ESSENTIAL NUMBER THEORY

An introduction to p-adic L-functions

Joaquín Rodrigues Jacinto and Chris Williams

2025

vol. 4 no. 1

msp

Essential Number Theory
Vol. 4, No. 1, 2025
https://doi.org/10.2140/ent.2025.4.101

An introduction to p-adic L-functions

Joaquín Rodrigues Jacinto and Chris Williams

This is an expository introduction to p-adic L-functions and the foundations of Iwasawa theory. We focus on Kubota–Leopoldt's p-adic analogue of the Riemann zeta function, which we describe in three different ways. We first present a measure-theoretic (analytic) p-adic interpolation of special values of the Riemann zeta function. Next, we describe Coleman's (arithmetic) construction via cyclotomic units. Finally, we examine Iwasawa's (algebraic) construction via Galois modules over the Iwasawa algebra.

The *Iwasawa Main Conjecture*, now a theorem due to Mazur and Wiles, says that these constructions agree. We will state the conjecture precisely, and give a proof when p is a Vandiver prime (which conjecturally covers every prime). Throughout, we discuss generalisations of these constructions and their connections to modern research directions in number theory.

MSC2020: 11F33, 11F67, 11R23.
Keywords: p-adic L-functions, Iwasawa theory, Iwasawa Main Conjecture, Euler system, Kubota–Leopoldt, p-adic zeta function.

1. Introduction

The theory of L-functions, and their special values, has been central in number theory for 200 years. Their study spans from classical results, such as Gauss's class number formula and the proof of Dirichlet's theorem on primes in arithmetic progressions, to two major problems in mathematics: the Riemann hypothesis and the Birch and Swinnerton-Dyer conjecture. They are also central in the Langlands program, a vast project connecting the fields of number theory, geometry and representation theory.

The Birch and Swinnerton-Dyer conjecture is one example of a huge network of conjectures on the special values of L-functions, including the Beilinson, Deligne, and Bloch–Kato conjectures. At their heart, these problems relate complex analytic information — such as the order of vanishing and special values of meromorphic functions — to arithmetic data, such as invariants attached to algebraic varieties and Galois representations. A fruitful approach to these problems has been the use of p-adic methods, for p a prime number. Naively, one might consider the complex world a "bad" place to do arithmetic, as the integers are discrete in $\mathbb{C}$. This is not the case when one instead considers finite extensions of $\mathbb{Q}_p$. The p-adic setting brings extra flexibility and methods with which to attack these open problems, including p-adic L-functions, Euler systems, and Hida and Coleman families of modular/automorphic forms.

The study of p-adic properties of special values of L-functions is generally known as *Iwasawa theory*. In these notes, we give an introduction to this subject, focussing on perhaps the most fundamental of all L-functions: the Riemann zeta function $\zeta(s)$. We describe what a p-adic L-function is, construct it in this setting, and then describe Iwasawa's Main Conjecture[1] in this case. We try to anchor the theory in the context of current research activity, indicating how the various concepts we discuss have been generalised, and where the reader should turn next to learn more.

1.1. ***What do we cover in these notes?*** We now summarise the main results we cover. In Section 2, we give a broad introduction to p-adic L-functions, with an emphasis on how one can naturally move from complex to p-adic L-functions. We make this precise in our case of interest by stating some of the main results of Part I.

Our focus for the rest of the notes is on the Kubota–Leopoldt p-adic L-function (or p-adic zeta function), which is the p-adic analogue of the Riemann zeta function. We will see three constructions of this object, each of a different flavour, and describe the connections between them.

[1] Iwasawa's original conjecture was proved in full by Mazur and Wiles in [61]. However analogous conjectures, relating Selmer groups and p-adic L-functions, have been formulated in a large generality, for example for elliptic curves, modular forms, and beyond. These are also (somewhat confusingly) referred to as "Iwasawa Main Conjectures", even in the special cases (such as the one we consider) where they have been proved. We discuss such generalisations in Section 13.5 and Appendix B.

Part I is devoted to the construction and study of an *analytic* version of the Kubota–Leopoldt p-adic L-function. This has the clearest connection to the classical complex Riemann zeta function; it is a pseudomeasure ζ_p^{an} on $\mathbb{Z}_p^\times$ that interpolates the (rational numbers) $\zeta(1-k)$ for all positive integers k.[2]

- In Section 3, we describe some basic tools and results from p-adic analysis needed to parse the previous statement, including measures/pseudomeasures, Iwasawa algebras, and their connections to power series.
- In Section 4 we use the techniques developed in Section 3 to prove Theorem 2.13 (see also Theorem 4.1) on the existence of the Kubota–Leopoldt p-adic L-function ζ_p^{an}.
- In Section 5 we prove that ζ_p^{an} also interpolates special values of L-functions of Dirichlet characters of p-power conductor, and construct analogues for arbitrary Dirichlet characters.
- In Section 6, we describe a result of Leopoldt, showing that the values of the p-adic L-function of a nontrivial Dirichlet character 1 are related to logarithms of cyclotomic units, establishing one of the first instances of the p-adic Beilinson conjectures. The (untwisted) p-adic zeta function has a simple pole at $s = 1$; in Section 7, we prove an analogous result describing its residue.
- Finally in Section 8 we discuss an approach to p-adic L-functions based on the theory of families of Eisenstein series.

In Part II, we give two more constructions of the Kubota–Leopoldt p-adic L-function: *arithmetic* and *algebraic* versions.

- In Section 10, we give an arithmetic construction. The *cyclotomic units* are special elements in cyclotomic fields. As one considers the tower $\mathbb{Q}_p(\mu_{p^n})$ of cyclotomic extensions of $\mathbb{Q}_p$, the cyclotomic units fit together into a norm-compatible tower/system. The *Coleman map* is a map that attaches a p-adic measure to any such tower of units. Via this process, we show that to the cyclotomic units, one can naturally attach a pseudomeasure ζ_p^{arith} on $\mathbb{Z}_p^\times$. One connection between arithmetic and analysis, fully explained in Section 10, is that $\zeta_p^{\mathrm{an}} = \zeta_p^{\mathrm{arith}}$.
- In Sections 11 and 12, we deepen the arithmetic picture, respectively stating and proving *Iwasawa's theorem* describing the zeros of the p-adic zeta function via modules of cyclotomic units.
- In Section 13, we build on Iwasawa's theorem to give an algebraic construction of the Kubota–Leopoldt p-adic L-function, as an ideal ζ_p^{alg} in the Iwasawa algebra. This ideal arises from the structure of a Galois module over the Iwasawa algebra.

[2]The precise meaning of this will be clear later. Here the word interpolation is as in Lagrange's interpolation formula, i.e., a single object that hits certain specific values when evaluated at various points.

We also describe this module in terms of Selmer groups and discuss generalisations of the Main Conjecture.

The *Iwasawa Main Conjecture* says that the ideal ζ_p^{alg} is generated by the analytic/arithmetic Kubota–Leopoldt p-adic L-function, connecting the analytic, arithmetic and algebraic constructions, and ultimately connecting special complex L-values and Selmer groups. We state this precisely in Section 13, and prove it in the special case where p is a Vandiver prime.

The reader interested in taking a minimal path to the Iwasawa Main Conjecture can do so by reading the following sections: Section 2.1, Sections 2.3–2.4, Sections 3.2–3.6, Section 4, Sections 10.1–10.4, Sections 11 and 12, and Sections 13.1–13.4.

In Appendix B, we conclude with remarks on how the analytic, arithmetic and algebraic constructions above have been generalised to other situations, each spawning a field of study in its own right. We illustrate this by giving a sketch in the case of modular forms.

Further reading. For more information and detail on Part I of these notes, the reader could consult [52]. The construction of the p-adic zeta function we give here is based on Colmez's beautiful lecture notes [22].

Part II can serve as a prelude to a number of more advanced treatments, such as Rubin's (complete) proof of the Main Conjecture using the theory of Euler systems. We must mention the book of Coates and Sujatha [16], which inspired our original course, and whose aim was to present Rubin's proof. A canonical book in the field is [81], which introduces further topics in classical Iwasawa theory that there was not space to treat here. We give a flavour of such topics in Appendix A.

2. What is a p-adic L-function, and what should it do?

This introductory section aims to motivate the definition and study of p-adic L-functions. We start with a general discussion on complex L-functions and then lean slowly towards the p-adic world, focussing on the example of most importance to us in these lectures: the Riemann zeta function.

2.1. ***Classical L-functions.*** We first give some important examples of L-functions.

• The *Riemann zeta function*, the most famous and fundamental of all L-functions, is defined by

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1},$$

where the last product — an *Euler product* — runs over all prime numbers p and the second equality is a consequence of the unique prime factorisation of integers. The sum converges absolutely whenever s is a complex variable with real part

greater than 1, making ζ a well-defined holomorphic function in a right half-plane $\{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$. It can be meromorphically continued to the whole complex plane, and satisfies a *functional equation*, a symmetry relating the values $\zeta(s)$ and $\zeta(1-s)$.

- Let F be a number field. The *zeta function of* F is

$$\zeta_F(s) := \sum_{0 \neq I \subset \mathcal{O}_F} N(I)^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

where the sum is over all nonzero ideals in the ring of integers, and the product is over all nonzero prime ideals of K. Again, this sum converges absolutely for $\mathrm{Re}(s) > 1$, can be meromorphically continued to $\mathbb{C}$, and satisfies a functional equation relating $\zeta_F(s)$ and $\zeta_F(1-s)$. The existence of the Euler product again follows from unique factorisation.

- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. We extend χ to a function $\chi : \mathbb{Z} \to \mathbb{C}$ by setting $\chi(m) = \chi(m \pmod N)$ if m is prime to N, and $\chi(m) = 0$ otherwise. The L-function of χ is

$$L(\chi, s) := \sum_{n \geq 1} \chi(n) n^{-s} = \prod_{p} (1 - \chi(p) p^{-s})^{-1}.$$

Yet again, the above sum defining $L(\chi, s)$ converges for $\mathrm{Re}(s) > 1$, admits meromorphic continuation to $\mathbb{C}$ (analytic when χ is nontrivial), and satisfies a functional equation relating the values at s and $1-s$.

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. One can define an L-function

$$L(E, s) := \sum_{n \geq 1} a_n(E) n^{-s} = \prod_{p \nmid N} (1 - a_p(E) p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N} L_p(s),$$

where $a_p(E) = p + 1 - \#E(\boldsymbol{F}_p)$, and the $a_n(E)$ are defined recursively from the $a_p(E)$. The factors $L_p(s)$ at bad primes $p \mid N$ are defined as $L_p(s) = 1$ (resp. $(1 - p^{-s})^{-1}$, resp. $(1 + p^{-s})^{-1}$) if E has bad additive (resp. split multiplicative, resp. nonsplit multiplicative) reduction at p. The above sum defining the function $L(E, s)$ converges for $\mathrm{Re}(s) > \frac{3}{2}$, admits analytic continuation to $\mathbb{C}$, and satisfies a functional equation relating the values at s and $2-s$.

- Let

$$f = \sum_{n \geq 1} a_n(f) q^n \in S_k(\Gamma_0(N), \omega_f)$$

be a modular newform of weight k, level N and character ω_f. The L-function associated to f is given by

$$\begin{aligned} L(f, s) &:= \sum_{n \geq 1} a_n(f) n^{-s} \\ &= \prod_{p \nmid N} (1 - a_p(f) p^{-s} + \omega_f(p) p^{k-1-2s})^{-1} \prod_{p \mid N} (1 - a_p(f) p^{-s})^{-1}. \end{aligned}$$

This sum converges for $\mathrm{Re}(s) > \frac{1}{2}(k+1)$, admits analytic continuation to $\mathbb{C}$, and satisfies a functional equation relating the values at s and $k-s$. Such objects are introduced, and these results proved, in [30, Section 5].

The above examples share common features. The "arithmetic" L-functions of most interest to us should have the following basic properties (which can, nevertheless, be extremely deep):

(1) an Euler product converging absolutely in a right-half plane;

(2) a meromorphic continuation to the whole complex plane;

(3) a functional equation relating s and $k-s$ for some $k \in \mathbb{R}$.

Remark 2.1. More generally, let $\mathscr{G}_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ denote the absolute Galois group of $\mathbb{Q}$ and let $V \in \mathrm{Rep}_L \mathscr{G}_{\mathbb{Q}}$ be a p-adic Galois representation (i.e., a finite-dimensional vector space over a finite extension L of $\mathbb{Q}_p$ equipped with a continuous linear action of $\mathscr{G}_{\mathbb{Q}}$). One defines the global L-function of V as a formal Euler product

$$L(V,s) = \prod_{\ell} L_\ell(V,s)$$

of local factors. For $\ell \neq p$ a rational prime, the local factor at ℓ is defined as

$$L_\ell(V,s) := \det(\mathrm{Id} - \mathrm{Frob}_\ell^{-1} \ell^{-s} | V^{I_\ell})^{-1},$$

where Frob_ℓ denotes the arithmetic Frobenius at ℓ, and I_ℓ denotes the inertia group at ℓ (all described in [74, Section I]). At p, defining the local factor is considerably more complicated, requiring p-adic Hodge theory, as described in [6; 7]. In this case, one defines

$$L_p(V,s) := \det(\mathrm{Id} - \varphi^{-1} p^{-s} | \boldsymbol{D}_{\mathrm{cris}}(V))^{-1},$$

where $\boldsymbol{D}_{\mathrm{cris}}(V)$ denotes the crystalline module of $V|_{\mathscr{G}_{\mathbb{Q}_p}}$, equipped with a crystalline Frobenius denoted by φ.

When V is the representation attached to an arithmetic object,[3] the L-function of the representation is typically equal to the L-function attached to that object; for example, taking $V = \mathbb{Q}_p(\chi)$ (that is, V is 1-dimensional, with $\mathscr{G}_{\mathbb{Q}}$ acting through the character χ via class field theory), one recovers the Dirichlet L-functions described above. See [3] for further introductions to these topics.

2.2. *Motivating questions for Iwasawa theory.*

2.2.1. *Special values and arithmetic data.* There are deep results and conjectures relating special values of L-functions to important arithmetic information, of which a prototypical example is the following (see, for example, [64, Section 5]):

[3] For example, a number field, a Dirichlet character, an elliptic curve, a modular form, or much more generally — in the spirit of the Langlands program — an automorphic representation of a reductive group.

Theorem 2.2 (class number formula). *Let F be a number field with r_1 real embeddings, r_2 pairs of complex embeddings, w roots of unity, discriminant D, and regulator R. The zeta function ζ_F has a simple pole at $s = 1$ with residue*

$$\operatorname{res}_{s=1}\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}R}{w\sqrt{|D|}}h_F,$$

where h_F is the class number of F.

On the left-hand side, we have a special value of a complex meromorphic function, from the world of analysis. On the right-hand side, we have invariants attached to a number field, from the world of arithmetic. The class number formula thus provides a deep connection between two different fields of mathematics.

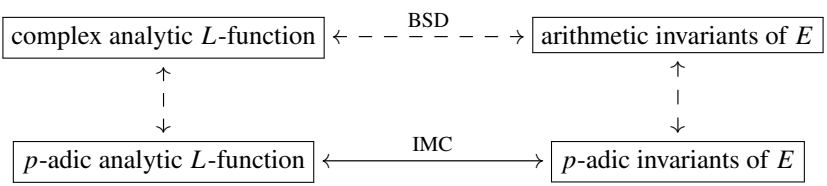
A second famous example of such a connection comes in the form of the *Birch and Swinnerton-Dyer* (*BSD*) *conjecture*. Let $E/\mathbb{Q}$ be an elliptic curve. The set of rational points $E(\mathbb{Q})$ forms a finitely generated abelian group and, based on computer computations, Birch and Swinnerton-Dyer predicted that

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

They also predicted a closer analogue of the class number formula: that the leading term of the L-function can be described in terms of arithmetic invariants attached to E.

Again, the left-hand side is from the world of analysis, the right-hand side is from the world of arithmetic, and this prediction is inherently surprising. The worlds are so different that the analytic L-function defies easy study using arithmetic properties of the elliptic curve. For example, when the conjecture was formulated, the left-hand side was not even known to exist: nobody had proved that $L(E, s)$ was defined at the value $s = 1$. This relies on analytic continuation of the L-function; such a proof would not follow for several decades, and even now the only proof we have goes through another deep connection between arithmetic and analysis, namely Wiles' modularity theorem.

2.2.2. *Iwasawa Main Conjectures.* One of the goals of Iwasawa theory is to seek and prove p-adic analogues of BSD and its generalisations, replacing complex analysis (which is poorly suited to arithmetic) with p-adic analysis (where arithmetic arises naturally). For each prime p, there is a p-adic *Iwasawa Main Conjecture* (IMC) for the elliptic curve E, relating a p-adic analytic L-function to certain p-adic arithmetic invariants of E:



One has many more tools available to attack the bottom row than the top, including Euler systems, p-adic families and eigenvarieties, p-adic Hodge theory and (φ, Γ)-modules, and more. As a result, the p-adic conjectures are much more tractable than their complex counterparts. Indeed, whilst BSD remains open beyond low-rank special cases, the IMC for elliptic curves has been proved much more widely by Skinner–Urban (see [77]), following work of Kato (see [47]). See also [32] for a recent summary of known results on the IMC for elliptic curves.

2.2.3. *Applications of p-adic methods to classical BSD.* Each new p-adic Iwasawa Main Conjecture that is proved brings the worlds of analysis and arithmetic a little closer together. They can also bring us closer to our original goal of, for example, BSD. Indeed, the current state-of-the-art results towards BSD have arisen as consequences of Iwasawa theory.

To elaborate, let us summarise some fundamental work (p-adic and otherwise) on BSD. There are two natural subquestions:

(a) We could try to prove that $\mathrm{ord}_{s=1} L(E, s) \leq \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$. A natural approach is to try to construct enough independent rational points on the elliptic curve. The theory of *Heegner points* is based on such an idea. A Heegner point in $E(\mathbb{Q})$ has infinite order if and only if $\mathrm{ord}_{s=1} L(E, s) = 1$. This yields the above inequality in this case.

(b) Conversely, we could try and prove that $\mathrm{ord}_{s=1} L(E, s) \geq \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$. In this case we want to bound the number of rational points. One method for trying to do this uses *Euler systems* attached to p-adic Galois representations (see [70] for a comprehensive introduction). The main application of Euler systems is in bounding certain Galois cohomology groups, known as *Selmer groups* (see Section 13.5), which are defined using local behaviour and can be viewed as a cohomological interpretation of the group of rational points on E. Indeed, let $Ш(E/\mathbb{Q})$ denote the *Tate–Shafarevich group* of E, a torsion abelian group that is conjecturally finite. If the subgroup $Ш(E/\mathbb{Q})[p^\infty] \leq Ш(E/\mathbb{Q})$ of elements with p-power order is finite, then the $\mathbb{Z}$-rank of $E(\mathbb{Q})$ is equal to the $\mathbb{Z}_p$-corank[4] of the p-Selmer group. In this case, bounding the p-Selmer group is equivalent to bounding $E(\mathbb{Q})$.

The ideas above have led to special cases of the conjecture; in particular, we now know it to be true (under some assumptions) when $\mathrm{ord}_{s=1} L(E, s) \leq 1$ due to work of Kolyvagin [51], Gross–Zagier [39] and Murty–Murty [63]. More recent Iwasawa-theoretic research building on the above has led to results towards the converse [76], as well as towards the leading-term formula [45].

We emphasise that whilst these methods have yielded important progress towards BSD, to date such results have been fundamentally limited to elliptic curves defined

[4]That is, the rank of the Pontryagin dual of the p-Selmer group; see [75, Section 2.1.4].

over $\mathbb{Q}$ and of rank ≤ 1. It is natural to try to execute such strategies in more general settings. More recently, the p-adic theory of *Stark–Heegner points*, a p-adic analogue of (a) initiated in [23], has been used with some success for elliptic curves over totally real fields. Heegner and Stark–Heegner points are beautifully summarised in [24] and [25]. A more recent overview of work on Heegner and Stark–Heegner points, and the relationships between them, is given in [9]. There has also been encouraging (and fundamentally p-adic) work on analogous questions in rank 2 and beyond; for example, see [12; 27].

Remark 2.3. The study of p-adic L-functions is intrinsic to (b), and they also feature prominently in the p-adic analogues of (a). Mazur, Tate and Teitelbaum formulated a p-adic BSD conjecture (see [62] and also [19]), which relates the order of vanishing of a p-adic L-function at $s = 1$ to the rank of the rational points of the elliptic curve, and expresses its principal coefficient in terms of arithmetic data in a manner analogous to the classical BSD conjecture (replacing the complex regulator by a p-adic regulator).

For an elliptic curve over $\mathbb{Q}$ of analytic rank 0, we know that the order of vanishing of its attached p-adic L-function is always 0 or 1. The possible extra zero, discussed in [37; 62], is known as a *trivial zero* of the p-adic L-function and is well understood in terms of local data attached to E at p. If the Tate–Shafarevich group $Ш(E/\mathbb{Q})$ is finite, the p-adic and classical BSD conjectures are equivalent in this case.

Under the assumption of the nondegeneration of the p-adic height pairing, the p-adic IMC for elliptic curves implies the p-adic BSD conjecture (see [72]).

2.2.4. *The IMC for the Riemann zeta function.* We mention the elliptic curve case only to motivate the study of p-adic L-functions and Iwasawa theory. In these notes, we will focus on a simpler example of the above picture, namely the Main Conjecture for the p-adic Riemann zeta function, as formulated by Iwasawa himself. Here the picture above is essentially complete; the full IMC is known for any prime p (thanks to [61] for p odd, and [83] for $p = 2$). We will (for odd p) construct the p-adic analogue of the zeta function on the way to stating the Main Conjecture, which we will prove for a special case.

2.3. ***The Riemann zeta function.*** Since the Riemann zeta function will be a central player in the rest of these notes, we take a brief detour to describe some of the classical theory surrounding it. We start with the following general result.

Theorem 2.4. *Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be a rapidly decreasing $\mathscr{C}^\infty$-function (i.e., such that f and all of its derivatives $f', f'', \ldots$ decay exponentially at infinity). Let*

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

be the usual gamma function. The function

$$L(f,s) := \frac{1}{\Gamma(s)} \int_0^\infty f(t) t^{s-1}\, dt, \quad s \in \mathbb{C},$$

which converges to a holomorphic function for $\mathrm{Re}(s) > 0$, *has an analytic continuation to the whole complex plane, and*

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

We call $L(f,s)$ *the* ***Mellin transform*** *of* f.

Proof. To show analytic continuation, we claim that when $\mathrm{Re}(s) > 1$, we have

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

where $f' = df/dt$. This is an exercise in integration by parts, using the identity $\Gamma(s) = (s-1)\Gamma(s-1)$, and gives the analytic continuation to all of $\mathbb{C}$ by iteration. Finally, iterating the same identity $n+1$ times shows that

$$L(f,-n) = (-1)^{n+1} L(f^{(n+1)}, 1) = (-1)^{n+1} \int_0^\infty f^{(n+1)}(t)\, dt = (-1)^n f^{(n)}(0)$$

from the fundamental theorem of calculus, giving the result. □

We would like to use the Mellin transform to recover the Riemann zeta function and its properties. For this, we pick a specific choice of f, namely, we let

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

the generating function for the Bernoulli numbers B_n.

Remark 2.5. The Bernoulli numbers are highly combinatorial, and they satisfy recurrence relations that ensure they are *rational* numbers; for example, the first few are

$$B_0 = 1, \quad B_1 = -\tfrac{1}{2}, \quad B_2 = \tfrac{1}{6}, \quad B_3 = 0, \quad B_4 = -\tfrac{1}{30}, \quad \ldots.$$

For $k \geq 3$ odd, $B_k = 0$.

We want to plug this function into Theorem 2.4, and for this, we require:[5]

Lemma 2.6. *The function* $f(t)$ *and all of its derivatives decay exponentially at infinity.*

Proof. For $t > 0$, we may expand $f(t)$ as a geometric series

$$f(t) = t(e^{-t} + e^{-2t} + e^{-3t} + \cdots) =: tF(t).$$

[5]We thank Keith Conrad for pointing out this proof.

Note $f'(t) = F(t) + tF'(t)$ and $f''(t) = 2F'(t) + tF''(t)$; arguing inductively we see

$$\begin{aligned} f^{(n)}(t) &= nF^{(n-1)}(t) + tF^{(n)}(t) \\ &= n(-1)^{n-1}(e^{-t} + 2^{n-1}e^{-2t} + 3^{n-1}e^{-3t} + \cdots \quad) \\ &\qquad + (-1)^n t(e^{-t} + 2^n e^{-2t} + 3^n e^{-3t} + \cdots) \\ &\sim (-1)^n te^{-t} \qquad \text{as } t \to \infty. \end{aligned}$$

This decays exponentially. □

Lemma 2.7. *For the choice of f as above, we have*

$$(s-1)\zeta(s) = L(f, s-1).$$

Proof. Substituting t for nt and rearranging in (2-1) defining $\Gamma(s)$, we obtain

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

Now, when $\mathrm{Re}(s)$ is sufficiently large, we can write

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \frac{1}{\Gamma(s)} \sum_{n\geq 1} \int_0^\infty e^{-nt} t^{s-1}\, dt = \frac{1}{\Gamma(s)} \int_0^\infty \Big(\sum_{n\geq 1} e^{-nt} \Big) t \cdot t^{s-2}\, dt,$$

and the result now follows from the identity

$$\frac{1}{e^t - 1} = \sum_{n\geq 1} e^{-nt}.$$ □

From the theorem above, we immediately obtain:

Corollary 2.8. *For $n \geq 0$, we have*

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

In particular, $\zeta(-n) \in \mathbb{Q}$ for $n \geq 0$, and $\zeta(-n) = 0$ if $n \geq 2$ is even.

2.4. ***p-adic L-functions.*** As explained in the introduction, p-adic L-functions are excellent tools to study special values of L-functions. In this section, we explain what a p-adic L-function is and the properties it should satisfy.

2.4.1. *p-adic L-functions, a first idea.* The complex ζ-function is a complex analytic function

$$\zeta : \mathbb{C} \to \mathbb{C}$$

which is rational at negative integers. Since $\mathbb{Z}$ is a common subset of both $\mathbb{C}$ and $\mathbb{Z}_p \subseteq \mathbb{C}_p$, it is natural to ask if there exists a function

$$\zeta_p : \mathbb{Z}_p \to \mathbb{C}_p$$

that is "p-adic analytic" (in some sense to be defined) and which agrees with the complex L-function at negative integers in the sense that

$$\zeta_p(1-n) = (*) \cdot \zeta(1-n), \tag{2-2}$$

for some explicit factor $(*)$. We would say that such a function "p-adically interpolates the special values of $\zeta(s)$". Ideally, one would like these properties to uniquely characterise ζ_p.

2.4.2. *Ideles, measures and Tate's thesis.* In practice, there is no *single* analytic function on $\mathbb{Z}_p$ that interpolates all of the special values,[6] as we shall explain in Section 5.3. Instead, a better way of thinking about L-functions is to use a viewpoint initiated by Tate in his thesis [78] (and later independently by Iwasawa [43]). This viewpoint sees L-functions as *measures on ideles*, and allows one to package together *all* Dirichlet L-functions, including the Riemann zeta function, into a single object. We will give a brief account of the classical theory here, but for fuller accounts, one should consult the references above.

We begin with some observations on characters.

Proposition 2.9. *The following assertions hold.*

(i) *There is an identification between Dirichlet characters χ and continuous characters*

$$\chi : \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times \to \mathbb{C}^\times,$$

where the source is equipped with the product of the ℓ-adic topologies.

(ii) *There is an identification of $\mathbb{C}$ with the space $\mathrm{Hom}_{\mathrm{cts}}(\mathbb{R}_{>0}, \mathbb{C}^\times)$ of continuous multiplicative characters by sending s to $x \mapsto x^s$.*

In particular, each pair (χ, s), where χ is a Dirichlet character and $s \in \mathbb{C}$, corresponds to a (unique) continuous character

$$\kappa_{\chi,s} : \mathbb{R}_{>0} \times \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times \to \mathbb{C}^\times, \quad (x, y) \mapsto x^s \chi(y),$$

where we equip the source with the product topology, and all continuous characters on this group are of this form.

Proof. First, observe that any Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ induces naturally a character

$$\chi : \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times \to \mathbb{C}^\times.$$

[6] Rather, there are $p-1$ different analytic functions $\zeta_{p,1}, \ldots, \zeta_{p,p-1}$ on $\mathbb{Z}_p$, and $\zeta_{p,i}$ interpolates only the values $\zeta(1-k)$ for which $k \equiv i \pmod{p-1}$.

Indeed, suppose first that $N = \ell^n$ is a power of some prime ℓ, with $n \geq 1$. As $(\mathbb{Z}/\ell^n\mathbb{Z})^\times \cong \mathbb{Z}_\ell^\times/(1+\ell^n\mathbb{Z}_\ell)$, we can lift χ from $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ to a function on $\mathbb{Z}_\ell^\times$. The case for general N follows from the Chinese remainder theorem. Conversely, any continuous character $\chi : \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times \to \mathbb{C}^\times$ must factor through a finite quotient $(\mathbb{Z}/N\mathbb{Z})^\times$ of $\prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times$ for some large enough N. Indeed, the image of a sufficiently small open neighbourhood

$$U_N := \left\{ x \in \prod_\ell \mathbb{Z}_\ell^\times : x \equiv 1 \pmod{N} \right\}$$

of 1 is contained in $\{z \in \mathbb{C} : |z-1| < 1\}$. This image is a compact subgroup, but the only compact subgroup of the latter set is $\{1\}$. Hence χ is trivial on U_N, and factors through $\left(\prod_\ell \mathbb{Z}_\ell^\times\right)/U_N = (\mathbb{Z}/N\mathbb{Z})^\times$, inducing a Dirichlet character. These two procedures are inverse to each other, showing the first point.

We now prove the second point. For $s \in \mathbb{C}$, the function $x \mapsto x^s$ is visibly a continuous character on $\mathbb{R}_{>0}$. We want to show that all such characters are of this form. After taking a logarithm, this is equivalent to showing that all continuous homomorphisms (of additive groups) $g : \mathbb{R} \to \mathbb{C}$ are of the form $g(x) = xg(1)$, which is shown by directly computing the values of g on $\mathbb{Q}$ and extending by continuity. □

The product space in Proposition 2.9 is more usually written using ideles.

Definition 2.10. Define the *ideles* $\boldsymbol{A}^\times$ of $\mathbb{Q}$ to be

$$\begin{aligned} \boldsymbol{A}^\times = \boldsymbol{A}_{\mathbb{Q}}^\times &:= \mathbb{R}^\times \times \prod_{\ell \text{ prime}}{}' \mathbb{Q}_\ell^\times \\ &= \{(x_\mathbb{R}, x_2, x_3, x_5, \dots) : x_\ell \in \mathbb{Z}_\ell^\times \text{ for all but finitely many } \ell\}. \end{aligned}$$

(The prime on the product denotes *restricted product*, which indicates the almost everywhere integral property in the definition.) The ideles form a topological ring equipped with the restricted product topology, namely the topology with a basis of open neighbourhoods given by subsets of the form $U \times \prod_\ell U_\ell$ with $U \subseteq \mathbb{R}^\times$ and $U_\ell \subseteq \mathbb{Q}_\ell^\times$ open subsets such that $U_\ell = \mathbb{Z}_\ell^\times$ for almost all primes ℓ. The units $\mathbb{Q}^\times$ embed diagonally in $\boldsymbol{A}^\times$ (that is, via $x \mapsto (x, x, x, \dots)$) and we have:

Proposition 2.11 (strong approximation). *There is a topological isomorphism*

$$\mathbb{Q}^\times \backslash \boldsymbol{A}^\times \cong \mathbb{R}_{>0} \times \prod_{\ell \text{ prime}} \mathbb{Z}_\ell^\times.$$

Hence all continuous characters

$$\mathbb{Q}^\times \backslash \boldsymbol{A}^\times \to \mathbb{C}^\times$$

are of the form $\kappa_{\chi,s}$ as above, where χ is a Dirichlet character and $s \in \mathbb{C}$.

Proof. See [34, Proposition I.4.6]. □

Remark 2.12. The space $\mathbb{Q}^\times\backslash\boldsymbol{A}^\times$ is the *idele class group* of $\mathbb{Q}$, and features prominently in the idelic formulation of class field theory.

By the identification of $\mathbb{C}$ with $\mathrm{Hom}_{\mathrm{cts}}(\mathbb{R}_{>0},\mathbb{C}^\times)$ one can view ζ as a function

$$\zeta:\mathrm{Hom}_{\mathrm{cts}}(\mathbb{R}_{>0},\mathbb{C}^\times)\to\mathbb{C},\quad [x\mapsto x^s]\mapsto\zeta(s).$$

But now we can consider *all* complex Dirichlet L-functions *at once* via the function

$$L:\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Q}^\times\backslash\boldsymbol{A}^\times,\mathbb{C}^\times)\to\mathbb{C},\quad \kappa_{\chi,s}\mapsto L(\chi,s). \tag{2-3}$$

In the framework of Tate, this function L can be viewed as integrating $\kappa_{\chi,s}$ against the *Haar measure* on $\mathbb{Q}^\times\backslash\boldsymbol{A}^\times$. In Tate's thesis, he showed properties such as the analytic continuation and functional equations of Dirichlet L-functions using harmonic analysis on measures. Indeed, the idelic formulation gives a beautiful conceptual explanation for the appearance of the Γ-functions and powers of $2\pi i$ in the functional equation of the zeta function; these factors form the "Euler factor at the archimedean place". The measure-theoretic perspective has proven to be a powerful method of defining and studying automorphic L-functions in wide generality.

2.4.3. *p-adic L-functions via measures.* To obtain a p-adic version of this picture, by analogy with (2-3), a natural thing to do is to consider $\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Q}^\times\backslash\boldsymbol{A}^\times,\mathbb{C}_p^\times)$ (that is, replacing $\mathbb{C}$ with $\mathbb{C}_p$). Again, by strong approximation, an element of this space corresponds to a $\mathbb{C}_p$-valued character on $\mathbb{R}_{>0}\times\prod\mathbb{Z}_\ell^\times$. Since $\mathbb{R}_{>0}$ is connected and $\mathbb{C}_p$ is totally disconnected, the restriction of any such character to $\mathbb{R}_{>0}$ is trivial. Also using topological arguments we find that the restriction to $\prod_{\ell\neq p}\mathbb{Z}_\ell^\times$ factors through a finite quotient, so gives rise to some Dirichlet character of conductor prime to p. This leaves the restriction to $\mathbb{Z}_p^\times$, i.e., $\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times,\mathbb{C}_p^\times)$, which is by far the most interesting part.

In particular, in the spirit of (2-2), we look for a "p-adic analytic" function

$$\zeta_p:\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times,\mathbb{C}_p^\times)\to\mathbb{C}_p$$

which "sees" the special values of $\zeta(s)$ in the sense that

$$\zeta_p(x\mapsto x^k)=(*)\cdot\zeta(1-k),\quad k\geq 1$$

for an explicit factor $(*)$.

In Section 3, we will develop the appropriate notion of "p-adic analytic" object in this setting: p-adic measures[7] (and pseudomeasures) on $\mathbb{Z}_p^\times$. Then in Section 4 we will prove:

[7]It is not immediately obvious why we describe these as analytic, but in the background such objects can be described in terms of *rigid analysis*, a p-adic analogue of complex analysis. Whilst we will not explicitly use rigid analysis, the connection is described precisely in Remark 3.47.

In this language, measures correspond to analytic functions, and pseudomeasures to meromorphic functions with at worst simple poles.

Theorem 2.13 (Kubota–Leopoldt; Iwasawa). *There is a unique pseudomeasure ζ_p on $\mathbb{Z}_p^\times$ such that, for all $k > 0$,*

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

Remark 2.14. Note that the factor $(1 - p^{k-1})$ is the inverse of the factor at the prime p of the product formula $\zeta(s) = \prod_\ell (1 - \ell^{-s})^{-1}$, evaluated at $s = 1 - k$. So, even though the Euler product does not converge at $s = 1 - k$, Theorem 2.13 morally says that, removing the factor at p from the Euler product formula, one can p-adically interpolate the Riemann zeta function. This is a general phenomenon appearing in the theory of p-adic L-functions.

From the pseudomeasure ζ_p, we can build $p-1$ (meromorphic) functions on $\mathbb{Z}_p$, each satisfying a partial version of (2-2). If we stick with the measure-theoretic approach, however, we have much more. The following result illustrates this power. In constructing ζ_p, we use only values of $\zeta(s)$, without referring to Dirichlet characters at all. However, we also have:

Theorem 2.15. *Let χ be a Dirichlet character of conductor p^n, $n \geq 0$, viewed as a locally constant character on $\mathbb{Z}_p^\times$.*[8] *Then, for all $k > 0$,*

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

Thus ζ_p also interpolates all the negative integer values $L(\chi, -k)$ for *all* Dirichlet L-functions of p-power conductor. This is very surprising, since a priori one constructs ζ_p using only information about the untwisted special L-values.

To complete the picture given in Section 2.4.2, one also considers Dirichlet characters of conductor prime to p. Similar ideas can also be used to show:

Theorem 2.16. *Let $D > 1$ be any integer coprime to p, and let η denote a (primitive) Dirichlet character of conductor D. There exists a unique measure ζ_η on $\mathbb{Z}_p^\times$ with the following interpolation property: for all primitive Dirichlet characters χ with conductor p^n for some $n \geq 0$, we have, for all $k > 0$,*

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot \zeta_\eta = (1 - \chi\eta(p)p^{k-1})L(\chi\eta, 1-k).$$

Remark 2.17. Let $(\mathbb{Z}/D\mathbb{Z})^{\times\wedge}$ denote the space of characters on $(\mathbb{Z}/D\mathbb{Z})^\times$. The measures given by Theorem 2.16 can be seen as functions on

$$\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times) \times (\mathbb{Z}/D\mathbb{Z})^{\times\wedge},$$

[8] That is, a character on $\mathbb{Z}_p^\times$ factoring through $\mathbb{Z}_p^\times/(1 + p^n\mathbb{Z}_p)$ for some large enough n.

and they are compatible with respect to the natural maps $(\mathbb{Z}/E\mathbb{Z})^{\times\wedge} \to (\mathbb{Z}/D\mathbb{Z})^{\times\wedge}$ for $E|D$. This shows that they define a function on

$$\begin{aligned}\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times) \times \varinjlim_{(D,p)=1} (\mathbb{Z}/D\mathbb{Z})^{\times\wedge} &= \mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times) \times \left(\prod_{\ell\neq p} \mathbb{Z}_\ell^\times\right)^\wedge \\ &= \mathrm{Hom}_{\mathrm{cts}}(\mathbb{Q}^\times \backslash \boldsymbol{A}^\times, \mathbb{C}_p^\times).\end{aligned}$$

In other words, they give a measure on the idele class group of $\mathbb{Q}$.

Remark 2.18. Note that if $k \equiv \ell \pmod{p^{m-1}(p-1)}$, then $x^k \equiv x^\ell \pmod{p^m}$ for any $x \in \mathbb{Z}_p^\times$. In particular, for any Dirichlet character η of conductor prime to p, these theorems tell us that the special values of L-functions satisfy congruences

$$(1-\eta(p)p^{k-1})L(\eta, 1-k) \equiv (1-\eta(p)p^{\ell-1})L(\eta, 1-\ell) \pmod{p^m}.$$

For the Riemann zeta function, these are the (*generalised*) *Kummer congruences*, which played a role in his classification of irregular primes, and which provided significant motivation for Theorem 2.13. This gives an alternative way of viewing p-adic L-functions: as p-adic analytic objects that package together systematic congruences between L-values.

Part I: The Kubota–Leopoldt p-adic L-function

In this part, we give constructions of the Kubota–Leopoldt p-adic L-function and the p-adic L-functions of Dirichlet characters. In Section 3, we introduce the necessary formalism of p-adic (pseudo)measures and Iwasawa algebras, and — via Mahler transforms — their relationship with spaces of power series. This section sets up language and correspondences we will use throughout the rest of these notes.

In Section 4, we construct a pseudomeasure on $\mathbb{Z}_p^\times$ that interpolates the values of the Riemann zeta function at negative integers. In Section 5, we show moreover that this pseudomeasure interpolates the values $L(\chi, -k)$ for $k > 0$ and χ any Dirichlet character of p-power conductor. Further, if η is a Dirichlet character of conductor prime to p, we construct a measure on $\mathbb{Z}_p$ that interpolates the values $L(\chi\eta, -k)$ for the same range of k and χ. In Section 5.3 we rephrase the construction in terms of analytic functions on $\mathbb{Z}_p$ via the Mellin transform. In Sections 6 and 7 we describe the behaviour at $s = 1$ of these analytic functions, a point outside the region of interpolation. Finally, in Section 8 we discuss how these results can be used to construct the p-adic family of Eisenstein series, a prototype for Hida and Coleman families.

3. Measures and Iwasawa algebras

In this section, we formally develop the theory of p-adic analysis that we will be using in the sequel. Whilst some of the results may appear a little dry in

isolation, fluency in the measure-theoretic language will greatly help us simplify later calculations that would otherwise be very technical.

We start in a general setting, letting G be a profinite abelian group, and introducing p-adic measures on G. We then show that the space of p-adic measures is isomorphic to the Iwasawa algebra of G. Additionally, in the special case where $G = \mathbb{Z}_p$, we give a third perspective, showing that the Iwasawa algebra is also isomorphic to a space of power series via the Mahler transform. After developing a measure-theoretical toolkit for later use, we introduce pseudomeasures. We then conclude by discussing generalisations, including locally analytic distributions and rigid analytic functions.

Throughout, we fix a finite extension L of $\mathbb{Q}_p$, with the p-adic valuation normalised so that $v_p(p) = 1$; this will be the coefficient field. We write $\mathcal{O}_L$ for its ring of integers.

3.1. ***Preliminaries on p-adic Banach spaces.*** We first collect some technical general definitions to anchor our discussions. This is intended only to make precise some of the notions we subsequently use, and the reader comfortable with p-adic Banach spaces and orthonormal bases may skip to Section 3.2. For more details, see [20, Section I.1].

Definition 3.1. Let B be an L-vector space. A *valuation* on B is a function $v : B \to \mathbb{R} \cup \{+\infty\}$ such that

(i) $v(x) = +\infty$ if and only if $x = 0$;

(ii) $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in B$; and

(iii) $v(\lambda x) = v_p(\lambda) + v(x)$ for all $\lambda \in L, x \in B$.

Such a valuation induces a norm (hence a topology) on B.

Definition 3.2. An *L-Banach space* is a complete topological L-vector space B whose topology is induced from a valuation v.

Definition 3.3. (1) Let I be a set, and $\ell^0_\infty(I, L)$ the set of sequences $(a_i)_{i\in I}$ in L that tend to 0 in the sense that for all $\varepsilon > 0$, we have $|a_i|_L < \varepsilon$ for all but finitely many i. This is naturally an L-Banach space with valuation $v((a_i)_i) = \inf_{i\in I} v_p(a_i)$.

(2) If B is an L-Banach space, an *orthonormal basis* of B is a collection $(e_i)_{i\in I}$, for some set I, such that we have an isometry

$$\ell^0_\infty(I, L) \to B, \quad (a_i)_{i\in I} \mapsto \sum_{i\in I} a_i e_i.$$

Remark 3.4. By [20, Proposition I.1.5], if B is an L-Banach space with valuation v_B, and $v_B(B) = v_p(L)$, then B admits an orthonormal basis.

We shall also be concerned with dual spaces. If B is a topological L-vector space, denote its continuous linear dual by

$$B^* := \mathrm{Hom}_{\mathrm{cts}}(B, L).$$

If B is an L-Banach space, there are two natural topologies on B^*.

Definition 3.5. Let B be an L-Banach space and B^* its continuous dual.

