# Topics in Number Theory: $p$-Adic L-functions

Jan Vonk

Draft version May 18, 2021. Please send corrections and suggestions to
j.b.vonk@math.leidenuniv.nl

# Contents

CHAPTER 1

# Some results of Euler and Kummer

In this short motivational chapter, we discuss the historical roots of the remarkable subject of *cyclotomy* (Greek: κύκλος circle, τέμνειν to cut) and the deep connections that exist between special values of zeta functions and class groups of cyclotomic fields. We will focus on the monumental achievements of Euler and Kummer in seemingly very different contexts, the only common characters in the two stories being the Bernoulli numbers, which will feature prominently in the body of this course.

## 1.1. Euler and the Basel problem

Our story begins with the formulation of the famous *Basel problem* by Pietro Mengoli in 1650. It asks to evaluate the infinite sum

$$\zeta(2) := 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots = \sum_{n \geq 1} n^{-2}.$$

This problem eluded mathematicians for nearly a century, until it was solved by a young Leonard Euler in 1734, a feat which brought him instant fame. His solution not only allowed him to evaluate the above sum as $\pi^2/6$, but it also gives a closed form expression for the more general quantities

$$\zeta(2k) := \sum_{n \geq 1} n^{-2k}, \qquad k \geq 1.$$

The proof of Euler was read on 5 December 1735 in The Saint Petersburg Academy of Sciences, and relied on a number identities that could not at the time be fully justified in the absence of the theory of Weierstraß that is known to mathematical audiences today. Euler did produce a proof that was considered fully rigorous by his contemporaries a few years later. In keeping with the tone of his original proof, we shall present a version of his argument where the verification of some claims is left to the (contemporary) reader.

Leonhard Euler

The starting point for Euler was the identity

$$\sin(\pi z) = \pi z \prod_{n\geq 1}\left(1-\frac{z^2}{n^2}\right) \tag{1}$$

By taking the logarithmic derivative, we obtain the following identities

$$\pi z\cot(\pi z) = 1-2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{n^{2k}} \tag{2}$$

$$= 1-2\sum_{k=1}^{\infty}\zeta(2k)z^{2k} \tag{3}$$

On the other hand, the cotangent function appearing above may be written in terms of exponential functions using Euler's formula $e^{i\theta}=\cos(\theta)+i\sin(\theta)$ as

$$\pi z\cot(\pi z) = -\pi i z\frac{e^{\pi iz}+e^{-\pi iz}}{e^{\pi iz}-e^{-\pi iz}} \tag{4}$$

$$= -\pi i z\frac{e^{2\pi iz}+1}{e^{2\pi iz}-1} \tag{5}$$

$$= 1-\sum_{k\geq 1}\frac{(-1)^{k-1}2^{2k}B_{2k}}{(2k)!}\cdot(\pi z)^{2k} \tag{6}$$

where $B_{2k}$ denotes the $2k$-th *Bernoulli number*, defined via the generating series

$$\frac{t}{e^t-1}=\sum_{k=0}^{\infty}B_k\frac{t^k}{k!} \tag{7}$$

It now follows formally from (3) and (6) that

$$\zeta(2k) = \frac{(-1)^{k-1}(2\pi)^{2k}}{2(2k)!}B_{2k}. \tag{8}$$

For future reference, we include a table of the first few Bernoulli numbers. Note that the first entry in this table gives the conclusion that was most coveted in Euler's days, namely that $\zeta(2)=\pi^2/6$.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $B_2$ | $\frac{1}{6}$ | $B_{14}$ | $\frac{7}{6}$ | $B_{26}$ | $\frac{8553103}{6}$ | $B_{38}$ | $\frac{2929993913841559}{6}$ |
| $B_4$ | $-\frac{1}{30}$ | $B_{16}$ | $-\frac{3617}{510}$ | $B_{28}$ | $-\frac{23749461029}{870}$ | $B_{40}$ | $-\frac{26108271849644912 2051}{13530}$ |
| $B_6$ | $\frac{1}{42}$ | $B_{18}$ | $\frac{43867}{798}$ | $B_{30}$ | $\frac{8615841276005}{14322}$ | $B_{42}$ | $\frac{1520097643918070802691}{1806}$ |
| $B_8$ | $-\frac{1}{30}$ | $B_{20}$ | $-\frac{174611}{330}$ | $B_{32}$ | $-\frac{7709321041217}{510}$ | $B_{44}$ | $-\frac{27833269579301024235023}{690}$ |
| $B_{10}$ | $\frac{5}{66}$ | $B_{22}$ | $\frac{854513}{138}$ | $B_{34}$ | $\frac{2577687858367}{6}$ | $B_{46}$ | $\frac{596451111593912163277961}{282}$ |
| $B_{12}$ | $-\frac{691}{2730}$ | $B_{24}$ | $-\frac{236364091}{2730}$ | $B_{36}$ | $-\frac{26315271553053477373}{1919190}$ | $B_{48}$ | $\frac{5609403368997817686249127547}{46410}$ |

The investigations of Euler on the Basel problem, and particularly his evaluation of the quantities $\zeta(2k)$ for $k\geq 1$, later inspired Riemann to introduce his famous function

$$\zeta(s) := \sum_{n\geq 1} n^{-s}, \qquad \mathrm{Re}(s)>1.$$

In his celebrated 1859 paper *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Riemann established its meromorphic continuation to all $s \in \mathbf{C}$, as well as the functional equation

$$\xi(s) = \xi(1-s), \qquad \text{where } \xi(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

This function continues to this day to elude mathematicians, and the end of this story is not yet in sight. We will content ourselves here with the observation that the functional equation implies a particularly satisfactory formulation of Euler's result. Instead of stating his result at *positive even* integers, its equivalent statement at *negative odd* integers becomes

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}.$$

Note in particular that this is a *rational number*. This extraordinary fact is extremely significant, and lies at the basis of our later investigations on $p$-adic L-functions.

## 1.2. Kummer and Fermat's Last Theorem

The second part of this motivational diptych comes from the seemingly unrelated work of Kummer on Fermat's Last Theorem, where the hinge between both panels is made of Bernoulli numbers. We start with the following result of Kummer:

THEOREM 1.1 (Kummer 1847). *Suppose $p > 2$ is a prime that does not divide the class number of the cyclotomic field $\mathbf{Q}(\zeta_p)$. Then there are no solutions in non-zero integers $x, y, z$ to the equation*

$$x^p + y^p = z^p.$$

From your extensive experience in similar situations that arose in the Mastermath course *Algebraic Number Theory*, you will be able to guess the broad strokes of the proof strategy. Particularly, you will be able to guess how the condition on the class number might be used is Kummer's proof. The full argument is quite difficult, and we shall omit it here, referring instead to the excellent treatment in [**Was97**].

Ernst Kummer

The arguments of Kummer have been hugely influential, well beyond their use for Fermat's Last Theorem, and the investigations of Kummer surrounding these results form the cradle of the later established theory of $p$-adic numbers. We highlight two statements that occur in the work of Kummer:

- Since already for moderately sized primes $p$, the computation of the class number of $\mathbf{Q}(\zeta_p)$ poses serious difficulties. Kummer proved a remarkable result that characterises this condition in a much more computationally efficient way. Surprisingly, the criterion uses the Bernoulli numbers that

showed up also in Euler's results on special values of the zeta function! More precisely, Kummer showed that $p > 2$ does not divide the class number of $\mathbf{Q}(\zeta_p)$ if and only if $p$ does not divide the numerator of $B_n$ for any $n = 2, 4, \ldots, p-3$. Such primes are called *regular primes*.

For instance, without computing the class number of $\mathbf{Q}(\zeta_{691})$, we know that

$$691 \quad | \quad h(\mathbf{Q}(\zeta_{691}))$$

since $B_{12}$ has numerator divisible by 691. We say 691 is an *irregular prime*.

- In light of the previous result, it seems interesting to investigate $p$-adic properties of Bernoulli numbers. The following result was proved by Kummer:
  Let $m, n > 0$ be even integers, not divisible by $(p-1)$. If $m \equiv n \bmod (p-1)p^a$, then

$$(1 - p^{m-1}) \cdot \frac{B_m}{m} \equiv (1 - p^{n-1}) \cdot \frac{B_n}{n} \pmod{p^{a+1}}. \tag{9}$$

  These identities are known as the *Kummer congruences*.

The work of Kummer was seminal for several important research themes that arose later. One was the introduction of $p$-adic numbers by Hensel in 1897 [**Hen97**]. Clearly, such a theory is called for by Kummer's congruences, which suggest that the quantities

$$(1 - p^{m-1}) \cdot \frac{B_m}{m}$$

should extend to a continuous function of $m$ in a fixed coset of $(p-1)\,\mathbf{Z}$ in $\mathbf{Z}$, with respect to a $p$-adic notion of distance whereby two numbers are considered "close" if their difference is highly divisible by $p$.

### 1.3. Historical developments

In these notes, we will continue the natural line of investigation initiated by Kummer, and introduce some of the most central and heavily studied objects in contemporary number theory: $p$-adic L-functions.

As we previously pointed out, the origins of $p$-adic numbers can be traced to the work of Kummer. They inspired some important early developments, such as the introduction of the abstract notion of fields by Steinitz [**Ste10**] and the work of Minkowski [**Min84**] on the theory of quadratic forms which was reinterpreted and strengthened by Hasse [**Has23, Has24**] to yield the famous statement that a quadratic form

$$Q(x_1, \ldots, x_n) = 0$$

over a number field $K$ has a solution $(x_1, \ldots, x_n) \in K^n$ if and only if it has a solution in every completion of $K$, which means the completion with respect to both the archimedean places, and the non-archimedean places corresponding to the primes of $K$. Further credibility was given to these methods when Chevalley [**Che33, Che40**] introduced the concept of idèles, and reformulated much of class field theory in this language, leading to a greatly simplified treatment. We will not discuss these developments here, as important as they are, and interested students enrolled in the simultaneous course by Arno Kret at the UvA this semester will be able to learn more about it there.

In these notes, we discuss more recent developments, which transformed the field of number theory after some groundbreaking developments in the first two decades after World War II. The various chapters of these notes have the following historical context:

- *2. Foundations of $p$-adic analysis.* After the early work of Hensel and Krasner in $p$-adic analysis, which was discussed in the notes of Stevenhagen, the subject experienced a hugely influential renaissance starting in the 60's with the work of Dwork [**Dwo60, Dwo62**]. Excellent accounts of the foundations of $p$-adic analysis and its application to the proof of rationality of zeta functions of hypersurfaces can be found in the book of Dwork, Gerotto, Sullivan [**DGS94**]. The insights of Dwork, Grothendieck, Katz, and many others saw the development of $p$-adic cohomology theories, $p$-adic differential equations, and crystals. Their applications range from modern areas like the Langlands programme to ancient problems like the resolution of Diophantine equations. See for instance Kedlaya [**Ked07, Ked10**] and Kim [**Kim05, Kim10**].

- *3. Distributions and measures.* An extremely important development came with the doctoral thesis of Tate [**Tat50**] and simultaneous independent work of Iwasawa [**Iwa52b, Iwa52a**]. It introduced tools from harmonic analysis and Fourier transforms to the non-archimedean world, and used them in spectacular fashion to prove statements of analytic continuation and functional equations for L-functions. This chapter of the notes treats the basics of functional analysis on $\mathbf{Z}_p$, in the spirit of later developments building on Tate's innovations. We were guided by the treatments of Washington [**Was97**], Coates–Sujatha [**CS06**], and Colmez [**Col10**].

- *4. $p$-Adic L-functions.* Another big conceptual leap was taken in the work of Kubota–Leopoldt [**KL64**] who introduced the $p$-adic zeta function $\zeta_p(s)$ interpolating certain special values of classical L-functions, and used it to explain the Kummer congruences that were discovered more than a century earlier. In these notes we take a more modern viewpoint of their results that makes use of functional analysis on $\mathbf{Z}_p$, following ideas of Manin, Mazur, Tate, and many others. Great sources for this material are Coates–Sujatha [**CS06**], Colmez [**Col**], and Rodrigues–Williams [**RW**].

- *5. Iwasawa theory.* Deep connections between the arithmetic of number fields and $p$-adic L-functions were exhibited by Iwasawa, who gave an algebraic construction based on cyclotomic units. The celebrated *Iwasawa main conjecture* asserts the equivalence of the algebraic and analytic constructions of $p$-adic L-functions. It was proved by Mazur–Wiles [**MW84**], and using the notion of Euler systems by Rubin [**Rub00**]. The development of Iwasawa theory continues to this day with greater vigour than ever. A recent advancement of Skinner–Urban [**SU14**], building on Kato [**Kat04**], uses a version of the Iwasawa main conjecture for elliptic curves to prove a $p$-adic version of the Birch–Swinnerton-Dyer conjecture due to Mazur–Tate–Teitelbaum [**MTT86**].

We hope that this overview underscores both the fact that the subject is more active today than it has ever been, and at the same time retains a strong continuity with themes and ideas that were around since the time of Kummer and even before. Due to the rapid succession in which groundbreaking insights are being produced, it becomes especially important to retain a connection with the work of practitioners in centuries past, and view the subject as part of a growing scientific tradition with ancient roots.

## 1.4. Acknowledgements

Numerous errors in an early version of these notes were pointed out by Mike Daas, and further corrections were suggested by Corijn Rudrum. I am very grateful for their careful reading and comments, and the improvements to which this led.

## 1.5. Exercises

(1) Give a rigorous proof of the identity

$$\sin(\pi z) = \pi z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2}\right).$$

(2) Using the table of Bernoulli numbers, and Kummer's criterion, find the smallest irregular prime.

CHAPTER 2

# Foundations of $p$-adic analysis

In this chapter, we will develop some foundational results in $p$-adic analysis. Notably, we prove Mahler's theorem about continuous functions on $\mathbf{Z}_p$, and we introduce the fundamental tool of Newton polygons to study the set of zeroes of analytic functions. Even though we take a somewhat minimalist approach, guided by our ultimate goals in this course, it should be noted that $p$-adic analysis is a vast and beautiful subject with very powerful applications. We mention in particular the work of Bernard Dwork and his disciples on rationality of zeta functions of hypersurfaces, a deep theorem in algebraic geometry.

This chapter was inspired by the excellent treatments of Cassels [**Cas86**] and Dwork–Gerotto–Sullivan [**DGS94**], and to a lesser extent, by the accounts of Koblitz [**Kob84**] and Washington [**Was97**].

**Notation.** Throughout this chapter, we choose a finite extension $L$ of $\mathbf{Q}_p$. We use the notation $\overline{\mathbf{Q}}_p$ for a chosen algebraic closure of $\mathbf{Q}_p$, and $\mathbf{C}_p$ for its completion with respect to the extension of the $p$-adic valuation characterised by $|p|_p = p^{-1}$. It is algebraically closed. We define its *order function*

$$\mathrm{ord} : \mathbf{C}_p \longrightarrow \mathbf{Q} \cup \{\infty\}, \quad x \longmapsto \mathrm{ord}(x) := -\frac{\log |x|_p}{\log(p)}$$

which satisfies the following properties

- $\mathrm{ord}(x) = \infty$ if and only if $x = 0$,
- $\mathrm{ord}(xy) = \mathrm{ord}(x) + \mathrm{ord}(y)$,
- $\mathrm{ord}(x + y) \geq \min\{\mathrm{ord}(x), \mathrm{ord}(y)\}$ with equality if $\mathrm{ord}(x) \neq \mathrm{ord}(y)$.

## 2.1. Continuous functions on $\mathbf{Z}_p$

In this section, we will study the space of continuous functions $f : \mathbf{Z}_p \longrightarrow L$, where $L$ is a finite extension of $\mathbf{Q}_p$. We prove a few structural results on such functions, most notably Mahler's theorem on uniform approximation by polynomials, and give a few important examples that play a role later on.

**2.1.1. Rearranging infinite series.** Before we delve into the specifics of $\mathbf{Z}_p$ as a domain for continuous functions, we briefly discuss some of the conveniences of non-archimedean analysis for future reference. We have seen that for any complete non-archimedean field $K$ an infinite series

$$\sum_i a_i$$

converges in $K$, if and only if $a_i \to 0$. In a similar spirit, rearrangements of series, which require a careful study in the fields $\mathbf{R}$ and $\mathbf{C}$, are quite straightforward in the setting of non-archimedean fields.

Lemma 2.1. *Let $K$ be a complete non-archimedean field.*

- *Let $a_n$ be a sequence of elements of $K$ such that $a_n \to 0$ as $n$ grows. For any rearrangement $\{a'_n\}$ of the sequence $\{a_n\}$ we have that the two series*

$$\sum_n a_n \qquad \sum_n a'_n$$

*both converge, and are equal to each other.*

- *Let $b_{mn}$ be a collection of elements in $K$ such that $b_{mn} \to 0$ as $\max\{m,n\}$ grows. Then*

$$\sum_m \sum_n b_{mn} \qquad \sum_n \sum_m b_{mn}$$

*both converge, and are equal to each other.*

**Proof.** The proof of both statements is a consequence of the ultrametric inequality, and is left as an exercise to the reader. □

**2.1.2. Two simple properties of $\mathbf{Z}_p$.** Before we dive into the celebrated theorem of Mahler, we take some time to highlight two simple, but important, facts about $\mathbf{Z}_p$ that underly some of the stronger structural results we will prove in the future: The compactness of $\mathbf{Z}_p$, and the density of $\mathbf{N}$ inside $\mathbf{Z}_p$.

We begin with the former. Recall the theorem of Heine–Cantor, about continuous real-valued functions on a closed interval $[a,b] \subset \mathbf{R}$. This classical theorem assures that such a function is *uniformly continuous*. In other words, for any $\varepsilon > 0$ there exists a $\delta > 0$ such that we have

$$|f(x) - f(y)| < \varepsilon, \qquad \text{whenever} \quad |x-y| < \delta.$$

This theorem may be proved topologically, relying only on the compactness of the interval $[a,b]$. Therefore, it is readily extended to the context of the compact space $\mathbf{Z}_p$:

LEMMA 2.2 (Heine–Cantor). *If $f : \mathbf{Z}_p \longrightarrow L$ is continuous, then it is also uniformly continuous.*

**Proof.** Choose a constant $\varepsilon > 0$. The continuity of the function $f$ implies that for any element $x_0$ of $\mathbf{Z}_p$, there exists some constant $\delta_{x_0} > 0$ such that

$$|f(x_0) - f(x)| < \varepsilon$$

whenever $x \in B(x_0, \delta_{x_0}) := \{x \in \mathbf{Z}_p : |x_0 - x| < \delta_{x_0}\}$. The covering

$$\mathbf{Z}_p = \bigcup_{x_0 \in \mathbf{Z}_p} B(x_0, \delta_{x_0})$$

has a finite subcovering, by the compactness of $\mathbf{Z}_p$. Letting $\delta$ be the minimum of the radii $\delta_{x_0}$ occurring in this finite subcovering, we obtain the statement from the ultrametric inequality. □

Most natural examples of continuous functions $f : \mathbf{Z}_p \longrightarrow L$ of interest to us are obtained through the process of $p$-adic interpolation from functions that are initially defined on the dense subset of natural numbers $\mathbf{N}$ inside $\mathbf{Z}_p$. This is analogous to the way several functions from real analysis are constructed, for instance the function $s \mapsto a^s$ on $\mathbf{R}$ for $a > 0$ which interpolates the exponential $n \mapsto a^n$, or the $\Gamma$-function on $\mathbf{R}_{>0}$ which interpolates the factorial $n \mapsto n!$.

