AN INTRODUCTION TO p-ADIC L-FUNCTIONS

by

Joaquín Rodrigues Jacinto & Chris Williams

Contents

General overview ... 2
1. Introduction ... 2
  1.1. Motivation ... 2
  1.2. The Riemann zeta function ... 5
  1.3. p-adic L-functions ... 6
  1.4. Structure of the course ... 11

Part I: The Kubota–Leopoldt p-adic L-function ... 12
2. Measures and Iwasawa algebras ... 12
  2.1. The Iwasawa algebra ... 12
  2.2. p-adic analysis and Mahler transforms ... 14
  2.3. An example: Dirac measures ... 15
  2.4. A measure-theoretic toolbox ... 15
3. The Kubota-Leopoldt p-adic L-function ... 17
  3.1. The measure μ_a ... 17
  3.2. Restriction to $\mathbf{Z}_p^\times$ ... 18
  3.3. Pseudo-measures ... 19
4. Interpolation at Dirichlet characters ... 21
  4.1. Characters of p-power conductor ... 21
  4.2. Non-trivial tame conductors ... 23
  4.3. Analytic functions on $\mathbf{Z}_p$ via the Mellin transform ... 25
  4.4. The values at $s = 1$ ... 27
5. The p-adic family of Eisenstein series ... 29

Part II: Iwasawa's main conjecture ... 31
6. The Coleman map ... 32
  6.1. Notation and Coleman's theorem ... 32
  6.2. Example: cyclotomic units ... 33
  6.3. Proof of Coleman's theorem ... 34
  6.4. The logarithmic derivative ... 36
  6.5. The Coleman map ... 39
  6.6. The Kummer sequence, Euler systems and p-adic L-functions ... 40
7. The Main Conjecture ... 42
  7.1. The Λ-modules arising from Galois theory ... 43
  7.2. Measures on Galois groups ... 44
  7.3. The main conjecture ... 46
  7.4. Cyclotomic units ... 47
  7.5. On a theorem of Iwasawa ... 48
  7.6. An application of class field theory ... 49
  7.7. Some consequences of Iwasawa theory ... 50
8. Iwasawa's μ-invariant ... 51
  8.1. Iwasawa's theorem ... 51
  8.2. Some consequences of Iwasawa's theorem ... 56

Appendix ... 58

9. The complex class number formula 58
10. Class field theory 59
11. Power series and Iwasawa algebras 61

References 63

General overview

In these lectures, we aim to give an introduction to p-adic L-functions and the foundations of Iwasawa theory. Iwasawa's work found overarching structures that explained previous results of Kummer linking special values of L-functions with the arithmetic of cyclotomic fields. His methods have been applied with stunning success in other settings, and much of what we know today about long-standing conjectures such as the Birch and Swinnerton-Dyer conjecture has its roots in Iwasawa theory.

We will focus mainly on the construction and study of Kubota and Leopoldt's p-adic interpolation of the Riemann zeta function and on the ideas surrounding the *Iwasawa Main conjecture*, now a theorem due to Mazur and Wiles (see [**MW84**]). We will describe some classical results linking L-values and arithmetic data that led to the study of p-adic L-functions, and give several constructions of the p-adic zeta function. In particular, a construction due to Coleman using cyclotomic units will naturally lead to the statement of the Main conjecture, which we will prove when p is a Vandiver prime (which conjecturally, at least, covers every prime). We will finally see a theorem of Iwasawa describing the growth of the p-part of the class group of cyclotomic fields.

Recommended reading: The material in Part I of these notes is largely contained in Lang's *Cyclotomic fields I and II* (see [**Lan90**]) and Colmez's lecture notes [**Col**]. Part II is based on the book *Cyclotomic fields and zeta values* by Coates and Sujatha (see [**CS06**]). Part III is based on Washington's book *An introduction to cyclotomic fields* (see [**Was97**], especially §13). These lectures can be regarded as an introduction to the topics treated in the references mentioned above, which the reader is urged to consult for further details, and as a prelude to Rubin's proof of the Main Conjecture using the theory of Euler systems, as described in [**CS06**] and [**Lan90**, Appendix].

1. Introduction

1.1. Motivation. —

1.1.1. *Classical L-functions.* — The study of L-functions and their special values goes back centuries, and they are central objects of modern number theory. Examples include:

– The famous *Riemann zeta function*, defined by

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p} (1 - p^{-s})^{-1}, \quad s \in \mathbf{C},$$

where the last product runs over all prime numbers p and the second equality follows is a conseqence of the unique factorisation theorem. The sum converges absolutely for the real part of s greater than 1, making ζ a holomorphic function in a right half-plane. The expression as a product is called an *Euler product*.

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

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

where the sum is over all non-zero ideals in the ring of integers (and which again converges for $\mathrm{Re}(s) > 1$), and the product is over all non-zero prime ideals of K. The existence of the Euler product again follows from unique factorisation.

– Let $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ be a Dirichlet character, and extend it to a function $\chi : \mathbf{Z} \to \mathbf{C}$ by setting it to be 0 at integers not coprime to N. 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, this converges in a right half-plane.

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

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

where $a_p(E) = p + 1 - \#E(\mathbf{F}_p)$ and the factors $L_p(s)$ at bad primes 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. non-split multiplicative) reduction at p.

– Let $f = \sum_{n=1}^{+\infty} a_n(p) q^n \in S_k(\Gamma_0(N), \omega_f)$ be a (normalised) newform of weight k, level N and character ω_f. The L-function associated to f is given by

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

Any reasonably behaved L-function should have the following basic properties (which may be non-trivial to prove!) [(1)]:

(1) A meromorphic continuation to the whole complex plane;
(2) A functional equation relating s and $k - s$ for some $k \in \mathbf{R}$;
(3) An Euler product.

Remark 1.1. — More generally, let $\mathscr{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ denote the absolute Galois group of $\mathbf{Q}$ and let $V \in \mathrm{Rep}_L \mathscr{G}_{\mathbf{Q}}$ be a p-adic Galois representation (i.e. a finite dimensional vector space over a finite extension L of $\mathbf{Q}_p$ equipped with a continuous linear action of $\mathscr{G}_{\mathbf{Q}}$). For $\ell \neq p$ a rational prime, one defines a local factor at ℓ 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. One defines a local factor at p as

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

where this time $\mathbf{D}_{\mathrm{cris}}(V)$ denotes the crystalline module of $V|_{\mathscr{G}_{\mathbf{Q}_p}}$ from p-adic Hodge theory and φ denotes the crystalline Frobenius. One then defines the global L-function of V as the formal product

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

[(1)] We will treat the meromorphic continuation of the Riemann zeta function in the sequel.

When V is the representation attached to am arithmetic object[(2)] the L-function of the representation is typically equal to the L-function attached to that object; for example, taking $V = \mathbf{Q}_p(\chi)$ (that is, $V = \mathbf{Q}_p$ with $\mathscr{G}_{\mathbf{Q}}$ acting through the character χ via class field theory), one recovers the Dirichlet L-functions described above. See [**Bel09**] for an introduction to these topics.

1.1.2. *Special values and arithmetic data.* — Much of the interest of L-functions comes through their special values. There are deep results and conjectures relating special values of L-functions to important arithmetic information, of which a prototypical example is the following:

Theorem 1.2 **(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*

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

where h_F is the class number of F.

In theory, this gives a method for calculating the class number of a number field, although in general computing the regulator is difficult. In special cases related to cyclotomic fields, though, it can give an effective computation of the class number.

A second famous example of links between special values of L-functions and arithmetic information comes in the form of the *Birch and Swinnerton–Dyer conjecture*. Let $E/\mathbf{Q}$ be an elliptic curve. The set of rational points $E(\mathbf{Q})$ forms a finitely generated abelian group, and Birch and Swinnerton–Dyer predicted that

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

Let's say we want to attack the conjecture. There are two natural subquestions:

(a) We could try to prove that $\mathrm{rank}_{\mathbf{Z}}E(\mathbf{Q}) \geq \mathrm{ord}_{s=1}L(E,s)$. A natural approach is to try to construct rational points on the elliptic curve. The theory of *Heegner points* is based on such an idea. More recently, the p-adic theory of *Stark–Heegner points* has been used with some success (see [**Dar01**], where the theory was initiated). These constructions tend to give points of infinite order on $E(\mathbf{Q})$ if and only if the L-function vanishes to a certain order (for example, a Heegner point has infinite order if and only if the order of vanishing is precisely 1).

(b) Conversely, we could try and prove that $\mathrm{rank}\ E(\mathbf{Q}) \leq \mathrm{ord}_{s=1}L(E,s)$. In this case we want to *bound* the number of points. One method for trying to do this uses *Euler systems* (see [**Rub00**] for a comprehensive introduction). The primary application of the theory of Euler systems is in bounding certain Galois cohomology groups, known as *Selmer groups*, which are defined using local behaviour and can be viewed as a cohomological interpretation of the group of rational points on E. The difference between the Selmer group and $E(\mathbf{Q})$ is captured in the *Tate–Shafarevich group* $Ш(E/\mathbf{Q})$, which is a torsion abelian group that is conjecturally finite. If the p-part of $Ш(E/\mathbf{Q})$ is finite, then the p-Selmer group and the group $E(\mathbf{Q})$ have the same rank (as abelian groups), so bounding the Selmer group is equivalent to bounding $E(\mathbf{Q})$.

The ideas above have led to the only known 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, Gross–Zagier and Murty–Murty (see [**Kol88**], [**GZ86**] and [**MM91**]).

(2) For example, a number field, an elliptic curve, a modular form, etc.

Remark 1.3. — Something that both (a) and (b) have in common is their use of *p-adic L-functions*. In fact, there is a p-adic version of Birch and Swinnerton-Dyer, due to Mazur, Tate and Teitelbaum (see [**MTT86**]), which relates the rank of the p-Selmer group to the order of vanishing of a p-adic L-function at $s = 1$. This formulation (which is conjecturally equivalent to the standard formulation[(3)]) has recently been *proved* in many cases by Skinner–Urban (see [**SU14**]), following work of Kato (see [**Kat04**]). Their proof uses a version of the *Iwasawa Main Conjecture* for elliptic curves.

1.1.3. *Iwasawa's main conjecture: a general picture.* — As it has been mentioned, many arithmetic objects have associated *Galois representations*, and these Galois representations come with L-functions. In general, one might expect that where there is an L-function, there is a p-adic L-function, and that there is a version of the Main conjecture for this p-adic L-function. The main conjecture essentially says that the p-adic L-function should control the size of the Selmer groups of the Galois representation it is attached to (recalling from above that the Selmer groups are subgroups of the Galois cohomology defined by local conditions).

$$\begin{array}{ccc} \{\text{Galois representations}\} & \longrightarrow & \{L-\text{functions}\} \\ \downarrow & & \downarrow \\ \{\text{Galois cohomology}\} & \xleftarrow{\text{IMC}} & \{p\text{-adic } L\text{-functions}\} \end{array}$$

In the case of elliptic curves, the application of this to Birch and Swinnerton–Dyer comes through the links between the Selmer groups and $E(\mathbf{Q})$.

In this lecture course, we will focus on the simplest example of the above picture, namely the Main conjecture for the Riemann zeta function, as formulated by Iwasawa himself. In the process, we will 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. In doing so, we hope to give an introduction to the rich area of p-adic L-functions and Iwasawa theory.

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

Theorem 1.4. — *Let $f : \mathbf{R}_{\geq 0} \longrightarrow \mathbf{R}$ be a $\mathscr{C}^\infty$-function that decays exponentially at infinity, and let*

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

be the usual Gamma function. The function

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

which converges to a holomorphic function for $Re(s) > 0$, 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.*

(3) To show that p-adic Birch and Swinnerton–Dyer implies classical Birch and Swinnerton–Dyer, one must show finiteness of Ш and prove a precise relation between the order of vanishing of the classical and p-adic L-functions. Both of these are, naturally, extremely difficult open problems.

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 easy exercise in integration by parts, using the identity $\Gamma(s) = (s-1)\Gamma(s-1)$, and gives the analytic continuation to all of $\mathbf{C}$ by iteration. Finally, iterating the same identity $n + 1$ times shows that

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

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

Now 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 1.5. — The Bernoulli numbers satisfy a recurrence relation that ensures they are *rational* numbers; for example, the first few are

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

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

Lemma 1.6. — *For the choice of f as above, we have*

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

Proof. — We use the classical formula for $\Gamma(s)$ above. Substituting t for nt and rearranging, 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 1.7. — *For $n \geq 0$, we have*

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

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

1.3. p-adic L-functions. — We have already seen two examples where special values of L-functions should be able tell us information about arithmetic objects. In fact, there are very general conjectures (for example, the Bloch–Kato and Beilinson conjectures) predicting that these links exist on a much wider scale, and despite some partial results in special cases these conjectures remain deep open problems. Much of what we *do* know about these conjectures comes through the theory of *p-adic L-functions.* In this section, we explain what a p-adic L-function is and the properties it should satisfy.

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

$$\zeta : \mathbf{C} \longrightarrow \mathbf{C}$$

with complex analytic properties which is rational at negative integers. Since $\mathbf{Z}$ is a common subset of both $\mathbf{C}$ and $\mathbf{Z}_p \subseteq \mathbf{C}_p$, and since they are dense in $\mathbf{Z}_p$, it is natural to ask if there exists a function

$$\zeta_p : \mathbf{Z}_p \longrightarrow \mathbf{C}_p$$

that is 'p-adic analytic' (in some sense to be defined) and which is uniquely characterized by the property that it agrees with the complex L-function at negative integers in the sense that

$$\zeta_p(1-n) = (*) \cdot \zeta(1-n),$$

for some explicit factor $(*)$. We would say that such a function 'p-adically interpolates the special values of $\zeta(s)$'.

1.3.2. *Ideles, measures and Tate's thesis.* — In practice, there is no *single* analytic function on $\mathbf{Z}_p$ that interpolates all of the special values[(4)], as we will explain in Section 4.3. Instead, a better way of thinking about L-functions is to use a viewpoint initiated by Tate in his thesis **[Tat50]** (and later independently by Iwasawa; see **[Iwa52]**). 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 the following observations.

Lemma 1.8. — (i) *Let $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times$ be a Dirichlet character. Then χ can be seen as a function*

$$\chi : \prod_{\ell \,\text{prime}} \mathbf{Z}_\ell^\times \longrightarrow \mathbf{C}^\times.$$

(ii) *There exists an identification of $\mathbf{C}$ with $\mathrm{Hom}_{\mathrm{cts}}(\mathbf{R}_{>0}, \mathbf{C}^\times)$ by sending s to the character $x \mapsto x^s$.*

Proof. — To see part (i), suppose that $N = \ell^n$ is a power of some prime ℓ; then we can see χ as a function on $\mathbf{Z}_\ell^\times$ via the identification

$$\mathbf{Z}_\ell^\times \cong (\mathbf{Z}/\ell^n\mathbf{Z})^\times \times (1 + \ell^n\mathbf{Z}_\ell).$$

The general case follows from the Chinese remainder theorem.

We turn to part (ii). For $s \in \mathbf{C}$, the function $x \mapsto x^s$ is visibly a continuous character on $\mathbf{R}_{>0}$. 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) $g : \mathbf{R} \to \mathbf{C}$ are of the form $g(x) = xg(1)$, which is easily shown by directly computing the values of g on $\mathbf{Q}$ and extending by continuity. □

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

$$\begin{aligned} \zeta : \mathrm{Hom}_{\mathrm{cts}}(\mathbf{R}_{>0}, \mathbf{C}^\times) &\longrightarrow \mathbf{C} \\ \left[x \mapsto x^s\right] &\longmapsto \zeta(s). \end{aligned}$$

But we can add in Dirichlet characters using the following.

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

Proposition 1.9. — *Under the identifications above, each pair (χ, s), where χ is a Dirichlet character and $s \in \mathbf{C}$, corresponds to a (unique) continuous character*

$$\begin{aligned}\kappa_{\chi,s} : \mathbf{R}_{>0} \times \prod_{\ell \,\text{prime}} \mathbf{Z}_\ell^\times &\longrightarrow \mathbf{C}^\times \\ (x, y) &\longmapsto x^s \chi(y),\end{aligned}$$

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

Proof. — The first assertion is immediate from above. To see the converse, let κ be such a character. Then we already know that the restriction of κ to $\mathbf{R}_{>0}$ must be of the form $x \mapsto x^s$. Furthermore, we have an isomorphism of topological groups

$$\prod_{\ell \,\text{prime}} \mathbf{Z}_\ell^\times \cong \varprojlim (\mathbf{Z}/M\mathbf{Z})^\times,$$

where the right hand side is equipped with the profinite topology, and by taking a sufficiently small open neighbourhood of 1 in $\mathbf{C}^\times$ we see that any continuous character κ' from this to $\mathbf{C}^\times$ must have open kernel. Hence the kernel has finite index, and κ descends to the (finite) quotient, which one can check is of the form $(\mathbf{Z}/N\mathbf{Z})^\times$ for some N, giving rise to a Dirichlet character χ of conductor N. Then $\kappa = \kappa_{\chi,s}$. □

The product space is more usually written as follows.

Definition 1.10. — Define the *ideles* $\mathbf{A}^\times$ of $\mathbf{Q}$ to be

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

(The prime on the product denotes *restricted product*, which indicates the almost everywhere integral property in the definition). It's a good exercise to check that:

***Proposition 1.11* (Strong approximation).** — *There is a decomposition*

$$\mathbf{A}^\times \cong \mathbf{Q}^\times \times \mathbf{R}_{>0} \times \prod_{\ell \,\text{prime}} \mathbf{Z}_\ell^\times.$$

Hence all continuous characters

$$\mathbf{Q}^\times \backslash \mathbf{A}^\times \longrightarrow \mathbf{C}^\times$$

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

Now we can consider *all* Dirichlet L-functions *at once* via the function

$$\begin{aligned}L : \mathrm{Hom}_{\mathrm{cts}}(\mathbf{Q}^\times \backslash \mathbf{A}^\times, \mathbf{C}^\times) &\longrightarrow \mathbf{C} \\ \kappa_{\chi,s} &\longmapsto L(\chi, s).\end{aligned}$$

In the framework of Tate, this function L can be viewed as integrating $\kappa_{\chi,s}$ against the *Haar measure* on $\mathbf{Q}^\times \backslash \mathbf{A}^\times$. In his thesis, Tate showed that properties such as the analytic continuation and functional equations of Dirichlet L-functions by 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 are the 'Euler factors 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.

Remark 1.12. —

– If K is any number field, one can analogously define the ideles $\mathbf{A}_K^\times$ of K as the restricted product $\prod_v K_v^\times$ over all places v of K. Continuous homomorphisms $K^\times\backslash\mathbf{A}_K^\times \to \mathbf{C}^\times$ are called *Hecke characters* or *Größencharacters*. They are examples of automorphic forms for GL_1/K.

– By class field theory, the idele class group $K^\times\backslash\mathbf{A}_K^\times$ injects (with dense image) into $\mathscr{G}_K^{\mathrm{ab}} := \mathrm{Gal}(K^{\mathrm{ab}}/K)$, where K^{ab} denotes the maximal abelian extension of K. Since any character of $\mathscr{G}_K$ must factor through $\mathscr{G}_K^{\mathrm{ab}}$, under this identification we have $\mathrm{Hom}_{\mathrm{cts}}(K^\times\backslash\mathbf{A}_K^\times, \mathbf{C}^\times) = \mathrm{Hom}_{\mathrm{cts}}(\mathscr{G}_K, \mathbf{C}^\times) = \mathrm{Hom}_{\mathrm{cts}}(\mathscr{G}_K, \mathrm{GL}_1(\mathbf{C}))$, where $\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$ denotes the absolute Galois group of $\mathbf{Q}$. We can then package Dirichlet L-functions over K into a complex analytic function on the space of one dimensional complex representations of the absolute Galois group $\mathscr{G}_K$.

1.3.3. *p-adic L-functions via measures.* — To obtain a p-adic version of this picture, a natural thing to do is to look at continuous characters from $\mathbf{Q}^\times\backslash\mathbf{A}^\times$ into $\mathbf{C}_p^\times$ (rather than $\mathbf{C}^\times$). Again, such a function corresponds to a function on $\mathbf{R}_{>0} \times \prod \mathbf{Z}_\ell^\times$. Since $\mathbf{R}_{>0}$ is connected and $\mathbf{C}_p$ is totally disconnected, the restriction of any such character to $\mathbf{R}_{>0}$ is trivial. Also using topological arguments we find that the restriction to $\prod_{\ell\neq p}\mathbf{Z}_\ell^\times$ factors through a finite quotient, so gives rise to some Dirichlet character of conductor prime to p. This leaves the restriction to $\mathbf{Z}_p^\times$, which is by far the most interesting part.