- The *strong topology* is induced by the natural dual valuation v^*, where

$$v^*(\mu) := \inf_{x \in B} \big(v_p(\mu(x)) - v(x) \big).$$

This is the coarsest topology such that a sequence $(\mu_j)_j \subset B^*$ converges if and only if it converges uniformly (in the usual sense of continuous functions on B).

- The *weak topology* is induced by the family of semivaluations[9] $\{v_x : x \in B\}$, where

$$v_x(\mu) := v_p(\mu(x)).$$

This is the topology of pointwise convergence, the coarsest such that a sequence $(\mu_j)_j \subset B^*$ converges if and only if $\mu_j(x)$ converges for all $x \in B$.

Remark 3.6. The dual B^* is complete with both of these topologies. However generally it is an L-Banach space only for the strong topology, whilst B is reflexive (canonically isomorphic to its double continuous dual) only when B^* is equipped with the weak topology.

3.2. ***p-adic measures.*** We now return to our specific setting, and introduce the p-adic measures fundamental to our story. Let G be a profinite abelian group; the examples $G = \mathbb{Z}_p$ or $G = \mathbb{Z}_p^\times$ are of most interest to us.

Definition 3.7. We denote by $\mathscr{C}(G, L)$ the space of continuous functions $\phi : G \to L$. We equip this space with a valuation

$$v_{\mathscr{C}}(\phi) = \inf_{x \in G} v_p(\phi(x)), \quad \phi \in \mathscr{C}(G, L),$$

noting this is well defined as G is compact (hence ϕ is bounded).

This valuation induces the sup norm on $\mathscr{C}(G, L)$, and endows it with the structure of an L-Banach space, in the sense of Definition 3.2.

Definition 3.8. We define the space $\mathscr{M}(G, L)$ of *L-valued measures on G* as the continuous linear dual $\mathscr{C}(G, L)^* = \mathrm{Hom}_{\mathrm{cts}}(\mathscr{C}(G, L), L)$. If $\phi \in \mathscr{C}(G, L)$ and $\mu \in \mathscr{M}(G, L)$, the evaluation of μ at ϕ will be denoted by

$$\int_G \phi(x) \cdot \mu(x),$$

or by $\int_G \phi \cdot \mu$ if the variable of integration is clear from the context.

[9] That is, functions v that satisfy (ii) and (iii) of Definition 3.1, but not necessarily (i).

We say that an element $\mu \in \mathscr{M}(G, L)$ is an *$\mathscr{O}_L$-valued measure*, and write $\mu \in \mathscr{M}(G, \mathscr{O}_L)$, if $\int_G \phi \cdot \mu \in \mathscr{O}_L$ for every $\mathscr{O}_L$-valued function ϕ. Since measures are continuous (or equivalently, bounded), we have $\mathscr{M}(G, L) = \mathscr{M}(G, \mathscr{O}_L) \otimes_{\mathscr{O}_L} L$. We will be mainly concerned with $\mathscr{O}_L$-valued functions and measures.

Remark 3.9. All parts of Definitions 3.7 and 3.8 apply identically if we replace G with any subset $X \subset G$ equipped with the subspace topology (noting that X no longer need be a group).

The following simple example will be crucial in later sections.

Example 3.10. For any $g \in G$, the *Dirac measure* $\delta_g \in \mathscr{M}(G, \mathscr{O}_L)$ is the linear functional "evaluation at g", that is, the measure defined by

$$\delta_g : \mathscr{C}(G, \mathscr{O}_L) \to \mathscr{O}_L, \quad \phi \mapsto \phi(g).$$

We will give a number of alternative descriptions of p-adic measures. Firstly, we make the following simplifications.

Remark 3.11. Let $\mathscr{C}^{\mathrm{lc}}(G, \mathscr{O}_L)$ denote the space of locally constant functions $G \to \mathscr{O}_L$; this is a dense subspace of the continuous functions $\mathscr{C}(G, \mathscr{O}_L)$. Indeed, any continuous function $\phi \in \mathscr{C}(G, \mathscr{O}_L)$ can be p-adically approximated by its locally constant truncations $\phi_n(x) = \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})} \phi(a) \mathbf{1}_{a+p^n\mathbb{Z}_p}(x)$, where $\mathbf{1}_{a+p^n\mathbb{Z}_p}(x)$ denotes the characteristic function of $a + p^n\mathbb{Z}_p$. Let

$$\mathscr{M}^{\mathrm{lc}}(G, \mathscr{O}_L) := \mathscr{C}^{\mathrm{lc}}(G, \mathscr{O}_L)^*$$

be the continuous dual, the space of "locally constant measures on G". We claim restriction from $\mathscr{C}$ to $\mathscr{C}^{\mathrm{lc}}$ defines a canonical isomorphism

$$\mathscr{M}(G, \mathscr{O}_L) \xrightarrow{\sim} \mathscr{M}^{\mathrm{lc}}(G, \mathscr{O}_L). \tag{3-1}$$

To see this, we write down an inverse. Suppose $\mu^{\mathrm{lc}} \in \mathscr{M}^{\mathrm{lc}}(G, \mathscr{O}_L)$, and let $\phi \in \mathscr{C}(G, \mathscr{O}_L)$. Using density, choose a sequence $\phi_n \in \mathscr{C}^{\mathrm{lc}}(G, \mathscr{O}_L)$ with $\phi_n \to \phi$ and define

$$\int_G \phi \cdot \mu := \lim_{n \to \infty} \int_G \phi_n \cdot \mu^{\mathrm{lc}}.$$

By continuity, the limit is well defined and independent of the choice of ϕ_n, and hence we obtain a well-defined measure $\mu \in \mathscr{M}(G, \mathscr{O}_L)$. This gives a map

$$\mathscr{M}^{\mathrm{lc}}(G, \mathscr{O}_L) \to \mathscr{M}(G, \mathscr{O}_L)$$

visibly inverse to (3-1).

Henceforth we drop the notation μ^{lc} and just write μ.

Remark 3.12. We have an identification of $\mathscr{M}^{\mathrm{lc}}(G, \mathscr{O}_L)$ with the space of additive functions

$$\mu : \{\text{open compact subsets of } G\} \to \mathscr{O}_L. \tag{3-2}$$

Indeed, if $\mu \in \mathscr{M}^{\mathrm{lc}}(G, \mathscr{O}_L)$ and $U \subset G$ is an open compact set, one defines $\mu(U) := \int_G \mathbf{1}_U(x) \cdot \mu(x)$, where $\mathbf{1}_U(x)$ denotes the characteristic function of U.

Conversely, let μ be such a function and let $\phi \in \mathscr{C}^{\mathrm{lc}}(G, \mathscr{O}_L)$. We will see how to integrate ϕ against μ. As ϕ is locally constant, there is some open subgroup H of G such that ϕ can be viewed as a function on G/H. We define the integral of ϕ against μ to be

$$\int_G \phi \cdot \mu := \sum_{[a] \in G/H} \phi(a)\mu(aH).$$

Combining Remarks 3.11 and 3.12, we have an identification of $\mathscr{M}(G, \mathscr{O}_L)$ with the space of additive functions on the open compact subsets of G.

Remark 3.13. On $\mathbb{Z}_p$, we have a (real-valued) Haar measure defined so that open compact subsets of the form $a + p^n\mathbb{Z}_p$ have measure p^{-n}. Whilst this is probably the most natural measure one might consider on $\mathbb{Z}_p$, observe that this is *not* a p-adic measure, as it is not p-adically bounded!

Example 3.14. For $g \in G$, the Dirac measure δ_g from Example 3.10 corresponds to the function $\widetilde{\delta}_g$ on open compact subsets given by

$$\widetilde{\delta}_g(X) = \begin{cases} 1 & \text{if } g \in X, \\ 0 & \text{if } g \notin X, \end{cases}$$

as can be seen directly from the identification above.

3.3. ***The Iwasawa algebra.*** We will now express measures in algebraic terms. As a prototype, we recall a useful fact from representation theory. If G is a finite abelian group, let $\mathscr{C}(G, \mathbb{Z})$ be the space of functions $G \to \mathbb{Z}$, and $\mathscr{M}(G, \mathbb{Z})$ its dual, the space of "continuous measures" on G (when we equip G with the discrete topology). For any $g \in G$ we have the Dirac measure $\delta_g \in \mathscr{M}(G, \mathbb{Z})$ given by $\delta_g(\phi) := \phi(g)$, as in Example 3.10. Then recall the following classical result.

Proposition 3.15. *If G is a finite abelian group, the map $[g] \mapsto \delta_g$ induces an isomorphism between the group algebra $\mathbb{Z}[G]$ and $\mathscr{M}(G, \mathbb{Z})$.*

When G is profinite abelian, we have an analogous p-adic result after replacing the group algebra with its profinite completion, the Iwasawa algebra.

Proposition 3.16. *We have an natural isomorphism*

$$\mathscr{M}(G, \mathscr{O}_L) \cong \varprojlim_H \mathscr{O}_L[G/H],$$

where the limit is over all open subgroups of G.

Proof. By Remark 3.11, we have a canonical isomorphism

$$\mathscr{M}(G, \mathscr{O}_L) \cong \mathscr{M}^{\mathrm{lc}}(G, \mathscr{O}_L) = \mathrm{Hom}_{\mathrm{cts}}(\mathscr{C}^{\mathrm{lc}}(G, \mathscr{O}_L), \mathscr{O}_L).$$

As any locally constant function factors through G/H for some open compact subgroup $H \leq G$, we also have a natural isomorphism

$$\mathscr{C}^{\mathrm{lc}}(G, \mathscr{O}_L) \cong \varinjlim_H \mathscr{C}(G/H, \mathscr{O}_L).$$

We thus have

$$\mathscr{M}(G, \mathscr{O}_L) \cong \mathrm{Hom}_{\mathrm{cts}}(\varinjlim_H \mathscr{C}(G/H, \mathscr{O}_L), \mathscr{O}_L) \cong \varprojlim_H \mathscr{M}(G/H, \mathscr{O}_L), \tag{3-3}$$

the final isomorphism following from compatibility of duals with limits. As G/H is a finite group, by Proposition 3.15 we have that $\mathscr{M}(G/H, \mathscr{O}_L) \cong \mathscr{O}_L[G/H]$. □

We explicitly describe both maps in this isomorphism.

Let μ be a measure, considered as an additive function as in (3-2), and let H be an open subgroup of G. We define an element λ_H of $\mathscr{O}_L[G/H]$ by setting

$$\lambda_H := \sum_{[a] \in G/H} \mu(aH)[a].$$

By the additivity property of μ, we see that $(\lambda_H)_H \in \varprojlim \mathscr{O}_L[G/H]$, and this gives the map from measures to the inverse limit.

Conversely, given such an element λ of the inverse limit, write λ_H for its image in $\mathscr{O}_L[G/H]$ under the natural projection. Then

$$\lambda_H = \sum_{[a] \in G/H} c_a[a].$$

We define

$$\mu(aH) = c_a.$$

Since the λ_H are compatible under projection maps, this defines an additive function on the open compact subsets of G, i.e., an element $\mu \in \mathscr{M}(G, \mathscr{O}_L)$.

Definition 3.17. We define the *Iwasawa algebra of* G to be the profinite completion of the group algebra $\mathscr{O}_L[G]$, i.e.,

$$\Lambda(G) := \varprojlim_H \mathscr{O}_L[G/H].$$

(Note that we suppress L from the notation.)

Remark 3.18. The Iwasawa algebra $\Lambda(\mathbb{Z}_p)$ has a natural $\mathscr{O}_L$-algebra structure, and hence by transport of structure we obtain such a structure on $\mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L)$. As with the classical situation for finite group rings, the algebra structure on the space of measures can be described directly via *convolution of measures*. For a general profinite abelian group G, given two measures $\mu, \lambda \in \mathscr{M}(G, \mathscr{O}_L)$, one defines their convolution $\mu * \lambda$ to be

$$\int_G \phi \cdot (\mu * \lambda) = \int_G \left(\int_G \phi(x + y) \cdot \lambda(y) \right) \cdot \mu(x).$$

One checks that this does give an algebra structure and that the isomorphism above is an isomorphism of $\mathscr{O}_L$-algebras.

Example 3.19. Let $a \in \mathbb{Z}_p$, and let δ_a be the Dirac measure on $\mathbb{Z}_p$ from Example 3.10. Recall this corresponds to the function $\widetilde{\delta}_a$ on open compact subsets given by $\widetilde{\delta}_a(a) = 1$ (if $a \in X$) and $\widetilde{\delta}_a(a) = 0$ (if $a \notin X$). Under the isomorphism of Proposition 3.16, δ_a corresponds to the projective system

$$([a + p^n\mathbb{Z}_p])_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathscr{O}_L[\mathbb{Z}_p/p^n\mathbb{Z}_p].$$

In the inverse limit this yields an element of the Iwasawa algebra that we denote by $[a]$.

3.4. ***p-adic analysis and Mahler transforms.*** So far we have given three equivalent descriptions of p-adic measures on a profinite abelian group G:

(1) as linear functionals on $\mathscr{C}(G, L)$,

(2) as additive functions on open compact subsets of G, and

(3) as elements of the Iwasawa algebra of G.

In this section we specialise to $G = \mathbb{Z}_p$, and in this case give yet another equivalent description, via the power series ring $\mathscr{O}_L[\![T]\!]$.

Definition 3.20. For $x \in \mathbb{Z}_p$, let

$$\binom{x}{n} := \frac{x(x-1)\cdots(x-n+1)}{n!} \quad \text{for } n \geq 1 \qquad \text{and} \qquad \binom{x}{0} = 1.$$

One easily checks that $x \mapsto \binom{x}{n}$ defines an element in $\mathscr{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ of valuation $v_{\mathscr{C}}\left(\binom{x}{n}\right) = 0$. The following theorem is fundamental in all that follows. It says that the functions $\binom{x}{n}$ form an orthonormal basis for the L-Banach space $\mathscr{C}(\mathbb{Z}_p, L)$ (in the sense of Definition 3.3).

Theorem 3.21 (Mahler). *Let $\phi : \mathbb{Z}_p \to L$ be a continuous function. There exists a unique expansion*

$$\phi(x) = \sum_{n\geq 0} a_n(\phi)\binom{x}{n},$$

where $a_n(\phi) \in L$ and $a_n(\phi) \to 0$ as $n \to \infty$. Moreover, $v_{\mathscr{C}}(\phi) = \inf_{n\in\mathbb{N}} v_p(a_n(\phi))$.

Proof. See [20, Théorème 1.2.3.]. □

Remark 3.22. The coefficients $a_n(\phi)$ are called the *Mahler coefficients* of ϕ. One can write down the Mahler coefficients of ϕ very simply: we define the *discrete derivatives* of ϕ by

$$\phi^{[0]} = \phi, \quad \phi^{[k+1]}(x) = \phi^{[k]}(x+1) - \phi^{[k]}(x),$$

and then $a_n(\phi) = \phi^{[n]}(0)$.

It is natural to study a measure by looking at its values on the elements of the (orthonormal) Mahler basis. We encode these values in the following power series.

Definition 3.23. Let $\mu \in \mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L)$ be a p-adic measure on $\mathbb{Z}_p$. Define the *Mahler transform* (or *Amice transform*) of μ to be

$$\mathscr{A}_\mu(T) := \int_{\mathbb{Z}_p} (1+T)^x \cdot \mu(x) = \sum_{n\geq 0} \left(\int_{\mathbb{Z}_p} \binom{x}{n} \cdot \mu \right) T^n \in \mathscr{O}_L[\![T]\!].$$

Example 3.24. Let $a \in \mathbb{Z}_p$, and recall the Dirac measure δ_a. By definition, its Mahler transform is

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

Before stating the main theorem concerning the Mahler transform, let us consider how it interacts with the isomorphism $\mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L) \xrightarrow{\sim} \Lambda(\mathbb{Z}_p)$ of Proposition 3.16. As 1 is a topological generator of (the additive group) $\mathbb{Z}_p$, and likewise $1+T$ is a topological generator of $\mathscr{O}_L[\![T]\!]$, one may check that $[1] \mapsto (1+T)$ induces an isomorphism $\Lambda(\mathbb{Z}_p) \xrightarrow{\sim} \mathscr{O}_L[\![T]\!]$, fitting into a commutative diagram

$$\begin{array}{ccc} \mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L) & \longrightarrow & \mathscr{O}_L[\![T]\!] \\ \downarrow & \nearrow & \\ \Lambda(\mathbb{Z}_p) & & \end{array} \tag{3-4}$$

Indeed, by continuity it suffices to check on Dirac measures. As $\delta_a \mapsto (1+T)^a$ under the top arrow, and $\delta_a \mapsto [a] \mapsto (1+T)^a$ under the bottom arrows, we are done.

Given the bottom two arrows in (3-4) are isomorphisms, the following theorem should not be surprising.

Theorem 3.25. *The Mahler transform gives an $\mathscr{O}_L$-algebra isomorphism*

$$\mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L) \xrightarrow{\sim} \mathscr{O}_L[\![T]\!].$$

Proof. This is almost a tautology from the definition of orthonormal basis. By continuity and linearity, any measure $\mu \in \mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L)$ is uniquely determined by the values $\int_{\mathbb{Z}_p} \binom{x}{n} \cdot \mu$. Indeed, let $\phi \in \mathscr{C}(\mathbb{Z}_p, \mathscr{O}_L)$. By Mahler's theorem, we can write $\phi(x) = \sum_{n\geq 0} a_n(\phi) \binom{x}{n}$ for some unique $a_n(\phi) \in \mathscr{O}_L$ such that $a_n(\phi) \to 0$ as $n \to \infty$; and then we have

$$\int_{\mathbb{Z}_p} \phi \cdot \mu = \sum_{n\geq 0} a_n(\phi) \int_{\mathbb{Z}_p} \binom{x}{n} \cdot \mu.$$

Conversely, given any collection of values $c_n \in \mathscr{O}_L$, defining an element $g = \sum_{n\geq 0} c_n T^n \in \mathscr{O}_L[\![T]\!]$, there is a unique measure μ_g with $\int_{\mathbb{Z}_p} \binom{x}{n} \cdot \mu_g = c_n$. Concretely,

for any $\phi = \sum_{n\geq 0} a_n(\phi)\binom{x}{n} \in \mathscr{C}(\mathbb{Z}_p, \mathscr{O}_L)$ as above, we define

$$\int_{\mathbb{Z}_p} \phi \cdot \mu_g = \sum_{n\geq 0} a_n(\phi) c_n,$$

which converges to an element in $\mathscr{O}_L$. Visibly we have $\mathscr{A}_{\mu_g} = g$, so this defines an inverse to the Mahler transform. □

Remark 3.26. Each space in the diagram (3-4) has a description as an inverse limit. For measures, this is (3-3); for the Iwasawa algebra, this is by definition; and for power series, we have

$$\mathscr{O}_L[\![T]\!] \cong \varprojlim_n \mathscr{O}_L[T]/((1+T)^{p^n} - 1).$$

The appearance of the expression $(1+T)^{p^n} - 1$ will become clearer in Section 3.5.5 below (and its importance further recognised in Appendix A).

We invite the reader to spell out maps between the "level n" terms of the inverse limits, analogous to (3-4) and such that the following diagram commutes:

$$\begin{array}{ccc} \mathscr{M}(\mathbb{Z}/p^n\mathbb{Z}, \mathscr{O}_L) & \longrightarrow & \mathscr{O}_L[T]/((1+T)^{p^n} - 1) \\ \downarrow & \nearrow & \\ \mathscr{O}_L[\mathbb{Z}/p^n\mathbb{Z}] & & \end{array}$$

Definition 3.27. If $g \in \mathscr{O}_L[\![T]\!]$, we continue to write $\mu_g \in \mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L)$ for the corresponding ($\mathscr{O}_L$-valued) measure on $\mathbb{Z}_p$ (so that $\mathscr{A}_{\mu_g} = g$).

Remark 3.28. (1) Mahler's isomorphism induces an isomorphism

$$\mathscr{M}(\mathbb{Z}_p, L) \cong \mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L) \otimes_{\mathscr{O}_L} L \xrightarrow{\sim} \mathscr{O}[\![T]\!] \otimes_{\mathscr{O}_L} L \cong \mathscr{O}[\![T]\!][1/p].$$

(2) Let $g \in \mathscr{O}_L[\![T]\!]$ with associated measure μ_g. From the definitions, it is easily seen that

$$\int_{\mathbb{Z}_p} \mu_g = g(0), \quad \int_{\mathbb{Z}_p} x \cdot \mu_g = g'(0), \quad \int_{\mathbb{Z}_p} x^2 \cdot \mu_g = g''(0) + g'(0),$$

$$\int_{\mathbb{Z}_p} x^3 \cdot \mu_g = g'''(0) + 3g''(0) + g'(0), \quad \ldots,$$

that is, for every n, the value $\int_{\mathbb{Z}_p} x^n \cdot \mu_g$ can be written as an integer combination of $g^{(r)}(0)$ for $0 \leq r \leq n$. We simplify this in Corollary 3.30 below.

(3) Recall (from Definition 3.5) that there are two natural topologies on $\mathscr{M}(\mathbb{Z}_p, \mathscr{O}_L)$. One can check that under the isomorphism of Theorem 3.25, the strong topology corresponds to the p-adic topology on $\mathscr{O}_L[\![T]\!]$, whilst the weak topology corresponds to the (p, T)-adic topology. Analogously to Remark 3.6, the p-adic topology on $\mathscr{O}_L[\![T]\!]$ is that of uniform convergence in the power series coefficients,

whilst the (p, T)-adic topology is that of pointwise (term-by-term) convergence. For example, consider the sequence $1, T, T^2, T^3, \ldots$ in $\mathscr{O}_L[\![T]\!]$. This converges to 0 pointwise, and in the (p, T)-adic (weak) topology; but it does not converge uniformly, or in the p-adic (strong) topology.

3.5. ***A measure-theoretic toolbox.*** There are natural operations one might consider on measures, and via the Mahler transform these give rise to operators on power series. The following operations can be considered as a "toolbox" for working with measures and power series; as we shall see in the sequel, the ability to manipulate measures in this way has important consequences. For further details (and more operations), see [20].

Notation. In light of the isomorphism between the space $\mathscr{M}(G, \mathscr{O}_L)$ of measures and the Iwasawa algebra $\Lambda(G)$, we will frequently conflate the two. In particular, it is convenient — and indeed standard — to write $\mu \in \Lambda(G)$ for measures on G, typically suppressing the coefficient field L, which is fixed throughout.

3.5.1. *Multiplication by x.* Given a measure μ on $\mathbb{Z}_p$, we naturally wish to compute $\int_{\mathbb{Z}_p} x^k \cdot \mu$ for k a positive integer. To allow us to do that, we let $x\mu$ be the measure defined by

$$\int_{\mathbb{Z}_p} f(x) \cdot x\mu = \int_{\mathbb{Z}_p} xf(x) \cdot \mu.$$

We can ask what the operation $\mu \mapsto x\mu$ does on Mahler transforms; we find:

Lemma 3.29. *We have*

$$\mathscr{A}_{x\mu} = \partial \mathscr{A}_\mu,$$

where ∂ denotes the differential operator $(1+T)\frac{d}{dT}$.

Proof. The result follows directly from computing

$$x\binom{x}{n} = (x-n)\binom{x}{n} + n\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n}. \qquad \square$$

From the above lemma, we immediately obtain the following expressions, completing the examples seen in Remark 3.28.

Corollary 3.30. *For $\mu \in \Lambda(\mathbb{Z}_p)$, we have*

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

3.5.2. *Multiplication by z^x.* Totally analogously to the above, if $g \in \mathscr{C}(\mathbb{Z}_p, L)$ and μ is a measure on $\mathbb{Z}_p$, then we can define a measure $g(x)\mu$ by

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

Of particular interest is the measure $z^x\mu$, for $z \in \mathscr{O}_L$ such that $|z-1| < 1$. We claim the Mahler transform of $z^x\mu$ is

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

Indeed, from the definition of the Mahler transform, we see that

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

and this is precisely the Mahler transform of $z^x\mu$ (one has to be slightly careful about convergence issues).

3.5.3. *Restriction to open compact subsets.* Consider an open compact subset $X \subset \mathbb{Z}_p$, and write $\mathbf{1}_X$ for the characteristic function of X. The "restriction of μ to X" is the measure $\mathrm{Res}_X(\mu)$ on $\mathbb{Z}_p$ defined by

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

It is also standard (and intuitive) to denote this quantity as

$$\int_X f \cdot \mu.$$

We say a measure μ is *supported on* X if $\mu = \mathrm{Res}_X(\mu)$.

Remark 3.31. Note that we may view this restriction as a measure on X as follows. For any continuous function $g : X \to L$, let $\widetilde{g} : \mathbb{Z}_p \to L$ denote its extension by 0 outside X. The map

$$\mathscr{C}(X, L) \to L, \quad g \mapsto \int_{\mathbb{Z}_p} \widetilde{g} \cdot \mu$$

defines a measure on X. Abusing notation, we also denote this measure by $\mathrm{Res}_X(\mu)$, noting it is intuitively compatible with its cousin defined on $\mathbb{Z}_p$. Indeed we will often blur the distinction between considering $\mathrm{Res}_X(\mu)$ as a measure on $\mathbb{Z}_p$ or on X.

When $X = b + p^n\mathbb{Z}_p$, we can write the characteristic function explicitly as

$$\mathbf{1}_{b+p^n\mathbb{Z}_p}(x) = \frac{1}{p^n} \sum_{\xi \in \mu_{p^n}} \xi^{x-b},$$

and then using the above, we calculate the Mahler transform of $\mathrm{Res}_{b+p^n\mathbb{Z}_p}(\mu)$ to be

$$\mathscr{A}_{\mathrm{Res}_{b+p^n\mathbb{Z}_p}(\mu)}(T) = \frac{1}{p^n} \sum_{\xi \in \mu_{p^n}} \xi^{-b} \mathscr{A}_\mu((1+T)\xi - 1). \tag{3-5}$$

3.5.4. *Restriction to $\mathbb{Z}_p^\times$.* Immediately from the above applied to $b = 0$ and $n = 1$,

$$\mathscr{A}_{\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu)}(T) = \mathscr{A}_\mu(T) - \frac{1}{p} \sum_{\xi \in \mu_p} \mathscr{A}_\mu((1+T)\xi - 1). \tag{3-6}$$

In order to calculate a formula for the restriction to an arbitrary open compact subset $X \subseteq \mathbb{Z}_p$, we can write X (or its complement, as we did with $\mathbb{Z}_p^\times$) as a disjoint union of sets of the form $b + p^n\mathbb{Z}_p$ and apply the formulas obtained before.

3.5.5. *The action of $\mathbb{Z}_p^\times$, φ and ψ.* We introduce an action of $\mathbb{Z}_p^\times$ that serves as a precursor to a Galois action later on. Let $a \in \mathbb{Z}_p^\times$. We can define a measure $\sigma_a(\mu)$ by

$$\int_{\mathbb{Z}_p} f(x) \cdot \sigma_a(\mu) = \int_{\mathbb{Z}_p} f(ax) \cdot \mu.$$

This has Mahler transform

$$\mathscr{A}_{\sigma_a(\mu)} = \mathscr{A}_\mu((1+T)^a - 1).$$

In a similar manner, we can define an operator φ acting as "σ_p" by

$$\int_{\mathbb{Z}_p} f(x) \cdot \varphi(\mu) = \int_{\mathbb{Z}_p} f(px) \cdot \mu,$$

and this corresponds to

$$\mathscr{A}_{\varphi(\mu)} = \varphi(\mathscr{A}_\mu) := \mathscr{A}_\mu((1+T)^p - 1). \tag{3-7}$$

Finally, we also define the analogous operator for p^{-1}; we define a measure $\psi(\mu)$ on $\mathbb{Z}_p$ by defining

$$\int_{\mathbb{Z}_p} f(x) \cdot \psi(\mu) = \int_{p\mathbb{Z}_p} f(p^{-1}x) \cdot \mu.$$

Note that $\psi \circ \varphi = \mathrm{id}$, whilst $\varphi \circ \psi(\mu) = \mathrm{Res}_{p\mathbb{Z}_p}(\mu)$. Indeed, we have

$$\begin{aligned}\int_{\mathbb{Z}_p} f(x) \cdot \psi \circ \varphi(\mu) &= \int_{\mathbb{Z}_p} \mathbf{1}_{p\mathbb{Z}_p}(x) f(p^{-1}x) \cdot \varphi(\mu) \\ &= \int_{\mathbb{Z}_p} \mathbf{1}_{p\mathbb{Z}_p}(px) f(x) \cdot \varphi(\mu) = \int_{\mathbb{Z}_p} f(x) \cdot \mu\end{aligned}$$

and

$$\int_{\mathbb{Z}_p} f(x) \cdot \varphi \circ \psi(\mu) = \int_{\mathbb{Z}_p} f(px) \cdot \psi(\mu) = \int_{p\mathbb{Z}_p} f(x) \cdot \mu = \int_{\mathbb{Z}_p} f(x) \cdot \mathrm{Res}_{p\mathbb{Z}_p}(\mu).$$

In particular, we have

$$\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu) = (1 - \varphi \circ \psi)(\mu). \tag{3-8}$$

The operator ψ also gives an operator on any $F(T) \in \mathscr{O}_L[\![T]\!]$ under the Mahler transform, and using the restriction formula above, we see that it is the unique operator satisfying

$$\varphi \circ \psi(F)(T) = \frac{1}{p} \sum_{\xi \in \mu_p} F((1+T)\xi - 1). \tag{3-9}$$

The following result will be useful in Part II.

Corollary 3.32. *A measure $\mu \in \Lambda(\mathbb{Z}_p)$ is supported on $\mathbb{Z}_p^\times$ if and only if $\psi(\mathscr{A}_\mu) = 0$.*

Proof. Let $\mu \in \Lambda(\mathbb{Z}_p)$. Then μ is supported on $\mathbb{Z}_p^\times$ if and only if $\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu) = \mu$, or equivalently if and only if $\mathscr{A}_\mu = \mathscr{A}_\mu - \varphi \circ \psi(\mathscr{A}_\mu)$, which happens if and only if $\psi(\mathscr{A}_\mu) = 0$, since the operator φ is injective. □

Remark 3.33. We have an injection $\iota : \Lambda(\mathbb{Z}_p^\times) \hookrightarrow \Lambda(\mathbb{Z}_p)$ given by

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

and because $\mathrm{Res}_{\mathbb{Z}_p^\times} \circ \iota$ is the identity on $\Lambda(\mathbb{Z}_p^\times)$, we can identify $\Lambda(\mathbb{Z}_p^\times)$ with its image as a subset of $\Lambda(\mathbb{Z}_p)$. By Corollary 3.32, a measure $\mu \in \Lambda(\mathbb{Z}_p)$ lies in $\Lambda(\mathbb{Z}_p^\times)$ if and only if $\psi(\mu) = 0$. Whilst we identify $\Lambda(\mathbb{Z}_p^\times)$ with a subset of $\Lambda(\mathbb{Z}_p)$, it is important to remark that it is *not* a subalgebra. Indeed, convolution of measures on a group G uses the group structure of G; for $\mathbb{Z}_p^\times$ this is multiplicative, and for $\mathbb{Z}_p$ this is additive (see Remark 3.18). If λ and μ are two measures on $\mathbb{Z}_p^\times$, writing $\mu *_{\mathbb{Z}_p^\times} \lambda$ for the convolution over $\mathbb{Z}_p^\times$, we have

$$\int_{\mathbb{Z}_p^\times} f(x) \cdot (\mu *_{\mathbb{Z}_p^\times} \lambda) = \int_{\mathbb{Z}_p^\times} \left(\int_{\mathbb{Z}_p^\times} f(xy) \cdot \mu(x) \right) \cdot \lambda(y). \tag{3-10}$$

3.6. ***Pseudomeasures.*** The Mahler transform gives a correspondence between p-adic measures and p-adic analytic functions on the open unit ball (explained in Remark 3.39 below). The Riemann zeta function, however, is not analytic everywhere, as it has a simple pole at $s = 1$. To reflect this, we also need to be able to handle simple poles on the p-adic side. We do this via the theory of pseudomeasures.

Definition 3.34. Let G be a profinite abelian group, and let $Q(G)$ denote the ring of fractions of the Iwasawa algebra $\Lambda(G)$. A *pseudomeasure* on G is an element $\lambda \in Q(G)$ such that

$$([g] - [1])\lambda \in \Lambda(G)$$

for all $g \in G$. (This is using the natural product on the Iwasawa algebra $\Lambda(G)$, which we recall corresponds to convolution (3-10) of measures).

We first explain how to integrate certain functions against pseudomeasures. Let $\chi : G \to \mathbb{C}_p^\times$ be a nontrivial character, and let $\lambda \in Q(G)$ be a pseudomeasure. Then one can define

$$\int_G \chi \cdot \lambda := (\chi(g) - 1)^{-1} \int_G \chi \cdot ([g] - [1])\lambda, \tag{3-11}$$

where $g \in G$ is any element such that $\chi(g) \neq 1$. This definition does not depend on the choice of $g \in G$. Indeed one has

$$(\chi(h)-1)\int_G \chi\cdot([g]-[1])\lambda = \int_G \chi\cdot([g]-1)([h]-1)\lambda$$
$$= (\chi(g)-1)\int_G \chi\cdot([h]-1)\mu.$$

Here we used the convolution product and that G is abelian.

Remark 3.35. To motivate this definition, note that if $\chi : G \to \mathbb{C}_p^\times$ is a nontrivial character, then from the definition of convolution product, the function

$$\Lambda(G) \to \mathbb{C}_p, \quad \mu \mapsto \int_G \chi\cdot\mu$$

is a ring homomorphism. This induces a unique homomorphism $Q(G) \to \mathbb{C}_p$, which — when applied to a pseudomeasure — yields the expression (3-11) above.

We will be most interested in pseudomeasures on $G = \mathbb{Z}_p^\times$. The following lemma shows that a pseudomeasure μ on $\mathbb{Z}_p^\times$ is uniquely determined by the values $\int_{\mathbb{Z}_p^\times} x^k\cdot\mu$ for $k > 0$.

Lemma 3.36. (i) *Let $\mu \in \Lambda(\mathbb{Z}_p^\times)$ be such that*

$$\int_{\mathbb{Z}_p^\times} x^k\cdot\mu = 0$$

for all $k > 0$. Then $\mu = 0$.

(ii) *Let $\mu \in \Lambda(\mathbb{Z}_p^\times)$ be such that*

$$\int_{\mathbb{Z}_p^\times} x^k\cdot\mu \neq 0$$

for all $k > 0$. Then μ is not a zero divisor in $\Lambda(\mathbb{Z}_p^\times)$.

(iii) *Part* (i) *holds if, more generally, μ is a pseudomeasure.*

Proof. (i) Note that the vanishing condition forces the Mahler transform $\mathscr{A}_\mu(T) = \sum_{k\geq 0}\big(\int_{\mathbb{Z}_p}\binom{x}{k}\cdot\mu\big)T^k$ of μ to be constant, since each nontrivial binomial polynomial is a linear combination of strictly positive powers of x. As μ is a measure on $\mathbb{Z}_p^\times$, we also have $\psi(\mathscr{A}_\mu)(T) = 0$ by (3-8). Since ψ is the identity on constants (using, e.g., (3-9)), we deduce that $\mathscr{A}_\mu(T) = 0$, so $\mu = 0$.

(ii) Suppose there exists a measure λ such that $\mu *_{\mathbb{Z}_p^\times} \lambda = 0$, where the product is the convolution product on $\mathbb{Z}_p^\times$ (see Remark 3.33). Then

$$0 = \int_{\mathbb{Z}_p^\times} x^k\cdot(\mu *_{\mathbb{Z}_p^\times}\lambda) = \int_{\mathbb{Z}_p^\times}\left(\int_{\mathbb{Z}_p^\times}(xy)^k\cdot\mu(x)\right)\cdot\lambda(y) = \left(\int_{\mathbb{Z}_p^\times} x^k\cdot\mu\right)\left(\int_{\mathbb{Z}_p^\times} x^k\cdot\lambda\right),$$

which forces $\lambda = 0$ by part (i). In particular μ is not a zero divisor.

(iii) Let μ be a pseudomeasure satisfying the vanishing condition. Let $a \neq 1$ be an integer prime to p; then $\lambda = ([a]-[1])\mu \in \Lambda(\mathbb{Z}_p^\times)$ is a measure by the definition of pseudomeasure, and by (3-11) we have

$$\int_{\mathbb{Z}_p^\times} x^k \cdot \lambda = (a^k - 1) \int_{\mathbb{Z}_p^\times} x^k \cdot \mu = 0$$

for all $k > 0$. By part (i), we have $\lambda = 0$. But $[a]-[1]$ satisfies the condition of part (ii), so it is not a zero-divisor, and this forces $\mu = 0$, as required. □

Finally, we give a simpler process for writing down pseudomeasures on $\mathbb{Z}_p^\times$.

Definition 3.37. The *augmentation ideal* $I((\mathbb{Z}_p/p^n)^\times) \subset \mathcal{O}_L[(\mathbb{Z}_p/p^n)^\times]$ is the kernel of the natural "degree" map

$$\mathcal{O}_L[(\mathbb{Z}/p^n\mathbb{Z})^\times] \to \mathcal{O}_L, \quad \sum_a c_a[a] \mapsto \sum_a c_a.$$

These fit together into a degree map $\Lambda(\mathbb{Z}_p^\times) \to \mathcal{O}_L$; we call its kernel the augmentation ideal $I(\mathbb{Z}_p^\times) \subset \Lambda(\mathbb{Z}_p^\times)$. One may check directly there is an isomorphism

$$I(\mathbb{Z}_p^\times) \cong \varprojlim I((\mathbb{Z}_p/p^n)^\times).$$

Lemma 3.38. *Let a be any topological generator of $\mathbb{Z}_p^\times$ (for example, take a to be a primitive root modulo p such that $a^{p-1} \not\equiv 1 \pmod{p}^2$), and $\mu \in \Lambda(\mathbb{Z}_p^\times)$ a measure. Then*

$$\mu' := \frac{\mu}{[a]-[1]} \in Q(\mathbb{Z}_p^\times)$$

is a pseudomeasure.

Proof. As p is odd, $(\mathbb{Z}_p/p^n)^\times$ is cyclic, generated by $\bar{a} := a \pmod{p^n}$, and we have

$$I((\mathbb{Z}_p/p^n)^\times) = ([\bar{a}]-[\bar{1}])\mathcal{O}_L[(\mathbb{Z}_p/p^n)^\times].$$

In the inverse limit we see that

$$I(\mathbb{Z}_p^\times) = ([a]-[1])\Lambda(\mathbb{Z}_p^\times).$$

Thus if $g \in \mathbb{Z}_p^\times$, we have $[g]-[1] \in I(\mathbb{Z}_p^\times)$, and we must have

$$[g]-[1] = \nu([a]-[1])$$

for some $\nu \in \Lambda(\mathbb{Z}_p^\times)$. Then

$$([g]-[1])\mu' = \nu([a]-[1])\mu' = \nu \cdot \mu \in \Lambda(\mathbb{Z}_p^\times),$$

that is, μ' is a pseudomeasure. □

Note moreover that *all* pseudomeasures have this shape. Indeed, let μ' be a pseudomeasure, and $a \in \mathbb{Z}_p^\times$ a topological generator; then $\mu = ([a]-[1])\mu'$ is a measure, and $\mu' = \mu/([a]-[1])$ as above.

3.7. ***Locally analytic functions and distributions.*** We finally introduce another important space of functions and its dual, namely *locally analytic functions* and *locally analytic distributions*. This subsection may be safely skipped on a first reading, and indeed we make only peripheral use of its content in these notes (in Sections 6.2 and 7, to study values of the p-adic zeta function). The locally analytic theory is nonetheless of fundamental importance in more general settings, so we include a sketch here, and indicate how it dovetails beautifully with the theory of measures we have already studied. All of this — and other related theories in p-adic functional analysis — are described in detail in [20].

As motivation, we first note the following.

Remark 3.39. The space $\mathscr{M}(\mathbb{Z}_p, L)$ of measures has an interpretation via rigid analysis. To explain this, consider the p-adic open unit ball in $\mathbb{C}_p$, i.e., the space

$$B(0, 1) = \{z \in \mathbb{C}_p : |z| < 1\} \subset \mathbb{C}_p.$$

This is the set of $\mathbb{C}_p$-points of a rigid analytic space in the sense of [10]. An L-valued function on $B(0, 1)$ is *rigid analytic* if it can be written as a power series $\sum_{n\geq 0} a_n T^n \in L[\![T]\!]$ that is everywhere convergent on $B(0, 1)$ (i.e., $|a_n|r^n \to 0$ as $n \to \infty$ for all $r < 1$); write $\mathscr{R}^+ \subset L[\![T]\!]$ for the space of such functions. A rigid analytic function is *bounded* if the $|a_i|$ are bounded.

Note that the space of bounded L-valued rigid analytic functions is $\mathscr{O}_L[\![T]\!] \otimes_{\mathscr{O}_L} L$, which, via the Mahler transform (Remark 3.28), is isomorphic to $\mathscr{M}(\mathbb{Z}_p, L)$. Hence p-adic measures on $\mathbb{Z}_p$ can be viewed as bounded rigid analytic functions on $B(0, 1)$.

It is natural to ask if the Mahler correspondence, as studied in Theorem 3.25, can be extended from $\mathscr{O}_L[\![T]\!]$ to all of $\mathscr{R}^+$. Such an extension is given by locally analytic distributions, in the sense described in Theorem 3.43 and (3-12) below.

Definition 3.40. Let $L/\mathbb{Q}_p$ be a finite extension, and let $f : \mathbb{Z}_p \to L$ be a function.

(1) For $z \in \mathbb{Z}_p$, we say f is *locally analytic at* z if f can be described locally around z by a convergent power series. Precisely, this means there exists some integer $n_z \geq 0$ and numbers $\{a_k(z) \in L : k \geq 0\}$ such that

$$\sum_{k\geq 0} a_k(z) \cdot (x - z)^k$$

converges to $f(x)$ for all $x \in U_z := z + p^{n_z}\mathbb{Z}_p$.

(2) We say f is *locally analytic* if it is locally analytic at all $z \in \mathbb{Z}_p$.

(3) We write $\mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L)$ for the L-vector space of all locally analytic functions $\mathbb{Z}_p \to L$.

Recall that $\mathscr{C}(\mathbb{Z}_p, L)$ can be equipped with a valuation that makes it into an L-Banach space, and that the space of measures $\mathscr{M}(\mathbb{Z}_p, L)$ was defined as its continuous dual. Analogously, the space $\mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L)$ has a natural topology, described

as follows (see [20, Section I.4] for more details). For each $n \in \mathbb{N}$, we say a function $f : \mathbb{Z}_p \to L$ is *locally analytic of radius* p^{-n} if it is locally analytic and moreover we can take $n_z = n$ for all $z \in \mathbb{Z}_p$; in other words, it is analytic (described by a single power series) on each open set of form $z + p^n\mathbb{Z}_p$. Denote by $\mathscr{C}^{n-\mathrm{an}}(\mathbb{Z}_p, L)$ the subspace of such functions. Then one can check that $\mathscr{C}^{n-\mathrm{an}}(\mathbb{Z}_p, L)$ is an L-Banach space with valuation given by

$$v_n(f) := \inf_{z \in (\mathbb{Z}_p/p^n\mathbb{Z}_p)} \inf_{k \in \mathbb{N}} \big(nk + v_p(a_k(z))\big),$$

or, equivalently, norm given by

$$\|f\|_n := \sup_{z \in (\mathbb{Z}_p/p^n\mathbb{Z}_p)} \sup_{k \in \mathbb{N}} |a_k(z)|\, p^{-nk}.$$

Moreover, almost by definition, we have that $\mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L) = \varinjlim_{n \in \mathbb{N}} \mathscr{C}^{n-\mathrm{an}}(\mathbb{Z}_p, L)$, and so it inherits a natural topology given by the direct limit topology.

