Then $(\varphi - 1)b = x$ and

$$c_{x,y}(g) = \frac{g-1}{\gamma - 1} y - (g-1)b = \frac{g-1}{\gamma - 1}(\gamma - 1)\tilde{e} - (g-1)(\tilde{e} - e) = (g-1)e = c_g$$

$\boxed{i > 1}$ Note that we have

$$H^2(C^\bullet_{\varphi,\gamma}(K, V)) = \frac{D(V)}{(\gamma - 1, \varphi - 1)}$$

and $H^i(C^\bullet_{\varphi,\gamma}(K, V)) = 0$, for $i \geq 3$.

From Equation (16) we get a long exact sequence in cohomology

$$0 \to V^{H_K} \to D(V) \xrightarrow{\varphi - 1} D(V) \to H^1(H_K, V) \to 0 \tag{17}$$

As $A \otimes V \cong \oplus(A/p^i)$ as H_K-modules and $H^i(H_K, A/pA) = 0$, so $H^i(H_K, A \otimes V) = 0$ for every $i \geq 1$. Therefore the above exact sequence tells us that

$$H^1(H_K, V) = \frac{D(V)}{\varphi - 1} \tag{18}$$

By the Hochschild-Serre spectral sequence (see [23]) for $1 \to H_K \to G_K \to \Gamma_K \to 1$, we have $H^i(\Gamma_K, H^j(H_K, V)) \Rightarrow H^{i+j}(G_K, V)$. Then the cohomology vanishes for j or $i \geq 2$ so we have

$$H^i(G_K, V) = 0 \quad \text{for } i \geq 3$$

For $i = 1, j = 1$ we get $H^2(G_K, V) \cong H^1(\Gamma_K, H^1(H_K, V))$. Since $H^1(H_K, V) = \frac{D(V)}{\varphi - 1}$, we have

$$H^2(G_K, V) \cong \frac{\frac{D(V)}{(\varphi - 1)}}{\frac{(\gamma - 1)D(V)}{(\varphi - 1)}}$$

□

Observation 5.9. We have $H^1(H_K, V)^{\Gamma_K} = \frac{D(V)}{\varphi - 1}^{\Gamma_K}$ by Equation (18). On the other hand, taking cohomology $H^i(\Gamma_K, -)$ in the exact sequence Equation (17) gives an exact sequence

$$D(V)^{\gamma = 1} \to \left(\frac{D(V)}{\varphi - 1}\right)^{\gamma = 1} \to H^1(\Gamma_K, V^{H_K})$$

And so we have that $H^1(\Gamma_K, V^{H_K}) = \frac{D(V)^{\varphi=1}}{\gamma-1}$. Therefore the inflation-restriction exact sequence for G_K and H_K becomes the exact sequence

$$0 \to \frac{D(V)^{\varphi=1}}{\gamma-1} \to H^1(G_K, V) \to \left(\frac{D(V)}{\varphi-1}\right)^{\Gamma_K} \to 0$$

Definition 5.23. The complex $C_{\psi,\gamma}(K,V)^\bullet$ is the following one

$$0 \to D(V) \xrightarrow{(\psi-1,\gamma-1)} D(V) \oplus D(V) \xrightarrow{(\gamma-1)pr_1-(\psi-1)pr_2} D(V) \to 0$$

Proposition 5.10. The commutative diagram of complexes

$$\begin{array}{ccccccccc} C_{\varphi,\gamma}: 0 & \longrightarrow & D(V) & \longrightarrow & D(V)\oplus D(V) & \longrightarrow & D(V) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Id} & & \downarrow{\scriptstyle (-\psi, Id)} & & \downarrow{\scriptstyle -\psi} & & \\ C_{\psi,\gamma}: 0 & \longrightarrow & D(V) & \longrightarrow & D(V)\oplus D(V) & \longrightarrow & D(V) & \longrightarrow & 0 \end{array}$$

induces an isomorphism on cohomology.

Proof. The diagram commutes as $(-\psi)(\varphi-1) = \psi - 1$, and ψ commutes with γ (c.f Proposition 5.5). Moreover, ψ is surjective, so the cokernel complex ix 0. The kernel complex is

$$0 \to 0 \to D(V)^{\psi=0} \xrightarrow{\gamma-1} D(V)^{\psi=0} \to 0$$

But this complex has no cohomology because of Proposition 5.9. □

Therefore, as a corollary we have the following theorem

Theorem 5.7. *If V is a $\mathbb{Z}_p$ or a $\mathbb{Q}_p$ representation of G_K, then we have*

i) $H^0(G_K, V) = D(V)^{\psi=1,\gamma=1} = D(V)^{\varphi=1,\gamma=1}$
ii) $H^2(G_K, V) \cong \frac{D(V)}{(\psi-1,\gamma-1)}$
iii) We have an exact sequence

$$0 \to \frac{D(V)^{\psi=1}}{\gamma-1} \to H^1(G_K, V) \to \left(\frac{D(V)}{\psi-1}\right)^{\gamma=1} \to 0$$

5.6 Iwasawa theory

Notation. Assume that Γ_K is procyclic and denote γ_n the topological generator of $\mathrm{Gal}(K_\infty/K_n)$. We choose γ_n to be compatible, that is, $\gamma_n = \gamma_1^{p^{n-1}}$.

Definition 5.24. The *Iwasawa algebra* is $\mathbb{Z}_p[[\Gamma_K]]$. It's isomorphic to $\mathbb{Z}_p[[T]]$ via $T \mapsto \gamma - 1$.

Definition 5.25. Let V be a $\mathbb{Z}_p$ representation of G_K. We define the *Iwasawa cohomology* groups as

$$H^i_{Iw}(K, V) = \varprojlim_n H^i(G_{K_n}, V)$$

where the transition maps are the corestriction maps.

If V' is instead a $\mathbb{Q}_p$-representation, we choose a stable $\mathbb{Z}_p$ lattice T in V' and define

$$H^i_{Iw}(K, V') = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i_{Iw}(K, T)$$

We want to relate $H^1_{Iw}(K, V)$ with (φ, Γ)-modules. First we need a lemma:

Lemma 5.7. If M is compact with a continuous action of Γ_K; then we have

$$M \cong \varprojlim_n \frac{M}{\gamma_n - 1}$$

Proof. There is a natural map $M \to \varprojlim_n \frac{M}{\gamma_n - 1}$. To prove injectivity, it's enough to show that $\bigcup_{n\in\mathbb{N}}(\gamma_n - 1)M = 0$. Choose a neighbourhood V of 0 in M. By continuity of the action of Γ_K, $\forall x \in M$, there exists $n_x \in \mathbb{N}$ and $U_x \ni x$ open set such that $(\gamma_{n_x} - 1)x' \in V$, for every $x' \in U_x$. Then, $M = \bigcup U_x$ and by compactness we can choose a finite subcovering $M = \bigcup_{i=1}^k U_{x_i}$. Choose $n = \max n_{x_k}$ and we have $(\gamma_n - 1)M \subseteq V$. This holds for every V, so the injectivity is proved.

Now let's prove surjectivity. We have a Cauchy sequence $(x_n) \in \varprojlim_n (M/(\gamma_n - 1))$. By compactness, $\exists x = \lim x_n$. We have $(x_{n+k} - x_n) = (\gamma_n - 1)y_k$. Again by compactness, y_k has a limit, so we get $x - x_n = (\gamma_n - 1)y$, so (x_n) is the image of x by the natural map $M \to \varprojlim_n \frac{M}{\gamma_n - 1}$. □

Theorem 5.8. *There is an isomorphism*

$$Exp^* : H^1_{Iw}(K, V) \to D(V)^{\psi=1}$$

Proof. Let $\tau_n = \frac{\gamma_n - 1}{\gamma_{n-1} - 1} = 1 + \gamma_{n-1} + \cdots + \gamma_{n-1}^p$. Then, we have the following commutative diagram

$$\begin{array}{ccccccccc}
C_{\psi,\gamma_n} : 0 & \longrightarrow & D(V) & \longrightarrow & D(V) \oplus D(V) & \longrightarrow & D(V) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau_n} & & \downarrow{\scriptstyle (\tau_n, Id)} & & \downarrow{\scriptstyle Id} & & \\
C_{\psi,\gamma_{n-1}} : 0 & \longrightarrow & D(V) & \longrightarrow & D(V) \oplus D(V) & \longrightarrow & D(V) & \longrightarrow & 0
\end{array}$$

It induces corestrictions on H^i, as it is a functor and induces the trace map $Tr_{K_n/K_{n-1}}$ on H^0. Therefore, we have the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{D(V)^{\psi=1}}{\gamma_n - 1} & \longrightarrow & H^1(G_{K_n}, V) & \longrightarrow & \frac{D(V)^{\gamma_n=1}}{\psi - 1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle cor} & & \downarrow{\scriptstyle \tau_n} & & \\
0 & \longrightarrow & \frac{D(V)^{\psi=1}}{\gamma_{n-1} - 1} & \longrightarrow & H^1(G_{K_{n-1}}, V) & \longrightarrow & \frac{D(V)^{\gamma_{n-1}=1}}{\psi - 1} & \longrightarrow & 0
\end{array}$$

Using the $\varprojlim$ functor, we get the sequence

$$0 \to \varprojlim \frac{D(V)^{\psi=1}}{\gamma_n - 1} \to H^1_{Iw}(K, V) \to \varprojlim \left(\frac{D(V)}{\psi - 1}\right)^{\gamma_n=1}$$

As $D(V)^{\psi=1}$ is compact (c.f Proposition 5.7), then by Lemma 5.7 we have $\varprojlim \frac{D(V)^{\psi=1}}{\gamma_n - 1} \equiv D(V)^{\psi=1}$. Moreover, $\left(\frac{D(V)}{\psi-1}\right)^{\gamma_n=1}$ is increasing and $\frac{D(V)}{\psi-1}$ is finite dimensional (c.f Proposition 5.8), so it must be stationary for some n, say N. But then τ_n is just multiplication by p for $n \geq N$, and so every element of $\frac{D(V)}{\psi-1}^{\gamma_N}$ is (infinitely) p-divisible. But $\frac{D(V)}{\psi-1}$ does not contain p-divisible elements. Indeed, any p-divisible element in $\frac{D(V)}{\psi-1}$ can be represented by $x \in D(V)$ and we have that $\forall n, \exists y_n, z_n$ such that $x = p^n y_n + (\psi - 1)z_n$. Therefore, fixing m, we have that z_n is a solution of $(\psi - 1)(z) = x \mod p^{m+1}$ for every $n \geq m + 1$. As $D(V)^{\psi=1}$ is compact, we can extract a convergent partial subsequence, and it is possible to do that (by diagonal extraction) to obtain a sequence that converges modulo p^m for every m. Then, if z is the limit of such sequence, $x = (\psi - 1)z$ and so it is 0 on $\frac{D(V)}{\psi-1}$.