In the measure-theoretic viewpoint of L-functions, it is then natural to look for an analytic[5] function

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

in such a way that

$$\zeta_p(x \mapsto x^k) = (*)\cdot\zeta(-k), \quad k \geq 0$$

for an explicit factor $(*)$, that is, for a function on p-adic characters interpolating the values $\zeta(-k)$ for $k \geq 0$. We say such a function is a *measure on* $\mathbf{Z}_p^\times$. In equivalent and more elementary terms, a measure on $\mathbf{Z}_p^\times$ is an element of the continuous dual of the space of continuous functions on $\mathbf{Z}_p^\times$. We will prove:

***Theorem 1.13* (Kubota-Leopoldt, Iwasawa).** — *There exists a (pseudo-)measure*[6] *ζ_p on $\mathbf{Z}_p^\times$ such that, for all $k \geq 0$,*

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

Remark 1.14. — Note that we removed the Euler factor at p. This is a general phenomenon appearing in the theory of p-adic L-functions.

From such an object, we can build the (meromorphic) functions on $\mathbf{Z}_p$ we were initially looking for. But now, we have much more, and the power of the measure-theoretic approach becomes obvious:

Theorem 1.15. — *Let χ be a Dirichlet character of conductor p^n, $n \geq 0$, viewed as a locally constant character on $\mathbf{Z}_p^\times$. Then, for all $k \geq 0$,*

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

[5] Precisely, since $\mathbf{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbf{Z}_p)$, the space $\mathrm{Hom}_{\mathrm{cts}}(\mathbf{Z}_p^\times, \mathbf{C}_p^\times)$ can be identified with $p-1$ copies of the open unit ball in $\mathbf{C}_p$ (see the exercises). It carries the structure of a rigid analytic p-adic space, and a function on this space is *rigid analytic* if it can be written as a convergent power series on each ball. Such an analytic function will be a measure if these coefficients are bounded.

[6] *Pseudo-measures* will be defined in Section 3. Roughly speaking, such an object is a measure that is allowed to have simple poles.

In other words, when viewed as a measure the Kubota–Leopoldt p-adic L-function is a *single* p-adic gadget that encodes the special values not only of the Riemann zeta function, but also of *all* of its twists by characters of p-power conductor. This is pretty magic! Indeed, even though one only uses the values $\zeta(-k)$ to construct the measure ζ_p, Theorem 1.15 affirms that its values at infinitely many different points are still related to the complex L-function. We will also see a formula of Leopoldt showing another striking resemblance when evaluating at the character $x \mapsto \chi x^{-1}$.

To complete the image given in §1.3.2, one can take into account Dirichlet characters of conductor prime to p. The ideas that go into the proof of Theorem 1.15 can also be used to show:

Theorem 1.16. — *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 μ_η on $\mathbf{Z}_p^\times$ with the following interpolation property: for all primitive Dirichlet characters χ with conductor p^n for some $n \geq 0$, we have, for all $k > 0$,*

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

Remark 1.17. — Let $(\mathbf{Z}/D\mathbf{Z})^{\times\wedge}$ denote the space of characters on $(\mathbf{Z}/D\mathbf{Z})^\times$. The measures given by Theorem 1.16 can be seen as functions on $\mathrm{Hom}_{\mathrm{cts}}(\mathbf{Z}_p^\times, \mathbf{C}_p^\times) \times (\mathbf{Z}/D\mathbf{Z})^{\times\wedge}$ and they are compatible with respect to the natural maps $(\mathbf{Z}/D\mathbf{Z})^{\times\wedge} \to (\mathbf{Z}/E\mathbf{Z})^{\times\wedge}$ for $E|D$. This shows that they define a function on

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

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

Remark 1.18. — The measure-theoretic interpretation of p-adic L-functions also allows us to generalise to number fields in a clean and conceptual way, as we elaborate in this remark.

– Let $F_\infty = \mathbf{Q}(\mu_{p^\infty})$ denote the field extension of $\mathbf{Q}$ obtained by adjoining all p-power roots of unity. This is a Galois extension of $\mathbf{Q}$ with $\mathrm{Gal}(F_\infty/\mathbf{Q}) \cong \mathbf{Z}_p^\times$ via the cyclotomic character (see, for example, the notation at the start of Part II). Under this isomorphism, we can see ζ_p as a pseudo-measure on $\mathrm{Gal}(F_\infty/\mathbf{Q})$.

– Note that F_∞ is the maximal abelian extension of $\mathbf{Q}$ that is unramified outside p. Indeed, the Kronecker-Weber theorem states that if $K/\mathbf{Q}$ is abelian, then $K \subset \mathbf{Q}(\mu_m)$ for some minimal m. By the ramification properties of cyclotomic fields, if a prime ℓ ramifies in K, then $\ell|m$, and hence if K is unramified outside p, there exists some n such that $K \subset \mathbf{Q}(\mu_{p^n}) = F_n \subset F_\infty$.

– Now let $K/\mathbf{Q}$ be a number field; then the p-adic analogue of the zeta function $\zeta_K(s)$ should be a pseudo-measure on $\mathrm{Gal}(K^{\mathrm{ab},p}/K)$, where $K^{\mathrm{ab},p}$ is the maximal abelian extension of K unramified outside primes above p. This is also the natural setting for the construction of p-adic L-functions of other arithmetic objects, such as elliptic curves or modular forms over K. It is possible to translate measures on this Galois group into measures on $(\mathscr{O}_K \otimes \mathbf{Z}_p)^\times$ or analytic functions on $\mathscr{O}_K \otimes \mathbf{Z}_p$, but this is not as clean; over $\mathbf{Q}$, things work nicely since the class number is 1 and the totally positive global units are trivial. For a general number field K, the strong approximation theorem takes a more complicated form, and we end up with a collection of measures/analytic functions indexed by a class group. For an example of the theory for modular forms over imaginary quadratic fields, see [**Loe14**] (for measures/distributions) or [**BSW17**, §3] (for analytic functions).

1.4. Structure of the course. — The course will be split into three major parts. In Part I, we construct the p-adic analogue of the Riemann zeta function, called the *Kubota-Leopoldt p-adic L-function*, and prove that it interpolates special values of Dirichlet L-functions. In Part II, we will look at the Main conjecture. In particular, we'll explore some of the deeper underlying structure discovered by Iwasawa, proving a connection between certain units in cyclotomic fields and the p-adic L-function. This will naturally lead to the statement of the Main conjecture, which we will prove in a special case. In Part III, we will look at further topics in Iwasawa theory, including the λ- and μ-invariants of a $\mathbf{Z}_p$-extension. The latter theory allows precise control of the p-part of the ideal class group in a tower of p-extensions of number fields.

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

In this part, we give a construction of the Kubota–Leopoldt p-adic L-function and the p-adic L-functions of Dirichlet characters. In Section 2, we introduce the necessary formalism of p-adic measures and Iwasawa algebras, and show that there is an isomorphism from the Iwasawa algebra of $\mathbf{Z}_p$ to the space $\mathbf{Z}_p[[T]]$ of power series over $\mathbf{Z}_p$, given by the Mahler transform. In Section 3, we construct a pseudo-measure on $\mathbf{Z}_p^\times$ that interpolates the values of the Riemann zeta function at negative integers. In Section 4, we show moreover that this pseudo-measure interpolates the values $L(\chi, -k)$ for χ a Dirichlet character of p-power conductor. Further, if η is a Dirichlet character of conductor prime to p, we construct a measure on $\mathbf{Z}_p$ that interpolates the values $L(\chi\eta, -k)$ as χ runs over Dirichlet characters of p-power conductor. Finally, in Section 4.3 we rephrase the construction in terms of analytic functions on $\mathbf{Z}_p$ via the Mellin transform.

2. Measures and Iwasawa algebras

In the introduction, we explained that a natural way to construct p-adic L-functions is to construct suitable p-adic measures on $\mathbf{Z}_p^\times$. In this section, we introduce the formalism of the theory of p-adic analysis that we will be using in the sequel. Whilst some of the results of this section may appear a little dry in isolation, fluency in the measure-theoretic language will greatly help us simplify calculations that would otherwise be very technical.

2.1. The Iwasawa algebra. — We fix a finite extension L of $\mathbf{Q}_p$, equipped with the p-adic valuation normalized such that $v_p(p) = 1$; this will serve as the coefficient field. We write $\mathscr{O}_L$ for its ring of integers. Let G be a profinite abelian group (e.g. $G = \mathbf{Z}_p$ or $G = \mathbf{Z}_p^\times$, which are the examples of most interest to us).

We denote by $\mathscr{C}(G, L)$ the space of continuous functions $\phi : G \to L$, equipped with the valuation $v_{\mathscr{C}}(\phi) = \inf_{x\in G} v_p(\phi(x))$ (giving rise to the sup norm). This valuation makes $\mathscr{C}(G, L)$ into an L-Banach space, i.e. a complete topological L-vector space whose topology is defined by a valuation $v_{\mathscr{C}}$ satisfying

(i) $v_{\mathscr{C}}(f) = +\infty$ if and only if $f = 0$;
(ii) $v_{\mathscr{C}}(f + g) \geq v_{\mathscr{C}}(f) + v_{\mathscr{C}}(g)$ for all $f, g \in \mathscr{C}(G, L)$;
(iii) and $v_{\mathscr{C}}(\lambda f) = v_p(\lambda) + v_{\mathscr{C}}(f)$ for all $\lambda \in L, f \in \mathscr{C}(G, L)$.

Definition 2.1. — We define the space $\mathscr{M}(G, L)$ of *L-valued measures on G* as the dual $\mathrm{Hom}_{\mathrm{cts}}(\mathscr{C}(G, L), L)$ equipped with the strong topology. 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 (in the literature, this is sometimes written alternatively as $\int_G \phi \cdot d\mu$). 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 μ takes values in $\mathscr{O}_L$. Since G is compact and measures are continuous (or, equivalently, bounded), we have that $\mathscr{M}(G, L) = \mathscr{M}(G, \mathscr{O}_L) \otimes_{\mathscr{O}_L} L$. We will be mainly concerned with $\mathscr{O}_L$-valued functions and measures.

Remark 2.2. — We can think of measures as additive functions

$$\mu : \{\text{compact open subsets of } G\} \longrightarrow \mathscr{O}_L.$$

Indeed, let μ be such a function and let $\phi \in \mathscr{C}(G, \mathscr{O}_L)$. We will see how to integrate ϕ against μ. Assume first that ϕ is locally constant. Then 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

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

In the general case, we can write $\phi = \lim_{n\to\infty} \phi_n$, where each ϕ_n is locally constant. Then we can define

$$\int_G \phi \cdot \mu := \lim_{n\to\infty} \int_G \phi_n \cdot \mu,$$

which exists and is independent of the choice of ϕ_n we take. This defines an element in $\mathscr{M}(G, \mathscr{O}_L)$.

Conversely, if $\mu \in \mathscr{M}(G, \mathscr{O}_L)$ 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.

Proposition 2.3. — *We have an 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. — Let μ be a measure, 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 $(\lambda_H)_H \in \varprojlim \mathscr{O}_L[G/H]$, so we have a map from measures to this 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 subgroups of G, i.e. an element $\mu \in \mathscr{M}(G, \mathscr{O}_L)$. □

Definition 2.4. — We define the *Iwasawa algebra of G* to be

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

(Note that we suppress L from the notation).

Remark 2.5. — The Iwasawa algebra $\Lambda(\mathbf{Z}_p)$ has a natural $\mathscr{O}_L$-algebra structure, and hence by transport of structure we obtain such a structure on $\mathscr{M}(\mathbf{Z}_p, \mathscr{O}_L)$. It turns out that the algebra structure can be described directly via *convolution of measures*. For general 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.

2.2. p-adic analysis and Mahler transforms. — In this section we establish a link between p-adic measures on $\mathbf{Z}_p$ and power series.

Definition 2.6. — For $x \in \mathbf{Z}_p$ and $n \geq 1$, let

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

and let $\binom{x}{0} = 1$.

Remark 2.7. — One easily checks that $x \mapsto \binom{x}{n}$ defines an element in $\mathscr{C}(\mathbf{Z}_p, \mathbf{Z}_p)$ of valuation $v_{\mathscr{C}}\left(\binom{x}{n}\right) = 0$.

The following theorem says that the functions $\binom{x}{n}$ form an orthonormal basis [(7)] for the space $\mathscr{C}(\mathbf{Z}_p, L)$ and is fundamental in everything that follows.

***Theorem 2.8* (Mahler).** — *Let $\phi : \mathbf{Z}_p \to L$ 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 $a_n \to 0$ as $n \to \infty$. Moreover, $v_{\mathscr{C}}(\phi) = \inf_{n \in \mathbf{N}} v_p(a_n(\phi))$.

Proof. — See [**Col10a**, Théorème 1.2.3.]. □

Remark 2.9. — 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 $a_n(\phi) = \phi^{[n]}(0)$.

Definition 2.10. — Let $\mu \in \Lambda(\mathbf{Z}_p)$ be a p-adic measure on $\mathbf{Z}_p$. Define the *Mahler transform* (or *Amice transform*) of μ to be

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

Theorem 2.11. — *The Mahler transform gives an $\mathscr{O}_L$-algebra isomorphism*

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

Proof. — We can explicitly define an inverse to the transform. Let $g(T) = \sum_{n \geq 0} c_n T^n \in \mathscr{O}_L[[T]]$. Let $H \subset \mathbf{Z}_p$ be an open subgroup, and for each $[a] \in \mathbf{Z}_p/H$ let $\mathbf{1}_{aH}$ denote the characteristic function of the coset $aH \subset \mathbf{Z}_p$. This is a continuous function on $\mathbf{Z}_p$, and hence has a Mahler expansion

$$\mathbf{1}_{aH}(x) = \sum_{n \geq 0} a_n^{[a]} \binom{x}{n},$$

with $a_n^{[a]} \in \mathscr{O}_L$. Then define

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

and

$$\mu_H = \sum_{[a] \in \mathbf{Z}_p/H} \mu_{[a]}[a].$$

(7) If B is an L-Banach space, an orthonormal basis of B is a collection $(e_i)_{i \in I}$ such that $(a_i)_{i \in I} \mapsto \sum_{i \in I} a_i e_i$ defines an isometry between $\ell^0_\infty(I, L)$ and B, where $\ell^0_\infty(I, L)$ is the set of sequences in L indexed by I that tend to 0 (in a sense that depends on I). One can show that every L-Banach space B with valuation v_B such that $v_B(B) = v_p(L)$ admits an orthonormal basis.

It is an easy check that $(\mu_H)_H$ is an element of the Iwasawa algebra and the resulting function $\mathscr{O}_L[[T]] \to \Lambda(\mathbf{Z}_p)$ is an inverse to the Mahler transform. □

Definition 2.12. — If $g \in \mathscr{O}_L[[T]]$, we write $\mu_g \in \Lambda(\mathbf{Z}_p)$ for the corresponding ($\mathscr{O}_L$-valued) measure on $\mathbf{Z}_p$ (so that $\mathscr{A}_{\mu_g} = g$).

Remark 2.13. — Let $g \in \mathscr{O}_L[[T]]$ with associated measure μ_g. From the definitions, it is evident that

$$\int_{\mathbf{Z}_p} \mu_g = g(0).$$

2.3. An example: Dirac measures. — In this section, we give an example of the above theory in action via Dirac measures.

Definition 2.14. — Let $a \in \mathbf{Z}_p$. The *Dirac measure* $\delta_a \in \mathscr{M}(\mathbf{Z}_p, \mathscr{O}_L)$ is the linear functional 'evaluation at a', that is, the measure defined by

$$\begin{aligned} \delta_a : \mathscr{C}(\mathbf{Z}_p, \mathscr{O}_L) &\longrightarrow \mathscr{O}_L \\ \phi &\longmapsto \phi(a). \end{aligned}$$

Under the identification of measures with additive functions on open compact subsets of $\mathbf{Z}_p$, we find that this corresponds to the function

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

as can be seen directly from the proof of the identification.

As an element of the Iwasawa algebra, again from the proof we find that at finite level δ_a corresponds to the basis element $[a + p^n\mathbf{Z}_p] \in \mathscr{O}_L[\mathbf{Z}_p/p^n\mathbf{Z}_p]$, which in the inverse limit we denote by $[a]$.

Finally, we compute the Mahler transform of δ_a. If $a \in \mathbf{Z}_p^\times$ then, by definition, this is

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

2.4. A measure-theoretic toolbox. — There are natural operations one might consider on measures, and via the Mellin transform these give rise to operators on power series. As such, the following operations can be considered as a 'toolbox' for working with measures and power series, and as we shall see in the sequel, the ability to manipulate measures in this way has important consequences. For further details (and even more operations), see **[Col10a]**.

2.4.1. *Multiplication by x.* — Given a measure μ on $\mathbf{Z}_p$, it's natural to wish to evaluate it at the function x^k for a positive integer k. To allow us to do that, we define $x\mu$ to be the measure defined by

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

We can ask what this operation does on Mahler transforms; we find:

Lemma 2.15. — *We have*

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

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

Proof. — We have

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

The result follows directly. □

From the above lemma and Remark 2.13, we immediately obtain:

Corollary 2.16. — *For $g \in \mathbf{Z}_p[[T]]$, we have*

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

2.4.2. *Multiplication by z^x.* — Let z be such that $|z-1| < 1$. Then the Mahler transform of $z^x\mu$ is

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

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

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

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

2.4.3. *Restriction to open compact subsets.* — Consider an open compact subset $X \subset \mathbf{Z}_p$. If we define $\mathbf{1}_X$ to be the characteristic function of this subset, we can consider the restriction $\mathrm{Res}_X(\mu)$ of μ to X defined by

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

In the case $X = b + p^n\mathbf{Z}_p$, we can write this characteristic function explicitly as

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

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

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

2.4.4. *Restriction to $\mathbf{Z}_p^\times$.* — From the above applied to $b = 0$ and $n = 1$, it is immediate that

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

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

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

This has Mahler transform

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

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

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

and this corresponds to $\mathscr{A}_{\varphi(\mu)} = \varphi(\mathscr{A}_\mu) := \mathscr{A}_\mu\big((1+T)^p - 1\big)$. Finally, we also define the analogous operator for p^{-1}; we define a measure $\psi(\mu)$ on $\mathbf{Z}_p$ by defining

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

Note that $\psi \circ \varphi = \mathrm{id}$, whilst

$$\varphi \circ \psi(\mu) = \mathrm{Res}_{p\mathbf{Z}_p}(\mu).$$

In particular, we have

$$\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu) = (1 - \varphi \circ \psi)(\mu). \tag{2}$$

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

$$\varphi \circ \psi(F)(T) = \frac{1}{p} \sum_{\zeta \in \mu_p} F\big((1+T)\zeta - 1\big).$$

The following result will be useful in Part II.

Corollary 2.17. — *Let $\mu \in \Lambda(\mathbf{Z}_p)$ be a measure. Then μ is supported on $\mathbf{Z}_p^\times$ if and only if $\psi(\mathscr{A}_\mu) = 0$.*

Proof. — The operator φ is easily seen to be injective. We have an injection $\iota : \Lambda(\mathbf{Z}_p^\times) \hookrightarrow \Lambda(\mathbf{Z}_p)$ given by

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

and as $\mathrm{Res}_{\mathbf{Z}_p^\times} \circ \iota$ is the identity on $\Lambda(\mathbf{Z}_p^\times)$, we can identify $\Lambda(\mathbf{Z}_p^\times)$ with its image as a subset of $\Lambda(\mathbf{Z}_p)$. If $\mu \in \Lambda(\mathbf{Z}_p)$, then $\mu \in \Lambda(\mathbf{Z}_p^\times)$ if and only if $\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu) = \mu$, or equivalently if and only if $\mathscr{A}_\mu = \mathscr{A}_\mu - \varphi \circ \psi(\mathscr{A}_\mu)$, which happens if and only if $\psi(\mathscr{A}_\mu) = 0$. □

Remark 2.18. — Whilst we identify $\Lambda(\mathbf{Z}_p^\times)$ with a subset of $\Lambda(\mathbf{Z}_p)$, it is important to remark that it is *not* a subalgebra. Indeed, convolution of measures on $\mathbf{Z}_p^\times$ uses the multiplicative group structure whilst convolution of measures on $\mathbf{Z}_p$ uses the additive group structure, so if λ and μ are two measures on $\mathbf{Z}_p^\times$, we do not have $\mu *_{\mathbf{Z}_p^\times} \lambda = \mu *_{\mathbf{Z}_p} \lambda$.