Remark 3.41. Locally analytic functions are continuous, so $\mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L) \subset \mathscr{C}(\mathbb{Z}_p, L)$. Note, however, that the topology we just defined on $\mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L)$ is *not* the one induced from $\mathscr{C}(\mathbb{Z}_p, L)$. Nonetheless the image of this inclusion is dense, as, for example, locally constant functions are locally analytic functions and are dense in $\mathscr{C}(\mathbb{Z}_p, L)$.

Analogously to Definition 3.8, we make the following definition.

Definition 3.42. We define the space $\mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p, L)$ of locally analytic distributions on $\mathbb{Z}_p$ to be the continuous dual $\mathrm{Hom}_{\mathrm{cts}}(\mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L), L)$.

If μ is a locally analytic distribution on $\mathbb{Z}_p$, and $\phi \in \mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L)$, we continue to write

$$\int_{\mathbb{Z}_p} \phi(x) \cdot \mu(x) := \mu(\phi).$$

The binomial polynomials $\binom{x}{n}$ are visibly locally analytic, so we may also extend the Mahler transform to this generality; namely, if $\mu \in \mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p, L)$, define

$$\mathscr{A}_\mu(T) := \int_{\mathbb{Z}_p} (1+T)^x \cdot \mu(x) = \sum_{n \geq 0} \left(\int_{\mathbb{Z}_p} \binom{x}{n} \cdot \mu \right) T^n \in L[\![T]\!].$$

The following crucial result provides the desired extension of the Mahler transform beyond bounded measures/power series.

Theorem 3.43. *The Mahler transform induces a bijection*

$$\mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p, L) \to \mathscr{R}^+ \subset L[\![T]\!].$$

Proof. This is [20, Theorem II.2.2]. □

As with Theorem 3.25, the theorem says more: the bijection respects natural topologies on both sides. Here the topologies are as follows:

- $\mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p, L)$ is the inverse limit of the continuous duals $\mathscr{D}^{n-\mathrm{an}}(\mathbb{Z}_p, L)$; each of these is a Banach space with the natural dual (strong) topology (see Remark 3.6). This endows $\mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p, L)$ with the corresponding inverse limit topology.
- As the open unit disc is the union of the closed discs $B(0, r) := \{z \in \mathbb{C}_p : |z| \leq r\}$ of radius $r < 1$, we can write $\mathscr{R}^+$ as the inverse limit over $r < 1$ of the Banach spaces $\mathcal{O}(B(0, r))$ of analytic functions on $B(0, r)$. Again we get an inverse limit topology on $\mathscr{R}^+$.

A topology induced from an inverse limit of Banach spaces is called a *Fréchet topology*. The Mahler transform is then an isomorphism of Fréchet spaces.

Remark 3.44. If $\mu \in \mathscr{M}(\mathbb{Z}_p, L)$ is any measure, then we obtain a locally analytic distribution $\widetilde{\mu} \in \mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p, L)$ by restricting to $\mathscr{C}^{\mathrm{la}}(\mathbb{Z}_p, L) \subset \mathscr{C}(\mathbb{Z}_p, L)$. As locally analytic functions are dense inside continuous functions, the association $\mu \mapsto \widetilde{\mu}$ is injective, and hence this identification allows us to consider $\mathscr{M}(\mathbb{Z}_p, L) \subset \mathscr{D}^{\mathrm{la}}$ as a subset. The combination of Theorems 3.25 and 3.43 says that this inclusion is compatible with the natural inclusion of bounded power series inside power series converging in the open unit disc, that is, the following diagram commutes:

$$\begin{array}{ccc} \mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p, L) & \xrightarrow{\mu \mapsto \mathscr{A}_\mu} & \mathscr{R}^+ \\ \cup & & \cup \\ \mathscr{M}(\mathbb{Z}_p, L) & \xrightarrow{\mu \mapsto \mathscr{A}_\mu} & \mathcal{O}_L[\![T]\!] \otimes_{\mathcal{O}_L} L \end{array} \tag{3-12}$$

Remark 3.45. Observe that every part of our "measure-theoretic toolbox" from Section 3.5, including corresponding operations on Mahler transforms, carries over identically to the setting of locally analytic distributions.

Remark 3.46. Locally analytic p-adic analysis is fundamentally important in the study of p-adic L-functions (and in many other areas, such as in the study of p-adic automorphic forms, in the p-adic Langlands correspondence, in p-adic Hodge theory, etc.). Indeed, more general p-adic L-functions — for example, those attached to elliptic curves and modular forms — are frequently not measures or pseudomeasures, but rather locally analytic distributions with prescribed growth, in the sense of [1]. We discuss this further in Appendix B.

3.8. ***Further remarks.*** The following remarks will not be seriously used in the sequel, but are included for completeness, and to illustrate some other ways that the objects studied in this section appear in the literature.

Remark 3.47. We have an analogue of Remark 3.39 for measures on $\mathbb{Z}_p^\times$, using instead the multiplicative structure. The key object here is the *weight space*

$$\mathcal{W}(\mathbb{C}_p) = \mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times).$$

Since $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, we have

$$\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times) \cong \mathrm{Hom}_{\mathrm{cts}}(\mu_{p-1}, \mathbb{C}_p^\times) \times \mathrm{Hom}_{\mathrm{cts}}(1 + p\mathbb{Z}_p, \mathbb{C}_p^\times).$$

Evaluation at a topological generator of $1 + p\mathbb{Z}_p$ identifies $\mathrm{Hom}_{\mathrm{cts}}(1 + p\mathbb{Z}_p, \mathbb{C}_p^\times)$ with $B(0, 1)$ from above. Hence we may identify $\mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ with $p-1$ copies of $B(0, 1)$. Summarising,

$$\mathcal{W}(\mathbb{C}_p) = \bigsqcup_{\nu \in (\mu_{p-1})^\vee} U_\nu,$$

where:

- ν ranges over the $p - 1$ different characters of μ_{p-1}.
- $U_\nu \subset \mathcal{W}(\mathbb{C}_p)$ is the subset of characters χ of $\mathbb{Z}_p^\times$ with $\chi|_{\mu_{p-1}} = \nu$.
- Each U_ν may be identified with $B(0, 1)$.

This space can also be given more structure; there is a rigid analytic space $\mathcal{W}$ such that the elements of $\mathcal{W}(\mathbb{C}_p)$ are the $\mathbb{C}_p$-points of $\mathcal{W}$. Analogously to above, a theorem of Amice says that giving a measure μ on $\mathbb{Z}_p^\times$ is equivalent to giving a bounded rigid analytic function F_μ on $\mathcal{W}$. This equivalence is given as follows: if μ is a measure on $\mathbb{Z}_p^\times$ and $\chi : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$ is a character (seen as a point on $\mathcal{W}(\mathbb{C}_p)$), then one defines $F_\mu(\chi) := \int_{\mathbb{Z}_p^\times} \chi \cdot \mu$. Observe that the multiplicative convolution product corresponds to pointwise multiplication of rigid functions.

Finally, if $\lambda \in Q(\mathbb{Z}_p^\times)$ is a pseudomeasure, then it is of the form $\mu/([a] - [1])$ for some topological generator $a \in \mathbb{Z}_p^\times$ and some measure $\mu \in \Lambda(\mathbb{Z}_p^\times)$. Note $\int_{\mathbb{Z}_p^\times} \chi \cdot ([a] - [1]) = 0$ if and only if $\chi(a) = 1$, which — as a is a topological generator of $\mathbb{Z}_p^\times$ — implies χ is the trivial character. Hence, as a function on the weight space, λ might have a simple pole at the trivial character. So pseudomeasures can be seen as rigid analytic functions on the weight space that possibly have a simple pole at the trivial character.

Remark 3.48. Power series rings have been generalised to what now are called Fontaine rings. It turns out that Galois representations are connected to certain modules over these rings called (φ, Γ)-modules. The operations described above generalise to fundamental operations on (φ, Γ)-modules, and their interpretation via p-adic analysis inspired the proof of the p-adic Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ (see [21]).

4. The Kubota–Leopoldt p-adic L-function

In this section, we prove the following:

Theorem 4.1. *There is a unique pseudomeasure ζ_p on $\mathbb{Z}_p^\times$ such that, for all $k > 0$,*

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

This pseudomeasure, denoted by ζ_p^{an} in Section 1, is the *Kubota–Leopoldt p-adic L-function*.

4.1. ***The measure μ_a.*** Recall from Lemma 2.7 that we can write the Riemann zeta function in the form

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

where $f(t) = t/(e^t - 1)$, and that $\zeta(-k) = (d^k f/dt^k)(0) = (-1)^k B_{k+1}/(k+1)$. We want to remove the smoothing factor at $s = 1$. For this, let a be an integer coprime to p and consider the related function

$$f_a(t) = \frac{1}{e^t - 1} - \frac{a}{e^{at} - 1}.$$

This is also $\mathscr{C}^\infty$ and rapidly decreasing, so we can apply Theorem 2.4 and consider the function $L(f_a, s)$. The presence of a removes the factor of $s - 1$, at the cost of introducing a different smoothing factor.

Lemma 4.2. *We have*

$$L(f_a, s) = (1 - a^{1-s})\zeta(s),$$

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

$$f_a^{(k)}(0) = (-1)^k (1 - a^{1+k})\zeta(-k).$$

Proof. This follows from calculations similar to those in the proof of Lemma 2.7. □

We now introduce the p-adic tools we have developed into the picture. We will start with the function $f_a(t)$, and slowly manipulate it until we construct a (pseudo)measure with the desired interpolation properties. Note first the following very simple observation.

Lemma 4.3. *Under the substitution $e^t = T + 1$, the derivative d/dt becomes the operator $\partial = (1 + T)\frac{d}{dT}$. In particular, if we define*

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

we have

$$f_a^{(k)}(0) = (\partial^k F_a)(0). \tag{4-1}$$

The left-hand side of (4-1) computes the L-value $\zeta(-k)$ by Lemma 4.2. The right-hand side is similar to Corollary 3.30, which expressed the integral $\int_{\mathbb{Z}_p} x^k \cdot \mu$ in terms of the Mahler transform $\mathscr{A}_\mu$. This motivates us to seek a measure μ_a with $\mathscr{A}_{\mu_a} = F_a$. This is possible by:

Proposition 4.4. *The function $F_a(T)$ is an element of $\mathbb{Z}_p[\![T]\!]$.*

Proof. We can expand

$$(1+T)^a - 1 = \sum_{n\geq 1} \binom{a}{n} T^n = aT(1+Tg(T)),$$

where $g(T) = \sum_{n\geq 2} \frac{1}{a}\binom{a}{n} T^{n-2}$ has coefficients in $\mathbb{Z}_p$ since we have chosen a coprime to p. Hence, expanding the geometric series, we find

$$\frac{1}{T} - \frac{a}{(1+T)^a - 1} = \frac{1}{T} \sum_{n\geq 1} (-T)^n g(T)^n,$$

which is visibly an element of $\mathbb{Z}_p[\![T]\!]$. □

Definition 4.5. Let μ_a be the measure on $\mathbb{Z}_p$ whose Mahler transform is $F_a(T)$.

Proposition 4.6. *For $k \geq 0$, we have*

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

Proof. By Corollary 3.30, the left-hand side is $(\partial^k \mathscr{A}_{\mu_a})(0)$. By definition of μ_a and Lemma 4.3 this is $(\partial^k F_a)(0) = f_a^{(k)}(0)$. This equals the right-hand side by Lemma 4.2. □

4.2. ***Restriction to $\mathbb{Z}_p^\times$.*** Recall from the introduction that we want the p-adic analogue of the Riemann zeta function to be a measure on $\mathbb{Z}_p^\times$, not all of $\mathbb{Z}_p$. We have already defined a restriction operator in (3-8), which on Mahler transforms acts as $1 - \varphi \circ \psi$. We begin with a short but important property of the measure μ_a.

Lemma 4.7. *We have $\psi(\mu_a) = \mu_a$.*

Proof. We show the result by considering the action on power series. We wish to show $\psi(F_a) = F_a$. First note that $F_a(T) = \frac{1}{T} - a \cdot \sigma_a\left(\frac{1}{T}\right)$, for σ_a as in Section 3.5.5. As ψ commutes with σ_a, we have $\psi(F_a) = \psi\left(\frac{1}{T}\right) - a \cdot \sigma_a \psi\left(\frac{1}{T}\right)$, so it suffices to show $\psi\left(\frac{1}{T}\right) = \frac{1}{T}$.

By definition (see (3-9)) we have

$$(\varphi \circ \psi)\left(\frac{1}{T}\right) = p^{-1} \sum_{\xi \in \mu_p} \frac{1}{(1+T)\xi - 1} = \frac{1}{(1+T)^p - 1} = \varphi\left(\frac{1}{T}\right),$$

as can be seen by calculating the partial fraction expansion. By injectivity of φ, we deduce that $\psi\left(\frac{1}{T}\right) = \frac{1}{T}$, and conclude. □

Proposition 4.8. *We have*

$$\int_{\mathbb{Z}_p^\times} x^k \cdot \mu_a = (-1)^k (1-p^k)(1-a^{k+1})\zeta(-k). \tag{4-2}$$

(*In other words, restricting to* $\mathbb{Z}_p^\times$ *removes the Euler factor at* p).

Proof. Since $\mathrm{Res}_{\mathbb{Z}_p^\times} = 1 - \varphi \circ \psi$, we deduce that

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

where for the second equality we have used Lemma 4.7. This finishes the proof. □

4.3. ***Rescaling and removing dependence on a.*** Finally we remove the dependence on a. Thus far, the presence of a has acted as a "smoothing factor" which removes the pole of the Riemann zeta function; so to remove it, we must be able to handle such poles on the p-adic side. We use the notion of pseudomeasures from Section 3.6.

Definition 4.9. Let a be an integer that is prime to p, and let θ_a denote the element of $\Lambda(\mathbb{Z}_p^\times)$ corresponding to $[a]-[1]$. Note that, by definition, we have

$$\int_{\mathbb{Z}_p^\times} x^k \cdot \theta_a = a^k - 1.$$

However, in (4-2) it is $a^{k+1}-1$ that appears. To bridge this gap, note that on $\mathbb{Z}_p^\times$, we have a well-defined operation "multiplication by x^{-1}" given by

$$\int_{\mathbb{Z}_p^\times} f(x)\cdot x^{-1}\mu := \int_{\mathbb{Z}_p^\times} x^{-1} f(x)\cdot \mu, \tag{4-3}$$

and that

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

We comment further on this multiplication by x^{-1} in Remark 12.7.

Definition 4.10. Let a be a topological generator of $\mathbb{Z}_p^\times$. The *p-adic zeta function* is

$$\zeta_p := \frac{x^{-1}\,\mathrm{Res}_{\mathbb{Z}_p^\times}\,\mu_a}{\theta_a} \in Q(\mathbb{Z}_p^\times).$$

Proposition 4.11. *The element* ζ_p *is a well-defined pseudomeasure satisfying*

$$\int_{\mathbb{Z}_p^\times} x^k \cdot \zeta_p = (1-p^{k-1})\zeta(1-k) \quad \textit{for all } k>0.$$

Proof. We see ζ_p is a pseudomeasure by Lemma 3.38. It is independent of the choice of a by Lemma 3.36(iii).

Using (3-11) (to integrate the pseudomeasure) and Proposition 4.8, we obtain the interpolation property

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

The result follows since $\zeta(1-k) \neq 0$ if and only if k is even (that is, if and only if $(-1)^k = 1$). □

We finally prove Theorem 4.1. Existence of the pseudomeasure is Proposition 4.11. To conclude the proof we need only show uniqueness; but this follows from Lemma 3.36(iii). □

5. Interpolation at Dirichlet characters

In our study of the Kubota–Leopoldt p-adic L-function, the entire construction was essentially built to interpolate special values of the Riemann zeta function, so this property should not have come as a surprise. Now, however, some real magic happens. Since the introduction, we've not mentioned Dirichlet L-functions once — but, miraculously, the Kubota–Leopoldt p-adic L-function also interpolates Dirichlet L-values as well.

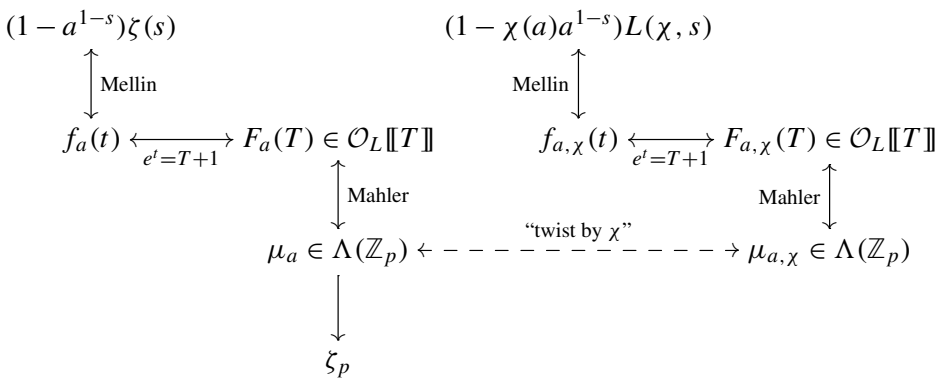
5.1. ***Characters of p-power conductor.*** We start studying the interpolation properties when twisting by a Dirichlet character of conductor a power of p.

Theorem 5.1. *Let χ be a (primitive) Dirichlet character of conductor p^n for some integer $n \geq 1$ (seen as a locally constant character of $\mathbb{Z}_p^\times$; see Section 2.4.2). Then, for $k > 0$, we have*

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

The rest of this subsection will contain the proof of this result. The proof is somewhat calculation-heavy, but — given familiarity with the dictionary between measures and power series — is not conceptually difficult.

In particular: the Riemann zeta function was the complex Mellin transform of a real analytic function, which — via Theorem 2.4 — gave us a formula for its special values. Under the transformation $e^t = T + 1$, we obtained a p-adic power series; and under the measures–power series correspondence given by the Mahler transform, this gave us a measure on $\mathbb{Z}_p$, from which we constructed ζ_p. To obtain interpolation at Dirichlet characters, we pursue this in reverse, as summarised in the diagram at the top of the next page.



Firstly, we introduce a twisting operation on measures. If μ is a measure on $\mathbb{Z}_p$, we define a measure μ_χ on $\mathbb{Z}_p$ by

$$\int_{\mathbb{Z}_p} f(x)\cdot\mu_\chi = \int_{\mathbb{Z}_p} \chi(x)f(x)\cdot\mu. \tag{5-1}$$

Observe that, as χ is supported on $\mathbb{Z}_p^\times$, the twisted measure μ_χ is automatically supported on $\mathbb{Z}_p^\times$ as well. In particular, under this we have

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k\cdot\zeta_p = \int_{\mathbb{Z}_p^\times} x^k\cdot(\zeta_p)_\chi = (\partial^k\mathscr{A}_{(\zeta_p)_\chi})(0),$$

where the last equality follows from Corollary 3.30. Thus we want to determine the Mahler transform of μ_χ in terms of $\mathscr{A}_\mu$, for which we use our measure-theoretic toolkit. This requires a classical definition.

Definition 5.2. Let χ be a primitive Dirichlet character of conductor p^n, $n\geq 1$. Define the *Gauss sum of* χ as

$$G(\chi) := \sum_{c\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)\varepsilon_{p^n}^c,$$

where $(\varepsilon_{p^n})_{n\in\mathbb{N}}$ denotes a system of primitive p-power roots of unity in $\overline{\mathbb{Q}}_p$ such that $\varepsilon_{p^{n+1}}^p=\varepsilon_{p^n}$ for all $n\geq 0$ (if we fix an isomorphism $\overline{\mathbb{Q}}_p\cong\mathbb{C}$, then one can take $\varepsilon_{p^n}:=e^{2\pi i/p^n}$).

Remark 5.3. We note the following basic properties of Gauss sums (see [30, Section 4.3]):

(i) $G(\chi)G(\chi^{-1})=\chi(-1)p^n$.

(ii) $G(\chi)=\chi(a)\sum_{c\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\chi(c)\varepsilon_{p^n}^{ac}$ for any $a\in\mathbb{Z}_p^\times$.

Lemma 5.4. *The Mahler transform of* μ_χ *is*

$$\mathscr{A}_{\mu_\chi}(T)=\frac{1}{G(\chi^{-1})}\sum_{c\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\chi(c)^{-1}\mathscr{A}_\mu((1+T)\varepsilon_{p^n}^c-1).$$

Proof. Since χ is constant modulo p^n, the measure μ_χ is simply

$$\mu_\chi = \sum_{c \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)\,\mathrm{Res}_{c+p^n\mathbb{Z}_p}(\mu).$$

Using this expression and the formula for the Mahler transform of the restriction of a measure to $c + p^n\mathbb{Z}_p$ given in (3-5), we find that

$$\mathscr{A}_{\mu_\chi}(T) = \frac{1}{p^n} \sum_{b \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(b) \sum_{\xi \in \mu_{p^n}} \xi^{-b} \mathscr{A}_\mu((1+T)\xi - 1).$$

Writing $\mu_{p^n} = \{\varepsilon_{p^n}^c : c = 0, \ldots, p^n - 1\}$, and rearranging the sums, we have

$$\begin{aligned}
\mathscr{A}_{\mu_\chi}(T) &= \frac{1}{p^n} \sum_{c \pmod{p^n}} \sum_{b \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(b)\varepsilon_{p^n}^{-bc} \mathscr{A}_\mu((1+T)\varepsilon_{p^n}^c - 1) \\
&= \frac{1}{p^n} \sum_{c \in (\mathbb{Z}/p^n\mathbb{Z})^\times} G(\chi)\chi(-c)^{-1} \mathscr{A}_\mu((1+T)\varepsilon_{p^n}^c - 1) \\
&= \frac{1}{G(\chi^{-1})} \sum_{c \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)^{-1} \mathscr{A}_\mu((1+T)\varepsilon_{p^n}^c - 1),
\end{aligned}$$

where the second equality follows from Remark 5.3(ii) and the last one from Remark 5.3(i). This finishes the proof. □

We now consider the case where $\mu = \mu_a$ from Definition 4.5, the measure from which we built the Kubota–Leopoldt p-adic L-function, and which has Mahler transform

$$\mathscr{A}_{\mu_a}(T) = \frac{1}{T} - \frac{a}{(1+T)^a - 1}.$$

Applying the above transformation, we obtain a measure $\mu_{\chi,a}$ with Mahler transform

$$F_{\chi,a}(T) = \frac{1}{G(\chi^{-1})} \sum_{c \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)^{-1} \left(\frac{1}{(1+T)\varepsilon_{p^n}^c - 1} - \frac{a}{(1+T)^a \varepsilon_{p^n}^{ac} - 1} \right).$$

Via the standard substitution $e^t = T + 1$, this motivates the study of the function

$$f_{\chi,a}(t) = \frac{1}{G(\chi^{-1})} \sum_{c \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)^{-1} \left(\frac{1}{e^t \varepsilon_{p^n}^c - 1} - \frac{a}{e^{at} \varepsilon_{p^n}^{ac} - 1} \right),$$

by analogy with the case of the Riemann zeta function.

Lemma 5.5. *We have*

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

where $L(f_{\chi,a}, s)$ is as defined in Theorem 2.4.

Moreover, for $k \geq 0$, we have

$$f_{\chi,a}^{(k)}(0) = \begin{cases} -(1-\chi(a)a^{k+1})L(\chi,-k) & \text{if } \chi(-1)(-1)^k = -1, \\ 0 & \text{if } \chi(-1)(-1)^k = 1. \end{cases}$$

Proof. We follow a similar strategy to that used for the Riemann zeta function (in Lemma 2.7). In particular, expanding as a geometric series, we obtain

$$\frac{1}{e^t \varepsilon_{p^n}^c - 1} = \sum_{k\geq 1} e^{-kt} \varepsilon_{p^n}^{-kc}.$$

Then we have

$$L(f_{\chi,a},s) = \frac{1}{\Gamma(s)G(\chi^{-1})} \int_0^\infty \sum_{c\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)^{-1} \sum_{k\geq 1} (e^{-kt}\varepsilon_{p^n}^{-kc} - e^{-akt}\varepsilon_{p^n}^{-akc}) t^{s-1}\, dt.$$

Note that

$$\sum_{c\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)^{-1}\varepsilon_{p^n}^{-akc} = \chi(-ak)G(\chi^{-1}),$$

and similarly for the first term, so that the expression collapses to

$$L(f_{\chi,a},s) = \frac{1}{\Gamma(s)} \int_0^\infty \sum_{k\geq 1} \chi(-k)(e^{-kt} - \chi(a)e^{-akt}) t^{s-1}\, dt.$$

For $\mathrm{Re}(s) \gg 0$, we can rearrange the sum and the integral, and then we can evaluate the k-th term of the sum easily to $(1-\chi(a)a^{1-s})k^{-s}$, giving

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

showing the equality of L-functions.

To see the final statement about special values, we use Theorem 2.4, which immediately says

$$f_{\chi,a}^{(k)}(0) = (-1)^k \chi(-1)(1-\chi(a)a^{k+1})L(\chi,-k). \tag{5-2}$$

To get the claimed statement, we note that

$$\frac{1}{e^{-t}\varepsilon_{p^n}^c - 1} = -1 - \frac{1}{e^t \varepsilon_{p^n}^{-c} - 1},$$

and using this twice, we find

$$f_{\chi,a}(-t) = -\frac{1}{G(\chi^{-1})} \sum_{c\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \chi(c)^{-1} \left(\frac{1}{e^t\varepsilon_{p^n}^{-c} - 1} - \frac{a}{e^{at}\varepsilon_{p^n}^{-ac} - 1} \right).$$

Changing c for $-c$ yields $f_{\chi,a}(-t) = -\chi(-1)f_{\chi,a}(t)$, whence $(-1)^k f_{\chi,a}^{(k)}(0) = -\chi(-1)f_{\chi,a}^{(k)}(0)$. This implies that $f_{\chi,a}^{(k)}(0) = 0$ unless $\chi(-1)(-1)^k = -1$, concluding the proof. □

Remark 5.6. By (5-2) and the above proof, we recover the well-known fact that $L(\chi, -k) = 0$ if $\chi(-1)(-1)^k = 1$.

We can now prove Theorem 5.1.

Proof of Theorem 5.1. Since χ is 0 on $p\mathbb{Z}_p$, we have

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot \mu_a = \int_{\mathbb{Z}_p} \chi(x)x^k \cdot \mu_a = \int_{\mathbb{Z}_p} x^k \cdot \mu_{\chi,a},$$

where $\mu_{\chi,a}$ is the twist of μ_a by χ. We know this integral to be

$$(\partial^k F_{\chi,a})(0) = f_{\chi,a}^{(k)}(0),$$

under the standard transform $e^t = T + 1$. Hence, by Lemma 5.5, we find

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot \mu_a = -(1 - \chi(a)a^{k+1})L(\chi, -k),$$

so that

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot x^{-1}\mu_a = -(1 - \chi(a)a^k)L(\chi, 1-k).$$

By definition, we have

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot \theta_a = -(1 - \chi(a)a^k),$$

and hence we find

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

5.2. ***Nontrivial tame conductors.*** We can go even further. The theorem above deals with the case of "tame conductor 1", in that we have constructed a p-adic measure that interpolates all of the L-values $L(\chi, 1-k)$ for $k > 0$ and $\mathrm{cond}(\chi) = p^n$ with $n \geq 0$ (where trivial conductor corresponds to the Riemann zeta function). More generally, we have the following result.

Theorem 5.7. *Let $D > 1$ be any integer coprime to p, and let η denote a (primitive) Dirichlet character of conductor D. There exists a unique measure $\zeta_\eta \in \Lambda(\mathbb{Z}_p^\times)$ such that, for all primitive Dirichlet characters χ with conductor p^n, $n \geq 0$, and for all $k > 0$, we have*

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot \zeta_\eta = (1 - \chi\eta(p)p^{k-1})L(\chi\eta, 1-k).$$

Remark 5.8. (1) In this case, we obtain a genuine measure rather than a pseudomeasure. As L-functions of nontrivial Dirichlet characters are everywhere holomorphic, there is no need for the smoothing factor involving a.

(2) Implicit in this theorem is the fact that the relevant Iwasawa algebra is defined over a (fixed) finite extension $L/\mathbb{Q}_p$ containing the values of η.

Proof. Since many of the ideas involved in proving the above theorem are present in the case of trivial tame conductor, the proof of Theorem 5.7 is a good exercise. As such, we give only the main ideas involved in the proof.

For χ of p-power conductor, note that the calculation relating $L(f_{\chi,a}, s)$ to $L(\chi, s)$ above was entirely classical, in the sense that p did not appear anywhere. We can thus perform a similar calculation for general conductors. As there is no need for the smoothing factor a, we consider the function

$$f_\eta(t) = -\frac{1}{G(\eta^{-1})} \sum_{c \in (\mathbb{Z}/D\mathbb{Z})^\times} \frac{\eta(c)^{-1}}{e^t \varepsilon_D^c - 1}.$$

(This scaling by -1 also appears in the trivial tame conductor situation, but it is incorporated into θ_a). In the above definition, the Gauss sum $G(\eta^{-1})$ of a Dirichlet character η of conductor D is defined as in Definition 5.2, replacing the power of p by D. Define $F_\eta(T)$ by substituting $T+1$ for e^t, i.e.,

$$F_\eta(T) := -\frac{1}{G(\eta^{-1})} \sum_{c \in (\mathbb{Z}/D\mathbb{Z})^\times} \frac{\eta(c)^{-1}}{(1+T)\varepsilon_D^c - 1}. \tag{5-3}$$

Expanding the geometric series, we find

$$F_\eta(T) = -\frac{1}{G(\eta^{-1})} \sum_{c \in (\mathbb{Z}/D\mathbb{Z})^\times} \eta(c)^{-1} \sum_{k \geq 0} \frac{\varepsilon_D^{kc}}{(\varepsilon_D^c - 1)^{k+1}} T^k.$$

This is an element of $\mathscr{O}_L[\![T]\!]$ for some sufficiently large finite extension L of $\mathbb{Q}_p$, since the Gauss sum is a p-adic unit (indeed, we have $G(\eta)G(\eta^{-1}) = \eta(-1)D$ and D is coprime to p) and $\varepsilon_D^c - 1 \in \mathscr{O}_L^\times$ (since it has norm dividing D). There is therefore a measure $\mu_\eta \in \Lambda(\mathbb{Z}_p)$, the Iwasawa algebra over $\mathscr{O}_L$, corresponding to F_η under the Mahler transform.

Lemma 5.9. *We have $L(f_\eta, s) = -\eta(-1)L(\eta, s)$. Hence for $k \geq 0$ we have*

$$\int_{\mathbb{Z}_p} x^k \cdot \mu_\eta = L(\eta, -k).$$

Proof. The first statement is proved in a similar manner to Lemma 5.5. The second is proved by equating ∂ with d/dt and using the general theory described in Theorem 2.4. □

The following is the analogue of Lemma 4.7.

Lemma 5.10. *We have $\psi(F_\eta) = \eta(p)F_\eta$.*

Proof. We show first that

$$\frac{1}{p} \sum_{\xi \in \mu_p} \frac{1}{(1+T)\xi\varepsilon_D^c - 1} = \frac{1}{(1+T)^p \varepsilon_D^{pc} - 1}. \tag{5-4}$$

Expanding each summand as a geometric series, the left-hand side is

$$-\frac{1}{p}\sum_{\xi\in\mu_p}\sum_{n\geq 0}(1+T)^n\varepsilon_D^{nc}\xi^n=-\sum_{n\geq 0}(1+T)^{pn}\varepsilon_D^{pcn},$$

and summing the geometric series gives the right-hand side of (5-4). It follows that

$$\begin{aligned}(\varphi\circ\psi)(F_\eta)&=-\frac{1}{pG(\eta)^{-1}}\sum_{\xi\in\mu_p}\sum_{c\in(\mathbb{Z}/D\mathbb{Z})^\times}\frac{\eta(c)^{-1}}{(1+T)\xi\varepsilon_D^c-1}\\&=-\frac{1}{G(\eta^{-1})}\sum_{c\in(\mathbb{Z}/D\mathbb{Z})^\times}\frac{\eta(c)^{-1}}{(1+T)^p\varepsilon_D^{pc}-1}\\&=\eta(p)\varphi(F_\eta).\end{aligned}$$

The result now follows from the injectivity of φ. □

We can now show the interpolation property at powers of x.

Lemma 5.11. *We have*

$$\int_{\mathbb{Z}_p^\times}x^k\cdot\mu_\eta=(1-\eta(p)p^k)L(\eta,-k).$$

Proof. By Lemma 5.10 we have

$$\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu_\eta)=(1-\varphi\circ\psi)(\mu_\eta)=\mu_\eta-\eta(p)\varphi(\mu_\eta),$$

and

$$\int_{\mathbb{Z}_p}x^k\cdot\varphi(\mu_\eta)=p^k\int_{\mathbb{Z}_p}x^k\cdot\mu_\eta.$$

The result now follows from Lemma 5.9. □

Now let χ be a Dirichlet character of conductor p^n for some $n\geq 0$, and let $\theta:=\chi\eta$ the product (a Dirichlet character of conductor Dp^n). For such $\theta=\chi\eta$, we define

$$\mu_\theta:=(\mu_\eta)_\chi. \tag{5-5}$$

Using Lemma 5.4, we find easily that:

Lemma 5.12. *The Mahler transform of μ_θ is*

$$F_\theta(T):=\mathscr{A}_{\mu_\theta}(T)=-\frac{1}{G(\theta^{-1})}\sum_{c\in(\mathbb{Z}/Dp^n\mathbb{Z})^\times}\frac{\theta(c)^{-1}}{(1+T)\varepsilon_{Dp^n}^c-1}.$$

Via a calculation essentially identical to the cases already seen, we can prove

$$\int_{\mathbb{Z}_p}\chi(x)x^k\cdot\mu_\eta=\int_{\mathbb{Z}_p}x^k\cdot\mu_\theta=L(\theta,-k)$$

and that

$$\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu_\theta)=(1-\theta(p)\varphi)\mu_\theta. \tag{5-6}$$

(Here, note that if χ is nontrivial, then μ_θ is already supported on $\mathbb{Z}_p^\times$; but this is consistent, as $\theta(p) = 0$ in this case). Combining the above we find

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot \mu_\eta = (1 - \theta(p)p^k)L(\theta, -k).$$

Finally, to complete the proof of Theorem 5.7 and to ensure compatibility with the construction of ζ_p, we introduce a shift by 1. The following is directly analogous to the construction of ζ_p; note again that ζ_η is truly a measure, not a pseudomeasure.

Definition 5.13. Define $\zeta_\eta := x^{-1} \operatorname{Res}_{\mathbb{Z}_p^\times}(\mu_\eta)$.

We see that

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k \cdot \zeta_\eta = (1 - \theta(p)p^{k-1})L(\theta, 1-k),$$

which completes the proof of Theorem 5.7. □

5.3. ***Analytic functions on $\mathbb{Z}_p$ via the Mellin transform.*** The reader should hopefully now be convinced that measures are a natural language with which to discuss p-adic L-functions. In this subsection, we use this (more powerful) language to answer the question we originally posed in the introduction: namely, we define analytic functions on $\mathbb{Z}_p$ interpolating the values $\zeta(1-k)$ for $k > 0$. In passing from measures to analytic functions on $\mathbb{Z}_p$, we lose the clean interpolation statements. In particular, there is no *single* analytic function on $\mathbb{Z}_p$ interpolating the values $\zeta(1-k)$ for all $k > 0$, but rather $p-1$ different "branches" of the Kubota–Leopoldt p-adic L-function on $\mathbb{Z}_p$, each interpolating a different range.

The reason we cannot define a single p-adic L-function on $\mathbb{Z}_p$ is down to the following technicality. We'd *like* to be able to define "$\zeta_p(s) = \int_{\mathbb{Z}_p^\times} x^{-s} \cdot \zeta_p$" for $s \in \mathbb{Z}_p$. The natural way to define the exponential $x \mapsto x^s$ is as

$$x^s = \exp(s \cdot \log(x)),$$

but unfortunately in the p-adic world the exponential map does not converge on all of $\mathbb{Z}_p$, so this is not well defined for general $x \in \mathbb{Z}_p^\times$. Instead:

Lemma 5.14. *The p-adic exponential map converges on $p\mathbb{Z}_p$. Hence, for any $s \in \mathbb{Z}_p$, the function $1 + p\mathbb{Z}_p \to \mathbb{Z}_p$ given by $x \mapsto x^s := \exp(s \cdot \log(x))$ is well defined.*

Proof. This is a standard result in the theory of local fields; see, for example, [11, Section 12]. □

Definition 5.15. Recall that we assume p to be odd and that we have a decomposition $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. Let

$$\omega : \mathbb{Z}_p^\times \to \mu_{p-1} \quad \text{and} \quad \langle \cdot \rangle : \mathbb{Z}_p^\times \to 1 + p\mathbb{Z}_p,$$

where $\omega(x) :=$ Teichmüller lift of the reduction modulo p of x and $\langle x\rangle := \omega^{-1}(x)x$ denote the projections to the first and second factors respectively. If $x \in \mathbb{Z}_p^\times$, then we can write $x = \omega(x)\langle x\rangle$.

By Lemma 5.14, the function $x \mapsto \langle x\rangle^s$ is well defined for any $s \in \mathbb{Z}_p$. For each $i = 1, \ldots, p-1$ we can define an injection

$$\mathbb{Z}_p \hookrightarrow \mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times), \quad s \mapsto [x \mapsto \omega(x)^i\langle x\rangle^s],$$

and hence we can define a meromorphic function as follows.

Definition 5.16. We define the i-th branch of the p-adic zeta function as

$$\zeta_{p,i} : \mathbb{Z}_p \to \mathbb{C}_p, \quad s \mapsto \int_{\mathbb{Z}_p^\times} \omega(x)^i\langle x\rangle^{1-s} \cdot \zeta_p.$$

This function *does not* interpolate as wide a range of values as the measure ζ_p, because the character x^k can be written in the form $\omega(x)^i\langle x\rangle^k$ if and only if $k \equiv i \pmod{p-1}$, and in this case x^k is the value of $\omega(x)^i\langle x\rangle^{1-s}$ at the value $s = 1-k$. Then we have the following result.

Theorem 5.17. *For all $k \geq 1$ with $k \equiv i \pmod{p-1}$, we have*

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

Note that the above theorem implies that $\zeta_{p,i}$ is identically zero whenever i is odd (as by Corollary 2.8 the value $\zeta(1-k)$ is zero for every odd positive integer $k \geq 1$). More generally, we can twist by Dirichlet characters as we have done before.

Definition 5.18. Let $\theta = \chi\eta$ be a Dirichlet character, where η has conductor D prime to p and χ has conductor p^n for $n \geq 0$. Define

$$L_p(\theta, s) := \int_{\mathbb{Z}_p^\times} \chi(x)\langle x\rangle^{1-s} \cdot \zeta_\eta, \quad s \in \mathbb{Z}_p.$$

Remark 5.19. An equivalent definition is

$$L_p(\theta, s) = \int_{\mathbb{Z}_p^\times} \chi\omega^{-1}(x)\langle x\rangle^{-s} \cdot \mu_\eta = \int_{\mathbb{Z}_p^\times} \chi\omega^{s-1}(x)x^{-s} \cdot \mu_\eta. \tag{5-7}$$

Note here we use the measure μ_η, rather than the (shifted-by-1) analogue ζ_η. In [81], the analytic functions $L_p(\theta, s)$ are constructed directly without using measures, and the more direct approach differs from the one obtained using our measure-theoretic approach by precisely this factor of ω. This twist by 1 also appears naturally when we study the Iwasawa Main Conjecture.

Theorem 5.20. *For all $k \geq 1$, we have*

$$L_p(\theta, 1-k) = (1-\theta\omega^{-k}(p)p^{k-1})L(\theta\omega^{-k}, 1-k).$$

Proof. We use the description of (5-7). From the definitions, we have

$$\chi\omega^{-1}(x)\langle x\rangle^{k-1} = \chi\omega^{-k}(x)\cdot\omega^{k-1}(x)\langle x\rangle^{k-1} = \chi\omega^{-k}(x)x^{k-1},$$

so that

$$\begin{aligned}\int_{\mathbb{Z}_p^\times} \chi(x)\langle x\rangle^{k-1}\cdot\mu_\eta &= \int_{\mathbb{Z}_p^\times} \chi\omega^{-k}(x)x^{k-1}\cdot\mu_\eta \\ &= (1-\theta\omega^{-k}(p)p^{k-1})L(\theta\omega^{-k},1-k),\end{aligned}$$

as required. The last equality here is Lemma 5.11. □

Remark 5.21. Directly from the definitions, we have $\zeta_{p,i}(s) = L_p(\omega^i, s)$. Hence for arbitrary $k > 0$, Theorem 5.20 gives

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

Of course, ω^{i-k} is just the trivial character when $i \equiv k \pmod{p-1}$, so we recover Theorem 5.17 from Theorem 5.20.

In general, for any measure μ on $\mathbb{Z}_p^\times$ one can define

$$\mathrm{Mel}_{\mu,i}(s) = \int_{\mathbb{Z}_p^\times} \omega(x)^i\langle x\rangle^s\cdot\mu,$$

the *Mellin transform* of μ at i. We have then $\zeta_{p,i}(s) = \mathrm{Mel}_{\zeta_p,i}(1-s)$. This transform gives a way to pass from p-adic measures on $\mathbb{Z}_p$ to analytic functions on $\mathbb{Z}_p$.

Remark 5.22. The results of this section are simply a more concrete version of Remark 3.47. There we described how a measure (resp. pseudomeasure) μ on $\mathbb{Z}_p^\times$ gives rise to a rigid analytic (resp. rigid meromorphic) function F_μ on weight space $\mathcal{W}(\mathbb{C}_p)$. The function $\zeta_{p,i}$ above corresponds to the restriction of F_μ to the open ball $U_{\omega^i} \subset \mathcal{W}(\mathbb{Z}_p)$ (again explaining why we need $p-1$ such functions, corresponding to the $p-1$ disjoint open balls).

6. The values at $s = 1$

In the following we give an example of further remarkable links between the classical and p-adic zeta functions. Let θ be a nontrivial Dirichlet character, which as usual we write in the form $\chi\eta$, where χ has conductor p^n and η has conductor D prime to p. By Theorem 5.7, for any integer $k > 0$, we have

$$\int_{\mathbb{Z}_p^\times} \chi(x)x^k\cdot\zeta_\eta = L(\theta,1-k).$$

It's natural to ask what happens outside the range of interpolation $k > 0$. In particular, what happens when we take $k = 0$? Since this is *outside* the range of interpolation, this value may a priori have nothing to do with classical L-values. Indeed, the

classical value $L(\theta, 1)$ is transcendental,[10] so one cannot see it as a p-adic number in a natural way. However, even though we cannot directly equate the two values, it turns out that there is a formula for the p-adic L-function at $s = 1$ which is strikingly similar to its classical analogue.

Theorem 6.1. *Let θ be a nontrivial Dirichlet character of conductor N, and let ε_N denote a primitive N-th root of unity. Then*:

(i) (*classical value at $s = 1$*). *We have*

$$L(\theta, 1) = -\frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \log(1 - \varepsilon_N^c).$$

(ii) (*p-adic value at $s = 1$*). *We have*

$$L_p(\theta, 1) = -(1 - \theta(p)p^{-1}) \frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \log_p(1 - \varepsilon_N^c).$$

Remark 6.2. Part (ii) of Theorem 6.1 is due to Leopoldt. Values in the range of interpolation, where the link to classical L-values is explicit, are often called *critical* values. Values outside this range, such as those studied in Theorem 6.1, are called *noncritical* values. The above result is an instance of the p-adic Beilinson or Perrin-Riou conjectures, which give arithmetic descriptions of noncritical special values of p-adic L-functions. We refer the interested reader to [67] (or Remark 6.8 below) for more details on this.