LEMMA 2.3. *Suppose that $f : \mathbf{N} \longrightarrow L$ is a uniformly continuous function, where $\mathbf{N} \subset \mathbf{Z}_p$ is given the subspace topology. Then $f$ uniquely extends to a continuous function $f : \mathbf{Z}_p \longrightarrow L$.*

**Proof.** Let $s \in \mathbf{Z}_p$, then we may define $f(s) = \lim_n f(a_n)$ where $(a_n)$ is a Cauchy sequence of natural numbers that converge to $s$, which always exists by the density of $\mathbf{N}$ in $\mathbf{Z}_p$. This limit is independent from the choice of Cauchy sequence by the uniform continuity of $f$, and therefore we obtain a unique

$$f : \mathbf{Z}_p \longrightarrow L$$

which coincides with the given function $f$ on the subset of natural numbers $\mathbf{N} \subset \mathbf{Z}_p$, and which is easily seen to be continuous. □

**2.1.3. Mahler's theorem.** An important structural result states that a continuous function on a closed real interval can be uniformly approximated by polynomials.[1] For $n \in \mathbf{N}$ we define the polynomial

$$\binom{x}{n} := \begin{cases} 1 & \text{if} \quad n = 0 \\ \dfrac{x(x-1)\cdots(x-n+1)}{n!} & \text{if} \quad n \geq 1 \end{cases}$$

This is clearly a continuous function of $x \in \mathbf{Z}_p$, which takes values in $\mathbf{Z}_p$. As we will now see, any continuous function may be written as an infinite linear combination of these polynomials. The same statement was proved for compact subsets of $\mathbf{Q}_p$ by Dieudonné [**Die44**], and sharpened into the following constructive version due to Mahler [**Mah58**]. We follow the proof of Bojanic [**Boj74**].

THEOREM 2.4 (Mahler). *Let $f : \mathbf{Z}_p \longrightarrow L$ be a continuous function. There exist unique $a_n \in L$ such that*

$$f(x) = \sum_{n \geq 0} a_n \binom{x}{n}, \qquad \textit{with} \quad \lim_{n\to\infty} a_n = 0. \tag{10}$$

**Proof.** We define the *finite differences* $\Delta^{[n]} f$ for $n \geq 0$ by the recursion

$$\begin{aligned} \Delta^{[0]} f(x) &= f(x) \\ \Delta^{[n+1]} f(x) &= \Delta^{[n]} f(x+1) - \Delta^{[n]} f(x), \qquad n \geq 0. \end{aligned}$$

One directly verifies the identities

$$\begin{aligned} \Delta^{[n]} f(x) &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k) \\ &= \sum_{j=0}^{m} \binom{m}{j} \Delta^{[n+j]} f(x-m), \end{aligned}$$

valid for any $m, n \in \mathbf{N}$. In particular, setting $x = m$ and defining $a_n := \Delta^{[n]} f(0)$, we obtain

$$\sum_{j=0}^{m} \binom{m}{j} a_{n+j} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k+m). \tag{11}$$

With this definition of $a_n := \Delta^{[n]} f(0)$, it remains to prove the following two statements:

I. The right hand side of (10) converges to a continuous function on $\mathbf{Z}_p$,
II. This continuous function agrees with $f(x)$ on a dense subset of $\mathbf{Z}_p$.

[1] This is a $p$-adic analogue of the Stone–Weierstraß theorem from real analysis

To prove statement I, note that by the Heine–Cantor lemma, the function $f$ is uniformly continuous on $\mathbf{Z}_p$. If we choose $s \geq 1$, there exists a $t \geq 1$ such that

$$|x - y| \leq p^{-t} \Rightarrow |f(x) - f(y)| \leq p^{-s}.$$

Setting $m = p^t$ in equation (11), we find that

$$a_{n+p^t} = -\sum_{j=1}^{p^t-1} \binom{p^t}{j} a_{n+j} + \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \left(f(k+p^t) - f(k)\right)$$

Note that the binomial coefficients in the first sum satisfy

$$\binom{p^t}{j} \equiv 0 \pmod{p}, \qquad \text{whenever } 1 \leq j \leq p^t - 1.$$

so that we obtain the following estimate from the ultrametric inequality:

$$|a_{n+p^t}| \ \leq \ \max\left\{ \frac{1}{p^s} \, , \, \frac{1}{p}|a_{n+j}| \, , \, 1 \leq j \leq p^t - 1 \right\}.$$

After rescaling $f$ to be valued in $\mathcal{O}_L$, we may assume without loss of generality that we have $|a_n| \leq 1$ for all $n$, from which we inductively deduce that

$$\begin{array}{lll} |a_n| \leq p^{-1} & \text{when} & n \geq p^t \\ |a_n| \leq p^{-2} & \text{when} & n \geq 2p^t \\ \vdots & & \vdots \\ |a_n| \leq p^{-s} & \text{when} & n \geq sp^t \end{array}$$

Since $s$ may be chosen arbitrarily large, statement I follows.

To prove statement II, note that equation (11) implies that the continuous function defined by the right hand side of (10) agrees with $f(x)$ on $x \in \mathbf{N}$, since we find

$$f(m) = \sum_{j=0}^{m} a_j \binom{m}{j}.$$

Because $\mathbf{N}$ is dense in $\mathbf{Z}_p$, the theorem follows. □

The expression (10) is sometimes called the *Mahler expansion* of the continuous function $f$, and the $a_n$ are sometimes referred to as its *Mahler coefficients*. Note that the proof is constructive, and in many situations one may efficiently compute the Mahler coefficients in practice.

The space of continuous functions is denoted by $\mathrm{Cont}(\mathbf{Z}_p, L)$. It is equipped with a supremum norm

$$\|f\| := \sup_{x \in \mathbf{Z}_p} |f(x)|.$$

Note that this supremum is finite, since $\mathbf{Z}_p$ is compact, which implies that any continuous function on it must be bounded. The supremum norm makes $\mathrm{Cont}(\mathbf{Z}_p, L)$ into a complete $L$-vector space which satisfies

$$\begin{cases} \|f\| = 0 \iff f = 0, & \\ \|f + g\| \leq \max\{\|f\|, \|g\|\} & \forall\, f, g \in \mathrm{Cont}(\mathbf{Z}_p, L) \\ \|\lambda f\| = |\lambda| \cdot \|f\| & \forall\, f \in \mathrm{Cont}(\mathbf{Z}_p, L),\ \forall\, \lambda \in L. \end{cases}$$

These properties, and the completeness of the topology, are sometimes summarised by saying that $\mathrm{Cont}(\mathbf{Z}_p, L)$ is a *Banach space* over $L$ with respect to the supremum norm. This norm in particular endows $\mathrm{Cont}(\mathbf{Z}_p, L)$ with a topology. One can show (see exercises) that

$$\|f\| = \sup_n |a_n|,$$

i.e. the supremum norm of $f$ may be read off from its Mahler coefficients.

## 2.2. Analytic functions

The space of continuous functions on $\mathbf{Z}_p$ is completely described by the theory of Mahler. However, this space is in many ways too large to allow us to prove strong results about concepts like convergence, zeroes, integration, etc. In order to alleviate this, we will now specialise to a more structured subspace, namely that of *analytic functions*. In this section, we will denote

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots, \qquad \text{in } L[\![x]\!]$$

for a power series whose coefficients $a_i$ belong to a finite extension $L$ of $\mathbf{Q}_p$.

Remark 2.5. Note that if $a_i \to 0$, this series converges for all $x \in \mathbf{Z}_p$ to a continuous function. However, the subspace of analytic functions is much smaller than the full space of continuous functions. More precisely, it can be shown that a continuous function $f : \mathbf{Z}_p \longrightarrow L$ with Mahler expansion

$$f(x) = \sum_n b_n \binom{x}{n}$$

is analytic if and only if $\lim_n b_n/n! \to 0$. Therefore the subspace of analytic functions can be easily characterised in terms of its Mahler coefficients, by a growth condition stronger than $b_n \to 0$.

**2.2.1. Radius of convergence.** One of the perks of an analytic function $f(x) = a_0 + a_1 x + \ldots$ is that it may be evaluated at $x$ in extensions of the field of $p$-adic numbers $\mathbf{Q}_p$. In order to solidify this idea, we will first introduce the field $\mathbf{C}_p$, and then discuss the notion of radius of convergence for $f$, determining for which $x \in \mathbf{C}_p$ we get a meaningful evaluation.

Consider the algebraic closure $\overline{\mathbf{Q}}_p$ of the field of $p$-adic numbers $\mathbf{Q}_p$, which is of infinite degree over $\mathbf{Q}_p$. We have studied the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\,\mathbf{Q}_p)$ and endowed it with a ramification filtration, and we showed also that the $p$-adic absolute value has a unique extension to $\overline{\mathbf{Q}}_p$. However, this field is not complete with respect to this valuation (see exercises) so it is natural to consider its completion $\mathbf{C}_p$.

Lemma 2.6. *The field $\mathbf{C}_p$ is algebraically closed.*

**Proof.** Consider a polynomial

$$F(x) = \prod_{i=1}^{n} (x - \alpha_i) \qquad \in \ \mathbf{C}_p[x],$$

and let $\alpha = \alpha_1$ be one of its roots in the algebraic closure of $\mathbf{C}_p$. Choose a polynomial $G(x) \in \overline{\mathbf{Q}}_p[x]$ of degree $n$ whose coefficients are very close to those of $F(x)$, and write

$$G(x) = \prod_{i=1}^{n} (x - \beta_i)$$

then we must have that $G(\alpha)$ is very small, and therefore one of the quantities $|\alpha - \beta_i|$ must be very small. This shows that if we choose $G(x)$ close enough to $F(x)$, we will get

$$|\alpha - \beta_i| < |\alpha - \alpha_j|$$

for all $j > 1$. It follows from Krasner's lemma that $\mathbf{C}_p(\alpha) \subseteq \mathbf{C}_p(\beta_i)$. However, the polynomial $G(x)$ is necessarily defined over a finite extension of $\mathbf{Q}_p$, and therefore $\beta \in \overline{\mathbf{Q}}_p$. This shows that $\mathbf{C}_p(\alpha) = \mathbf{C}_p$ and therefore $\mathbf{C}_p$ is algebraically closed. □

Finally, we are ready to define the radius of convergence. Consider an analytic function

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots \in \mathbf{C}_p[\![x]\!]$$

then we define its *radius of convergence* $R$ by

$$\frac{1}{R} = \limsup_n |a_n|^{1/n}.$$

so that $0 \leq R \leq +\infty$ with the obvious conventions. With this definition, we find that the power series $f(x)$ converges for a given value $x$ in $\mathbf{C}_p$ if and only if we have

$$\begin{array}{rcll} |x| & \leq & R & \text{if} \quad |a_n| R^n \to 0 \\ |x| & < & R & \text{otherwise.} \end{array}$$

Remark 2.7. Note that once again, some subtleties that are present for analytic functions on $\mathbf{R}$ or $\mathbf{C}$ resolve themselves in the $p$-adic context. The notion of radius of convergence of a power series over $\mathbf{R}$ or $\mathbf{C}$ is more slippery at the boundary. Consider for instance the series

$$f(x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \ldots \quad \in \quad \mathbf{C}[\![x]\!]$$

which is the Taylor expansion of the complex logarithm $\log(1+x)$ in a neighbourhood of 1. One computes that its radius of convergence is $R = 1$. Then $f(x)$ converges when $|x| < 1$ and diverges when $|x| > 1$, but the situation on $|x| = 1$ is more subtle: We get divergence for $x = -1$ but convergence for any other point in the boundary $|x| = 1$. This phenomenon never appears in the $p$-adic setting, where any power series either converges on the entire boundary $|x| = R$ or nowhere at all on the boundary.

**2.2.2. The $p$-adic logarithm.** A very important analytic function is the $p$-adic logarithm, defined by

$$\log_p(1+x) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{x^i}{i}. \tag{12}$$

which has radius of convergence $R = 1$ and does not converge anywhere on the boundary $|x| = 1$. The following "extension" of the logarithm to arbitrary arguments in $\mathbf{C}_p^\times$ is commonly referred to as the *Iwasawa branch* of the $p$-adic logarithm.

Proposition 2.8. *There exists a unique function*

$$\log_p : \mathbf{C}_p^\times \longrightarrow \mathbf{C}_p$$

*such that*

- $\log_p(1+x)$ *is given by the power series* (12) *when* $|x| < 1$,
- $\log_p(xy) = \log_p(x) + \log_p(y)$ *for all* $x, y \in \mathbf{C}_p^\times$,
- $\log_p(p) = 0$.

**Proof.** Choose an element $p^r$ for any $r \in \mathbf{Q}$ such that $p^{r+s} = p^r \cdot p^s$ for all $r, s \in \mathbf{Q}$. Since $\mathbf{C}_p$ is the completion of $\overline{\mathbf{Q}}_p$ it must have value group $p^{\mathbf{Q}}$ and therefore we may write any $\alpha \in \mathbf{C}_p$ as

$$\alpha = p^r \cdot \alpha_0, \qquad r \in \mathbf{Q},\ |\alpha_0| = 1.$$

The element $\alpha_0$ in turn may be written uniquely as a root of unity $w$ of order coprime to $p$ times an element $\alpha_1$ such that $|\alpha_1 - 1| < 1$. To see this, we note once more that $\mathbf{C}_p$ is the completion of $\overline{\mathbf{Q}}_p$, and any sequence of elements in $\overline{\mathbf{Q}}_p$ approximating $\alpha_0$ determines a sequence of elements in the residue field of $\overline{\mathbf{Q}}_p$ which is eventually constant. By Hensel's lemma, we may lift this element to a root of unity $w$ with the required properties. We then define $\log_p(\alpha)$ by

$$\log_p(\alpha) := \log_p(\alpha_1)$$

where the right hand side is defined by (12). This satisfies all the required properties. □

REMARK 2.9. Prom the proof we see that the above theorem remains true if we instead demanded $\log_p(\varpi) = 0$ for some element $\varpi$ of positive order. The choice of logarithm function defined by this choice of $\varpi$ is typically called a *branch* of the $p$-adic logarithm. Only the natural choice of $\varpi = p$ made in the above proposition is what typically goes by the name of the *Iwasawa branch* of the $p$-adic logarithm.

**2.2.3. The $p$-adic exponential.** Consider the analytic function defined by

$$\exp_p(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}. \tag{13}$$

We see that determining its radius of convergence is essentially equivalent to bounding $\mathrm{ord}(i!)$. The trivial estimates on the floor functions allow the following simple upper bound by a geometric series[2]

$$\mathrm{ord}(i!) = \left\lfloor \frac{i}{p} \right\rfloor + \left\lfloor \frac{i}{p^2} \right\rfloor + \ldots < \frac{i}{p-1}.$$

On the other hand, suppose that $p^a \leq i < p^{a+1}$ then we have

$$\begin{aligned} \left\lfloor \frac{i}{p} \right\rfloor + \left\lfloor \frac{i}{p^2} \right\rfloor + \ldots &> \frac{i}{p} + \ldots + \frac{i}{p^a} - a \\ &= \frac{i}{p-1} - \frac{ip^{-a}}{p-1} - a \\ &> \frac{i-p}{p-1} - \frac{\log(i)}{\log(p)}. \end{aligned}$$

It follows that, as $i$ grows, we have asymptotically that $\mathrm{ord}(i!) \sim i/(p-1)$ and thus the radius of convergence of the $p$-adic exponential function is given by

$$R = p^{-1/(p-1)} \quad < 1.$$

[2]In fact, by counting slightly more carefully it is not much harder to show the stronger upper bound $\mathrm{ord}_p(i!) \leq \frac{i-1}{p-1}$. For an even more precise estimate of the valuation in terms of the $p$-adic expansion of $i$, see Exercise 14.

In contrast with the relative ease with which we were able to extend the logarithm to $\mathbf{C}_p^\times$, there is no similar extension of the the exponential to larger disks. It is sometimes useful to consider the Artin–Hasse exponential instead, see § 2.4, which has slightly better convergence properties. Restricted to the appropriate domains of convergence, the $p$-adic logarithm and exponential are mutually inverse:

PROPOSITION 2.10. *If* $|x| < p^{-1/(p-1)}$ *then*

$$\begin{array}{rcl} \log_p(\exp_p(x)) & = & x \\ \exp_p(\log_p(1+x)) & = & 1+x \end{array}$$

**Proof.** When $|x| < p^{-1/(p-1)}$ we have that $|x^n/n!| < 1$ for all $n \geq 1$ so that $|\exp_p(x) - 1| < 1$ and therefore the $p$-adic logarithm is given by the power series (12) which formally satisfies the first identity. For the second identity, using Exercise 14 we find that for any $n \geq 2$ we have

$$|x^{n-1}/n!| < p^{-(n-1)/(p-1)}/|n!| < 1.$$

Therefore

$$|\log_p(1+x)| = |x - x^2/2 + \ldots| = |x|$$

which is smaller than the radius of convergence for $\exp_p$ so that $\exp_p(\log_p(1+x))$ converges. The second identity follows from the corresponding identity of formal power series. □

**2.2.4. The power function.** We now want to define a $p$-adic version of $s \mapsto a^s$. Assume for simplicity that $p$ is odd, the case $p = 2$ being similar. Recall that the Teichmüller representatives gave us an isomorphism $\mathbf{Z}_p^\times \simeq \mu_{p-1} \times (1 + p\,\mathbf{Z}_p)$, and we denote the projections onto the factors by

$$\begin{array}{rcccl} \omega & : & \mathbf{Z}_p^\times & \longrightarrow & \mu_{p-1} \\ \langle\,\cdot\,\rangle & : & \mathbf{Z}_p^\times & \longrightarrow & 1 + p\,\mathbf{Z}_p \end{array}$$

In other words, $\omega$ is the function that sends $x$ to the Teichmüller representative of the reduction of $x$ modulo $p$, and then $\langle x \rangle := x\omega(x)^{-1}$. We may now define the *power function* of any $a \in \mathbf{Z}_p^\times$ by

$$\langle a \rangle^s \,:\, s \longmapsto \exp_p(s \cdot \log_p(\langle a \rangle)).$$

Its radius of convergence depends on $a$, but it is larger than 1 (see exercises).