Therefore $\varprojlim \left(\frac{D(V)}{\psi-1}\right)^{\gamma_n=1} = 0$ and so we have an isomorphism

$$H^1_{Iw}(K, V) \to D(V)^{\psi=1}$$

□

6 $\mathbb{Z}_p(1)$ and Kubota-Leopoldt zeta function

In this section we give an alternative construction of the Kubota-Leopoldt zeta function, based on the theory of (φ, Γ)-modules of last chapter. In particular, we will produce the Kubota-Leopoldt zeta function from a compatible system of cyclotomic units. As we will see in the next chapter, this system of cyclotomic units can be extended to form an Euler system, so the construction that we give in this chapter builds a relation between the p-adic L-function of Kubota-Leopoldt and the Euler system of cyclotomic units, associated to the representation $\mathbb{Q}_p(1)$.

The following observation gives an alternative approach to measures, that we will use.

Observation 6.1. $(A^+_{\mathbb{Q}_p})^{\psi=0}$ can be seen as measures on $\mathbb{Z}_p^*$. This is a consequence of the isomorphism $\mathbb{Z}_p[[T]] \cong A^+_{\mathbb{Q}_p} = \mathbb{Z}_p[[\pi]]$ given by $T \mapsto \pi$. Moreover, the isomorphism preserves the actions of φ and ψ, so $(A^+_{\mathbb{Q}_p})^{\psi=0}$ correspond to measures with support in $\mathbb{Z}_p^*$ via the isomorphism with $\mathbb{Z}_p[[T]]$ and the Amice transform.

Moreover, $(\pi A^+_{\mathbb{Q}_p})^{\psi=0}$ correspond to measures in $\mathbb{Z}_p^*$, such that $\int_{\mathbb{Z}_p^*} \mu = 0$ (its Amice transform has the T^0 coefficient null).

Definition 6.1. Let $\mathbb{Z}_p(1)$ be the module $\mathbb{Z}_p$ with an action pf $G_{\mathbb{Q}_p}$ given by $g(x) = \chi(g)x$, where χ is the cyclotomic character.

Similarly, $A_{\mathbb{Q}_p}(1) = D(\mathbb{Z}_p(1)) = (A \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1))^{H_{\mathbb{Q}_p}} = A_{\mathbb{Q}_p}(1)$, which is just $A_{\mathbb{Q}_p}$ with the usual actions of φ, ψ and an action of Γ given by

$$\gamma(f(\pi)) = \chi(\gamma) f((1+\pi)^{\chi(\gamma)} - 1)$$

Proposition 6.1. i) $A^{\psi=1}_{\mathbb{Q}_p} = \mathbb{Z}_p \frac{1}{\pi} \oplus (A^+_{\mathbb{Q}_p})^{\psi=1}$

ii) We have an exact sequence

$$0 \to \mathbb{Z}_p \to (A^+_{Q_p})^{\psi=1} \xrightarrow{\varphi-1} (\pi A^+_{\mathbb{Q}_p})^{\psi=0} \to 0$$

Proof. i) We know that $\psi(A^+_{\mathbb{Q}_p}) \subseteq A^+_{\mathbb{Q}_p}$ (see Lemma 5.4), $\psi(\frac{1}{\pi}) = \frac{1}{\pi}$ (see Proposition 3.3), and that $v_E(\psi(x)) \geq \left[\frac{v_E(x)}{p}\right]$ if $x \in E_{\mathbb{Q}_p}$ (see Proposition 5.7). This implies that $\psi - 1$ is injective on $E_{\mathbb{Q}_p}/\overline{\pi}^{-1}E^+_{\mathbb{Q}_p}$ and hence also on $A_{\mathbb{Q}_p}/\pi^{-1}A^+_{\mathbb{Q}_p}$. Therefore, if $x \in (A_{\mathbb{Q}_p})^{\psi=1}$, we have $\psi(x) = x$ and so $x \in \pi^{-1}A^+_{\mathbb{Q}_p} = \mathbb{Z}_p \frac{1}{\pi} \oplus (A^+_{\mathbb{Q}_p})^{\psi=1}$.

ii) First of all, note that the exact sequence

$$0 \to \mathbb{Z}_p \to (A^+_{Q_p})^{\psi=1} \xrightarrow{\varphi-1} (\pi A^+_{\mathbb{Q}_p})^{\psi=0} \to 0$$

is well defined. Indeed, we have $(\varphi - 1)A^+_{\mathbb{Q}_p} \subseteq \pi A^+_{\mathbb{Q}_p}$. This is immediate as $A^+_{\mathbb{Q}_p} = \mathbb{Z}_p[[\pi]]$. Moreover, $\psi(\varphi-1)(A^+_{\mathbb{Q}_p})^{\psi=1} = (\psi\varphi - \psi)A^+_{\mathbb{Q}_p})^{\psi=1} = 0$ as $\psi = 1$ on $(A^+_{\mathbb{Q}_p})^{\psi=1}$ and $\psi\varphi = 1$ always.

On the other side, again because $A^+_{\mathbb{Q}_p} = \mathbb{Z}_p[[\pi]]$, it's clear that $\ker(\varphi - 1) = \mathbb{Z}_p$ and that $\mathbb{Z}_p \to A^+_{\mathbb{Q}_p}$ is an inclusion. So it only remains to show the surjectivity of $\varphi - 1$. But, if

$x \in (\pi A^+_{\mathbb{Q}_p})^{\psi=0}$, then $\lim_{n\to\infty} \varphi^n(x) = 0$ as $\varphi^n(x) \in \varphi(\pi)^n A^+_{\mathbb{Q}_p}$, and so $y = \sum_{n=0}^{\infty} \varphi^n(x)$ converges, and one has $(\varphi - 1)(-y) = x$ so $(\varphi - 1)$ is surjective.

□

Notation. Recall that we've fixed $\epsilon = (1, \epsilon^{(1)}, \epsilon^{(2)}, \dots,) \in E^+_{\mathbb{Q}_p}$, with $\epsilon^{(1)} \neq 1$. Let $\pi_n = \epsilon^{(n)} - 1$ and $F_n = \mathbb{Q}_p(\pi_n)$.

Observation 6.2. We have $N_{F_{n+1}/F_n}(\pi_{n+1}) = N_{F_{n+1}/F_n}(\epsilon^{(n+1)} - 1) = \prod_{\eta^p=1}(\epsilon^{(n+1)}\eta - 1)$, as the minimal polynomial of $\epsilon^{(n+1)}$ over F_n is $X^p - \epsilon^{(n)}$, and so for every $g \in \mathrm{Gal}(F_{n+1}/F_n)$, $g(\epsilon^{(n+1)}) = \eta\epsilon^{(n+1)}$, for some η such that $\eta^p = 1$. Moreover, we have $\prod_{\eta^p=1}(X\eta - 1) = X^p - 1$ and so $N_{F_{n+1}/F_n}(\pi_{n+1}) = \pi_n$, and we have $\mathcal{O}_{F_{n+1}} = \mathcal{O}_{F_n}[\pi_{n+1}]/(1 + \pi_{n+1})^p = (1 + \pi_n)$.

Definition 6.2. We will define a *Kummer map* κ as follows:

For every element $a \in F_n^*$, we choose $x = (a, x^{(1)}, \dots) \in \tilde{E}$. The choice of x is unique up to product by ϵ^u, with $u \in \mathbb{Z}_p$. As G_{F_n} leaves a invariant, $g(x) = (a, x'^{(1)}, \dots)$ and so

$$\frac{g(x)}{x} = \epsilon^{c(g)} \qquad \text{with } c(g) \in \mathbb{Z}_p$$

Therefore this defines a map $\kappa : F_n^* \to H^1(G_{F_n}, \mathbb{Z}_p(1))$ given by $a \mapsto \kappa(a) : g \mapsto c(g)$.

It should be checked that the Kummer map is well defined. First of all, $\kappa(a)$ is continuous, as $c(g) \in p^m\mathbb{Z}_p$ implies that g fixes the first m coordinates of x, that is, $g \in G_{F_{n+m}}$. Moreover, for $g_1, g_2 \in G_{F_n}$, we have

$$\frac{g_1g_2(x)}{x} = \frac{g_1(\epsilon^{c(g_2)}x)}{x} = \frac{\epsilon^{\chi(g_1)c(g_2)}g_1(x)}{x} = \epsilon^{\chi(g_1)c(g_2)+c(g_1)}$$

Therefore, $c(g_1g_2) = \chi(g_1)c(g_2) + c(g_1)$ and so $g_1c(g_2) - c(g_1g_2) + c(g_1) = \chi(g_1)c(g_2) - c(g_1g_2) + c(g_1) = 0$ and $\kappa(a)$ is a cocycle. It only remains to see that the choice of x is not relevant. Indeed, take $x' = \epsilon^u x$ and we have another cocycle c' given by

$$\epsilon^{c'(g)} = \frac{g(x')}{x'} = \frac{g(\epsilon^u x)}{\epsilon^u x} = \frac{g(\epsilon^u)}{\epsilon^u}\epsilon^{c(g)}$$

In conclusion, $c'(g) - c(g) = g(u) - u = (g-1)u$ so they define the same element in $H^1(G_{F_n}, \mathbb{Z}_p(1))$.

Observation 6.3. i) The following diagram is commutative

$$\begin{array}{ccc} F_{n+1}^* & \xrightarrow{\kappa} & H^1(G_{F_{n+1}}, \mathbb{Z}_p(1)) \\ \downarrow{\scriptstyle N_{F_{n+1}/F_n}} & & \downarrow{\scriptstyle cor} \\ F_n n^* & \xrightarrow{\kappa} & H^1(G_{F_n}, \mathbb{Z}_p(1)) \end{array}$$

ii) $H^1(G_{F_n}, \mathbb{Z}_p(1)) = \mathbb{Z}_p\kappa(\pi_n) \oplus \kappa(\mathcal{O}^*_{F_n})$.