If θ is an odd character, both sides of the p-adic formula vanish. In any case, the formulae are identical up to replacing log with its p-adic avatar and, as usual, deleting the Euler factor at p. This result can be used to prove a p-adic analogue of the class number formula.

6.1. ***The complex value at $s = 1$.*** For completeness, we prove the complex case of Theorem 6.1, following [81, Theorem 4.9].

Proof of Theorem 6.1 (i). Write

$$L(\theta, s) = \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta(a) \sum_{n \equiv a \pmod{D}} n^{-s}.$$

Using the fact that

$$\frac{1}{N} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})} \varepsilon_N^{(a-n)c} = \begin{cases} 0 & \text{if } n \not\equiv a \bmod N, \\ 1 & \text{if } n \equiv a \bmod N, \end{cases}$$

[10] This follows from Baker's theorem and Theorem 6.1(i).

we show that the above formula equals

$$\begin{aligned}\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\theta(a)\frac{1}{N}\sum_{n\geq 1}\sum_{c\in(\mathbb{Z}/N\mathbb{Z})}\varepsilon_N^{(a-n)c}n^{-s}&\\ =\frac{1}{N}\sum_{c\in(\mathbb{Z}/N\mathbb{Z})}\Bigg(\sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\theta(a)\varepsilon_N^{ac}\Bigg)\sum_{n\geq 1}\frac{\varepsilon_N^{-nc}}{n^s}&\\ =\frac{G(\theta)}{N}\sum_{c\in(\mathbb{Z}/N\mathbb{Z})}\theta^{-1}(c)\sum_{n\geq 1}\frac{\varepsilon_N^{-nc}}{n^s}&\\ =\frac{\theta(-1)}{G(\theta^{-1})}\sum_{c\in(\mathbb{Z}/N\mathbb{Z})^\times}\theta^{-1}(c)\sum_{n\geq 1}\frac{\varepsilon_N^{-nc}}{n^s}&\\ =\frac{1}{G(\theta^{-1})}\sum_{c\in(\mathbb{Z}/N\mathbb{Z})^\times}\theta^{-1}(c)\sum_{n\geq 1}\frac{\varepsilon_N^{nc}}{n^s}.&\qquad(6\text{-}1)\end{aligned}$$

The penultimate equality uses the standard identity $G(\theta)G(\theta^{-1})=\theta(-1)\operatorname{cond}(\theta)$ of Gauss sums (see Remark 5.3(i)) and that $\theta^{-1}(c)=0$ if $(c,N)\neq 1$, and the last equality follows from the change of variables $c\mapsto -c$.

Finally we evaluate this expression at $s=1$. As θ is not trivial we have $N>1$, so $\varepsilon_N^c\neq 1$ for any $c\in(\mathbb{Z}/N\mathbb{Z})^\times$. Thus we may consider the Taylor series expansion

$$-\log(1-\varepsilon_N^c)=\sum_{n\geq 1}\varepsilon_N^{nc}n^{-1}.$$

Substituting this into (6-1), we see the series converges at $s=1$ to the required result. □

Remark 6.3. We can further refine this expression depending on the parity of θ. If θ is even then $\theta^{-1}(c)\log(1-\varepsilon_N^c)+\theta^{-1}(-c)\log(1-\varepsilon_N^{-c})=2\theta^{-1}(c)\log|1-\varepsilon_N^c|$, so, rearranging,

$$L(\theta,1)=-\frac{1}{G(\theta^{-1})}\sum_{c\in(\mathbb{Z}/N\mathbb{Z})^\times}\theta^{-1}(c)\log|1-\varepsilon^c|.$$

If θ is odd, we can use the functional equation to obtain

$$L(\theta,1)=-i\pi\frac{1}{G(\theta^{-1})}B_{1,\theta^{-1}},$$

where $B_{k,\theta^{-1}}$ denotes the k-th twisted Bernoulli number (see [81, Chapter 4]).

6.2. ***The p-adic value at s = 1.*** We now compute

$$L_p(\theta,1):=\int_{\mathbb{Z}_p^\times}\chi(x)x^{-1}\cdot\mu_\eta=\int_{\mathbb{Z}_p^\times}x^{-1}\cdot\mu_\theta.\qquad(6\text{-}2)$$

A tempting argument to study this goes as follows. Suppose that k is divisible by $p-1$. We know from (5-7) that

$$L_p(\theta, 1-k) = \int_{\mathbb{Z}_p^\times} \chi(x) x^{k-1} \cdot \mu_\eta,$$

noting that $\omega^{(1-k)-1} = \omega^{-k} = 1$ as ω has order $p-1$. For $k > 0$, we showed above that

$$\int_{\mathbb{Z}_p^\times} \chi(x) x^{k-1} \cdot \mu_\eta = \mathscr{A}_{\mathrm{Res}_{\mathbb{Z}_p^\times}(x^{k-1}\mu_\theta)}(0) = (1-\theta(p)p^{k-1})(\partial^{k-1}F_\theta)(0).$$

We want to compute this for $k = 0$. Identically we could try to argue that

$$L_p(\theta, 1) = \mathscr{A}_{\mathrm{Res}_{\mathbb{Z}_p^\times}(x^{-1}\mu_\theta)}(0) = (1-\theta(p)p^{-1})(\partial^{-1}F_\theta)(0). \tag{6-3}$$

Then, recalling that by Lemma 5.12 we have

$$F_\theta(T) = -\frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \frac{\theta(c)^{-1}}{(1+T)\varepsilon_N^c - 1},$$

we observe that, if we define

$$\widetilde{F}_\theta(T) = -\frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \log((1+T)\varepsilon_N^c - 1),$$

then formally $\partial \widetilde{F}_\theta = F_\theta$; we will show this in the proof of Lemma 6.5 below. In particular, $\widetilde{F}_\theta$ is a good candidate for $\partial^{-1}F_\theta$. Plugging in $T = 0$ and combining with (6-3) would give the claimed value of $L_p(\theta, 1)$.

In order to make this reasoning rigorous, one needs to deal with the fact that x^{-1} is not a well-defined operation on measures on $\mathbb{Z}_p$, rendering $x^{-1}\mu_\theta$ ill-defined. On power series, this is captured by the indeterminacy in defining ∂^{-1}. In particular, $\widetilde{F}_\theta(T)$ is *not* necessarily a bounded power series, so under the Mahler correspondence, does not correspond to a p-adic measure. However we do have the following. Recall that $\mathscr{R}^+$ (from Remark 3.39) denotes the space of power series $\sum a_n T^n$ such that $|a_n| r^n \to 0$ for any $0 \le r < 1$.

Lemma 6.4. *The power series $\widetilde{F}_\theta(T)$ is an element of $\mathscr{R}^+$.*

Proof. We can write

$$\begin{aligned}\log((1+T)\varepsilon_N^c - 1) &= \log_p(\varepsilon_N^c - 1) + \log\left(1 + \frac{\varepsilon_N^c T}{\varepsilon_N^c - 1}\right) \\ &= \log_p(\varepsilon_N^c - 1) + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \cdot \frac{\varepsilon_N^{cn}}{(\varepsilon_N^c - 1)^n} T^n.\end{aligned}$$

We now consider two cases. If $(N, p) = 1$, we know that $(\varepsilon_N^c - 1)$ is a p-adic unit; then the coefficient of T^n has p-adic valuation bounded below by $-v_p(n)$. This means the coefficients in $\widetilde{F}_\theta(T)$ have logarithmic growth, and in particular

$\widetilde{F}_\theta(T) \in \mathscr{R}^+$. More generally, suppose that $N = Dp^n$ with $(D, p) = 1$. We write $\theta = \eta\chi$, with η and χ characters of conductors D and p^n respectively. Then, as in Lemma 5.4 or Lemma 5.12, we have

$$\widetilde{F}_\theta(T) = (\widetilde{F}_\eta)_\chi(T) = -\frac{1}{G(\chi^{-1})} \sum_{c \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \chi^{-1}(c)\widetilde{F}_\eta((1+T)\varepsilon_{p^n}^c - 1).$$

As $\widetilde{F}_\eta(T) \in \mathscr{R}^+$, the same holds for $\widetilde{F}_\theta(T)$. □

By Theorem 3.43, $\widetilde{F}_\theta(T)$ is the Mahler transform of a locally analytic distribution $\widetilde{\mu}_\theta$ on $\mathbb{Z}_p$. We now relate this distribution to $x^{-1}\operatorname{Res}_{\mathbb{Z}_p^\times}(\mu_\theta)$, as appeared in (6-2).

Lemma 6.5. *We have*

$$x\widetilde{\mu}_\theta = \mu_\theta.$$

In particular,

$$\operatorname{Res}_{\mathbb{Z}_p^\times}(\widetilde{\mu}_\theta) = x^{-1}\operatorname{Res}_{\mathbb{Z}_p^\times}(\mu_\theta).$$

Proof. The first equality can be checked on Mahler transforms. By Lemma 3.29, this means showing

$$\partial\widetilde{F}_\theta(T) = (1+T)\frac{d}{dT}\widetilde{F}_\theta(T) = \mathscr{A}_{\mu_\theta}(T). \tag{6-4}$$

By Lemma 5.12, we have

$$\mathscr{A}_{\mu_\theta}(T) = F_\theta(T) = -\frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \frac{\theta(c)^{-1}}{(1+T)\varepsilon_N^c - 1}.$$

Then (6-4) follows immediately from the formula

$$\partial \log((1+T)\varepsilon_D^c - 1) = \frac{(1+T)\varepsilon_D^c}{(1+T)\varepsilon_D^c - 1} = 1 + \frac{1}{(1+T)\varepsilon_D^c - 1}$$

and the fact that $\sum_{c \in (\mathbb{Z}/D\mathbb{Z})^\times} \theta^{-1}(c) = 0$.

To see the second equality, note that as measures on $\mathbb{Z}_p^\times$, we visibly have $x\operatorname{Res}_{\mathbb{Z}_p^\times}(\widetilde{\mu}_\theta) = \operatorname{Res}_{\mathbb{Z}_p^\times}(\mu_\theta)$. It follows that $\operatorname{Res}_{\mathbb{Z}_p^\times}(\widetilde{\mu}_\theta) = x^{-1}\operatorname{Res}_{\mathbb{Z}_p^\times}(\mu_\theta)$ as "multiplication by x" is an invertible operator on measures/distributions on $\mathbb{Z}_p^\times$. □

From the above, we now know that

$$L_p(\theta, 1) = \mathscr{A}_{x^{-1}\operatorname{Res}_{\mathbb{Z}_p^\times}(\mu_\theta)}(0) = \mathscr{A}_{\operatorname{Res}_{\mathbb{Z}_p^\times}(\widetilde{\mu}_\theta)}(0) = ((1 - \varphi \circ \psi)\widetilde{F}_\theta)(0), \tag{6-5}$$

where the last equality follows from the formula for the restriction of a distribution to $\mathbb{Z}_p^\times$ (see (3-8), and Remark 3.45). We are now ready to prove Theorem 6.1(ii).

Proof of Theorem 6.1 (ii). We compute the right-hand side of (6-5). Recall from Section 3.5.5 that $\varphi \circ \psi(\widetilde{F}_\theta)$ is the Mahler transform of $\operatorname{Res}_{p\mathbb{Z}_p}(\widetilde{\mu}_\theta)$. Recall $N = Dp^n$ and $\theta = \eta\chi$, where η has prime-to-p conductor D, and χ has conductor p^n. To compute this we break into two cases.

(1) First assume that $n > 1$, so that $\chi \neq 1$; then, as $\chi|_{p\mathbb{Z}_p} = 0$, we see $\widetilde{\mu}_\theta = (\widetilde{\mu}_\eta)_\chi$ is automatically supported on $\mathbb{Z}_p^\times$ by (5-1). In particular, $\mathrm{Res}_{p\mathbb{Z}_p}(\widetilde{\mu}_\theta) = 0$, and thus $\varphi \circ \psi(\widetilde{F}_\theta) = 0$. In particular, in this case,

$$L_p(\theta, 1) = \widetilde{F}_\theta(0).$$

It is convenient to write this in the form $L_p(\theta, 1) = (1 - \theta(p)p^{-1})\widetilde{F}_\theta(0)$ using that $\theta(p) = 0$.

(2) Now assume $n = 0$, so $N = D$ is coprime to p and hence $\theta = \eta$. By (3-9),

$$\begin{aligned}\varphi \circ \psi(\widetilde{F}_\theta) &= \frac{1}{p}\sum_{\xi \in \mu_p} \widetilde{F}_\theta((1+T)\xi - 1) \\ &= -\frac{1}{G(\theta^{-1})} \cdot \frac{1}{p} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \sum_{\xi \in \mu_p} \log_p((1+T)\xi\varepsilon_N^c - 1).\end{aligned}$$

Evaluating at $T = 0$, we get

$$\begin{aligned}\varphi \circ \psi(\widetilde{F}_\theta)(0) &= -\frac{1}{G(\theta^{-1})} \cdot \frac{1}{p} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \sum_{\xi \in \mu_p} \log_p(\xi\varepsilon_N^c - 1) \\ &= -\frac{1}{G(\theta^{-1})} \cdot \frac{1}{p} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \log_p(\varepsilon_N^{pc} - 1) \\ &= -\frac{1}{G(\theta^{-1})} \cdot \frac{\theta(p)}{p} \sum_{c' \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c') \log_p(\varepsilon_N^{c'} - 1) \\ &= \frac{\theta(p)}{p}\widetilde{F}_\theta(0).\end{aligned}$$

Here, we used that, since $p \nmid N$, the assignment $c \mapsto c' = pc$ defines an automorphism of $(\mathbb{Z}/N\mathbb{Z})^\times$. Hence in this case we also find that

$$L_p(\theta, 1) = ((1 - \varphi \circ \psi)\widetilde{F}_\theta)(0) = (1 - \theta(p)p^{-1})\widetilde{F}_\theta(0).$$

To complete the proof, we simply evaluate the expression $\widetilde{F}_\theta(0)$ (and use that $\log_p(x) = \log_p(-x)$ for $x \in \mathbb{C}_p^\times$) to find, for all N, that

$$L_p(\theta, 1) = -(1 - \theta(p)p^{-1})\frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \log_p(1 - \varepsilon_N^c). \qquad \square$$

Remark 6.6. Theorem 6.1 has been generalised by Coleman in [17] for every positive integer value $s = k \geq 1$. More precisely, for $s, z \in \mathbb{C}$, let $\mathrm{Li}_s(z) := \sum_{n \geq 1} z^n/n^s$ be the polylogarithm function; recall that it admits a unique analytic continuation to $\mathbb{C} \setminus \{z \in \mathbb{R} : z \geq 1\}$. In particular, one sees that $\mathrm{Li}_s(1) = \zeta(s)$, and $\mathrm{Li}_1(z) = -\log(1 - z)$. Coleman constructed p-adic analogues $\mathrm{Li}_{k,p}(z)$, which are locally analytic functions on $\mathbb{C}_p \setminus \{1\}$, and showed:

Theorem 6.7 [17]. *Let θ be a nontrivial Dirichlet character of conductor N, let $k \geq 1$ be an integer, and let ε_N denote a primitive N-th root of unity. Then*:

(i) (*classical value at $s = k$*). *We have*

$$L(\theta, k) = \frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \operatorname{Li}_k(\varepsilon_N^c).$$

(ii) (*p-adic value at $s = k$*). *We have*

$$L_p(\theta, k) = (1 - \theta(p)p^{-k}) \frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(c) \operatorname{Li}_{k,p}(\varepsilon_N^c).$$

Remark 6.8. We highlighted in Remark 6.2 that Theorem 6.1(ii) is an instance of Perrin-Riou's p-adic Beilinson conjectures. More precisely, her conjectures describe special, noncritical values of p-adic L-functions of motives in terms of arithmetic data. Specialised to the case of the Kubota–Leopoldt p-adic L-function (see [67, Section 4.3.3]), this gives formulas for the values of $L_p(\theta, k)$ in terms of p-adic regulators of the cyclotomic units, special elements that we will see later; the right-hand sides of Theorems 6.1(ii) and 6.7(ii) can be reinterpreted in such terms, justifying Remark 6.2. We refer to [67] for more details, and [18] for an excellent survey on all of this.

We also mention the pioneering work of Gross [38], based on Coleman's work, as well as [50], for another approach expressing values of Dirichlet p-adic L-functions at odd positive integers in terms of syntomic regulators and K-theory.

7. The residue of ζ_p at $s = 1$

In the previous section, we described the value of the Dirichlet p-adic L-functions $L_p(\theta, s)$ at $s = 1$ for a nontrivial Dirichlet character θ. We now turn to the value at $s = 1$ of the *untwisted* p-adic zeta function, that is, the analogue when θ is trivial. Recall the Riemann zeta function has a simple pole at $s = 1$ with residue 1 and that, in the p-adic world, we have defined the p-adic zeta function as a pseudomeasure (rather than a measure) which implies, as explained in Remark 3.47, that there might be a potential pole at the trivial character. We now show that there is indeed a simple pole here, and calculate its residue.

As with $L_p(\theta, s)$, it is convenient to use the language of analytic functions $\zeta_{p,i}$ from Definition 5.16. The behaviour of ζ_p at the trivial character is captured by the behaviour of $\zeta_{p,p-1}(s)$ at $s = 1$. The main result of this section is the following.

Theorem 7.1. *Let $i \in \{1, 2, \ldots, p-1\}$. The following assertions hold*:

(i) *If $i \neq p-1$, then $\zeta_{p,i}$ is analytic at $s = 1$.*

(ii) *The function $\zeta_{p,p-1}$ has a simple pole at $s = 1$ with residue $(1 - p^{-1})$.*

The proof will occupy the rest of this section.

For any $i \in \{1, 2, \ldots, p-1\}$, by Definition 5.16 we have

$$\zeta_{p,i}(s) = \int_{Z_p^\times} \omega(x)^i \langle x \rangle^{1-s} \cdot \zeta_p.$$

Now, from Definition 4.10, we have

$$\zeta_p = \frac{x^{-1}\,\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu_a)}{\theta_a} = \frac{x^{-1}\,\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu_a)}{[a]-[1]},$$

where a is any topological generator of $\mathbb{Z}_p^\times$. Thus by the expression (3-11) for evaluating pseudomeasures, we find

$$\zeta_{p,i}(s) = \frac{\int_{\mathbb{Z}_p^\times} \omega(x)^i \langle x \rangle^{1-s} x^{-1} \cdot \mu_a}{\omega(a)^i \langle a \rangle^{1-s} - 1} = \frac{\int_{\mathbb{Z}_p^\times} \omega(x)^{s+i-1} x^{-s} \cdot \mu_a}{\omega(a)^i \langle a \rangle^{1-s} - 1}, \tag{7-1}$$

where we have used $\langle x \rangle = \omega^{-1}(x)x$ in the second equality. Let

$$g_{a,i}(s) := \omega(a)^i \langle a \rangle^{1-s} - 1$$

be the denominator of (7-1).

Lemma 7.2. *The following assertions hold.*

(i) *If $i \neq p-1$, then $g_{a,i}(1) \neq 0$. In particular, Theorem 7.1 (i) holds.*

(ii) *We have $g_{a,p-1}(1) = 0$, and*

$$\lim_{s \to 1} (s-1)^{-1} g_{a,p-1}(s) = -\log_p(a).$$

Proof. Since a is a topological generator of $\mathbb{Z}_p^\times$, we see $\omega(a)$ is a primitive $(p-1)$-th root of unity. Hence the denominator $\omega(a)^i \langle a \rangle^{1-s} - 1$ of (7-1) vanishes at $s = 1$ if and only if $i = p-1$. This already implies Theorem 7.1(i), as the expression (7-1) does not have a pole at $s = 1$.

If $i = p-1$, we know $\omega(a)^i = 1$, so $g_{a,p-1}(1) = 0$. Moreover,

$$\begin{aligned} g_{a,p-1}(s) = \omega(a)^{p-1} \langle a \rangle^{1-s} - 1 &= \langle a \rangle^{1-s} - 1 \\ &= \sum_{n \geq 1} \binom{1-s}{n} (\langle a \rangle - 1)^n \\ &= (1-s) \sum_{n \geq 1} \frac{1}{n} \binom{-s}{n-1} (\langle a \rangle - 1)^n, \end{aligned} \tag{7-2}$$

where in the last equality we have used the identity $\binom{1-s}{n} = \frac{1-s}{n}\binom{-s}{n-1}$ for $n \geq 1$. The sum in (7-2) evaluates at $s = 1$ to

$$\sum_{n \geq 1} \frac{1}{n} \binom{-1}{n-1} (\langle a \rangle - 1)^n = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} (\langle a \rangle - 1)^n = \log_p(\langle a \rangle) = \log_p(a),$$

where we have used $\binom{-1}{n-1} = (-1)^{n-1}$ (direct from Definition 3.20). We deduce that

$$\lim_{s\to 1}[(s-1)^{-1} g_{a,s-1}(s)] = -\log_p(a). \qquad \square$$

Combining Lemma 7.2(ii) with (7-1), we deduce

$$\lim_{s\to 1}(s-1)\zeta_{p,p-1}(s) = -\frac{\int_{\mathbb{Z}_p^\times} x^{-1}\cdot\mu_a}{\log_p(a)}. \tag{7-3}$$

We calculate the numerator in this expression via similar methods to those used in Section 6.2. Recall that $F_a(T) = (1/T) - a/((1+T)^a - 1)$ is the Mahler transform of μ_a; we find a power series $\widetilde{F}_a(T)$ such that $\partial\widetilde{F}_a(T) = F_a(T)$, where $\partial = (1+T)\frac{d}{dT}$. Then, via Lemma 6.5 and directly analogously to (6-5), we find

$$\int_{\mathbb{Z}_p^\times} x^{-1}\mu_a = ((1-\varphi\circ\psi)\widetilde{F}_a)(0). \tag{7-4}$$

To this end, let

$$\widetilde{F}_a(T) := \log\left(\frac{T}{1+T}\cdot\frac{(1+T)^a}{(1+T)^a-1}\right).$$

Lemma 7.3. *Formally, we have*

$$\partial\widetilde{F}_a(T) = F_a(T).$$

Proof. We let the reader check that

$$\partial\log\left(\frac{(1+T)^a-1}{(1+T)^a}\right) = \frac{a}{(1+T)^a-1}.$$

In particular, taking $a=1$, we also get

$$\partial\log\left(\frac{T}{1+T}\right) = \frac{1}{T}.$$

We conclude as

$$\begin{aligned}\partial\widetilde{F}_a(T) &= \partial\log\left(\frac{T}{1+T}\right) - \partial\log\left(\frac{(1+T)^a-1}{(1+T)^a}\right)\\ &= \frac{1}{T} - \frac{a}{(1+T)^a-1} = F_a(T).\end{aligned} \qquad \square$$

As in Lemma 6.4, we must also check that $\widetilde{F}_a(T) \in \mathscr{R}^+$ to use the Mahler correspondence.

Lemma 7.4. *We have* $\widetilde{F}_a(T) \in \mathscr{R}^+$.

Proof. It is convenient to note

$$\widetilde{F}_a(T) = \log\left(\frac{T}{(1+T)^a-1}\cdot(1+T)^{a-1}\right). \tag{7-5}$$

As in Proposition 4.4, write

$$(1+T)^a - 1 = aT(1+Tg(T)), \quad g(T) = \sum_{n\geq 2} a^{-1}\binom{a}{n}T^{n-2}.$$

Recall from the proof of that proposition that we have

$$\frac{1}{(1+T)^a-1} = \frac{1}{aT}(1+Th(T)), \tag{7-6}$$

with

$$h(T) = \sum_{n\geq 1}(-1)^n T^{n-1} g(T)^n \in \mathbb{Z}_p[\![T]\!].$$

We thus see that

$$\frac{T}{(1+T)^a-1} = a^{-1}(1+Th(T)),$$

whose logarithm is given by

$$\begin{aligned}\log\left(\frac{T}{(1+T)^a-1}\right) &= -\log_p(a) + \log(1+Th(T)) \\ &= -\log_p(a) + \sum_{n\geq 1}\frac{(-1)^{n+1}}{n}T^n h(T)^n. \end{aligned}\tag{7-7}$$

As in Lemma 6.4, the coefficients here have logarithmic growth in n, so this lies in $\mathscr{R}^+$. Identically, $(1+T)^{a-1} = 1 + T\sum_{n\geq 1}\binom{a-1}{n}T^{n-1}$ also has well-defined logarithm in $\mathscr{R}^+$. Adding these two elements of $\mathscr{R}^+$ yields $\widetilde{F}_a(T)$ and completes the proof. □

Lemma 7.5. *We have* $((1-\varphi\circ\psi)\widetilde{F}_a)(0) = -(1-p^{-1})\log_p(a)$.

Proof. First, by (7-5) we know that

$$\widetilde{F}_a(0) = \log\left(\frac{T}{(1+T)^a-1}\right)\Big|_{T=0} + \log((1+T)^{a-1})|_{T=0} = -\log_p(a) + 0, \tag{7-8}$$

where we use (7-7) to evaluate the first summand. Secondly, we have

$$\begin{aligned}\varphi\circ\psi(\widetilde{F}_a)(T) &= \frac{1}{p}\sum_{\xi\in\mu_p}\widetilde{F}_a((1+T)\xi - 1) \\ &= \frac{1}{p}\sum_{\xi\in\mu_p}\log\left(\frac{(1+T)\xi-1}{(1+T)\xi}\cdot\frac{(1+T)^a\xi^a}{(1+T)^a\xi^a-1}\right) \\ &= \frac{1}{p}\sum_{\xi\in\mu_p}\log\left(\frac{(1+T)\xi-1}{(1+T)^a\xi^a-1}\cdot(1+T)^{a-1}\xi^{a-1}\right).\end{aligned}$$

This rearranges to

$$\frac{1}{p}\log\Bigg(\prod_{\xi\in\mu_p}\frac{(1+T)\xi-1}{(1+T)^a\xi^a-1}\cdot(1+T)^{a-1}\xi^{a-1}\Bigg) = \frac{1}{p}\log\Bigg(\frac{(1+T)^p-1}{(1+T)^{ap}-1}\cdot(1+T)^{(a-1)p}\Bigg).$$

Here we simplify both terms of the fraction using $\prod_{\xi\in\mu_p}(X\xi-1)=X^p-1$, in the denominator noting that as a is a topological generator of $\mathbb{Z}_p^\times$, we have $\{\xi^a:\xi\in\mu_p\}=\mu_p$. In the final term we use that $\prod_{\xi\in\mu_p}\xi^{a-1}=\big(\prod_{\xi\in\mu_p}\xi\big)^{a-1}=1$.

Writing

$$(1+T)^p-1=pT(1+Tj(T)),\qquad \frac{1}{(1+T)^{ap}-1}=\frac{1}{apT}(1+Tk(T)),$$

analogously to (7-6), we find ultimately that

$$\varphi\circ\psi(\widetilde{F}_a)(T)=\frac{1}{p}\log\Big(\frac{1}{a}(1+Tj(T))(1+Tk(T))\cdot(1+T)^{(a-1)p}\Big),$$

and the right-hand side at $T=0$ collapses to $-p^{-1}\log_p(a)$. Combining with (7-8),

$$\begin{aligned}((1-\varphi\circ\psi)\widetilde{F}_a)(0)&=\widetilde{F}_a(0)-(\varphi\circ\psi)\widetilde{F}_a(0)\\&=-\log_p(a)-p^{-1}\log_p(a)=-(1-p^{-1})\log_p(a),\end{aligned}$$

as required. □

Combining (7-3) and (7-4) with Lemma 7.5, we deduce that

$$\lim_{s\to1}(s-1)\zeta_{p,p-1}(s)=1-p^{-1},$$

completing the proof of Theorem 7.1(ii). □

8. The p-adic family of Eisenstein series

We finally take a brief detour to illustrate another example of p-adic variation in number theory, namely the p-adic variation of modular forms. In constructing the Kubota–Leopoldt p-adic L-function, we have seen many of the key ideas that go into the simplest example of this, namely the p-adic family of Eisenstein series, which we will illustrate below.

Let $k\geq4$ be an even integer. The *Eisenstein series of level k*, defined as

$$G_k(z):=\sum_{\substack{c,d\in\mathbb{Z}\\(c,d)\neq(0,0)}}\frac{1}{(cz+d)^k},\qquad z\in\mathcal{H}:=\{z\in\mathbb{C}:\mathrm{Im}(z)>0\},$$

can be viewed as a two-dimensional analogue of the zeta value $\zeta(k)$. It is an

example of a *modular form of weight* k. In the classical theory of modular forms, one computes the normalised Fourier expansion of such an object to be

$$E_k(z) := \frac{G_k(z)(k-1)!}{2\cdot(2\pi i)^k} = \frac{\zeta(1-k)}{2} + \sum_{n\geq 1}\sigma_{k-1}(n)q^n,$$

where $\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}$ and $q = e^{2i\pi z}$. In particular, it is a power series with rational coefficients. (This is a standard exercise; see [30, Chapter 1.1] for details).

From the definition, we see the Kubota–Leopoldt p-adic L-function as a pseudomeasure that, when evaluated at x^k with $k \geq 4$ even, gives (up to an Euler factor) the constant coefficient of the Eisenstein series of weight k. The idea now is to find measures giving similar interpolations of the other coefficients. Fortunately, these are much easier to deal with: we only need interpolations of the functions $k \mapsto d^k$, where k is varying p-adically. When d is coprime to p, we do this by viewing d as an element of $\mathbb{Z}_p^\times$ and considering the Dirac measure δ_d at d (that is, evaluation at d). Indeed, $\int_{\mathbb{Z}_p^\times} x^k \cdot \delta_d = d^k$ for any $k \in \mathbb{Z}$.

When d is divisible by p, however, we run into an immutable obstacle. There is no Dirac measure on $\mathbb{Z}_p^\times$ corresponding to evaluation at p, since $p \notin \mathbb{Z}_p^\times$. Moreover, the function $k \mapsto p^k$ can *never* be interpolated continuously p-adically; it simply behaves too badly for this to be possible. Suppose there was indeed a measure θ_p with

$$\int_{\mathbb{Z}_p^\times} x^k \cdot \theta_p = p^k,$$

and then suppose k_n is a strictly increasing sequence of integers p-adically tending to k. Then

$$p^{k_n} = \int_{\mathbb{Z}_p^\times} x^{k_n}\cdot\theta_p \to \int_{\mathbb{Z}_p^\times} x^k\cdot\theta_p = p^k,$$

which is clearly impossible since p^{k_n} tends to 0.

We get around this issue by taking p-stabilisations to kill the coefficients at p.

Definition 8.1. We define the *p-stabilisation of E_k* to be

$$E_k^{(p)}(z) := E_k(z) - p^{k-1}E_k(pz).$$

An easy check shows that

$$E_k^{(p)} = \tfrac{1}{2}(1-p^{k-1})\zeta(1-k) + \sum_{n\geq 1}\sigma_{k-1}^p(n)q^n,$$

where

$$\sigma_{k-1}^p(n) = \sum_{\substack{0<d|n\\ p\nmid d}} d^{k-1}.$$

Note $E_k^{(p)}$ is a modular form of weight k and level $\Gamma_0(p) = \left\{\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : p \mid c\right\}$.

We've done all the work in proving the following result.

Theorem 8.2. *There exists a power series*

$$\boldsymbol{E}(z) = \sum_{n\geq 0} A_n q^n \in Q(\mathbb{Z}_p^\times)[\![q]\!]$$

such that:

(a) A_0 *is a pseudomeasure, and* $A_n \in \Lambda(\mathbb{Z}_p^\times)$ *for all* $n \geq 1$.

(b) *For all even* $k \geq 4$, *we have*

$$\int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \boldsymbol{E}(z) := \sum_{n\geq 0} \left(\int_{\mathbb{Z}_p^\times} x^{k-1} \cdot A_n \right) q^n = E_k^{(p)}(z).$$

Proof. The pseudomeasure A_0 is simply $x\zeta_p/2$ (shifting by 1 again, but in the opposite direction to before). We then define

$$A_n = \sum_{\substack{0<d|n \\ p\nmid d}} \delta_d \in \Lambda(\mathbb{Z}_p^\times).$$

By the interpolation property of the Kubota–Leopoldt p-adic L-function, A_0 interpolates the constant term of the Eisenstein series. We also have

$$\int_{\mathbb{Z}_p^\times} x^{k-1} \cdot A_n = \sum_{\substack{0<d|n \\ p\nmid d}} \int_{\mathbb{Z}_p^\times} x^{k-1} \cdot \delta_d = \sum_{\substack{0<d|n \\ p\nmid d}} d^{k-1} = \sigma_{k-1}^p(n),$$

so we get the required interpolation property. □

Remark 8.3. (1) The power series $\boldsymbol{E}(z)$ is an example of a Λ-*adic modular form*. In particular, it can be colloquially described as the statement:

> Eisenstein series vary p-adically continuously as you change the weight; if k and k' are close p-adically, then the Fourier expansions of E_k and $E_{k'}$ are close p-adically.

The theory of p-adic modular forms, and in particular the construction and study of p-adic families of Eisenstein series, was introduced by Serre [73] to give a new construction of the p-adic zeta function of a totally real number field. Indeed, the main idea of Serre's paper (see [73, Corollaire 2]) was to show that if one can interpolate all of the nonconstant coefficients — which, as we saw above, is quite simple — then this automatically gives an interpolation of the constant term, namely the p-adic zeta function, which is much more difficult to interpolate directly.

(2) These results are often presented instead using the weight space $\mathcal{W}$ from Remark 3.47. The integers are naturally a subset of $\mathcal{W}(\mathbb{C}_p)$ via the maps $\kappa_k : x \mapsto x^k$, and two integers k and k' lie in the same unit ball if and only if $k \equiv k' \pmod{p-1}$. Let $\mathscr{O}^+(\mathcal{W})$ be the space of bounded rigid analytic functions on $\mathcal{W}$ (corresponding to measures on $\mathbb{Z}_p^\times$), and $\mathcal{Q}(\mathcal{W})$ the space of rigid meromorphic functions on $\mathcal{W}$

with a possible (simple) pole only at the trivial character (corresponding to pseudo-measures on $\mathbb{Z}_p^\times$). Then we can view $\boldsymbol{E}$ as a power series $\boldsymbol{E}(q) = \sum_{n\geq 0} B_n q^n \in \mathcal{Q}(\mathcal{W})[\![q]\!]$, with $B_n \in \mathscr{O}^+(\mathcal{W})$ for all $n > 0$, such that for all $k \geq 4$, we have $\boldsymbol{E}(q)(\kappa_k) := \sum_{n\geq 0} B_n(\kappa_k) q^n = E_k^{(p)}(z)$. Hence we see $\boldsymbol{E}$ as a p-adic interpolation of the Eisenstein series over the weight space.

(3) These two remarks go hand in hand. Indeed, pioneering work of Hida went much further on the study of p-adic weight families of modular forms, showing that similar families (known as *Hida families*) exist for far more general modular forms. His work has been vastly generalised to the theory of Coleman families and eigenvarieties, parametrising the p-adic variation of modular/automorphic forms over appropriate weight spaces. Such families have important applications to the construction and study of p-adic L-functions; notable constructions in this direction are given in [4; 68]. For a flavour of the theory of Hida and Coleman families of modular forms, see the books [41] or [5].

Part II: Iwasawa's Main Conjecture

The second part of this work is devoted to the motivation, formulation and study of Iwasawa's Main Conjecture. We will start by studying the Coleman map, a map between towers of local units and p-adic measures. This gives a connection between the tower of cyclotomic units — historically important for their connection to class numbers — and the Kubota–Leopoldt p-adic L-function ζ_p from Part I, and hence a new arithmetic construction of ζ_p (Theorem 10.15). This construction can be seen as an arithmetic manifestation of the Euler product expression of the zeta function, and this point of view has led to beautiful generalisations now known as the theory of Euler systems. We then prove a theorem of Iwasawa (Theorem 12.23) relating the zeros of the p-adic L-function to arithmetic information in terms of units. Using these two results and class field theory, we will naturally arrive at the formulation and proof of (a special case of) the Main Conjecture (Theorem 13.8).

9. Notation

Our study of the Iwasawa Main Conjecture requires a certain amount of notation, which we introduce straight away for convenience. The following should be used as an index of the key notation, and the reader is urged to consult the definition of new objects as they appear in the text.

Let p be an odd prime. Throughout this section, we work with coefficient field $L = \mathbb{Q}_p$. For $n \in \mathbb{N}$, write

$$F_n := \mathbb{Q}(\mu_{p^n}), \quad F_n^+ := \mathbb{Q}(\mu_{p^n})^+, \quad \mathscr{V}_n := \mathscr{O}_{F_n}^\times, \quad \mathscr{V}_n^+ := \mathscr{O}_{F_n^+}^\times,$$
$$K_n := \mathbb{Q}_p(\mu_{p^n}), \quad K_n^+ := \mathbb{Q}_p(\mu_{p^n})^+, \quad \mathscr{U}_n := \mathscr{O}_{K_n}^\times, \quad \mathscr{U}_n^+ := \mathscr{O}_{K_n^+}^\times,$$

where $(-)^+$ denotes the maximal totally real subfield (i.e., the fixed points under complex conjugation). The extensions $F_n/\mathbb{Q}$, $K_n/\mathbb{Q}_p$, $F_n^+/\mathbb{Q}$ and $K_n^+/\mathbb{Q}_p$ are Galois and totally ramified at p (the first two of degree $(p-1)p^{n-1}$ and the last two of degree $\frac{1}{2}(p-1)p^{n-1}$) and we denote by $\mathfrak{p}_n$ (resp. $\mathfrak{p}_n^+$) the unique prime ideal of F_n (resp. F_n^+) above the rational prime p. We let

$$F_\infty = \mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n\geq 1} F_n, \quad F_\infty^+ := (F_\infty)^+ = \bigcup_{n\geq 1} F_n^+,$$
$$K_\infty = \mathbb{Q}_p(\mu_{p^\infty}) = \bigcup_{n\geq 1} K_n, \quad K_\infty^+ := (K_\infty)^+ = \bigcup_{n\geq 1} K_n^+,$$

and denote by $\mathfrak{p}$ (resp. $\mathfrak{p}^+$) the unique prime of F_∞ (resp. F_∞^+) above p.

Write $\Gamma := \mathrm{Gal}(F_\infty/\mathbb{Q})$ and $\Gamma^+ := \mathrm{Gal}(F_\infty^+/\mathbb{Q}) = \Gamma/\langle c\rangle$, where c denotes the complex conjugation. Since $\mathrm{Gal}(F_n/\mathbb{Q})$ sends a primitive p^n-th root of unity to a primitive p^n-th root of unity, one deduces an isomorphism

$$\chi_n : \mathrm{Gal}(F_n/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times$$

determined by the identity

$$\sigma(\xi) = \xi^{\chi_n(\sigma)},$$

for $\sigma \in \mathrm{Gal}(F_n/\mathbb{Q})$ and $\xi \in \mu_{p^n}$ any primitive p^n-th root of unity. By infinite Galois theory,

$$\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q}) := \varprojlim_n \mathrm{Gal}(F_n/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times, \tag{9-1}$$

via the *cyclotomic character* $\chi := \varprojlim \chi_n$. Note χ induces an isomorphism $\Gamma^+ \cong \mathbb{Z}_p^\times/\{\pm 1\}$.

We also define

$$\mathscr{U}_{n,1} := \{u \in \mathscr{U}_n : u \equiv 1 \pmod{\mathfrak{p}_n}\}, \quad \mathscr{U}_{n,1}^+ := \mathscr{U}_{n,1} \cap \mathscr{U}_n^+. \tag{9-2}$$

The subsets $\mathscr{U}_{n,1}$ and $\mathscr{U}_{n,1}^+$ are important as they have the structure of $\mathbb{Z}_p$-modules (indeed, if $u \in \mathscr{U}_{n,1}$ or $\mathscr{U}_{n,1}^+$ and $a \in \mathbb{Z}_p$, then $u^a = \sum_{k\geq 0}\binom{a}{k}(u-1)^k$ converges). By contrast, the full local units $\mathscr{U}_n$ and $\mathscr{U}_n^+$ are only $\mathbb{Z}$-modules.

In general, our notation satisfies the following logic: if X_n is any subgroup of $\mathscr{U}_n$, then we let $X_n^+ = X_n \cap \mathscr{U}_n^+$, $X_{n,1} = X_n \cap \mathscr{U}_{n,1}$ and $X_{n,1}^+ = X_n^+ \cap \mathscr{U}_{n,1}^+$. Observe that, since $\mathscr{V}_n \subseteq \mathscr{U}_n$, the same applies for any subgroup X_n of $\mathscr{V}_n$.

It will be essential for our constructions and methods to consider these modules at all levels simultaneously. We define

$$\mathscr{U}_\infty := \varprojlim_n \mathscr{U}_n, \quad \mathscr{U}_{\infty,1} := \varprojlim_n \mathscr{U}_{n,1}, \tag{9-3}$$
$$\mathscr{U}_\infty^+ := \varprojlim_n \mathscr{U}_n^+, \quad \mathscr{U}_{\infty,1}^+ := \varprojlim_n \mathscr{U}_{n,1}^+,$$

where all limits are taken with respect to the norm maps. All of these infinite-level modules are compact $\mathbb{Z}_p$-modules (since they are inverse limits of compact $\mathbb{Z}_p$-modules) and moreover they are all endowed with natural continuous actions of $\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q})$ or $\Gamma^+ = \mathrm{Gal}(F_\infty^+/\mathbb{Q})$. Accordingly, they are endowed with continuous actions of the Iwasawa algebras $\Lambda(\Gamma)$ or $\Lambda(\Gamma^+)$ (which is the primary reason for passing to infinite-level objects).

We fix once and for all a compatible system of roots of unity $(\xi_{p^n})_{n\in\mathbb{N}}$, that is, a sequence where ξ_{p^n} is a primitive p^n-th root of unity such that $\xi_{p^{n+1}}^p = \xi_{p^n}$ for all $n \in \mathbb{N}$. We let $\pi_n = \xi_{p^n} - 1$, which is a uniformiser of K_n.

10. The Coleman map

In this section we prove a theorem of Coleman relating local units to power series over $\mathbb{Z}_p$. Using this result, we construct in Section 10 the *Coleman map*, a device for constructing p-adic L-functions from the data of a compatible system of units. We will explain how the Kubota–Leopoldt p-adic L-function can be constructed from towers of cyclotomic units using the Coleman map. This map thus provides an important bridge between analytic objects (p-adic L-functions) and arithmetic structures (cyclotomic units), and will serve as the key step in our formulation of the Main Conjecture.

In Section 10.5, we discuss a program started by Perrin-Riou to generalise Coleman's work. Given a p-adic Galois representation, Perrin-Riou's big logarithm maps construct a p-adic L-function from certain compatible systems of cohomology classes. Specialising to the representation $\mathbb{Q}_p(1)$, her map recovers the Coleman map. The results of this section are thus a prototype for studying p-adic L-functions in a larger, more conceptual framework.

10.1. ***Notation and Coleman's theorem.*** Recall that $K_n = \mathbb{Q}_p(\mu_{p^n})$ and $K_\infty = \mathbb{Q}_p(\mu_{p^\infty})$ are the local versions of $F_n = \mathbb{Q}(\mu_{p^n})$ and $F_\infty = \mathbb{Q}(\mu_{p^\infty})$. We also defined

$$\mathscr{U}_n = \mathscr{O}_{K_n}^\times$$

to be the module of local units at level n, took a compatible system (ξ_{p^n}) of primitive p^n-th roots of unity, and defined $\pi_n := \xi_{p^n} - 1$, a uniformiser of K_n. Recall that we defined

$$\mathscr{U}_\infty := \varprojlim_n \mathscr{U}_n,$$

where the projective limit is taken with respect to the norm maps $N_{n,n-1} : K_n \to K_{n-1}$.