## 2.3. Newton polygons

One of the most useful tools for studying roots of polynomials over complete non-archimedean fields are *Newton polygons*. They allow us to easily infer information about the valuations of the roots of polynomials or power series, using only their coefficients. This yields a remarkably simple procedure that allows us to quickly access very useful information about roots that may otherwise be completely intractable.

REMARK 2.11. In our discussion of Newton polygons, we work for simplicity over a subfield $K \subset \mathbf{C}_p$ which is complete with respect to the induced valuation. This is justified by the fact that it covers all the cases of interest to us, but it should be clear to the reader that most of the proofs, and all of the results, remain valid for any complete non-archimedean field $K$.

**2.3.1. Polynomials.** Suppose we have a polynomial over $K$ of degree $n$

$$f = a_n x^n + \ldots + a_1 x + a_0 \quad \in K[x]$$

then we define its *Newton polygon* $\mathrm{NP}(f)$ to be the lower convex hull of the finite set of points

$$\mathcal{S} = \{(i, \mathrm{ord}(a_i)) \,:\, i = 0, \ldots, n\} \;\subset\; \mathbf{R}^2 \,.$$

This means that $\mathrm{NP}(f)$ is the union of all line segments joining two of the points in $\mathcal{S}$ which do not run strictly above any of the other points. Every such segment has a *slope*, and we call its *multiplicity* the positive difference between the first coordinates of its endpoints. In other words, the *multiplicity* of a segment is the length of its projection to the horizontal axis. The multiplicity is extended to arbitrary $\lambda \in \mathbf{Q}$ by setting it to be zero if $\lambda$ does not arise as the slope of a segment of $\mathrm{NP}(f)$.

Example 2.12. Consider the polynomial

$$f = 100x^4 + 75x^2 + \frac{5}{2}x + 10 \qquad \mathbf{Q}[x]. \tag{14}$$

Since $f$ has rational coefficients, we may view it as a polynomial over any $p$-adic completion $K = \mathbf{Q}_p$ and determine its Newton polygon. Viewed as a polynomial over $\mathbf{Q}_2$ and $\mathbf{Q}_5$, we obtain the following pictures for the corresponding Newton polygons $\mathrm{NP}(f)$:

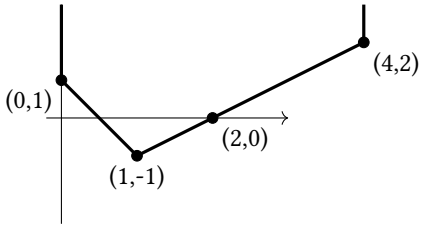



Figure 1. $\mathrm{NP}(f)$ for $K = \mathbf{Q}_2$

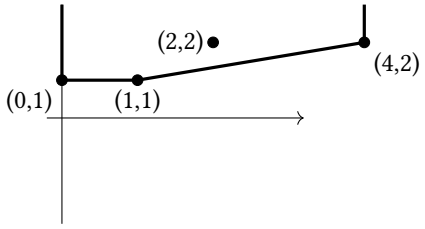



Figure 2. $\mathrm{NP}(f)$ for $K = \mathbf{Q}_5$

We see that the Newton polygon over $\mathbf{Q}_2$ has precisely two slopes. The first slope is $-2$ and has multiplicity $1$. The second slope is $1$ and has multiplicity $3$. Over $\mathbf{Q}_5$ on the other hand, there are two slopes, namely $0$ with multiplicity $1$ and $1/3$ with multiplicity $3$.

On the other hand, when viewed as a polynomial over $K = \mathbf{Q}_p$ for any $p \notin \{2, 5\}$, we see that $\mathrm{ord}(a_i) = 0$ for all coefficients $a_i$ of the polynomial $f \in K[x]$. As a consequence, the Newton polygon $\mathrm{NP}(f)$ over all these completions is given as in Figure 3. It has a single slope $0$ with multiplicity $4$.

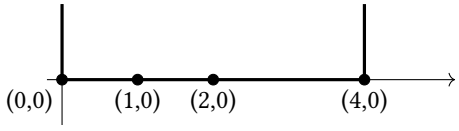



Figure 3. $\mathrm{NP}(f)$ for $K = \mathbf{Q}_p$ where $p \notin \{2, 5\}$

These definitions are justified by the following theorem, which states that the number of roots of $f$ of order $-\lambda$ is given by the multiplicity of the slope $\lambda$ in the Newton polygon $\mathrm{NP}(f)$. Note that the proof of this theorem relies on little more than the ultrametric inequality.

THEOREM 2.13. *Let $f \in K[x]$, and write $f = a_n \prod_{\lambda \in \mathbf{Q}} f_\lambda$ where*

$$f_\lambda(x) = \prod_{\substack{f(r)=0 \\ \mathrm{ord}(r) = -\lambda}} (x - r).$$

*Then $f_\lambda(x) \in K[x]$, and its degree is equal to the multiplicity of $\lambda$ in the Newton polygon $\mathrm{NP}(f)$.*

**Proof.** Suppose $g \in K[x]$ is any irreducible factor of $f$. Then the roots of $g$ form a single orbit for the action of the Galois group $\mathrm{Gal}(\overline{K}/K)$. Since the valuation is preserved by this action, all the roots of $g$ must have the same valuation. This implies that $f_\lambda \in K[x]$.

Note that the statement about the multiplicities of the slopes is invariant under scaling by $K$ and multiplication by powers of $x$, so that it suffices to prove the statement when $f$ is of the form

$$f = 1 + a_1 x + \ldots + a_n x^n = \prod_{i=1}^{n} (1 + \alpha_i x).$$

Order the factors such that

$$\mathrm{ord}(\alpha_1) \leq \mathrm{ord}(\alpha_2) \leq \ldots \leq \mathrm{ord}(\alpha_n).$$

Suppose that $\{\mathrm{ord}(\alpha_1), \ldots, \mathrm{ord}(\alpha_n)\} = \{\nu_1, \ldots, \nu_l\}$ for $\nu_1 < \ldots < \nu_\ell$, and let $\kappa_i$ be the number of $\alpha_j$ such that $\mathrm{ord}(\alpha_j) = \nu_i$. In other words, our numberings are such that

$$\begin{array}{lcccll}
\mathrm{ord}(\alpha_1) & = & \ldots & = & \mathrm{ord}(\alpha_{\kappa_1}) & = \nu_1, \\
\mathrm{ord}(\alpha_{\kappa_1+1}) & = & \ldots & = & \mathrm{ord}(\alpha_{\kappa_1+\kappa_2}) & = \nu_2, \\
\vdots & & & & & \vdots \\
\mathrm{ord}(\alpha_{\kappa_1+\kappa_2+\ldots+\kappa_{\ell-1}+1}) & = & \ldots & = & \mathrm{ord}(\alpha_{\kappa_1+\kappa_2+\ldots+\kappa_\ell}) & = \nu_\ell.
\end{array}$$

Note that for any $1 \leq s \leq n$ we have the following expression for the coefficient $a_s$ of $f$:

$$a_s = \sum_{1 \leq i_1 < \ldots < i_s \leq n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_s} \tag{15}$$

From this expression, we estimate $\mathrm{ord}(a_s)$ via the ultrametric inequality. There are two cases.

(I) $s = \kappa_1 + \kappa_2 + \ldots + \kappa_\rho$, for some $0 \leq \rho \leq \ell$:
In this case $\mathrm{ord}(\alpha_{s+1}) > \mathrm{ord}(\alpha_s)$ so that (15) implies the equality

$$\begin{array}{rcl}
\mathrm{ord}(a_s) & = & \mathrm{ord}(\alpha_1 \cdots \alpha_s) \\
& = & \nu_1 \kappa_1 + \ldots + \nu_\rho \kappa_\rho.
\end{array}$$

(II) $\kappa_1 + \kappa_2 + \ldots + \kappa_\rho < s < \kappa_0 + \kappa_1 + \kappa_2 + \ldots + \kappa_\rho + \kappa_{\rho+1}$, for some $0 \leq \rho < \ell$:
In this case (15) merely implies the estimate

$$\begin{array}{rcl}
\mathrm{ord}(a_s) & \geq & \mathrm{ord}(\alpha_1 \cdots \alpha_s) \\
& = & \nu_1 \kappa_1 + \ldots + \nu_\rho \kappa_\rho - \nu_{\rho+1}(s - \kappa_1 - \ldots - \kappa_\rho).
\end{array}$$

This shows that in case (I) the point $P_\rho := (s, \nu_1\kappa_1 + \ldots + \nu_i\kappa_i)$ is in the set $\mathcal{S}$ defining the Newton polygon $\mathrm{NP}(f)$. In case (II) on the other hand, the inequality on $\mathrm{ord}(a_s)$ is equivalent to the statement that $(s, \mathrm{ord}(a_s))$ lies on or above the line segment fro m $P_\rho$ to $P_{\rho+1}$. This implies that $[P_\rho, P_{\rho+1}]$ is a segment of the Newton polygon $\mathrm{NP}(f)$ for each $0 \leq \rho < \ell$, from which the theorem follows. □

**2.3.2. Power series.** The construction of Newton polygons, and the relation between roots and slopes, have suitable counterparts for power series. More precisely, let

$$f = a_0 + a_1 x + a_2 x^2 + \ldots \qquad \in K[\![x]\!]$$

be a power series with radius of convergence $R$. We define the Newton polygon exactly as before, by setting $\mathrm{NP}(f)$ to be the lower convex hull of the set of points

$$\mathcal{S} = \{(i, \mathrm{ord}(a_i)) \,:\, i = 0, 1, 2, \ldots\} \,\subset\, \mathbf{R}^2\,.$$

The Newton polygon $\mathrm{NP}(f)$ now has a possibly infinite set of finite slopes, and we define its multiplicity to be the length of the projection of the corresponding edge of the Newton polygon to the horizontal axis. Note that the multiplicity may be infinite. There are three basic possibilities.

(1) The set of finite slopes is empty: This happens for instance for the series

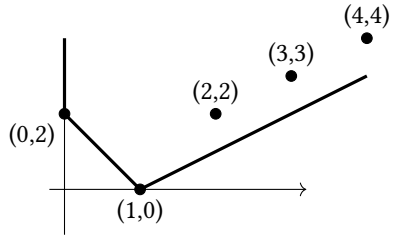
$$f = \sum_{n=0}^{\infty} p^{-n^2} x^n$$

The Newton polygon $\mathrm{NP}(f)$ in this case consists of a single vertical line (which we say is of "infinite slope") that coincides with the vertical coordinate axis.

(2) The set of finite slopes is finite: This happens for example in the case of the power series

$$f(X) = -p^2 + x + \sum_{n\geq 2}^{\infty} p^n x^n.$$

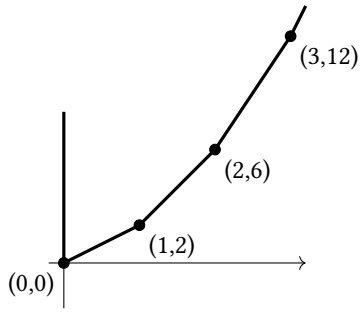
The Newton polygon $\mathrm{NP}(f)$ is now easily seen to have two finite slopes. The first is $-2$ and has multiplicity one. The second is $1$ and has infinite multiplicity.




(3) The set of finite slopes is infinite: This happens for example in the case of the power series

$$f(X) = \sum_{n=0}^{\infty} p^{n^2+n} x^n,$$

in which case the Newton polygon has infinitely many finite slopes, which are precisely the positive even integers, all with multiplicity one. Pictorially, we have:




The additive counterpart of the radius of convergence is the *order of convergence* $M$, defined by

$$-M = \liminf_n \frac{\mathrm{ord}(a_n)}{n}.$$

This quantity is characterised as the smallest number such that $f(x)$ converges whenever $x \in \mathbf{C}_p$ is such that $\mathrm{ord}(x) > M$. Alternatively, $-M$ may be characterised as the supremum of all the slopes of $\mathrm{NP}(f)$.

Just like the case of polynomials, there is a very close relation between the $p$-adic valuations of the roots of a power series, and the slopes of its Newton polygon. More precisely, we have the following analogon of Theorem 2.13. The main idea of the proof is to truncate the power series at some large degree, apply Theorem 2.13, and pass to the limit. The details and casework are somewhat lengthy, so we omit the proof.

THEOREM 2.14. *Let $f(x) \in K[\![x]\!]$ and suppose $\lambda$ is a slope of $\mathrm{NP}(f)$ of finite multiplicity $m_\lambda$. Then $f$ has precisely $m_\lambda$ roots $\alpha_i$ of order $\mathrm{ord}(\alpha_i) = -\lambda$ and we have a factorisation*

$$f(x) = P(x)Q(x), \qquad P(x) = \prod_{i=1}^{m_\lambda}(x - \alpha_i),$$

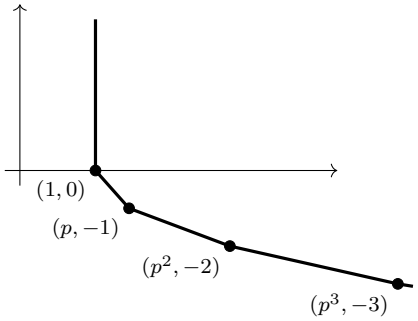
*where $Q(x) \in K[\![x]\!]$ is such that $\mathrm{NP}(Q)$ does not have a side of slope $\lambda$.*

**Proof.** See [**DGS94**, Theorem 2.1]. □

EXAMPLE 2.15. Let us look once more at the $p$-adic logarithm $\log_p$ which is given by

$$\log_p(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

defined on $\{x \in \mathbf{C}_p : |x| < 1\}$. Its Newton polygon is given by



As a consequence, the logarithm function $\log_p(1+x)$ has

$$\begin{array}{ccc} 1 & \text{zero} \quad \text{of order} & \infty \\ p-1 & \text{zeroes of order} & (p-1)^{-1} \\ p^2-p & \text{zeroes of order} & (p^2-p)^{-1} \\ \vdots & & \vdots \end{array}$$

in the set $\{x \in \mathbf{C}_p : |x| < 1\}$. Furthermore, in this case we know precisely what the zeroes are. The single zero of order $\infty$ is $x = 0$, whereas the set of zeroes of order $(p^t - p^{t-1})^{-1}$ certainly contains

$$x = \zeta_{p^t}^j - 1 \qquad \text{for } j \in (\mathbf{Z}/p^t\,\mathbf{Z})^\times$$

since $\log_p(1+x) = \log_p(\zeta_{p^t}^j) = 0$. There are precisely $p^t - p^{t-1}$ zeroes of this form, and therefore this accounts for all the zeroes of the $p$-adic logarithm $\log_p$ in the set $\{x \in \mathbf{C}_p : |x| < 1\}$.

We end this discussion with a classical result known as the *Weierstraß preparation theorem*. We say a polynomial $P(x) \in \mathcal{O}_K[x]$ is *distinguished* if we have

$$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0, \qquad \text{with} \quad \operatorname{ord}(a_i) > 0.$$

In other words, a polynomial is distinguished if it is monic and all of its roots have positive order. The Weierstraß preparation theorem states that, up to a power of the uniformiser, any power series over a discrete valuation ring can be written as a distinguished polynomial times an invertible series. It follows as a corollary from our discussion of Newton polygons. For a direct proof, see [**Was97**, Theorem 7.3].

Corollary 2.16 (Weierstraß preparation). *Suppose $K$ is discretely valued, with uniformiser $\varpi$ and valuation ring $\mathcal{O}_K$, and let $f \in \mathcal{O}_K[\![x]\!]$ be non-zero. Then there is a unique factorisation*

$$f = \varpi^\mu \cdot P(x) \cdot U(x)$$

*where $\mu$ is a non-negative integer, $P(x)$ is a distinguished polynomial, and $U(x)$ is a unit.*

**Proof.** First, we set $\mu = \min_n\{\operatorname{ord}_p(a_n) : n \geq 0\}$ so that $f \cdot \varpi^{-\mu}$ has coefficients of trivial valuation. Let $d$ be the smallest natural number such that $\operatorname{ord}(a_i) = 0$, then $(i, \operatorname{ord}(a_i))$ must be a vertex of the Newton polygon $\mathrm{NP}(f)$. This implies that that

$$P(x) = \prod_{\substack{f(\alpha)=0 \\ \operatorname{ord}(\alpha)>0}} (x - \alpha)$$

is a distinguished polynomial of degree $i$ such that $f \cdot \varpi^{-\mu} = P(x) \cdot U(x)$ for a power series $U(x)$ which has no roots of positive valuation, and is therefore a unit. □

## 2.4. Dwork's lemma

Though it will not be needed for our purposes, we would be remiss here not to mention Dwork's lemma, and its significance in the context of the rationality of zeta-functions of hypersurfaces, a deep and very important theorem in algebraic geometry that was one of the big early triumphs of $p$-adic analysis.

If the scope of these notes were to be expanded some day, this may be a natural point to treat in more detail the arguments and mathematics of this particular direction of the field. At the core of many of its most celebrated developments lies the following innocent looking lemma:

LEMMA 2.17. *Let $F(x) \in 1 + x \cdot \mathbf{Q}_p[\![x]\!]$. Then*

$$\begin{array}{rlll} & F(x) & \in & 1 + \ x \cdot \mathbf{Z}_p[\![x]\!] \\ \iff & F(x^p)/(F(x))^p & \in & 1 + px \cdot \mathbf{Z}_p[\![x]\!]. \end{array}$$

**Proof.** Assume first that $F(x) \in 1 + \ x \cdot \mathbf{Z}_p[\![x]\!]$ then we have

$$(F(x))^p = F(x^p) + pG(x)$$

for some $G(x) \in x \cdot \mathbf{Z}_p[\![x]\!]$. Because $(F(x))^p$ is invertible in $\mathbf{Z}_p[\![x]\!]$ we obtain the desired claim.