As a consequence, we can induce a Kummer map

$$\kappa : \varprojlim F_n^* \to H^1_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1))$$

where the transition maps of the projective limit are the norm maps N_{F_{n+1}/F_n}. Moreover, we have

$$H^1_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1)) = \mathbb{Z}_p\kappa(\pi_n) \oplus \kappa(\varprojlim \mathcal{O}^*_{F_n})$$

6.1 Coleman's power series

The aim of this section is to prove Theorem 6.1. Here we follow [8] and [19] instead of Colmez's notes. We start by defining a norm operator on $\mathbb{Z}_p[[T]]$, which is a multiplicative analogue of ψ.

Definition 6.3. $N : \mathbb{Z}_p[[T]] \to \mathbb{Z}_p[[T]]$ is defined by

$$N(f)((1+T)^p - 1) = \prod_{z^p=1} f((1+T)z - 1)$$

Lemma 6.1. ([8], Lemma 2.3.1) If $\varphi(f)(T) \equiv 1 \mod p^k$, then $f(T) \equiv 1 \mod p^k$.

Proof. Write f in the following form

$$f(T) - 1 = \left(\sum_{n=0}^{\infty} a_n T^n\right) p^m$$

Where $m \geq 0$ is such that p doesn't divide all the coefficients a_k. Note that it's enough to see that $m \geq k$.

Let r be the smallest integer such that $p \nmid a_r$. Then we have $\varphi(f)(T) - 1 = p^m h(T)$, with $h(T) = \sum_{n=0}^{\infty} a_n \varphi(T)^n$. But we have $\varphi(T) \equiv T^p \mod p$, and so $h(T) \equiv a_r T^{pr} + \dots \mod p$. As $p \nmid a_r$, we have that $p \nmid h(T)$, and so we have $\varphi(f)(T) - 1 \not\equiv 0 \mod p^{m+1}$, and therefore we must have $m \geq k$. □

Now we can prove some properties about the operator N.

Lemma 6.2. i) $N_{F_{n+1}/F_n}(f(\pi_{n+1})) = N(f)(\pi_n)$
ii) If $f \in \mathbb{Z}_p[[T]]^*$, we have $N(f) \equiv f \mod p$.
iii) If $f \in \mathbb{Z}_p[[T]]^*$ and $f \equiv 1 \mod p^k$, then $N(f) \equiv 1 \mod p^{k+1}$
iv) If $f \in \mathbb{Z}_p[[T]]^*$, $k_2 \geq k_1 \geq 0$, then $N^{k_2}(f) \equiv N^{k_1}(f) \mod p^{k_1+1}$

Proof. i) On one side, we have $N(f)(\pi_n) = N(f)((1+\pi_{n+1})^p - 1) = \prod_{z^p=1} f(\epsilon^p z - 1)$. On the other side, $N_{F_{n+1}/F_n}(f(\pi_{n+1})) = \prod_{g \in \mathrm{Gal}(F_{n+1}/F_n)} g(f(\pi_{n+1})) = \prod_{g \in \mathrm{Gal}(F_{n+1}/F_n)} f(g(\pi_{n+1}))$. But the Galois conjugates of π_{n+1} are precisely those $\epsilon^{(n+1)} z - 1$, for $z^p = 1$, and this proves the first equality.

ii) If $z^p = 1$, then $z \equiv 1 \mod p$: Indeed $z \equiv a \mod p$ and so $z^p \equiv a^p \equiv a \mod p$ and so we must have $a = 1$. Therefore, modulo p we have

$$N(f)(T^p) \equiv N(f)((1+T)^p - 1) = \prod_{z^p=1} f((1+T)z - 1) \equiv f(T)^p \equiv f(T^p) \mod p$$

Therefore $N(f)(T) \equiv f(T) \mod p$ as desired.

iii) Suppose that $f \equiv 1 \mod p^k$. Let $\mathfrak{p}_1$ denote the maximal ideal of $\mathcal{O}_{F_1}$. For each z such that $z^p = 1$, we have

$$z(1+T) - 1 \equiv T \mod \mathfrak{p}_1 \mathbb{Z}_p[[T]]$$

And therefore, looking term by term we have

$$f(z(1+T) - 1) \equiv f(T) \mod \mathfrak{p}_1 p^k \mathbb{Z}_p[[T]]$$

But then $(\varphi \circ N(f)) = \prod_{z^p=1} f(z(1+T)-1) \equiv f(T)^p \mod \mathfrak{p}_1 p^k \mathbb{Z}_p[[T]]$. But both polynomials belong to $\mathbb{Z}_p[[T]]$, so its an equality modulo $\mathfrak{p}_1 p^k \cap \mathbb{Z}_p = p^{k+1}$. In conclusion,

$$\varphi(N(f)) \equiv f(T)^p \equiv 1 \mod p^{k+1}$$

But then, using Lemma 6.1, we have that $N(f) \equiv 1 \mod p^{k+1}$.

iv) From a repeated application of (ii), we have that

$$\frac{N^{k_2-k_1}(f)}{f} \equiv 1 \mod p$$

But then, using (iii) k_1 times we get $N^{k_2}(f) \equiv N^{k_1}(f) \mod p^{k_1+1}$.

□

Lemma 6.3. (Weierstrass preparation theorem)([8], Theorem 2.1.3) Every $f \in \mathbb{Z}_p[[T]]$ can be uniquely written in the form $f(T) = p^m u(T) g(T)$, where $u \in \mathbb{Z}_p[[T]]^*$, and $g(T)$ is a distinguished polynomial (i.e. it's monic and its lower coefficients are multiples of p).

Theorem 6.1. *(Coleman's power series) Let $u \in \varprojlim \mathcal{O}_{F_n} - \{0\}$, where the projective limit is built bu the maps N_{F_{n+1}/F_n}. Then, there exists a unique power series $f_u \in \mathbb{Z}_p[[T]]$ such that $f_u(\pi_n) = u_n$, for every n.*

Proof. First we prove uniqueness. Note that every $f \in \mathbb{Z}_p[[T]]$ converges and yields a function on $\mathfrak{m}_{\mathbb{C}_p}$, and $\pi_n \in \mathfrak{m}_{\mathbb{C}_p}$. It follows from Lemma 6.3 that $f \in \mathbb{Z}_p[[T]]$ can only have a finite number of roots in $\mathfrak{m}_{\mathbb{C}_p}$, as units in $\mathbb{Z}_p[[T]]$ can't have roots in $\mathfrak{m}_{\mathbb{C}_p}$. Therefore, if f, g satisfy the conditions of the theorem, $(f-g)(\pi_n) = 0$, so $f-g$ has infinitely many roots, and we must have $f = g$.

Now we prove the existence of f_u. First of all, note that we can reduce to the situation such that $u \in \varprojlim \mathcal{O}_{F_n}^*$, as we can write $u_n = \pi_n^k \alpha u'_n$, with $\alpha \in \mu_{p-1}$, and $u'_n \in 1 + \mathfrak{m}_{F_n}$. Then $N_{F_{n+1}/F_n}(u'_{n+1}) = u'_n$, and so if there exists $f_{u'}$ such that $f_{u'}(\pi_n) = u'_n$, we can let $f_u = T^k \alpha f_{u'}$. So let $u \in \varprojlim \mathcal{O}_{F_n}^*$, and choose an arbitrary f_n such that $f_n(\pi_n) = u_n$. Then $f_n \in \mathbb{Z}_p[[T]]^*$, and let's define $g_n := N^n(f_{2n})$. By Lemma 6.2, $g_n \in \mathbb{Z}_p[[T]]^*$ too. We claim that, if $m \geq n$, then

$$g_m(\pi_n) \equiv u_n \mod p^{m+1}$$

To prove the claim, note that $u_{n-1} = N_{F_n/F_{n-1}}(u_n)$, and so $u_{n-1} = N(f_n)(\pi_{n-1})$, using Lemma 6.2, (i). Repeating this k times, we have $u_{n-k} = N^k(f_n)(\pi_{n-k})$. Not let $k = 2m-n$, and we have, using Lemma 6.2 (iv), and that $2m - n \geq m$,

$$u_n = N^{2m-n} f_{2m}(\pi_{2m-(2m-n)}) \equiv N^m f_{2m}(\pi_n) = g_m(\pi_n) \qquad \mod p^{m+1}$$

Therefore any convergent sub-sequence $\{g'_m\}$ of $\{g_m\}$ satisfies the required property of the theorem. We know that such a sequence exists as $\mathbb{Z}_p[[T]]$ is compact. Therefore let $f_u := \lim_{m\to\infty} g'_m$. □

Finally, we see the relation between Coleman's power series and the p-adic zeta function. For this we need to introduce the logarithmic derivation.

Notation. Given $f \in \mathbb{Z}_p[[T]]$, we denote $\partial f = (1+T)\frac{df}{dT}$.

Theorem 6.2. *For f_u like in Theorem 6.1, we have*

i) $N(f_u) = f_u$

ii) $\psi\left(\frac{\partial f_u}{f_u}\right) = \frac{\partial f_u}{f_u}$.

Proof. i) By (i) in Lemma 6.2, we have that $N(f_u)(\pi_n) = N_{F_{n+1}/F_n}(f_u(\pi_{n+1})) = f_u(\pi_n)$, and therefore $N(f_u) - f_u$ has infinitely many zeros, so we have $N(f_u) = f_u$.

ii) Note that it's enough to see that $\psi(\partial \log f_u) = \partial(\log N(f_u))$, as then it follows

$$\psi\left(\frac{\partial f_u}{f_u}\right) = \psi(\partial \log f_u) = \partial(\log N(f_u)) = \partial(\log f_u) = \frac{\partial f_u}{f_u}$$

Moreover, by injectivity of φ, it's enough to see that $\varphi(\psi(\partial \log f)) = \varphi(\partial \log N(f))$. Recall that we have $p\varphi(\psi(f)) = \sum_{z^p=1} f(z(1+T)^p - 1)$, and $\varphi(N(f)) = \prod_{z^p=1} f(z(1+T)^p - 1)$. We have, on one site,

$$p\varphi(\psi(\partial \log f)) = p\psi\left(\frac{\partial f}{f}\right)((1+T)^p - 1) = \sum_{z^p=1} \frac{\partial f}{f}((1+T)z - 1) =$$

$$= \sum_{z^p=1} \frac{(1+T)zf'((1+T)z-1)}{f((1+T)z-1)} = \partial\left(\log \prod_{z^p=1} f((1+T)z-1)\right) = \partial(\log \varphi(N(f)))$$

On the other hand, noting that $\partial \circ \varphi = p\varphi \circ \partial$, we get

$$\varphi(\partial \log N(f)) = p\varphi\left(\frac{\partial N(f)}{N(f)}\right) = \partial(\log \varphi(N(f)))$$

On conclusion,

$$\varphi(\psi(\partial \log f)) = \frac{1}{p}\partial(\log \varphi(N(f))) = \varphi(\partial \log N(f))$$

And by injectivity of φ the result is proved.