Let us first motivate Coleman's theorem. The elements π_n give a sequence of elements in the open unit ball

$$B(0,1) = \{z \in \mathbb{C}_p : |z| < 1\},$$

which approaches the boundary $\{|z| = 1\}$ as $n \to \infty$. Now, recall from Remark 3.39 that an element $f \in \mathbb{Z}_p[\![T]\!]$ can be viewed as a bounded rigid analytic function on $B(0, 1)$; so any such f gives a sequence $f(\pi_n)$ of elements of $\mathscr{O}_{K_n}$. As we shall see below, the Weierstrass preparation theorem implies that f is uniquely determined by this sequence.

In the spirit of earlier sections, where we sought analytic objects interpolating collections of specific values, it is natural to ask which sequences arise in this way. Precisely, given a sequence $\{u_n \in \mathscr{O}_{K_n}\}$, can it be interpolated by a power series f, in the sense that $f(\pi_n) = u_n$ for all n? Coleman's theorem gives a positive answer to this question for norm-compatible sequences of units $(u_n)_{n\in\mathbb{N}} \in \mathscr{U}_\infty$.

We begin with a simple observation, for a single fixed n.

Lemma 10.1. *Let $u \in \mathscr{U}_n$ be a local unit at level n. There exists a power series $f \in \mathbb{Z}_p[\![T]\!]^\times$ such that $f(\pi_n) = u$.*

Proof. This is essentially immediate from the fact that π_n is a uniformiser. Indeed, K_n is totally ramified, so one can choose some $a_0 \in \mathbb{Z}_p$ such that

$$a_0 \equiv u \pmod{\pi_n},$$

and then $a_1 \in \mathbb{Z}_p$ such that

$$a_1 \equiv \frac{u - a_0}{\pi_n} \pmod{\pi_n},$$

and so on, defining $f(T) = \sum_n a_n T^n \in \mathbb{Z}_p[\![T]\!]$. By construction, $f(\pi_n) = u$. As u is a unit, we have $a_0 \in \mathbb{Z}_p^\times$. It's then an exercise to see $f \in \mathbb{Z}_p[\![T]\!]^\times$ is invertible. □

The problem with this proposition is that such a power series f is far from being unique, since we had an abundance of choices for each coefficient. In the usual spirit of Iwasawa theory, Coleman realised that it was possible to solve this problem by passing to the infinite tower K_∞, considering all n simultaneously.

Theorem 10.2 (Coleman). *There exists a unique injective homomorphism*

$$\mathscr{U}_\infty \to \mathbb{Z}_p[\![T]\!]^\times, \quad u \mapsto f_u$$

of multiplicative groups such that $f_u(\pi_n) = u_n$ for all $u \in \mathscr{U}_\infty$ and $n \geq 1$.

Coleman actually proved something stronger. He described a precise subspace of $\mathbb{Z}_p[\![T]\!]$ in which the associated interpolating power series f_u lives; it is invariant under a certain norm operator $\mathcal{N}$ on $\mathbb{Z}_p[\![T]\!]$. In particular, norm-compatibility on the right-hand side translates into norm-invariance on the left-hand side. We will prove all of this in Section 10.3 below.

First, though, we study an important application, explaining how this theorem is related to the Kubota–Leopoldt p-adic L-function.

10.2. ***Example: cyclotomic units.*** Let $a \in \mathbb{Z}$ prime to p, and define

$$c_n(a) := \frac{\xi_{p^n}^a - 1}{\xi_{p^n} - 1} \in \mathscr{U}_n.$$

This is indeed a unit, as both $\xi_{p^n}^a - 1$ and $\xi_{p^n} - 1$ are uniformisers in K_n.

Lemma 10.3. *We have* $c(a) := (c_n(a))_n \in \mathscr{U}_\infty$.

Proof. This is equivalent to proving that $N_{n,n-1}(c_n(a)) = c_{n-1}(a)$. Since the minimal polynomial of ξ_{p^n} over K_{n-1} is $X^p - \xi_{p^{n-1}}$, for any b prime to p we see that

$$N_{n,n-1}(\xi_{p^n}^b - 1) = \prod_{\eta \in \mu_p} (\xi_{p^n}^b \eta - 1) = \xi_{p^n}^{bp} - 1 = \xi_{p^{n-1}}^b - 1,$$

where in the penultimate equality we have used the identity $X^p - 1 = \prod_{\eta \in \mu_p}(X\eta - 1)$. Applying this with $b = a$ shows the numerator of $c(a)$ is norm-compatible, and with $b = 1$ the denominator. We conclude as norm is multiplicative. □

It is possible to write down $f_{c(a)} \in \mathbb{Z}_p[\![T]\!]^\times$ directly by inspection. Indeed, we see that

$$f_{c(a)}(T) = \frac{(1+T)^a - 1}{T}$$

satisfies the required property (and $f_{c(a)}$ is even a polynomial). We now connect this to the construction studied in Section 4. Recall the operator $\partial = (1+T)\frac{d}{dT}$ from Lemma 3.29.

Proposition 10.4. *Let* $F_a(T)$ *be the power series defined in Lemma 4.3. Then*

$$\partial \log f_{c(a)}(T) = a - 1 - F_a(T).$$

Proof. We compute directly that

$$\begin{aligned} \partial \log f_{c(a)} &= \partial \log((1+T)^a - 1) - \partial \log(T) \\ &= \frac{a(1+T)^a}{(1+T)^a - 1} - \frac{T+1}{T} \\ &= a - 1 - \frac{1}{T} + \frac{a}{(1+T)^a - 1} \\ &= a - 1 - F_a(T). \end{aligned}$$

□

Lemma 10.5. *Let* μ_a *be the measure in Definition 4.5. Then*

$$\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu_{\partial \log f_{c(a)}}) = -\mathrm{Res}_{\mathbb{Z}_p^\times}(\mu_a).$$

Proof. In terms of power series, the restriction to $\mathbb{Z}_p^\times$ corresponds to applying the operator $(1 - \varphi \circ \psi)$. As $1 - \varphi \circ \psi$ kills the term $a - 1$, we find that, as required,

$$(1 - \varphi \circ \psi)\partial \log f_{c(a)} = -(1 - \varphi \circ \psi)F_a.$$

□

Remark 10.6. The measure μ_a was used in the construction of ζ_p. Later in Section 10 we will use Theorem 10.2 to give a new construction of ζ_p via the cyclotomic units. We will see more about the units $c_n(a)$, and in particular the module they generate in $\mathscr{U}_n$, in Section 11.

10.3. ***Proof of Coleman's theorem.*** First we see that there is at most one power series f_u attached to a system of units u.

Lemma 10.7. *Suppose $u = (u_n) \in \mathscr{U}_\infty$ and $f, g \in \mathbb{Z}_p[\![T]\!]^\times$ both satisfy*

$$f(\pi_n) = g(\pi_n) = u_n$$

for all $n \geq 1$. Then $f = g$.

Proof. The Weierstrass preparation theorem says that we can write any nonzero $h(T) \in \mathbb{Z}_p[\![T]\!]$ in the form $p^m u(T) r(T)$, where $u(T)$ is a unit and $r(T)$ is a polynomial. Any such $h(T)$ converges to a function on the maximal ideal in the ring of integers of $\overline{\mathbb{Q}}_p$, and since $u(T)$ cannot have zeros, we deduce that $h(T)$ has a finite number of zeros in this maximal ideal. Now $(\pi_n)_{n\geq 1}$ is an infinite sequence of elements in this maximal ideal, so the fact that $(f-g)(\pi_n) = 0$ for all $n \geq 1$ implies that $f = g$, as required. □

We now move to showing the existence of such a series f_u. The key idea in the proof is to identify the subspace of $f \in \mathbb{Z}_p[\![T]\!]^\times$ such that $(f(\pi_n))_n \in \mathscr{U}_\infty$; that is, identify the *image* in Theorem 10.2. For this, we want norm-compatibility of $f(\pi_n)$. Lemma 10.8 and Proposition 10.10 below will show the existence of a norm operator on power series, and then translate the norm-compatibility condition of units into norm-invariance of power series; Lemma 10.11 will show certain continuity properties of this norm operator, which will allow us to prove Coleman's theorem by a standard diagonal argument.

Recall that the action of φ on $f(T) \in \mathbb{Z}_p[\![T]\!]$ is defined by

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

(see (3-7)) and that this action is injective. Importantly, we also have

$$\varphi(f)(\pi_{n+1}) = f((\pi_{n+1}+1)^p - 1) = f(\xi_{p^{n+1}}^p - 1) = f(\xi_{p^n} - 1) = f(\pi_n). \quad (10\text{-}1)$$

From our work with measures (see Section 3.5.5), we have also seen the existence of an additive operator ψ with the property that

$$(\varphi \circ \psi)(f)(T) = \frac{1}{p} \sum_{\eta \in \mu_p} f(\eta(1+T) - 1).$$

We henceforth call ψ the *trace* operator (this terminology will become clear after Lemma 10.8). We now define a multiplicative version of this operator.

Lemma 10.8. *There exists a unique multiplicative operator $\mathcal{N}$ on $\mathbb{Z}_p[\![T]\!]$, the* ***norm operator****, such that*

$$(\varphi \circ \mathcal{N})(f)(T) = \prod_{\eta \in \mu_p} f(\eta(1+T) - 1).$$

Proof. The ring $B = \mathbb{Z}_p[\![T]\!]$ is an extension of $A = \mathbb{Z}_p[\![\varphi(T)]\!] = \varphi(\mathbb{Z}_p[\![T]\!])$ of degree p, the former being obtained by adjoining a p-th root of $(1+T)^p$ to the latter. Each automorphism of B over A is given by $T \mapsto (1+T)\eta - 1$ for some $\eta \in \mu_p$. There is a norm map

$$N_{B/A} : \mathbb{Z}_p[\![T]\!] \to \varphi(\mathbb{Z}_p[\![T]\!]), \quad f(T) \mapsto \prod_{\eta \in \mu_p} f((1+T)\eta - 1).$$

The norm operator $\mathcal{N}$ is then defined to be $\varphi^{-1} \circ N_{B/A}$, recalling that φ is injective. □

We similarly have $\psi = p^{-1}\varphi^{-1} \circ \mathrm{Tr}_{B/A}$, where $\mathrm{Tr}_{B/A}$ is the trace operator for the extension B/A in the proof of Lemma 10.8. Note that as $\mathcal{N}$ is multiplicative, it preserves $\mathbb{Z}_p[\![T]\!]^\times$. Moreover, it is closely related to the norm operator $N_{n+1,n} : \mathscr{U}_{n+1} \to \mathscr{U}_n$ used to defined $\mathscr{U}_\infty$, via the following lemma.

Lemma 10.9. *The following diagram commutes*:

$$\begin{array}{ccc} \mathbb{Z}_p[\![T]\!]^\times & \xrightarrow{f \mapsto f(\pi_{n+1})} & \mathcal{U}_{n+1} \\ \Big\downarrow{\scriptstyle \mathcal{N}} & & \Big\downarrow{\scriptstyle N_{n+1,n}} \\ \mathbb{Z}_p[\![T]\!]^\times & \xrightarrow[f \mapsto f(\pi_n)]{} & \mathcal{U}_n \end{array} \tag{10-2}$$

Proof. If $f \in \mathbb{Z}_p[\![T]\!]^\times$, then $f(\pi_n) \in \mathscr{U}_n$ for all n, as $f(\pi_n)^{-1} = f^{-1}(\pi_n)$ is also integral. In particular, the horizontal maps are well defined.

Observe now that, as the minimal polynomial of $\xi_{p^{n+1}}$ over K_n is $X^p - \xi_{p^n} = 0$, we can write the right-hand norm as

$$N_{n+1,n}(f(\pi_{n+1})) = \prod_{\eta \in \mu_p} f(\eta\xi_{p^{n+1}} - 1) = (\varphi \circ \mathcal{N})(f)(\pi_{n+1}) = (\mathcal{N}f)(\pi_n),$$

giving exactly the claimed commutativity. In the final step we have used (10-1). □

In particular, we get the following.

Proposition 10.10. *There is an injective map*

$$R : (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}} \hookrightarrow \mathscr{U}_\infty, \quad f \mapsto (f(\pi_n))_n.$$

Proof. Suppose $\mathcal{N}(f) = f$. By Lemma 10.9, we deduce that

$$N_{n+1,n}(f(\pi_{n+1})) = f(\pi_n), \tag{10-3}$$

so $(f(\pi_n))_n \in \mathscr{U}_\infty$. □

To prove Theorem 10.2 it suffices to prove that the map R is surjective. We need the following lemma on the behaviour of $\mathcal{N}$ modulo powers of p.

Lemma 10.11. *Let $f(T) \in \mathbb{Z}_p[\![T]\!]$. Then*:

(i) *If $\varphi(f)(T) \equiv 1 \pmod{p^k}$ for some $k \geq 0$, then $f(T) \equiv 1 \pmod{p^k}$.*

(ii) *We have*

$$\mathcal{N}(f) \equiv f \pmod{p}.$$

Now suppose $f \in \mathbb{Z}_p[\![T]\!]^\times$. Then:

(iii) *If $f \equiv 1 \pmod{p^k}$ with $k \geq 1$, then*

$$\mathcal{N}(f) \equiv 1 \pmod{p^{k+1}}.$$

(iv) *If $k_2 \geq k_1 \geq 0$, then*

$$\mathcal{N}^{k_2}(f) \equiv \mathcal{N}^{k_1}(f) \pmod{p^{k_1+1}}.$$

Proof. We leave parts (i) and (ii) as an exercise (see [16, Lemma 2.3.1]). To see part (iii), suppose that $f \equiv 1 \pmod{p^k}$ with $k \geq 1$, and recall that $\mathfrak{p}_1$ is the maximal ideal of the ring of integers of $K_1 = \mathbb{Q}_p(\mu_p)$. For each $\eta \in \mu_p$, as $(\eta - 1)(1 + T) \in \mathfrak{p}_1\mathbb{Z}_p[\![T]\!]$, we have

$$\eta(1 + T) - 1 \equiv T \pmod{\mathfrak{p}_1\mathbb{Z}_p[\![T]\!]},$$

so that

$$f(\eta(1 + T) - 1) \equiv f(T) \pmod{\mathfrak{p}_1 p^k \mathbb{Z}_p[\![T]\!]}$$

by considering each term separately. It follows that

$$\begin{aligned}\varphi \circ \mathcal{N}(f)(T) &= \prod_{\eta \in \mu_p} f(\eta(1 + T) - 1) \\ &\equiv f(T)^p \pmod{\mathfrak{p}_1 p^k \mathbb{Z}_p[\![T]\!]}.\end{aligned}$$

Since both $\varphi \circ \mathcal{N}(f)$ and $f(T)^p$ are elements of $\mathbb{Z}_p[\![T]\!]$, this is in fact an equivalence modulo $\mathfrak{p}_1 p^k \cap \mathbb{Z}_p = p^{k+1}$. If $f(T) \equiv 1 \pmod{p^k}$, then $f(T)^p \equiv 1 \pmod{p^{k+1}}$, and then the proof follows from part (i).

To see part (iv), from part (ii) we see that

$$\frac{\mathcal{N}^{k_2-k_1} f}{f} \equiv 1 \pmod{p}.$$

Then iterating $\mathcal{N}$ and using part (iii) k_1 times, we obtain the result. □

Proposition 10.12. *The map $R : (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}} \hookrightarrow \mathscr{U}_\infty$ is surjective.*

Proof. Let $u = (u_n)_{n \geq 1} \in \mathscr{U}_\infty$. For each n, choose $f_n \in \mathbb{Z}_p[\![T]\!]^\times$ such that

$$f_n(\pi_n) = u_n.$$

We claim that $\mathcal{N} f_{n+1}(\pi_n) = u_n$. Indeed, using Lemma 10.9 we have

$$\mathcal{N} f_{n+1}(\pi_n) = N_{n+1,n}(f_{n+1}(\pi_{n+1})) = N_{n+1,n}(u_{n+1}) = u_n.$$

Iterating, for any $k \geq 0$ we have

$$(\mathcal{N}^k f_{n+k})(\pi_n) = u_n. \tag{10-4}$$

In view of Lemma 10.11(iv), we define

$$g_n := \mathcal{N}^n f_{2n} \in \mathbb{Z}_p[\![T]\!]^\times.$$

Then, for any $m \geq n$, we have

$$\begin{aligned} u_n &= \mathcal{N}^{2m-n} f_{2m}(\pi_n) \\ &\equiv \mathcal{N}^m f_{2m}(\pi_n) = g_m(\pi_n) \pmod{p^{m+1}}, \end{aligned}$$

where the first equality is (10-4) and the congruence is Lemma 10.11(iv), taking $k_2 = 2m - n$ and $k_1 = m$. Hence as $m \to \infty$, we have $g_m(\pi_n) \to u_n$ for all n. It thus suffices to find a convergent subsequence of (g_m); but such a subsequence exists, as $\mathbb{Z}_p[\![T]\!]^\times$ is compact. Letting $f_u \in \mathbb{Z}_p[\![T]\!]^\times$ denote the limit of this subsequence, we have $f_u(\pi_n) = u_n$ for all n.

It remains to show that $\mathcal{N}(f_u) = f_u$. Indeed, as the sequence (u_n) is norm-compatible, we have, using Lemma 10.9,

$$\mathcal{N}(f_u)(\pi_n) = N_{n+1,n} f_u(\pi_{n+1}) = N_{n+1,n}(u_{n+1}) = u_n = f_u(\pi_n).$$

As $\mathcal{N}(f_u)$ and f_u are both Coleman power series for u, by Lemma 10.7 they are equal. □

With this in hand, we have proved the following more precise version of Theorem 10.2.

Theorem 10.13. *There exists a unique isomorphism of groups*

$$\mathscr{U}_\infty \to (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}}, \quad u \mapsto f_u$$

such that $f_u(\pi_n) = u_n$ *for all* $u \in \mathscr{U}_\infty$ *and* $n \geq 1$.

Proof. By Propositions 10.10 and 10.12, we have a bijection

$$R : (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}} \xrightarrow{\sim} \mathscr{U}_\infty.$$

This is an isomorphism, and R^{-1} gives the required map. We have $f_u(\pi_n) = u_n$ by construction of R and uniqueness follows from Lemma 10.7. □

10.4. ***Definition of the Coleman map.*** The Coleman map is motivated by the example of Section 10.2, where we saw that a distinguished family of local units — the cyclotomic units — are strongly linked to the Kubota–Leopoldt p-adic L-function.

In particular, given the construction of ζ_p in Section 4 and Lemma 10.5, ζ_p can be defined by the following procedure:

(1) Consider the tower $c(a)$ of cyclotomic units.

(2) Take its Coleman power series $f_{c(a)}$.

(3) Apply $\partial \log$.

(4) Apply $(1 - \varphi \circ \psi)$.

(5) Apply ∂^{-1}.

(6) Pass to the corresponding measure on $\mathbb{Z}_p^\times$ by inverting the Mahler transform.

(7) Finally, divide by θ_a.

Recall that in terms of measures, step (4) corresponds to restriction to $\mathbb{Z}_p^\times$, and (5) to multiplication by x^{-1}. We are therefore led to consider the following construction.

Definition 10.14. Let

$$\mathrm{Col} : \mathscr{U}_\infty \xrightarrow{u \mapsto f_u(T)} (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}} \xrightarrow{\partial \log} \mathbb{Z}_p[\![T]\!] \xrightarrow{1-\varphi\circ\psi} \mathbb{Z}_p[\![T]\!]^{\psi=0} \xrightarrow{\partial^{-1}} \mathbb{Z}_p[\![T]\!]^{\psi=0} \xrightarrow{\mathscr{M}^{-1}} \Lambda(\mathbb{Z}_p^\times),$$

where the first map is Coleman's isomorphism, the second is the logarithmic derivative appearing in Section 10.2, the third is the measure-theoretic restriction from $\mathbb{Z}_p$ to $\mathbb{Z}_p^\times$, the fourth is multiplication by x^{-1}, and the last is the Mahler correspondence (Section 3.4 and Corollary 3.32).

Via Section 10.2, we have the following description of the Kubota–Leopoldt p-adic L-function.

Theorem 10.15. *For any topological generator a of $\mathbb{Z}_p^\times$, we have an equality of pseudomeasures*

$$\zeta_p = \frac{\mathrm{Col}(c(a))}{\theta_a} \in Q(\mathbb{Z}_p^\times).$$

10.5. ***Generalisations: the Kummer sequence, Euler systems and p-adic L-functions.*** We conclude this section with a digression on the generalisation of the Coleman map that leads to a conjectural construction, under the assumption of the existence of certain global cohomological elements, of p-adic L-functions of more general motives. This section is included as additional context and may be skipped on a first reading. Throughout, if F is a number field, we let $\mathscr{G}_F$ denote its absolute Galois group.

Consider, for $m \geq 1$, the Kummer exact sequence

$$0 \to \mu_{p^m} \to \boldsymbol{G}_{\mathrm{m}} \xrightarrow{x \mapsto x^{p^m}} \boldsymbol{G}_{\mathrm{m}} \to 0. \tag{10-5}$$

Evaluating at $\overline{\mathbb{Q}}$ and taking fixed points by $\mathscr{G}_F$, this short exact sequence induces, for any number field F, a long exact sequence on cohomology

$$0 \to \mu_{p^m}(F) \to F^\times \xrightarrow{x \mapsto x^{p^m}} F^\times \to H^1(F, \mu_{p^m}) \to H^1(F, \overline{\mathbb{Q}}^\times). \tag{10-6}$$

Here, for any topological $\mathscr{G}_F$-module A, we write $H^1(F, A) \coloneqq H^1(\mathscr{G}_F, A)$ for the Galois cohomology, i.e., the continuous group cohomology of $\mathscr{G}_F$. By Hilbert 90, we have $H^1(F, \overline{\mathbb{Q}}^\times) = 0$. Taking inverse limits over $m \geq 1$, which is exact, we obtain an isomorphism called the Kummer map,

$$\delta : F^\times \otimes \mathbb{Z}_p \xrightarrow{\sim} H^1(F, \mathbb{Z}_p(1)). \tag{10-7}$$

Explicitly, at each finite level, the isomorphism

$$F^\times \otimes \mathbb{Z}/p^n\mathbb{Z} = F^\times/(F^\times)^{p^n} \xrightarrow{\sim} H^1(\mathscr{G}_F, \mu_{p^n})$$

is given as follows. Take $a \in F^\times$ and take any $b \in \overline{\mathbb{Q}}^\times$ such that $b^{p^n} = a$. Then $c_a : \sigma \mapsto \sigma(b)/b$ defines a 1-cocycle on $\mathscr{G}_F$ and it is a coboundary if and only if a is a p^n-th power in $F^\times$, which shows that the map sending the class of a to the class of c_a is well defined.

Let $m = Dp^n$, $n \geq 1$, and define

$$\boldsymbol{c}_m \coloneqq \frac{\xi_m^{-1} - 1}{\xi_m - 1} \in \mathscr{O}^\times_{\mathbb{Q}(\mu_m)},$$

a generalisation of the cyclotomic units $c_n(-1)$ (where $D = 1$) from Section 10.2, where $(\xi_m)_m$ denotes a compatible system of m-th roots of unity. One can show that these elements satisfy the following relations with respect to the norm maps:

$$\mathrm{N}_{\mathbb{Q}(\mu_{m\ell})/\mathbb{Q}(\mu_m)}(\boldsymbol{c}_{m\ell}) = \begin{cases} \boldsymbol{c}_m & \text{if } \ell \mid m, \\ (1 - \ell^{-1})\boldsymbol{c}_m & \text{if } \ell \nmid m. \end{cases}$$

Using the Kummer map (10-7), we get elements $\mathbb{Z}_m \coloneqq \delta(\boldsymbol{c}_m) \in H^1(\mathbb{Q}(\mu_m), \mathbb{Z}_p(1))$ satisfying

$$\mathrm{cores}_{\mathbb{Q}(\mu_{m\ell})/\mathbb{Q}(\mu_m)}(\mathbb{Z}_{m\ell}) = \begin{cases} \mathbb{Z}_m & \text{if } \ell \mid m, \\ (1 - \mathrm{Frob}_\ell^{-1})\mathbb{Z}_m & \text{if } \ell \nmid m, \end{cases}$$

where we have used that Frob_ℓ acts on $\mathbb{Z}_p(1)$ simply by multiplication by ℓ on $\mathbb{Z}_p(1)$. Observe also that $(1 - \ell^{-1})$ is the Euler factor at ℓ of the Riemann zeta function (evaluated at $s = 1$). This admits the following huge generalisation, as described comprehensively in [70].

Definition 10.16. Let Σ be a finite set of primes containing p, let $V \in \mathrm{Rep}_L \mathscr{G}_\mathbb{Q}$ be a global p-adic Galois representation which is unramified outside Σ, and let $T \subseteq V$

be an $\mathcal{O}_L$-lattice stable under $\mathcal{G}_{\mathbb{Q}}$. An *Euler system* for (V, T, Σ) is a collection of classes

$$\mathbb{Z}_m \in H^1(\mathbb{Q}(\mu_m), T),$$

where m is of the form $m = p^n m'$ with $n \geq 0$, and where m' is a square-free product of prime numbers not belonging to Σ, satisfying

$$\mathrm{cores}_{\mathbb{Q}(\mu_{m\ell})/\mathbb{Q}(\mu_m)}(\mathbb{Z}_{m\ell}) = \begin{cases} \mathbb{Z}_m & \text{if } \ell = p, \\ P_\ell(V^*(1), \sigma_\ell^{-1})\mathbb{Z}_m & \text{if } \ell \neq p, \end{cases}$$

where $P_\ell(V^*(1), X) = \det(1 - \mathrm{Frob}_\ell^{-1} X | V^*(1)^{I_\ell})$ is the Euler factor at ℓ of the L-function associated to $V^*(1)$ and σ_ℓ denotes the image of Frob_ℓ in $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$.

The cyclotomic units form an Euler system for the representation $\mathbb{Z}_p(1)$, and lie at the heart of Rubin's proof of the Main Conjecture. In general, constructing Euler systems for a Galois representation is a very difficult task, and few examples exist at the moment.

We now describe a rephrasing of Coleman's map that more easily generalises. Above, we showed that evaluating Kummer's exact sequence (10-5) at $\overline{\mathbb{Q}}$, taking the long exact sequence in Galois cohomology for F, and taking an inverse limit, we get an isomorphism $F^\times \otimes \mathbb{Z}_p \cong H^1(F, \mathbb{Z}_p(1))$. In exactly the same way, replacing $\overline{\mathbb{Q}}$ by $\overline{\mathbb{Q}}_p$, and F by the finite extension K_n of $\mathbb{Q}_p$ for $n \geq 1$, we obtain an isomorphism

$$K_n^\times \otimes \mathbb{Z}_p \cong H^1(K_n, \mathbb{Z}_p(1)).$$

These isomorphisms intertwine the norm maps on the left-hand side with the corestriction maps in cohomology on the right-hand side, and hence, considering the inverse limit over all n, we see that there is an isomorphism

$$\varprojlim_{n\geq 1} K_n^\times \otimes \mathbb{Z}_p \cong \varprojlim_{n\geq 1} H^1(K_n, \mathbb{Z}_p(1)). \tag{10-8}$$

We define the *Iwasawa cohomology* to be

$$H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{Q}_p(1)) := \varprojlim_{n\geq 1} H^1(K_n, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Such groups can be attached to general Galois representations (see below), and they are a natural generalisation of the local units.

To make this precise, note that the inclusion $\mathscr{U}_n = \mathscr{O}_{K_n}^\times \subset K_n^\times$ induces a natural map $\mathscr{U}_n \to K_n^\times \otimes \mathbb{Z}_p$, yielding a map $\mathscr{U}_\infty \to \varprojlim K_n^\times \otimes \mathbb{Z}_p$. Composing this with (10-8), we obtain a map

$$\kappa : \mathscr{U}_\infty \to \varprojlim_{n\geq 1} H^1(K_n, \mathbb{Z}_p(1)).$$

One can then show that there exists a map

$$\mathrm{Col}' : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{Q}_p(1)) \to \mathscr{M}(\mathbb{Z}_p^\times, \mathbb{Q}_p),$$

where we recall that $\mathscr{M}(\mathbb{Z}_p^\times, \mathbb{Q}_p) = \Lambda(\mathbb{Z}_p^\times) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is the space of $\mathbb{Q}_p$-valued measures on Γ, making the diagram

$$\begin{array}{ccc} \mathscr{U}_\infty & \xrightarrow{\quad\kappa\quad} & H^1_{\mathrm{Iw}}(\mathbb{Q}_p, \mathbb{Q}_p(1)) \\ & {\scriptstyle \mathrm{Col}} \searrow \quad \swarrow {\scriptstyle \mathrm{Col}'} & \\ & \mathcal{M}(\mathbb{Z}_p^\times, \mathbb{Q}_p) & \end{array}$$

commute.

By localising, the Euler system of cyclotomic units give rise to an element of the Iwasawa cohomology. By combining the above with Proposition 10.4, we see that the p-adic zeta function can be obtained by evaluating Col' at this Iwasawa cohomology class (and dividing through by the measure θ_a to make it independent of a, which introduces a pole).

The advantage of this reformulation is that Iwasawa cohomology generalises well, as we now explain. Let $V \in \mathrm{Rep}_L \mathscr{G}_{\mathbb{Q}_p}$ be any p-adic representation of $\mathscr{G}_{\mathbb{Q}_p}$, i.e., a finite-dimensional L-vector space V equipped with a continuous linear action of $\mathscr{G}_{\mathbb{Q}_p}$. As before, we define its Iwasawa cohomology groups as

$$H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) := \varprojlim_{n \geq 1} H^1(K_n, T) \otimes_{\mathscr{O}_L} L,$$

where $T \subseteq V$ denotes any $\mathscr{O}_L$-lattice of V stable under the action of the Galois group $\mathscr{G}_{\mathbb{Q}_p}$ and, as before, the inverse limit is taken with respect to the corestriction maps in cohomology. Morally, Iwasawa cohomology groups are the groups where the local part at p of an Euler system of a global p-adic representation lives. Assuming the representation is crystalline,[11] the Coleman map has been generalised by Perrin-Riou [67]. Under some choices, she constructed *big logarithm maps*

$$\mathrm{Log}_V : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \to \mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p^\times, L),$$

where $\mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p^\times, L)$ denotes the space of L-valued locally analytic distributions on $\mathbb{Z}_p^\times$ (in the sense of Section 3.7). The map Log_V satisfies certain interpolation properties expressed in terms of Bloch and Kato's exponential and dual exponential maps and, for $V = \mathbb{Q}_p(1)$, we recover Col'.

The general idea is that, given an Euler system for a global p-adic Galois representation, localising it at the place p and applying Perrin-Riou's map, one can construct a p-adic L-function for V. In a diagram:

$$\{\text{Euler systems}\} \xrightarrow{\mathrm{loc}_p} H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V) \xrightarrow{\mathrm{Log}_V} \{p\text{-adic } L\text{-functions}\}.$$

[11] Loosely, a p-adic representation of $\mathscr{G}_{\mathbb{Q}_p}$ being *crystalline* is a condition from p-adic Hodge theory that is the p-adic equivalent to an ℓ-adic representation of $\mathscr{G}_{\mathbb{Q}_p}$ (with $\ell \neq p$) being unramified. For the Galois representation attached to an elliptic curve E defined over $\mathbb{Q}$, this amounts to asking that E has good reduction at p. An extension of these results in the case of bad reduction can be found in [69].

This splits the problem of constructing p-adic L-functions for motives into a global problem (finding an Euler system) and a purely local problem (constructing the big logarithm maps). See [18] for further references on this subject.

11. Iwasawa's theorem on the zeros of the p-adic zeta function

In the previous section, the Coleman map allowed us to give a construction of the Kubota–Leopoldt p-adic L-function ζ_p using a specific tower of cyclotomic units. We now describe a theorem of Iwasawa (Theorem 11.9) that puts this on a deeper footing. This theorem describes the zeros of ζ_p — captured by a canonically attached ideal in the Iwasawa algebra — in terms of arithmetic data, via the *module* of cyclotomic units inside the local units. The Coleman map from Section 10 will be the key step for connecting both worlds.

With the aim of moving all the analytic information to the Galois side, we will start by reformulating the definition of the p-adic zeta function as a pseudomeasure on the Galois group $\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times$. We then introduce the global and local modules of cyclotomic units (which will be systematically studied later), stating the connection to class numbers, and state Iwasawa's theorem.

11.1. ***Measures on Galois groups.*** Recall that $F_\infty = \bigcup_{n\geq 1} \mathbb{Q}(\mu_{p^n})$, that $\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q})$, and that the cyclotomic character gives an isomorphism $\chi : \Gamma \xrightarrow{\sim} \mathbb{Z}_p^\times$. This isomorphism induces an identification between measures on $\mathbb{Z}_p^\times$ and measures on the Galois group Γ. From now on, we will let $\Lambda(\Gamma)$ be the space of measures on Γ, which we identify with $\Lambda(\mathbb{Z}_p^\times)$ via the cyclotomic character. We may thus naturally consider ζ_p as a pseudomeasure on Γ.

Similarly, the Galois group $\Gamma^+ = \mathrm{Gal}(F_\infty^+/\mathbb{Q}) = \Gamma/\langle c\rangle$ is identified through the cyclotomic character with $\mathbb{Z}_p^\times/\{\pm 1\}$. Observe that ζ_p, which ostensibly is an element of $Q(\Gamma)$, vanishes at the characters χ^k, for any odd integer $k > 1$. We will use this fact to show that ζ_p actually descends to a pseudomeasure on Γ^+.

Lemma 11.1. *Let $c \in \Gamma$ denote complex conjugation. Let R be a ring in which 2 is invertible and M an R-module with a continuous action of Γ. Then*

$$M \cong M^+ \oplus M^-$$

is a decomposition of M, with c acting as $+1$ on M^+ and as -1 on M^-.

Proof. This follows directly by using the idempotents $\frac{1}{2}(1+c)$ and $\frac{1}{2}(1-c)$, which act as projectors to the corresponding M^+ and M^-. □

We are assuming that p is odd, so $\Lambda(\Gamma) \cong \Lambda(\Gamma)^+ \oplus \Lambda(\Gamma)^-$. In fact, the module $\Lambda(\Gamma)^+$ admits a description solely in terms of the quotient Γ^+.

Lemma 11.2. *There is a natural isomorphism*

$$\Lambda(\Gamma)^+ \cong \Lambda(\Gamma^+).$$

Proof. We work at finite level. Let $\Gamma_n := \mathrm{Gal}(F_n/\mathbb{Q})$, and $\Gamma_n^+ := \mathrm{Gal}(F_n^+/\mathbb{Q})$. Then there is a natural surjection

$$\mathbb{Z}_p[\Gamma_n] \to \mathbb{Z}_p[\Gamma_n^+]$$

induced by the natural quotient map on Galois groups. Since this must necessarily map $\mathbb{Z}_p[\Gamma_n]^-$ to 0, this induces a map $\mathbb{Z}_p[\Gamma_n]^+ \to \mathbb{Z}_p[\Gamma_n^+]$. The result now follows at finite level by a dimension count (because both are free $\mathbb{Z}_p$-modules of rank $(p-1)p^{n-1}/2$, and one sees easily that the map sends a basis of the first module to a basis of the second). We obtain the required result by passing to the inverse limit. □

We henceforth freely identify $\Lambda(\Gamma^+)$ with the submodule $\Lambda(\Gamma)^+$ of $\Lambda(\Gamma)$.

Lemma 11.3. *Let $\mu \in \Lambda(\Gamma)$. Then $\mu \in \Lambda(\Gamma^+)$ if and only if*

$$\int_\Gamma \chi(x)^k \cdot \mu = 0$$

for all odd $k \geq 1$.

Proof. By Lemma 11.1, we can write $\mu = \mu^+ + \mu^-$, where $\mu^\pm = \frac{1}{2}(1 \pm c)\mu$. We want to show that $\mu^- = 0$ if and only if $\int_\Gamma \chi(x)^k \cdot \mu = 0$ for all odd $k \geq 1$. Since $\chi(c) = -1$, we have

$$\int_\Gamma \chi(x)^k \cdot \mu^+ = \frac{1}{2}\left(\int_\Gamma \chi^k \cdot \mu + (-1)^k \int_\Gamma \chi^k \cdot \mu \right).$$

If k is odd, the above expression vanishes, showing that $\int_\Gamma \chi(x)^k \cdot \mu = \int_\Gamma \chi(k) \cdot \mu^+$ for all odd k. On the other hand, the same argument shows that $\int_\Gamma \chi(x)^k \cdot \mu^-$ vanishes for all k even. The result follows then by Lemma 3.36. □

Corollary 11.4. *The p-adic zeta function is a pseudomeasure on Γ^+.*

Proof. This follows from the interpolation property, as $\zeta(1-k) = 0$ for odd $k \geq 1$. □

11.2. ***The ideal generated by the p-adic zeta function.*** It is natural to ask about the zeros of the p-adic zeta function. Since the zeros are not modified if we multiply by a unit, studying the zeros of a measure on Γ is equivalent to studying the ideal in $\Lambda(\Gamma)$ generated by the measure.

Even though Kubota–Leopoldt is only a pseudomeasure — hence not an element of $\Lambda(\Gamma)$ — we now see that it still "generates" a natural ideal in $\Lambda(\Gamma)$. By definition of pseudomeasures, the elements $([g]-[1])\zeta_p$ belong to the Iwasawa algebra $\Lambda(\Gamma)$ for any $g \in \Gamma$. Recall from Definition 3.37 that $I(\Gamma)$ denotes the *augmentation ideal* of $\Lambda(\Gamma)$, that is, the ideal

$$I(\Gamma) = \ker(\Lambda(\Gamma) \to \mathbb{Z}_p),$$

where $\Lambda(\Gamma) \twoheadrightarrow \mathbb{Z}_p$ is the map induced by $[g] \mapsto 1$ for any $\sigma \in \Gamma$. We define $I(\Gamma^+)$ similarly.

Proposition 11.5. *The module $I(\Gamma)\zeta_p$ is an ideal in $\Lambda(\Gamma)$. Similarly, the module $I(\Gamma^+)\zeta_p$ is an ideal in $\Lambda(\Gamma^+)$.*

Proof. Since ζ_p is a pseudomeasure, we know $([g]-[1])\zeta_p \in \Lambda(\Gamma)$ for all $g \in \Gamma$. Hence the result follows as $I(\Gamma)$ is the topological ideal generated by the elements $[g]-[1]$ for $g \in \Gamma$. The same argument holds for $I(\Gamma^+)\zeta_p$. □

11.3. ***Cyclotomic units and Iwasawa's theorem.*** Iwasawa's theorem describes the ideal $I(\Gamma)\zeta_p$ in terms of the module of cyclotomic units. We now recall this module, and its classical connection to class numbers, and then state Iwasawa's theorem.

Definition 11.6. For $n \geq 1$, we define the group $\mathscr{D}_n$ of cyclotomic units of F_n to be the intersection of $\mathscr{O}_{F_n}^\times$ and the multiplicative subgroup of $F_n^\times$ generated by $\{\pm\xi_{p^n}, \xi_{p^n}^a - 1 : 1 \leq a \leq p^n - 1\}$. We set $\mathscr{D}_n^+ = \mathscr{D}_n \cap F_n^+$.

We will study the structure of cyclotomic units more in detail in subsequent sections. The following result shows their connection to class numbers.

Theorem 11.7. *Let $n \geq 1$. The group $\mathscr{D}_n$ (resp. $\mathscr{D}_n^+$) is of finite index in the group of units $\mathscr{V}_n$ (resp. $\mathscr{V}_n^+$) in F_n (resp. F_n^+), and we have*

$$h_n^+ = [\mathscr{V}_n : \mathscr{D}_n] = [\mathscr{V}_n^+ : \mathscr{D}_n^+],$$

where $h_n^+ := \#\mathrm{Cl}(F_n^+)$ is the class number of F_n^+.

Proof. We will not prove this here; see [81, Theorem 8.2]. The proof goes by showing that the regulator of cyclotomic units is given in terms of special L-values at $s = 1$ of Dirichlet L-functions, and then using the class number formula. □

As we explained in Section 10.4, the construction of the p-adic zeta function via the Coleman map goes as follows. The cyclotomic units $c_n(a)$, introduced in Section 10.2, are naturally elements of $\mathscr{D}_n$, hence global. One then considers their image inside the space of local units, and then applies the Coleman map (Definition 10.14), which is a purely local procedure. In this spirit it is natural to switch here from studying the global modules $\mathscr{D}_n$ and $\mathscr{D}_n^+$ to their closures in the space of local units. Recall $\mathscr{U}_{\infty,1}^+$ from the notational introduction to Part II; it is the group of norm-compatible local units congruent to 1 (mod p).

Definition 11.8. For any $n \geq 1$, define $\mathscr{C}_n$ as the p-adic closure of $\mathscr{D}_n$ inside the local units $\mathscr{U}_n$,[12] let $\mathscr{C}_n^+ := \mathscr{C}_n \cap \mathscr{U}_n^+$, and let

$$\mathscr{C}_{n,1} := \mathscr{C}_n \cap \mathscr{U}_{n,1}, \qquad \mathscr{C}_{n,1}^+ := \mathscr{C}_n^+ \cap \mathscr{U}_{n,1},$$
$$\mathscr{C}_{\infty,1} := \varprojlim_{n\geq 1} \mathscr{C}_{n,1}, \qquad \mathscr{C}_{\infty,1}^+ := \varprojlim_{n\geq 1} \mathscr{C}_{n,1}^+.$$

[12] We will describe this closure more explicitly in Lemma 12.20 below.

We will see that $\mathscr{U}^+_{\infty,1}$, and its quotient $\mathscr{U}^+_{\infty,1}/\mathscr{C}^+_{\infty,1}$, naturally have $\Lambda(\Gamma^+)$-module structures. Moreover, Iwasawa explicitly related this quotient to the p-adic zeta function. The following theorem, which we prove in Section 12, says that the cyclotomic units capture the zeros of ζ_p and ultimately motivated Iwasawa to formulate his Main Conjecture.

Theorem 11.9. *The Coleman map induces an isomorphism of $\Lambda(\Gamma^+)$-modules*

$$\mathscr{U}^+_{\infty,1}/\mathscr{C}^+_{\infty,1} \xrightarrow{\sim} \Lambda(\Gamma^+)/I(\Gamma^+)\zeta_p.$$

The quotient $\mathscr{U}^+_{\infty,1}/\mathscr{C}^+_{\infty,1}$ is a local analogue, at infinite level, of the cyclotomic units inside the global units, whose indices compute class numbers in the cyclotomic tower (Theorem 11.7). They will in turn be related (see Corollary 13.14) to the Galois modules appearing in the formulation of the Iwasawa Main Conjecture. This theorem is hence the first step into proving a remarkable and deep connection between class groups and the p-adic zeta function, which will be the main purpose of the Iwasawa Main Conjecture.

12. Proof of Iwasawa's theorem

In this section, we prove Theorem 11.9. First, we equip the local units with an action of $\Lambda(\Gamma)$, and prove that the Coleman map is equivariant with respect to this action. Then, in Theorem 12.17, we compute the kernel and cokernel of the Coleman map. Finally we describe generators of the modules of cyclotomic units, and compute their image under the Coleman map. We combine all of this to prove Theorem 11.9.