Remark 2.19. — Power series rings have been generalized 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 are examples of the basic operations we have on (φ, Γ)-modules and their interpretation with p-adic analysis inspired the proof of the p-adic Langlands correspondence for $\mathrm{GL}_2(\mathbf{Q}_p)$. For further details, see **[Col10b]**.

3. The Kubota-Leopoldt p-adic L-function

3.1. The measure μ_a. — Recall the results of the introduction: we can write the Riemann zeta function in the form

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

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 has exponential decay at infinity, so we can consider the function $L(f_a, s)$ as in the introduction. The presence of a removes the factor of $s-1$, at the cost of introducing a different smoothing factor:

Lemma 3.1. — *We have*

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

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

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

We now introduce the p-adic theory from above. Note the following very simple observation.

Lemma 3.2. — (i) *Under the substitution* $e^t = T + 1$*, the derivative* d/dt *becomes the operator* $\partial = (1 + T)\frac{d}{dT}$.

(ii) *In particular, if we define*

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

we have

$$f_a^{(k)}(0) = \big(\partial^k F_a\big)(0).$$

The right hand side in (ii) should look familiar as the expression in Corollary 2.16, which expressed the integral of the function x^k over $\mathbf{Z}_p$ in terms of its Mahler transform. So, if $F_a(T)$ can be written as an element of $\mathbf{Z}_p[[T]]$, then we will get a measure on $\mathbf{Z}_p$ that sees values of the Riemann zeta function.

Proposition 3.3. — *The function* $F_a(T)$ *is an element of* $\mathbf{Z}_p[[T]]$.

Proof. — We can expand

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

where $g(T) = \sum_{n\geq 2} \frac{1}{a}\binom{a}{n}T^{n-2}$ has coefficients in $\mathbf{Z}_p$ 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 $\mathbf{Z}_p[[T]]$. □

Definition 3.4. — Let μ_a denote the measure on $\mathbf{Z}_p$ corresponding to $F_a(T)$ under the Mahler transform.

We have proved:

Proposition 3.5. — *For* $n \geq 0$*, we have*

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

3.2. Restriction to $\mathbf{Z}_p^\times$. — Recall from the introduction that we want the p-adic analogue of the Riemann zeta function to be a measure on $\mathbf{Z}_p^\times$, not all of $\mathbf{Z}_p$. We have already defined a restriction operator in equation (2), which on Mahler transforms acts as $1 - \varphi \circ \psi$.

Proposition 3.6. — *We have*

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

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

Proof. — We first show that $\psi(\mu_a) = \mu_a$ by consider the action on power series. Indeed, we have by definition

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

as can be seen by calculating the partial fraction expansion. By injectivity of φ, we deduce that $\psi(\frac{1}{T}) = \frac{1}{T}$ and hence $\psi(\mu_a) = \mu_a$ since ψ commutes with the action of $\mathbf{Z}_p^\times$.

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

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

as required. □

3.3. Pseudo-measures. — It remains to remove the dependence on a. To do so, we need to introduce the notion of a *pseudo-measure*. The Riemann zeta function has a simple pole at $s = 1$, and pseudo-measures let us take this into account on the p-adic side. (Thus far, the presence of a has acted as a 'smoothing factor' which removes this pole).

Definition 3.7. — Let G be an abelian profinite group, and let $Q(G)$ denote the fraction field of the Iwasawa algebra $\Lambda(G)$. A *pseudo-measure* on G is an element $\lambda \in Q(G)$ such that

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

for all $g \in G$.

The following lemma shows that a pseudo-measure μ on $\mathbf{Z}_p^\times$ is uniquely determined by the values $\int_{\mathbf{Z}_p^\times} x^k \cdot \mu$ for $k > 0$.

Lemma 3.8. — (i) *Let $\mu \in \Lambda(\mathbf{Z}_p^\times)$ such that*

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

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

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

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

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

(iii) *Part (i) holds if, more generally, μ is a pseudo-measure.*

Proof. — To prove part (i), note that the vanishing condition forces the Mahler transform of μ to be constant, since each non-trivial binomial polynomial is divisible by x. But as μ is a measure on $\mathbf{Z}_p^\times$, it vanishes under ψ, so must be zero.

For part (ii), suppose there exists a measure λ such that $\mu\lambda = 0$. Then

$$0 = \int_{\mathbf{Z}_p^\times} x^k \cdot (\mu\lambda) = \Big(\int_{\mathbf{Z}_p^\times} x^k \cdot \mu \Big) \Big(\int_{\mathbf{Z}_p^\times} x^k \cdot \lambda \Big),$$

which forces $\lambda = 0$ by part (i).

Finally, let μ be a pseudo-measure satisfying the vanishing condition. Let $a \neq 1$ be an integer prime to p; then there is a natural measure

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

with $\int_{\mathbf{Z}_p^\times} f \cdot ([a]-[1]) = f(a) - f(1)$. Consider the measure $\lambda = ([a]-[1])\mu \in \Lambda(\mathbf{Z}_p^\times)$. Then λ satisfies the condition of part (i), so $\lambda = 0$. But $[a]-[1]$ satisfies the condition of part (ii), so it is not a zero-divisor, and this forces $\mu = 0$, as required. □

Definition 3.9. — Let a be an integer that is prime to p, and let $\widetilde{\theta}_a$ denote the element of $\Lambda(\mathbf{Z}_p^\times)$ corresponding to $[a]-[1]$. Note that

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \widetilde{\theta}_a = a^k - 1$$

from the definitions. Then define $\theta_a := x\widetilde{\theta_a}$, so that

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \theta_a = a^{k+1} - 1,$$

the term arising in our interpolation formula. Then define

$$\zeta_p := \frac{\mu_a}{\theta_a} \in Q(\mathbf{Z}_p^\times).$$

Proposition 3.10. — *The element ζ_p is a well-defined pseudo-measure that is independent of the choice of a.*

Proof. — The element θ_a is not a zero-divisor by Lemma 3.8, so ζ_p is well-defined. To prove independence, if a and b are two integers coprime to p, then

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

for all $k \geq 0$, so that

$$\theta_a \mu_b = \theta_b \mu_a,$$

by Lemma 3.8, giving the required independence.

Finally, the proof that ζ_p is a pseudo-measure is contained in the exercises. □

Remark 3.11. — One must take care in the above when discussing products of measures. As remarked in Remark 2.18, whilst we identify $\Lambda(\mathbf{Z}_p^\times)$ as a subset of $\Lambda(\mathbf{Z}_p)$, it is *not* a subalgebra; the convolution of measures over $\mathbf{Z}_p$ uses the additive group structure, and the convolution of measures over $\mathbf{Z}_p^\times$ the multiplicative group structure. Writing $\mu *_{\mathbf{Z}_p^\times} \lambda$ for the convolution over $\mathbf{Z}_p^\times$, we have

$$\int_{\mathbf{Z}_p^\times} x^k \cdot (\mu *_{\mathbf{Z}_p^\times} \lambda) = \int_{\mathbf{Z}_p^\times} \Big(\int_{\mathbf{Z}_p^\times} (xy)^k \cdot \mu(x) \Big) \cdot \lambda(y) = \Big(\int_{\mathbf{Z}_p^\times} x^k \cdot \mu \Big) \Big(\int_{\mathbf{Z}_p^\times} x^k \cdot \lambda \Big),$$

justifying the calculations above.

We've removed the dependence on a. We summarise the main result:

Theorem 3.12. — *There is a unique pseudo-measure ζ_p on $\mathbf{Z}_p^\times$ such that*

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

(Note that we can remove the $(-1)^{k+1}$ from the interpolation formula as $\zeta(-k) \neq 0$ if and only if k is odd).

Definition 3.13. — We call ζ_p the *Kubota–Leopoldt p-adic L-function* (or the *p-adic zeta function*).

4. Interpolation at Dirichlet characters

4.1. Characters of p-power conductor. — Throughout the construction of the Kubota–Leopoldt p-adic L-function, we've kept half an eye on the interpolation property and links to the values of the Riemann zeta function, so the interpolation of these values should not have come as a surprise. However, now some real magic happens. Since the introduction, we've failed to mention Dirichlet L-functions once – but, miraculously, the Kubota–Leopoldt p-adic L-function also interpolates Dirichlet L-values as well.

Theorem 4.1. — *Let χ be a (primitive) Dirichlet character of conductor p^n for some integer $n \geq 1$ (seen as a locally constant character of $\mathbf{Z}_p^\times$). Then, for $k > 0$, we have*

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

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

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

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

We use our measure-theoretic toolkit to determine the Mahler transform of μ_χ in terms of $\mathscr{A}_\mu$. First recall a classical definition

Definition 4.2. — Let χ be a primitive Dirichlet character of conductor p^n, $n \geq 1$. Define the *Gauss sum of* χ as

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

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

Remark 4.3. — We will make constant use of the following basic properties of Gauss sums, whose proofs are left as exercises:

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

– $G(\chi) = \chi(a)\sum_{c\in(\mathbf{Z}/p^n\mathbf{Z})^\times} \chi(c)\varepsilon_{p^n}^{ac}$ for any $a \in \mathbf{Z}_p$. Note that, if $a \notin \mathbf{Z}_p^\times$, both sides vanish.

Lemma 4.4. — *The Mahler transform of μ_χ is*

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

Proof. — Since χ is constant $(\mathrm{mod}\, p^n)$, the measure μ_χ is simply

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

Using this expression and the formula for the Mahler transform of the restriction of a measure to $c + p^n\mathbf{Z}_p$, we find that

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

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

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

where the last equality follows from the standard identity

$$\sum_{b \in (\mathbf{Z}/p^n\mathbf{Z})^\times} \chi(b)\varepsilon_{p^n}^{-bc} = \chi(-c)^{-1}G(\chi)$$

of Gauss sums. We complete the proof by using the identity $G(\chi)G(\chi^{-1}) = \chi(-1)p^n$. □

Now consider the case where $\mu = \mu_a$, 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

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

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

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

by way of analogy with the case of the Riemann zeta function.

Lemma 4.5. — *We have*

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

where $L(f_{\chi,a}, s)$ is as defined in Theorem 1.4. Hence, for $k \geq 0$, we have

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

Proof. — We follow a similar strategy as in the case of the Riemann zeta function. In particular, we can expand as a geometric series, obtaining

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

Then we have

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

Note that

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

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

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

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

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

showing the equality of L-functions. To prove the final statement about special values, observe that a simple computation shows that $f_{\chi,a}(-t) = -\chi(-1)f_{\chi,a}(t)$, which implies (looking at the series expansions) that $f^{(k)}_{\chi,a}(0) = 0$ unless $\chi(-1)(-1)^k = -1$. This concludes the proof. □

Note that, in the proof of Lemma 4.5, we have also shown the following useful fact.

Lemma 4.6. — *If χ is an even character, that is if $\chi(-1) = 1$, then $L(\chi, -k) = 0$ if k is even. If χ is an odd character, then $L(\chi, -k) = 0$ if k is odd.*

We can now prove Theorem 4.1.

Proof. — *(Theorem 4.1).* Since χ is 0 on $p\mathbf{Z}_p$, and by the above, we have

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

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

$$\big(\partial^k F_{\chi,a}\big)(0) = f^{(k)}_{\chi,a}(0),$$

under the standard transform $e^t = T + 1$. Hence, by Lemma 4.5, we find

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

By definition, we have

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

and hence we find

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

as was to be proved. □

4.2. Non-trivial 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:

Theorem 4.7. — *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 $\mu_\eta \in \Lambda(\mathbf{Z}_p^\times)$ such that, for all primitive Dirichlet characters χ with conductor p^n, $n \geq 0$, and for all $k > 0$, we have*

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

Remark 4.8. — (i) In this case, we obtain a genuine measure rather than a pseudo-measure. As L-functions of non-trivial Dirichlet characters are everywhere holomorphic, there is no need for the smoothing factor involving a.

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

Since many of the ideas involved in proving the above theorem are present in the case of trivial tame conductor, the proof of Theorem 4.7 is a good exercise. As such, we give only the main ideas involved in the proof. Note first 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; accordingly, we can perform a similar calculation in the general case. Since there is no need for the smoothing factor a, we can then consider the function

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

(This scaling by -1 also appears in the trivial tame conductor situation, but it is incorporated into θ_a). Defining $F_\eta(T)$ by substituting $T+1$ for e^t and expanding the geometric series, we find

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

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

Lemma 4.9. — *We have $L(f_\eta, s) = -\eta(-1)L(\eta, s)$. Hence*

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

for $k \geq 0$.

Proof. — This is proved in a similar manner to above, equating ∂ with d/dt and using the general theory described in Theorem 1.4. □

The measure we desire will be the restriction of μ_η to $\mathbf{Z}_p^\times$.

Lemma 4.10. — *We have $\psi(F_\eta) = \eta(p)F_\eta$. Hence*

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

Proof. — We show first that

$$\frac{1}{p} \sum_{\zeta \in \mu_p} \frac{1}{(1+T)\zeta\varepsilon_D^c - 1} = \frac{1}{(1+T)^p \varepsilon_D^{pc} - 1}. \tag{3}$$

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

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

and summing the geometric series now gives the right hand side of (3). It follows that

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

The first claim now follows by the injectivity of φ. For the second, we note that

$$\begin{aligned}\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_\eta) &= (1 - \varphi \circ \psi)(\mu_\eta) \\ &= \mu_\eta - \eta(p)\varphi(\mu_\eta),\end{aligned}$$

and

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

The result now follows simply from Lemma 4.9. □

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). Using Lemma 4.4, we find easily that:

Lemma 4.11. — *The Mahler transform of $\mu_\theta := (\mu_\eta)_\chi$ is*

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

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

$$\begin{aligned} \int_{\mathbf{Z}_p} \chi(x)x^k \cdot \mu_\eta &= \int_{\mathbf{Z}_p} x^k \cdot \mu_\theta \\ &= L(\theta, -k), \end{aligned}$$

that

$$\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_\theta) = \big(1 - \theta(p)\varphi\big)(\mu_\theta),$$

and that accordingly

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

which completes the proof.

4.3. Analytic functions on $\mathbf{Z}_p$ via the Mellin transform. — The reader should hopefully now be convinced that the language of measures is a natural one in 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 $\mathbf{Z}_p$ that interpolate the values $\zeta(-k)$ for $k \geq 0$. In passing from measures to analytic functions on $\mathbf{Z}_p$, we lose the clean interpolation statements. In particular, there is no *single* analytic function on $\mathbf{Z}_p$ interpolating the values $\zeta(-k)$ for all k; rather, there are $p-1$ different 'branches' of the Kubota–Leopoldt p-adic L-function on $\mathbf{Z}_p$, each interpolating a different range.

The reason we cannot define a single p-adic L-function on $\mathbf{Z}_p$ is down to the following technicality. We'd *like* to be able to define "$\zeta_p(s) = \int_{\mathbf{Z}_p^\times} x^{-s} \cdot \zeta_p$" for $s \in \mathbf{Z}_p$. 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 $\mathbf{Z}_p$, so this is not well-defined for general $x \in \mathbf{Z}_p^\times$. Instead:

Lemma 4.12. — *The p-adic exponential map converges on $p\mathbf{Z}_p$. Hence, for any $s \in \mathbf{Z}_p$, the function $1 + p\mathbf{Z}_p \to \mathbf{Z}_p$ 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, **[Cas86]**. □

Definition 4.13. — Recall that we assume p to be odd and that we have a decomposition $\mathbf{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbf{Z}_p)$. Let

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

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. Note that if $x \in \mathbf{Z}_p^\times$, then we can write $x = \omega(x)\langle x \rangle$.

Hence the function $\langle x \rangle^s$ is well-defined. When p is odd, for each $i = 1, .., p-1$ we can define an injection

$$\begin{aligned} \mathbf{Z}_p &\hookrightarrow \mathrm{Hom}_{\mathrm{cts}}(\mathbf{Z}_p^\times, \mathbf{C}_p^\times) \\ s &\longmapsto \big[x \mapsto \omega(x)^i \langle x \rangle^s\big], \end{aligned}$$

and hence we can define an analytic function

$$\begin{aligned}\zeta_{p,i} : \mathbf{Z}_p &\longrightarrow \mathbf{C}_p \\ s &\longmapsto \int_{\mathbf{Z}_p^\times} \omega(x)^{-i}\langle x\rangle^{-s} \cdot \zeta_p.\end{aligned}$$

This function *does not* interpolate as wide a range of values as the measure ζ_p, since the character x^k can be written in the form $\omega(x)^i\langle x\rangle^k$ if and only if $k \equiv i \pmod{p-1}$. We do, however, have:

Theorem 4.14. — *For all $k \geq 0$ with $k \equiv i \pmod{p-1}$, we have*

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

More generally:

Definition 4.15. — 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

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

Remark 4.16. —

– In the context of our previous work, the appearance of ω^{-1}, which renormalises the values by 1, seems unnatural. We have introduced it simply because this formulation is much more common in the literature. For example, in **[Was97]**, 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 will also appear when we study the Iwasawa main conjecture.

– Directly from the definitions, we have $\zeta_{p,i}(s) = L_p(\omega^{i+1}, s)$. Hence for arbitrary $k \geq 0$, we have

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

Of course, ω^{i-k} is just the trivial character when $i \equiv k \pmod{p-1}$, so we recover Theorem 4.14.

Theorem 4.17. — *For all $k \geq 1$, we have*

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

Proof. — 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

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

as required. □

More generally, for any measure μ on $\mathbf{Z}_p^\times$ we define

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

the *Mellin transform* of μ at i. So $\zeta_{p,i}(s) = \mathrm{Mel}_{\mu,-i}(-s)$.

4.4. The values at $s = 1$. — We end Part I with an example of further remarkable links between the classical and p-adic zeta functions. Let θ be a non-trivial 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. As explained above, we have

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

for $k \geq 0$; we say that the range of interpolation is $\{0, -1, -2, -3, ...\}$. It's natural to ask what happens outside this range of interpolation. In particular, what happens when we take $k = -1$? Since this is *outside* the range of interpolation this value may have *a priori* nothing to do with classical L-values. Indeed, the classical value $L(\theta, 1)$ is transcendental[(8)], and if it is transcendental one cannot see it as a p-adic number in a natural way. However, just because we cannot directly equate the two values does not mean there is no relationship between them; there is a formula for the p-adic L-function at $s = 1$ which is strikingly similar to its classical analogue.

Theorem 4.18. — *Let θ be a non-trivial even Dirichlet character of conductor N, and let ζ denote a primitive Nth root of unity. Then:*

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

$$L(\theta, 1) = -\frac{1}{G(\theta^{-1})} \sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times} \theta^{-1}(a) \log\big(1 - \zeta^a\big).$$

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

$$L_p(\theta, 1) = -\big(1 - \theta(p)p^{-1}\big)\frac{1}{G(\theta^{-1})} \sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times} \theta^{-1}(a) \log_p\big(1 - \zeta^a\big).$$

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. For completeness, we prove these results below.

4.4.1. *The complex value at $s = 1$.* —

Proof. — *(Theorem 4.18, classical value).* Write

$$L(\theta, 1) = \sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times} \theta(a) \sum_{n\equiv a \pmod D} n^{-s}.$$

Using the fact that

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

we show that the above formula equals

$$\begin{aligned}\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times} \theta(a)\frac{1}{N}\sum_{n\geq 1}\sum_{c\in(\mathbf{Z}/N\mathbf{Z})} \zeta^{(a-n)c}n^{-s} &= \frac{1}{N}\sum_{c\in(\mathbf{Z}/N\mathbf{Z})}\left(\sum_{a\in(\mathbf{Z}/N\mathbf{Z})^\times}\theta(a)\zeta^{ac}\right)\sum_{n\geq 1}\zeta^{-nc}n^{-s} \\ &= \frac{G(\theta)}{N}\sum_{c\in(\mathbf{Z}/N\mathbf{Z})}\theta^{-1}(c)\sum_{n\geq 1}\zeta^{-nc}n^{-s},\end{aligned}$$

the last equality following from one of the standard identities for Gauss sums. Evaluating this expression at $s = 1$ (checking that there is no convergence problem) and using the Taylor series expansion of the logarithm, and applying the other standard identity of Gauss sums, we obtain the result. □

(8) This follows from Baker's theorem and Theorem 4.18, part (i).