□

Observation 6.4. Let $a \in Z$ such that $a \neq 1$, $(a,p) = 1$. Then, let

$$u_n = \frac{e^{-a\frac{2\pi i}{p^n}} - 1}{e^{-\frac{2\pi i}{p^n}} - 1} \in \mathbb{Q}(\mu_{p^n})$$

We have that $N_{F_{n+1}/F_n}(u_{n+1}) = u_n$ and therefore we have an element $u = \varprojlim \mathcal{O}_{F_n}$. It's clear that

$$f_u = \frac{(1+T)^{-a} - 1}{(1+T)^{-1} - 1}$$

And therefore

$$\frac{\partial f_u}{f_u} = \frac{a}{(1+T)^a - 1} - \frac{1}{T} = A_{\lambda_a}(T)$$

Therefore $u \mapsto \frac{\partial f_u}{f_u}$ produces the Kubota-Leopoldt zeta function from the system of cyclotomic units (u_n).

6.2 Explicit reciprocity law

Theorem 6.3. *(Explicit reciprocity law for $Z_p(1)$) The following diagram is commutative*

$$\begin{array}{ccc} \varprojlim \mathcal{O}_{F_n} \setminus \{0\} & \xrightarrow{\qquad\kappa\qquad} & H^1_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \\ & {\scriptstyle u \mapsto \frac{\partial f_u}{f_u}} \searrow \quad \swarrow {\scriptstyle Exp^*} & \\ & D(\mathbb{Z}_p(1))^{\psi=1} & \end{array}$$

Observation 6.5. This explicit reciprocity law relates a system of compatible cohomology classes with the p-adic zeta function, using elements from the theory of (φ, Γ)-modules: Exp^* produces the Amice transform of the measure λ_a from the system of cyclotomic units

$$u_n = \frac{e^{-a\frac{2\pi i}{p^n}} - 1}{e^{-\frac{2\pi i}{p^n}} - 1} \in \mathbb{Q}(\mu_{p^n})$$

This is the simplest instance of a very general (conjectural) phenomena, which relates an Euler system attached to a Galois representation (in this case, $V = \mathbb{Q}_p(1)$) with the p-adic L-function. We will treat this conjectural phenomena with some more detail in the following chapter.

Let's begin with the proof of the Explicit reciprocity law. We need some lemmas first.

Notation. Let $u \in \varprojlim(\mathcal{O}_{F_n} - \{0\})$. We denote by $g \mapsto C_n(g)$ the cocycle of G_{F_n} given by Kummer theory:

$$\varprojlim(\mathcal{O}_{F_n} - \{0\}) \underset{\kappa}{\to} H^1_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \to H^1(G_{F_n}, \mathbb{Z}_p(1))$$

On the other side, let $y \in D(\mathbb{Z}_p(1)) = A^{\psi=1}_{\mathbb{Q}_p}(1)$, and denote $g \mapsto C'_n(g)$ the image of y under the map

$$D(\mathbb{Z}_p(1)) = A^{\psi=1}_{\mathbb{Q}_p}(1) \xrightarrow[(Exp^*)^{-1}]{} H^1_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1)) \to H^1(G_{F_n}, \mathbb{Z}_p(1))$$

Observation 6.6. It will be enough to prove that if $C_n(g) = C'_n(g)$ for every g and n, then $y = \frac{\partial f_u}{f_u}(\pi)$.

Lemma 6.4. Given $u \in \varprojlim(\mathcal{O}_{F_n} - \{0\})$ and $y \in A^{\psi=1}_{\mathbb{Q}_p}(1)$

i) $\exists k \in \mathbb{Z}$ and $b'_n \in \mathcal{O}_{\mathbb{C}_p}/p^n$ such that

$$p^2 C'_n(g) = \frac{p^2 \log \chi(\gamma_n)}{p^n} \cdot \frac{g-1}{\gamma_n - 1} y(\pi_{n+k}) + (g-1) b'_n \in \mathcal{O}_{\mathbb{C}_p}/p^n$$

ii) $\exists b_n'' \in \mathcal{O}_{\mathbb{C}_p}/p^n$ such that

$$p^2 C_n(g) = \frac{p^2 \log \chi(g)}{p^n} \cdot \frac{\partial f_u}{f_u}(\pi_n) + (g-1)b_n'' \in \mathcal{O}_{\mathbb{C}_p}/p^n$$

Proof. i) From the definition of Exp^*, we have that

$$(Exp^*)^{-1} : y \mapsto C_n'(g) = \frac{\log \chi(\gamma_n)}{p^n} \cdot \frac{g-1}{\gamma_n - 1} y - (g-1)b_n$$

Now we observe that

- In $\tilde{A}^+$, φ is invertible, and so we can define $\tilde{\pi_n} := \varphi^{-n}(\pi) = [\epsilon^{1/p^n}] - 1$
- $C_n'(g) \in \mathbb{Z}_p$, so φ is the identity on $C_n'(g)$ and so we have

$$\varphi^{-(n+k)} C_n'(g) = C_n'(g)$$

- Let $b_n = \sum_{l \geq 0} p^l [z_l]$. By the multiplicativity of the valuation v_E,

$$v_E(\varphi^{-k}(z_l)) = \frac{1}{p^k} v_E(z_l)$$

And so $\exists k$ such that $v_E(\varphi^{(-n+k)}(z_l)) \geq -1$.

Now choose $[\tilde{p}] \in \tilde{A}^+$, with $\tilde{p} \in \tilde{E}^+$, $\tilde{p} = (p, \dots)$. Then we have that, choosing k adequately as above, $\tilde{p}\varphi^{-(n+k)}(z_l) \in \tilde{E}^+$. Then, applying $\varphi^{-(n+k)}$ to the expression of $C_n'(g)$ (and using that φ commutes with the action of the Galois group), we get

$$C_n'(g) = \frac{\log \chi(\gamma_n)}{p^n} \cdot \frac{g-1}{\gamma_n - 1} y(\tilde{\pi}_{n+k}) - (g-1)\varphi^{-(n+k)}(b_n)$$

Now we just have to multiply by $[\tilde{p}]^2$, reduce $\mod p^n$ and apply $\theta : \tilde{A}^+/p^n \to \mathcal{O}_{\mathbb{C}_p}/p^n$, sending $[\tilde{p}] \mapsto p$. We get

$$p^2 C_n'(g) = \frac{p^2 \log \chi(\gamma_n)}{p^n} \cdot \frac{g-1}{\gamma_n - 1} y(\pi_{n+k}) + (g-1)b_n' \in \mathcal{O}_{\mathbb{C}_p}/p^n$$

where we have set $b_n' = \theta([\tilde{p}]^2 \varphi^{-(n+k)}(b_n))$.

ii) Note that any $u \in \varprojlim(\mathcal{O}_{F_n} - \{0\})$ can be written as $(u_n) = (\pi_n^k)(v_n)$, with $v_n \in \mathcal{O}_{F_n}^*$. Moreover, we have that $\kappa(u_1 u_2) = \kappa(u_1) + \kappa(u_2)$ by definition of the Kummer map, and $\frac{\partial f_{u_1 u_2}}{f_{u_1 u_2}} = \frac{\partial f_{u_1}}{f_{u_1}} + \frac{\partial f_{u_2}}{f_{u_2}}$. Therefore, we can reduce to prove the result for π and v. In particular, it's enough to prove the formula for u such that $v_p(u_n) \leq 1$.

Now we define the following morphism

$$H : 1 + (\ker \theta) B_{dR}^+ \to \mathbb{C}_p, \qquad x \mapsto \theta\left(\frac{x-1}{\pi}\right)$$

Note that, given two elements of $1+(\ker\theta)B_{dR}^+$, $x=1+x'$ and $y=1+y'$, we have

$$H(xy)=H(1+\pi(x'+y')+\pi^2x'y')=H(x)+H(y)$$

Now let $\tilde{u_n}:=[(u_n,u_n^{1/p},\dots)]$. Then we have $\frac{g(\tilde{u_n})}{\tilde{u_n}}=[\epsilon]^{C_n(g)}=\sum_{m=0}^{\infty}\binom{C_n(g)}{m}([\epsilon]-1)^m=1+C_n(g)\pi+\dots$. Therefore

$$C_n(g)=H\left(\frac{g(\tilde{u_n})}{\tilde{u_n}}\right) \tag{19}$$

Then, we have

$$\frac{g(f_u(\tilde{\pi_n}))}{f_u(\tilde{\pi_n})}=\frac{(f_u((1+\tilde{\pi_n})^{\chi(g)}-1)}{f_u(\tilde{\pi_n})}=\frac{(f_u((1+\pi)^{\frac{\chi(g)-1}{p^n}}(1+\tilde{\pi_n}))}{f_u(\tilde{\pi_n})}$$

Taking the Taylor expansion of the numerator at point $\tilde{\pi_n}$, we get that $\frac{g(f_u(\tilde{\pi_n}))}{f_u(\tilde{\pi_n})}=1+\frac{\partial f_u}{f_u}(\tilde{\pi_n})\frac{\chi(g)-1}{p^n}+\dots$. Therefore, using that $\theta(\tilde{\pi_n})=\pi_n$ by Proposition 5.3, we have

$$H\left(\frac{g(f_u(\tilde{\pi_n}))}{f_u(\tilde{\pi_n})}\right)=\frac{\chi(g)-1}{p^n}\frac{\partial f_u}{f_u}(\pi_n) \tag{20}$$

Again by Proposition 5.3, $\theta(\tilde{u_n})=u_n$. Then,

$$\theta(f_u(\tilde{\pi_n}))=f_u(\theta(\tilde{\pi_n}))=f_u(\pi_n)=u_n=\theta(\tilde{u_n})$$

So we have that $\theta(\frac{f_u(\tilde{\pi_n})}{\tilde{u_n}})=1$. Let's define $a_n:=\frac{f_u(\tilde{\pi_n})}{\tilde{u_n}}$. In particular we have $a_n\in 1+(\ker\theta)B_{dR}^+$.