12.1. ***Equivariance properties of the Coleman map.*** Theorem 11.9 is a statement about $\Lambda(\Gamma^+)$-modules. Here it is important that we work over the full Iwasawa algebra; the structure theorem for modules over $\Lambda(\Gamma)$ and $\Lambda(\Gamma^+)$ — stated in Theorem 13.1 below — is crucial in studying the Iwasawa Main Conjecture. It is desirable, then, to equip $\mathscr{U}_\infty$ with a $\Lambda(\Gamma)$-module structure. As $\Lambda(\Gamma)$ is the completed group ring of Γ over $\mathbb{Z}_p$, this amounts to equipping it with compatible actions of $\mathbb{Z}_p$ and Γ. For the latter, we use the natural Galois action on the local units. For the former, however, we are stuck: whilst there is a natural action of $\mathbb{Z}$ on $\mathscr{U}_\infty$ by $u \mapsto u^a$ for an integer a, this does not extend to an action of $\mathbb{Z}_p$.

12.1.1. *The action of $\mathbb{Z}_p$.* To fix the absence of a $\mathbb{Z}_p$-action on local units, we recall the definition of the subgroup $\mathscr{U}_{\infty,1} \subset \mathscr{U}_\infty$ introduced in (9-3). In particular, we showed there that the action of $\mathbb{Z}$ *does* extend to $\mathbb{Z}_p$ on $\mathscr{U}_{\infty,1}$. For convenience, we recall (see Definition 10.14) that the Coleman map was defined as the following composition:

$$\mathrm{Col} : \mathscr{U}_\infty \xrightarrow{u \mapsto f_u(T)} (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}} \xrightarrow{\partial \log} \mathbb{Z}_p[\![T]\!] \xrightarrow{1-\varphi\circ\psi} \mathbb{Z}_p[\![T]\!]^{\psi=0}$$
$$\xrightarrow{\partial^{-1}} \mathbb{Z}_p[\![T]\!]^{\psi=0} \xrightarrow{\mathscr{A}^{-1}} \Lambda(\mathbb{Z}_p^\times).$$

Proposition 12.1. *The map* Col *restricts to a* $\mathbb{Z}_p$*-equivariant map*

$$\mathrm{Col} : \mathscr{U}_{\infty,1} \to \Lambda(\mathbb{Z}_p^\times).$$

Proof. It suffices to check $\mathbb{Z}_p$-equivariance for each map in the composition in Definition 10.14. The action of $a \in \mathbb{Z}_p$ on $u \in \mathscr{U}_{\infty,1}$ is given by $u \mapsto u^a := \sum_{k\geq 0} \binom{a}{k}(u-1)^k$. Write $f_u = \sum_{k\geq 1} a_k(u)T^k$. We first claim that

$$a_0(u) \equiv 1 \pmod{p}. \tag{12-1}$$

Indeed, by definition $f_u(\pi_n) = u_n \equiv 1 \pmod{\mathfrak{p}_n}$ for each n, and as π_n is a uniformiser for K_n, we see

$$f_u(\pi_n) = a_0(u) + \sum_{k\geq 1} a_k(u)\pi_n^k \in a_0(u) + \mathfrak{p}_n,$$

from which we see that $a_0(u) \equiv 1 \pmod{\mathfrak{p}_n}$. But $a_0(u)$ lies in $\mathbb{Z}_p$, giving (12-1).

Thus $f_u(T) - 1 \in (p, T)$. As $\mathbb{Z}_p[\![T]\!]$ is complete in the (p, T)-adic topology,

$$f_u(T)^a = \sum_{j\geq 0} \binom{a}{j} (f_u(T) - 1)^j$$

converges to a power series $f_u^a(T) \in \mathbb{Z}_p[\![T]\!]$. Since by construction $f_u(\pi_n)^a = u_n^a$, by Lemma 10.7 we have

$$f_u^a = f_{u^a} \in (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}}.$$

As a result, we have equipped the image of $\mathscr{U}_{\infty,1}$ inside $\mathbb{Z}_p[\![T]\!]$ under the map $u \mapsto f_u$ with a $\mathbb{Z}_p$-action such that the restriction of the Coleman isomorphism is $\mathbb{Z}_p$-equivariant. We compute that $\partial \log(f_u^a) = a\partial \log(f_u)$, so $\partial \log$ is equivariant for the natural $\mathbb{Z}_p$-action on $\mathbb{Z}_p[\![T]\!]$. Finally the maps $(1 - \varphi \circ \psi)$, ∂^{-1} and $\mathscr{A}^{-1}$ are $\mathbb{Z}_p$-equivariant by definition. □

The next two lemmas show that we have not lost any information by restricting.

Lemma 12.2. *We have* $\mathscr{U}_\infty = \mu_{p-1} \times \mathscr{U}_{\infty,1}$.

Proof. We start at finite level n. As p is totally ramified in K_n for all n, there is a unique prime $\mathfrak{p}_n$ of K_n above p, and reduction modulo $\mathfrak{p}_n$ gives a short exact sequence

$$1 \to \mathscr{U}_{n,1} \to \mathscr{U}_n \to \mu_{p-1} \to 1,$$

which is split, so $\mathscr{U}_n = \mu_{p-1} \times \mathscr{U}_{n,1}$. The result follows in the inverse limit. □

Lemma 12.3. *The subgroup* μ_{p-1} *of* $\mathscr{U}_\infty$ *is killed by* Col. *In particular, no information is lost when restricting to* $\mathscr{U}_{\infty,1}$.

Proof. Note $\mu_{p-1} \subset \mathbb{Z}_p^\times$. The first map $u \mapsto f_u$ is an isomorphism that sends $v = (v)_{n\in\mathbb{N}} \in \mu_{p-1} \subset \mathscr{U}_\infty$ to the constant power series $f_v(T) = v$. But constant

power series are killed by the second map $\mathbb{Z}_p[\![T]\!] \xrightarrow{\partial \log} \mathbb{Z}_p[\![T]\!]$, which involves differentiation. Thus μ_{p-1} is mapped to zero under the composition, and hence under Col. □

Remark 12.4. The kernel of $\partial \log$ is comprised of constant power series. Moreover, if $f \in \mathbb{Z}_p[\![T]\!]$ is constant and invariant under $\mathcal{N}$, then this forces $f^p = f$. Thus the kernel of the composition of the first two maps is exactly μ_{p-1}.

12.1.2. *The Galois action.* The Galois group $\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q})$ is naturally isomorphic to $\mathrm{Gal}(K_\infty/\mathbb{Q}_p)$, as p is totally ramified in F_∞. Thus Γ acts on $\mathscr{U}_\infty$.

Notation. For $a \in \mathbb{Z}_p^\times$, let $\sigma_a \in \Gamma$ be the corresponding element of Γ with $\chi(\sigma_a) = a$, recalling that $\chi : \Gamma \xrightarrow{\sim} \mathbb{Z}_p^\times$ is the cyclotomic character from (9-1).

Proposition 12.5. *The Coleman map* $\mathrm{Col} : \mathscr{U}_\infty \to \Lambda(\Gamma)$ *is* Γ*-equivariant.*

Proof. We must show that if $a \in \mathbb{Z}_p^\times$, and $u \in \mathscr{U}_\infty$, we have

$$\mathrm{Col}(\sigma_a(u)) = \sigma_a(\mathrm{Col}(u)).$$

This is easy to check if we understand how Γ acts on each of the modules involved. If $u = (u_n)_{n\geq 1} \in \mathscr{U}_\infty$, then

$$\sigma_a(u) = (\sigma_a(u_n))_{n\geq 1} \in \mathscr{U}_\infty,$$

and if $f(T) \in \mathbb{Z}_p[\![T]\!]$, then

$$\sigma_a(f)(T) = f((1+T)^a - 1).$$

Then:

- We have

$$(\sigma_a f_u)(\pi_n) = f_u((1+\pi_n)^a - 1) = f_u(\xi_{p^n}^a - 1) = f_u(\sigma_a(\xi_{p^n} - 1)) \\ = \sigma_a(f_u(\xi_{p^n} - 1)) = \sigma_a(u_n),$$

so that $u \mapsto f_u(T)$ is Γ-equivariant.

- If $f(T) \in \mathbb{Z}_p[\![T]\!]^\times$, then an easy calculation on power series shows that

$$\partial \log(\sigma_a(f)) = a\sigma_a(\partial \log(f)). \tag{12-2}$$

- On measures, restriction to $\mathbb{Z}_p^\times$ is Γ-equivariant since the action of σ_a is by multiplying the variable by $a \in \mathbb{Z}_p^\times$, which obviously stabilises both $\mathbb{Z}_p^\times$ and $p\mathbb{Z}_p$.

- As operations on $\mathbb{Z}_p[\![T]\!]^{\psi=0}$, we have

$$\partial^{-1} \circ \sigma_a = a^{-1}\sigma_a \circ \partial^{-1}, \tag{12-3}$$

as is easily checked on measures. Indeed,

$$\begin{aligned}\int_{\mathbb{Z}_p^\times} f(x)\cdot\partial^{-1}\sigma_a\mu &= \int_{\mathbb{Z}_p^\times}\frac{f(x)}{x}\cdot\sigma_a\mu\\ &= \int_{\mathbb{Z}_p^\times}\frac{f(ax)}{ax}\cdot\mu\\ &= a^{-1}\int_{\mathbb{Z}_p^\times} f(ax)\cdot\partial^{-1}\mu = a^{-1}\int_{\mathbb{Z}_p^\times} f(x)\cdot\sigma_a\partial^{-1}\mu.\end{aligned}$$

• By definition of the action, the inverse Mahler transform $\mathscr{A}^{-1}$ is equivariant under σ_a.

Putting all that together, the result follows. □

Now, the Γ-action on $\mathscr{U}_\infty$ fixes $1\in\mu_{p-1}$, so it stabilises the subspace $\mathscr{U}_{\infty,1}$. This action commutes with the $\mathbb{Z}_p$-action on $\mathscr{U}_{\infty,1}$. We deduce that $\mathscr{U}_{\infty,1}$ is a $\Lambda(\Gamma)$-module. The results of Section 12.1 can then be summarised as follows.

Corollary 12.6. *The map* Col *restricts to a map* $\mathscr{U}_{\infty,1}\to\Lambda(\Gamma)$ *of* $\Lambda(\Gamma)$*-modules.*

Remark 12.7. In the construction of ζ_p, we renormalised by "dividing by x" (in Section 4.3). This appears here via ∂^{-1}. We see from (12-3) that ∂^{-1} really is essential for the Coleman map to be Γ-equivariant, motivating the appearance of x^{-1} in Section 4.3. Conceptually, ζ and ζ_p are the L-function and p-adic L-function of the trivial Galois representation $\mathbb{Q}_p$, whilst the cyclotomic units in $\mathscr{U}_\infty$ form an Euler system for its twist $\mathbb{Q}_p(1)$; the ∂^{-1} bridges between these two Galois representations.

12.2. ***The fundamental exact sequence.*** Theorem 11.9 says that the Coleman map induces an isomorphism $\mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+\cong\Lambda(\Gamma^+)/I(\Gamma^+)\zeta_p$. To prove this, we must study the kernel and cokernel of the Coleman map. We do so here (in Theorem 12.17) via a careful study of each of its constituent maps.

12.2.1. *The logarithmic derivative.* We will now show that the logarithmic derivative translates norm-invariance into trace-invariance (recalling the trace operator ψ). The key result is Theorem 12.9. For convenience of notation, and consistency with [16], we make the following definition.

Definition 12.8. For $f(T)\in\mathbb{Z}_p[\![T]\!]^\times$, define its logarithmic derivative as

$$\Delta(f) := \partial\log f = \frac{\partial f(T)}{f(T)} = (1+T)\frac{f'(T)}{f(T)}.$$

The main result of this section is the following.

Theorem 12.9. *The logarithmic derivative induces a short exact sequence*

$$0\to\mu_{p-1}\to(\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}}\xrightarrow{\Delta}\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}\to 0.$$

We described the kernel of Δ in Remark 12.4 above, so it suffices to deal with its image. We first prove that this image is contained in $\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$ (Lemma 12.10). We then reduce the proof of surjectivity, via Lemma 12.11, to surjectivity modulo p. Finally, in Lemmas 12.12 and 12.13 we calculate the reduction modulo p of both spaces.

For convenience, let $\mathscr{W} := (\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}}$.

Lemma 12.10. *We have* $\Delta(\mathscr{W}) \subseteq \mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$.

Proof. If $f \in \mathscr{W}$, then

$$\varphi(f) = (\varphi \circ \mathcal{N})(f) = \prod_{\eta \in \mu_p} f((1+T)\eta - 1).$$

Applying Δ to the above equality and using the fact that $\Delta \circ \varphi = p\varphi \circ \Delta$ (which is easy to see on power series from the definitions), we obtain

$$(\varphi \circ \Delta)(f) = p^{-1} \sum_{\eta \in \mu_p} \Delta(f)((1+T)\eta - 1) = (\varphi \circ \psi)(\Delta(f)).$$

By injectivity of φ, we deduce $\psi(\Delta(f)) = \Delta(f)$. □

We move now to the proof of surjectivity. In the following, let

$$A = \overline{\Delta(\mathscr{W})} \subseteq \boldsymbol{F}_p[\![T]\!], \quad B = \overline{\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}} \subseteq \boldsymbol{F}_p[\![T]\!]$$

be the reduction modulo p of the modules we need to compare.

Lemma 12.11. *If* $A = B$, *then* $\Delta(\mathscr{W}) = \mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$.

Proof. Let $f_0 \in \mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$. By hypothesis, there exists a $g_1 \in \mathscr{W}$ such that

$$\Delta(g_1) - f_0 = pf_1 \quad \text{for some } f_1 \in \mathbb{Z}_p[\![T]\!].$$

Since $\Delta(\mathscr{W}) \subseteq \mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$ by Lemma 12.10, we see that ψ fixes both $\Delta(g_1)$ and f_0 and hence, by additivity, ψ fixes f_1; so again by hypothesis, there exists some $g_2 \in \mathscr{W}$ such that

$$\Delta(g_2) - f_1 = pf_2 \quad \text{for some } f_2 \in \mathbb{Z}_p[\![T]\!].$$

By induction, there exist $g_i \in \mathscr{W}$ and $f_i \in \mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$, $i \geq 1$, such that

$$\Delta(g_i) - f_{i-1} = pf_i.$$

Now let

$$h_n = \prod_{k=1}^{n} g_k^{(-1)^{k-1}p^{k-1}} \in \mathscr{W},$$

i.e.,

$$h_1 = g_1, \quad h_2 = \frac{g_1}{g_2^p}, \quad h_3 = \frac{g_1 \cdot g_3^{p^2}}{g_2^p}, \quad h_4 = \frac{g_1 \cdot g_3^{p^2}}{g_2^p \cdot g_4^{p^3}},$$

etc. As Δ transforms multiplication into addition, we have

$$\begin{aligned}\Delta(h_n) &= \Delta(g_1) - p\Delta(g_2) + \cdots + (-1)^{n-1} p^{n-1} \Delta(g_n) \\ &= (f_0 + pf_1) - (pf_1 + p^2 f_2) + \cdots + (-1)^{n-1}(p^{n-1} f_{n-1} + p^n f_n) \\ &= f_0 + (-1)^{n-1} p^n f_n.\end{aligned}$$

By compactness, the sequence $(h_n)_{n\geq 1}$ admits a convergent subsequence converging to an element $h \in \mathscr{W}$ satisfying $\Delta(h) = f_0$, which shows the result. □

Lemma 12.12. *We have* $\overline{\mathscr{W}} := \mathscr{W} \pmod p = \boldsymbol{F}_p[\![T]\!]^\times$.

Proof. The inclusion $\subset$ is obvious. Conversely, for any element $f \in \boldsymbol{F}_p[\![T]\!]^\times$, lift it to an element $\widetilde{f_0} \in \mathbb{Z}_p[\![T]\!]^\times$. By points (ii) and (iv) of Lemma 10.11, the sequence $\mathcal{N}^k(\widetilde{f_0})$ converges to an element $\widetilde{f}$ that is invariant under $\mathcal{N}$ and whose reduction modulo p is f. □

The most delicate and technical part of the proof of Theorem 12.9 is contained in the following two lemmas describing the reduction of $\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$ modulo p.

Lemma 12.13. *We have* $B = \Delta(\boldsymbol{F}_p[\![T]\!]^\times)$.

Proof. We have $\Delta(\mathscr{W}) \subseteq \mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$ by Lemma 12.10, and therefore the inclusion $\Delta(\boldsymbol{F}_p[\![T]\!]^\times) \subset B$ is clear using Lemma 12.12. For the other inclusion, take any $f \in B$ and use Lemma 12.14 below to write

$$f = \Delta(a) + b$$

for some $a \in \boldsymbol{F}_p[\![T]\!]^\times$ and $b = \sum_{m=1}^{+\infty} d_m \frac{T+1}{T} T^{pm}$. Since $\psi(f) = f$ and $\psi(\Delta(a)) = \Delta(a)$ (by a slight abuse of notation, as f and $\Delta(a)$ are actually the reduction modulo p of elements fixed by ψ), we deduce that $\psi(b) = b$. But we can explicitly calculate the action of ψ on b. Using the identity[13] $\psi(g \cdot \varphi(f)) = \psi(g) f$, the identity $T^{pm} = \varphi(T^m)$ in $\boldsymbol{F}_p[\![T]\!]$ and the fact that ψ fixes $\frac{T+1}{T}$ (see the proof of Lemma 4.7), we deduce that

$$\psi(b) = \sum_{m=1}^{+\infty} d_m \frac{T+1}{T} T^m,$$

which immediately implies $b = 0$ and concludes the proof. □

Lemma 12.14. *We have*

$$\boldsymbol{F}_p[\![T]\!] = \Delta(\boldsymbol{F}_p[\![T]\!]^\times) + \frac{T+1}{T} C,$$

where $C = \left\{ \sum_{n=1}^{+\infty} a_n T^{pn} \right\} \subseteq \boldsymbol{F}_p[\![T]\!]$.

[13] Again, this can be easily checked on measures.

Proof. One inclusion is clear. Take $g \in \boldsymbol{F}_p[\![T]\!]$ and write $\frac{T}{T+1}g = \sum_{n=1}^{+\infty} a_n T^n$. Define

$$h = \sum_{\substack{m=1 \\ (m,p)=1}}^{+\infty} a_m \sum_{k=0}^{+\infty} T^{mp^k}.$$

Clearly $\frac{T}{T+1}g - h \in C$, so it suffices to show that $\frac{T+1}{T}h \in \Delta(\boldsymbol{F}_p[\![T]\!]^\times)$. Indeed, we will show by induction that, for every $m \geq 1$, there exists $\alpha_i \in \boldsymbol{F}_p$ for $1 \leq i < m$ such that

$$h_m := \frac{T+1}{T}h - \left(\sum_{i=1}^{m-1} \Delta(1-\alpha_i T^i)\right) \in T^{m-1}\boldsymbol{F}_p[\![T]\!].$$

The case $m = 1$ is empty. Suppose that the claim is true for m and that $\alpha_1, \ldots, \alpha_{m-1}$ have been chosen. Observe first that

$$\Delta(1-\alpha_i T^i) = -\frac{T+1}{T}\sum_{k=1}^{+\infty} i\alpha_i^k T^{ik},$$

so we can write

$$h_m = \frac{T+1}{T}\sum_{k=m}^{+\infty} d_k T^k.$$

Observe that, by construction of h and h_m, we have $d_n = d_{np}$ for all n. If $d_m = 0$ then we set $\alpha_m = 0$. If $d_m \neq 0$ then, by what we have just remarked, m must be prime to p, hence invertible in $\boldsymbol{F}_p$, and we set $\alpha_m = -d_m/m$. One can then check that

$$g = \prod_{n=1}^{+\infty}(1-\alpha_n T^n) \in \boldsymbol{F}_p[\![T]\!]$$

satisfies $\Delta(g) = \frac{T+1}{T}h$, which concludes the proof. □

We can now complete the proof of Theorem 12.9.

Proof of Theorem 12.9. By Lemma 12.10, the map Δ is well defined, and its kernel is μ_p by Remark 12.4. It remains to prove surjectivity. By Lemma 12.11, it suffices to prove that $A = B$, which follows directly from Lemmas 12.12 and 12.13. □

12.2.2. *The fundamental exact sequence.* Finally, we will study the fundamental exact sequence describing the kernel and cokernel of the Coleman map. The only remaining map to study is $1 - \varphi \circ \psi$. By Theorem 12.9, it suffices to study this on $\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$.

Lemma 12.15. *There is an exact sequence*

$$0 \to \mathbb{Z}_p \to \mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}} \xrightarrow{1-\varphi} \mathbb{Z}_p[\![T]\!]^{\psi=0} \to \mathbb{Z}_p \to 0,$$

where the first map is the natural inclusion and the last map is evaluation at $T = 0$.

Proof. Injectivity of the first map is trivial. To see surjectivity of the last map, note that $\psi(1+T)=0$, since

$$(\varphi\circ\psi)(1+T)=p^{-1}\sum_{\eta\in\mu_p}\eta(1+T)=0.$$

Thus $1+T\in\mathbb{Z}_p[\![T]\!]^{\psi=0}$ and is mapped to 1 under the last map.

Let $f(T)\in\mathbb{Z}_p[\![T]\!]^{\psi=0}$ be in the kernel of the last map, that is, be such that $f(0)=0$. Then $\varphi^n(f)$ goes to zero (in the weak $/(p,T)$-adic topology) and hence $\sum_{n\geq 0}\varphi^n(f)$ converges to an element $g(T)$ whose image under $(1-\varphi)$ is $f(T)$. Since $\psi\circ\varphi=\mathrm{id}$, we also have

$$\psi(g)=\sum_{n\geq 0}\psi\circ\varphi^n(f)=\psi(f)+\sum_{n\geq 1}\varphi^{n-1}(f)=g,$$

as $\psi(f)=0$, which shows that

$$f\in(1-\varphi)(\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}})$$

and hence that the sequence is exact at $\mathbb{Z}_p[\![T]\!]^{\psi=0}$. Finally, if $f(T)\in\mathbb{Z}_p[\![T]\!]$ is not constant, then $f(T)=a_0+a_rT^r+\cdots$ for some $a_r\neq 0$ and $\varphi(f)(T)=a_0+pa_rT^r+\cdots\neq f(T)$, which shows that $\ker(1-\varphi)=\mathbb{Z}_p$, finishing the proof. □

Definition 12.16. Let $\mathbb{Z}_p(1):=\varprojlim\mu_{p^n}$, the module $\mathbb{Z}_p$ with an action of Γ by $\sigma\cdot x=\chi(\sigma)x$, recalling χ is the cyclotomic character. This is an integral version of $\mathbb{Q}_p(1)$.

Theorem 12.17. *The Coleman map induces an exact sequence of Γ-modules*

$$0\to\mu_{p-1}\times\mathbb{Z}_p(1)\to\mathscr{U}_\infty\xrightarrow{\mathrm{Col}}\Lambda(\Gamma)\to\mathbb{Z}_p(1)\to 0,$$

where the last map sends $\mu\in\Lambda(\Gamma)$ to $\int_\Gamma\chi\cdot\mu$. In particular, it induces an exact sequence

$$0\to\mathbb{Z}_p(1)\to\mathscr{U}_{\infty,1}\xrightarrow{\mathrm{Col}}\Lambda(\Gamma)\to\mathbb{Z}_p(1)\to 0$$

of $\Lambda(\Gamma)$-modules.

Proof. We first compute the kernel of the Coleman map, which we recall from Definition 10.14 is the composition

$$\mathrm{Col}:\mathscr{U}_\infty\xrightarrow{u\mapsto f_u(T)}(\mathbb{Z}_p[\![T]\!]^\times)^{\mathcal{N}=\mathrm{id}}\xrightarrow{\Delta}\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}\xrightarrow{1-\varphi\circ\psi}\mathbb{Z}_p[\![T]\!]^{\psi=0}\xrightarrow{\partial^{-1}}\mathbb{Z}_p[\![T]\!]^{\psi=0}\xrightarrow{\mathscr{A}^{-1}}\Lambda(\mathbb{Z}_p^\times).$$

In the third term, we have used Theorem 12.9 to replace $\mathbb{Z}_p[\![T]\!]$ with $\mathbb{Z}_p[\![T]\!]^{\psi=\mathrm{id}}$.

The first map is an isomorphism by Theorem 10.13. By Theorem 12.9, the second map surjects with kernel μ_{p-1}. By Lemma 12.15 the third map has kernel $\mathbb{Z}_p$; this is

the image of $\{(1+T)^a : a \in \mathbb{Z}_p\}$ under Δ. This is the power series interpolating the sequence $(\xi_{p^n}^a)_{n\geq 1}$. Accordingly, when we pull this back to $\mathscr{U}_\infty$, we get the factor

$$\mathbb{Z}_p(1) = \{(\xi_{p^n}^a)_n : a \in \mathbb{Z}_p\} \subset \mathscr{U}_\infty.$$

Finally, the fourth and fifth maps are isomorphisms, so ultimately the kernel of Col is as claimed.

We now compute the cokernel. The first two and last two maps in Col are surjective, and the third map has cokernel $\mathbb{Z}_p$ by Lemma 12.15, showing the exactness of the sequence.

Finally, we turn to the Γ-equivariance. The subspace $\mu_{p-1} \times \mathbb{Z}_p(1) \subset \mathscr{U}_\infty$ is preserved by Γ, so the first map is Γ-equivariant. That Col is Γ-equivariant was Corollary 12.6. The last map is Γ-equivariant since

$$\int_\Gamma \chi(x) \cdot \sigma\mu(x) = \int_\Gamma \chi(\sigma x) \cdot \mu(x) = \chi(\sigma) \int_\Gamma \chi \cdot \mu,$$

and Γ acts on $\mathbb{Z}_p(1)$ through the cyclotomic character χ. □

12.3. ***Generators for the global cyclotomic units.*** Recall the (global) module of cyclotomic units $\mathscr{D}_n$ is the intersection of $\mathscr{O}_{F_n}^\times$ with the multiplicative subgroup of $F_n^\times$ generated by $\pm\xi_{p^n}$ and $\xi_{p^n}^a - 1$ with $1 \leq a < p^n$, and $\mathscr{D}_n^+ = \mathscr{D}_n \cap F_n^+$. We now show this module is cyclic over the group ring $\mathbb{Z}[\Gamma_n^+]$. This is essential preparation for treating the local analogue $\mathscr{C}_{n,1}^+$ in the next subsection.

Recall that we defined

$$c_n(a) := \frac{\xi_{p^n}^a - 1}{\xi_{p^n} - 1} \in \mathscr{D}_n,$$

and note that

$$\gamma_{n,a} := \xi_{p^n}^{(1-a)/2} c_n(a) = \frac{\xi_{p^n}^{a/2} - \xi_{p^n}^{-a/2}}{\xi_{p^n}^{1/2} - \xi_{p^n}^{-1/2}}$$

is fixed by conjugation $c \in \Gamma$, hence gives an element of $\mathscr{D}_n^+$. In fact:

Lemma 12.18. *Let $n \geq 1$. Then*:

(i) *The group $\mathscr{D}_n^+$ is generated by -1 and*

$$\left\{\gamma_{n,a} : 1 < a < \tfrac{1}{2}p^n, (a, p) = 1\right\}.$$

(ii) *The group $\mathscr{D}_n$ is generated by ξ_{p^n} and $\mathscr{D}_n^+$.*

Proof. We first show that we need only consider those elements $\xi_{p^n}^a - 1$ with a prime to p. Indeed, this follows from the identity

$$\xi_{p^n}^{bp^m} - 1 = \prod_{j=0}^{p^m-1} (\xi_{p^n}^{b+jp^{n-m}} - 1),$$

where $(b, p) = 1$ and $1 \le m < n$, noting that $b + jp^{n-m}$ is prime to p. Also, since $\xi_{p^n}^a - 1 = -\xi_{p^n}^a(\xi_{p^n}^{-a} - 1)$, we can restrict to considering $1 \le a < \frac{1}{2}p^n$ (recall here that p is odd).

Suppose that

$$\gamma = \pm\xi_{p^n}^d \prod_{\substack{1\le a<\frac{1}{2}p^n \\ (a,p)=1}} (\xi_{p^n}^a - 1)^{e_a} \in \mathscr{D}_n,$$

for some integers d and e_a. Since $v_p(\xi_{p^n}^d) = 0$ and all the p-adic valuations of $\xi_{p^n}^a - 1$ coincide $\big($namely, $v_p(\xi_{p^n}^a - 1) = \frac{1}{(p-1)p^{n-1}}\big)$, we deduce that $\sum_a e_a = 0$. Therefore we can write

$$\gamma = \pm\xi_{p^n}^d \prod_a \left(\frac{\xi_{p^n}^a - 1}{\xi_{p^n} - 1}\right)^{e_a} = \pm\xi_{p^n}^e \prod_a \gamma_{n,a}^{e_a},$$

where $e = d + \frac{1}{2}\sum_a e_a(a-1)$. This shows the second point; the first point follows by observing that every term $\gamma_{n,a}^{e_a}$ of the product is real, so $\gamma \in \mathscr{D}_n^+$ if and only if $e = 0$. □

Corollary 12.19. *If a generates $(\mathbb{Z}/p^n\mathbb{Z})^\times$, then $\gamma_{n,a}$ generates $\mathscr{D}_n^+$ as a $\mathbb{Z}[\Gamma_n^+]$-module.*

Proof. If $1 \le b < p^n$ is prime to p, then $b \equiv a^r \pmod{p}^n$ for some $r \ge 0$, and hence

$$\gamma_{n,b} = \frac{\xi_{p^n}^{a^r} - 1}{\xi_{p^n} - 1} = \prod_{i=0}^{r-1} \frac{\xi_{p^n}^{a^{i+1}} - 1}{\xi_{p^n}^{a^i} - 1} = \prod_{i=0}^{r-1} (\gamma_{n,a})^{\sigma_a^i}. \qquad \square$$

12.4. ***Generators for the local cyclotomic units.*** We now move to analogous results for the local cyclotomic units, that is, the p-adic closure of the global cyclotomic units.

A natural guess might be that "as $\mathscr{D}_n^+$ is generated by $\gamma_{n,a}$ as a $\mathbb{Z}[\Gamma_n^+]$-module, $\mathscr{C}_n^+$ is generated by $\gamma_{n,a}$ as a $\mathbb{Z}_p[\Gamma_n^+]$-module". However, this is nonsense, since $\mathscr{C}_n^+$ is not a $\mathbb{Z}_p$-module; to parse this, we must pass to the principal cyclotomic units $\mathscr{C}_{n,1}^+$. The following simple lemma then describes precisely the p-adic closure.

Lemma 12.20. *Let $g_1, \dots, g_r \in \mathscr{U}_{n,1}$, and let $X = \langle g_1, \dots, g_r\rangle \subset \mathscr{U}_{n,1}$ be the $\mathbb{Z}$-module they generate (multiplicatively[14]). Then the p-adic closure $\overline{X}$ of X in $\mathscr{U}_{n,1}$ is the $\mathbb{Z}_p$-submodule of $\mathscr{U}_{n,1}$ generated by $g_1, \dots, g_r$.*

Proof. Let $a \in \mathbb{Z}_p$, and a_j be any sequence of integers tending to $a \in \mathbb{Z}_p$. Then

$$g_i^{a_j} = \sum_{k\ge 0} \binom{a_j}{k} (g_i - 1)^k \;\to\; \sum_{k\ge 0} \binom{a}{k} (g_i - 1)^k = g_i^a, \tag{12-4}$$

[14]By which we mean, the $\mathbb{Z}$-module structure is given by exponentiation, i.e., $(a, g) \mapsto g^a$ for $a \in \mathbb{Z}$ (or $\mathbb{Z}_p$). As is standard, but perhaps confusingly, we sometimes use additive notation ag for this module structure.

since $g_i - 1 \equiv 0 \pmod{\mathfrak{p}_n}$ (as $g_i \in \mathscr{U}_{n,1}$). Thus g_i^a lies in the p-adic closure. An identical argument shows more generally that the $\mathbb{Z}_p$-span of the g_i's is a subset of the p-adic closure.

To see the converse, let $g \in \overline{X}$. Then by definition there exists a sequence $(g_1^{a_{1,j}} \cdots g_r^{a_{r,j}})_j \subset X$ tending to g, with each $a_{i,j} \in \mathbb{Z}$. This gives a sequence $(a_{1,j}, \ldots, a_{r,j})_j \subset \mathbb{Z}^r \subset \mathbb{Z}_p^r$. By compactness of $\mathbb{Z}_p^r$, there exists a convergent subsequence

$$(b_{1,k}, \ldots, b_{r,k})_k \to (b_1, \ldots, b_r) \in \mathbb{Z}_p^r.$$

Then $(g_1^{b_{1,k}} \cdots g_r^{b_{r,k}})_k$ converges to $g_1^{b_1} \cdots g_r^{b_r}$ by (12-4); but by construction it also converges to g. Thus $g = g_1^{b_1} \cdots g_r^{b_r}$, showing that g lies in the $\mathbb{Z}_p$-span of the g_i's, as required. □

We now put Corollary 12.19 into a form useful for Lemma 12.20.

Lemma 12.21. *Let $a \in \mathbb{Z}$ be a topological generator of $\mathbb{Z}_p^\times$, and $w \in \mu_{p-1} \subset \mathscr{U}_n$ be such that $aw \equiv 1 \pmod{\mathfrak{p}_n}$. Then*:

(i) $w\gamma_{n,a} \in \mathscr{U}_{n,1}$.

(ii) $(w\gamma_{n,a})^{p-1} = \gamma_{n,a}^{p-1}$ *lies in $\mathscr{U}_{n,1}^+$, and generates the cyclic $\mathbb{Z}[\Gamma_n^+]$-module*

$$\mathbb{Z}[\Gamma_n^+] \cdot (w\gamma_{n,a})^{p-1} = (p-1)\mathscr{D}_n^+ = \{\gamma^{p-1} : \gamma \in \mathscr{D}_n^+\} \subset \mathscr{U}_{n,1}^+.$$

Proof. (i) We first claim $\gamma_{n,a} \equiv a \pmod{\mathfrak{p}_n}$. Indeed, by definition, $\gamma_{n,a} = \xi_{p^n}^{a/2} c_n(a)$. Recall $\pi_n = \xi_{p^n} - 1$ is a uniformiser in $\mathfrak{p}_n$, so $\xi_{p^n}^{a/2} \equiv 1 \pmod{\mathfrak{p}_n}$. It thus suffices to show

$$c_n(a) \equiv a \pmod{\mathfrak{p}_n}.$$

For this, recall that by construction of the Coleman power series attached to any unit $u = (u_n) \in \mathscr{U}_\infty$, we have

$$u_n = f_u(\pi_n) \equiv f_u(0) \pmod{\mathfrak{p}_n}.$$

For $u = c(a)$, recall we have $f_{c(a)} = ((1+T)^a - 1)/T$; so $c_n(a) \equiv f_{c(a)}(0) = a \pmod{\mathfrak{p}_n}$, proving the claim. Thus w is the unique element of μ_{p-1} such that $w\gamma_{n,a} \equiv 1 \pmod{\mathfrak{p}_n}$, and hence $w\gamma_{n,a} \in \mathscr{U}_{n,1}$, as required.

(ii) By Corollary 12.19, we know $\gamma_{n,a}$ generates $\mathscr{D}_n^+$, and deduce $\gamma_{n,a}^{p-1}$ generates $(p-1)\mathscr{D}_n^+$. In particular $\gamma_{n,a}^{p-1}$ lies in $\mathscr{U}_{n,1}^+$. Because $w^{p-1} = 1$, we have $\gamma_{n,a}^{p-1} = (w\gamma_{n,a})^{p-1}$, giving (ii). □

Lemma 12.22. *Let $a \in \mathbb{Z}$ be a topological generator of $\mathbb{Z}_p^\times$, and $w \in \mu_{p-1} \subset \mathscr{U}_n$ be such that $aw \equiv 1 \pmod{\mathfrak{p}_n}$. Then*:

(i) *The module $\mathscr{C}_{n,1}^+$ is a cyclic $\mathbb{Z}_p[\Gamma_n^+]$-module generated by $w\gamma_{n,a}$.*

(ii) *The module $\mathscr{C}_{\infty,1}^+$ is a cyclic $\Lambda(\Gamma^+)$-module generated by $(w\gamma_{n,a})_{n\geq 1}$.*

Proof. (i) By Lemma 12.21(ii),

$$(p-1)\mathscr{D}_n^+ = (p-1)\mathscr{D}_{n,1}^+ \subset \mathscr{U}_{n,1}^+$$

is generated as a $\mathbb{Z}[\Gamma_n^+]$-module by $(w\gamma_{n,a})^{p-1}$. By Lemma 12.20 the p-adic closure $(p-1)\mathscr{C}_{n,1}^+$ of $(p-1)\mathscr{D}_{n,1}^+$ is generated as a $\mathbb{Z}_p[\Gamma_n^+]$-module by $(w\gamma_{n,a})^{p-1}$. As $p-1$ is invertible in $\mathbb{Z}_p$, we conclude $(p-1)\mathscr{C}_{n,1}^+ = \mathscr{C}_{n,1}^+$ is generated by $w\gamma_{n,a}$. We use here that $w\gamma_{n,a} \equiv 1 \pmod{\mathfrak{p}_n}$, so that $w\gamma_{n,a}$ is the unique $(p-1)$-th root of $(w\gamma_{n,a})^{p-1}$ lying in $\mathscr{C}_{n,1}^+$.

(ii) Observe that

$$\mathscr{C}_{\infty,1}^+ \cong \varprojlim \mathscr{C}_{n,1}^+ = \varprojlim (\mathbb{Z}_p[\Gamma_n^+] \cdot w\gamma_{n,a}) \cong \Lambda(\Gamma^+) \cdot (w\gamma_{n,a})_n,$$

as required, with all maps as $\Lambda(\Gamma^+)$-modules and where the middle equality is from (i). □

12.5. ***End of the proof.*** Finally we can prove Iwasawa's theorem, Theorem 11.9.

Theorem 12.23. *The Coleman map induces*

(i) *a short exact sequence of* $\Lambda(\Gamma)$*-modules*

$$0 \to \mathscr{U}_{\infty,1}/\mathscr{C}_{\infty,1} \to \Lambda(\Gamma)/I(\Gamma)\zeta_p \to \mathbb{Z}_p(1) \to 0,$$

(ii) *an isomorphism of* $\Lambda(\Gamma^+)$*-modules*

$$\mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ \xrightarrow{\sim} \Lambda(\Gamma^+)/I(\Gamma^+)\zeta_p.$$

Proof. Theorem 12.17 gave an exact sequence of $\Lambda(\Gamma)$-modules

$$0 \to \mathbb{Z}_p(1) \to \mathscr{U}_{\infty,1} \xrightarrow{\mathrm{Col}} \Lambda(\Gamma) \to \mathbb{Z}_p(1) \to 0.$$

The theorem will follow by calculating the image of the modules $\mathscr{C}_{\infty,1}$ and $\mathscr{C}_{\infty,1}^+$ under the Coleman map. By Lemma 12.22, it suffices to calculate the image under Col of an element $(\xi_{p^n}^b \gamma_{n,a})_{n\geq 1} \in \mathscr{U}_{\infty,1}$, for $a, b \in \mathbb{Z}_p^\times$. But this has already been done: by Theorem 10.15, and the fact that $\xi_{p^n}^b$ lies in the kernel of the Coleman map, we know that

$$\mathrm{Col}((\xi_{p^n}^b \gamma_{n,a})_{n\geq 1}) = \mathrm{Col}(\xi_{p^n}^{-(1-a)/2}(\gamma_{n,a})_{n\geq 1}) = \mathrm{Col}(c(a)) = ([\sigma_a] - [1])\zeta_p,$$

where as usual σ_a denotes an element of Γ such that $\chi(\sigma_a) = a$. Since $a \in \mathbb{Z}_p^\times$ was arbitrary, we conclude that the image of $\mathscr{C}_{\infty,1}$ (resp. $\mathscr{C}_{\infty,1}^+$) under Col is $I(\Gamma)\zeta_p$ (resp. $I(\Gamma^+)\zeta_p$). We deduce an exact sequence

$$0 \to \mathscr{U}_{\infty,1}/\mathscr{C}_{\infty,1} \to \Lambda(\Gamma)/I(\Gamma)\zeta_p \to \mathbb{Z}_p(1) \to 0.$$

This shows (i). Since p is odd, taking invariants under the group $\langle c\rangle \subset \Gamma$ of order two generated by complex conjugation is exact. As c acts on $\mathbb{Z}_p(1)$ by -1, we see that $\mathbb{Z}_p(1)^{\langle c\rangle} = 0$, which shows (ii) and concludes the proof of the theorem. □

13. The Iwasawa Main Conjecture

We now move from arithmetic to algebra. To state the Iwasawa Main Conjecture, we use the structure theory of Λ-modules. We first summarise this theory. We then define modules from the Galois theory of abelian extensions that will be needed. These modules carry an action of the Galois group $\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times$, and hence obtain the structure of $\Lambda(\Gamma)$-modules. The Iwasawa Main Conjecture describes the characteristic ideal of one of these Galois modules in terms of the Kubota–Leopoldt p-adic L-function.

In the interests of space, we state without proof some relevant auxiliary results.

13.1. ***Structure theory for Λ-modules.*** There is a rich structure theory of modules over Iwasawa algebras, which looks similar to that of modules over PIDs. Here we state (without proof) some basic yet fundamental results.

Let L be a finite extension of $\mathbb{Q}_p$, and $\mathcal{O}_L$ its ring of integers, and let $\Lambda := \Lambda(\mathbb{Z}_p) = \varprojlim \mathcal{O}_L[\mathbb{Z}_p/p^n\mathbb{Z}_p] \cong \mathcal{O}_L[\![T]\!]$ be the Iwasawa algebra of $\mathbb{Z}_p$ over $\mathcal{O}_L$. Let M and M' be two Λ-modules. We say that M is pseudoisomorphic to M', and we write $M \sim M'$, if there exists a homomorphism $M \to M'$ with finite kernel and cokernel, i.e., if there is an exact sequence

$$0 \to A \to M \to M' \to B \to 0,$$

with A and B finite Λ-modules (just in case: A and B have finite cardinality!). We remark that $\sim$ is *not* an equivalence relation (see [81, Warning, Section 13.2]) but it *is* an equivalence relation between *finitely generated*, *torsion* Λ-modules. The following is the main result concerning the structure theory of finitely generated Λ-modules.

Theorem 13.1 [81, Theorem 13.12]. *Let M be a finitely generated Λ-module. Then*

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\right),$$

for some $r, s, t \geq 0$, $n_i, m_j \geq 1$ and irreducible distinguished polynomials $f_j(T) \in \mathcal{O}[T]$.

Here we call a polynomial $P(T) \in \mathcal{O}_L[T]$ *distinguished* if $P(T) = a_0 + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n$ with $a_i \in \mathfrak{p}$ for every $0 \leq i \leq n-1$.

Remark 13.2. We do *not* have a similar result for the finite-level group algebras $\mathcal{O}_L[\mathbb{Z}_p/p^n\mathbb{Z}_p]$, only for the projective limit. This is another major example of the

fundamental concept of Iwasawa theory, where it is profitable to study a whole tower of objects all in one go, rather than individually at finite level.

Definition 13.3. Suppose M is a finitely generated torsion Λ-module. Then $r = 0$ in the structure theorem. We define the *characteristic ideal* of M to be the ideal

$$\mathrm{Ch}_\Lambda(M) = (p^n) \prod_{j=1}^{t} (f_j^{m_j}) \subset \Lambda, \quad \text{where } n = \sum_{i=1}^{s} n_i.$$

We will apply this theory more generally. Suppose $\Gamma = H \times \Gamma'$, where H is a finite commutative group of order prime to p and $\Gamma' \cong \mathbb{Z}_p$. A key example to have in mind is $\Gamma = \mathbb{Z}_p^\times$, $H = \mu_{p-1}$ and $\Gamma' = 1 + p\mathbb{Z}_p$. Then we have a decomposition

$$\Lambda(\Gamma) \cong \mathscr{O}_L[H] \otimes \Lambda.$$

Let M be a finitely generated torsion $\Lambda(\Gamma)$-module. Let $H^\wedge$ denote the group of characters of H and define, for any $\omega \in H^\wedge$, the projector to the isotypic component

$$e_\omega := \frac{1}{|H|} \sum_{a \in H} \omega^{-1}(a)[a] \in \mathscr{O}_L[H],$$

possibly after extending L by adjoining the values of ω. As the order of H is prime to p, one can easily show the following result.