Remark 4.19. — We see from the formula above that the parity of the character θ plays an important role on the behaviour of the zeta function at $s = 1$. Making some elementary calculations we can deduce that, if θ is even, then

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

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

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

where $B_{k,\theta}$ denotes the kth twisted Bernoulli number (see [**Was97**, Chapter 4]).

4.4.2. *The p-adic value at $s = 1$.* — Recall the power series

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

which gives rise to a measure μ_θ on $\mathbf{Z}_p$ that interpolates the special values of $L(\theta, s)$. Accordingly, by the measure-theoretic arguments we've employed repeatedly above, we have

$$\begin{aligned} L_p(\theta, 1) &:= \int_{\mathbf{Z}_p^\times} x^{-1} \cdot \mu_\theta \\ &= \mathscr{A}_{\mathrm{Res}_{\mathbf{Z}_p^\times}(x^{-1}\mu_\theta)}(0). \end{aligned}$$

We first compute $\mathscr{A}_{x^{-1}\mu_\theta}$.

Lemma 4.20. — *There exists a constant C such that*

$$\mathscr{A}_{x^{-1}\mu_\theta}(T) = -\frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbf{Z}/N\mathbf{Z})^\times} \theta^{-1}(c) \log\big((1+T)\zeta^c - 1\big) + C.$$

Proof. — This follows immediately from the formula

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

and the fact that $\sum_{c \in (\mathbf{Z}/N\mathbf{Z})} \theta^{-1}(c) = 0$. □

Lemma 4.21. — *We have*

$$\mathscr{A}_{\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_\theta)}(T) = \mathscr{A}_{x^{-1}\mu_\theta}(T) - \theta(p)p^{-1}\mathscr{A}_{x^{-1}\mu_\theta}\big((1+T)^p - 1\big).$$

Proof. — This is immediate from the formula

$$\mathscr{A}_{\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_\chi)}(T) = (1 - \varphi \circ \psi)\mathscr{A}_{\mu_\chi}(T)$$

and the fact that

$$\begin{aligned} \psi(x^{-1}\mu_\theta) &= p^{-1}x^{-1}\psi(\mu_\theta) \\ &= \chi(p)p^{-1}x^{-1}\mu_\theta. \end{aligned}$$

□

We can now complete the proof of Theorem 4.18.

Proof. — *(Theorem 4.18, p-adic value).* Evaluating at $T = 0$ the formula of Lemma 4.21 and using Lemma 4.20 we obtain

$$\begin{aligned} L_p(\theta, 1) &= -(1 - \theta(p)p^{-1})\mathscr{A}_{x^{-1}\mu_\theta}(0) \\ &= -(1 - \theta(p)p^{-1})\frac{1}{G(\theta^{-1})} \sum_{c \in (\mathbf{Z}/N\mathbf{Z})^\times} \theta^{-1}(c) \log_p(\zeta^c - 1), \end{aligned}$$

as required. □

5. The p-adic family of Eisenstein series

We now 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. For simplicity, in this section we'll take p an odd prime.

Let $k \geq 4$ be an even integer. The *Eisenstein series of level k*, defined as

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

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 [**DS05**, Chapter 1.1] for details).

From the definition, we see the Kubota–Leopoldt p-adic L-function as a pseudo-measure that, when evaluated at x^k with $k \geq 4$ even, gives 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 want interpolations of the functions $d \mapsto d^{k-1}$, where k is varying p-adically. When d is coprime to p, we can define this measure simply to be δ_d, the Dirac measure at d (recalling this is defined by evaluation at d).

When d is divisible by p, however, we run into an immutable obstacle. There is no Dirac measure on $\mathbf{Z}_p^\times$ corresponding to evaluation at p, since $p \notin \mathbf{Z}_p^\times$. Moreover, the function $p \mapsto p^k$ 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

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

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

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

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 5.1. — 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

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

where

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

(The series $E_k^{(p)}$ defines a modular form of weight k and level $\Gamma_0(p)$).

We've done all the work in proving:

Theorem 5.2. — *There exists a power series*

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

such that:

(a) *A_0 is a pseudo-measure, and $A_n \in \Lambda(\mathbf{Z}_p^\times)$ for all $n \geq 1$;*

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

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

Proof. — Clearly, A_0 is simply the pseudo-measure $\zeta_p/2$. We then define

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

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

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

so we get the required interpolation property. □

Remark. —

– These results are often presented in a different (equivalent) way. One defines the *weight space*

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

and shows that, topologically, it is the union of $p-1$ open unit balls in $\mathbf{C}_p$ (centered around the $(p-1)$th roots of unity). The integers are naturally a subset of $\mathcal{W}(\mathbf{C}_p)$ via the maps $x \mapsto x^k$, and two integers k, k' lie in the same unit ball if and only if $k \equiv k' \pmod{p-1}$. This space can be given more structure; there is a rigid analytic space $\mathcal{W}$ such that the elements of $\mathcal{W}(\mathbf{C}_p)$ are the $\mathbf{C}_p$-points of $\mathcal{W}$. Giving a measure on $\mathbf{Z}_p^\times$ is equivalent to giving a bounded rigid analytic function on $\mathcal{W}$. Defining $\mathscr{O}(\mathcal{W})$ to be the space of rigid analytic functions on $\mathcal{W}$, we can view $\mathbf{E}$ as a power series in $\mathscr{O}(\mathcal{W})[[q]]$. We see it as a p-adic interpolation of the Eisenstein series over the weight space.

– The power series $\mathbf{E}(z)$ 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 p-adic families of Eisenstein series, was introduced by Serre to give a new construction of the p-adic zeta function of a totally real number field. Pioneering work of Hida went much further than this, showing that similar families (known as *Hida families*) exist for far more general modular forms, and his work has been vastly generalised to the theory of Coleman families and eigenvarieties. For a flavour of Hida's work, see his book [**Hid93**].

Part II: Iwasawa's main conjecture

This Part is devoted to the formulation and study of Iwasawa's Main Conjecture. We start by studying cyclotomic units, which will play a central role in the sequel, and by showing their relation to class numbers. We then state and prove the existence Coleman's interpolating power series. These interpolating power series and the study of their logarithmic derivatives will lead to al alternative construction of the p-adic zeta function. Although a priori more obscure, this new construction will stablish a tangible connection between units in the cyclotomic tower and the p-adic zeta function. Finally, using class field theory, we will naturally arrive to the formulation and proof of (a special case of) the Main Conjecture.

Notation. — Our study of the Iwasawa main conjecture requires a lot 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. For $n \in \mathbf{N}$, write

$$\begin{aligned} F_n &:= \mathbf{Q}(\mu_{p^n}), \quad F_n^+ := \mathbf{Q}(\mu_{p^n})^+; \\ \mathscr{V}_n &:= \mathscr{O}_{F_n}^\times, \quad \mathscr{V}_n^+ := \mathscr{O}_{F_n^+}^\times; \\ K_n &:= \mathbf{Q}_p(\mu_{p^n}), \quad K_n^+ := \mathbf{Q}_p(\mu_{p^n})^+; \\ \mathscr{U}_n &:= \mathscr{O}_{K_n}^\times, \quad \mathscr{U}_n^+ := \mathscr{O}_{K_n^+}^\times. \end{aligned}$$

The extensions $F_n/\mathbf{Q}$, $K_n/\mathbf{Q}_p$, $F_n^+/\mathbf{Q}$ and $K_n^+/\mathbf{Q}_p$ are Galois and totally ramified (the first two of degree $(p-1)p^{n-1}$ and the last two of degree $\frac{p-1}{2}p^{n-1}$) and we denote $\mathfrak{p}_n$ the unique prime ideal above the rational prime p. We note

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

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

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

given by

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

for $\sigma \in \mathrm{Gal}(F_n/\mathbf{Q})$ and $\zeta \in \mu_{p^n}$ any primitive p^nth root of unity. By infinite Galois theory, we then see that

$$\mathcal{G} = \mathrm{Gal}(F_\infty/\mathbf{Q}) := \varprojlim_n \mathrm{Gal}(F_n/\mathbf{Q}) = \varprojlim_n (\mathbf{Z}/p^n\mathbf{Z})^\times \cong \mathbf{Z}_p^\times,$$

via the *cyclotomic character* $\chi := \varprojlim \chi_n$. Observe that χ induces an isomorphism $\mathcal{G}^+ \cong \mathbf{Z}_p^\times/\{\pm 1\}$.

We also define

$$\mathscr{U}_{n,1} := \{u \in \mathscr{U}_n \ : \ u \equiv 1 \ (\mathrm{mod}\ \mathfrak{p}_n)\}, \quad \mathscr{U}_{n,1}^+ := \mathscr{U}_{n,1} \cap \mathscr{U}_n^+.$$

The subsets $\mathscr{U}_{n,1}$ and $\mathscr{U}_{n,1}^+$ are important as they have the structure of $\mathbf{Z}_p$-modules (indeed, if $u \in \mathscr{U}_{n,1}$ or $\mathscr{U}_{n,1}^+$ and $a \in \mathbf{Z}_p^\times$, 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 $\mathbf{Z}$-modules.

In general, our notations satisfy 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. In that spirit, we define

$$\mathscr{U}_\infty := \varprojlim_n \mathscr{U}_n, \quad \mathscr{U}_{\infty,1} := \varprojlim_n \mathscr{U}_{n,1};$$

$$\mathscr{U}_\infty^+ := \varprojlim_n \mathscr{U}_n^+, \quad \mathscr{U}_{\infty,1}^+ := \varprojlim_n \mathscr{U}_{n,1}^+;$$

where all limits are taken with respect to the norm maps. All of these infinite level modules are compact $\mathbf{Z}_p$-modules (since they are inverse limits of compact $\mathbf{Z}_p$-modules) and moreover they are all endowed with a natural continuous action of $\mathcal{G} = \mathrm{Gal}(F_\infty/\mathbf{Q})$ or $\mathcal{G}^+ = \mathrm{Gal}(F_\infty^+/\mathbf{Q}) = \mathcal{G}^{\{\pm 1\}}$. Accordingly, they are endowed with continuous actions of the Iwasawa algebras $\Lambda(\mathcal{G})$ or $\Lambda(\mathcal{G}^+)$ (which is the primary reason for passing to infinite level objects).

We fix once for all a compatible system of roots of unity $(\zeta_{p^n})_{n\in\mathbf{N}}$, that is, a sequence where ζ_{p^n} is a primitive p^nth root of unity such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for all $n \in \mathbf{N}$. We let $\pi_n = \zeta_{p^n} - 1$, which is a uniformiser of K_n.

6. The Coleman map

In §6.4 and §6.5, we use the identifications above to construct the *Coleman map*, which can be seen as a machine for constructing p-adic L-functions from a compatible system of units. We also explain (very!) briefly how this map can be generalised to a machine conjecturally capable of constructing p-adic L-functions for a very large class of p-adic Galois representations. Coleman's work is important as it puts the construction of the p-adic zeta function into a larger and more conceptual framework. Even more importantly, it provides an important bridge between analytic objects (p-adic L-functions) and algebraic structures (the arithmetic of cyclotomic fields), and will serve as the key step in our formulation of the main conjecture in the next section.

6.1. Notation and Coleman's theorem. — In the notational introduction to Part II, we defined

$$K_n = \mathbf{Q}_p(\mu_{p^n}), \quad K_\infty = \mathbf{Q}_p(\mu_{p^\infty})$$

to be the local versions of F_n and F_∞ from the previous section. 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 (ζ_{p^n}) of primitive p^nth roots of unity, and defined $\pi_n := \zeta_{p^n} - 1$, a uniformiser for K_n.

Proposition 6.1. — *Let $u \in \mathscr{U}_n$ be a local unit at level n. There exists a power series $f \in \mathbf{Z}_p[[T]]$ 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 $a_0 \in \mathbf{Z}_p$ such that

$$a_0 \equiv u \,(\mathrm{mod}\, \pi_n),$$

and then $a_1 \in \mathbf{Z}_p$ such that

$$a_1 \equiv \frac{u - a_0}{\pi_n} \,(\mathrm{mod}\, \pi_n),$$

and so on, and then define $f(T) = \sum_n a_n T^n$. By construction, this satisfies the required property. □

The problem with this proposition is that such a power series f is far from unique, since we had an abundance of choice at each coefficient. In the usual spirit of Iwasawa theory, Coleman realised it was possible to solve this problem by passing to the infinite tower K_∞. Recall that we defined

$$\mathscr{U}_\infty := \varprojlim_n \mathscr{U}_n,$$

where the projective limit is taken with respect to the norm maps $K_n \to K_{n-1}$. Coleman's theorem says that for each $u \in \mathscr{U}_\infty$, there is a *unique* power series f_u satisfying the condition of the above proposition for all n. A more useful formulation of this statement is:

***Theorem 6.2* (Coleman).** — *There exists a unique injective multiplicative map*

$$\begin{aligned} \mathscr{U}_\infty &\to \mathbf{Z}_p[[T]] \\ u &\mapsto f_u \end{aligned}$$

such that $f_u(\pi_n) = u_n$ for all $u \in \mathscr{U}_\infty$ and $n \geq 1$.

6.2. Example: cyclotomic units. — This theorem allows an alternative construction of the Kubota–Leopoldt p-adic L-function. In particular, let $a \in \mathbf{Z}$ prime to p, and define

$$c_n(a) := \frac{\zeta_{p^n}^a - 1}{\zeta_{p^n} - 1} \in \mathscr{U}_n.$$

Lemma 6.3. — *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 ζ_{p^n} over K_{n-1} is $X^p - \zeta_{p^{n-1}}$, we see that

$$\begin{aligned} N_{n,n-1}(\zeta_{p^n}^a - 1) &= \prod_{\eta \in \mu_p} (\zeta_{p^n}^a \eta - 1) \\ &= \zeta_{p^n}^{ap} - 1 = \zeta_{p^{n-1}}^a - 1, \end{aligned}$$

where in the penultimate equality we have used the identity $X^p - 1 = \prod_{\eta \in \mu_p}(X\eta - 1)$. The result now follows since the norm is multiplicative. □

It is possible to write down $f_{c(a)} \in \mathbf{Z}_p[[T]]$ directly by inspection; indeed, we see that

$$f_{c(a)}(T) = \frac{(1+T)^a - 1}{T}$$

satisfies the required property. (Indeed, $f_{c(a)}$ is even a polynomial).

Proposition 6.4. — *We have*

$$\partial \log f_{c(a)} = a - 1 - F_a(T),$$

where $F_a(T)$ is the power series defined in Lemma 3.2.

Proof. — We compute directly that

$$\begin{aligned} \partial \log f_{c(a)} &= \partial \log \big((1+T)^a - 1\big) - \partial \log(T) \\ &= \frac{a(1+T)^a}{(1+T)^a - 1} - \frac{T+1}{T} \\ &= a - 1 + \frac{a}{(1+T)^a - 1} - \frac{1}{T} \\ &= a - 1 - F_a(T), \end{aligned}$$

as required. □

In particular, we find that

$$(1-\varphi)\partial \log f_{c(a)} = (1-\varphi)F_a,$$

since $1-\varphi$ kills the constant term. In terms of measures, this means that the measure $\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_{f_{c(a)}})$ is equal to the measure $\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_a)$ which we used in the construction of ζ_p. Hence Coleman's isomorphism allows us to study ζ_p, and in particular the structure of $\Lambda(\mathcal{G})/\zeta_p I(\mathcal{G})$, using local units. We will see more about the units $c_n(a)$, and in particular the module in $\mathscr{U}_n$ generated by them, in the next section.

6.3. Proof of Coleman's theorem. — The proof of Theorem 6.2 will occupy the rest of this section. We begin by showing the injectivity of the map $u \mapsto f_u$.

Lemma 6.5. — *Suppose $u = (u_n) \in \mathscr{U}_\infty$ and $f, g \in \mathbf{Z}_p[[T]]$ both satisfy*

$$f(\pi_n) = g(\pi_n) = u_n$$

for all $n \geq 1$. Then $f = g$.

Proof. — The Weierstrass preparation theorem (Proposition 11.2 of the appendix) says that we can write any non-zero power series $h(T) \in \mathbf{Z}_p[[T]]$ in the form $p^m u(T) r(T)$, where $u(T)$ is a unit and $r(T)$ is a distinguished polynomial. Any such $h(T)$ converges to a function on the maximal ideal in the ring of integers of $\overline{\mathbf{Q}}_p$, 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. Lemma 6.6 and Proposition 6.7 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 6.8 will show certain continuity properties of this norm operator, which will allow us to prove the theorem by a standard diagonal argument.

Recall that the action of φ on $\mathbf{Z}_p[[T]]$ is defined by $\varphi(f)(T) = f((1+T)^p - 1)$, $f(T) \in \mathbf{Z}_p[[T]]$, and that this action is injective. Importantly, we also have

$$\varphi(f)(\pi_{n+1}) = f((\pi_{n+1}+1)^p - 1) = f(\zeta_{p^{n+1}}^p - 1) = f(\pi_n).$$

From our work with measures, we have also seen the existence of an additive operator ψ with the property that

$$(\varphi \circ \psi)(f)(T) = \frac{1}{p} \sum_{\zeta \in \mu_p} f(\zeta(1+T) - 1),$$

and that we henceforth call the *trace* operator (this terminology will become clear in the proof of Lemma 6.6). We now define a multiplicative version of this operator.

Lemma 6.6. — *There exists a unique multiplicative operator $\mathcal{N}$, the* norm *operator, such that*

$$(\varphi \circ \mathcal{N})(f)(T) = \prod_{\zeta \in \mu_p} f(\zeta(1+T) - 1).$$

Proof. — The ring $B = \mathbf{Z}_p[[T]]$ is an extension of $A = \mathbf{Z}_p[[\varphi(T)]] = \varphi(\mathbf{Z}_p[[T]])$ of degree p, the former being obtained by adjoining a pth root of $(1+T)^p$ to the latter. Each automorphism of B over A is given by $T \mapsto (1+T)\zeta - 1$ for some $\zeta \in \mu_p$. There is a norm

map

$$N_{B/A} : \mathbf{Z}_p[[T]] \longrightarrow \varphi(\mathbf{Z}_p[[T]])$$
$$f(T) \longmapsto \prod_{\zeta \in \mu_p} f((1+T)\zeta - 1).$$

The norm operator $\mathcal{N}$ is then defined to be $\varphi^{-1} \circ N_{B/A}$. (The trace operator is similarly equal to $p^{-1}\varphi^{-1} \circ \mathrm{Tr}_{B/A}$, where $\mathrm{Tr}_{B/A}$ is the trace operator for the same extension). □

Let $f \in \mathbf{Z}_p[[T]]^\times$; then $f(\pi_n) \in \mathscr{U}_n$ for all n. Suppose additionally that $\mathcal{N}(f) = f$, that is, f is invariant under the norm map. Then:

Proposition 6.7. — *For f as above, we have*

$$N_{n+1,n}\big(f(\pi_{n+1})\big) = f(\pi_n),$$

so that $(f(\pi_n))_n \in U_\infty$ is a norm compatible system of local units.

Proof. — Since the minimal equation of ζ_{n+1} over K_n is $X^p - \zeta_n = 0$, we can write the norm as

$$N_{n+1,n}\big(f(\zeta_{n+1} - 1)\big) = \prod_{\nu \in \mu_p} f(\nu\zeta_{n+1} - 1).$$

By the definition of $\mathcal{N}$, since $\mathcal{N}(f) = f$, we have $\varphi(f)(T) = \prod_{\nu\in\mu_p} f(\nu(1+T) - 1)$, so that

$$\varphi(f)(\pi_{n+1}) = \prod_{\nu \in \mu_p} f(\nu\zeta_{n+1} - 1).$$

Since $\varphi(f)(\pi_{n+1}) = f(\pi_n)$, we are done. □

Let $\mathscr{W}$ denote the subspace of $\mathbf{Z}_p[[T]]^\times$ on which $\mathcal{N}$ acts as the identity. Since the Coleman power series attached to a system of units is unique, we have an injection $\mathscr{W} \hookrightarrow \mathscr{U}_\infty$ given by evaluation at $(\pi_n)_{n\geq 1}$. To prove Theorem 6.2 it suffices to prove that this map is also surjective. We need the following lemma on the behaviour of $\mathcal{N}$ modulo powers of p.