Putting everything together, we have that

$$C_n(g)=H\left(\frac{g(\tilde{u_n})}{\tilde{u_n}}\right)=H\left(\frac{g(f_u(\tilde{\pi_n}))}{f_u(\tilde{\pi_n})}\right)-H\left(\frac{g(a_n)}{a_n}\right)=\frac{\chi(g)-1}{p^n}\frac{\partial f_u}{f_u}(\pi_n)-(\chi(g)-1)H(a_n) \tag{21}$$

Where we have used Equation (19) in the first equality, the definition of a_n in the second one, and in the last one, Equation (20) and the property of $H(xy)=H(x)+H(y)$.

Now note that

$$H(a_n)=\theta\left(\frac{[\tilde{p}]a_n-[\tilde{p}]}{[\tilde{p}]\pi}\right)=\theta\left(\frac{[\tilde{p}]a_n-[\tilde{p}]}{\pi/\tilde{\pi_1}}\right)\theta\left(\frac{1}{[\tilde{p}]\tilde{\pi_1}}\right)$$

But $\pi/\tilde{\pi_1}$ is a generator of $\ker\theta$ as $\theta(\pi/\tilde{\pi_1})=0$ and it has valuation $v_E(\pi/\tilde{\pi_1})=\left(1-\frac{1}{p}\right)v_E(\epsilon-1)=1$. Then $\theta\left(\frac{[\tilde{p}]a_n-[\tilde{p}]}{\pi/\tilde{\pi_1}}\right)\in\mathcal{O}_{\mathbb{C}_p}$. Therefore $H(a_n)\in\frac{1}{p\pi_1}\mathcal{O}_{\mathbb{C}_p}$. In particular, $p^2H(a_n)\in\mathcal{O}_{\mathbb{C}_p}$. Therefore, multiplying Equation (21) by p^2 we get the following equality in $\mathcal{O}_{\mathbb{C}_p}$

$$p^2 C_n(g) = p^2 \frac{\chi(g)-1}{p^n} \frac{\partial f_u}{f_u}(\pi_n) - (\chi(g)-1)p^2 H(a_n)$$

Now we just have to note that $\chi(g) \equiv 1 \mod p^n$, so we have that

$$\frac{\chi(g)-1}{p^n} \equiv \frac{\exp(\log \chi(g))-1}{p^n} \equiv \frac{\log \chi(g)}{p^n} \mod p^n$$

And denoting $b_n'' = -p^2 H(a_n)$ we have the desired result.

□

Now we need to introduce the notion of normalized trace maps.

Definition 6.4. *Tate's normalized trace maps* are the maps $R_n : F_\infty \to F_n$ are defined by $p^{-k} Tr_{F_{n+k}/F_n} x$, for any k such that $x \in F_{n+k}$.

These maps are well defined: Indeed, let m be the minimum natural number such that $x \in F_{n+m}$. Then, for every $k \geq m$ we have

$$p^{-k} Tr_{F_{n+k}/F_n} x = p^{-k} Tr_{F_{n+m}/F_n} Tr_{F_{n+k}/F_{n+m}} x = p^{-k} Tr_{F_{n+m}/F_n} p^{k-m} x = p^{-m} Tr_{F_{n+m}/F_n} x$$

In conclusion, $p^{-k} Tr_{F_{n+k}/F_n} x$ doesn't depend on the k chosen, so the trace maps are well defined.

Definition 6.5. Let's denote $Y_i = \{x \in F_i \text{ such that } Tr_{F_i/F_{i-1}} x = 0\}$. We also define

$$R_{n+i}^*(x) = R_{n+i}(x) - R_{n+i-1}(x) \in Y_{n+i}$$

Observation 6.7. Given $x \in F_\infty$, we can write

$$x = R_n(x) + \sum_{i=0}^{\infty} R_{n+i}^*(x)$$

Lemma 6.5. $v_p(x) \geq 0$ if and only if $v_p(R_n(x)) \geq 0$ and $v_p(R_{n+i}^*(x)) \geq 0$.

Proof. The inverse implication is an immediate consequence of the observation below. On the other hand, given $x \in \mathcal{O}_{n+k}$, we can write, for some $a_j \in \mathcal{O}_{F_n}$

$$x = \sum_{j=0}^{p^k-1} a_j (1+\pi_{n+k})^k$$

Calculating the trace with the irreducible polynomial of $(1+\pi_{n+k})^j$, it's immediate that

$$R_m((1+\pi_{n+k})^j) = \begin{cases} (1+\pi_{n+k})^j & \text{if } (1+\pi_{n+k})^j \in F_m \\ 0 & \text{otherwise} \end{cases}$$

Therefore, $R_n(x) = a_0$ and $R^*_{n+i}(x) = \sum_{j=0}^{p^k-1} a_j R_{n+i}((1+\pi_{n+k})^j) - R_{n+i-i}((1+\pi_{n+k})^j)$. Each summand only survives if $(1+\pi_{n+k})^j \in F_{n+i}$ but $(1+\pi_{n+k})^j \notin F_{n+i-1}$. Then, only the terms of index $j = p^{k-i}j'$, with $(p, j') = 1$ survive, and so

$$R^*_{n+i}(x) = \sum_{(j',p)=1} a_{p^{n-i}j'}(1+\pi_{n+i})^{j'}$$

Then, $v_p(R_n(x)) \geq v_p(x)$ and $v_p(R^*_{n+i}(x)) \geq v_p(x)$ (we are taking the minimum of the valuations of a subset of the summands of x) and the result holds. □

Lemma 6.6. Let $j \leq i-1$. Let $u \in \mathbb{Z}_p^*$ and let's denote by γ_j a generator of Γ_j. Then, if $v_p(u-1) > v_p(\pi_1)$ then $u\gamma_j - 1$ is invertible on Y_i, and moreover, given $x \in Y_i$, $v_p((u\gamma_j-1)^{-1}x) \geq v_p(x) - v_p(\pi_1)$.

Proof. Choosing the γ_j adequately, we can assume that $\gamma_{i-1} = \gamma_j^{p^{i-j-1}}$. Then, we have that

$$(u\gamma_j - 1)^{-1} = (u^{p^{i-j-1}}\gamma_{i-1} - 1)^{-1}(1 + (u\gamma_j) + \cdots + (u\gamma_j)^{p^{i-j-1}-1})$$

Therefore, to prove the invertibility of $(u\gamma_j - 1)$ it's enough to prove that of $(u^{p^{i-j-1}}\gamma_{i-1} - 1)$. Therefore we can reduce to the case $j = i-1$. As $\{\epsilon^{(i)}{}^a\}_{a=1,\ldots,p-1}$ is a basis of F_i over F_{i-1}, we have that every $x \in \mathcal{O}_{F_i} \cap Y_i$ can be written (for certain $x_a \in \mathcal{O}_{F_{i-1}}$) as

$$x = \sum_{a=1}^{p-1} x_a(1+\pi_i)^a$$

Now let $\chi(\gamma_{i-1}) = 1 + p^{i-1}v$, with $v \in \mathbb{Z}_p^*$. Just by immediate calculation we have

$$(u\gamma_{i-1} - 1)x = \sum_{a=1}^{p-1} ux_a(1+\pi_i)^{a(1+p^{i-1}v)} - x_a(1+\pi_i)^a = \sum_{a=1}^{p-1} x_a(1+\pi_i)^a(u(1+\pi_1)^{av} - 1)$$

Then it is immediate that $(u\gamma_{i-1} - 1)$ has an inverse, which we can write explicitly as

$$(u\gamma_{i-1} - 1)^{-1}x = \sum_{a=1}^{p-1} \frac{x_a}{(u(1+\pi_1)^{av} - 1)}(1+\pi_i)^a$$

Then, developing $(u(1+\pi_1)^{av} - 1)$ in power series, we get $(u(1+\pi_1)^{av} - 1) = (u-1) + u\pi_1 + \ldots$. Then as $v_p(u-1) \geq v_p(\pi_1)$ we have that $v_p(u(1+\pi_1)^{av} - 1) = v_p(u\pi_1) = v_p(\pi_1)$. Therefore on each summand

$$v_p\left(\frac{x_a}{(u(1+\pi_1)^{av} - 1)}(1+\pi_i)^a\right) \geq v_p(x_a(1+\pi_i)^a) - v_p(u(1+\pi_1)^{av} - 1) \geq v_p(x_a(1+\pi_i)^a) - v_p(\pi_1)$$

As this holds on every summand, taking minimums on each side we get

$$v_p((u\gamma_{i-1} - 1)^{-1}x) \geq v_p(x) - v_p(\pi_1)$$

□

Lemma 6.7. (Ax's theorem) There exists a constant $C \in \mathbb{N}$ such that, given $x \in \mathbb{C}_p$, $H \subset G_{\mathbb{Q}_p}$ a closed subgroup, if for every $g \in H$ we have $v_p((g-1)x) \geq a$ for some a, then there exists $y \in \mathbb{C}_p^H$ such that $v_p(x-y) \geq a - C$.

Proof. This is a well known result from Ax, which he uses in the proof of Ax-Sen-Tate's theorem. One can find the proof in [4], Proposition 2. The statement in Ax's paper is the same, if one takes into account that $\Delta(x)$ is defined as $\{\min_{g\in H} v_p(gx-x)\}$, and so the condition $v_p((g-1)x) \geq a$, $\forall g \in H$ is equivalent to $a \leq \Delta(x)$. □

Lemma 6.8. There exists a constant $C \in \mathbb{N}$ such that for all n, k, if $x \in \mathcal{O}_{F_\infty}$ and $b \in \mathcal{O}_{\mathbb{C}_p}$ are such that

$$v_p\left(\frac{g-1}{\gamma_n - 1}x - (g-1)b\right) \geq n \qquad \forall g \in G_{F_n}$$

Then,

$$R_n(x) \in p^{n-C}\mathcal{O}_{F_n}$$

Proof. We will show that the result holds even for $x \in \mathcal{O}_{\hat{F_\infty}}$. For every $g \in \ker\chi := H_{\mathbb{Q}_p}$, we get by hypothesis that

$$v_p((g-1)b) \geq n$$

Then by Lemma 6.7 there exists a $b' \in \hat{F_\infty}$ such that $v_p(b-b') \geq n - C$.
On the other hand, if we take $g = \gamma_n$ by hypothesis we have

$$v_p\left(\frac{\gamma_n - 1}{\gamma_n - 1}x - (\gamma_n - 1)b\right) = v_p(x - (\gamma_n - 1)b) \geq n$$