Conversely, assume that $F(x^p) = (F(x))^p G(x)$ for some

$$G(x) \in 1 + px \cdot \mathbf{Z}_p[\![x]\!].$$

Let $F(x) = \sum_i a_i x^i$, then we will show by induction that $a_i \in \mathbf{Z}_p$. We know that $a_0 = 1$. Suppose we have shown that $a_i \in \mathbf{Z}_p$ for all $i < n$, then computing the coefficient of $x^n$ of the identity

$$F(x^p) = (F(x))^p G(x)$$

gives us by the induction hypothesis the relation

$$\begin{cases} a_{n/p} & \equiv & a_{n/p}^p + pa_n & (\mathrm{mod}\ p\,\mathbf{Z}_p) & \text{if } p \mid n \\ 0 & \equiv & pa_n & (\mathrm{mod}\ p\,\mathbf{Z}_p) & \text{otherwise.} \end{cases}$$

from which we conclude that in either case $a_n \in \mathbf{Z}_p$. The lemma follows by induction. □

The significance of this result and its variants is hard to overestimate in the context of modern developments in $p$-adic cohomology, which have their roots in the highly original work of Bernard Dwork.

**2.4.1. The Artin–Hasse exponential.** An important function in $p$-adic analysis is the so-called *Artin–Hasse exponential*. We barely scratch the surface here, and regard it somewhat naively as an "improvement" of the $p$-adic exponential $\exp_p$, converging on the open unit disk in $\mathbf{C}_p$.

LEMMA 2.18. *Define the Artin–Hasse exponential by*

$$E(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \dots\right).$$

*We have $E(x) \in 1 + x \cdot \mathbf{Z}_p[\![x]\!]$.*

**Proof.** By Dwork's lemma, it suffices to check that

$$\frac{E(x)^p}{E(x^p)} = \frac{\exp\left(px + x^p + \frac{x^{p^2}}{p} + \dots\right)}{\exp\left(x^p + \frac{x^{p^2}}{p} + \dots\right)} = \exp(px) \quad \in 1 + px \cdot \mathbf{Z}_p[\![x]\!]$$

This follows from the estimates in our discussion of the exponential function $\exp_p$ in § 2.2.3. □

The above lemma shows that the Artin–Hasse exponential converges for all $x$ in $\{x \in \mathbf{C}_p : |x| < 1\}$, which is an improvement on the radius of convergence $p^{-1/(p-1)}$ of the $p$-adic exponential $\exp_p$. The comparison between the two functions has a similar flavour to the theme of removing the "Euler factors" at $p$ which we will see in our discussion on $p$-adic L-functions.

More precisely, define the Möbius function $\mu : \mathbf{N} \longrightarrow \mathbf{Z}$ by

$$\mu(n) := \begin{cases} (-1)^k & \text{if } n \text{ is squarefree, with } k \text{ prime divisors,} \\ 0 & \text{otherwise.} \end{cases}$$

One can then show that

$$\exp_p(x) = \prod_{n \geq 1} (1 - x^n)^{-\mu(n)/n} \qquad E(x) = \prod_{\substack{n \geq 1 \\ p \nmid n}} (1 - x^n)^{-\mu(n)/n}$$

In other words, the two functions are given by similar infinite product expansions, where the Artin–Hasse exponential has the factors 'at $p$' removed. This is a common phenomenon, whose roots are already present in the work of Kummer on congruences between Bernouilli numbers, as discussed in § 1.

## 2.5. Exercises

(1) Prove that the supremum norm of $f \in \mathrm{Cont}(\mathbf{Z}_p, L)$ is obtained from the Mahler coefficients $a_n$ of the continuous function $f$ by the equality

$$\|f\| = \sup_{n \geq 0} |a_n|.$$

(2) Extend the definition of the power function $s \mapsto \langle a \rangle^s$ to all primes $p$, including $p = 2$, and determine its radius of convergence for $s \in \mathbf{C}_p$, in terms of the chosen $\langle a \rangle \in 1 + p\,\mathbf{Z}_p$.

(3) Define the Fibonacci sequence $F_n$ by $F_0 = 1, F_1 = 1$ and

$$F_{n+1} = F_n + F_{n-1} \qquad {}^\forall n \geq 1.$$

Define the function

$$f : \mathbf{N} \to \mathbf{Z},\ n \mapsto F_n.$$

Does $f$ extend to a uniformly continuous function $f : \mathbf{Z}_p \to \mathbf{Z}_p$ for all primes $p$?

(4) Define the Nagell sequence $a_n$ by $a_0 = 0, a_1 = 1$ and

$$a_{n+1} = a_n - 2a_{n-1} \qquad {}^\forall n \geq 1.$$

Show that there are precisely 5 values of $n \geq 1$ such that $a_n = \pm 1$. [Hint: Show that for a fixed $r$, the function $m \mapsto a_{r+10m}$ is analytic in $m$ over $\mathbf{Q}_{11}$, and compute its first few coefficients.]

(5) Use the previous exercise to find all integer solutions $(x, y) \in \mathbf{Z}^2$ to

$$x^2 + 7 = 2^y.$$

(6) Define the Courgette sequence $c_n$ by $c_0 = 0, c_1 = 1$ and

$$c_{n+1} = 14c_n + 11c_{n-1} \qquad {}^\forall n \geq 1.$$

- Find the smallest value of $n > 0$ such that $c_n \equiv 0 \pmod{7^4}$.
- Show that there are $n > 0$ such that $c_n$ is divisible by an arbitrarily high power of 7.

(7) Let $c_n$ be the Courgette sequence, defined in the previous question. Show that there are $n > 0$ such that $c_n$ is divisible by an arbitrarily high power of 7, and such that $n$ is not divisible by 6. Can you also take $n$ not divisible by 2?

(8) Prove the following identities:

$$\begin{aligned} \sum_{n\geq 1} \frac{2^n}{n} &= 0 && \in \mathbf{Q}_2 \\ \sum_{n\geq 1} (-1)^n \frac{3^{2n}}{n4^{2n}} &= 2\sum_{n\geq 1} \frac{3^{2n}}{n4^n} && \in \mathbf{Q}_3 \end{aligned}$$

(9) Let $p$ be a prime. This exercise will show that $\overline{\mathbf{Q}}_p$ is not complete with respect to the unique extension of the absolute value on $\mathbf{Q}_p$. Assume on the contrary that $\overline{\mathbf{Q}}_p$ were complete, then:

- For any $n \geq 1$, choose a primitive $n$-th root of unity $\zeta_n$ in $\overline{\mathbf{Q}}_p$, and define $\tilde{\zeta}_n := \zeta_n$ when $(n, p) = 1$, and $\tilde{\zeta}_n = 1$ otherwise. For any $N \geq 1$, define

$$\alpha_N := \sum_{n=1}^{N} \tilde{\zeta}_n \cdot p^n \qquad \in \overline{\mathbf{Q}}_p$$

  Show that $(\alpha_N)_N$ is a Cauchy sequence.
- Show that this sequence converges to an element $\alpha$ in a finite extension $K/\mathbf{Q}_p$.
- Let $m \geq 1$ be the smallest integer such that $\tilde{\zeta}_n \in K$ for all $n < m$, and $\tilde{\zeta}_m \notin K$. Consider

$$\beta = p^{-m}\left(\alpha - \sum_{n=1}^{m-1} \tilde{\zeta}_n \cdot p^n\right).$$

  Show that $\beta \in K$, and $\beta \equiv \zeta_m \pmod{p}$.
- Use Hensel's Lemma to derive a contradiction, and conclude that $\overline{\mathbf{Q}}_p$ cannot be complete.

(10) Let $K$ be a finite extension of $\mathbf{Q}_p$ of degree $n$. Show that there is a constant $M$ depending only on $n$, such that $|\log_p(x)| \leq M$ for all $x \in K$.

(11) Show that the Iwasawa branch of the logarithm $\log_p : \mathbf{C}_p^\times \to \mathbf{C}_p$

- is surjective,
- cannot be extended to a continuous function $\mathbf{C}_p \to \mathbf{C}_p$.

(12) Suppose that $x \in \{x \in \mathbf{C}_p : |x - 1| < 1\}$. Show that

$$\log_p(x) = \lim_{n\to\infty} \frac{x^{p^n} - 1}{p^n}.$$

(13) Suppose $n \in \mathbf{N}$ and denote its $p$-adic expansion by

$$n = a_0 + a_1 p + \ldots + a_k p^k, \qquad a_i \in \{0, \ldots, p-1\}$$

Sharpen the estimates for the factorial $n!$ that were proved above, by showing the exact formula

$$\mathrm{ord}_p(n!) = \frac{n - (a_0 + \ldots + a_k)}{p-1}.$$

(14) Let $f \in K[\![x]\!]$ be a power series over a subfield $K \subset \mathbf{C}_p$. Show that the slopes of $\mathrm{NP}(f)$ of finite multiplicity are rational numbers (or infinity). Show that the slopes of $\mathrm{NP}(f)$ that do not have finite multiplicity need not be rational, by giving a counterexample.

(15) Consider the power series

$$f(x) = \exp_p\left(b_0 + b_1 x^p + b_2 x^{p^2} + \ldots\right)$$

with $b_i \in \mathbf{Q}_p$. Use Dwork's lemma to prove that

$$f(x) \in 1 + x \cdot \mathbf{Z}_p[\![x]\!] \iff b_{i-1} - p b_i \in p\,\mathbf{Z}_p,\ {}^\forall i \in \{1, 2, \ldots\}.$$

(16) Prove that $\exp_p(x)$ and $E(x)$ have no zeroes in their regions of convergence.

CHAPTER 3

# Distributions and measures

In this chapter we study $p$-adic functional analysis, and discuss measures and their Mahler transforms. The material in this chapter is inspired by the excellent treatments of Koblitz [**Kob80, Kob84**], Rodrigues–Williams [**RW**], and Washington [**Was97**] as well as the much more thorough account of the theory by Colmez [**Col10**], which we recommend to any reader who wants to know more.

**Notation.** The results in this chapter are valid for any profinite abelian group $G$, but the only examples of interest to us in this course are the following groups

$$\begin{array}{rcccl} G & = & \mathbf{Z}_p & = & \varprojlim_n \ \mathbf{Z}/p^n\mathbf{Z} \\ G & = & \mathbf{Z}_p^\times & = & \varprojlim_n \ (\mathbf{Z}/p^n\mathbf{Z})^\times. \end{array}$$

We fix $G$ to be either of these two in what follows, and let $L \subset \mathbf{C}_p$ be a complete subfield.

## 3.1. Distributions

A function $f : G \to L$ is said to be *locally constant* if every point of $G$ has an open neighbourhood on which $f$ is constant. The $L$-vector space of locally constant functions on $G$ is denoted by $\mathrm{LC}(G, L)$. Any locally constant function is continuous. The space $\mathrm{LC}(G, L)$ is reminiscent of the 'step functions' which occur in the theory of integration for real analytic functions, in the notion of Riemann sums. In our $p$-adic context, such a theory of integration is procured through the notions of distributions and measures.

We define a *distribution* $\mu$ to be an element of the dual space of $\mathrm{LC}(G, L)$, i.e. a linear functional

$$\mu : \mathrm{LC}(G, L) \longrightarrow L.$$

The space of distributions $\mu$ on $G$ is denoted by $\mathrm{Dist}(G, L)$. Suppose that $f$ is a locally constant function on $G$, then the value $\mu(f)$ of the distribution $\mu$ at the function $f$ is denoted by the symbol

$$\int_G f(x) \cdot \mu(x) := \mu(f).$$

When no ambiguity can arise, we often omit the variable name and simply write

$$\int_G f \cdot \mu := \mu(f).$$

Example 3.1. A simple example is the *Dirac distribution* $\delta_a$ where $a$ is an element of $G$, defined by

$$\delta_a(f) = f(a).$$

The datum of a distribution $\mu$ contains a vast amount of information, since there is a tremendous amount of locally constant functions. Since $G$ is compact, any locally constant function must be a finite

linear combination of characteristic functions $\mathbf{1}_U$ on disjoint compact open subsets $U \subset G$, defined by

$$\mathbf{1}_U(x) := \begin{cases} 1 & \text{if } x \in U, \\ 0 & \text{otherwise.} \end{cases}$$

We therefore see that a distribution $\mu$ on $G$ is determined by the function $\mu(U) := \mu(\mathbf{1}_U)$ on compact open subsets, which is finite additive in the sense that if $U \subseteq G$ is the disjoint union of compact open sets $U_1, \ldots, U_k$ we have

$$\mu(U) = \mu(U_1) + \ldots + \mu(U_k).$$

Conversely, we see that any such finite additive function on compact open subsets uniquely extends to a distribution $\mu$ in $\mathrm{Dist}(G, L)$. This alternative way of describing a distribution is frequently useful, particularly on the group $G = \mathbf{Z}_p$ where the basis of open neighbourhoods of the form $a + p^n \mathbf{Z}_p$ allows us to describe a distribution $\mu$ by an even smaller amount of data.

LEMMA 3.2. *Every map $\mu$ from the collection of open sets $a + p^n \mathbf{Z}_p$ to $L$ for which*

$$\mu(a + p^n \mathbf{Z}_p) = \sum_{b=0}^{p-1} \mu(a + bp^n + p^{n+1} \mathbf{Z}_p) \tag{16}$$

*for all $a \in \mathbf{Z}_p$ and $n \geq 0$, extends uniquely to a distribution $\mu$ in $\mathrm{Dist}(\mathbf{Z}_p, L)$.*

**Proof.** Let $U$ be a compact open subset of $\mathbf{Z}_p$, write it as a finite union of subsets $V_i$ of the form

$$V_i = a + p^n \mathbf{Z}_p,$$

and define $\mu(U) = \mu(V_i)$. To prove the lemma, we need to show that (1) this definition is well-defined, i.e. it is independent of the chosen partition of $U$ into subsets of the form $a+p^n \mathbf{Z}_p$, and (2) this function $\mu$ is finite additive on compact opens $U$. The second property is clear. To check the well-definedness of $\mu(U)$, note that whenever we have

$$U = \bigcup_i V_i = \bigcup_j V_i'$$

there is a common refinement $\bigcup_k W_k$ of both coverings, where all $W_k$ are of the form $a + p^n \mathbf{Z}_p$. By the property (16) we have that

$$\sum_i \mu(V_i) = \sum_k \mu(W_k) = \sum_j \mu(V_j').$$

and therefore the value $\mu(U)$ is well-defined, and the lemma follows. □

The above lemma is what frequently allows one to describe explicit distributions $\mu$ in $\mathrm{Dist}(\mathbf{Z}_p, L)$ of arithmetic interest. All we need to do is describe the value of a tentative distribution on the basis of compact open neighbourhoods, and check that it is additive in the sense of the above lemma.

EXAMPLE 3.3. We define the *Haar distribution* $\mu_{\mathrm{Haar}}$ by

$$\mu_{\mathrm{Haar}}(a + p^n \mathbf{Z}_p) = p^{-n}.$$

The name comes from the fact that this coincides with the Haar measure on the open set $a + p^n \mathbf{Z}_p$, but we do not need to know what that means to verify that this simple definition gives a distribution, since

$$\sum_{b=0}^{p-1} \mu_{\mathrm{Haar}}(a + bp^n + p^{n+1} \mathbf{Z}_p) = \sum_{b=0}^{p-1} p^{-n-1} = p^{-n}.$$

so that $\mu_{\mathrm{Haar}}$ uniquely extends to a distribution in $\mathrm{Dist}(\mathbf{Z}_p, \mathbf{Q}_p)$.

EXAMPLE 3.4. We define the *Mazur distribution* $\mu_{\mathrm{Mazur}}$ by

$$\mu_{\mathrm{Mazur}}(a + p^n \mathbf{Z}_p) = \frac{a}{p^n} - \frac{1}{2},$$

where $0 \leq a \leq p^n - 1$. Once again, we easily check that it satisfies the additivity condition of Lemma 3.2.

## 3.2. Measures

We have seen that distributions are formally what we need to integrate locally constant functions on $G$. Since locally constant functions $\mathrm{LC}(G, L)$ are dense in the space of continuous functions $\mathrm{Cont}(G, L)$ (see exercises) it is tempting to ask which distributions can be used to integrate continuous functions instead. This leads us to the notion of *measures*, which are elements of the dual space of $\mathrm{Cont}(G, L)$.

We define a *measure* $\mu$ to be an element of the continuous dual of $\mathrm{Cont}(G, L)$, i.e. a functional

$$\mu : \mathrm{Cont}(G, L) \longrightarrow L$$

which is continuous with respect to the topology on $\mathrm{Cont}(G, L)$ induced by the supremum norm. The space of measures $\mu$ on $G$ is denoted by $\mathrm{Meas}(G, L)$. Note that since any locally constant function is continuous, any measure defines in particular a distribution, i.e. $\mathrm{Meas}(G, L) \subset \mathrm{Dist}(G, L)$. Suppose that $f$ is a continuous function on $G$. Then as before the value $\mu(f)$ of the measure $\mu$ at the function $f$ is denoted by the symbol

$$\int_G f(x) \cdot \mu(x) := \mu(f).$$

When no confusion can arise, we will omit the variable from this notation, and simply write

$$\int_G f \cdot \mu := \mu(f).$$

EXAMPLE 3.5. The *Dirac distribution* $\delta_a$ defined in § 3.1 extends to a measure, with the same definition. In other words, we have $\delta_a \in \mathrm{Meas}(G, L) \subset \mathrm{Dist}(G, L)$. This is indeed clear from its definition

$$\delta_a(f) = f(a).$$

which makes sense for general continuous functions $f$, and not just locally constant ones.

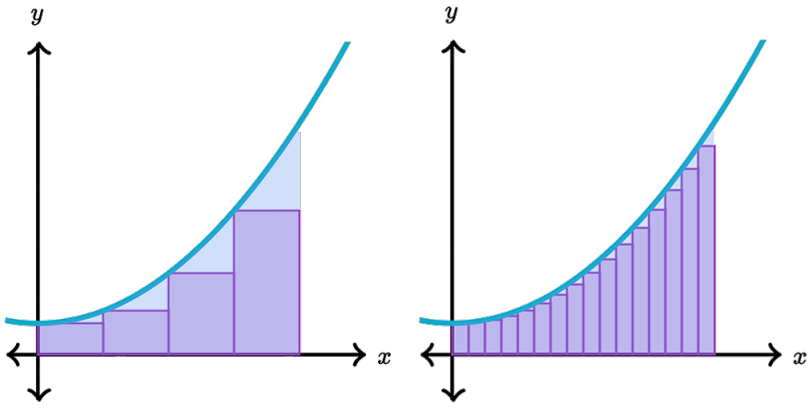
Since $\mathbf{Z}_p$ is compact, any continuous function is also uniformly continuous by Lemma 2.2. This implies that any continuous function on $\mathbf{Z}_p$ is the limit of a sequence of locally constant functions with respect to the supremum norm. In other words, the subspace $\mathrm{LC}(\mathbf{Z}_p, L) \subset \mathrm{Cont}(\mathbf{Z}_p, L)$ is dense. Therefore a measure $\mu$ on $\mathbf{Z}_p$ is determined by the finite additive function $\mu(U) := \mu(\mathbf{1}_U)$ on compact open subsets.