Lemma 6.8. — *Let $f(T) \in \mathbf{Z}_p[[T]]$. We have*

(i) *If $\varphi(f)(T) \equiv 1 \pmod{p^k}$ for some $k \geq 0$, then $f(T) \equiv 1 \pmod{p^k}$.*

(ii) *For $f \in \mathbf{Z}_p[[T]]^\times$, we have*

$$\mathcal{N}(f) \equiv f \pmod{p}.$$

(iii) *For f as above, if $f \equiv 1 \pmod{p^k}$ with $k \geq 1$, then*

$$\mathcal{N}(f) \equiv 1 \pmod{p^{k+1}}.$$

(iv) *If $f \in \mathbf{Z}_p[[T]]^\times$, and $k_2 \geq k_1 \geq 0$, 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. To see part (iii), suppose that $f \equiv 1 \pmod{p^k}$ with $k \geq 1$, and let $\mathfrak{p}$ denote the maximal ideal of $K_1 = \mathbf{Q}_p(\mu_p)$. For each $\zeta \in \mu_p$, as $(\zeta - 1)(1+T) \in \mathfrak{p}\mathbf{Z}_p[[T]]$, we have

$$\zeta(1+T) - 1 \equiv T \pmod{\mathfrak{p}\mathbf{Z}_p[[T]]},$$

so that

$$f\big(\zeta(1+T) - 1\big) \equiv f(T) \pmod{\mathfrak{p}p^k\mathbf{Z}_p[[T]]}$$

by considering each term seperately. It follows that

$$\varphi \circ \mathcal{N}(f)(T) = \prod_{\zeta\in\mu_p} f\big(\zeta(1+T) - 1\big)$$
$$\equiv f(T)^p \pmod{\mathfrak{p}p^k\mathbf{Z}_p[[T]]},$$

but since both $\varphi \circ \mathcal{N}(f)$ and $f(T)^p$ are elements of $\mathbf{Z}_p[[T]]$, this is actually an equivalence modulo $\mathfrak{p}p^k \cap \mathbf{Z}_p = p^{k+1}$. 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. □

With this in hand, we can complete the proof.

Proof of Theorem 6.2. — Uniqueness and injectivity of the map was proved in Lemma 6.5. We now prove that the map $\mathscr{W} \hookrightarrow \mathscr{U}_\infty$ is surjective. Let $u = (u_n)_{n\geq 1} \in \mathscr{U}_\infty$. For each n, choose $f_n \in \mathbf{Z}_p[[T]]$ such that

$$f_n(\pi_n) = u_n$$

and define $g_n = \mathcal{N}^{2n} f_n$. One can use Lemma 6.8 to show that

$$g_m(\pi_n) \equiv u_n \pmod{p^{m+1}},$$

so that $\lim_{m\to+\infty} g_m(\pi_n) = u_n$. So it suffices to find a convergent subsequence of (g_m); but such a subsequence exists, since $\mathbf{Z}_p[[T]]$ is compact. If we let f_u denote the limit of this subsequence, then we have $f_u(\pi_n) = u_n$ for all n, proving the required existence. □

In fact, since, by construction, $\mathcal{N}(f_u) = f_u$ in the above proof, we have proved:

Theorem 6.9. — *The association $u \mapsto f_u$ induces an isomorphism*

$$\mathscr{U}_\infty \xrightarrow{\sim} (\mathbf{Z}_p[[T]]^\times)^{\mathcal{N}=1}.$$

6.4. The logarithmic derivative. — Recall Proposition 6.4. This said that if we consider the system $c(a) \in \mathscr{U}_\infty$ of cyclotomic units, and apply Theorem 6.2, then we can recover the power series $F_a(T) \in \mathbf{Z}_p[[T]]^{\psi=1}$, and hence – using the results of §3.1 – we recover the p-adic zeta function. More precisely, we showed that the *logarithmic derivative* $\partial \log$ of the Coleman power series $f_{c(a)}$ was, up to the addition of a constant, equal to $-F_a$. In this section, we put this result into a larger framework by showing that any element fixed by ψ is the logarithmic derivative of an element fixed by the norm operator.

Definition 6.10. — Define, for $f(T) \in \mathbf{Z}_p[[T]]^\times$, its logarithmic derivative as

$$\Delta(f) := \frac{\partial f(T)}{f(T)} = (1+T)\frac{f'(T)}{f(T)}.$$

The main result of this section is the following.

Theorem 6.11. — *The logarithmic derivative induces a surjection*

$$\left(\mathbf{Z}_p[[T]]^\times\right)^{\mathcal{N}=1} \to \mathbf{Z}_p[[T]]^{\psi=1}$$

with kernel μ_{p-1}.

The difficulty of the proof of Theorem 6.11 lies in the fact that, in general, the module $\mathbf{Z}_p[[T]]^{\psi=1}$ admits no simple description. We first prove (Lemma 6.12) that the image of the logarithmic derivative is contained $\mathbf{Z}_p[[T]]^{\psi=1}$ and calculate its kernel. We then reduce the proof, via Lemma 6.13, to the analogous result modulo p. Finally, in Lemma 6.14 and Lemma 6.15 we calculate the reduction modulo p of both spaces. Recall that we defined $\mathscr{W} = \left(\mathbf{Z}_p[[T]]^\times\right)^{\mathcal{N}=1}$.

Lemma 6.12. — *We have $\Delta(\mathscr{W}) \subseteq \mathbf{Z}_p[[T]]^{\psi=1}$ and the kernel of Δ on $\mathscr{W}$ is μ_{p-1}.*

Proof. — If $f \in \mathscr{W}$, then

$$\varphi(f) = (\varphi \circ \mathcal{N})(f) = \prod_{\zeta \in \mu_p} f((1+T)\zeta - 1).$$

Applying Δ to the above equality and using the fact[(9)] that $\Delta \circ \varphi = p\,\varphi \circ \Delta$, we obtain

$$(\varphi \circ \Delta)(f) = p^{-1} \sum_{\zeta \in \mu_p} \Delta(f)((1+T)\zeta - 1) = (\varphi \circ \psi)(\Delta(f)),$$

which shows that $\psi(\Delta(f)) = \Delta(f)$ by injectivity of φ. □

We move now to the proof of surjectivity. In the following, let

$$A = \overline{\Delta(\mathscr{W})} \subseteq \mathbf{F}_p[[T]]; \quad B = \overline{\mathbf{Z}_p[[T]]^{\psi=1}} \subseteq \mathbf{F}_p[[T]]$$

be the reduction modulo p of the modules we need to compare.

Lemma 6.13. — *If $A = B$, then $\Delta(\mathscr{W}) = \mathbf{Z}_p[[T]]^{\psi=1}$.*

Proof. — Let $f_0 \in \mathbf{Z}_p[[T]]^{\psi=1}$. By hypothesis, there exists a $g_1 \in \mathscr{W}$ such that $\Delta(g_1) - f_0 = pf_1$ for some $f_1 \in \mathbf{Z}_p[[T]]$. Since $\Delta(\mathscr{W}) \subseteq \mathbf{Z}_p[[T]]^{\psi=1}$ by Lemma 6.12, we deduce that $\psi(f_1) = f_1$ and hence there exists some $g_2 \in \mathscr{W}$ such that $\Delta(g_2) - f_1 = pf_2$ for some $f_2 \in \mathbf{Z}_p[[T]]$. We deduce by induction the existence of $g_i \in \mathscr{W}$ and $f_i \in \mathbf{Z}_p[[T]]^{\psi=1}$, $i \geq 1$, such that

$$\Delta(g_i) - f_{i-1} = pf_i.$$

Since $\Delta(a) = 0$ for any $a \in \mathbf{Z}_p^\times$ and since ψ is linear, we can assume that $g_i(0) \equiv 0 \pmod{p}$ for all $i \geq 1$. If we let

$$h_n = \prod_{k=1}^{n} (-1)^{k-1} (g_k)^{p^k} \in \mathscr{W},$$

then one easily checks that $\Delta(h_n) = f_0 + (-1)^{n-1} p^{n+1} f_n$. 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. □

The following lemma calculates the reduction modulo p of $\mathscr{W}$.

Lemma 6.14. — *We have $\overline{\mathscr{W}} = \mathbf{F}_p[[T]]^\times$.*

Proof. — One inclusion is obvious. Conversely, for any element $f \in \mathbf{F}_p[[T]]^\times$, lift it to an element $\tilde{f}_0 \in \mathbf{Z}_p[[T]]^\times$ and, by points (ii) and (iv) of Lemma 6.8, the sequence $\mathcal{N}^k(\tilde{f}_0)$ converges to an element $\tilde{f}$ that is invariant under $\mathcal{N}$ and whose reduction modulo p is f. □

As we pointed out, the delicate and technical part of the proof of Theorem 6.11 is contained in the following two lemmas describing the reduction of $\mathbf{Z}_p[[T]]^{\psi=1}$ modulo p.

Lemma 6.15. — *We have $B = \Delta(\mathbf{F}_p[[T]]^\times)$.*

Proof. — We have $\Delta(\mathscr{W}) \subseteq \mathbf{Z}_p[[T]]^{\psi=1}$ by Lemma 6.12, so the inclusion $\Delta(\mathbf{F}_p[[T]]^\times) \subset B$ is clear using Lemma 6.14. For the other inclusion, take any $f \in B$ and use Lemma 6.16 below to write

$$f = \Delta(a) + b$$

for some $a \in \mathbf{F}_p[[T]]^\times$ 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

(9) It is easy to see on power series using the definitions.

b. Using the identity[10] $\psi(g \cdot \varphi(f)) = \psi(g)f$, the identity $T^{pm} = \varphi(T^m)$ in $\mathbf{F}_p[[T]]$ and the fact that ψ fixes $\frac{T+1}{T}$, 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 6.16. — *We have*

$$\mathbf{F}_p[[T]] = \Delta(\mathbf{F}_p[[T]]^\times) + \frac{T+1}{T} C,$$

where $C = \{\sum_{n=1}^{+\infty} a_n T^{pn}\} \subseteq \mathbf{F}_p[[T]]$.

Proof. — One inclusion is clear. Take $g \in \mathbf{F}_p[[T]]$ 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 $\frac{T+1}{T} h \in \Delta(\mathbf{F}_p[[T]]^\times)$. Indeed, we will show by induction that, for every $m \geq 1$, there exists $\alpha_i \in \mathbf{F}_p$ for $1 \leq i < m$ such that

$$h_m := \frac{T+1}{T} h - \Big(\sum_{i=1}^{m-1} \Delta(1 - \alpha_i T^i) \Big) \in T^m \mathbf{F}_p[[T]].$$

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 $\mathbf{F}_p$, and we set $\alpha_m = -\frac{d_m}{m}$. One can then check that

$$g = \prod_{n=1}^{+\infty} (1 - \alpha_n T^n) \in \mathbf{F}_p[[T]]$$

satisfies $\Delta(g) = \frac{T+1}{T} h$, which concludes the proof. □

Corollary 6.17. — *The map* $\Delta : \mathscr{W} \to \mathbf{Z}_p[[T]]^{\psi=1}$ *is surjective.*

Proof. — By Lemma 6.13, it suffices to prove that $A = B$, which follows directly from Lemma 6.14 and Lemma 6.15. □

The above corollary finishes the proof of Theorem 6.11.

[10] Again, this can be easily checked on measures.

6.5. The Coleman map. — To continue developing Proposition 6.4, we study the restriction to $\mathbf{Z}_p^\times$ of the logarithmic derivative of a Coleman interpolating power series.

Definition 6.18. — We define the Coleman map

$$\mathrm{Col} : \mathscr{U}_\infty \longrightarrow \Lambda(\mathcal{G})$$

as the composition

$$\mathscr{U}_\infty \xrightarrow{u\mapsto f_u(T)} (\mathbf{Z}_p[[T]]^\times)^{\mathcal{N}=1} \xrightarrow{\Delta} \mathbf{Z}_p[[T]]^{\psi=1} \xrightarrow{\partial^{-1}(1-\varphi)} \mathbf{Z}_p[[T]]^{\psi=0} \xrightarrow{\mathscr{A}^{-1}} \Lambda(\mathbf{Z}_p^\times) \cong \Lambda(\mathcal{G}),$$

where the last isomorphism follows by identifying $\mathbf{Z}_p^\times$ with $\mathcal{G}$ via the cyclotomic character.

Remark 6.19. — Observe that Col can also be written as $x^{-1}\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_{\Delta(f_u)})$. The factor x^{-1} is harmless since multiplication by x^{-1} is an isomorphism on $\Lambda(\mathbf{Z}_p^\times)$. This factor will make the sequence in Theorem 6.20 below $\mathcal{G}$-equivariant. On the other hand, it corresponds precisely to the shift by 1 described in Remark 7.3 below, renormalising the p-adic zeta function to be the p-adic L-function associated to the Galois representation $\mathbf{Q}_p(1)$ so as to give the main conjecture, which will be better suited for the formulation of the main conjecture.

Here is the main theorem of this section.

Theorem 6.20. — *The Coleman map induces an exact sequence of $\mathcal{G}$-modules*

$$0 \to \mu_{p-1} \times \mathbf{Z}_p(1) \longrightarrow \mathscr{U}_\infty \xrightarrow{\mathrm{Col}} \Lambda(\mathcal{G}) \longrightarrow \mathbf{Z}_p(1) \to 0,$$

where the last map sends $\mu \in \Lambda(\mathcal{G})$ to $\int_{\mathcal{G}} \chi \cdot \mu$.

Proof. — The first map in the composition defining Col is an isomorphism by Theorem 6.9. The second map is surjective with kernel μ_{p-1} by Theorem 6.11. By Lemma 6.22, the third map has kernel $\mathbf{Z}_p$, which is the image of $(1+T)^a$ for $a \in \mathbf{Z}_p$, under Δ. This is the power series interpolating the sequence $(\zeta_{p^n}^a)_{n\geq 1}$. Accordingly, when we pull this back to $\mathscr{U}_\infty$, we get the factor[(11)]

$$\mathbf{Z}_p(1) = \{\zeta_{p^n}^a : a \in \mathbf{Z}_p\} \subset \mathscr{U}_\infty.$$

Finally, the first two maps are surjective and the third map has cokernel $\mathbf{Z}_p$ by Lemma 6.22, showing the exactness of the sequence.

In order to conclude the proof of the theorem, we need to show that the sequence is $\mathcal{G}$-equivariant. This is easy to check if we understand how $\mathcal{G} \cong \mathbf{Z}_p^\times$ acts on each of the modules involved. Let us recall these actions for the sake of clarity. Let $a \in \mathbf{Z}_p^\times$, and let $\sigma_a \in \mathcal{G}$ be such that $\chi(\sigma_a) = a$, where χ is the cyclotomic character. 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 $f(T) \in \mathbf{Z}_p[[T]]$, then

$$\sigma_a(f)(T) = f\big((1+T)^a - 1\big).$$

Then:

– We have

$$\begin{aligned}(\sigma_a f_u)(\pi_n) &= f_u((1+\pi_n)^a - 1)\\ &= f_u(\zeta_{p^n}^a - 1)\\ &= f_u(\sigma_a(\zeta_{p^n} - 1))\\ &= \sigma_a(u_n),\end{aligned}$$

so that $u \mapsto f_u(T)$ is $\mathcal{G}$-equivariant.

(11) $\mathbf{Z}_p(1) := \varprojlim \mu_{p^n}$ is a free $\mathbf{Z}_p$-module of rank 1 on which the absolute Galois group $\mathscr{G}_\mathbf{Q}$ acts by the cyclotomic character. It is an integral version of $\mathbf{Q}_p(1)$.

– If $f(T) \in \mathbf{Z}_p[[T]]^\times$, then an easy calculation on power series shows that

$$\Delta(\sigma_a(f)) = a\sigma_a(\Delta(f)).$$

– The map $(1-\varphi)$ is clearly $\mathcal{G}$-equivariant since φ commutes with σ_a.
– We have $\partial^{-1} \circ \sigma_a = a^{-1}\sigma_a \circ \partial^{-1}$ as one can easily check on measures.

Putting all that together, the $\mathcal{G}$-equivariance follows. □

Remark 6.21. — Note, again, that this sequence would *not* be $\mathcal{G}$-equivariant if we took the definition of Col to omit the operator ∂^{-1}, which might initially seem more natural.

Lemma 6.22. — *There is an exact sequence*

$$0 \to \mathbf{Z}_p \to \mathbf{Z}_p[[T]]^{\psi=1} \xrightarrow{1-\varphi} \mathbf{Z}_p[[T]]^{\psi=0} \to \mathbf{Z}_p \to 0,$$

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. Surjectivity of the last map follows, for example, from the fact that $\psi(1+T) = 0$, since

$$(\varphi \circ \psi)(1+T) = p^{-1} \sum_{\zeta^p} \zeta(1+T) = 0.$$

Let $f(T) \in \mathbf{Z}_p[[T]]^{\psi=0}$ 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 topology[(12)]) 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

$$f \in (1-\varphi)\left(\mathbf{Z}_p[[T]]^{\psi=1}\right)$$

and hence that the sequence is exact at $\mathbf{Z}_p[[T]]^{\psi=0}$. Finally, if $f(T) \in \mathbf{Z}_p[[T]]$ is not constant, then $f(T) = a_0 + a_r T^r + \ldots$ for some $a_r \neq 0$ and $\varphi(f)(T) = a_0 + p a_r T^r + \ldots \neq f(T)$, which shows that $\ker(1-\varphi) = \mathbf{Z}_p$ and finishes the proof. □

We conclude this section by the following digression on the generalisations of Coleman's map that lead to a conjectural construction (under the assumption of the existence of certain global cohomological elements) of p-adic L-functions of more general motives.

6.6. The Kummer sequence, Euler systems and p-adic L-functions. — We end this section with a disgression about how the picture described here generalizes to more general contexts. Let $\mathscr{G}_{\mathbf{Q}}$ be the absolute Galois group of $\mathbf{Q}$ and consider, for $m \geq 1$, the Kummer exact sequence

$$0 \to \mu_{p^m} \to \mathbf{G}_{\mathrm{m}} \xrightarrow{x \mapsto x^{p^m}} \mathbf{G}_m \to 0. \tag{4}$$

Evaluating at $\overline{\mathbf{Q}}$, this short exact sequence induces, for any number field F, a long exact sequence on cohomology

$$0 \to \mu_{p^m}(F) \to F^\times \xrightarrow{x \mapsto x^{p^m}} F^\times \to H^1(F, \mu_{p^m}) \to H^1(F, \overline{\mathbf{Q}}^\times).$$

Here, for any topological $\mathscr{G}_F$-module A, we write $H^1(F, A) := H^1(\mathscr{G}_F, A)$ for the Galois cohomology, that is the continuous group cohomology of $\mathscr{G}_F$. By Hilbert 90, we have $H^1(F, F^\times) = 0$. Taking inverse limits, which is exact, over $m \geq 1$, we obtain

$$F^\times \otimes \mathbf{Z}_p \cong H^1(F, \mathbf{Z}_p(1)).$$

(12) Recall: the weak topology corresponds to the (p,T)-adic topology on $\mathbf{Z}_p[[T]]$.