Therefore,

$$v_p(x-(\gamma_n-1)b') = v_p(x-(\gamma_n-1)b+(\gamma_n-1)(b-b')) \geq \min\{v_p(x-(\gamma_n-1)b), v_p((\gamma_n-1)(b-b'))\}$$

But above we've seen that $v_p(x-(\gamma_n-1)b) \geq n$ and by Lemma 6.6, $v_p((\gamma_n-1)(b-b')) \geq v_p(b-b') + v_p(\pi_1) \geq n - C$, and so we have that

$$v_p(x-(\gamma_n-1)b') \geq n - C$$

As the Galois action commutes with the trace operators, $R_n\gamma_n = \gamma_n R_n = R_n$ and we have that

$$R_n(x) = R_n(x-(\gamma_n-1)b')$$

Taking valuations, and recalling that by Lemma 6.5 we have that $v_p(R_n(x)) \geq v_p(x)$,

$$v_p(R_n(x)) = v_p(R_n(x-(\gamma_n-1)b')) \geq v_p(x-(\gamma_n-1)b') \geq n - C$$

□

Proof. (of the Explicit Reciprocity Law) Following the idea of the proof already outlined before (Observation 6.6), take $y \in D(\mathbb{Z}_p(1))^{\psi=1}$. So by hypothesis we have that $y = \psi(y)$. Then, as we've seen in the proof of Lemma 6.5, we have that

$$R_n(y(\pi_{n+k})) = y(\pi_n) \tag{22}$$

Moreover we already know from Theorem 6.2 that

$$\psi\left(\frac{\partial f_u}{f_u}\right) = \frac{\partial f_u}{f_u}$$

Now we let

$$x := p^2 \frac{\log \chi(\gamma_n)}{p^n}(y(\pi_{n+k}) - \frac{\partial f_u}{f_u}(\pi_n))$$

and $b := b'_n - b''_n$. By the equations above we know that

$$R_n(x) = p^2 \frac{\log \chi(\gamma_n)}{p^n}(y(\pi_n) - \frac{\partial f_u}{f_u}(\pi_n))$$

Then, using that for every $x \in F_n$, $\frac{g-1}{\gamma_n - 1}x = \frac{\log \chi(g)}{\log \chi(\gamma_n)}x \mod p^n$, we have by Lemma 6.4:

$$\frac{g-1}{\gamma_n - 1}(x) + (g-1)b = p^2(C'_n(g) - C_n(g)) = 0 \in \mathcal{O}_{\mathbb{C}_p}/p^n$$

That is,

$$v_p\left(\frac{g-1}{\gamma_n - 1}(x) + (g-1)b\right) \geq n$$

Therefore, using Lemma 6.8, we get that

$$R_n(x) = p^2 \frac{\log \chi(\gamma_n)}{p^n}\left(y(\pi_n) - \frac{\partial f_u}{f_u}(\pi_n)\right) \in p^{n-c}\mathcal{O}_{F_n}$$

Therefore, for every n, we have that

$$\frac{\log \chi(\gamma_n)}{p^n}\left(y(\pi_n) - \frac{\partial f_u}{f_u}(\pi_n)\right) \in p^{n-c-2}\mathcal{O}_{F_n}$$

Finally, let $h = y - \frac{\partial f_u}{f_u}$. Using Equation (22) and the fact that $R_n(\mathcal{O}_{F_{n+k}}) \subseteq \mathcal{O}_{F_n}$, we have that, for every $n \geq i$,

$$h(\pi_i) = R_i(h(\pi_n)) \in p^{n-c-2}\mathcal{O}_{F_i}$$

As this holds for every n, we have that $h(\pi_i) = 0$ for every i and so $h = 0$, as it can't have infinite roots. This completes the proof. □

7 p-adic L-functions and Euler systems: The big picture

Through this thesis we have studied the construction of the Kubota-Leopoldt zeta function and of L-functions attached to modular forms, via p-adic interpolation. In the first case we've also given an alternative arithmetic construction, using the Euler system of cyclotomic units, and we have proven an explicit reciprocity law for this situation. This final chapter picks up the thread of the exposition in the introduction, and pretends to contextualize which role do the constructions we've explained play in a big conjectural picture. This chapter is more a summary and intends to give a general view, so many details and proofs are skipped. We mainly follow the exposition about Euler systems in [17], and we also use some interesting points of view in the introduction of [19] and [24].

7.1 Galois representations and the Bloch-Kato conjecture

Let K be a number field, and (ρ, V) be a p-adic Galois representation of $\mathrm{Gal}(\overline{K}/K)$. We are interested in a particular kind of representations, those *coming from geometry*.

Definition 7.1. We say that the representation (ρ, V) *comes from geometry* if it is a quotient of a subspace of $H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Q}_p)(j) := \varprojlim_n H^i_{\acute{e}t}(X_{\overline{K}}, \mathbb{Z}/p^n\mathbb{Z}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p(j)$, for some smooth algebraic variety X/K and i, j integers.

Example 7.1. Given E an elliptic curve defined over K, the representation $V_p(E) = \varprojlim E[n] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = H^1_{\acute{e}t}(E_{\overline{K}}, \mathbb{Q}_p)$, and so it's a representation coming from geometry.

In particular, representations coming from geometry are unramified except at p and primes of bad reduction of X.

Now let's define the L-function attached to a representation. Let $\mathfrak{p} \mid p$ be a prime of $\mathcal{O}_{\overline{K}}$. We have an exact sequence

$$1 \to I_{\mathfrak{p}} \to G_{\mathbb{Q},\mathfrak{p}} \to G_{\mathbb{F}_p} \to 1$$

Therefore, if (V, ρ) is *unramified* at p (i.e. the representation is trivial on the inertia subgroup of $\mathfrak{p}$, $\rho(I_{\mathfrak{p}}) = 1$, for every $\mathfrak{p} \mid p$) the lift $\rho(Frob_p)$ is well defined. In particular, the following definition makes sense:

Definition 7.2. Let v be an unramified prime in K. The *local Euler factor at v* is

$$P_v(V, T) = \det(1 - T\rho(Frob_v^{-1})) \in \mathbb{Q}_p[T]$$

There's also a more complicated way of defining the local factor at v for bad primes, which we won't discuss.

Definition 7.3. The L-function attached to the representation (V, ρ) is defined as

$$L(V, s) = \prod_{v \text{ prime in } \mathcal{O}_K} P_v(V, |\mathcal{O}_K/v|^{-s})$$

Example 7.2. For the representation $\mathbb{Q}_p(n)$, we get $P_v(\mathbb{Q}_p(1), T) = 1 - \frac{T}{l^n}$ and so

$$L(V, s) = \prod_{l \text{ prime}} \frac{1}{1 - l^{-s-n}} = \zeta(s + n)$$

We want to study the Galois cohomology of the representation. It's usually useful to impose some local conditions on the cohomology groups, which leads to the definition of *Selmer groups*. Observe that if v is a prime of K, we have a natural inclusion $G_{K_v} \hookrightarrow G_K$. This induces morphisms in cohomology

$$H^i(G_K, V) \to H^i(G_{K_v}, V)$$

Definition 7.4. A *local condition* on V at a prime v is a submodule $\mathcal{F}_v \subseteq H^1(G_{K_v}, V)$.

The most used examples of local conditions are $\mathcal{F}_{v,\text{ strict}} = 0$, $\mathcal{F}_{v,\text{ relaxed}} = H^1(G_{K_v}, V)$, $\mathcal{F}_{v,\text{ ur}} = \text{Im}(H^1(G_{K_v}/I_v, V^{I_v}) \to H^1(G_{K_v}, V))$ and $\mathcal{F}_{v,\text{BK}}$, which is defined in terms of a condition from p-adic Hodge theory.

Definition 7.5. A *Selmer structure* is a collection $\mathcal{F} = (\mathcal{F}_v)_{v \text{ prime of K}}$ satisfying that for almost all v, we have $\mathcal{F}_v = \mathcal{F}_{v,\text{ ur}}$. Given a Selmer structure we define a *Selmer group*

$$Sel_{\mathcal{F}}(K, V) = \{x \in H^1(G_K, V) | loc_v(x) \in \mathcal{F}_v, \forall v\}$$

Equivalently, we can write it as

$$Sel_{\mathcal{F}}(K, V) = \ker\left(H^1(G_K, V) \to \prod_v H^1(G_{K_v}, V)/\mathcal{F}_v\right)$$

We're mostly interested in 3 different Selmer groups: Sel_{strict}, Sel_{BK} and $Sel_{relaxed}$ which correspond to the choice of local conditions $\mathcal{F}_v = \mathcal{F}_{v,\text{ ur}}$ for all primes $v \nmid p$ and for primes $v \mid p$, $\mathcal{F}_v = \mathcal{F}_{v,\text{ strict}}, \mathcal{F}_{v,\text{ BK}}, \mathcal{F}_{v,\text{ relaxed}}$, respectively.

There is a conjectural relation between the dimension of Block-Kato Selmer groups and the order of a certain L-function: This is the Bloch-Kato conjecture, which can be seen as a generalization of the BSD conjecture for an arbitrary Galois representation. Note that, as stated in the introduction, it relates an analytic object (L-functions) with an algebraic one (Selmer groups).

Conjecture 7.1. *(Bloch-Kato) Let V be a representation coming from geometry. Then,*

$$\dim Sel_{BK}(K, V) - \dim H^0(K, V) = ord_{s=0} L(V^*(1), s)$$

Where V^* denotes the dual representation.

Observation 7.1. This very general definition of Selmer groups is modelled out of the case of Selmer groups of an elliptic curve E. Indeed, for this case we have an exact sequence

$$0 \to E[m] \to E \underset{m}{\to} E \to 0$$

And so this gives a long exact sequence in cohomology

$$0 \to E(K)[m] \to E(K) \underset{m}{\to} E(K) \to H^1(G_K, E[m]) \to H^1(G_K, E) \underset{m}{\to} H^1(G_K, E) \to ...$$

This can be rewritten to obtain the *Kummer sequence* for an elliptic curve

$$0 \to E(K)/mE(K) \to H^1(G_K, E[m]) \to H^1(G_K, E)[m] \to 0$$

Then, using the restriction maps on cohomology, we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(G_K, E[m]) & \longrightarrow & H^1(G_K, E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/mE(K_v) & \longrightarrow & \prod_v H^1(G_{Kv}, E[m]) & \longrightarrow & \prod_v H^1(G_{Kv}, E)[m] & \longrightarrow & 0 \end{array}$$

And one defines

$$Sel^{(m)}(E/K) = \ker\left(H^1(G_K, E[m]) \to \prod_v H^1(G_{K_v}, E)[m]\right)$$

It can be seen that $H^1(G_{Kv}, E)[m] = H^1(G_{K_v}, E[m])/\mathrm{Im}\kappa_v$, where κ_v is the local Kummer map $\kappa_v : E(K_v)/mE(K_v) \to H^1(G_{K_v}, E[m])$. Therefore the elements in the Selmer group can be seen as those that come from K_v-rational points via the Kummer map.