Now suppose conversely that we are given a distribution $\mu$ and we want to know whether it determines a measure. In other words, we would like to know how to integrate a continuous function $f$ against $\mu$. Since any continuous function $f$ is the limit of a sequence $f_1, f_2, \ldots$ of locally constant functions, we are led to wonder whether the limit

$$\mu(f) := \lim_{n \to \infty} \mu(f_n)$$

exists. This is analogous to the concept of Riemann sums in the theory of integration of real functions, whereby the integral of a function $f : [a, b] \to \mathbf{R}$ on a closed interval in $\mathbf{R}$ is defined as the limit of

integrals of step functions that converge to $f$, if this limit exists. Therefore we can use the same mental picture in the non-archimedean theory as we did in the archimedean theory of integration:




If the distribution $\mu$ comes from a measure, then one can show (see exercises) that $\mu$ is bounded, i.e. there exists a constant $C$ such that

$$|\mu(U)| \leq C$$

for all compact open subsets $U \subset \mathbf{Z}_p$. It turns out that the converse is also true, namely if a distribution is bounded, then we can define $\mu(f)$ for any continuous function $f$ by the limit above, which is convergent.

LEMMA 3.6. *Let $X \subset \mathbf{Z}_p$ be a compact open subset. Suppose $\mu \in \mathrm{Dist}(X, L)$ is bounded, and let $f \in \mathrm{Cont}(X, L)$. Define an infinite sequence of "Riemann sums"*

$$S_n := \sum_{a+p^n \mathbf{Z}_p \subset X} f(x_{a,n}) \cdot \mu(a + p^n \mathbf{Z}_p)$$

*where $x_{a,n}$ is an arbitrarily chosen point in $a + p^n \mathbf{Z}_p$. Then $S_n$ converges to a limit $\mu(f)$ as $n \to \infty$ which does not depend of the choices of points $x_{a,n}$ and $f \mapsto \mu(f)$ defines a measure on $X$.*

**Proof.** Choose $\varepsilon > 0$ arbitrary, and suppose $C > 0$ is such that

$$|\mu(U)| \leq C$$

for all compact open subsets $U$ of $X$. Taking $n$ to be very large, we may assume that

- Every subset $a + p^n \mathbf{Z}_p$ in $\mathbf{Z}_p$ is either contained in $X$ or disjoint from $X$,
- We have $|f(x) - f(y)| < \varepsilon$ for all $x, y \in a + p^n \mathbf{Z}_p$.

For any $m > n$ we then obtain the following estimates

$$|S_m - S_n| \leq \varepsilon \cdot \left| \sum_{a+p^m \mathbf{Z}_p \subset X} \mu(a + p^m \mathbf{Z}_p) \right| \leq \varepsilon C$$

by the ultrametric inequality. Since $\varepsilon$ was arbitrary and $C$ was fixed, we see that the sums have a limit which is independent of choices, from which all statements immediately follow. □

In conclusion, we found that measures are the same as *bounded* distributions. This means that we may always rescale a measure so as to obtain a measure valued in $\mathcal{O}_L$, i.e.

$$\mathrm{Meas}(G, \mathcal{O}_L) \otimes L = \mathrm{Meas}(G, L).$$

Note that in contrast with the Dirac distribution, neither the Haar distribution $\mu_{\mathrm{Haar}}$ nor the Mazur distribution $\mu_{\mathrm{Mazur}}$ described in § 3.1 define measures, since we can easily see neither of them is bounded.

## 3.3. Mahler transforms

Measures encode a large amount of information. We have two ways to determine a measure $\mu$:

- By its values $\mu(U)$ on all compact open subsets $U$ of $G$,
- By the integrals of all binomial polynomials, which determine $\mu$ uniquely by Mahler's theorem.

All the data in the first description can be encoded into a single element of a certain ring $\Lambda(G)$ that goes by the name of the *Iwasawa algebra*. The data in the second description is encoded into a single power series in $\mathcal{O}_L[\![T]\!]$, called the *Mahler transform* of $\mu$. We will see that there is an isomorphism $\Lambda(G) \simeq \mathcal{O}_L[\![T]\!]$ of $\mathcal{O}_L$-algebras, giving an identification between these two different descriptions of a measure. This allows us to produce and study arithmetically interesting measures with great ease later.

Define the *Iwasawa algebra* $\Lambda(G)$ as the projective limit

$$\Lambda(G) := \varprojlim_U \mathcal{O}_L[G/U]$$

where $U$ ranges over all open subgroups $U$ of $G$, and $\mathcal{O}_L[G/U]$ denotes the group algebra[1] over the finite group $G/U$. It is an $\mathcal{O}_L$-algebra. The Iwasawa algebra is naturally isomorphic to the space of measures $\mathrm{Meas}(G, \mathcal{O}_L)$. To see this, we begin by choosing an open subgroup $U$ of $G$, and defining the map

$$\begin{array}{rcccc} \alpha_U & : & \mathrm{Meas}(G, \mathcal{O}_L) & \longrightarrow & \mathcal{O}_L[G/U] \\ & & \mu & \longmapsto & \displaystyle\sum_{g \in G/U} \mu(g+U)[g]. \end{array}$$

By the additivity of $\mu$, the maps $\alpha_U$ form a projective system as $U$ varies, so that we obtain a map

$$\alpha := \varprojlim_U \alpha_U \quad : \quad \mathrm{Meas}(G, \mathcal{O}_L) \longrightarrow \Lambda(G).$$

Lemma 3.7. *The map $\alpha$ is an isomorphism of $\mathcal{O}_L$-modules.*

**Proof.** The map $\alpha$ is clearly $\mathcal{O}_L$-linear. Suppose we are given an element $f$ of the Iwasawa algebra $\Lambda(G)$. Let $U$ be an open subgroup of $G$, and we denote the image of $f$ in the group ring over $G/U$ by

$$f_U = \sum_{a \in G/U} c_a[a+U] \quad \in \quad \mathcal{O}_L[G/U]$$

Define $\mu(a+U) := c_a$, then $\mu$ defines a measure: Since $f$ is an element of the inverse limit, the map $\mu$ is finite additive and defines a distribution. Since $c_a \in \mathcal{O}_L$, the distribution is bounded, so that $\mu$ defines a measure. It is clear that $\alpha(\mu) = f$, so $\alpha$ is surjective. It is clear that $\alpha$ is injective. □

[1] Suppose $A$ is a group, and $R$ is a ring, then the *group ring* $R[A]$ is defined as the free $R$-module with generators $[a]$ indexed by $a \in A$. It is naturally an $R$-algebra with multiplication determined by the relations $[a_1] \cdot [a_2] = [a_1 a_2]$ for any $a_1, a_2 \in A$.

This isomorphism gives us two fundamentally different ways to think about measures, and depending on the situation it may be fruitful to change your point of view from one to the other via the above isomorphism $\alpha$. Moreover, note that the Iwasawa algebra is naturally an $\mathcal{O}_L$-algebra! The multiplication may therefore be carried over to the space of measures $\mathrm{Meas}(G, \mathcal{O}_L)$, where it obtains the following concrete description: The product $\mu_1 \star \mu_2$ of two measures $\mu_1$ and $\mu_2$ is given by *convolution*, defined by

$$\int_G f \cdot (\mu_1 \star \mu_2) = \int_G \left( \int_G f(x+y) \cdot \mu_2(y) \right) \cdot \mu_1(x)$$

Suppose $\mu \in \Lambda(\mathbf{Z}_p)$ is a measure on $\mathbf{Z}_p$. Define its *Mahler transform* to be

$$\begin{aligned} \mathscr{A}_\mu(T) &= \int_{\mathbf{Z}_p} (1+T)^x \mu(x) \\ &= \sum_{n \geq 0} \left( \int_{\mathbf{Z}_p} \binom{x}{n} \mu \right) T^n. \end{aligned}$$

In other words, the Mahler transform of a measure is the generating series of its values on the basis of continuous functions provided by Mahler's theorem. From this observation, we see that the Mahler transform uniquely determines the measure, so the Mahler transform is injective. It is in fact also surjective.

THEOREM 3.8. *The Mahler transform gives an $\mathcal{O}_L$-algebra isomorphism*

$$\Lambda(\mathbf{Z}_p) \xrightarrow{\sim} \mathcal{O}_L[\![T]\!]$$

**Proof.** We will define an explicit inverse. Suppose we are given a power series

$$f(T) = a_0 + a_1 T + a_2 T^2 + \dots$$

in $\mathcal{O}_L[\![T]\!]$. Let $U$ be an open subgroup in $\mathbf{Z}_p$. Then for each $a \in \mathbf{Z}_p / U$ the characteristic function on $a + U$ is continuous, so that by Mahler's theorem we may write it as a linear combination

$$\mathbf{1}_{a+U}(x) = \sum_{n \geq 0} b_{a,n} \binom{x}{n}$$

for some coefficients $b_{a,n} \in \mathcal{O}_L$. Now define the quantity

$$\mu_{[a]} := \sum_{n \geq 0} a_n b_{a,n}$$

which converges since $a_n \to 0$, and define furthermore

$$\mu_U := \sum_{a \in \mathbf{Z}_p / U} \mu_{[a]}[a] \quad \in \mathcal{O}_L[\mathbf{Z}_p / U].$$

If we let $V \subset U$ another open subgroup, then we likewise obtain $\mu_V \in \mathcal{O}_L[\mathbf{Z}_p / V]$ which maps to $\mu_U$ in the natural quotient, since $\mathbf{1}_{a+U}(x)$ is the sum of the characteristic functions on all the cosets of $V$ contained in $aU$, and the definition of $\mu_{[a]}$ is linear in the coefficients $b_{a,n}$. Therefore we obtain

$$\mu := \varprojlim_U \mu_U \in \Lambda(\mathbf{Z}_p)$$

whose Mahler transform is clearly equal to $f(T)$. □

EXAMPLE 3.9. Let us illustrate the various ways of thinking about measures on the example of the Dirac measure $\delta_a \in \mathrm{Meas}(\mathbf{Z}_p, L)$. As an element of the Iwasawa algebra $[a] \in \Lambda(\mathbf{Z}_p)$ we find that it has image

$$[a + p^n\,\mathbf{Z}_p] \in \mathcal{O}_L[\mathbf{Z}_p\,/p^n\mathbf{Z}_p]$$

in the finite group ring of $\mathbf{Z}_p\,/p^n\mathbf{Z}_p$ over $\mathcal{O}_L$. Its Mahler transform is

$$\mathscr{A}_{\delta_a}(T) = \sum_{n\geq 0}\binom{a}{n}T^n = (1+T)^a.$$

REMARK 3.10. Note that for any measure $\mu \in \mathrm{Meas}(\mathbf{Z}_p, L)$ we have

$$\int_{\mathbf{Z}_p} \mu = \mathscr{A}_\mu(0). \tag{17}$$

## 3.4. Operations on measures

Finally, we introduce a number of operations on measures, such as multiplication by functions, restriction to compact open subsets, and actions of $\mathbf{Z}_p^\times$ and the operators $\varphi$ and $\psi$.

**3.4.1. Multiplication by a function.** Suppose $f \in \mathrm{Cont}(\mathbf{Z}_p, L)$ and $\mu \in \mathrm{Meas}(\mathbf{Z}_p, L)$ then we define a new measure $f\mu$ by the rule

$$\int_{\mathbf{Z}_p} g(x)\cdot(f\mu)(x) = \int_{\mathbf{Z}_p} f(x)g(x)\cdot\mu(x).$$

Some examples of particular importance are the following:

- *Multiplication by $x$.* It follows from the identity

$$x\cdot\binom{x}{n} = (x-n+n)\cdot\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n}$$

that in this example we have

$$\mathscr{A}_{x\mu}(T) = \partial\,\mathscr{A}_\mu, \qquad \text{where } \partial = (1+T)\frac{d}{dT}.$$

- *Multiplication by $z^x$.* Suppose $z \in \mathbf{Z}_p^\times$ satisfies $|z-1| < 1$, then the Mahler transform of $z^x\mu$ is

$$\mathscr{A}_{z^x\mu}(T) = \mathscr{A}_\mu((1+T)z - 1),$$

which one can deduce from the formal identity

$$\mathscr{A}_\mu((1+T)z-1) = \int_{\mathbf{Z}_p}((1+T)z)^x\mu.$$

REMARK 3.11. Note that as an immediate consequence, we find the following generalisation of (17). For any $\mu \in \mathrm{Meas}(\mathbf{Z}_p, L)$ and any $k \geq 0$ we have the following expression for the "$k$-th moment" of $\mu$:

$$\int_{\mathbf{Z}_p} x^k\cdot\mu = \partial^k\,\mathscr{A}_\mu(0). \tag{18}$$

**3.4.2. Restriction to compact subgroups.** Another important operation is restriction to a compact open subset $X \subset \mathbf{Z}_p$, which is defined to be the measure obtained by multiplication with the characteristic function $\mathbf{1}_X$ on $X$. In other words, the measure $\mathrm{Res}_X(\mu)$ is defined by

$$\int_{\mathbf{Z}_p} f \cdot \mathrm{Res}_X(\mu) = \int_{\mathbf{Z}_p} f\mathbf{1}_X \cdot \mu.$$

In the special case where $X = a + p^n\,\mathbf{Z}_p$ we can write $\mathbf{1}_X$ explicitly as

$$\mathbf{1}_X(x) = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{x-a}$$

which shows that the Mahler transform of $\mathrm{Res}_X(\mu)$ is given by

$$\mathscr{A}_{\mathrm{Res}_X(\mu)} = \frac{1}{p^n} \sum_{\zeta^{p^n}=1} \zeta^{-a}\, \mathscr{A}_\mu((1+T)\zeta - 1).$$

Finally, we come to one of the most important operations on $\mathrm{Meas}(\mathbf{Z}_p, L)$: Restriction to the compact open $X = \mathbf{Z}_p^\times$. By the above, we find that the Mahler transform of $\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu)$ is given explicitly by

$$\mathscr{A}_{\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu)}(T) = \mathscr{A}_\mu(T) - \frac{1}{p} \sum_{\zeta^p=1} \mathscr{A}_\mu((1+T)\zeta - 1).$$

**3.4.3. Actions of $\mathbf{Z}_p^\times$, $\phi$ and $\psi$.** The space of measures is endowed with an action of the group $\mathbf{Z}_p^\times$, as well as operators $\varphi$ and $\psi$. These play an important role in our analysis of the Kubota–Leopoldt zeta function, and permit to establish connections with the Galois theory of cyclotomic fields.

- Suppose $a \in \mathbf{Z}_p^\times$ and $\mu \in \mathrm{Meas}(\mathbf{Z}_p, L)$ then we define $\sigma_a(\mu)$ by
$$\int_{\mathbf{Z}_p} f(x)\sigma_a(\mu) = \int_{\mathbf{Z}_p} f(ax)\mu.$$
One checks that this measure has Mahler transform
$$\mathscr{A}_{\sigma_a(\mu)}(T) = \mathscr{A}_\mu((1+T)^a - 1).$$
- We define the operator $\varphi$ by
$$\int_{\mathbf{Z}_p} f(x)\varphi(\mu) = \int_{\mathbf{Z}_p} f(px)\mu.$$
One checks that this measure has Mahler transform
$$\mathscr{A}_{\varphi(\mu)}(T) = \mathscr{A}_\mu((1+T)^p - 1).$$
- We define the operator $\psi$ by
$$\int_{\mathbf{Z}_p} f(x)\psi(\mu) = \int_{p\mathbf{Z}_p} f(p^{-1}x)\mu.$$
The Mahler transform of the measure $\psi(\mu)$ is more complicated, and given by
$$\mathscr{A}_{\psi(\mu)}(T) = \psi(\mathscr{A}_\mu),$$
where the operation $\psi$ on a power series $F(T)$ is determined by the condition
$$\psi(F)((1+T)^p - 1) = \frac{1}{p} \sum_{\zeta^p=1} F((1+T)\zeta - 1).$$

One can check that $\sigma_a$ and $\varphi$ are injective, but the operator $\psi$ is not, see Exercise 11. These actions satisfy various relations. For any $a \in \mathbf{Z}_p^\times$ we have

$$\begin{aligned} \psi \circ \sigma_a &= \sigma_a \circ \psi \\ \varphi \circ \sigma_a &= \sigma_a \circ \varphi \end{aligned} \tag{19}$$

and the operators $\varphi$ and $\psi$ furthermore satisfy

$$\begin{aligned} (\psi \circ \varphi)(\mu) &= \mu \\ (\varphi \circ \psi)(\mu) &= \mathrm{Res}_{p\mathbf{Z}_p}(\mu). \end{aligned} \tag{20}$$

The operator $\psi$ lies deeper than the rest, and its action on power series via the Mahler transform is difficult to make explicit. In certain special cases, we can however compute it explicitly, using the following Lemma.

LEMMA 3.12. *Suppose $\mu$ is a measure whose Mahler transform can be written in the form*

$$\mathscr{A}_\mu(T) = \sum_{n \geq 0} b_n (1+T)^n,$$

*for some $b_n \in L$. Then the Mahler transform of $\psi(\mu)$ is given by*

$$\mathscr{A}_{\psi(\mu)}(T) = \sum_{n \geq 0} b_{np} (1+T)^n.$$

**Proof.** Since $(\varphi \circ \psi)(\mu) = \mathrm{Res}_{p\mathbf{Z}_p}(\mu)$ we have

$$(\varphi \circ \psi)(\mathscr{A}_\mu) = \frac{1}{p} \sum_{n \geq 0} \sum_{\zeta^p = 1} b_n \zeta^n (1+T)^n.$$

For any $n \geq 0$ we have the relation

$$\frac{1}{p} \sum_{\zeta^p = 1} \zeta^n = \begin{cases} 0 & \text{if } p \nmid n \\ 1 & \text{if } p \mid n \end{cases}$$

which implies that

$$\varphi\left(\mathscr{A}_{\psi(\mu)}\right) = (\varphi \circ \psi)(\mathscr{A}_\mu) = \sum_{n \geq 0} b_{np} (1+T)^{np} = \varphi\left( \sum_{n \geq 0} b_{np} (1+T)^n \right)$$

since the operator $\varphi$ is injective, the statement follows. □

Finally, we note that a measure $\mu$ is supported on $\mathbf{Z}_p^\times$ if and only if $\psi(\mu) = 0$.