Explicitly, at each finite level, the isomorphism

$$F^\times \otimes \mathbf{Z}/p^n\mathbf{Z} = F^\times/(F^\times)^{p^n} \xrightarrow{\sim} H^1(\mathscr{G}_F, \mu_{p^n})$$

is given as follows. Take $a \in F^\times$ and take any $b \in \overline{\mathbf{Q}}^\times$ such that $b^{p^n} = a$. Then $c_a : \sigma \mapsto \frac{\sigma(b)}{b}$ defines a 1-coycle on $\mathscr{G}_F$ and it is a coboundary if and only if a is a p^n-th root of unity 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

$$\mathbf{c}_m := \frac{\zeta_m^{-1} - 1}{\zeta_m - 1} \in \mathscr{O}^\times_{\mathbf{Q}(\mu_m)},$$

which is a global analogue and a generalization of the cyclotomic units $c_n(-1)$ considered in Example 6.2. One can show that these elements satisfy the following relations with respect to the norm maps:

$$\mathrm{N}_{\mathbf{Q}(\mu_{m\ell})/\mathbf{Q}(\mu_m)}(\mathbf{c}_{m\ell}) = \begin{cases} \mathbf{c}_m & \text{if } \ell \mid m \\ (1-\ell^{-1})\mathbf{c}_m & \text{if } \ell \nmid m. \end{cases}$$

Using the Kummer map described below, we get elements $\mathbf{z}_m := \partial(\mathbf{c}_m) \in H^1(\mathbf{Q}(\mu_m), \mathbf{Z}_p(1))$ satisfying

$$\mathrm{cores}_{\mathbf{Q}(\mu_{m\ell})/\mathbf{Q}(\mu_m)}(\mathbf{z}_{m\ell}) = \begin{cases} \mathbf{z}_m & \text{if } \ell \mid m \\ (1-\ell^{-1})\mathbf{z}_m & \text{if } \ell \nmid m, \end{cases}$$

where we have used that Frob_ℓ acts on $\mathbf{Z}_p(1)$ simply by multiplication by ℓ. Observe also that $(1-\ell^{-1})$ is the Euler factor at ℓ of the Riemann zeta function.

Definition 6.23. — Let $V \in \mathrm{Rep}_L \mathscr{G}_\mathbf{Q}$ be a global p-adic Galois representation, which is unramified outside a finite set Σ of primes and let $T \subseteq V$ be an $\mathscr{O}_L$-lattice stable by $\mathscr{G}_\mathbf{Q}$. An *Euler system* for (V, T, Σ) is a collection of classes

$$\mathbf{z}_m \in H^1(\mathbf{Q}(\mu_m), T), \quad (m, \Sigma) = \{p\}$$

satisfying

$$\mathrm{cores}_{\mathbf{Q}(\mu_{m\ell})/\mathbf{Q}(\mu_m)}(\mathbf{z}_{m\ell}) = \begin{cases} \mathbf{z}_m & \text{if } \ell \mid m \\ P_\ell(V^*(1), \sigma_\ell^{-1})\mathbf{z}_m & \text{if } \ell \nmid m, \end{cases}$$

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 $\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})$.

By what we have mentioned before, cyclotomic units form an Euler system for the representation $\mathbf{Z}_p(1)$. These elements are at the base of Rubin's proof of the main conjecture. In general, constructing Euler systems for a Galois representation is a very difficult task, and very few examples exist at the moment. Moreover, there is no actual axiomatic study of Euler systems allowing us to study the few examples known under the same setting.

In exactly the same way, replacing $\overline{\mathbf{Q}}$ by $\overline{\mathbf{Q}}_p$ and F by a finite extension K of $\mathbf{Q}_p$, and observing that $K^\times \otimes \mathbf{Z}_p = K^\times$ since $K^\times$ is already p-adically complete, we obtain from Kummer's exact sequence (4) an isomorphism

$$K^\times \cong H^1(K, \mathbf{Z}_p(1)).$$

Taking $K = K_n$ for $n \geq 1$ in the last isomorphism of the above paragraph, and considering the inverse limit over all n, we see that there is a map

$$\mathscr{U}_\infty \longrightarrow \varprojlim_{n \geq 1} H^1(K_n, \mathbf{Z}_p(1)),$$

where the inverse limit is taken with respect to corestriction maps in Galois cohomology. We define *Iwasawa cohomology groups* by

$$H^1_{\mathrm{Iw}}(\mathbf{Q}_p, \mathbf{Q}_p(1)) := \varprojlim_{n\geq 1} H^1(K_n, \mathbf{Z}_p(1)) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p.$$

The remarks made so far allow one to reinterpret the Coleman map as a map

$$\mathrm{Col} : H^1_{\mathrm{Iw}}(\mathbf{Q}_p, \mathbf{Q}_p(1)) \to \mathscr{M}(\mathcal{G}, \mathbf{Q}_p),$$

where we recall that $\mathscr{M}(\mathcal{G}, \mathbf{Q}_p) = \Lambda(\mathcal{G}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is the space of $\mathbf{Q}_p$-valued measures on $\mathcal{G}$. The cyclotomic units $c_n(a)$ we saw earlier form what is known as an *Euler system*, a system of (global) Galois cohomology classes that are compatible under corestriction maps. By localising, the cyclotomic units give rise to an element of the Iwasawa cohomology. By combining the above with Proposition 6.4, we see that the p-adic zeta function can be obtained by evaluating Col at this Iwasawa cohomology class (and, as usual, dividing through by the measure θ_a to account for the pole).

Let now $V \in \mathrm{Rep}_L \mathscr{G}_{\mathbf{Q}_p}$ be any p-adic representation of $\mathscr{G}_{\mathbf{Q}_p}$, i.e a finite dimensional L-vector space V equipped with a continuous linear action of $\mathscr{G}_{\mathbf{Q}_p}$. As before, we define its Iwasawa cohomology groups as

$$H^1_{\mathrm{Iw}}(\mathbf{Q}_p, V) := \varprojlim_{n\geq 1} H^1(K_n, T) \otimes_{\mathscr{O}_L} L,$$

where $T \subseteq V$ denotes any $\mathscr{O}_L$-lattice of V stable under the action of the Galois group $\mathscr{G}_{\mathbf{Q}_p}$, and where 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 parts at p of Euler systems of a global p-adic representation live. Assuming that the representation is crystalline[(13)], the Coleman map has been generalized by Perrin-Riou [**PR95**]. Under some choices, she constructed *big logarithm maps*

$$\mathrm{Log}_V : H^1_{\mathrm{Iw}}(\mathbf{Q}_p, V) \to \mathscr{D}(\mathcal{G}, L),$$

where $\mathscr{D}(\mathcal{G}, L)$ denotes the space of L-valued distributions on $\mathcal{G}$ [(14)]. The map Log_V satisfies certain interpolation properties expressed in terms of Bloch-Kato's exponential and dual exponential maps and, for $V = \mathbf{Q}_p(1)$, we reobtain the Coleman map.

The general idea is that, given an Euler system for a global p-adic Galois representation, localizing it at the place p and applying Perrin-Riou's machine, one can construct a p-adic L-function for V. In a diagram:

$$\big\{\text{Euler systems}\big\} \xrightarrow{\mathrm{loc}_p} H^1_{\mathrm{Iw}}(\mathbf{Q}_p, V) \xrightarrow{\mathrm{Log}_V} \big\{p-\text{adic } L\text{-functions}\big\}.$$

See [**Col00**] for further references on this subject.

7. The Main Conjecture

In this section we will continue moving from the analytic picture we developed in Part I to a more arithmetic setting. We have already seen that cyclotomic units are intimately related to the p-adic zeta function, and in this section we will study further properties of the module generated by the cyclotomic units. In particular, we will consider the p-adic closure of the

(13) Loosely, a p-adic representation of $\mathscr{G}_{\mathbf{Q}_p}$ being *crystalline* is a condition from p-adic Hodge theory that is equivalent to an ℓ-adic representation of $\mathscr{G}_{\mathbf{Q}_p}$ (with $\ell \neq p$) being unramified.

(14) Recall that measures were interpreted as bounded rigid analytic functions on the p-adic weight space. The space $\mathscr{D}(\mathcal{G}, L)$ is precisely defined as (not necessarily bounded) rigid analytic functions. Equivalently, in terms of p-adic functional analysis, it is the continuous dual of the space of locally analytic functions (i.e continuous functions that locally admit a power series expansion).

cyclotomic units inside the local units, and show a theorem of Iwasawa calculating the exact image of this closure under the Coleman map (in terms of the p-adic zeta function). This endows the connection between cyclotomic units and the p-adic zeta function with a deeper algebraic structure. We will next use class field theory to relate these modules to Galois groups, and hence state Iwasawa's Main Conjecture. Under certain assumptions that will be proved later and, most importantly, under a crucial assumption on the prime p (which conjecturally always holds), we will provide a proof of the main conjecture.

7.1. The Λ-modules arising from Galois theory. — As in the last section, we introduce the Λ-modules that will be the protagonists of the Galois side of the main conjecture, and we urge the reader to refer back to this as these objects appear in the text. Define

$$\mathscr{M}_n := \text{maximal abelian } p\text{-extension of } F_n \text{ unramified outside the unique prime of } F_n \text{ over } p,$$

$$\mathscr{M}_n^+ := \text{maximal abelian } p\text{-extension of } F_n^+ \text{ unramified outside the unique prime of } F_n^+ \text{ over } p,$$

$$\mathscr{L}_n := \text{maximal unramified abelian } p\text{-extension of } F_n,$$

$$\mathscr{L}_n^+ := \text{maximal unramified abelian } p\text{-extension of } F_n^+,$$

and set

$$\mathscr{M}_\infty := \cup_{n\geq 1}\mathscr{M}_n = \text{maximal abelian } p\text{-extension of } F_\infty \text{ unramified outside } \mathfrak{p}$$

$$\mathscr{M}_\infty^+ := \cup_{n\geq 1}\mathscr{M}_n^+ = \text{maximal abelian } p\text{-extension of } F_\infty^+ \text{ unramified outside } \mathfrak{p}$$

$$\mathscr{L}_\infty := \cup_{n\geq 1}\mathscr{L}_n = \text{maximal unramified abelian } p\text{-extension of } F_\infty.$$

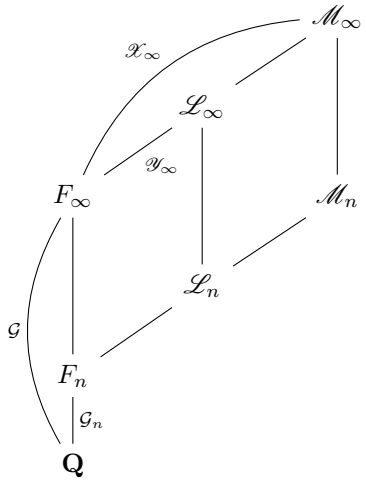
$$\mathscr{L}_\infty^+ := \cup_{n\geq 1}\mathscr{L}_n^{(+)} = \text{maximal unramified abelian } p\text{-extension of } F_\infty^+.$$

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 everything adorned by a superscript $+$).

We defer to the appendix an interpretation of these modules in terms of ideles and ideal class groups, as given by class field theory.

Remark 7.1. — Recall that $\mathcal{G} = \mathrm{Gal}(F_\infty/\mathbf{Q})$ was defined at the start of the previous section. The advantage of considering the whole cyclotomic tower instead of considering each level individually is that we get in this fashion modules over the Iwasawa algebras $\Lambda(\mathcal{G}) = \mathscr{O}_L[[\mathcal{G}]]$ and $\Lambda(\mathcal{G}^+) = \mathscr{O}_L[[\mathcal{G}^+]]$, whose structure is simpler than that of modules over $\mathscr{O}_L[\mathcal{G}_n]$ (resp. $\mathscr{O}_L[\mathcal{G}_n^+]$). Let's describe this action: take elements $\sigma \in \mathscr{X}_\infty$, $\gamma \in \mathcal{G}$ and choose any lifting $\tilde{\gamma} \in \mathrm{Gal}(\mathscr{M}_\infty/\mathbf{Q})$ of γ, then

$$\gamma \cdot x := \tilde{\gamma} x \tilde{\gamma}^{-1}$$

gives a well defined action of $\mathcal{G}$ on $\mathscr{X}_\infty$ which extends by linearity and continuity to an action of $\Lambda(\mathcal{G})$ on $\mathscr{X}_\infty$ (exercise: check these claims). In exactly the same way we define actions of $\Lambda(\mathcal{G})$ on $\mathscr{Y}_\infty$ and of $\Lambda(\mathcal{G}^+)$ on $\mathscr{X}_\infty^+$ and $\mathscr{Y}_\infty^+$. For further details on the structure of Λ-modules, where Λ is one of the Iwasawa algebras above, see the appendix.

7.2. Measures on Galois groups. — In the previous section, the fact that we can use the cyclotomic character to see the p-adic zeta function in terms of measures on $\mathcal{G}$ was heavily trailed, and we even took the Coleman map to have values in $\Lambda(\mathcal{G})$. In the process, we introduced a twist by 1, which ensured that the Coleman map was $\mathcal{G}$-equivariant. We now elaborate on this identification and conceptually explain why this twist is introduced in the context of the main conjecture. In the process, we pin down the normalisations around ζ_p that we will be using for the remainder of these notes.

Recall that $F_\infty = \cup_{n\geq 1}\mathbf{Q}(\mu_{p^n})$, that $\mathcal{G} = \mathrm{Gal}(F_\infty/\mathbf{Q}_p) \cong \mathbf{Z}_p^\times$ via the cyclotomic character, and that this isomorphism induces an identification of measures on $\mathbf{Z}_p^\times$ and measures on the Galois group $\mathcal{G}$, as has already been used in the definition of the Coleman map. Also, $\mathcal{G}^+ = \mathrm{Gal}(F_\infty^+/\mathbf{Q}) = \mathcal{G}/\langle c\rangle$ is identified through the cyclotomic character with $\mathbf{Z}_p^\times/\{\pm 1\}$.

Using this, we have the following reformulation of Theorem 3.12. The twist by 1 manifests itself in the fact that we now interpolate the values $\zeta(1-k)$ rather than $\zeta(-k)$.

Theorem 7.2. — *There exists a unique pseudo-measure ζ_p on $\mathcal{G}$ such that, for every integer $k \geq 2$, we have*

$$\int_{\mathcal{G}} \chi^k \cdot \zeta_p = (1 - p^{k-1})\zeta(1-k).$$

Remark 7.3. —

– From now on, when we write ζ_p, we mean the pseudo-measure on $\mathcal{G}$ satisfying this interpolation property (with the twist by 1), *not* the measure on $\mathbf{Z}_p^\times$ we constructed previously. We retain the notation ζ_p for ease of notation.

– Let $\mathscr{G}_\mathbf{Q} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ denote the absolute Galois group of $\mathbf{Q}$. There is a natural projection $\mathscr{G}_\mathbf{Q} \to \mathcal{G}$ given by restriction to F_∞, and if we compose χ with this projection, we get a map

$$\chi : \mathscr{G}_\mathbf{Q} \longrightarrow \mathbf{Z}_p^\times$$

that we continue to call the cyclotomic character. This allows us to define a Galois representation

$$\chi : \mathscr{G}_\mathbf{Q} \longrightarrow \mathrm{GL}(V),$$

where V is a 1-dimensional $\mathbf{Q}_p$-vector space, under $\mathbf{Z}_p^\times \subset \mathbf{Q}_p^\times = \mathrm{GL}(V)$. We write $V = \mathbf{Q}_p(1)$ for this Galois representation. Recall from the introduction that, whenever we have a global Galois representation, we can construct a complex L-function defined as an Euler product, and note that

$$L(\mathbf{Q}_p(1), s) = \zeta(s+1),$$

so rescaling the p-adic or complex zeta function corresponds to twisting the Galois representation.

– Note that in this formulation, ζ_p is precisely the p-adic L-function of the Galois representation $\mathbf{Q}_p(1)$, and this twist by 1 corresponds to the fact that we get $\zeta(s+1)$, not $\zeta(s)$. The main conjecture (as we will state it) can be viewed as a precise relation between the Selmer group and the p-adic L-function of $\mathbf{Q}_p(1)$, so it is more natural in this context to include the twist by 1.

7.2.1. *Passing to $\mathcal{G}^+$.* — Now observe that ζ_p (with the new normalisation!), which ostensibly is an element of $Q(\mathcal{G})$, 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 pseudo-measure on $\mathcal{G}^+$.

Lemma 7.4. — *Let $c \in \mathcal{G}$ denote the action of complex conjugation. Let R be a ring in which 2 is invertible and M an R-module with a continuous action of $\mathcal{G}$. Then M decomposes as*

$$M \cong M^+ \oplus M^-,$$

where c acts as $+1$ on M^+ and as -1 on M^-.

Proof. — We prove this directly by using the idempotents $\frac{1+c}{2}$ and $\frac{1-c}{2}$, which act as projectors to the corresponding M^+ and M^-. □

Since we are assuming that p is odd, we see that $\Lambda(\mathcal{G}) \cong \Lambda(\mathcal{G})^+ \oplus \Lambda(\mathcal{G})^-$ (as $\Lambda(\mathcal{G})$-modules). In fact, the module $\Lambda(\mathcal{G})^+$ admits a description solely in terms of the quotient $\mathcal{G}^+$.

Lemma 7.5. — *There is a natural isomorphism*

$$\Lambda(\mathcal{G})^+ \cong \Lambda(\mathcal{G}^+).$$

Proof. — We work at finite level. Let $\mathcal{G}_n := \mathrm{Gal}(F_n/\mathbf{Q})$, and $\mathcal{G}_n^+ := \mathrm{Gal}(F_n^+/\mathbf{Q})$. Then there is a natural surjection

$$\mathbf{Z}_p[\mathcal{G}_n] \to \mathbf{Z}_p[\mathcal{G}_n^+]$$

induced by the natural quotient map on Galois groups. Since this must necessarily map $\mathbf{Z}_p[\mathcal{G}_n]^-$ to 0, this induces a map $\mathbf{Z}_p[\mathcal{G}_n]^+ \to \mathbf{Z}_p[\mathcal{G}_n^+]$. The result now follows at finite level by a dimension count (as both are free $\mathbf{Z}_p$-modules of rank $(p-1)p^{n-1}/2$). We obtain the required result by passing to the inverse limit. □

We henceforth freely identify $\Lambda(\mathcal{G}^+)$ with the submodule $\Lambda(\mathcal{G})^+$ of $\Lambda(\mathcal{G})$.

Lemma 7.6. — *Let $\mu \in \Lambda(\mathcal{G})$. Then $\mu \in \Lambda(\mathcal{G}^+)$ if and only if*

$$\int_{\mathcal{G}} \chi(x)^k \cdot \mu = 0$$

for all odd $k \geq 1$.

Proof. — By Lemma 7.4, we can write $\mu = \mu^+ + \mu^-$, where $\mu^\pm = \frac{1 \pm \iota}{2}\mu$. We want to show that $\mu^- = 0$ if and only if $\int_{\mathcal{G}} \chi(x)^k \cdot \mu = 0$ for all odd $k \geq 1$. Since $\chi(c) = -1$, we have

$$\int_{\mathcal{G}} \chi(x)^k \cdot \mu^- = \frac{1}{2}\Big(\int_{\mathcal{G}} \chi^k \cdot \mu - (-1)^k \int_{\mathcal{G}} \chi^k \cdot \mu \Big).$$

If k is even, the above expression vanishes. The result follows then by Lemma 3.8. □

Corollary 7.7. — *The p-adic zeta function is a pseudo-measure on $\mathcal{G}^+$.*

Proof. — This follows directly from the interpolation property, as $\zeta(1-k) = 0$ precisely when $k \geq 2$ is odd. □

7.3. The main conjecture. — It is natural to ask about the zeroes of the p-adic zeta function. Since the zeroes are not modified if we multiply by a unit, studying the zeroes of a measure is equivalent to studying the ideal generated by it. Recall that, even if ζ_p is not a measure but a pseudo-measure, the elements $([\sigma]-1)\zeta_p$, $\sigma \in \mathcal{G}$, belong to the Iwasawa algebra $\Lambda(\mathcal{G})$.

Definition 7.8. — Let $I(\mathcal{G})$ denote the *augmentation ideal* of $\Lambda(\mathcal{G})$, that is, the ideal

$$I(\mathcal{G}) = \mathscr{O}_L\text{-span of } \{[\sigma]-1 : \sigma \in \mathcal{G}\}.$$

Similarly, define $I(\mathcal{G}^+)$ to be the $\mathscr{O}_L$-span of $[\sigma]-1$ for $\sigma \in \mathcal{G}^+$.

Remark 7.9. — The Iwasawa algebra $\Lambda(\mathcal{G})$ is the completed group ring $\mathscr{O}_L[[\mathcal{G}]]$, and elements can be written as 'power series' of the form $\sum_{g\in\mathcal{G}} c_g[g]$. There is a natural degree map

$$\begin{aligned} \deg : \Lambda(\mathcal{G}) &\longrightarrow \mathscr{O}_L, \\ \sum_{g\in\mathcal{G}} c_g[g] &\longmapsto \sum_{g\in\mathcal{G}} c_g, \end{aligned}$$

and $I(\mathcal{G})$ is simply the kernel of this map.