If $V_p(E) := \varprojlim_m E[p^m] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ denotes the Galois representation attached to the Tate module of the ellpitic curve, we have $\mathcal{F}_{v,BK} = H^1(G_K, V_p(E))$, for $v \nmid p$, as $H^1(G_{K_v}, V_p(E)) = 0$.

On the other side, there is an isomorphism $E(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong Sel_{BK}(K, V)$, and so for $v \mid p$, we have that being in the image of $E(K_v)$ via the Kummer map is the same as being in $\mathcal{F}_{v,BK}$. In conclusion, $Sel_p(E/K) := \varprojlim Sel^{(p^n)}(E/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong Sel_{BK}(K, V_p(E))$, and so the Block-Kato Selmer groups are a generalization of the classical Selmer groups of an elliptic curve. See [5] for a detailed explanation and proof about this relation between $Sel_{BK}(K, V_p(E))$ and $Sel_p(E/K)$.

In addition, the Selmer groups yield an exact sequence

$$0 \to E(K)/mE(K) \to Sel^{(m)}(E) \to Ш_E[m] \to 0$$

If the Tate-Shafarevich groups $Ш_E[p^\infty]$ are finite (as it is conjectured), then we have

$$\dim_{\mathbb{Q}_p} \varprojlim Sel^{(p^n)}(E/K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathrm{rank}(E(K))$$

Moreover, $H^0(\mathbb{Q}_p, V_p(E)) = 0$ and $ord_{s=0}L(V^*(1), s) = ord_{s=1}L(E/K, s)$, so the Bloch-Kato conjecture is equivalent to the Birch and Swinnerton-Dyer conjecture if the Tate-Shafarevich groups are finite. Otherwise, the Bloch-Kato conjecture just predicts the inequality

$$\mathrm{rank}(E/K) \leq ord_{s=1}L(E/K, s)$$

This inequality can be proven (at least in some cases) using Euler Systems, which allow to control the size of Selmer groups.

7.2 Euler Systems

Euler systems are a tool for studying and controlling the size of Selmer groups. Let V be a p-adic Galois representation of $G_{\mathbb{Q}}$, $T \subset V$ a $\mathbb{Z}_p$ lattice stable by $G_{\mathbb{Q}}$ and Σ be a finite set of primes containing p and the ramified primes for V. For any number field K, we can regard V as a G_K representation, and this induces corestriction maps on cohomology

$$cor_K^L H^i(L, V) \to H^i(K, V) \quad \forall L \supseteq K$$

Definition 7.6. An *Euler System* for (T, Σ) is a collection $c = (c_m)_{m \geq 1}$, with $c_m \in H^1(\mathbb{Q}(\mu_m), T)$, satisfying that

$$cor_{\mathbb{Q}(\mu_m)}^{\mathbb{Q}(\mu_{ml})}(c_{ml}) = \begin{cases} c_m & \text{if } l \in \Sigma \text{ or } l \mid m \\ P_l(V^*(1), Frob_l^{-1})c_m & \text{otherwise} \end{cases}$$

The main reason why we should care about Euler Systems, is, as already said, that they allow to control the size of Selmer groups. In particular, we have the following result:

Theorem 7.1. *Suppose that c is an Euler system for (T, Σ) with $c_1 \neq 0$. If V satisfies some additional technical conditions,*

$$\dim Sel_{rel}(\mathbb{Q}, V) \leq \dim(V^{c=-1})$$

Where c denotes complex conjugation.

This result controls the size of Sel_{rel}, and so it also allows to control Sel_{BK}, as we have

$$Sel_{strict}(K, V) \subseteq Sel_{BK}(K, V) \subseteq Sel_{rel}(K, V)$$

This general definition of Euler systems is estrange, but as already discussed in Section 6, we have already encountered an example of Euler system, that of *cyclotomic units*.

Example 7.3. Consider the representation $V = \mathbb{Q}_p(1)$. Recall how we defined in Definition 6.2 a Kummer map $\kappa : F_n^* = \mathbb{Q}_p(\pi_n)^* \to H^1(G_{F_n}, \mathbb{Z}_p(1))$. We can repeat the same argument choosing a system of compatible $m - th$ roots of unity ζ_m for all m (not just powers of p), and define $u_m = \zeta_m - 1$. The same argument shows that there is a well defined Kummer map $\kappa : \mathbb{Q}(u_m)^* \to H^1(G_{\mathbb{Q}(u_m)}, \mathbb{Z}_p(1))$, and it commutes with norms and corestrictions.

Moreover, we have $V^*(1) = \mathbb{Q}_p$ and so $P_l(V^*(1), Frob_l^{-1}) = 1 - Frob_l^{-1}$ (see Example 7.2). It turns out that we have

$$N_{\mathbb{Q}(u_{ml})/\mathbb{Q}(u_m)} u_{ml} = \begin{cases} u_m & \text{if } l \mid m \\ (1 - Frob_l^{-1})u_m & \text{if } l \nmid m \text{ and } m \geq 1 \\ l & \text{if } m = 1 \end{cases}$$

Therefore, the elements $(\kappa(u_m))_m$ would nearly give an Euler system. However, there are some problems. On one side, we're seeing these factors for all primes, and we need to exclude at least the prime $p \in \Sigma$. Moreover, we haven't defined u_1. To solve this, we define

$$v_m = \begin{cases} u_m & \text{if } p \mid m \\ N_{\mathbb{Q}(u_{mp})/\mathbb{Q}(u_m)} u_{mp} & \text{if } p \nmid m \end{cases}$$

Theorem 7.2. *The classes $c_m = \kappa(v_m)$ are an Euler system for $(\mathbb{Z}_p(1), \{p\})$, called the system of cyclotomic units.*

Note that the elements $u_n \in \mathbb{Q}(\mu_{p^n})$ defined in Observation 6.4 (that we packed in $H_{Iw}(\mathbb{Q}_p, \mathbb{Z}_p(1))$) are exactly the v_{p^n} in the Euler system of cyclotomic units. Therefore, what we've proved in Section 6 is that we can **construct the p-adic L-function of Kubota-Leopoldt from the Euler system of cyclotomic units**, using Exp^*.

This is exactly an instance of the picture explained in the introduction: For the representation $V = \mathbb{Q}_p(1)$, we have the following commutative diagram.

$$\begin{array}{ccc} \text{Galois representation} & \longrightarrow & \text{L-function} \\ \downarrow & & \downarrow \text{p-adic interpolation} \\ \text{Euler system} & \xrightarrow{\text{Explicit reciprocity law}} & \text{p-adic L-function} \end{array}$$

This is a general conjectural phenomena: We expect to be able to build an "arithmetic" p-adic L-function from an Euler system:

$$\text{Euler system} \to H^1_{Iw}(\mathbb{Q}, V) \to H^1_{Iw}(\mathbb{Q}_p, V) \xrightarrow[Exp^*]{} D(V)^{\psi=1} \xrightarrow[\text{Amice transform}]{} \text{p-adic L-functions}$$

Moreover, we expect to have an explicit reciprocity law that relates this "arithmetic" p-adic L-function with the "analytic" p-adic L-function constructed via interpolation.

Observation 7.2. Applying the Amice transform to $D(V)^{\psi=1}$ works for the case of $\mathbb{Z}_p(1)$, because ψ improves denominators in π, and so $A_{\mathbb{Q}_p}^{\psi=1} \subseteq \frac{1}{\pi} A_{\mathbb{Q}_p}^{+}$, so we can see the elements of $D(\mathbb{Q}_p(1))^{\psi=1}$ as measures on $\mathbb{Z}_p$. However, this is more complicated in general, and we have to introduce more advanced tools from p-adic Hodge theory in order to be able to see the elements of $D(V)^{\psi=1}$ as measures on $\mathbb{Z}_p$.

Observation 7.3. This general picture is known to work in very few cases. One of them is the one that we have studied in detail, the case $V = \mathbb{Q}_p(1)$. Another one is the case of L-functions attached to modular forms. For this case, we have studied the construction of the p-adic L-function in Section 4. Proving that the rest of the picture can be constructed is much more difficult and falls beyond the scope of this study. It was done by Kato in [15].

7.3 Kato's Euler System

For completeness, this last section summarizes some results that lead to the definition of Kato's Euler system. This is based in the exposition [17]. First we give a short reminder about the definition of modular curves, that we will need for the construction.

Definition 7.7. Let Γ be a congruence subgroup. Then, there exists an algebraic variety $Y(\Gamma)$, defined over $\mathbb{Q}$, such that

$$Y(\Gamma)(\mathbb{C}) \cong \Gamma \backslash \mathcal{H}$$

$Y(\Gamma)$ is called a *modular curve*.

In particular, for the congruence subgroups $\Gamma(N)$ and $\Gamma_1(N)$, we have the modular curves $Y(N)$ and $Y_1(N)$.

$$Y(N)(\mathbb{C}) \cong \Gamma(N)\backslash\mathcal{H} \qquad Y_1(N)(\mathbb{C}) \cong \Gamma_1(N)\backslash\mathcal{H}$$

Moreover, for every $F/\mathbb{Q}$, the F-points of $Y_1(N)$ are in bijection with isomorphism classes of pairs (E, P), where E is an elliptic curve and P is a point of order N in E.

Observe that we have introduced L-functions attached to a modular form, but to fit this into the general picture about Galois representations (in particular, to build an Euler system), we should see that we can attach a Galois representation to a L-function.

Let $f = \sum a_n q^n \in S_k(N)$ be a primitive modular form. Then $\mathbb{Q}(f) = \mathbb{Q}(a_1, a_2, \dots)$ is a finite extension of $\mathbb{Q}$, and $\mathbb{Q}_p(f) = \mathbb{Q}_p(a_1, a_2, \dots)$ is a finite extension of $\mathbb{Q}_p$.