COROLLARY 3.13. *Let $\mu \in \Lambda(\mathbf{Z}_p)$ be a measure. Then $\mu$ is supported on $\mathbf{Z}_p^\times$ if and only if $\psi(\mathscr{A}_\mu) = 0$.*

**Proof.** There is a natural injection $\iota : \Lambda(\mathbf{Z}_p^\times) \hookrightarrow \Lambda(\mathbf{Z}_p)$ given explicitly by

$$\int_{\mathbf{Z}_p} f \cdot \iota(\mu) = \int_{\mathbf{Z}_p^\times} f\,|_{\mathbf{Z}_p^\times} \cdot \mu$$

Suppose that $\mu \in \Lambda(\mathbf{Z}_p)$, then $\mu$ has support in $\mathbf{Z}_p^\times$ if and only if it is in the image of $\iota$, which is equivalent to saying that $\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu) = \mu$ or in other words

$$\mathscr{A}_\mu = \mathscr{A}_\mu - \varphi \circ \psi(\mathscr{A}_\mu).$$

It is clear that $\varphi$ has trivial kernel, so that the latter is equivalent to $\psi(\mathscr{A}_\mu) = 0$. □

### 3.5. Exercises

(1) Let $f : \mathbf{Z}_p \to \mathbf{Q}_p$ be the function that sends $a \in \mathbf{Z}_p$ to the first digit $a_0$ in the $p$-adic expansion $a = a_0 + a_1 p + a_2 p^2 + \ldots$ with respect to the standard choice of digits

$$a_i \in \{0, 1, \ldots, p-1\} \subseteq \mathbf{Q}_p$$

Show that $f$ is locally constant, and compute the integrals

$$\int_{\mathbf{Z}_p} f \cdot \delta_a \qquad \int_{\mathbf{Z}_p} f \cdot \mu_{\text{Haar}} \qquad \int_{\mathbf{Z}_p} f \cdot \mu_{\text{Mazur}}$$

(2) Let $\mu$ be the function on compact opens $a + p^n \mathbf{Z}_p$ defined by

$$\mu(a + p^n \mathbf{Z}_p) := p^{-\lfloor \frac{n+1}{2} \rfloor}$$

if the first $\lfloor n/2 \rfloor$ digits of the $p$-adic expansion of $a$ corresponding to odd powers of $p$ vanish, and $\mu(a + p^n \mathbf{Z}_p) = 0$ otherwise. Prove that $\mu$ extends to a distribution on $\mathbf{Z}_p$.

(3) Let $\zeta \in \mathbf{C}_p$ be a root of unity whose order is a power of $p$, then show that $x \mapsto \zeta^x$ is a locally constant function. Show that the $\mathbf{C}_p$-subspace of $\mathrm{Cont}(\mathbf{Z}_p, \mathbf{C}_p)$ generated by these functions is dense.

(4) Let $X$ be a compact open subset of $\mathbf{Z}_p$. Show that $\mathrm{LC}(X, L)$ is dense in $\mathrm{Cont}(X, L)$. In other words, show that any continuous function $f : X \to L$ may be approximated arbitrarily closely by a locally constant function, with respect to the supremum norm.

(5) Recall that we defined a measure $\mu$ to be an element of the *continuous* dual $\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Cont}(G, L), L)$. Prove that the continuity of $\mu$ implies that it is bounded. [Hint: Use that $G$ is compact.]

(6) Define the vector space of *Lipschitz* functions to consist of $f : \mathbf{Z}_p \to L$ for which there exists some positive constant $A \in \mathbf{R}$ such that we have

$$|f(x) - f(y)| \leq A|x - y|$$

for all $x, y \in \mathbf{Z}_p$. Show that the space $\mathrm{Lip}(\mathbf{Z}_p, L)$ of all Lipschitz functions satisfies

$$\mathrm{LC}(\mathbf{Z}_p, L) \subset \mathrm{Lip}(\mathbf{Z}_p, L) \subset \mathrm{Cont}(\mathbf{Z}_p, L).$$

(7) Suppose that a distribution $\mu \in \mathrm{Dist}(\mathbf{Z}_p, L)$ is "boundedly increasing", meaning that

$$|p^n \mu(a + p^n \mathbf{Z}_p)| \to 0$$

as $n \to 0$, for any $a \in \mathbf{Z}_p$. Show that $\mu$ may be integrated against Lipschitz functions, i.e. that it can be extended to an element of the continuous dual of $\mathrm{Lip}(\mathbf{Z}_p, L)$:

$$\mu \in \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Lip}(\mathbf{Z}_p, L), L).$$

(8) Show that convolution of measures $\mu_1 \star \mu_2$ defined by

$$\int_G f \cdot (\mu_1 \star \mu_2) = \int_G \left( \int_G f(x + y) \cdot \mu_2(y) \right) \cdot \mu_1(x)$$

makes $\mathrm{Meas}(\mathbf{Z}_p, \mathcal{O}_L)$ into an $\mathcal{O}_L$-algebra. Show that the Mahler transform to the ring of power series $\mathcal{O}_L[\![T]\!]$ is an isomorphism of $\mathcal{O}_L$-algebras, by showing that

$$\mathscr{A}_{\mu_1 \star \mu_2}(T) = \mathscr{A}_{\mu_1}(T)\, \mathscr{A}_{\mu_2}(T).$$

(9) The space $\mathrm{Meas}(G, \mathcal{O}_L)$ can be equipped with two topologies, namely
   (a) The strong topology: This is the topology induced by the norm

$$\|\mu\| := \sup_{f \in \mathrm{Cont}(G, \mathcal{O}_L)} \frac{\|\mu(f)\|}{\|f\|}.$$

   In other words, this is the topology of *uniform* convergence.

   (b) The weak topology: This is the topology in which a sequence $\mu_n \to \mu$ if and only if

$$\mu_n(f) \to \mu(f)$$

   for all $f \in \mathrm{Cont}(G, \mathcal{O}_L)$.

   Show that under the Mahler transform, the strong topology corresponds to the $p$-adic topology on $\mathbf{Z}_p[\![T]\!]$, whereas the weak topology corresponds to the $(p, T)$-adic topology.

(10) Show that the $\mathcal{O}_L$-module generated by the Dirac measures $\delta_a$ for $a \in \mathbf{N}$ is dense in $\Lambda(\mathbf{Z}_p)$.

(11) Let $a \in \mathbf{Z}_p$ and $\delta_a$ the associated Dirac measure.

- Compute $\varphi(\delta_a)$ and $\psi(\delta_a)$, as well as $\sigma_b(\delta_a)$ for any $b \in \mathbf{Z}_p^\times$,
- Show that the operator $\psi : \mathbf{Z}_p[\![T]\!] \longrightarrow \mathbf{Z}_p[\![T]\!]$ is not injective,
- Show that the operators $\varphi$ and $\sigma_b$ for any $b \in \mathbf{Z}_p^\times$ are injective.

(12) Show that for any $a \in \mathbf{Z}_p^\times$, the map

$$\sigma_a : \mathbf{Z}_p[\![T]\!] \longrightarrow \mathbf{Z}_p[\![T]\!]$$

is an isometry for the $p$-adic topology. Show this is not true for $\varphi$ and $\psi$.

CHAPTER 4

# $p$-Adic L-functions

In this chapter we introduce and study $p$-adic L-functions, and discuss their special values and explicit calculation. The approach is an outgrowth of the influential viewpoint pioneered by Tate [**Tat50**] and Iwasawa [**Iwa52a, Iwa52b**] whereby L-functions are thought of as measures. We construct $p$-adic L-functions as the Mazur–Mellin transform of certain (pseudo-)measures, which are constructed via their Mahler transforms. This gives a more streamlined and powerful approach than the historical analytic treatment in the visionary work of Kubota–Leopoldt [**KL64**] in the early 60's.

## 4.1. The Riemann zeta function

We begin with a discussion of the analytic continuation and special values of the Riemann $\zeta$-function. Our treatment here differs slightly from the historical approach following Euler we adopted in § 1, since it may be carried over to the $p$-adic setting in a way that is more compellingly analogous.

LEMMA 4.1. *Suppose $f : \mathbf{R}_{\geq 0} \longrightarrow \mathbf{R}$ is a $C^\infty$ function that decays exponentially at infinity. Then*

$$L(f,s) := \frac{1}{\Gamma(s)} \int_0^\infty f(t) t^s \frac{dt}{t}, \qquad \mathrm{Re}(s) > 0$$

*admits an analytic continuation to the whole complex plane $s \in \mathbf{C}$, and for any $n \in \mathbf{Z}_{\geq 0}$ we have*

$$L(f,-n) = (-1)^n \frac{d^n}{dt^n} f(0).$$

**Proof.** Using the identity $\Gamma(s+1) = (s+1)\Gamma(s)$ and integration by parts, we find

$$L(f,s) = -L(f', s+1)$$

where the right hand side now converges for $\mathrm{Re}(s) > -1$. By iteration of this identity, we obtain analytic continuation to all $s \in \mathbf{C}$, and we find furthermore that

$$\begin{aligned} L(f,-n) &= (-1)^{n+1} L(f^{(n+1)}, 1), \qquad \text{where} \quad f^{(n)}(t) := \frac{d^n}{dt^n} f(t) \\ &= (-1)^{n+1} \int_0^\infty f^{(n+1)}(t) dt \\ &= (-1)^n f^{(n)}(0) \end{aligned}$$

which proves the required statement. □

This function $L(f,s)$ is called the *Mellin transform* of $f$. For the Riemann $\zeta$-function, we choose

$$f(t) \;=\; \frac{t}{e^t - 1} \;=\; \sum_{n \geq 0} B_n \frac{t^n}{n!}$$

which has exponential decay at infinity. Its Mellin transform is easily computed

$$\begin{aligned} L(f, s-1) &= \frac{1}{\Gamma(s-1)} \int_0^\infty \frac{t}{e^t - 1} t^{s-1} \frac{dt}{t} \\ &= \frac{s-1}{\Gamma(s)} \cdot \sum_{n \geq 1} \int_0^\infty e^{-nt} t^s \frac{dt}{t} \\ &= \frac{s-1}{\Gamma(s)} \cdot \sum_{n \geq 1} n^{-s} \int_0^\infty e^{-v} v^s \frac{dv}{v} \\ &= (s-1)\zeta(s) \end{aligned}$$

In particular, from Lemma 4.1 we recover[1] the special values

$$\zeta(1-k) = -\frac{B_k}{k}$$

which we obtained in § 1 as a consequence of the work of Euler. Though seemingly very different to the argument of Euler based around the sine function, some essential content of both his calculation and the one here are the same. It is worth reflecting on the similarities and differences.

## 4.2. The Kubota–Leopoldt zeta function

We will now emulate the story for $\zeta(s)$ by defining $\zeta_p(s)$ as a $p$-adic Mellin transform of a wisely chosen generating series for Bernoulli numbers. Like $\zeta(s)$, the $p$-adic zeta function $\zeta_p(s)$ has a simple pole at $s = 1$, which causes an additional technical complication. We first avoid it by considering a "smoothened" version of $\zeta_p$, eliminating the pole. For $\zeta_p$ itself, we work with *pseudo-measures* instead.

**4.2.1. The "smoothened" Kubota–Leopoldt zeta function.** We first introduce a "smoothing" by choosing an integer $a$ coprime to $p$ and defining the function

$$f_a(t) := \frac{1}{e^t - 1} - \frac{a}{e^{at} - 1} = \sum_{n \geq 0} (1 - a^{n+1}) \cdot \frac{B_{n+1}}{n+1} \cdot \frac{t^n}{n!},$$

which is related by the variable substitution $T = e^t - 1$ to the *integral* (see exercises) power series

$$F_a(T) := \frac{1}{T} - \frac{a}{(1+T)^a - 1} \qquad \in \mathbf{Z}_p[\![T]\!].$$

Consider the measure $\mu_a \in \mathrm{Meas}(\mathbf{Z}_p, \mathbf{Z}_p)$ whose Mahler transform is given by the power series $F_a(T)$. The variable substitution $T = e^t - 1$ gives us the identity

$$\partial := (1+T)\frac{d}{dT} = \frac{d}{dt}$$

[1]Note that $B_k = 0$ for odd $k$, so we may replace $(-1)^{k+1}$ by $-1$ in this formula.

of differential operators. Using equation (18) we may deduce that

$$\begin{aligned}\int_{\mathbf{Z}_p} x^k \cdot \mu_a &= (\partial^k F_a)(0) \\ &= \left(\frac{d^k}{dt^k} f_a\right)(0) \\ &= (-1)^k (1-a^{k+1}) \frac{B_{k+1}}{k+1} \\ &= (1-a^{k+1})\zeta(-k)\end{aligned}$$

for all $k \geq 0$. The following lemma studies the restriction to $\mathbf{Z}_p^\times$ of the measure $\mu_a$:

LEMMA 4.2. *We have*

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \mu_a = (1-p^k)(1-a^{k+1})\zeta(-k).$$

**Proof.** First, we will show that $\psi(\mu_a) = \mu_a$ by looking at the Mahler transform of $\mu_a$. Note that

$$\begin{aligned}\mathscr{A}_{\mu_a}(T) &= \frac{a}{1-(1+T)^a} - \frac{1}{1-(1+T)} \\ &= \sum_{n\geq 0} \lambda_n (1+T)^n\end{aligned}$$

where the coefficients $\lambda_n$ are given by

$$\lambda_n := \begin{cases} a-1 & \text{if} \quad a \mid n, \\ -1 & \text{if} \quad a \nmid n. \end{cases}$$

Since $p$ does not divide $a$, the condition $a \mid n$ is equivalent to $a \mid pn$, so that $\lambda_n = \lambda_{np}$ for all $n \geq 0$. It now follows from Lemma 3.12 that $\psi(\mu_a) = \mu_a$. Since $\mathrm{Res}_{\mathbf{Z}_p^\times} = 1 - \varphi \circ \psi$ we deduce that

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \mu_a = \int_{\mathbf{Z}_p} x^k \cdot (1-\varphi)\mu_a = (1-p^k) \int_{\mathbf{Z}_p} x^k \cdot \mu_a$$

which proves the lemma. □

**4.2.2. Pseudo-measures.** In order to remove the smoothing factor, which depends on the choice of $a$, we want to "divide out" the factor $(1-a^{k+1})$ that appears above. Note that

$$(1-a^{k+1}) = \int_{\mathbf{Z}_p^\times} x^k \cdot x([1]-[a])$$

where $[1]$ and $[a]$ are the Dirac measures at 1 and $a$ respectively. It therefore seems natural to try to divide the measure $\mathrm{Res}_{\mathbf{Z}_p^\times} \mu_a$ by the measure $x([1]-[a])$, which motivates the notion of pseudo-measures.

We write $Q(\mathbf{Z}_p^\times)$ for the ring of fractions of the Iwasawa algebra $\Lambda(\mathbf{Z}_p^\times)$, which consists of all quotients $r/s$ where $s$ is not a zero divisor in $\Lambda(\mathbf{Z}_p^\times)$. We say that an element $\lambda$ of $Q(\mathbf{Z}_p^\times)$ is a *pseudo-measure* if

$$([g]-[1])\lambda \quad \in \quad \Lambda(\mathbf{Z}_p^\times)$$

for all $g \in \mathbf{Z}_p^\times$. The set of all pseudo-measures is a $\mathbf{Z}_p$-module which we denote by $\widetilde{\Lambda}(\mathbf{Z}_p^\times)$, so that

$$\Lambda(\mathbf{Z}_p^\times) \subset \widetilde{\Lambda}(\mathbf{Z}_p^\times) \subset Q(\mathbf{Z}_p^\times).$$

When $\lambda$ is a pseudo-measure, we would like to still be able to integrate functions against it, as we are able to with measures. This is possible for the special case where we have a *group homomorphism*

$$f : \mathbf{Z}_p^\times \to L^\times$$

Consider two measures $\mu_1, \mu_2$ in $\Lambda(\mathbf{Z}_p^\times)$, then we compute that the integral of their convolution is

$$\begin{aligned}\int_{\mathbf{Z}_p^\times} f \cdot (\mu_1 \star \mu_2) &= \int_{\mathbf{Z}_p^\times} \left( \int_{\mathbf{Z}_p^\times} f(xy) \cdot \mu_2(y) \right) \cdot \mu_1(x) \\ &= \left( \int_{\mathbf{Z}_p^\times} f(x) \cdot \mu_1(x) \right) \left( \int_{\mathbf{Z}_p^\times} f(y) \cdot \mu_2(y) \right).\end{aligned}$$

In other words, we find that if $f$ is a group homomorphism, then the map $\Lambda(\mathbf{Z}_p^\times) \to L$ given by integration of $f$ over $\mathbf{Z}_p^\times$ is an algebra homomorphism. If $f$ is a group homomorphism that is not identically one, we may choose a $g \in \mathbf{Z}_p^\times$ such that $f(g) \neq 1$. We now see that for any pseudo-measure $\lambda$ the following quantity is independent of the choice of $g \in \mathbf{Z}_p^\times$:

$$\int_{\mathbf{Z}_p^\times} f \cdot \lambda := \frac{\int_{\mathbf{Z}_p^\times} f \cdot ([g] - [1])\lambda}{f(g) - 1} \qquad \in L.$$

The following lemma, whose proof is left as an exercise for the reader, assures that the integrals against the basic homomorphisms $x \mapsto x^k$ for $k > 0$ characterise $\lambda$ uniquely.

LEMMA 4.3. *Suppose $\lambda \in \widetilde{\Lambda}(\mathbf{Z}_p^\times)$ is a pseudo-measure. Then we have*

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \lambda = 0, \quad \forall k > 0 \qquad \Longleftrightarrow \qquad \lambda = 0.$$

The simplest example of a pseudo-measure is constructed as follows: First choose an integer $a$ whose reduction modulo $p^2$ generates the cyclic group $(\mathbf{Z}/p^2\mathbf{Z})^\times$. It then automatically generates the cyclic group $(\mathbf{Z}/p^n\mathbf{Z})^\times$ for every $n \geq 1$. With such a choice of $a$, one checks (see exercises) that

- $[1] - [a]$ is not a zero divisor in $\Lambda(\mathbf{Z}_p^\times)$,
- $1/([1] - [a])$ is a pseudo-measure.

To check the latter, we need to verify that

$$\frac{[1] - [g]}{[1] - [a]} \in \Lambda(\mathbf{Z}_p^\times)$$

for any $g \in \mathbf{Z}_p^\times$. Since the image of $a$ generates the cyclic quotient $(\mathbf{Z}/p^n\mathbf{Z})^\times$ for any $n \geq 1$, the image of $g$ is a power of the image of $a$, and the divisibility holds compatibly in every finite quotient.