Proposition 7.10. — *The module $I(\mathcal{G})\zeta_p$ is an ideal in $\Lambda(\mathcal{G})$. Similarly, the module $I(\mathcal{G}^+)\zeta_p$ is an ideal in $\Lambda(\mathcal{G}^+)$.*

Proof. — Since ζ_p is a psuedo-measure, we know $([g]-[1])\zeta_p \in \Lambda(\mathcal{G})$ for all $g \in \mathcal{G}$. Hence the result follows from the definition of $I(\mathcal{G})$. The same argument holds for $I(\mathcal{G}^+)\zeta_p$. □

Recall that $\mathscr{M}_\infty^+$ denotes the maximal abelian p-extension of F_∞^+ which is unramified outside the unique prime of F_∞^+ above p and $\mathscr{X}_\infty^+ = \mathrm{Gal}(\mathscr{M}_\infty^+/F_\infty^+)$ is endowed with an action of $\Lambda(\mathcal{G}^+)$. Recall the definition of the characteristic ideal $\mathrm{ch}_{\Lambda(\mathcal{G}^+)}(X)$ of a $\Lambda(\mathcal{G}^+)$-module X, as given in the appendix. We have then:

***Theorem 7.11* (Iwasawa Main Conjecture).** — *The module $\mathscr{X}_\infty^+$ is a finitely generated torsion $\Lambda(\mathcal{G}^+)$-module and we have*

$$\mathrm{ch}_{\Lambda(\mathcal{G}^+)}(\mathscr{X}_\infty^+) = I(\mathcal{G}^+)\zeta_p.$$

Remark 7.12. — It is usual in the literature to formulate Iwasawa main conjecture in terms of an even Dirichlet character of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$. 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 [**HK03**].

We intend to provide a proof of the main conjecture for primes not dividing the class number of the field $\mathbf{Q}(\mu_p)^+$. The arguments of this section form the origins of Iwasawa's formulation of the main conjecture, and should also be seen as motivation for it. Its complete proof involves much more sophisticated techniques: there are at least two proofs of it, each one showing one divisibility between the two modules and invoking the analytic class number formula to deduce the other one. One of them (explained in [**CS06**]) uses the theory of Euler systems, and we hope that this text will facilitate the reader's eventual study of this method.

7.4. Cyclotomic units. — We now return to cyclotomic units, and in particular study the subgroup generated by them in the (local and global) unit groups. In the global case, this subgroup has finite index in the whole unit group $\mathscr{V}_n$. Since the determination of the units of a number field is in general a difficult problem, and cyclotomic units provide a partial answer in the case of cyclotomic fields, they are objects of classical interest and have been extensively studied.

Definition 7.13. — 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 $\{\pm\zeta_{p^n}, \zeta_{p^n}^a - 1 : 1 \leq a \leq p^n - 1\}$. We set $\mathscr{D}_n^+ = \mathscr{D}_n \cap F_n^+$.

Recall we defined

$$c_n(a) := \frac{\zeta_{p^n}^a - 1}{\zeta_{p^n} - 1} \in \mathscr{D}_n,$$

and note that

$$\xi_{n,a} := \zeta_{p^n}^{(1-a)/2} c_n(a)$$

is an element of $\mathscr{D}_n^+$. In fact:

Lemma 7.14. — *Let $n \geq 1$. Then*

(1) *The group $\mathscr{D}_n^+$ is generated by -1 and*

$$\left\{\xi_{n,a} \ : \ 1 < a < \frac{p^n}{2}, (a,p) = 1\right\}.$$

(2) *The group $\mathscr{D}_n$ is generated by ζ_{p^n} and $\mathscr{D}_n^+$.*

Proof. — We first show that we need only consider those elements $\zeta_{p^n}^a - 1$ with a prime to p. Indeed, this follows from the identity

$$\zeta_{p^n}^{bp^m} = \prod_{j=0}^{p^m-1} (\zeta_{p^n}^{b+jp^{n-k}} - 1),$$

where $(b,p) = 1$ and $k \geq 1$, and noting that $b + jp^{n-k}$ is prime to p. Also, since $\zeta_{p^n}^a - 1 = -\zeta_{p^n}^a(\zeta_{p^n}^{-a} - 1)$, we can restrict to considering $1 \leq a \leq \frac{1}{2}p^n$.

So suppose that

$$\xi = \pm\zeta_{p^n}^d \prod_{\substack{1 \leq a < \frac{1}{2}p^n \\ (a,p)=1}} (\zeta_{p^n}^a - 1)^{e_a} \in \mathscr{D}_n,$$

for some integers d and e_a. Since $v_p(\zeta_{p^n}^d) = 0$ and all the p-adic valuations of $\zeta_{p^n}^a - 1$ coincide (namely, $v_p(\zeta_{p^n}^a - 1) = \frac{1}{(p-1)p^{n-1}}$), we deduce that $\sum_a e_a = 0$. Therefore we can write

$$\xi = \pm\zeta_{p^n}^d \prod_a \left(\frac{\zeta_{p^n}^a - 1}{\zeta_{p^n} - 1}\right)^{e_a} = \pm\zeta_{p^n}^e \prod_a \xi_{n,a}^{e_a},$$

where $e = d + \frac{1}{2}\sum_a e_a(a-1)$. This shows the second point and the first point follows by observing that every term $\xi_{n,a}^{e_a}$ of the product is real, so $\xi \in \mathscr{D}_n^+$ if and only if $e = 0$. □

Corollary 7.15. — *Let a be a generator of $(\mathbf{Z}/p^n\mathbf{Z})^\times$. Then ξ_a generates $\mathscr{D}_n^+$ as a $\mathbf{Z}[\mathcal{G}_n^+]$-module.*

Proof. — Indeed, for any integer $1 \leq b < p^n$ prime to p, $b \equiv a^r \pmod{p}$ for some $r \geq 0$, and hence

$$\xi_{n,b} = \prod_{i=0}^{r-1} (\xi_{n,b})^{\sigma_b^i}.$$

□

As we have already suggested, the group $\mathscr{D}_n$ (resp. $\mathscr{D}_n^+$) of cyclotomic units is of finite index in the group of units $\mathscr{V}_n$ (resp. $\mathscr{V}_n^+$) of F_n (resp. F_n^+), and this index turns out to be a class number.

Definition 7.16. — For $n \geq 1$, we write

$$h_n^+ := \#\mathrm{Cl}(F_n^+)$$

for the class number of F_n^+.

Proposition 7.17. — *Let $n \geq 1$. The group $\mathscr{D}_n$ (resp. $\mathscr{D}_n^+$) is of finite index in the group of units of F_n (resp. F_n^+) and we have*

$$h_n^+ = [\mathscr{V}_n : \mathscr{D}_n] = [\mathscr{V}_n^+ : \mathscr{D}_n^+]$$

Proof. — The result follows by showing that the regulator of cyclotomic units is given in terms of special L-values at $s = 1$ of Dirichlet L-functions and by the class number formula. See [**Was97**, Theorem 8.2]. □

7.5. On a theorem of Iwasawa. — We will calculate the image under the Coleman map of the p-adic closure of the module of cyclotomic units inside local units.

Definition 7.18. — For any $n \geq 1$, define $\mathscr{C}_n$ as the p-adic closure of $\mathscr{D}_n$ inside the local units $\mathscr{U}_n$, let $\mathscr{C}_n^+ := \mathscr{C}_n \cap \mathscr{U}_n^+$, and let

$$\mathscr{C}_{n,1} := \mathscr{C}_n \cap \mathscr{U}_{n,1}, \quad \mathscr{C}_{n,1}^+ := \mathscr{C}_n^+ \cap \mathscr{U}_{n,1};$$

$$\mathscr{C}_{\infty,1} := \varprojlim_{n \geq 1} \mathscr{C}_{n,1}, \quad \mathscr{C}_{\infty,1}^+ := \varprojlim_{n \geq 1} \mathscr{C}_{n,1}^+.$$

Remark 7.19. — As we have pointed out whilst defining notation at the beginning of the previous chapter, the process of considering elements congruent to 1 modulo the maximal ideal and taking the p-adic closure allows us to consider the modules $\mathscr{C}_{\infty,1}$ and $\mathscr{C}_{\infty,1}^+$ as $\Lambda(\mathcal{G})$ and $\Lambda(\mathcal{G}^+)$-modules respectively.

Observe that, as a consequence of Corollary 7.15, we easily deduce the following result.

Lemma 7.20. — *The module $\mathscr{C}_{\infty,1}^+$ is a cyclic $\Lambda(\mathcal{G}^+)$-module generated by $(u\xi_{n,a})_{n\geq 1}$, where $a \in \mathbf{Z}$ is a topological generator of $\mathbf{Z}_p^\times$ (for example, take a to be a primitive root modulo p such that $a^{p-1} \neq 1 \ (mod\ p)$) and $u \in \mu_{p-1}$ is such that $au \equiv 1 \ (mod\ p)$.*

Here is the main result of this section, putting the link between cyclotomic units and the p-adic zeta function into a deeper algebraic structure.

Theorem 7.21. — *The Coleman map induces:*

(1) *An isomorphism of $\Lambda(\mathcal{G}^+)$-modules*

$$\mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ \xrightarrow{\sim} \Lambda(\mathcal{G}^+)/I(\mathcal{G}^+)\zeta_p.$$

(2) *A short exact sequence of $\Lambda(\mathcal{G})$-modules*

$$0 \to \mathscr{U}_{\infty,1}/\mathscr{C}_{\infty,1} \to \Lambda(\mathcal{G})/I(\mathcal{G})\zeta_p \to \mathbf{Z}_p(1) \to 0.$$

Proof. — Consider the exact sequence of $\Lambda(\mathcal{G})$-modules of Theorem 6.20:

$$0 \to \mu_{p-1} \times \mathbf{Z}_p(1) \longrightarrow \mathscr{U}_\infty \xrightarrow{\mathrm{Col}} \Lambda(\mathcal{G}) \longrightarrow \mathbf{Z}_p(1) \to 0.$$

Since $\mathscr{U}_\infty = \mu_{p-1} \times \mathscr{U}_{\infty,1}$, we can rewrite the above as

$$0 \to \mathbf{Z}_p(1) \longrightarrow \mathscr{U}_{\infty,1} \xrightarrow{\mathrm{Col}} \Lambda(\mathcal{G}) \longrightarrow \mathbf{Z}_p(1) \to 0.$$

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 7.14, it suffices to calculate the image under Col of an element $(\zeta_{p^n}^b \xi_{n,a})_{n\geq 1} \in \mathscr{U}_{\infty,1}$, for $a, b \in \mathbf{Z}_p^\times$. But this has already been done: by Proposition 6.4, and the fact that $\zeta_{p^n}^b$ lies in the kernel of the Coleman map, we know that

$$\mathrm{Col}\big((\zeta_{p^n}^b \xi_{n,a})_{n\geq 1}\big) = \mathrm{Col}\left(\zeta_{p^n}^{(1-a)/2}(\xi_{n,a})_{n\geq 1}\right) = \mathrm{Col}\big(c(a)\big) = ([\sigma_a]-1)\zeta_p,$$

where as usual σ_a denotes an element of $\mathcal{G}$ such that $\chi(\sigma_a) = a$. Since $a \in \mathbf{Z}_p^\times$ was arbitrary, we conclude that the image of $\mathscr{C}_{\infty,1}$ (resp. $\mathscr{C}_{\infty,1}^+$) under Col is $I(\mathcal{G})\zeta_p$ (resp. $I(\mathcal{G}^+)\zeta_p$). We deduce an exact sequence

$$0 \to \mathscr{U}_{\infty,1}/\mathscr{C}_{\infty,1} \longrightarrow \Lambda(\mathcal{G})/I(\mathcal{G})\zeta_p \longrightarrow \mathbf{Z}_p(1) \to 0.$$

This shows the second point. Since p is odd, taking invariants under the group $\langle c\rangle \subset \mathcal{G}$ of order two generated by complex conjugation is exact. As c acts on $\mathbf{Z}_p(1)$ by -1, we see that $\mathbf{Z}_p(1)^{\langle c\rangle} = 0$, which shows the first point and concludes the proof of the theorem. □

Remark 7.22. — For the purposes of the main conjecture, we will be restricting to the first point of Theorem 7.21 above.

7.6. An application of class field theory. — We next use class field theory to reinterpret Theorem 7.21 in terms of some modules arising from Galois theory.

Definition 7.23. — For any $n \geq 1$, define $\mathscr{E}_n$ as the p-adic closure of $\mathscr{V}_n$ inside the local units $\mathscr{U}_n$, let $\mathscr{E}_n^+ := \mathscr{E}_n \cap \mathscr{U}_n^+$, and let

$$\mathscr{E}_{n,1} := \mathscr{E}_n \cap \mathscr{U}_{n,1}, \quad \mathscr{E}_{n,1}^+ := \mathscr{E}_n^+ \cap \mathscr{U}_{n,1};$$

$$\mathscr{E}_{\infty,1} := \varprojlim_{n\geq 1} \mathscr{E}_{n,1}, \quad \mathscr{E}_{\infty,1}^+ := \varprojlim_{n\geq 1} \mathscr{E}_{n,1}^+.$$

We have the following result, connecting units in the cyclotomic tower and modules coming from Galois theory.

Proposition 7.24. — *There is an exact sequence of $\Lambda(\mathcal{G}^+)$-modules*

$$0 \to \mathscr{E}_{\infty,1}^+ \to \mathscr{U}_{\infty,1}^+ \to \mathrm{Gal}(\mathscr{M}_\infty^+/\mathscr{L}_\infty^+) \to 0.$$

Proof. — By Proposition 10.5 of the appendix, we know that, if $\mathscr{M}_n^+$ (resp. $\mathscr{L}_n^+$) denotes the maximal abelian p-extension of K_n^+ unramified outside p (resp. everywhere), then $\mathrm{Gal}(\mathscr{M}_n^+/\mathscr{L}_n^+) = \mathscr{U}_{n,1}/\mathscr{E}_{n,1}$. This gives an exact sequence

$$0 \to \mathscr{E}_{n,1} \to \mathscr{U}_{n,1} \to \mathrm{Gal}(\mathscr{M}_n^+/\mathscr{L}_n^+) \to 0.$$

By taking inverse limits, which is exact since all modules in the short exact sequence above are finitely generated $\mathbf{Z}_p$-modules (and hence satisfy the Mittag-Leffler condition), we deduce the result. □

Having in mind that the Coleman map induces an isomorphism of $\Lambda(\mathcal{G}^+)$-modules between $\mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+$ and $\Lambda(\mathcal{G}^+)/I(\mathcal{G}^+)\zeta_p$, we rewrite the above result as follows.

Corollary 7.25. — *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. — This is an immediate consequence of Proposition 7.24. □

7.7. Some consequences of Iwasawa theory. — We will now state some classical results from Iwasawa theory that will be proved later and show how we can deduce from them the main conjecture assuming that the prime p does not divide the class number of the field $\mathbf{Q}(\mu_p)^+$.

Proposition 7.26. — *If $p \nmid h_1^+$ then $p \nmid h_n^+$ for any $n \geq 1$.*

Proof. — Recall that $\mathrm{Cl}(F_1^+) \otimes_{\mathbf{Z}} \mathbf{Z}_p = \mathrm{Gal}(\mathscr{L}_1^+/F_1^+)$ and $p \nmid \#\mathrm{Cl}(F_1^+)$ translates into $\mathscr{L}_1^+ = F_1^+$. By the control result of lemma 8.7 of the next section, we have, for all $n \geq 0$,

$$(\mathscr{Y}_\infty^+)_{\mathcal{G}_n^+} = \mathrm{Gal}(\mathscr{L}_n^+/F_n^+),$$

where we recall that $\mathcal{G}_n^+ = \mathrm{Gal}(F_\infty^+/F_n^+)$. We deduce that, if $p \nmid h_1^+$, then $(\mathscr{Y}_\infty^+)_{\mathcal{G}_0} = 0$. By Nakayama's lemma (cf. Lemma 8.8 below), this implies that $\mathscr{Y}_\infty^+ = 0$. We conclude that $\mathrm{Gal}(\mathscr{L}_n^+/F_n^+) = 0$ for all $n \neq 1$, i.e., $p \nmid h_n^+$, which finishes the proof. □

Corollary 7.27. — *Assume $p \nmid h_1^+$. Then*

$$\mathscr{Y}_\infty^+ = \mathscr{E}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ = 0.$$

Proof. — We have already seen in the proof of Proposition that $\mathscr{Y}_\infty^+ = 0$. We now show that $\mathscr{E}_{\infty,1}^+ = \mathscr{C}_{\infty,1}^+$. In Proposition 7.17 we saw that $[\mathscr{V}_n^+ : \mathscr{D}_n^+] = h_n^+$, which is prime to p by the previous proposition. Note now that $\mathscr{D}_{n,1}^+$ and $\mathscr{V}_{n,1}^+$ are the kernels of the reduction maps modulo p; moreover, the image of $\mathscr{D}_n^+ \pmod p$ is contained inside the image of $\mathscr{V}_n^+ \pmod p \subset \mathbf{F}_p^\times$, so we conclude that the index of $\mathscr{D}_{n,1}^+$ inside $\mathscr{V}_{n,1}^+$ divides $(p-1)h_n^+$. 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 by hypothesis. Tensoring the above exact sequence with $\mathbf{Z}_p$, we get

$$\mathscr{D}_{n,1}^+ \otimes_{\mathbf{Z}} \mathbf{Z}_p \cong \mathscr{V}_{n,1}^+ \otimes_{\mathbf{Z}} \mathbf{Z}_p.$$

Recall now 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 $\mathscr{C}_{n,1}^+ \subseteq \mathscr{E}_{n,1}^+$. Since we have natural surjections $\mathscr{D}_{n,1}^+ \otimes_{\mathbf{Z}} \mathbf{Z}_p \to \mathscr{C}_{n,1}^+$ and $\mathscr{V}_{n,1}^+ \otimes_{\mathbf{Z}} \mathbf{Z}_p \to \mathscr{E}_{n,1}^+$, we conclude that the inclusion $\mathscr{C}_{n,1}^+ \to \mathscr{E}_{n,1}^+$ is a surjection, which finishes the proof. □

We can now easily finish the proof of Iwasawa Main Conjecture when $p \nmid h_1^+$.

Theorem 7.28. — *if $p \nmid h_1^+$, we have an isomorphism of $\Lambda(\mathcal{G}^+)$-modules*

$$\mathscr{X}_\infty^+ \cong \Lambda(\mathcal{G}^+)/I(\mathcal{G}^+)\zeta_p.$$

In particular, Iwasawa's main conjecture holds.

Proof. — By Corollary 7.25 and Corollary 7.27, we have

$$\mathscr{X}_\infty^+ \cong \mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+.$$

By Theorem 7.21, we have $\mathscr{U}_{\infty,1}^+/\mathscr{C}_{\infty,1}^+ \cong \Lambda(\mathcal{G}^+)/I(\mathcal{G}^+)\zeta_p$, and we deduce

$$\mathscr{X}_\infty^+ \cong \Lambda(\mathcal{G}^+)/I(\mathcal{G}^+)\zeta_p.$$

In particular,

$$ch_{\Lambda(\mathcal{G}^+)}(\mathscr{X}_\infty^+) = ch_{\Lambda(\mathcal{G}^+)}\big(\Lambda(\mathcal{G}^+)/I(\mathcal{G}^+)\zeta_p\big) = I(\mathcal{G}^+)\zeta_p,$$

which finishes the proof. □

Remark 7.29. — Recall that a regular prime is a prime such that $p \nmid h_1$. A prime p such that $p \nmid h_1^+$ is called a Vandiver prime and that there are infinitely many irregular primes. Conjecturally, every prime is a Vandiver prime.

8. Iwasawa's μ-invariant

We turn finally to the study of some classical Iwasawa theory. We introduce the μ and λ-invariants of a $\mathbf{Z}_p$-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 7.25 are finitely generated torsion modules over the Iwasawa algebra. This completes the proof of the main conjecture given in the last section for a Vandiver prime. (Other than this rather peripheral appearence, however, the main conjecture does not appear again in this section, which is largely independent of the rest of these notes).