Theorem 7.3. *(Deligne) Given a primitive modular form $f \in S_k(N)$, there exists a $G_{\mathbb{Q}}$-representation $V_p(f)$, of dimension 2 over $\mathbb{Q}_p(f)$, non ramified outside Np, such that if $l \nmid Np$, then*

$$\det(1 - T\rho(Frob_l)^{-1}) = 1 - a_l T + l^{k-1}T^2$$

In particular,

$$L(V_p(f), s) = L(f, s)$$

Moreover, it was proved by Faltings, Tsuji and Saito that $V_p(f)$ is a de Rham representation ([10], Theorem 8.4.8 for the precise statement), and by construction of this representation, it comes from geometry: It is defined as the maximal subspace of $H^1_{\acute{e}t}(Y_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ where the Hecke operators T_l, for $l \nmid N$, act by multiplication by $a_l(f)$.

Now let's proceed to define an Euler system for $V_p(f)$. Kato does this using *Siegel units* on modular curves. Let's introduce this concept.

Definition 7.8. Let Γ be a congruence subgroup. Then, a *modular unit* or level Γ is a nowhere vanishing Γ-invariant holomorphic function $f : \mathcal{H} \to \mathbb{C}$ with poles of finite order at the cusps.

Observation 7.4. There is a bijective correspondence

$$\{\text{Modular units of level } \Gamma\} \longleftrightarrow \mathcal{O}(Y(\Gamma)(\mathbb{C}))^*$$

Where $\mathcal{O}$ denotes the coordinate ring of the algebraic variety. Therefore there are two different ways to look at modular units. In particular, we can talk about the field of definition of the modular unit.

Definition 7.9. Let $(\alpha, \beta) = (a/N, b/N) \neq (0, 0) \in \mathbb{Q}/\mathbb{Z}$. We define the functions $g_{\alpha,\beta} : \mathcal{H} \to \mathbb{C}$ as

$$g_{\alpha,\beta}(\tau) = q^{\omega} \prod_{n \geq 0}(1 - q^{n+a/N}\zeta_N^b) \prod_{n \geq 1}(1 - q^{n-a/N}\zeta_N^{-b})$$

Where N is a primitive N-th root of unity, and $\omega = \frac{1}{12} - \frac{a}{N} + \frac{a^2}{2N^2}$.

With a slight modification, these functions become $\Gamma_1(N)$-invariant, and are modular units.

Definition 7.10. Let $c > 1$ such that c is coprime to the order of $\alpha, \beta \in \mathbb{Q}/\mathbb{Z}$ and coprime to 6. Then, we define

$$ {}_c g_{\alpha,\beta} = \frac{(g_{\alpha,\beta})^{c^2}}{g_{c\alpha,c\beta}} $$

These are called *Siegel units*.

Theorem 7.4. *${}_c g_{0,1/N}$ are modular units of level $\Gamma_1(N)$, and are defined over $\mathbb{Q}$.*

Now, we want to construct an Euler system for $V_p(f)$. In fact, Kato builds an Euler system for $V_p(f)(2)$, but this is enough thanks to the following notion of twisting for Euler systems.

Theorem 7.5. *Let $\chi : G_{\mathbb{Q}} \to \mathbb{Z}_p$ be a continuous character unramified outside Σ (for instance, a power of the cyclotomic character). Then, there is a canonical bijection $c \mapsto c^{\chi}$ between Euler systems for (T, Σ) and Euler systems for $(T(\chi), \Sigma)$.*

To construct the Euler system we need to introduce several maps coming from étale cohomology.

Definition 7.11. Let X be an algebraic variety. Then, we have the following maps

- Kummer map. $\kappa_p : \mathcal{O}(X)^* \to H^1(X, \mathbb{Q}_p(1))$.
- Cup products. $\cup : H^i(X, \mathbb{Q}_p(m)) \times H^j(X, \mathbb{Q}_p(n)) \to H^{i+j}(X, \mathbb{Q}_p(n+m))$

Definition 7.12. Let c, d be integers coprime to $6Np$, where N is the level of the modular form f. We define

$$ u_N(\tau) = {}_c g_{1/N,0}(N\tau) \qquad v_N(\tau) = {}_d g_{0,1/N}(\tau) $$

Both units are of level $\Gamma_1(N)$. $u_N(\tau)$ is defined over $\mathbb{Q}(\mu_N)$ and $v_N(\tau)$ is defined over $\mathbb{Q}$.

Definition 7.13. Given $m, N > 2$ and $m \mid N$, we define

$$ z_{N,m} = \kappa_p(u_m) \cup \kappa_p(v_N) \in H^2_{\acute{e}t}(Y_1(N)_{\mathbb{Q}(\mu_m)}, \mathbb{Z}_p(2)) $$

The units $z_{N,m}$ are those that define Kato's Euler system. The main result is the following norm relation.

Theorem 7.6. *Let l be a prime. If $l \mid m$, then*

$$ norm^{\mathbb{Q}(\mu_{ml})}_{\mathbb{Q}(\mu_m)} z_{N,ml} = z_{N,m} $$

If $l \nmid mN$, then

$$ norm^{\mathbb{Q}(\mu_{ml})}_{\mathbb{Q}(\mu_m)} z_{N,ml} = (1 - \langle l \rangle^{-1} T_l (Frob_l)^{-1} + l \langle l \rangle^{-1} (Frob_l)^{-2}) z_{N,m} $$

Observation 7.5. These elements $(z_{N,m})_{m \geq 1}$ satisfy an appropriate norm relation, but they belong to $H^2_{\acute{e}t}(Y_1(N)_{\mathbb{Q}(\mu_m)}, \mathbb{Z}_p(2))$, and to have an Euler system for $V_p(f)(2)$ we need elements in $H^1(\mathbb{Q}(\mu_m), V_p(f)(2))$. However, it turns out that we have a Hochschild-Serre spectral sequence for étale cohomology, that induces a map

$$ H^2_{\acute{e}t}(Y_{\mathbb{Q}(\mu_m)}, \mathbb{Q}_p(m)) \to H^1(G_{\mathbb{Q}(\mu_m)}, H^1_{\acute{e}t}(Y_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)(m)) \to H^1(\mathbb{Q}(\mu_m), V_p(f)(2)) $$

And so we can translate $(z_{N,m})_{m\geq 1} \in H^1(\mathbb{Q}(\mu_m), V_p(f)(2))$

Moreover, via this map the Hecke operators T_l and $\langle l\rangle$ act as $a_l(f)$ and $\chi(l)$, respectively. Therefore, for the case $l \nmid mN$ the Euler factor becomes

$$norm_{\mathbb{Q}(\mu_m)}^{\mathbb{Q}(\mu_{ml})} z_{N,ml} = (1 - \chi(l)^{-1} a_l(f)(Frob_l)^{-1} + l\chi(l)^{-1}(Frob_l)^{-2}) z_{N,m}$$

Which is the Euler factor for $V_p(f \otimes \chi)$ evaluated at $(Frob_l)^{-1}$. Moreover, if $V = V_p(f)(2)$, $V^*(1) = V_p(f \otimes \chi)$ and so $(z_{N,m})_{m\geq 1}$ satisfy the Euler system relation for $V_p(f)(2)$.

In a same way as we did for the case of cyclotomic units, to remove the Euler factors at p, we replace $z_{N,m}$ by $z_{N,m}^{(p)} = norm_{\mathbb{Q}(\mu_m)}^{\mathbb{Q}(\mu_{mp})}(\zeta_{N,mp})$, and the elements $z_{N,m}^{(p)}$ form an Euler system for $V_p(f)(2)$.

References

[1] Bogdan Alecu. Master's thesis: Special values of rankin-selberg convolution l-functions. Avaliable at: https://warwick.ac.uk/fac/sci/maths/people/staff/david_loeffler/teaching/alecu.pdf.

[2] Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[3] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[4] James Ax. Zeros of polynomials over local fields—The Galois action. *J. Algebra*, 15:417–428, 1970.

[5] Joël Bellaïche. An introduction to the conjecture of bloch and kato. Avaliable at: http://virtualmath1.stanford.edu/~conrad/BSDseminar/refs/BKintro.pdf.

[6] Xavier Caruso. An introduction to p-adic period rings. In *An excursion into p-adic Hodge theory: from foundations to recent trends*, volume 54 of *Panor. Synthèses*, pages 19–92. Soc. Math. France, Paris, 2019.

[7] Frédéric Cherbonnier and Pierre Colmez. Théorie d'Iwasawa des représentations p-adiques d'un corps local. *J. Amer. Math. Soc.*, 12(1):241–268, 1999.

[8] J. Coates and R. Sujatha. *Cyclotomic fields and zeta values*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[9] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[10] Pierre Colmez. Fontaine's rings and p-adic l-functions, 2004. Avaliable at: http://staff.ustc.edu.cn/~yiouyang/colmez.pdf.

[11] Keith Conrad. Infinite series in p-adic fields. Avaliable at: https://kconrad.math.uconn.edu/blurbs/gradnumthy/infseriespadic.pdf.

[12] Henry Darmon. L-functions and modular forms. lecture 36: The p-adic l-function attached to dirichlet characters. Avaliable at: https://www.math.mcgill.ca/~darmon/courses/11-12/nt/notes/lecture36.pdf.

[13] Jean-Marc Fontaine and Yi Ouyang. *Theory of p-adic Galois Representations*. Springer-Verlag, 2021. Livre en préparation, avaliable at: https://www.imo.universite-paris-saclay.fr/~fontaine/galoisrep.pdf.

[14] Laurent Herr. Sur la cohomologie galoisienne des corps p-adiques. *Bull. Soc. Math. France*, 126(4):563–600, 1998.

[15] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. Number 295, pages ix, 117–290. 2004. Cohomologies p-adiques et applications arithmétiques. III.

[16] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[17] David Loeffler. Euler systems (iwasawa 2017 notes). Avaliable at: http://www.math.keio.ac.jp/~bannai/Loeffler.pdf.

[18] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[19] Joaquín Rodrigues Jacinto and Chris Williams. An introduction to p-adic l-functions. Avaliable at: https://warwick.ac.uk/fac/sci/maths/people/staff/cwilliams/lecturenotes/lecturenotes-change.pdf.

[20] J.-P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

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

[22] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[23] Tom Weston. The inflation-restriction sequence: An introduction to spectral sequences. Avaliable at: https://www.math.mcgill.ca/goren/SeminarOnCohomology/infres.pdf.

[24] Chris Williams. An introduction to p-adic l-functions ii: Modular forms. Avaliable at: https://warwick.ac.uk/fac/sci/maths/people/staff/cwilliams/lecturenotes/lecture_notes_part_ii.pdf.