**4.2.3. The Kubota–Leopoldt zeta function.** We can now define the Kubota–Leopoldt $p$-adic zeta function. Choose an integer $a$ that generates the cyclic group $(\mathbf{Z}/p^2\mathbf{Z})^\times$. Define the pseudo-measure

$$\zeta_p := \frac{x^{-1} \operatorname{Res}_{\mathbf{Z}_p^\times}(\mu_a)}{[1] - [a]} \qquad \in \widetilde{\Lambda}(\mathbf{Z}_p^\times).$$

PROPOSITION 4.4. *With these definitions, $\zeta_p$ is a pseudo-measure independent of the choice of $a$, and*

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \zeta_p = (1-p^{k-1})\zeta(1-k).$$

**Proof.** We know that $\zeta_p$ defines a pseudo-measure, and compute that

$$\begin{aligned}\int_{\mathbf{Z}_p^\times} x^k \cdot ([1]-[a_1])(x^{-1}\operatorname{Res}_{\mathbf{Z}_p^\times}\mu_{a_2}) &= (1-a_1^k)(1-a_2^k)(1-p^{k-1})\zeta(1-k)\\ &= \int_{\mathbf{Z}_p^\times} x^k \cdot ([1]-[a_2])(x^{-1}\operatorname{Res}_{\mathbf{Z}_p^\times}\mu_{a_1})\end{aligned}$$

so that it follows from Lemma 4.3 that

$$([1]-[a_1])(x^{-1}\operatorname{Res}_{\mathbf{Z}_p^\times}\mu_{a_2}) = ([1]-[a_2])(x^{-1}\operatorname{Res}_{\mathbf{Z}_p^\times}\mu_{a_1})$$

from which the independence of $\zeta_p$ on the choice of $a$ follows. The rest of the proposition follows. □

What gives us the right to refer to the pseudo-measure $\zeta_p$ as the Kubota–Leopoldt zeta "function"? We will now see how to interpret it as a function[2] via the $p$-adic Mellin transform, sometimes known as the *Mazur–Mellin transform.* Recall that the domain of Riemann zeta function $\zeta(s)$ is $s \in \mathbf{C}$. By sending $s \in \mathbf{C}$ to $(x \mapsto x^s)$, the domain of $\zeta(s)$ is naturally identified with the set of continuous homomorphisms

$$\operatorname{Hom}_{\text{cts}}(\mathbf{R}_{>0}^\times, \mathbf{C}^\times).$$

We argue that the above definition of $\zeta(s)$ as a Mellin transform shows that this description of the domain of the Riemann zeta function is much more natural. This is precisely the type of description we have for the domain of the Kubota–Leopoldt zeta function, which is the set of continuous homomorphisms

$$\operatorname{Hom}_{\text{cts}}(\mathbf{Z}_p^\times, \mathbf{C}_p^\times).$$

Reversing the process, we may try to view $\zeta_p$ as a function of a variable $s \in \mathbf{C}_p$, by evaluating $\zeta_p$ at some continuous homomorphism resembling $(x \mapsto x^s)$. This is what we will now make precise.

Recall the notation $q = p$ when $p$ is odd, and $q = 4$ when $p = 2$. We also discussed the Teichmüller map $\omega$ which sends an element of $\mathbf{Z}_p^\times$ to the unique root of unity in $\mathbf{Z}_p^\times$ closest to it, and $\langle x\rangle = x\omega(x)^{-1}$. The number of roots of unity in $\mathbf{Z}_p^\times$ is equal to

$$\varphi(q) = \begin{cases} p-1 & \text{if} \quad p > 2 \\ 2 & \text{if} \quad p = 2. \end{cases}$$

Suppose $i$ is a class in $\mathbf{Z}/\varphi(q)\,\mathbf{Z}$, then for any $s \in \mathbf{Z}_p$ we have

$$x \mapsto \omega(x)^i\langle x\rangle^s \quad \in \operatorname{Hom}_{\text{cts}}(\mathbf{Z}_p^\times, \mathbf{C}_p^\times).$$

We define the $i$-th Mellin transform of the pseudo-measure $\zeta_p$ to be the function

$$\zeta_{p,i}(s) := \int_{\mathbf{Z}_p^\times} \omega(x)^i\langle x\rangle^{1-s} \cdot \zeta_p$$

So we see that rather than a single function, we obtain rather a collection of functions, one for every root of unity in $\mathbf{Z}_p^\times$. We will now prove that all of these functions are analytic, with the exception of a simple pole at $s = 1$ when $i = 0$, whose residue is $(p-1)/p$.

[2]Or rather, a set of functions indexed by $(\mathbf{Z}/q\mathbf{Z})^\times$.

THEOREM 4.5. *For any $i \in \mathbf{Z}/\varphi(q)\mathbf{Z}$ the function*

$$(s-1)\zeta_{p,i}(s) : \mathbf{Z}_p \longrightarrow \mathbf{C}_p$$

*is analytic. This collection of functions satisfies the following properties:*

*(1) When $k \geq 1$ satisfies $k \equiv i \pmod{\varphi(q)}$ then*

$$\zeta_{p,i}(1-k) = (1-p^{k-1})\zeta(1-k).$$

*(2) At $s = 1$ we have*

$$\lim_{s\to 1}(s-1)\zeta_{p,i}(s) = \begin{cases} \frac{p-1}{p} & \text{if } i = 0 \\ 0 & \text{else.} \end{cases}$$

**Proof.** Let us first show that $(s-1)\zeta_{p,i}(s)$ is analytic. For any measure $\mu$ on $\mathbf{Z}_p^\times$, define a measure

$$\tilde{\mu}_i := \mathrm{Res}_{1+q\mathbf{Z}_p}\left(\sum_\tau \tau^i \sigma_\tau(\mu)\right)$$

where the sum runs over all Teichmüller representatives of the classes in $(\mathbf{Z}/q\mathbf{Z})^\times$ in $\mathbf{Z}_p^\times$, or, said differently, over all the roots of unity contained in $\mathbf{Z}_p^\times$. We may view $\tilde{\mu}_i$ as a measure on $\mathbf{Z}_p$ by composing any $f$ in $\mathrm{Cont}(\mathbf{Z}_p, L)$ with the map

$$\begin{array}{rccc} \theta & : & 1+q\mathbf{Z}_p & \longrightarrow & \mathbf{Z}_p \\ & & x & \longmapsto & \dfrac{\log_p(x)}{\log_p(1+q)} \end{array}$$

Writing $y = \theta(x)$ we find

$$(1+q)^{sy} = \exp_p(s\log_p(x)) = \langle x\rangle^s,$$

so that the Mahler transform of the measure $\tilde{\mu}_i$ on $\mathbf{Z}_p$ satisfies

$$\begin{aligned} \mathscr{A}_{\tilde{\mu}_i}\big((1+q)^s - 1\big) &= \int_{\mathbf{Z}_p} (1+q)^{sy}\cdot\tilde{\mu}_i(y) \\ &= \int_{1+q\mathbf{Z}_p} \langle x\rangle^s \cdot \left(\sum_\tau \tau^i\sigma_\tau(\mu)\right)(x) \\ &= \int_{\mathbf{Z}_p^\times} \omega(x)^i\langle x\rangle^s\cdot\mu \end{aligned}$$

where we used that $\langle \tau x\rangle = \langle x\rangle$, and if $x$ is contained in $\tau + q\mathbf{Z}_p$ then we have $\omega(x) = \tau$. The function $\zeta_{p,i}(s)$ is obtained from the Mellin transform of the measure $x^{-1}\mu_a$, after dividing by

$$\int_{\mathbf{Z}_p^\times} \omega(x)^i\langle x\rangle^{1-s}\cdot([1]-[a]) = 1-\omega(a)^i\langle a\rangle^{1-s}$$

Note that since $\langle a\rangle^{1-s} \in 1+q\mathbf{Z}_p$, this is an analytic function which is invertible if $i \not\equiv 0 \pmod{\varphi(q)}$, and which is the product of $(s-1)$ and an invertible function when $i = 0$. The statement about its special values at $s = 1-k$ follows immediately from Proposition 4.4. The calculation of the residue at $s = 1$ for $i \equiv 0$ is omitted, see for instance [**Col**]. □

Note that the analytic nature of the $p$-adic zeta function immediately puts into perspective many of the historical investigations of Kummer, like the following congruences between Bernoulli numbers:

THEOREM 4.6 (Kummer). *Let $m, n > 0$ be even integers, not divisible by $p-1$. When*

$$m \equiv n \bmod (p-1)p^a,$$

*then the following congruence holds:*

$$(1-p^{m-1}) \cdot \frac{B_m}{m} \equiv (1-p^{n-1}) \cdot \frac{B_n}{n} \pmod{p^{a+1}}. \tag{21}$$

**Proof.** By assumption we have $m \equiv n \equiv i \not\equiv 0 \pmod{p-1}$ for some $i$. The Kubota–Leopoldt zeta function $\zeta_{p,i}(s)$ is analytic in $s$, and we learned in the proof of Theorem 4.5 that it is in fact even an analytic function evaluated at the expression

$$(1+q)^{1-s} - 1 = \exp_p((1-s)\log_p(1+q)) - 1 \qquad \in \qquad p\,\mathbf{Z}_p[\![s]\!].$$

Since this expression is divisible by $p$, every coefficient of the power series $\zeta_{p,i}(s)$ – except possibly the constant coefficient – must also be divisible by $p$. From this observation, we deduce

$$\begin{aligned} \operatorname{ord}_p\left((1-p^{m-1}) \cdot \frac{B_m}{m} - (1-p^{n-1}) \cdot \frac{B_n}{n}\right) &= \operatorname{ord}_p\left(\zeta_{p,i}(1-m) - \zeta_{p,i}(1-n)\right) \\ &\geq \operatorname{ord}_p(n-m) + 1 \end{aligned}$$

□

It is truly remarkable that these results by Kummer only found their natural interpretation after a multitude of highly innovative developments of mathematics, and they were discovered in particular long before the inception of $p$-adic zeta functions, or even $p$-adic numbers.

## 4.3. Special values of $p$-adic L-functions

We now come to a property of the Kubota–Leopoldt zeta functions that is quite striking. Since we have presented the constructions of the Riemann and Kubota–Leopoldt zeta functions in parallel, centered around the same generating series for Bernoulli numbers, it may not have come as a complete shock that their special values at negative integers were closely related. However, the $p$-adic zeta function is also closely related to (complex) Dirichlet L-functions of characters $\chi$ of prime power conductor.

**Remark.** Previous comparisons of $p$-adic and complex numbers were restricted to rational numbers, which have a canonical interpretation through the embeddings $\mathbf{Q} \hookrightarrow \mathbf{C}$ and $\mathbf{Q} \hookrightarrow \mathbf{C}_p$. We shall now leave the realm of rational numbers, and to get meaningful comparisons we fix a pair of embeddings

$$\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}, \qquad \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}_p\,.$$

Let us begin by defining Dirichlet L-functions, which form a very natural generalisation of the Riemann zeta function. Let $N > 1$ be a positive integer. Let

$$\chi : (\mathbf{Z}/N\mathbf{Z})^\times \longrightarrow \overline{\mathbf{Q}}^\times$$

be a group homomorphism (typically called a *Dirichlet character*), extended to a function $\chi : \mathbf{Z} \longrightarrow \overline{\mathbf{Q}}$ by sending any element that is not coprime with $N$ to zero. We say $\chi$ is primitive if there does not exist a $\chi' : (\mathbf{Z}/d\,\mathbf{Z})^\times \to \overline{\mathbf{Q}}$ for a proper divisor $d$ of $N$, such that $\chi(n) = \chi'(n)$ for all $n$ coprime to $N$. In other words, $\chi$ is primitive if it is not constant on any subgroup $\{n \equiv 1 \pmod{d}\}$ of $(\mathbf{Z}/N\mathbf{Z})^\times$.

We define the *Dirichlet L-function* by

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

which converges for $\mathrm{Re}(s) > 1$. Dirichlet L-functions are common generalisations of the Riemann zeta function, and have many important applications in number theory, some of which you may already be familiar with. Their theory may largely be developed in analogy to our previous investigations into the Riemann zeta function. Choose a primitive $N$-th root of unity $\zeta_N$ and define

$$\begin{aligned} f_\chi(t) &= \frac{1}{G(\chi^{-1})} \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} \frac{\chi^{-1}(a)}{e^t \zeta_N^a - 1}, \qquad \text{where} \quad G(\chi) = \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} \chi(a)\zeta_N^a \\ &= \sum_{k \geq 1} \frac{B_{k,\chi}}{k} \cdot \frac{t^{k-1}}{(k-1)!}. \end{aligned}$$

The quantity $G(\chi)$ is called the *Gauß sum* of the character $\chi$, and the constants $B_{k,\chi} \in \overline{\mathbf{Q}}$ are known as *generalised Bernoulli numbers*. With these definitions, we check (see exercises) that

$$L(\chi, s) = \frac{1}{\Gamma(s)} \int_0^\infty f_\chi(t) t^s \frac{dt}{t}.$$

It now immediately follows from Lemma 4.1 that $L(\chi, s)$ has an analytic continuation to all $s \in \mathbf{C}$, and the special values at non-positive integers are given by

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

**4.3.1. Interpolation of characters at $p$.** The Kubota–Leopoldt $p$-adic zeta function was constructed from the special values $\zeta(1-k) \in \mathbf{Q}$ of the Riemann zeta function. We now show that it also knows the special values of Dirichlet L-functions associated to Dirichlet characters whose conductor is a power of $p$.

THEOREM 4.7. *Suppose $\chi : (\mathbf{Z}/p^n\mathbf{Z})^\times \to \overline{\mathbf{Q}}_p$ is a primitive Dirichlet character, then*

$$\int_{\mathbf{Z}_p^\times} \chi(x) x^k \cdot \zeta_p = L(\chi, 1-k)$$

**Proof.** We begin with the observation that if $\mu$ is any measure in $\mathrm{Meas}(\mathbf{Z}_p, L)$, then we may multiply it by the locally constant function $\chi$ on $\mathbf{Z}_p$ – which is supported on $\mathbf{Z}_p^\times$ – to obtain a measure $\chi\mu$. The Mahler transform of this measure $\chi\mu$ satisfies

$$\mathscr{A}_{\chi\mu}(T) = \frac{1}{G(\chi^{-1})} \sum_{j \in (\mathbf{Z}/p^n\mathbf{Z})^\times} \chi(j)^{-1} \mathscr{A}_\mu\left((1+T)\zeta_{p^n}^j - 1\right)$$

by the formal laws established in § 3.4, after a short calculation. When applied to the measures $\mu_a$ and $[1]-[a]$ we obtain after a direct calculation that

$$\begin{aligned}\int_{\mathbf{Z}_p^\times} \chi(x)x^k\cdot x^{-1}\mu_a &= \int_{\mathbf{Z}_p} x^{k-1}\cdot\chi\mu_a \\ &= \partial^{k-1}F_{\chi,a}(0) \\ &= (-1)^{k-1}\left(\frac{d}{dt}\right)^{k-1} f_{\chi,a}(0) \\ &= -(1-\chi(a)a^k)L(\chi,1-k) \\ \int_{\mathbf{Z}_p^\times} \chi(x)x^k\cdot([1]-[a]) &= -(1-\chi(a)a^k)\end{aligned}$$

where we defined $F_{\chi,a}(T)$ to be the Mahler transform of $\chi\mu_a$, explicitly given by

$$F_{\chi,a}(T)=\frac{1}{G(\chi^{-1})}\sum_{j\in(\mathbf{Z}/p^n\mathbf{Z})^\times}\chi(j)^{-1}\left(\frac{1}{(1+T)\zeta_{p^n}^j-1}-\frac{1}{(1+T)^a\zeta_{p^n}^{aj}-1}\right)$$

and $f_{\chi,a}(t)$ is obtained from $F_{\chi,a}(T)$ by substituting $T=e^t-1$. It satisfies

$$L(f_{\chi,a},s)=\chi(-1)(1-\chi(a)a^{1-s})L(\chi,s).$$

Taking the quotient, we obtain the required statement for $\zeta_p$. □

**4.3.2. Special values at $s=1$.** Even though at positive integers no direct equality is expected to exist between the special values of $p$-adic and complex zeta functions (since they are not expected to be contained in $\overline{\mathbf{Q}}$, there exist nonetheless compelling analogies between them. Of special importance is the value at $s=1$, just beyond the jurisdiction of the interpolation range.

Since we have come this far, it will now seem natural to expect that one may define in an entirely analogous fashion the $p$-adic L-function $L_p(\chi,s)$ for any Dirichlet character $\chi:(\mathbf{Z}/N\mathbf{Z})^\times\to\overline{\mathbf{Q}}$, whose special values in the interpolation range are related to the values of $L(\chi,s)$ by the rule

$$L_p(\chi,1-k)=(1-\chi\omega^{-k}(p)p^{k-1})\cdot L(\chi\omega^{-k},1-k),\qquad k\geq 1.$$

The required calculations and generating series are not more complicated than those appearing in the previous section, so we will leave them to the imagination (or indeed, determination) of the individual student. We note that the Kubota–Leopoldt $p$-adic zeta functions defined before are simply

$$\zeta_{p,i}(s)=L_p(\omega^i,s),$$

where $\omega:(\mathbf{Z}/p\mathbf{Z})^\times\to\overline{\mathbf{Q}}$ is the Teichmüller character. The special values we have so far encountered are therefore summarised in the following table, with the special appearances of the Riemann zeta function – the only piece of input for our definition of $\zeta_p$ – highlighted to bring them out more clearly:

| $s$ | $\cdots$ | $-3$ | $-2$ | $-1$ | $0$ | $1$ |
|---|---|---|---|---|---|---|
| $\zeta_{p,0}(s)$ | $\cdots$ | $L(\omega^{-4},-3)$ | $L(\omega^{-3},-2)$ | $L(\omega^{-2},-1)$ | $L(\omega^{-1},0)$ | pole |
| $\zeta_{p,1}(s)$ | $\cdots$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $\zeta_{p,2}(s)$ | $\cdots$ | $L(\omega^{-2},-3)$ | $L(\omega^{-1},-2)$ | $(1-p)\zeta(-1)$ | $L(\omega^{1},0)$ | ? |
| $\zeta_{p,3}(s)$ | $\cdots$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $\zeta_{p,4}(s)$ | $\cdots$ | $(1-p^3)\zeta(-3)$ | $L(\omega^{1},-2)$ | $L(\omega^{2},-1)$ | $L(\omega^{3},0)$ | ? |
| $\vdots$ | | | | | | |

There is therefore a close relation between the special values of the Kubota–Leopoldt zeta function and the Riemann zeta function at arguments

$$s \in \{\dots, -3, -2, -1, 0\}$$

which is typically referred to as the *interpolation range*. Outside the interpolation range, the special values of the $p$-adic and complex L-functions $L_p(\chi, s)$ and $L(\chi, s)$ have no direct relation, and both are often transcendental, so that no direct comparison is even possible. However, the following theorem shows that there is nonetheless a compelling analogy between the special values at $s = 1$.