Lemma 13.4 [16, A.1]. *The group H acts on $M^{(\omega)} := e_\omega M$ via multiplication by ω and we have a decomposition of $\Lambda(\Gamma)$-modules*

$$M = \bigoplus_{\omega \in H^\wedge} M^{(\omega)}.$$

Moreover, each $M^{(\omega)}$ is a finitely generated torsion Λ-module.

Definition 13.5. Let $\Gamma = H \times \mathbb{Z}_p$ be as above and let M be a finitely generated torsion $\Lambda(\Gamma)$-module. We define the *characteristic ideal* of M to be the ideal

$$\mathrm{Ch}_{\Lambda(\Gamma)}(M) := \bigoplus_{\omega \in H^\wedge} \mathrm{Ch}_\Lambda(M^{(\omega)}) \subseteq \Lambda(\Gamma).$$

Lemma 13.6 [16, A.1 Proposition 1]. *The characteristic ideal is multiplicative in exact sequences.*

13.2. ***The Λ-modules arising from Galois theory.*** The following Λ-modules will be the protagonists of the Galois side of the Main Conjecture; we urge the reader to refer back to the following definitions as these objects appear in the text. Recall $F_n = \mathbb{Q}(\mu_{p^n})$, that $\mathfrak{p}_n$ is the unique prime above p in F_n, and other similar notation from Section 9. Then define

$$\mathscr{M}_n := \text{maximal abelian } p\text{-extension of } F_n \text{ unramified outside } \mathfrak{p}_n,$$
$$\mathscr{M}_n^+ := \text{maximal abelian } p\text{-extension of } F_n^+ \text{ unramified outside } \mathfrak{p}_n^+,$$

$$\mathscr{L}_n := \text{maximal unramified abelian } p\text{-extension of } F_n,$$
$$\mathscr{L}_n^+ := \text{maximal unramified abelian } p\text{-extension of } F_n^+,$$

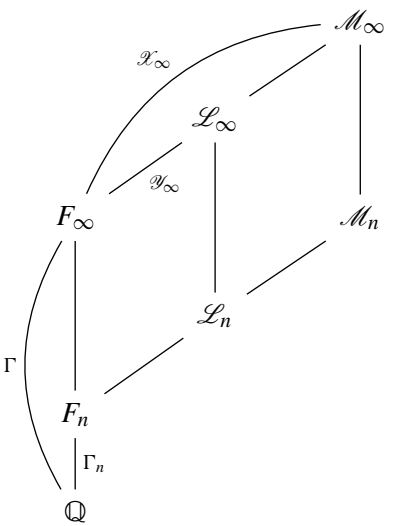
and set

$$\mathscr{M}_\infty := \bigcup_{n\geq 1} \mathscr{M}_n = \text{maximal abelian pro-}p\text{-extension of } F_\infty \text{ unramified outside } \mathfrak{p},$$
$$\mathscr{M}_\infty^+ := \bigcup_{n\geq 1} \mathscr{M}_n^+ = \text{maximal abelian pro-}p\text{-extension of } F_\infty^+ \text{ unramified outside } \mathfrak{p}^+,$$
$$\mathscr{L}_\infty := \bigcup_{n\geq 1} \mathscr{L}_n = \text{maximal unramified abelian pro-}p\text{-extension of } F_\infty,$$
$$\mathscr{L}_\infty^+ := \bigcup_{n\geq 1} \mathscr{L}_n^+ = \text{maximal unramified abelian pro-}p\text{-extension of } F_\infty^+.$$

Finally, define

$$\mathscr{X}_\infty := \mathrm{Gal}(\mathscr{M}_\infty/F_\infty), \quad \mathscr{X}_\infty^+ = \mathrm{Gal}(\mathscr{M}_\infty^+/F_\infty^+),$$
$$\mathscr{Y}_\infty := \mathrm{Gal}(\mathscr{L}_\infty/F_\infty), \quad \mathscr{Y}_\infty^+ = \mathrm{Gal}(\mathscr{L}_\infty^+/F_\infty^+).$$

These modules fit into the following diagram of field extensions:



There is an identical diagram for the totally real objects, with superscripts $^+$ everywhere.

Remark 13.7. In the limit, the module $\mathscr{X}_\infty$ is a $\Lambda(\Gamma)$-module, and thus can be studied via Theorem 13.1. To describe this, let $x \in \mathscr{X}_\infty$ and $\sigma \in \Gamma$, and choose any lifting $\widetilde{\sigma} \in \mathrm{Gal}(\mathscr{M}_\infty/\mathbb{Q})$ of σ; then

$$\sigma \cdot x := \widetilde{\sigma} x \widetilde{\sigma}^{-1}$$

gives a well-defined action of Γ on $\mathscr{X}_\infty$. As $\mathscr{O}_L[\Gamma]$ is dense in $\Lambda(\Gamma)$, and the latter is Hausdorff, this action extends by linearity and continuity to an action of $\Lambda(\Gamma)$ on $\mathscr{X}_\infty$. In exactly the same way we define actions of $\Lambda(\Gamma)$ on $\mathscr{Y}_\infty$ and of $\Lambda(\Gamma^+)$ on $\mathscr{X}_\infty^+$ and $\mathscr{Y}_\infty^+$.

13.3. ***The Main Conjecture.*** Recall the ideal $I(\Gamma^+)\zeta_p \subset \Lambda(\Gamma^+)$, and that this encodes the zeros of ζ_p. We already gave an arithmetic description of this ideal in Theorem 11.9 in terms of cyclotomic units. The Iwasawa Main Conjecture upgrades this to the following:

Theorem 13.8 (Iwasawa Main Conjecture). *$\mathscr{X}_\infty^+$ is a finitely generated torsion $\Lambda(\Gamma^+)$-module, and*

$$\mathrm{ch}_{\Lambda(\Gamma^+)}(\mathscr{X}_\infty^+) = I(\Gamma^+)\zeta_p.$$

Remark 13.9. It is usual in the literature to formulate the Iwasawa Main Conjecture in terms of an even Dirichlet character of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. As one can already observe from the behaviour of the Bernoulli numbers, there exists a certain dichotomy involving the parity of this character which makes the formulation of the Main Conjecture different in the even and odd cases. The above formulation takes into account every such even Dirichlet character. For a formulation of the Main Conjecture for odd Dirichlet characters, see [42].

13.4. ***The Iwasawa Main Conjecture for Vandiver primes.***

Definition 13.10. Let $h_n^+ := \#\mathrm{Cl}(F_n^+)$ be the class number of F_n^+. We say p is a *Vandiver prime* if $p \nmid h_1^+$.

The rest of these notes are dedicated to the following theorem of Iwasawa.

Theorem 13.11. *If p is a Vandiver prime, we have an isomorphism of $\Lambda(\Gamma^+)$-modules*

$$\mathscr{X}_\infty^+ \cong \Lambda(\Gamma^+)/I(\Gamma^+)\zeta_p.$$

In particular, Iwasawa's Main Conjecture holds.

The arguments of this section form the origins of Iwasawa's formulation of the Main Conjecture, and give further motivation for it. As our main goal is the study of p-adic L-functions, we omit the proofs of some more classical auxiliary results. Our approach follows that of [16, Section 4.5], which we suggest the reader consult for a more detailed exposition.

We first use class field theory to reinterpret Theorem 12.23 in terms of some modules arising from Galois theory.

Definition 13.12. For any $n \geq 1$, define $\mathscr{E}_n$ as the p-adic closure of the global units $\mathscr{V}_n = \mathscr{O}_{F_n}^\times$ inside the local units $\mathscr{U}_n$, let $\mathscr{E}_n^+ := \mathscr{E}_n \cap \mathscr{U}_n^+$, and let

$$\mathscr{E}_{n,1} := \mathscr{E}_n \cap \mathscr{U}_{n,1}, \qquad \mathscr{E}_{n,1}^+ := \mathscr{E}_n^+ \cap \mathscr{U}_{n,1},$$
$$\mathscr{E}_{\infty,1} := \varprojlim_{n \geq 1} \mathscr{E}_{n,1}, \qquad \mathscr{E}_{\infty,1}^+ := \varprojlim_{n \geq 1} \mathscr{E}_{n,1}^+.$$

Leopoldt's conjecture (which is known in this case by a theorem of Brumer) states that for any $n \geq 1$, the group $\mathscr{E}_n$ is a finite $\mathbb{Z}_p$-module of rank $r_1 + r_2 - 1 = p^{n-1}(p-1)/2$. Here as usual r_1 (resp. r_2) denotes the number of real (resp. half the number of complex) embeddings of F_n into $\mathbb{C}$. In light of Lemma 12.20, the conjecture says that if global units are (multiplicatively) independent over $\mathbb{Z}$, then they are independent over $\mathbb{Z}_p$.

Proposition 13.13. *There is an exact sequence of $\Lambda(\Gamma^+)$-modules*

$$0 \to \mathscr{E}_{\infty,1}^+ \to \mathscr{U}_{\infty,1}^+ \to \mathrm{Gal}(\mathscr{M}_\infty^+/\mathscr{L}_\infty^+) \to 0.$$

Proof. Global class field theory (see [81, Corollary 13.6]) gives a short exact sequence

$$0 \to \mathscr{E}_{n,1}^+ \to \mathscr{U}_{n,1}^+ \to \mathrm{Gal}(\mathscr{M}_n^+/\mathscr{L}_n^+) \to 0. \tag{13-1}$$

Taking the inverse limit over n gives the result. This is exact as all modules in the sequence above are finitely generated $\mathbb{Z}_p$-modules (so satisfy the Mittag-Leffler condition). □

We now rewrite the terms in this sequence, moving it closer to Theorem 13.11. Motivated by Theorem 11.9, we also introduce $\mathscr{C}_{\infty,1}^+$ into the picture. Then:

Corollary 13.14. *We have an exact sequence of $\Lambda(G)$-modules*

$$0 \to \mathscr{E}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ \to \mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ \to \mathscr{X}_\infty^+ \to \mathscr{Y}_\infty^+ \to 0.$$

Proof. The fundamental theorem of Galois theory yields a short exact sequence

$$0 \to \mathrm{Gal}(\mathscr{M}_\infty^+/\mathscr{L}_\infty^+) \to \mathscr{X}_\infty^+ \to \mathscr{Y}_\infty^+ \to 0.$$

The result now follows from Proposition 13.13, as

$$\mathrm{Gal}(\mathscr{M}_\infty^+/\mathscr{L}_\infty^+) \cong \mathscr{E}_{\infty,1}^+/\mathscr{U}_{\infty,1}^+ \cong (\mathscr{E}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+)/(\mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+),$$

the last identification being the third isomorphism theorem. □

Key to the proof of Theorem 13.11 is the following result from classical Iwasawa theory. For the sake of completeness we will give in Appendix A an introduction to this topic, including in particular a proof of the following result. Let

$$\mathscr{Y}_n^+ := \mathrm{Gal}(\mathscr{L}_n^+/F_n^+) \cong \mathrm{Cl}(F_n^+) \otimes_{\mathbb{Z}} \mathbb{Z}_p. \tag{13-2}$$

Proposition 13.15 [81, Proposition 13.22]. *For all $n \geq 0$, we have*

$$(\mathscr{Y}_\infty^+)_{\Gamma_n^+} = \mathscr{Y}_n^+,$$

where $\Gamma_n^+ = \mathrm{Gal}(F_\infty^+/F_n^+)$ and the left-hand side is the module of coinvariants.

Proof. See Proposition A.6. □

Corollary 13.16. *If p is a Vandiver prime, then*

(i) $\mathscr{Y}_\infty^+ = 0$;

(ii) $p \nmid h_n^+$ *for any* $n \geq 1$;

(iii) $\mathscr{E}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ = 0$.

Proof. By (13-2), we deduce that $p \nmid h_n^+$ if and only if $\mathscr{Y}_n^+ = 0$.

(i) By Proposition 13.15, if $p \nmid h_1^+$, then $0 = \mathscr{Y}_1^+ = (\mathscr{Y}_\infty^+)_{\Gamma_0} = 0$. By Nakayama's lemma, this implies that $\mathscr{Y}_\infty^+ = 0$.

(ii) Combining (i) with Proposition 13.15 shows $\mathscr{Y}_n^+ = 0$, hence the result.

(iii) In Theorem 11.7 we saw that $[\mathscr{V}_n^+ : \mathscr{D}_n^+] = h_n^+$, which is prime to p by (ii). We claim further that

$$[\mathscr{V}_{n,1}^+ : \mathscr{D}_{n,1}^+] \text{ is prime to } p. \tag{13-3}$$

Indeed, note $\mathscr{D}_{n,1}^+ = \mathscr{V}_{n,1}^+ \cap \mathscr{D}_n^+$ by definition; so applying the isomorphism theorem $S/(S \cap N) \cong SN/N \leq G/N$ to the subgroups $S = \mathscr{V}_{n,1}^+$ and $N = \mathscr{D}_n^+$ of $G = \mathscr{V}_n^+$, we see that $\mathscr{V}_{n,1}^+/\mathscr{D}_{n,1}^+$ is isomorphic to a subgroup of $\mathscr{V}_n^+/\mathscr{D}_n^+$, hence has order dividing h_n^+, which is prime to p. Hence there is an exact sequence

$$0 \to \mathscr{D}_{n,1}^+ \to \mathscr{V}_{n,1}^+ \to W_n \to 0,$$

where W_n is a finite group of order prime to p. We apply $-\otimes_{\mathbb{Z}} \mathbb{Z}_p$ to every term to get

$$\mathscr{D}_{n,1}^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathscr{V}_{n,1}^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Recall that $\mathscr{E}_{n,1}^+$ (resp. $\mathscr{C}_{n,1}^+$) is by definition the p-adic closure of $\mathscr{V}_{n,1}^+$ (resp. $\mathscr{D}_{n,1}^+$) inside $\mathscr{U}_{n,1}^+$, and that $\mathscr{C}_{n,1}^+ \subseteq \mathscr{E}_{n,1}^+$. By Lemma 12.20, we have natural surjections $\mathscr{D}_{n,1}^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathscr{C}_{n,1}^+$ and $\mathscr{V}_{n,1}^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathscr{E}_{n,1}^+$, making the diagram

$$\begin{array}{ccc} \mathscr{D}_{n,1}^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p & \xrightarrow{\sim} & \mathscr{V}_{n,1}^+ \otimes_{\mathbb{Z}} \mathbb{Z}_p \\ \downarrow & & \downarrow \\ \mathscr{C}_{n,1}^+ & \longrightarrow & \mathscr{E}_{n,1}^+ \end{array}$$

commute. Thus the inclusion $\mathscr{C}_{n,1}^+ \to \mathscr{E}_{n,1}^+$ is surjective, so an isomorphism. Taking inverse limits yields $\mathscr{C}_{\infty,1}^+ \cong \mathscr{E}_{\infty,1}^+$, which finishes the proof. □

We can now easily finish the proof of Iwasawa Main Conjecture for Vandiver primes.

Proof. By Corollaries 13.14 and 13.16 (i, iii) (for the first isomorphism) and Theorem 11.9 (for the second), we have

$$\mathscr{X}_\infty^+ \cong \mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ \cong \Lambda(\Gamma^+)/I(\Gamma^+)\zeta_p.$$

In particular,

$$\mathrm{ch}_{\Lambda(\Gamma^+)}(\mathscr{X}_\infty^+) = \mathrm{ch}_{\Lambda(\Gamma^+)}\big(\Lambda(\Gamma^+)/I(\Gamma^+)\zeta_p\big) = I(\Gamma^+)\zeta_p. \qquad \square$$

Remark 13.17. Conjecturally, every prime is a Vandiver prime, and under this conjecture we have proved the full Iwasawa Main Conjecture. The conditional proof above was due to Iwasawa himself. The first full proof of the Iwasawa Main Conjecture was given by Mazur–Wiles [61]. For a description of another proof, using Euler systems and due to Kolyvagin, Rubin, and Thaine, see [16] and [52].

13.5. ***Generalisations: Selmer groups, p-adic L-functions, Iwasawa–Greenberg Main Conjectures.*** Our focus throughout has been on Iwasawa's original Main Conjecture. We conclude with a sketch of a formulation due to Greenberg [36] of a Main Conjecture for more general Galois representations, which, for the trivial Galois representation, recovers Theorem 13.8. In order to do this, we first need to introduce Selmer groups. These are fundamental objects in arithmetic, lying at the core of two very important conjectures concerning L-functions: Iwasawa Main Conjectures and Bloch–Kato conjectures. The reader interested in this beautiful theory can learn more from [3; 36; 47; 67; 70; 75].

13.5.1. *Selmer groups over F_∞^+.* Selmer groups are objects that generalise one of the sides of the Iwasawa Main Conjecture. Let us start with a general definition. For compatibility with our earlier study, we will work over the field $F_\infty^+ = \mathbb{Q}(\mu_{p^\infty})^+$, which we denote by $\mathcal{F}$ (to ease notation). This differs from [36], in which the author works over the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ (see Remark 13.9). We continue to take coefficients in a fixed finite extension $L/\mathbb{Q}_p$.

Definition 13.18. (1) Let M be a topological $\mathcal{O}_L$-module equipped with a continuous $\mathcal{O}_L$-linear action of $\mathscr{G}_\mathcal{F}$, which is unramified outside a finite set of places.

(2) A *Selmer structure* $\mathcal{L} = (\mathcal{L}_v)_v$ for M over $\mathcal{F}$ is a choice of subspace $\mathcal{L}_v \subseteq H^1(\mathcal{F}_v, M)$ for every finite place v of $\mathcal{F}$ such that, for almost all v, we have $\mathcal{L}_v = H^1_{\mathrm{ur}}(\mathcal{F}_v, M)$.[15]

(3) Given a Selmer structure $\mathcal{L} = (\mathcal{L}_v)_v$ for M, we define the *Selmer group* to be

$$H^1_\mathcal{L}(\mathcal{F}, M) = \ker\left(H^1(\mathcal{F}, M) \to \bigoplus_v H^1(\mathcal{F}_v, M)/\mathcal{L}_v\right),$$

where v runs over every finite place of $\mathcal{F}$.

[15] Here, the *unramified cohomology groups* are defined as $H^1_{\mathrm{ur}}(\mathcal{F}_v, M) := \ker\big(H^1(\mathcal{F}_v, M) \to H^1(I_{\mathcal{F}_v}, M)\big)$, where $I_{\mathcal{F}_v}$ denotes the inertia group of $\mathcal{F}_v$ and the map is restriction.

In what follows, we will only be interested in Selmer structures with unramified local conditions for all places v not dividing p. Let T be a finite free $\mathbb{Z}_p$-module equipped with an action of $\mathscr{G}_{\mathbb{Q}}$. We let $V := T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $W := V/T$, which is a finite free $\mathbb{Q}_p/\mathbb{Z}_p$-representation of $\mathscr{G}_{\mathbb{Q}}$. We will assume that V is one of the representations that appeared in Section 2.1, i.e., a Galois representation attached to some arithmetic object, and take $M = W$.

Given the general definition of a Selmer structure and Selmer group, the next step is to give reasonable subspaces $\mathcal{L}_v$ for $v \in \Sigma$. There are two main approaches to this.

Definition 13.19. (1) (Greenberg's approach) To define interesting Selmer structures at p, Greenberg's approach assumes that the representation V is p-ordinary, in the sense that there exists a saturated, finite, $\mathscr{G}_{\mathbb{Q}}$-invariant filtration Fil^i of V such that the inertia group $I_{\mathbb{Q}_p}$ of $\mathscr{G}_{\mathbb{Q}_p}$ acts on the i-th graded piece $\mathrm{Fil}^i/\mathrm{Fil}^{i+1}$ as the i-th power of the cyclotomic character (from (9-1)). Let $\mathcal{F} = \mathbb{Q}(\mu_{p^\infty})^+$ as before and let v_p be the unique place of $\mathcal{F}$ above p. Then one defines

$$\mathcal{L}_{v_p}^{\mathrm{Gr}} := \ker\big(H^1(\mathcal{F}_{v_p}, W) \to H^1(I_{v_p}, W) \to H^1(I_{v_p}, W/\mathrm{Fil}^1 W)\big),$$

where $\mathrm{Fil}^1 W$ denotes the image of $\mathrm{Fil}^1 V$ under the natural map $V \to W$.

(2) (Bloch–Kato's approach) This approach uses technology coming from p-adic Hodge theory (see, e.g., [6; 7]), and we only mention it here for the sake of completeness. Letting V be as before, we define

$$H_f^1(\mathcal{F}_{v_p}, V) := \ker\big(H^1(\mathcal{F}_{v_p}, V) \to H^1(\mathcal{F}_{v_p}, V \otimes \boldsymbol{B}_{\mathrm{cris}})\big),$$

where $\boldsymbol{B}_{\mathrm{cris}}$ denotes Fontaine's ring of crystalline periods. Then one defines

$$\mathcal{L}_{v_p}^{\mathrm{BK}} := \mathrm{Im}\big(H_f^1(\mathcal{F}_{v_p}, V) \to H^1(\mathcal{F}_{v_p}, W)\big),$$

where the map is induced by the natural map $V \to W$.

Remark 13.20. Greenberg Selmer groups and Bloch–Kato Selmer groups coincide in some fundamental examples. For a general relation between them, we refer the reader to [47] and [67, Section 2.4.7].

13.5.2. *The module $\mathscr{X}_\infty^+$ via Selmer groups.* We now reinterpret the space $\mathscr{X}_\infty^+$ appearing in Theorem 13.8 in terms of a Greenberg Selmer group. We follow [36, Section 1]. Recall $F_\infty = \mathbb{Q}(\mu_{p^\infty})$ and the cyclotomic character $\chi : \mathrm{Gal}(F_\infty/\mathbb{Q}) \to \mathbb{Z}_p^\times$. Note that $\mathrm{Gal}(F_\infty/\mathbb{Q})$ is the quotient of $\mathscr{G}_{\mathbb{Q}}$ by $\mathscr{G}_{F_\infty}$, so that we may consider χ as a character of $\mathscr{G}_{\mathbb{Q}}$ that is trivial on $\mathscr{G}_{F_\infty}$. For $n \in \mathbb{Z}$, we consider the representation $T_n := \mathbb{Z}_p(n)$, that is, the space $\mathbb{Z}_p$ upon which $\mathscr{G}_{\mathbb{Q}}$ acts by χ^n (see Definition 12.16). Let $V_n := \mathbb{Q}_p(n)$ and $W_n := V_n/T_n = (\mathbb{Q}_p/\mathbb{Z}_p)(n)$.

By the above remark, $\mathscr{G}_{F_\infty}$ acts trivially on W_n, and we thus have

$$H^1(F_\infty, W_n) = \mathrm{Hom}_{\mathrm{cts}}(\mathscr{G}_{F_\infty}, W_n).$$

As $\mathrm{Gal}(F_\infty/F_\infty^+) = \{1, c\} \cong \{\pm 1\}$ (with the nontrivial element given by complex conjugation) and p is odd, the inflation-restriction sequence gives

$$H^1(\mathcal{F}, W_n) = H^1(\mathcal{G}_{F_\infty}, W_n)^{\{\pm 1\}} = \mathrm{Hom}_{\mathrm{cts},\{\pm 1\}}(\mathcal{G}_{F_\infty}, W_n),$$

recalling $\mathcal{F} = F_\infty^+$ and where the subscript $\{\pm 1\}$ denotes homomorphisms equivariant for $\mathrm{Gal}(F_\infty/F_\infty^+)$, acting on $\mathcal{G}_{F_\infty}$ as in Remark 13.7. We can thus describe the Greenberg Selmer group over $\mathcal{F}$ in the simpler language of group homomorphisms, rather than Galois cohomology classes.

We can refine this via local/global conditions. To do so, let $\sigma \in H^1(\mathcal{F}, W_n)$. Then:

(1) As W_n is abelian and p-power torsion, we find

$$H^1(\mathcal{F}, W_n) = \mathrm{Hom}_{\mathrm{cts},\{\pm 1\}}(\mathrm{Gal}(F_\infty^{\mathrm{ab,pro}-p}/F_\infty), W_n),$$

where $F_\infty^{\mathrm{ab,pro}-p}$ is the maximal abelian pro-p extension of F_∞.

(2) Finite primes away from p: Since the local condition at finite places $v \nmid p$ is the unramified condition, we deduce that σ is unramified at all $v \nmid p$. Then σ descends to a homomorphism on $\mathscr{X}_\infty = \mathrm{Gal}(\mathscr{M}_\infty/F_\infty)$, for $\mathscr{M}_\infty$ the maximal abelian pro-p extension of F_∞ unramified outside $\mathfrak{p}$ as in Section 13.2.

(3) The prime above p: At p, we have $\mathcal{F}_{v_p} = K_\infty^+ = \mathbb{Q}_p(\mu_{p^\infty})^+$. The filtration required by Greenberg is given by

$$\mathrm{Fil}^i \mathbb{Q}_p(n) = \begin{cases} \mathbb{Q}_p(n) & \text{if } i \le n, \\ 0 & \text{if } i > n. \end{cases}$$

From the definition, we see that

$$\mathcal{L}_{v_p}^{\mathrm{Gr}} = \begin{cases} H^1(K_\infty^+, W_n) & \text{if } n \ge 1, \\ H^1_{\mathrm{ur}}(K_\infty^+, W_n) & \text{if } n \le 0. \end{cases}$$

Thus if $n \ge 1$, the local condition at p is empty, while for $n \ge 0$ the local condition at p means σ is also unramified at p, so it descends further to $\mathscr{Y}_\infty = \mathrm{Gal}(\mathscr{L}_\infty/F_\infty)$ (for notation as in Section 13.2). We conclude that

$$H^1_{\mathcal{L}^{\mathrm{Gr}}}(F_\infty, W_n) = \begin{cases} \mathrm{Hom}_{\mathrm{cts},\{\pm 1\}}(\mathscr{X}_\infty, W_n) & \text{if } n \ge 1, \\ \mathrm{Hom}_{\mathrm{cts},\{\pm 1\}}(\mathscr{Y}_\infty, W_n) & \text{if } n \le 0. \end{cases}$$

(4) Equivariance for $\{\pm 1\}$: As p is odd, the action of $\mathrm{Gal}(F_\infty/F_\infty^+) = \{1, c\}$ yields a decomposition $\mathscr{X}_\infty = (\mathscr{X}_\infty)^{c=1} \oplus (\mathscr{X}_\infty)^{c=-1}$. There is a similar decomposition for $\mathscr{Y}_\infty$. Note also that c acts on W_n as $(-1)^n$. We see that if $n > 0$, we have

$$H^1_{\mathcal{L}^{\mathrm{Gr}}}(F_\infty, W_n) = \mathrm{Hom}_{\mathrm{cts}}((\mathscr{X}_\infty)^{c=(-1)^n}, W_n),$$

that is, we see the dual of $(\mathscr{X}_\infty)^{c=1}$ for even $n>0$, and of $(\mathscr{X}_\infty)^{c=-1}$ for odd $n>0$. Similarly for $n\leq 0$ we have

$$H^1_{\mathcal{L}^{\mathrm{Gr}}}(F_\infty, W_n) = \mathrm{Hom}_{\mathrm{cts}}((\mathscr{Y}_\infty)^{c=(-1)^n}, W_n).$$

As in [16, p. 6], the natural surjection $\mathscr{X}_\infty \to \mathscr{X}_\infty^+ = \mathrm{Gal}(\mathscr{M}_\infty^+/F_\infty^+)$ induces an isomorphism $(\mathscr{X}_\infty)^{c=1} \cong \mathscr{X}_\infty^+$ (and similarly $(\mathscr{Y}_\infty)^{c=1} \cong \mathscr{Y}_\infty^+$). Combining all of the above, we conclude that for even positive n, we have

$$H^1_{\mathcal{L}^{\mathrm{Gr}}}(F_\infty, W_n) = \mathrm{Hom}_{\mathrm{cts}}(\mathscr{X}_\infty^+, W_n),$$

(a twist of) the Pontryagin dual of the module $\mathscr{X}_\infty^+$ appearing in Theorem 13.8.

13.5.3. *The Iwasawa–Greenberg Main Conjecture.* Let T, V and W be representations as in Section 13.5.1. We also let $V^\vee = \mathrm{Hom}_{\mathrm{cts}}(V, \mathbb{Q}_p(1))$ be the Tate dual of V. In particular V is ordinary at p. Inspired by the Iwasawa Main Conjecture and by an analogous conjecture of Mazur for ordinary elliptic curves, Greenberg [36] described a Main Conjecture for V, which we now state.

Attached to V is an L-function $L(V,s)$, and an Euler factor at infinity $L_\infty(V,s)$ (called the gamma factor in [36]). This involves a product of certain translates of the usual gamma function $\Gamma(s)$ and has no zeros. We let r_V denote the order of the pole of $L_\infty(V,s)$ at $s=1$. For example, if $V=\mathbb{Q}_p(n)$, then $L(V,s)=\zeta(s-n)$ and $L_\infty(V,s)=\pi^{-(s-n)/2}\Gamma((s-n)/2)$. The poles of the last function are $s=n, n-2, n-4, \ldots$.

Coates–Perrin-Riou conjectured in [15] that there should exist a p-adic L-function for V, which in this context lies in the field of fractions of $\Lambda(\Gamma^+)$. We comment more on this conjecture in Section B.3.

Conjecture 13.21 (Greenberg). *The following assertions hold.*

(i) $H^1_{\mathcal{L}^{\mathrm{Gr}}}(\mathcal{F}, W)$ *has* $\Lambda(\Gamma^+)$*-corank equal to* r_V.

(ii) *If* $r_V = r_{V^\vee} = 0$, *then the characteristic ideal of the Pontryagin dual of* $H^1_{\mathcal{L}^{\mathrm{Gr}}}(\mathcal{F}, W)$ (*as a* $\Lambda(\Gamma^+)$*-module*) *coincides with the ideal generated by the p-adic L-function of* V.

Example 13.22. Suppose $n>0$ is even; then above we showed $H^1_{\mathcal{L}}(\mathcal{F}, W_n) = \mathrm{Hom}_{\mathrm{cts}}(\mathscr{X}_\infty^+, W_n)$. This has Pontryagin dual $\mathscr{X}_\infty^+(-n)$, the space $\mathscr{X}_\infty^+$ with $\Lambda(\Gamma^+)$-action twisted by χ^{-n}. In this case, the p-adic L-function in Greenberg's conjecture is $\partial^n\zeta_p$, the n-th twist of Kubota–Leopoldt, so we see that Greenberg's conjecture is essentially a (twist of) Theorem 13.8.

Remark 13.23. We described Theorem 13.8 as "the Main Conjecture for $V=\mathbb{Q}_p$". Although they are equivalent, strictly speaking, the case $n=0$ doesn't fit into Greenberg's picture. Indeed, the underlying assumption does not hold: here $\mathbb{Q}_p^\vee = \mathbb{Q}_p(1)$, so $L_\infty(\mathbb{Q}_p^\vee, s) = L_\infty(\mathbb{Q}_p, 1-s)$, hence $r_{\mathbb{Q}_p^\vee}=1$. In Greenberg's terminology,

$L(\mathbb{Q}_p(n), 1) = \zeta(1-n)$ and $L(\mathbb{Q}_p(n)^\vee, 1) = \zeta(n)$ are both critical only when n is even and (strictly) positive, or n is odd and negative, so the case $n = 0$ is not covered.

Remark 13.24. There exist more general, even noncommutative, statements of the Main conjecture. We refer the interested reader to [46] and [33].

Appendix A: Iwasawa's μ-invariant

We end these notes by giving a flavour of further topics in classical Iwasawa theory, introducing the μ- and λ-invariants of a $\mathbb{Z}_p$-extension. In proving Iwasawa's theorem on the μ- and λ-invariants, we develop techniques that can be used to show that the modules appearing in the exact sequence of Corollary 13.14 are finitely generated torsion modules over the Iwasawa algebra, a part of the general Iwasawa Main Conjecture (beyond the Vandiver case that we have already proved).

The following results will hold for an arbitrary $\mathbb{Z}_p$-extension of number fields, although we will only prove them under some hypotheses that slightly simplify the proofs.

Definition A.1. Let F be a number field. A $\mathbb{Z}_p$-extension F_∞ of F is a Galois extension such that $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$. If F_∞/F is a $\mathbb{Z}_p$-extension, we denote by F_n the subextension such that $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$.

Recall first that any number field has at least one $\mathbb{Z}_p$-extension, the *cyclotomic $\mathbb{Z}_p$-extension*. Indeed, by Galois theory, $\mathrm{Gal}(F(\mu_{p^\infty})/F)$ is an open subgroup of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$, and hence contains a maximal quotient isomorphic to $\mathbb{Z}_p$ (specifically, the quotient by the finite torsion subgroup μ_{p-1}). The corresponding field (under the fundamental theorem of Galois theory) is the cyclotomic $\mathbb{Z}_p$-extension.

Example A.2. Let $F = \mathbb{Q}(\mu_p)$. Then $F_\infty = \mathbb{Q}(\mu_{p^\infty})$ is the cyclotomic $\mathbb{Z}_p$-extension of F, and

$$F_n = \mathbb{Q}(\mu_{p^{n+1}}),$$

noting that earlier we denoted this field by F_{n+1}. The cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is the field $(F_\infty)^{\mu_{p-1}}$ in F_∞ fixed by the torsion subgroup $\mu_{p-1} \subset \mathrm{Gal}(F_\infty/\mathbb{Q})$.

Leopoldt's conjecture states that the number of independent $\mathbb{Z}_p$-extensions of a number field F is exactly r_2+1, where r_2 is the number of complex embeddings of F. In particular, the conjecture predicts that any totally real number field possesses a unique $\mathbb{Z}_p$-extension (the cyclotomic one). Whilst the conjecture remains open for general number fields, it is known in the case that F is an abelian extension of $\mathbb{Q}$ or an abelian extension of an imaginary quadratic field (see [65, Theorem 10.3.16]).

A.1. ***Iwasawa's theorem.*** Let F be a number field and F_∞/F a $\mathbb{Z}_p$-extension, let $\Gamma = \Gamma_F = \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$, and let γ_0 be a topological generator of Γ_F. Using this

choice of γ_0, we identify $\Lambda(\Gamma)$ with $\Lambda := \mathbb{Z}_p[\![T]\!]$ by sending γ_0 to $T+1$ (when γ_0 is sent to 1 by the isomorphism $\Gamma \cong \mathbb{Z}_p$, this is simply the Mahler transform, but this identification holds for any γ_0). Let $\mathscr{L}_n$ (resp. $\mathscr{L}_\infty$) be the maximal unramified abelian p-extension of F_n (resp. pro-p extension of F_∞), and write

$$\mathscr{Y}_{F,n} = \mathscr{Y}_n := \mathrm{Gal}(\mathscr{L}_n/F_n) = \mathrm{Cl}(F_n) \otimes \mathbb{Z}_p,$$

which is the p-Sylow subgroup of the ideal class group of F_n. Set

$$\mathscr{Y}_\infty = \mathscr{Y}_{F,\infty} := \varprojlim_n \mathscr{Y}_{F,n}.$$

Write $e_n = v_p(\#\mathscr{Y}_n)$ for the exponent of p in the class number of F_n. The following theorem is the main result we intend to show in this section.

Theorem A.3 (Iwasawa). *There exist integers* $\lambda \geq 0,\ \mu \geq 0,\ \nu \geq 0$, *and an integer* n_0, *such that, for all* $n \geq n_0$,

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

Remark A.4. (1) This is yet another typical example of the power of Iwasawa theory, in which we derive information at finite levels by considering all levels simultaneously.

There are two basic steps in the proof of Theorem A.3. We first show that the module $\mathscr{Y}_{F,\infty}$ is a finitely generated torsion $\Lambda(\Gamma)$-module. Using the structure theorem of $\Lambda(\Gamma)$-modules (Theorem 13.1), we study the situation at infinite level, and then we transfer the result back to finite level to get the result.

(2) We will only describe the proof for the case where the extension F_∞/F satisfies the following hypothesis: there is only one prime $\mathfrak{p}$ of F above p, and it ramifies completely in F_∞. The reduction of the general case to this case is not difficult, and is contained in [81, Section 13]. This assumption covers our cases of interest; in particular, it applies if $F = \mathbb{Q}(\mu_{p^m})$ or $F = \mathbb{Q}(\mu_{p^m})^+$ for some $m \geq 0$ and F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension.

A.1.1. *First step.* The first step of the proof of Theorem A.3 consists in showing (Proposition A.8) that the module $\mathscr{Y}_\infty$ is a finitely generated $\Lambda(\Gamma)$-module. Then Proposition A.6 will allow us to recover each $\mathscr{Y}_n$ from the whole tower $\mathscr{Y}_\infty$. We then use a variation of Nakayama's lemma to conclude.

Since $\mathfrak{p}$ is totally ramified in F_∞, and $\mathscr{L}_n$ is unramified over F_n, we deduce that $F_{n+1} \cap \mathscr{L}_n = F_n$ and hence

$$\mathscr{Y}_n = \mathrm{Gal}(\mathscr{L}_n/F_n) = \mathrm{Gal}(\mathscr{L}_n F_{n+1}/F_{n+1}) = \mathscr{Y}_{n+1}/\mathrm{Gal}(\mathscr{L}_{n+1}/\mathscr{L}_n F_{n+1}),$$

showing that $\mathscr{Y}_{n+1}$ surjects onto $\mathscr{Y}_n$. The module $\mathscr{Y}_\infty$ carries the natural Galois action of $\Lambda = \Lambda(\Gamma)$, and under the identification $\Lambda \cong \mathbb{Z}_p[\![T]\!]$, the polynomial $1+T \in \Lambda$ acts as $\gamma_0 \in \Gamma$.

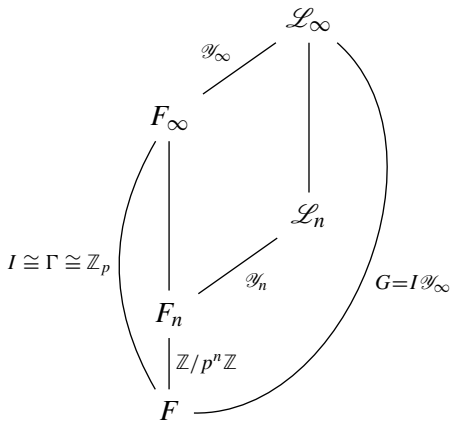
Let $\widetilde{\mathfrak{p}}$ be a prime of $\mathscr{L}_\infty$ above $\mathfrak{p}$, and write

$$I \subseteq G := \mathrm{Gal}(\mathscr{L}_\infty/F)$$

for its inertia group. Since $\mathscr{L}_\infty/F_\infty$ is unramified, all of the inertia occurs in the subextension F_∞/F. Accordingly $I \cap \mathscr{Y}_\infty = 1$ and since F_∞/F is totally ramified at $\mathfrak{p}$, the inclusion $I \hookrightarrow G/\mathscr{Y}_\infty \cong \Gamma$ is surjective, and hence bijective. We deduce that

$$G = I\mathscr{Y}_\infty = \Gamma\mathscr{Y}_\infty.$$

We've shown the following picture of extensions:



Let $\sigma \in I$ map to the topological generator $\gamma_0 \in \Gamma$ under the natural isomorphism $I \cong \Gamma$.

Proposition A.5. *Let G' be the closure of the commutator of G. Then*

$$G' = (\gamma_0 - 1) \cdot \mathscr{Y}_\infty = T\mathscr{Y}_\infty.$$

Proof. Recall that we have a decomposition $G = \Gamma\mathscr{Y}_\infty$. Let $a = \alpha x$, $b = \beta y \in G$, where $\alpha, \beta \in \Gamma$ and $x, y \in \mathscr{Y}_\infty$. Using the definition of the $\Lambda(\Gamma)$ structure of $\mathscr{Y}_\infty$, and the fact that Γ and $\mathscr{Y}_\infty$ are abelian, we get that

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= (\alpha x \alpha^{-1})(\alpha\beta y \beta^{-1}\alpha^{-1})(\alpha\beta x^{-1}\beta^{-1}\alpha^{-1})(\beta y^{-1}\beta^{-1}) \\ &= (x^\alpha)^{1-\beta}(y^\beta)^{\alpha-1}. \end{aligned}$$

Setting $\beta = 1$ and $\alpha = \gamma_0$, we deduce that $(\gamma_0 - 1)\mathscr{Y}_\infty \subseteq G'$. To see the other inclusion, write $\beta = \gamma_0^c$, where $c \in \mathbb{Z}_p$, so that $1 - \beta = -\sum_{n=1}^{+\infty} \binom{c}{n}(\gamma_0 - 1)^n = -\sum_{n=1}^{+\infty} \binom{c}{n} T^n \in T\Lambda$ and similarly for $\alpha - 1$, which allows us to conclude. □

Recall that the n-th power of the Frobenius operator on $\mathbb{Z}_p[\![T]\!]$ is given by $\varphi^n(T) = (1+T)^{p^n} - 1$. Let $\varphi^0(T) = T$.

Proposition A.6. *We have $\mathscr{Y}_n = \mathscr{Y}_\infty/\varphi^n(T)$.*

Proof. We treat first the case $n = 0$. Since $\mathscr{L}_0$ is the maximal unramified abelian p-extension of F and $\mathscr{L}_\infty/F$ is a p-extension, $\mathscr{L}_0/F$ is the maximal unramified abelian subextension of $\mathscr{L}_\infty$. In particular, $\mathscr{Y}_0 = \mathrm{Gal}(\mathscr{L}_0/F)$ is the quotient of G by the subgroup generated by the commutator G' and by the inertia group I of $\mathfrak{p}$. By the above lemma and the decomposition $G = I\mathscr{Y}_\infty$, we conclude that

$$\mathscr{Y}_0 = G/\langle G', I\rangle = \mathscr{Y}_\infty I/\langle(\gamma_0 - 1)\mathscr{Y}_\infty, I\rangle = \mathscr{Y}_\infty/(\gamma_0 - 1)\mathscr{Y}_\infty = \mathscr{Y}_\infty/T\mathscr{Y}_\infty.$$

For $n \geq 1$, we apply the arguments of the last paragraph, replacing F by F_n and γ_0 by $\gamma_0^{p^n}$, so that σ_0 becomes $\sigma_0^{p^n}$ and $(\gamma_0 - 1)\mathscr{Y}_\infty$ becomes

$$(\gamma_0^{p^n} - 1)\mathscr{Y}_\infty = ((1+T)^{p^n} - 1)\mathscr{Y}_\infty = \varphi^n(T)\mathscr{Y}_\infty,$$

which gives the result. □

We state next a variation of Nakayama's lemma for testing when a Λ-module is finitely generated, whose standard proof is left as an exercise.

Lemma A.7 (Nakayama's lemma; [81, Lemma 13.16]). *Let $\mathscr{Y}$ be a compact Λ-module. Then $\mathscr{Y}$ is finitely generated over Λ if and only if $\mathscr{Y}/(p, T)\mathscr{Y}$ is finite. Moreover, if the image of $x_1, \ldots, x_m$ generates $\mathscr{Y}/(p, T)\mathscr{Y}$ over $\mathbb{Z}$, then $x_1, \ldots, x_n$ generate $\mathscr{Y}$ as a Λ-module. In particular, if $\mathscr{Y}/(p, T)\mathscr{Y} = 0$, then $\mathscr{Y} = 0$.*

Applying this in our particular situation we obtain the following result.

Proposition A.8. *$\mathscr{Y}_\infty$ is a finitely generated Λ-module.*

Proof. Since

$$\varphi(T) = (1+T)^p - 1 = \sum_{k=1}^{p} \binom{p}{k} T^k \in (p, T),$$

the module $\mathscr{Y}_\infty/(p, T)\mathscr{Y}_\infty$ is a quotient of $\mathscr{Y}_\infty/\varphi(T)\mathscr{Y}_\infty = \mathscr{Y}_1 = \mathrm{Cl}(F_1) \otimes \mathbb{Z}_p$, the p-Sylow subgroup of $\mathrm{Cl}(F_1)$, which is finite. Therefore, applying Lemma A.7, we conclude that $\mathscr{Y}_\infty$ is a finitely generated Λ-module, as desired. □

A.1.2. *Second step.* Once we know that the module $\mathscr{Y}_\infty$ is a finitely generated Λ-module, we can invoke the structure theorem for these modules (Theorem 13.1) to get an exact sequence

$$0 \to Q \to \mathscr{Y}_\infty \to \mathscr{A} \to R \to 0,$$

where Q and R are finite modules and where

$$\mathscr{A} = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{k_j}) \right),$$

for some integers $s, r, t \geq 0$, $m_i, k_j \geq 1$ and some distinguished polynomials $f_j(T) \in \Lambda$.

Recall that we want to calculate the size of $\mathscr{Y}_n = \mathscr{Y}_\infty/\varphi^n(T)$. The following lemma reduces the problem to calculating the size of $\mathscr{A}/\varphi^n(T)$.

Lemma A.9. *There exists a constant c and an integer n_0 such that, for all $n \geq n_0$,*

$$|\mathscr{Y}_\infty/\varphi^n(T)| = p^c|\mathscr{A}/\varphi^n(T)|.$$

Proof. The full proof of this lemma is given in [80, Lemma 13.21]; we give a sketch.

Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \varphi^n(T)\mathscr{Y}_\infty & \longrightarrow & \mathscr{Y}_\infty & \longrightarrow & \mathscr{Y}_\infty/\varphi^n(T)\mathscr{Y}_\infty & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \varphi^n(T)\mathscr{A} & \longrightarrow & \mathscr{A} & \longrightarrow & \mathscr{A}/\varphi^n(T)\mathscr{A} & \longrightarrow & 0 \end{array}$$

By hypothesis, the kernel and cokernel of the middle vertical map are bounded. By elementary calculations and diagram chasing, one ends up showing that the kernel and the cokernel of the third vertical arrow stabilise for n large enough, which is what is needed to conclude the proof. □

We now proceed to calculate the size of the module $\mathscr{A}$.

Proposition A.10. *Let*

$$\mathscr{A} = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{k_j})\right),$$

for some integers $s, r, t \geq 0$ and $m_i, k_j \geq 1$ and some distinguished polynomials $f_j(T) \in \Lambda$, and write $m = \sum m_i$, $\ell = \sum k_j \deg(f_j)$. Suppose $\mathscr{A}/\varphi^n(T)\mathscr{A}$ is finite for all $n \geq 0$. Then $r = 0$ and there exist constants n_0 and c such that, for all $n \geq n_0$,

$$|\mathscr{A}/\varphi^n(T)| = p^{mp^n + \ell n + c}.$$

Proof. Step 1: First we show $r = 0$. Note that

$$\varphi^n(T) = (1+T)^{p^n} - 1 = T^{p^n} + \sum_{k=1}^{p^n-1} \binom{p^n}{k} T^k$$

is distinguished. We may therefore apply the division algorithm from Weierstrass preparation (a p-adic analytic analogue of Euclid's algorithm; see [10, Section 5.2.1]). This implies that any $f \in \mathbb{Z}_p[\![T]\!]$ can be written uniquely as $f(T) = q(T)\cdot((1+T)^{p^n}-1)+r(T)$, where $r(T)$ is a polynomial of degree $\leq p^n - 1$. We see

$$\Lambda/\varphi^n(T) = \mathbb{Z}_p[\![T]\!]/((1+T)^{p^n} - 1) \cong \{r(T) \in \mathbb{Z}_p[T] : \deg(r) \leq p^n - 1\} \quad \text{(A-1)}$$

is infinite. Since $\mathscr{A}/\varphi^n(T)$ is assumed to be finite, we deduce that $r = 0$.

Step 2: We now deal with the second summand. By (A-1), for any $k \geq 0$ we see that $\Lambda/(p^k, \varphi^n(T))$ is the space of polynomials over $\mathbb{Z}/p^k\mathbb{Z}$ of degree at most $p^n - 1$, whence

$$|\Lambda/(p^k, \varphi^n(T))| = p^{kp^n}.$$

We deduce from this that

$$\left| \left(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \right) \Big/ \varphi^n(T) \right| = p^{mp^n},$$

where $m = \sum_i m_i$.

Step 3: Finally, we deal with the last (and most involved) summand. Let $g(T) \in \mathbb{Z}_p[T]$ be a distinguished polynomial of degree d (that we don't assume is irreducible, as we want this to apply to $g = f_j^{k_j}$). Letting $V = \Lambda/(g(T))$, we want to compute the order of

$$V/\varphi^n(T) = \Lambda/(g, \varphi^n(T)).$$

We will show inductively that for sufficiently large n, $|V/\varphi^{n+1}(T)| = p^d |V/\varphi^n(T)|$.

As g is distinguished, $T^d \equiv p \cdot (\text{poly}) \pmod{g}$, where (poly) denotes some polynomial in $\mathbb{Z}_p[T]$. Further, $T^k \equiv p \cdot (\text{poly}) \pmod{g}$ for all $k \geq d$. Let n_0 be such that $p^{n_0} \geq d$. We will use the following lemma.

Lemma A.11. *For any $n > n_0$, we have*

$$\varphi^{n+1}(T) \cdot V = p\varphi^n(T) \cdot V.$$

Proof. First take $k \geq n_0$, allowing $k = n_0$. As $\varphi^k(T)$ is distinguished, we see that

$$\varphi^k(T) = T^{p^k} + p\,(\text{poly}) \equiv p \cdot (\text{poly}) \pmod{g},$$

as $p^k \geq d$. Write $\varphi^k(T) = pQ_k(T) \pmod{g}$, for $Q_k(T) \in \mathbb{Z}_p[T]$.

We use the identity

$$(X^{p^{k+1}} - 1) = (X^{p^k} - 1) \cdot (X^{p^k(p-1)} + X^{p^k(p-2)} + \cdots + X^{p^k} + 1).$$

Applying with $X = 1 + T$ yields

$$\begin{aligned}
&\varphi^{k+1}(T) \\
&\quad = (1+T)^{p^{k+1}} - 1 \\
&\quad = ((1+T)^{p^k} - 1) \cdot \left((1+T)^{p^k(p-1)} + \cdots + (1+T)^{p^k} + 1\right) \\
&\quad = \varphi^k(T) \cdot \left((\varphi^{p^k}(T) + 1)^{p-1} + \cdots + (\varphi^k(T) + 1) + 1\right) \\
&\quad \equiv \varphi^{p^k}(T) \cdot \left((pQ_k(T) + 1)^{p-1} + \cdots + (pQ_k(T) + 1) + 1\right) \pmod{g}. \qquad \text{(A-2)}
\end{aligned}$$

Expanding the binomials, every term is divisible by p except the constant term 1 in each expression; but these sum to p. In particular, we deduce

$$\varphi^{k+1}(T) \equiv p\varphi^k(T) \pmod{g}.$$

Applying this with $k = n_0$, we see that

$$pQ_{n_0+1}(T) \equiv \varphi^{n_0+1}(T) \equiv p\varphi^{n_0}(T) \equiv p^2 Q_n(T) \pmod{g},$$

so $Q_{n_0+1}(T) \equiv 0 \pmod{p}$. Inductively we see $Q_n(T) \equiv 0 \pmod{p}$ for all $n > n_0$.

Returning to the last line of (A-2), now take $k = n > n_0$. As $Q_n(T) = 0 \pmod{p}$, every term in each binomial expansion is now divisible by p^2, again except the constant terms, which sum to p. In particular, we deduce

$$\begin{aligned}\varphi^{n+1}(T) &\equiv \varphi^n(T) \cdot (p^2 \cdot (\text{poly}) + p) \\ &\equiv p\varphi^n(T) \cdot (p \cdot (\text{poly}) + 1) \pmod{g}.\end{aligned}$$

The term $p \cdot (\text{poly}) + 1$ is a unit in Λ, so its reduction is a unit in $V = \Lambda/(g)$. We find

$$\varphi^{n+1}(T) \pmod{g} \in p\varphi^n(T) \cdot V^\times,$$

from which $\varphi^{n+1}(T) \cdot V = p\varphi^n(T) \cdot V$, completing the proof of the lemma. □

We now go back to the proof of the proposition. For any $n > n_0$, Lemma A.11 implies that $\varphi^{n+1}(T)V \subset pV$, and

$$|V/\varphi^{n+1}(T)V| = |V/pV| \cdot |pV/\varphi^{n+1}(T)V| = |V/pV| \cdot |pV/p\varphi^n(T)V|.$$

Since $g(T)$ is distinguished of degree d, we have

$$|V/pV| = |\Lambda/(p, g(T))| = |\Lambda/(p, T^d)| = p^d.$$

Finally, we compute $|pV/p\varphi^{n+1}(T)V|$. Since $(g(T), p) = 1$, multiplication by p is injective on V and hence

$$|pV/p\varphi^{n+1}(T)V| = |V/\varphi^{n+1}(T)V|.$$

Recall that n_0 is fixed with $p^{n_0} \geq d$. Inducting on Lemma A.11, we find that, for any $n > n_0$, we have

$$\varphi^{n+1}(T)V = p^{n-n_0-1}\varphi^{n_0+1}(T)V.$$

Again by Weierstrass division, we know V is isomorphic to polynomials in $\mathbb{Z}_p[T]$ of degree $\leq d-1$. This means

$$|V/\varphi^{n+1}(T)V| = p^{d(n-n_0-1)}|V/\varphi^{n_0+1}(T)V|.$$

Putting everything together, we deduce that

$$|V/\varphi^n(T)V| = p^{nd+c},$$

for some constant c and all $n > n_0$. Applying this to the third summand of $\mathscr{A}$, we get

$$\left| \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{k_j}) \right) \Big/ \varphi^n(T) \right| = p^{\ell n + c},$$

for $n \geq n_0$, where n_0 is such that $p^{n_0} \geq k_j \deg(f_j)$ for all j, $\ell = \sum_j k_j \deg(f_j)$, and c is a constant. This finishes the proof of the proposition. □

Along the way, we have proven the following fact.

Corollary A.12. *Let $\mathscr{Y}$ be a finitely generated Λ-module. If $\mathscr{Y}/\varphi^n(T)\mathscr{Y}$ is finite for all n, then $\mathscr{Y}$ is torsion.*

Proof. If $\mathscr{A}$ is as in the statement of Proposition A.10, then we showed that $r = 0$ in the structure theorem for $\mathscr{Y}$. This implies that $\mathscr{A}$ is torsion; each element is annihilated by the characteristic ideal of $\mathscr{A}$. If $\mathscr{Y}$ is any finitely generated Λ-module, then $\mathscr{Y}$ is quasi-isomorphic to a module $\mathscr{A}$ as before, and as $\mathscr{A}$ is torsion, so is $\mathscr{Y}$. □

We can now complete the proof of Theorem A.3.

Proof of Theorem A.3. Applying Lemma A.9 and Proposition A.10, for $n \geq n_0$ we get

$$|\mathscr{Y}_n| = |\mathscr{Y}_\infty/\varphi^n(T)\mathscr{Y}_\infty| = p^c|\mathscr{A}/(\varphi^n(T))| = p^{\mu p^n + \lambda n + \nu}.$$

This finishes the proof of the theorem. □

A.2. ***Some consequences of Iwasawa's theorem.*** We have already seen one application of Iwasawa's theorem (Corollary 13.16) during the statement of the main conjecture. This stated that if one class number in a $\mathbb{Z}_p$-extension is coprime to p, then so are all the others. We list here some further interesting applications.

Recall that if A is a finite abelian group, then

$$A[p] := \{x \in A : px = 0\}$$

denotes the subgroup of p-torsion elements and its p-rank $\mathrm{rk}_p(A)$ is defined to be

$$\mathrm{rk}_p(A) = \dim_{\boldsymbol{F}_p}(A/pA) = \dim_{\boldsymbol{F}_p}(A[p]).$$

Equivalently, we can decompose A uniquely as a direct sum of cyclic groups of prime-power order; then the rank at p is the number of direct summands of p-power order.

Corollary A.13. *Let F_∞/F be a $\mathbb{Z}_p$-extension. It holds that $\mu = 0$ if and only if $\mathrm{rk}_p(\mathrm{Cl}(F_n))$ is bounded independently of n.*

Proof. Recall that

$$\mathrm{Cl}(F_n) \otimes \mathbb{Z}_p = \mathscr{Y}_n := \mathscr{Y}_\infty/(\varphi^n(T)),$$

that $\mathscr{Y}_\infty = \varprojlim \mathscr{Y}_n$ is quasi-isomorphic to a Λ-module $\mathscr{A} = \left(\bigoplus_{i=1}^s \Lambda/(p^{m_i})\right) \oplus \left(\bigoplus_{j=1}^t \Lambda/(g_j(T))\right)$ for some integers $s, t \geq 0$, $m_i \geq 1$, and $g_i(T) \in \mathscr{O}_L[T]$ distinguished polynomials, and that we have (see the proof of Proposition A.10) an exact sequence

$$0 \to C_n \to \mathscr{Y}_n \to \mathscr{A}_n \to B_n \to 0,$$

where $\mathscr{A}_n := \mathscr{A}/\varphi^n(T)$, with $|B_n|$ and $|C_n|$ bounded independently of n. It then suffices to show that $\mu = 0$ if and only if $\dim_{\boldsymbol{F}_p}(\mathscr{A}_n/p\mathscr{A}_n)$ is bounded independently of n.

We have

$$\mathscr{A}/p\mathscr{A}_n = \mathscr{A}/(p, \varphi^n(T)) = \left(\bigoplus_{i=1}^{s} \Lambda/(p, \varphi^n(T))\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(p, g_j(T), \varphi^n(T))\right).$$

Take n large enough such that $p^n \geq \deg(g_j)$ for all j and recall that g_j and $\varphi^n(T)$ are distinguished polynomials (in the sense that all but their leading coefficients are divisible by p). The above formula then equals

$$\left(\bigoplus_{i=1}^{s} \Lambda/(p, T^{p^n})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(p, T^{\deg(g_j)})\right) = (\mathbb{Z}/p\mathbb{Z})^{sp^n + tg},$$

where $g = \sum \deg(g_j)$. This shows that $\mathrm{rk}_p(\mathrm{Cl}(F_n))$ is bounded independently of n if and only if $s = 0$, i.e., if and only if $\mu = 0$. This finishes the proof. □

Concerning Iwasawa's invariants, we have the following results:

Theorem A.14 (Ferrero–Washington [81, Section 7.5]). *If F is an abelian number field and F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension of F, then $\mu = 0$.*

Finally, the following is an open conjecture of Greenberg [35].

Conjecture A.15 (Greenberg). *For any totally real field F, and any $\mathbb{Z}_p$-extension F_∞/F, we have $\mu = \lambda = 0$. In other words, the values $\#\mathrm{Cl}(F_n)$ are bounded as $n \to +\infty$.*

Appendix B: Iwasawa theory for modular forms

An interesting source of L-functions are those arising from automorphic forms, analytic functions on adelic groups that are symmetric for certain group actions. Dirichlet characters are algebraic automorphic forms for GL(1), so Parts I and II describe "Iwasawa theory for GL(1)". The next natural case, of GL(2), is that of *modular forms* (as explained in [82]). It is natural to ask how much of the theory above has an analogue for modular forms. The short answer is *all of it*, though our understanding of this case is not fully complete.

B.1. ***Recapping* GL(1).** We have described three different constructions of the Kubota–Leopoldt p-adic L-function ζ_p. Recall that $\Gamma^+ := \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})^+/\mathbb{Q}) \cong \mathbb{Z}_p^\times/\{\pm 1\}$ and that $\Lambda(\Gamma^+)$ is its Iwasawa algebra, with ring of fractions $Q(\Gamma^+)$.

(1) In Part I, we gave an *analytic* construction, a p-adic pseudomeasure $\zeta_p^{\mathrm{an}} \in Q(\Gamma^+)$ interpolating special values of the Riemann zeta function.

(2) In Section 10, we gave an *arithmetic* construction, defining ζ_p^{arith} via the image under Col of the family of cyclotomic units.

(3) In Section 13, we gave an *algebraic* construction. We described a torsion $\Lambda(\Gamma^+)$-module $\mathscr{X}_\infty^+$ with characteristic ideal $\zeta_p^{\mathrm{alg}} := \mathrm{Char}_{\Lambda(\Gamma^+)}(\mathscr{X}_\infty^+) \subset \Lambda(\Gamma^+)$.

Theorem 10.15 says that $\zeta_p^{\mathrm{an}} = \zeta_p^{\mathrm{arith}}$. The Iwasawa Main Conjecture says that $\zeta_p^{\mathrm{alg}} = I(\Gamma^+)\zeta_p^{\mathrm{an}}$.

B.2. ***Analogues for* GL(2).** Ultimately, versions of all of the above theory are known for sufficiently nice modular forms. Let f be a cuspidal Hecke eigenform of weight $k+2$ and level $\Gamma_0(N)$, with $p \mid N$, and let $L(f,s)$ be its attached L-function. There are three ways of associating a p-adic L-function to f.

B.2.1. *Analytic.* In the GL(1) story, the Kubota–Leopoldt p-adic L-function interpolated zeta values $L(\chi, -k)$ for $k \geq 0$ with $\chi(-1)(-1)^k = -1$. Such values are called "critical". For a more general L-function $L(s)$, Deligne [29, Definition 1.3] gave an arithmetic characterisation[16] of which values s should be critical for $L(s)$. For the modular form f, his criterion says the critical values of $L(f,s)$ are $L(f, \chi, j+1)$ for χ any Dirichlet character and $0 \leq j \leq k$.

The analytic p-adic L-function is an element $L_p^{\mathrm{an}}(f)$ in space of p-adic distributions $\mathscr{D}(\mathbb{Z}_p^\times)$ which interpolates these critical values. In particular, we have the following.

Theorem B.1. *Let α_p denote the U_p eigenvalue of f. If $v_p(\alpha_p) < k+1$, then there exists a unique locally analytic distribution $L_p^{\mathrm{an}}(f) \in \mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p^\times)$ on $\mathbb{Z}_p^\times$ such that*:

- *$L_p^{\mathrm{an}}(f)$ has growth of order $v_p(\alpha_p)$.*
- *For all Dirichlet characters χ of conductor p^n, and for all $0 \leq j \leq k$, we have*

$$\begin{aligned} L_p^{\mathrm{an}}(f, \overline{\chi}, j+1) &= \int_{\mathbb{Z}_p^\times} \chi(x) x^j \cdot L_p^{\mathrm{an}}(f) \\ &= -\alpha_p^{-n} \cdot \left(1 - \chi(p)\frac{p^j}{\alpha_p}\right) \cdot \frac{G(\chi) \cdot j! \cdot p^{nj}}{(2\pi i)^{j+1}} \cdot \frac{L(f, \overline{\chi}, j+1)}{\Omega_f^{\pm}}. \end{aligned}$$

We see that $L_p^{\mathrm{an}}(f)$ is, in this generality, only a locally analytic distribution (in the sense of Section 3.7). We note, however, that if f is p-ordinary (i.e., if $v_p(\alpha_p) = 0$) then the growth condition implies that $L_p^{\mathrm{an}}(f)$ lies in the subspace of p-adic measures on $\mathbb{Z}_p^\times$. This theorem was first proved in [1; 60; 79].

[16] Precisely, Deligne asks that given a "motivic" L-function $L(M,s)$, if $L_\infty(M,s)$ denotes the "Euler factor at infinity", then $s=j$ is critical for $L(M,s)$ if neither $L_\infty(M,s)$ nor $L_\infty(M,1-s)$ has a pole at j. For $\zeta(s)$, the factor at infinity is $\pi^{-s/2}\Gamma(s/2)$, and the Γ-function has poles at negative even integers. We deduce the critical values of $\zeta(s)$ are exactly the negative odd integers (as seen by Kubota–Leopoldt) and positive even integers, which relate to the negative odd integers through the functional equation for $\zeta(s)$.

If $\alpha_p \neq 0$, then we know that $v_p(\alpha_p) \leq k+1$, but the above theorem does not handle the case $v_p(\alpha) = k+1$. Subsequent work of Pollack–Stevens [68] and Bellaïche [4] means we have p-adic L-functions in this case too, though the statement is slightly different.

The case of $\alpha_p = 0$ is known as the *infinite slope* case. For certain particular cases, a construction of a p-adic L-function attached to elliptic curves of bad additive reduction (where $a_p = 0$) can be found in [28]. For arbitrary modular forms, partial p-adic L-functions with good interpolation properties have been constructed in [69], using Kato's Euler system and extending Perrin-Riou's big logarithm maps (as discussed in Section 10.5).

B.2.2. *Arithmetic.* As we sketched in Section 10.5, the appropriate generalisation of the arithmetic construction goes through Galois representations and Euler systems. Attached to a modular form f, we have a Galois representation V_f, constructed by Deligne inside the étale cohomology of the modular curve, in which we can pick a Galois-stable integral lattice T_f. The arithmetic p-adic L-function is then given by the following deep theorem of Kato, proved in his magisterial paper [47].

Theorem B.2 (Kato). *There exists an Euler system $\mathbb{Z}_{\mathrm{Kato}}(f)$ attached to T_f.*

In the yoga described in Section 10.5, we then consider the localisation of Kato's Euler system at p, which we still denote by the same name, and obtain a class

$$\mathbb{Z}_{\mathrm{Kato}}(f) \in H^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_f).$$

The arithmetic p-adic L-function is then the image of $\mathbb{Z}_{\mathrm{Kato}}(f)$ under the Perrin-Riou big logarithm map:

$$\mathrm{Log}_{V_f} : \mathrm{H}^1_{\mathrm{Iw}}(\mathbb{Q}_p, V_f) \to \mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p^\times), \quad \mathbb{Z}_{\mathrm{Kato}}(f) \mapsto L_p^{\mathrm{arith}}(f).$$

The second deep theorem of [47] is the following *explicit reciprocity law*.

Theorem B.3. *There is an equality*

$$L_p^{\mathrm{an}}(f) = L_p^{\mathrm{arith}}(f) \in \mathscr{D}^{\mathrm{la}}(\mathbb{Z}_p^\times).$$

B.2.3. *Algebraic.* Recall that, in Section 13.5, we described how the Iwasawa Main Conjecture for GL(1) (Theorem 13.8) can be generalised via Selmer groups. If f is a *p-ordinary* modular form, that is, when the eigenvalue α_p has $v_p(\alpha_p) = 0$, then its associated Galois representation V_f is p-ordinary in the sense of Definition 13.19; analogously to that section, we obtain a Selmer group $H^1(\mathbb{Q}(\mu_{p^\infty}), V_f)$ attached to f over the Iwasawa algebra $\Lambda(\Gamma)$ of $\Gamma := \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$. Kato [47] proved that this is a torsion Λ-module, and thus has a characteristic ideal

$$L_p^{\mathrm{alg}}(f) := \mathrm{ch}_{\Lambda(\mathbb{Z}_p^\times)}(\mathscr{X}_{p^\infty}(V_f)),$$

the *algebraic p-adic L-function of* f. When f is p-ordinary, the analytic/arithmetic p-adic L-function is actually a measure on $\mathbb{Z}_p^\times$, and hence lives in the subspace $\Lambda(\mathbb{Z}_p^\times) \subset \mathcal{D}(\mathbb{Z}_p^\times)$.

Theorem B.4 (Iwasawa Main Conjecture for f). *Under some mild additional technical hypotheses, we have*

$$L_p^{\mathrm{alg}}(f) = (L_p^{\mathrm{an}}(f)) \subset \Lambda(\mathbb{Z}_p^\times).$$

This is a theorem of Kato [47] and Skinner–Urban [77]. There has since been much further work weakening the required hypotheses, including analogues for nonordinary modular forms. For a description of up-to-date developments in this direction, see [32].

Remark B.5. The Iwasawa theory of modular forms has important applications to elliptic curves, and in particular to the BSD conjecture. An introduction to this is contained in Skinner's 2018 Arizona Winter School lectures [75].

Remark B.6. The topics described above comprise the *cyclotomic* Iwasawa theory of modular forms. There is also a rich *anticyclotomic* Iwasawa theory, working over an auxiliary imaginary quadratic field, with similarly spectacular applications to BSD. This is described in [8], and for a more recent overview, see [13].

B.3. ***Further results.*** The three constructions above, and the equalities between them, are expected to go through in very wide generality, but there are very few cases in which the whole picture has been completed. We sketch this here. Suppose that V is a Galois representation arising from a motive M and corresponding (at least conjecturally) under the Langlands correspondence to an automorphic representation π.

(1) Analytic: There should be a locally analytic p-adic distribution $L_p^{\mathrm{an}}(V)$ which interpolates critical values of $L(V, s)$. This analytic p-adic L-function is subject to precise conjectures of Coates–Perrin-Riou and Panchishkin [14; 15; 66].

All current techniques for proving such conjectures are automorphic; but this is already difficult, even assuming p-ordinarity. We illustrate this in the case of (regular algebraic, cuspidal, p-ordinary) automorphic representations of $\mathrm{GL}_n(\boldsymbol{A}_{\mathbb{Q}})$.

- The cases of GL(1) and GL(2) were described above.
- The case of GL(3) was only recently handled in [56]. Constructions in the special case where π is a symmetric square lift were given (decades earlier) in [40; 71].
- No general construction is known for any $n \geq 4$. The best known results are in further "degenerate" cases where π really comes from a different group (e.g., [2]).

For other groups, there are also many results; for example, in [31] for unitary groups, [54; 58] for Siegel modular forms, and [44; 48] for $\mathrm{GL}_{n+1} \times \mathrm{GL}_n$. The general picture remains, however, very fragmented.

We do not claim to give anything approaching a comprehensive list here. Indeed, we have only scratched the surface; there are also constructions for many other groups, with more general base fields, and without assuming ordinarity. We highlight mainly that there remain a vast number of open questions in the construction of analytic p-adic L-functions.

If one drops the cuspidality assumption, we know even less, with good results only for GL(2). Without the regular algebraic assumption, we know essentially nothing at all.

(2) Arithmetic: We also expect Euler systems, in the sense of [70], to exist in great generality, but known examples are scarcer still. Until relatively recently, Kato's Euler system and the cyclotomic units were two of only three examples of Euler systems, the other being the system of *elliptic units* (though the system of *Heegner points* is closely related). The last decade, though, has seen an explosion of activity in the area. Recent important examples of Euler systems include Euler systems for products of two modular forms [53], the *diagonal cycles* attached to triple products of modular forms [26], and Euler systems for GSp_4 [59].

Where an Euler system exists, one can apply a Perrin-Riou logarithm map and extract an arithmetic p-adic L-function; but proving an explicit reciprocity law is harder still. Such reciprocity laws were studied in the Rankin–Selberg setting in [49], for diagonal cycles in [9], and for GSp_4 in [57]. For a precise summary of the double- and triple-product settings, see [55, Section B].

(3) Algebraic: There are Iwasawa Main Conjectures in wide generality, at least in ordinary settings, and there are many partial results towards these too. Whenever one has an Euler system with the equality $L_p^{\mathrm{an}} = L_p^{\mathrm{arith}}$, for example, one has that the corresponding Selmer group is torsion and the divisibility $L_p^{\mathrm{alg}} \mid (L_p^{\mathrm{an}})$.

Acknowledgements

These notes started life as the lecture notes for a course at the London Taught Course Centre in 2017. We thank the organisers of the LTCC, and the participants of that course, for their attention and enthusiasm. We would also like to thank Martin Barič, Keith Conrad, David Corwin and Luis Santiago for their comments and corrections on earlier drafts of these notes. We first learnt of this construction of the Kubota–Leopoldt p-adic L-function from Pierre Colmez's notes [22], and we are grateful to him for allowing us to reproduce here the construction from his notes. We are also grateful to the three referees, whose careful reading and insightful suggestions and corrections greatly improved this text.

References

[1] Y. Amice and J. Vélu, "Distributions p-adiques associées aux séries de Hecke", pp. 119–131 in *Journées Arithmétiques de Bordeaux* (Univ. Bordeaux, 1974), Astérisque **24/25**, Soc. Math. France, Paris, 1975. MR Zbl

[2] A. Ash and D. Ginzburg, "p-adic L-functions for GL($2n$)", *Invent. Math.* **116**:1-3 (1994), 27–73. MR

[3] J. Bellaïche, "An introduction to the conjecture of Bloch and Kato", unpublished manuscript, 2009.

[4] J. Bellaïche, "Critical p-adic L-functions", *Invent. Math.* **189**:1 (2012), 1–60. MR Zbl

[5] J. Bellaïche, *The eigenbook: eigenvarieties, families of Galois representations, p-adic L-functions*, Birkhäuser, 2021. MR Zbl

[6] D. Benois, "An introduction to p-adic Hodge theory", pp. 69–219 in *Perfectoid spaces*, edited by D. Banerjee et al., Springer, 2022. MR Zbl

[7] L. Berger, "An introduction to the theory of p-adic representations", pp. 255–292 in *Geometric aspects of Dwork theory*, *I*, edited by A. Adolphson et al., De Gruyter, Berlin, New York, 2004. MR Zbl

[8] M. Bertolini and H. Darmon, "Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions", *Ann. of Math.* (2) **162**:1 (2005), 1–64. MR Zbl

[9] M. Bertolini, H. Darmon, V. Rotger, M. A. Seveso, and R. Venerucci, *Heegner points, Stark–Heegner points, and diagonal classes*, Astérisque **434**, Soc. Math. France, Paris, 2022. MR Zbl

[10] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis: a systematic approach to rigid analytic geometry*, Grundl. Math. Wissen. **261**, Springer, 1984. MR Zbl

[11] J. W. S. Cassels, *Local fields*, London Math. Soc. Student Texts **3**, Cambridge Univ. Press, 1986. MR Zbl

[12] F. Castella and M.-L. Hsieh, "On the nonvanishing of generalised Kato classes for elliptic curves of rank 2", *Forum Math. Sigma* **10** (2022), art. id. e12. MR Zbl

[13] F. Castella, G. Grossi, J. Lee, and C. Skinner, "On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes", *Invent. Math.* **227**:2 (2022), 517–580. MR

[14] J. Coates, "On p-adic L-functions attached to motives over $\mathbb{Q}$, II", *Bol. Soc. Brasil. Mat.* (*N.S.*) **20**:1 (1989), 101–112. MR Zbl

[15] J. Coates and B. Perrin-Riou, "On p-adic L-functions attached to motives over $\mathbb{Q}$", pp. 23–54 in *Algebraic number theory*, edited by J. Coates et al., Adv. Stud. Pure Math. **17**, Academic Press, Boston, 1989. MR

[16] J. Coates and R. Sujatha, *Cyclotomic fields and zeta values*, Springer, 2006. MR Zbl

[17] R. F. Coleman, "Dilogarithms, regulators and p-adic L-functions", *Invent. Math.* **69**:2 (1982), 171–208. MR Zbl

[18] P. Colmez, "Fonctions L p-adiques", exposé 851, pp. 21–58 in *Séminaire Bourbaki*, 1998/99, Astérisque **266**, Soc. Math. France, Paris, 2000. MR Zbl

[19] P. Colmez, "La conjecture de Birch et Swinnerton-Dyer p-adique", exposé 919, 251–319 in *Séminaire Bourbaki*, 2002/2003, Astérisque **294**, 2004. MR Zbl

[20] P. Colmez, "Fonctions d'une variable p-adique", pp. 13–59 in *Représentations p-adiques de groupes p-adiques*, *II*: *Représentations de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et* (ϕ, Γ)*-modules*, edited by L. Berger et al., Astérisque **330**, 2010. MR Zbl

[21] P. Colmez, "Représentations de $\mathrm{GL}_2(\mathbb{Q}_p)$ et (ϕ, Γ)-modules", pp. 281–509 in *Représentations p-adiques de groupes p-adiques, II: Représentations de $\mathrm{GL}_2(\mathbb{Q}_p)$ et (ϕ, Γ)-modules*, edited by L. Berger et al., Astérisque **330**, 2010. MR Zbl

[22] P. Colmez, "La fonction zeta p-adique, notes du cours de M2", unpublished notes.

[23] H. Darmon, "Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications", *Ann. of Math.* (2) **154**:3 (2001), 589–639. MR Zbl

[24] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conf. Ser. Math. **101**, Amer. Math. Soc., Providence, RI, 2004. MR Zbl

[25] H. Darmon, "Heegner points, Stark–Heegner points, and values of L-series", pp. 313–345 in *Proceedings of the International Congress of Mathematicians, II*, edited by M. Sanz-Solé et al., Eur. Math. Soc., Zürich, 2006. MR Zbl

[26] H. Darmon and V. Rotger, "Diagonal cycles and Euler systems, I: A p-adic Gross–Zagier formula", *Ann. Sci. Éc. Norm. Supér.* (4) **47**:4 (2014), 779–832. MR Zbl

[27] H. Darmon and V. Rotger, "Elliptic curves of rank two and generalised Kato classes", *Res. Math. Sci.* **3** (2016), art. id. 27. MR Zbl

[28] D. Delbourgo, "Iwasawa theory for elliptic curves at unstable primes", *Compositio Math.* **113**:2 (1998), 123–153. MR Zbl

[29] P. Deligne, "Valeurs de fonctions L et périodes d'intégrales", pp. 313–346 in *Automorphic forms, representations and L-functions, II* (Oregon State Univ., Corvallis, Ore., 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, RI, 1979. MR Zbl

[30] F. Diamond and J. Shurman, *A first course in modular forms*, Grad. Texts Math. **228**, Springer, 2005. MR Zbl

[31] E. Eischen, M. Harris, J. Li, and C. Skinner, "p-adic L-functions for unitary groups", *Forum Math. Pi* **8** (2020), art. id. e9. MR Zbl

[32] O. Fouquet and X. Wan, "The Iwasawa Main Conjecture for universal families of modular motives", preprint, 2021. arXiv 2107.13726

[33] T. Fukaya and K. Kato, "A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory", pp. 1–85 in *Proceedings of the St. Petersburg Mathematical Society, XII*, edited by N. N. Uraltseva, Amer. Math. Soc. Transl. Ser. 2 **219**, Amer. Math. Soc., Providence, RI, 2006. MR Zbl

[34] D. Goldfeld and J. Hundley, *Automorphic representations and L-functions for the general linear group, I*, Cambridge Stud. Adv. Math. **129**, Cambridge Univ. Press, 2011. MR Zbl

[35] R. Greenberg, "On the Iwasawa invariants of totally real number fields", *Amer. J. Math.* **98**:1 (1976), 263–284. MR Zbl

[36] R. Greenberg, "Iwasawa theory for p-adic representations", pp. 97–137 in *Algebraic number theory*, edited by J. Coates et al., Adv. Stud. Pure Math. **17**, Academic Press, Boston, 1989. MR Zbl

[37] R. Greenberg and G. Stevens, "p-adic L-functions and p-adic periods of modular forms", *Invent. Math.* **111**:2 (1993), 407–447. MR Zbl

[38] M. Gros, "Régulateurs syntomiques et valeurs de fonctions L p-adiques, I", *Invent. Math.* **99**:2 (1990), 293–320. MR Zbl

[39] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84**:2 (1986), 225–320. MR Zbl

[40] H. Hida, "p-adic L-functions for base change lifts of GL_2 to GL_3", pp. 93–142 in *Automorphic forms, Shimura varieties, and L-functions, II* (Ann Arbor, MI, 1988), edited by L. Clozel and J. S. Milne, Perspect. Math. **11**, Academic Press, Boston, 1990. MR

[41] H. Hida, *Elementary theory of L-functions and Eisenstein series*, London Math. Soc. Student Texts **26**, Cambridge Univ. Press, 1993. MR Zbl

[42] A. Huber and G. Kings, "Bloch–Kato conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters", *Duke Math. J.* **119**:3 (2003), 393–464. MR Zbl

[43] K. Iwasawa, "Some properties of (L)-groups", pp. 447–450 in *Proceedings of the International Congress of Mathematicians, II*, edited by L. M. Graves et al., Amer. Math. Soc., Providence, RI, 1952. MR Zbl

[44] F. Januszewski, "Non-abelian p-adic Rankin–Selberg L-functions and non-vanishing of central L-values", *Amer. J. Math.* **146**:2 (2024), 495–578. MR Zbl

[45] D. Jetchev, C. Skinner, and X. Wan, "The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one", *Camb. J. Math.* **5**:3 (2017), 369–434. MR Zbl

[46] K. Kato, "Lectures on the approach to Iwasawa theory for Hasse–Weil L-functions via B_{dR}, I", pp. 50–163 in *Arithmetic algebraic geometry* (Trento, 1991), edited by E. Ballico, Lecture Notes Math. **1553**, Springer, 1993. MR Zbl

[47] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", pp. 117–290 in *Cohomologies p-adiques et applications arithmétiques, III*, Astérisque **295**, 2004. MR Zbl

[48] D. Kazhdan, B. Mazur, and C.-G. Schmidt, "Relative modular symbols and Rankin–Selberg convolutions", *J. Reine Angew. Math.* **519** (2000), 97–141. MR Zbl

[49] G. Kings, D. Loeffler, and S. L. Zerbes, "Rankin–Eisenstein classes and explicit reciprocity laws", *Camb. J. Math.* **5**:1 (2017), 1–122. MR Zbl

[50] M. Kolster and T. Nguyen Quang Do, "Syntomic regulators and special values of p-adic L-functions", *Invent. Math.* **133**:2 (1998), 417–447. MR Zbl

[51] V. A. Kolyvagin, "Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **52**:3 (1988), 522–540. In Russian; translated in *Math. USSR-Izv.* **32**:3 (1989), 523–541. MR Zbl

[52] S. Lang, *Cyclotomic fields I and II*, 2nd ed., Grad. Texts Math. **121**, Springer, 1990. MR Zbl

[53] A. Lei, D. Loeffler, and S. L. Zerbes, "Euler systems for Rankin–Selberg convolutions of modular forms", *Ann. of Math.* (2) **180**:2 (2014), 653–771. MR Zbl

[54] Z. Liu, "p-adic L-functions for ordinary families on symplectic groups", *J. Inst. Math. Jussieu* **19**:4 (2020), 1287–1347. MR Zbl

[55] D. Loeffler and O. Rivero Salgado, "Eisenstein degeneration of Euler systems", *J. Reine Angew. Math.* **814** (2024), 241–282. MR

[56] D. Loeffler and C. Williams, "p-adic L-functions for GL(3)", preprint. arXiv 2111.04535

[57] D. Loeffler and S. L. Zerbes, "On the Bloch–Kato conjecture for GSp(4)", preprint, 2020. arXiv 2003.05960

[58] D. Loeffler, V. Pilloni, C. Skinner, and S. L. Zerbes, "Higher Hida theory and p-adic L-functions for GSp_4", *Duke Math. J.* **170**:18 (2021), 4033–4121. MR Zbl

[59] D. Loeffler, C. Skinner, and S. L. Zerbes, "Euler systems for GSp(4)", *J. Eur. Math. Soc.* (*JEMS*) **24**:2 (2022), 669–733. MR Zbl

[60] B. Mazur and P. Swinnerton-Dyer, "Arithmetic of Weil curves", *Invent. Math.* **25** (1974), 1–61. MR Zbl

[61] B. Mazur and A. Wiles, "Class fields of abelian extensions of $\mathbb{Q}$", *Invent. Math.* **76**:2 (1984), 179–330. MR Zbl

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

[63] M. R. Murty and V. K. Murty, "Mean values of derivatives of modular L-series", *Ann. of Math.* (2) **133**:3 (1991), 447–475. MR Zbl

[64] J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992. MR Zbl

[65] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundl. Math. Wissen. **323**, Springer, 2000. MR Zbl

[66] A. A. Panchishkin, "Motives over totally real fields and p-adic L-functions", *Ann. Inst. Fourier* (*Grenoble*) **44**:4 (1994), 989–1023. MR Zbl

[67] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229**, 1995. MR Zbl

[68] R. Pollack and G. Stevens, "Critical slope p-adic L-functions", *J. Lond. Math. Soc.* (2) **87**:2 (2013), 428–452. MR Zbl

[69] J. Rodrigues Jacinto, "(φ, Γ)-modules de de Rham et fonctions L p-adiques", *Algebra Number Theory* **12**:4 (2018), 885–934. MR Zbl

[70] K. Rubin, *Euler systems*, Annals Math. Stud. **147**, Princeton Univ. Press, 2000. MR Zbl

[71] C.-G. Schmidt, "p-adic measures attached to automorphic representations of GL(3)", *Invent. Math.* **92**:3 (1988), 597–631. MR

[72] P. Schneider, "p-adic height pairings, II", *Invent. Math.* **79**:2 (1985), 329–374. MR Zbl

[73] J.-P. Serre, "Formes modulaires et fonctions zêta p-adiques", pp. 191–268 in *Modular functions of one variable*, *III* (Proc. Internat. Summer School, Univ. Antwerp, 1972), edited by W. Kuyk and J.-P. Serre, Lecture Notes Math. **350**, Springer, 1973. MR Zbl

[74] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Res. Notes Math. **7**, A K Peters, Wellesley, MA, 1998. MR Zbl

[75] C. Skinner, "Lectures on the Iwasawa theory of elliptic curves", lecture notes from the 2018 Arizona Winter School, 2018, available at http://swc.math.arizona.edu/aws/2018/.

[76] C. Skinner, "A converse to a theorem of Gross, Zagier, and Kolyvagin", *Ann. of Math.* (2) **191**:2 (2020), 329–354. MR Zbl

[77] C. Skinner and E. Urban, "The Iwasawa main conjectures for GL_2", *Invent. Math.* **195**:1 (2014), 1–277. MR Zbl

[78] J. T. Tate, Jr., *Fourier analysis in number fields and Hecke's zeta-functions*, Ph.D. thesis, Princeton University, 1950, available at https://www.proquest.com/docview/304411725. MR Zbl

[79] M. M. Višik, "Nonarchimedean measures associated with Dirichlet series", *Mat. Sb.* (*N.S.*) **99(141)**:2 (1976), 248–260. In Russian; translated in *Math. USSR-Sb.* **28**:2 (1976), 216–228. MR Zbl

[80] L. C. Washington, *Introduction to cyclotomic fields*, Grad. Texts Math. **83**, Springer, 1982. MR Zbl

[81] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts Math. **83**, Springer, 1997. MR Zbl

[82] A. Weil, *Dirichlet series and automorphic forms*, Lecture Notes Math. **189**, Springer, 1971. Zbl

[83] A. Wiles, "The Iwasawa conjecture for totally real fields", *Ann. of Math.* (2) **131**:3 (1990), 493–540. MR Zbl

Received 26 Jun 2023. Revised 16 Dec 2024.

JOAQUÍN RODRIGUES JACINTO:

joaquin.rodrigues-jacinto@univ-amu.fr
Institut de Mathématiques de Marseille, Aix-Marseille Université, Marseille, France

CHRIS WILLIAMS:

chris.williams1@nottingham.ac.uk
School of Mathematical Sciences, University of Nottingham, United Kingdom

ESSENTIAL NUMBER THEORY

msp.org/ent

See inside back cover or msp.org/ent for submission instructions.

Essential Number Theory (ISSN 2834-4634 electronic, 2834-4626 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ENT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
https://msp.org/

ESSENTIAL NUMBER THEORY

2025 vol. 4 no. 1