THEOREM 4.8. *Let $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \overline{\mathbf{Q}}$ be a non-trivial character with $\chi(-1) = 1$, then*

$$\begin{aligned} L(\chi, 1) &= -\frac{1}{G(\chi^{-1})} \cdot \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} \chi^{-1}(a) \log\ (1 - \zeta_N^a), \\ \left(1 - \tfrac{\chi(p)}{p}\right)^{-1} L_p(\chi, 1) &= -\frac{1}{G(\chi^{-1})} \cdot \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} \chi^{-1}(a) \log_p(1 - \zeta_N^a). \end{aligned}$$

### 4.4. Explicit examples.

To define $p$-adic L-functions, we encountered a multitude of sophisticated and abstract notions. This may cloud these objects in a rather mysterious and seemingly impenetrable fog. Whereas it is true that many basic questions about them remain open to this day, it is also true that

$$(s-1)\zeta_{p,i}(s) \in \mathbf{Q}_p[\![s]\!]$$

are simply *power series*, and we know their special values at infinitely many negative integers. By the Weierstraß preparation theorem, this characterises them uniquely! When expanded upon, this simple observation allows us to compute some explicit examples. To explain how, take a non-zero congruence class $i$ modulo $\varphi(q)$, so that the function $\zeta_{p,i}(s)$ is analytic. Then do the following:

- For a large amount of $k \equiv i \pmod{\varphi(q)}$, compute the values
$$v_k = -(1 - p^{k-1})\frac{B_k}{k}.$$
- Using interpolation, compute a polynomial $P(s) \in \mathbf{Q}[s]$ such that, for all these $k$, we have
$$P(1-k) = v_k.$$

If one is slightly careful, one can argue that the polynomial $P(s)$ must agree with $\zeta_{p,i}(s)$ modulo some power of $p$, which gets larger as the "large amount" of values $v_k$ gets larger (this can be quantified). We encourage the reader with basic familiarity of programming to try this out for themselves, as it is an enlightening exercise that allows a newcomer to the theory to dispel a large part of the mystery that shrouds the Kubota–Leopoldt zeta functions at first sight.

The inspired reader can furthermore extend the above method to include $\zeta_{p,i}$ for $i \equiv 0$, when the zeta function has a pole. The truly inspired reader can also attempt to quantify the $p$-adic precision to which $P(s)$ can be guaranteed to agree with $\zeta_{p,i}(s)$.

**Example 1.** Let us begin by carrying out this procedure for the case $p = 2$. In this case, we have $q = 4$ and $\varphi(q) = 2$. We compute the special values $v_k$ for the first few values of $k$, to obtain

$i \equiv 0$ :

| $k$ | 0 | 2 | 4 | 6 | 8 | 10 |
|---|---|---|---|---|---|---|
| $v_k$ | $-1/6$ | $7/30$ | $-31/42$ | $127/30$ | $-2555/66$ | $1414477/2730$ |

$i \equiv 1$ :

| $k$ | 1 | 3 | 5 | 7 | 9 | 11 |
|---|---|---|---|---|---|---|
| $v_k$ | 0 | 0 | 0 | 0 | 0 | 0 |

where in reality we computed about one hundred values, though we will spare the reader of it here.

Finding the polynomial $P(s)$ which has these special values at $1 - k$ can be done, for instance, using Newton's divided differences method. When truncating the rational numbers to a low 2-adic precision, we keep the output manageable enough to be included here:

$$\begin{aligned} (1-s)\zeta_{p,0}(s) &= 2^{-1} + 261s + 257 \cdot 2s^2 + 137 \cdot 2^4 s^3 - 83 \cdot 2^3 s^4 + 119 \cdot 2^6 s^5 - 221 \cdot 2^6 s^6 \pmod{2^7}, \\ \zeta_{p,1}(s) &= 0 \pmod{2^7}. \end{aligned}$$

**Example 2.** Now let us consider $p = 5$, which gives rise to $\varphi(q) = 4$ functions. As before, we have

$$\zeta_{p,1}(s) = \zeta_{p,3}(s) = 0,$$

and we may compute the non-trivial 5-adic zeta functions using the same interpolation property we used above. This time, let us compute the expansions around $s = 1$. Working numerically modulo $5^{10}$ we find the following power series

$$\begin{aligned} (s-1)\zeta_{p,0}(s) = 4 \cdot 5^{-1} &+(4838826 \cdot 5)(s-1) &+(439093 \cdot 5)(s-1)^2 &-(2691469 \cdot 5^2)(s-1)^3 \\ &+(2187444 \cdot 5^2)(s-1)^4 &-(3051329 \cdot 5^4)(s-1)^5 &+(855172 \cdot 5^4)(s-1)^6 \\ &-(3669287 \cdot 5^5)(s-1)^7 &+(938714 \cdot 5^5)(s-1)^8 &+(3981241 \cdot 5^7)(s-1)^9 \\ &+(4589083 \cdot 5^8)(s-1)^{10} &-(2979334 \cdot 5^8)(s-1)^{11} &+(1938174 \cdot 5^8)(s-1)^{12} \end{aligned}$$

Whereas for $i = 2$ we obtain the following function modulo $5^{10}$:

$$\begin{aligned} \zeta_{p,2}(s) = 4163682 &-(3097056 \cdot 5)(s-1) &+(2446323 \cdot 5^2)(s-1)^2 &-(4645477 \cdot 5^3)(s-1)^3 \\ -(178876 \cdot 5^4)(s-1)^4 &-(1218884 \cdot 5^4)(s-1)^5 &-(1054906 \cdot 5^5)(s-1)^6 &-(3200479 \cdot 5^6)(s-1)^7 \\ +(914234 \cdot 5^7)(s-1)^8 &-(2434086 \cdot 5^8)(s-1)^9 &-(3550587 \cdot 5^8)(s-1)^{10} &+(1286609 \cdot 5^9)(s-1)^{11} \end{aligned}$$

What can we learn from the above computations? The best way is to experiment yourself, but just looking at the above data we may point out a few things that are worth recording.

- Note that all $p$-adic zeta functions for $i$ odd must vanish, as we observe here, since all Bernoulli numbers of odd index vanish. Since the $p$-adic zeta function is analytic, it can have at most finitely

many zeroes if it is non-zero, by the Weierstrass preparation theorem.

- The above examples illustrate very nicely the notion of the radius of convergence of these $p$-adic L-functions, which by its construction we can show to be $qp^{-1/(p-1)}$. This means that the order $\mathrm{ord}_p(a_n)$ of the $n$-th coefficient in the power series expansion should grow asymptotically as

$$\begin{array}{lcll} \mathrm{ord}_p(a_n) & \sim & n(p-2)/(p-1) & \text{if} \quad p>2 \\ \mathrm{ord}_p(a_n) & \sim & n & \text{if} \quad p=2 \end{array}$$

  which we see borne out in the data very nicely, especially when we compute more terms.

- We see that the residue of the pole that appears in $\zeta_{p,0}(s)$ at $s=1$ is indeed found experimentally to agree with $(p-1)/p$. This is very convincing in the second example, where we actually worked to a much higher $p$-adic precision than we displayed here. In the first example, it appears when we make the variable transformation $s \mapsto s+1$ to obtain the power series with respect to the variable $(s-1)$. Somewhat confusingly, we already see the constant term $1/2$ appearing in the power series expansion around $s=0$, which is not to be confused with the residue at $s=1$. In other words, we observe experimentally that

$$\zeta_{p,0}(0) = 1/2.$$

  Can you explain this?

**Example 3.** Let us compute the $p$-adic zeta functions for $p=37$, of which there are 36. Instead of viewing them as an analytic function of the variable $s$, we say that in fact we may view as an analytic function of the variable

$$T = (1+37)^{1-s} - 1$$

with respect to which it is an integral series in $\mathbf{Z}_{37}[\![T]\!]$ which converges in the open unit disk. This parameter is better suited to a study of the zeroes, about which easy information may be accessed through its Newton polygon. An explicit computation yields

$$\begin{array}{rcrrrrl} T\zeta_{p,0}\ (T) & = & 28552494 & +23400121\,T & +2718936\cdot 37\,T^2 & -5756294\,T^3 & (\mathrm{mod}\ 37^5, T^4) \\ \zeta_{p,2}\ (T) & = & 25436652 & +8029343\,T & +16870708\,T^2 & -7435444\,T^3 & (\mathrm{mod}\ 37^5, T^4) \\ \zeta_{p,4}\ (T) & = & -17811582 & +29378992\,T & +5926627\,T^2 & +14608764\,T^3 & (\mathrm{mod}\ 37^5, T^4) \\ \vdots & & \vdots & & & & \\ \zeta_{p,30}(T) & = & -28603965 & -6348916\,T & +1410038\cdot 37\,T^2 & +33287940\,T^3 & (\mathrm{mod}\ 37^5, T^4) \\ \zeta_{p,32}(T) & = & 10665687\cdot 37 & -28026406\,T & +1063943\,T^2 & +27968927\,T^3 & (\mathrm{mod}\ 37^5, T^4) \\ \zeta_{p,34}(T) & = & 14108187 & +2407041\,T & -30261768\,T^2 & -6096126\,T^3 & (\mathrm{mod}\ 37^5, T^4) \end{array}$$

Notice something quite remarkable here. All of the $p$-adic zeta functions (including the ones we did not show here) do not have a zero in their domain of convergence, except for $\zeta_{p,32}(s)$ which has a single zero $T_0$ with $\mathrm{ord}_p(T_0)=1$ by a Newton polygon argument. Note that the above computation does show this rigorously, in spite of it being only a numerical approximation. We may even compute an approximation of the zero itself, which yields:

$$T_0 = 25\cdot 37 + 20\cdot 37^2 + 5\cdot 37^3 + 7\cdot 37^4 + 33\cdot 37^5 + \ldots$$

**Example 4.** Now let $p = 157$. This is the smallest prime for which several of the Kubota–Leopoldt zeta functions have a zero in their domain. It concerns the following two:

$$\begin{array}{lcllll} \zeta_{p,62}(T) & = & -16646489529 \cdot 157 & -4338338876\,T & +20635641878\,T^2 & (\mathrm{mod}\ 157^5, T^3) \\ \zeta_{p,110}(T) & = & +2286894025 \cdot 157 & -36040391173\,T & +24461630362\,T^2 & (\mathrm{mod}\ 157^5, T^3) \end{array}$$

## 4.5. Exercises

(1) Show that for any integer $a$ prime to $p$ we have $F_a(T) \in \mathbf{Z}_p[\![T]\!]$ where, as above, we define

$$F_a(T) \ := \ \frac{1}{T} - \frac{a}{(1+T)^a - 1}.$$

(2) Choose an integer $a$ that generates the cyclic group $(\mathbf{Z}/p^2\mathbf{Z})^\times$.

- Prove that $a$ generates the cyclic group $(\mathbf{Z}/p^n\mathbf{Z})^\times$ for each $n \geq 1$.
- Prove that $[1] - [a]$ is not a zero divisor in the Iwasawa algebra $\Lambda(\mathbf{Z}_p^\times)$.
- Prove that $1/([1] - [a])$ is a pseudo-measure.

(3) Let $i$ be a non-zero residue class modulo $p-1$, and $\zeta_{p,i}(s)$ its associated Kubota–Leopoldt $p$-adic zeta function. Prove that $\zeta_{p,i}(s)$ has a zero if and only if

$$B_k \equiv 0 \pmod{p}, \qquad \forall k \equiv i \pmod{p-1}.$$

(4) Let $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \overline{\mathbf{Q}}$ be a Dirichlet character. Choose a primitive $N$-th root of unity $\zeta_N$ in $\overline{\mathbf{Q}}$ and define the function

$$f_\chi(t) := \frac{1}{G(\chi^{-1})} \sum_{a \,\in\, (\mathbf{Z}/N\mathbf{Z})^\times} \frac{\chi(a)}{e^t \zeta_N^a - 1}.$$

Prove that its Mellin transform is the Dirichlet L-function $L(\chi, s)$. In other words, prove that

$$L(\chi, s) = \frac{1}{\Gamma(s)} \int_0^\infty f_\chi(t) t^s \frac{dt}{t}.$$

CHAPTER 5

# Class numbers of cyclotomic fields

The study of $p$-adic L-functions has been a dominant theme in the second half of the 20th century, and has led to many spectacular applications in number theory. One of the most celebrated early discoveries is the connection with the class groups of the cyclotomic extensions

$$\mathbf{Q}(\zeta_{p^n})/\,\mathbf{Q}$$

where $\zeta_{p^n}$ is a primitive $p^n$-th root of unity. A very precise version of this relationship goes by the name of the *Iwasawa main conjecture*, after Kenkichi Iwasawa, the most important pioneer of this research field.

岩澤 健吉 Iwasawa Kenkichi

If we hearken back to the examples computed above, we will explore that it is no coincidence that **one** of the $p$-adic zeta functions had a simple zero when $p = 37$, and on the other hand, we have

$$|\ \mathrm{Cl}(\mathbf{Q}(\zeta_{37}))\ | \ = \ 37.$$

Even more strikingly, we found **two** $p$-adic L-functions with simple zeroes when $p = 157$, and on the other hand a formidable class number computation has revealed that

$$\begin{aligned} |\ \mathrm{Cl}(\mathbf{Q}(\zeta_{157}))\ | &= 562343277004018327670692 45 \\ &= 5 \cdot 13^2 \cdot 157^2 \cdot 1093 \cdot 1873 \cdot 418861 \cdot 3148601 \end{aligned}$$

In this chapter, we will explore some of the deep connections between $p$-adic zeta functions and the class groups of cyclotomic fields, which are studied in Iwasawa theory. This is not a formal part of the course material, and the further completion of these notes is not guaranteed. Rather, it is conditional on a large enough group of advanced students expressing their interest strongly enough, as well as their unquestionable dedication to a continuation of these proceedings, perhaps in the form of a collaborative seminar.

# Bibliography


[Boj74] R. Bojanic. A simple proof of Mahler's theorem on approximation of continuous functions of a $p$-adic variable by polynomials. *J. Number Theory*, 6:412–415, 1974. ↑13.

[Cas86] J. W. S. Cassels. *Local Fields*. Cambridge University Press, 1986. ↑11.

[Che33] C. Chevalley. La théorie des corps de classes pour les corps finis et les corps locaux (thesis). *J. Fac. Sci. Univ. Tokyo*, 2:365–474, 1933. ↑8.

[Che40] C. Chevalley. La théorie des corps de classes. *Ann. of Math.*, 41:394–418, 1940. ↑8.

[Col] P. Colmez. La fonction zeta $p$-adique. Notes du cours de M2. ↑9, 46.

[Col10] P. Colmez. Fonctions d'une variable $p$-adique. *Astérisque*, 330:13–59, 2010. ↑9, 29.

[CS06] J. Coates and R. Sujatha. *Cyclotomic fields and zeta values*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006. ↑9.

[DGS94] B. Dwork, G. Gerotto, and F. Sullivan. *An introduction to G-functions*, volume 133 of *Annals of Mathematics Studies*. Princeton University Press, 1994. ↑9, 11, 22.

[Die44] J. Dieudonné. Sur les fonctions continues $p$-adic. *Bull. Sci. Math.*, 68:79–95, 1944. ↑13.

[Dwo60] B. Dwork. On the rationality of the zeta function of an algebraic variety. *Amer. J. Math.*, 82(3):631–648, 1960. ↑9.

[Dwo62] B. Dwork. On the zeta function of a hypersurface. *Publ. Math. IHÉS*, (12):5–68, 1962. ↑9.

[Has23] H. Hasse. über die Darstellbarkeit von Zahlen durch quadratischen Formen im Körper der rationalen Zahlen. *J. Reine Angew. Math.*, 152:129–148, 1923. ↑8.

[Has24] H. Hasse. Darstellbarkeit von Zahlen durch quadratischen Formen in einem beliebigen algebraischen Zahlkörper. *J. Reine Angew. Math.*, 153:76–93, 1924. ↑8.

[Hen97] K. Hensel. über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresber. Deutsch. Math. Verein.*, 6(3):83–88, 1897. ↑8.

[Iwa52a] K. Iwasawa. Letter to j. dieudonné. Published in "Zeta functions in geometry (Tokyo 1990)", Adv. Stud. Pure Math. 21, 1952. ↑9, 41.

[Iwa52b] K. Iwasawa. A note on functions. *Proceedings of the ICM 1950*, 1952. ↑9, 41.

[Kat04] K. Kato. $p$-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004. ↑9.

[Ked07] K. Kedlaya. $p$-Adic cohomology: from theory to practice. *Arizona Winter School Notes*, 2007. ↑9.

[Ked10] K. Kedlaya. *$p$-adic differential equations*, volume 125 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2010. ↑9.

[Kim05] M. Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161:629–656, 2005. ↑9.

[Kim10] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑9.

[KL64] T. Kubota and H.-W. Leopoldt. Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.*, 214/215:328–339, 1964. ↑9, 41.

[Kob80] N. Koblitz. *$p$-Adic analysis: A short course on recent work*. Number 46 in London Math. Soc. Lecture Note Ser. Cambridge University Press, 1980. ↑29.

[Kob84] N. Koblitz. *$p$-Adic numbers, $p$-adic analysis, and zeta-functions*. Number 58 in Graduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition edition, 1984. ↑11, 29.

[Mah58] K. Mahler. An interpolation series for continuous functions of a $p$-adic variable. *J. Reine Angew. Math.*, 199:23–34, 1958. ↑13.

[Min84] H. Minkowski. Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten. Mémoires présentés par divers savants a l'Académie des Sciences de l'institut national de France, 1884. ↑8.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum. On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986. ↑9.

[MW84] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984. ↑9.

[Rub00] K. Rubin. *Euler systems*. Annals of Mathematics Studies. Princeton University Press, 2000. ↑9.

[RW] J. Rodrigues and C. Williams. An introduction to $p$-adic l-functions. Notes from a TCC Course. ↑9, 29.

[Ste10] E. Steinitz. Algebraische Theorie der Körper. *J. Reine Angew. Math.*, 137:167–309, 1910. ↑8.

[SU14] C. Skinner and E. Urban. The Iwasawa main conjectures for GL(2). *Invent. Math.*, 195(1):1–277, 2014. ↑9.

[Tat50] J. Tate. Fourier analysis in number fields, and Hecke's zeta-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 305–347, Washington, D.C., 1950. Thompson. ↑9, 41.

[Was97] L. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition edition, 1997. ↑7, 9, 11, 23, 29.