The following results will hold for an arbitrary $\mathbf{Z}_p$-extension of number fields, although we will only prove them under some hypotheses that slightly simplify the proofs.

Definition 8.1. — Let F be a number field. A $\mathbf{Z}_p$-extension F_∞ of F is a a Galois extension such that $\mathrm{Gal}(F_\infty/F) \cong \mathbf{Z}_p$.

If F_∞/F is a $\mathbf{Z}_p$-extension, we denote F_n the sub-extension fixed by the unique subgroup of Γ with quotient $\mathbf{Z}/p^n/Z$. Recall first that any number field has at least one $\mathbf{Z}_p$-extension, the *cyclotomic extension.* Indeed, consider the fields $F(\mu_{p^n})$, and let

$$F(\mu_{p^\infty}) = \bigcup_{n\geq 1} F(\mu_{p^n}).$$

By Galois theory $\mathrm{Gal}(F(\mu_{p^\infty})/F)$ is an open subgroup of $\mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \cong \mathbf{Z}_p^\times$, and hence contains a maximal quotient isomorphic to $\mathbf{Z}_p$ (specifically, the quotient by the finite torsion subgroup). The corresponding field (under the fundamental theorem of Galois theory) is the cyclotomic $\mathbf{Z}_p$-extension.

Definition 8.2. — Let F_∞/F be a $\mathbf{Z}_p$-extension. For each n, let F_n be the unique subextension of F_∞/F such that

$$\mathrm{Gal}(F_n/F) \cong \mathbf{Z}/p^n\mathbf{Z}.$$

Example 8.3. — Let $F = \mathbf{Q}(\mu_p)$. Then $F_\infty = \mathbf{Q}(\mu_{p^\infty})$ is the cyclotomic $\mathbf{Z}_p$-extension of F, and

$$F_n = \mathbf{Q}(\mu_{p^{n+1}}).$$

(Note that earlier we denoted this field F_{n+1}). The cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ is the field $F_\infty^{\mu_{p-1}}$, the fixed field in F_∞ of the torsion subgroup $\mu_{p-1} \subset \mathrm{Gal}(F_\infty/\mathbf{Q})$.

Leopoldt's conjecture states that the number of independent $\mathbf{Z}_p$-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 $\mathbf{Z}_p$-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 $\mathbf{Q}$ or and abelian extension of an imaginary quadratic field (See [**NSW99**, Theorem 10.3.16]).

8.1. Iwasawa's theorem. — Let F be a number field, F_∞/F a $\mathbf{Z}_p$-extension, $\Gamma = \Gamma_F = \mathrm{Gal}(F_\infty/F) \cong \mathbf{Z}_p$ and γ_0 a topological generator of Γ_F. Using this choice of γ_0, we identify $\Lambda(\Gamma)$ with $\Lambda := \mathbf{Z}_p[[T]]$ by sending γ_0 to $T+1$ (when γ_0 is sent to 1 by the isomorphism $\Gamma \cong \mathbf{Z}_p$, 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. F_∞), write

$$\mathscr{Y}_{F,n} = \mathscr{Y}_n := \mathrm{Gal}(\mathscr{L}_n/F_n) = \mathrm{Cl}(F_n) \otimes \mathbf{Z}_p,$$

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 8.4* (Iwasawa).** — *There exists an integer n_0 and integers $\lambda \geq 0$, $\mu \geq 0$, $\nu \geq 0$, all independent of n, such that, for all $n \geq n_0$, we have*

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

Remark 8.5. —

– This is 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 on the proof of Theorem 8.4. 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 (in the appendix), we study the situation at infinite level, and then we transfer the result back to finite level to get the result.

– 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 [**Was97**, §13]. This assumption covers our cases of interest; in particular, it applies if $F = \mathbf{Q}(\mu_{p^m})$ or $F = \mathbf{Q}(\mu_{p^m})^+$ for some $m \geq 0$ and F_∞/F is the cyclotomic $\mathbf{Z}_p$-extension.

8.1.1. *First step.* — The first step of the proof of Theorem 8.4 consists in showing (Proposition 8.9) that the module $\mathscr{Y}_\infty$ is a finitely generated $\Lambda(\Gamma)$-module. Then Lemma 8.7 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 $\mathscr{Y}_\infty$ is equipped with the natural Galois action of $\Lambda = \Lambda(\Gamma)$, and under the identification $\Lambda \cong \mathbf{Z}_p[[T]]$, the polynomial $1 + T \in \Lambda$ acts as $\gamma_0 \in \Gamma$.

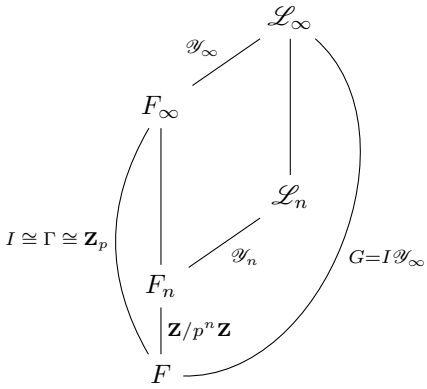
Let $\tilde{\mathfrak{p}}$ be the prime of $\mathscr{L}_\infty$ above $\mathfrak{p}$, and write

$$I \subseteq G := \mathrm{Gal}(\mathscr{L}_\infty/F)$$

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 $I \cong \Gamma$.

Lemma 8.6. — *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 $x, y \in \mathscr{Y}_\infty$. A straightforward calculation, using the definition of the $\Lambda(\Gamma)$ structure of $\mathscr{Y}_\infty$, shows that

$$aba^{-1}b^{-1} = (x^\alpha)^{1-\beta}(y^\beta)^{\alpha-1}.$$

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 $c \in \mathbf{Z}_p$, 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 nth power of the Frobenius operator on $\mathbf{Z}_p[[T]]$ is given by $\varphi^n(T) = (1+T)^{p^n} - 1$. Let $\varphi^0(T) = T$.

Lemma 8.7. — *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

$$\begin{aligned}\mathscr{Y}_0 &= G/\langle G', I\rangle \\ &= \mathscr{Y}_\infty I/\langle(\gamma_0 - 1)\mathscr{Y}_\infty, I\rangle \\ &= \mathscr{Y}_\infty/(\gamma_0 - 1)\mathscr{Y}_\infty = \mathscr{Y}_\infty/T\mathscr{Y}_\infty.\end{aligned}$$

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 is a Λ-module finitely generated, whose standard proof is left as an exercise.

***Lemma 8.8* (Nakayama's lemma).** — *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 $\mathbf{Z}$, 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 8.9. — *$\mathscr{Y}_\infty$ 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 $\mathscr{Y}_\infty/\varphi(T)\mathscr{Y}_\infty = \mathscr{Y}_1 = \mathrm{Cl}(F_1) \otimes \mathbf{Z}_p$, the p-Sylow subgrop of $\mathrm{Cl}(F_1)$, which is finite. Therefore, applying Lemma 8.8, we conclude that $\mathscr{Y}_\infty$ is a finitely generated Λ-module, as desired. □

8.1.2. *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 11.5) 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

$$\mathscr{A} = \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{k_j}) \Big).$$

for some integers $s, r, t \geq 0$, $m_i, k_j \geq 0$ 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 8.10. — *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. — 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 stabilize for n large enough, which is what is needed to conclude the proof. We leave the details of these calculations as an exercise. □

We now proceed to calculate the size of the module $\mathscr{A}$.

Lemma 8.11. — *Let*

$$\mathscr{A} = \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{k_j}) \Big),$$

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. — First observe that, since $\mathscr{A}/\varphi^n(T)$ is assumed to be finite and $\Lambda/\varphi^n(T)$ is infinite (use the division algorithm of Proposition 11.2), we deduce that $r = 0$.

We now deal with the second summand. Let $V = \Lambda/p^k$ for some $k \geq 1$. Since $\varphi^n(T) = T^{p^n} + \sum_{k=1}^{p^n-1} \binom{p^n}{k} T^k$ is distinguished, we have

$$|V/\varphi^n(T)| = |\Lambda/(p^k, T^{p^n})| = p^{kp^n},$$

where the last equality follows again by the division algorithm of Proposition 11.2. We deduce from this that

$$\left|\bigoplus_{i=1}^{s}\Lambda/(p^{m_i})\right| = p^{mp^n},$$

where $m = \sum_i m_i$.

Finally, we deal with the last summand. Let $g(T) \in \mathscr{O}_L[T]$ be a distinguished polynomial of degree d (that is not necessarily irreducible) and let $V = \Lambda/(g(T))$. Hence $T^d \equiv pQ(T) \bmod g$ for some $Q \in \mathscr{O}_L[T]$ so that $T^k \equiv p\,(\text{poly}) \bmod g$ for all $k \geq d$, where (poly) denotes some polynomial in $\mathscr{O}_L[T]$. For $p^n \geq d$, we deduce that

$$\begin{aligned}
\varphi^n(T) &= p\,(\text{poly}) + T^{p^n} \equiv p\,(\text{poly}) \bmod g.\\
\varphi^{n+1}(T) &\equiv p^2\,(\text{poly}) \bmod g.\\
\varphi^{n+2}(T) &= ((1+T)^{(p-1)p^{n+1}} + \ldots + (1+T)^{p^{n+1}} + 1)\varphi^{n+1}(T)\\
&\equiv p(1+p\,(\text{poly}))\varphi^{n+1}(T) \bmod g.
\end{aligned}$$

Since $((1+p\,(\text{poly})) \in \Lambda^\times$, we deduce that $\frac{\varphi^{n+2}(T)}{\varphi^{n+1}(T)}$ acts as p times a unit on $V = \Lambda/(g(T))$ and hence

$$\varphi^{n+2}(T)V = p\varphi^{n+1}(T)V.$$

Therefore

$$|V/\varphi^{n+2}(T)V| = |V/pV|\;|pV/p\varphi^{n+1}(T)V|.$$

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 $|pV/\varphi^{n+1}(T)V|$. Since $(g(T), p) = 1$, multiplication by p is injective on V and hence $|pV/p\varphi^{n+1}(T)V| = |V/\varphi^{n+1}(T)V|$. Fix one n_0 such that $p^{n_0} \geq d$. Then, using the identity

$$\varphi^{n+1}(T) = \frac{\varphi^{n+1}(T)}{\varphi^n(T)} \circ \ldots \circ \frac{\varphi^{n_0+2}(T)}{\varphi^{n_0+1}(T)} \circ \varphi^{n_0+1}(T)$$

and the fact that $\frac{\varphi^{k+1}(T)}{\varphi^k(T)}$ act on V as $p\,(\text{unit})$ for any $k > n_0$, we deduce that $\varphi^{n+1}(T)$ acts on V as $p^{(n-n_0-1)}\varphi^{n_0+1}(T)$ and hence

$$|V/\varphi^{n+1}(T)V| = p^{d(n-n_0-1)}|V/\varphi^{n_0+1}(T)V|.$$

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

$$\left|\bigoplus_{j=1}^{t}\Lambda/(f_j(T)^{k_j})\right| = p^{\ell n+c},$$

where $\ell = \sum_j k_j \deg(f_j)$ and some constant c. This finishes the proof of the proposition. □

Along the way, we have proven the following fact.

Corollary 8.12. — *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 8.11, 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 8.4.

Proof of Theorem 8.4. — Applying Lemma 8.10 and Lemma 8.11, 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. □

8.2. Some consequences of Iwasawa's theorem. — We have already seen one application of Iwasawa's theorem (Proposition 7.7) during the statement of the main conjecture. Namely if one class number in a $\mathbf{Z}_p$-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

$$\mathrm{rk}_p(A) = \dim_{\mathbf{F}_p}(A/pA) = \dim_{\mathbf{F}_p}(A[p]).$$

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 8.13. — *Let F_∞/F be a $\mathbf{Z}_p$-extensions. Then $\mu = 0$ if and only if $\mathrm{rk}_p(\mathrm{Cl}(F_n))$ is bounded independently of n.*

Proof. — Recall that

$$\mathrm{Cl}(F_n) \otimes \mathbf{Z}_p = \mathscr{Y}_n := \mathscr{Y}_\infty/(\varphi^n(T)),$$

that $\mathscr{Y}_\infty = \varprojlim \mathscr{Y}_n$ is quasi-isomorphic to a Λ-module $\mathscr{A} = \big(\bigoplus_{i=1}^s \Lambda/(p^{m_i})\big) \oplus \big(\bigoplus_{j=1}^t \Lambda/(g_j(T))\big)$ 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 (cf. the proof of Lemma 8.11) 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 suffices then to show that $\mu = 0$ if and only if $\dim_{\mathbf{F}_p}(\mathscr{A}_n/p\mathscr{A}_n)$ is bounded independently of n.

We have

$$\mathscr{A}/p\mathscr{A}_n = \mathscr{A}/(p, \varphi^n(T)) = \Big(\bigoplus_{i=1}^s \Lambda/(p, \varphi^n(T))\Big) \oplus \Big(\bigoplus_{j=1}^t \Lambda/(p, g_j(T), \varphi^n(T))\Big).$$

Take n big 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

$$\Big(\bigoplus_{i=1}^s \Lambda/(p, T^{p^n})\Big) \oplus \Big(\bigoplus_{j=1}^t \Lambda/(p, T^{\deg(g_j)})\Big) = (\mathbf{Z}/p\mathbf{Z})^{sp^n+tg},$$

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 8.14* (Ferrero-Washington).** — *If F is an abelian number field and F_∞/F is the cyclotomic $\mathbf{Z}_p$-extension of F, then $\mu = 0$.*

Proof. — The above theorem is proved by reducing the problem, using the duality coming from Kummer theory, to calculating the μ-invariant (i.e. the p-adic valuation) of some p-adic Dirichlet functions, which can be done explicitly from the constructions that we have given. See [**Was97**, §7.5]. □

Finally, the following is an open conjecture of Greenberg (see [**Gre76**]).

Conjecture 8.15 **(Greenberg).** — *For any totally real field F, and any $\mathbf{Z}_p$-extension F_∞/F, we have $\mu = \lambda = 0$. In other words, the values $\#\mathrm{Cl}(F_n)$ are bounded as n goes to $+\infty$.*

Appendix

9. The complex class number formula

Let $K/\mathbf{Q}$ be an abelian extension[15] of degree $d = [K : \mathbf{Q}]$. By the Kronecker-Weber theorem, $K \subseteq \mathbf{Q}(\mu_m)$ for some minimal positive integer m. Recall the definition of the Dedekind zeta function $\zeta_K(s)$ of K; this has an Euler product

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N\mathfrak{p}^s}\right)^{-1},$$

where the product runs over all primes in the ring of integers of K. Since K is abelian, it corresponds to a finite group X of Dirichlet characters of conductor m; these are precisely the characters of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ that factor through $\mathrm{Gal}(K/\mathbf{Q})$ [**Was97**, §3]. From [**Was97**, Theorem 4.3], we have a decomposition

$$\zeta_K(s) = \prod_{\chi \in X} L(\chi, s),$$

Looking at the residues at $s = 1$ of the above equality, one obtains the following alternative formulation of Theorem 1.2 from the introduction:

***Theorem 9.1* (Class Number Formula).** — *Let r_1 (resp. r_2), h_K, R, w, and D denote, respectively, the number of real (resp. complex) embeddings, the class number, the regulator, the number of roots of unity and the discriminant of the field K. Then we have*

$$\frac{2^{r_1}(2\pi)^{r_2} h_K R}{w|D|^{1/2}} = \prod_{\chi \neq 1} L(\chi, 1).$$

In particular, if K is real, we get the formula

$$\frac{h_K R}{|D|^{1/2}} = \prod_{\chi \neq 1} \frac{1}{2} L(\chi, 1).$$

If K is a CM field, then let h^+, R^+, and $d^+ = d/2 = r_2$ denote the class number, the regulator and the degree respectively of its maximal totally real subfield K^+. Let $Q = [\mathscr{O}_K^\times : \mu(K)\mathscr{O}_{K^+}^\times]$ be Hasse's unit index (which is equal to either 1 or 2; see [**Was97**, Theorem 4.12]). Decomposing the formula of Proposition 9.1 and using the formulas of Remark 4.19 one obtains the following:

Proposition 9.2. — *Let K be any CM abelian number field. Then we have*

$$h = h^+ Q w \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi}.$$

Define

$$h^- := h/h^+ = Q w \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi}.$$

Note that the above gives an easily computable product formula for h^- that has dispensed with the transcendental terms of the regular class number formula.

[15] We will only be using the following results when $K = \mathbf{Q}(\mu_m)$ or $K = \mathbf{Q}(\mu_m)^+$.

10. Class field theory

We recall some necessary basic statements of class field theory. Let K be a number field and denote by $\mathscr{O}$ its ring of integers. Denote by $K_\infty^\times = (K \otimes \mathbf{R})^\times = \prod_{v|\infty} K_v^\times$ the group of archimedean units of K and, for every finite place $\mathfrak{l}$ of K, denote by $\mathscr{O}_\mathfrak{l}^\times$ the units of the localisation $K_\mathfrak{l}$ of K at $\mathfrak{l}$. If $v \mid \infty$, we just let $\mathscr{O}_v = K_v^\times$.

Definition 10.1. — The idèles of K are defined as the restricted product

$$\mathbf{A}_K^\times := \prod_v{}' K_v^\times = \big\{\big(x_\infty, (x_\mathfrak{l})_\mathfrak{l}\big) : x_\infty \in K_\infty^\times,\ x_\mathfrak{l} \in \mathscr{O}_\mathfrak{l}^\times \text{ for all but finitely many } \mathfrak{l}\big\},$$

where the product runs over all places of K and $\mathfrak{l}$ over its finite places.

We equip $\mathbf{A}_K^\times$ with a topology, where a basis of open neighbourhoods of the identity is given by $U = \prod_v U_v = \prod_{v|\infty} U_v \times \prod_{\mathfrak{l}\text{ finite}} U_\mathfrak{l}$ such that $U_v \subseteq K_v^\times$ is open and $U_\mathfrak{l} = \mathscr{O}_\mathfrak{l}$ for almost all $\mathfrak{l}$, which makes $\mathbf{A}_K^\times$ a locally compact topological group. The global units $K^\times$ of K are diagonally embedded into $\mathbf{A}_K^\times$ and have discrete image.

Definition 10.2. — The quotient $\mathbf{C}_K := K^\times \backslash \mathbf{A}_K^\times$ is called the *idèle class group* of K.

If E/K is a finite extension and $\mathfrak{P}$ is a prime of E above a prime $\mathfrak{p}$ of K, then the norm maps $N_{E_\mathfrak{P}/K_\mathfrak{p}} : E_\mathfrak{P} \to K_\mathfrak{p}$ define a map

$$N_{E/K} : \mathbf{A}_E^\times \to \mathbf{A}_K^\times$$

sending $E^\times$ to $K^\times$ and hence inducing a map between idèle class groups. The main statements of global class field theory can be stated in the following way.

***Proposition 10.3* (Global Class Field Theory).** — *Let K be a number field. Then finite abelian extensions are in bijective correspondence with open subgroups of $\mathbf{C}_K$ of finite index. Precisely, if E/K is any finite abelian extension, then*

$$\mathrm{Gal}(E/K) \cong \mathbf{C}_K / N_{E/K}\mathbf{C}_E;$$

and, conversely, for every such finite index open subgroup H of $\mathbf{C}_K$ there exists a unique finite abelian extension E of K with $N_{E/K}\mathbf{C}_E = H$. Moreover, a place v of K is unramified in E if any only if $\mathscr{O}_v^\times \subseteq N_{E/K}\mathbf{C}_E$.

Remark 10.4. — Let K^{ab} be the maximal abelian extension of K. Passing to the limit in the above theorem, one gets an isomorphism between $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and the profinite completion of $\mathbf{C}_K$. In particular, continuous characters of $\mathbf{C}_K$ biject with continuous characters of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

We will give two examples. Let K be a number field and let $\mathscr{H}_K$ be its Hilbert class field, i.e. its maximal abelian unramified extension. By the above theorem, the extension $\mathscr{H}_K/K$ corresponds to the subgroup $K^\times\widetilde{\mathscr{U}_K}$ of $\mathbf{C}_K$, where $\widetilde{\mathscr{U}_K} = \prod_v \mathscr{O}_v^\times$, and we therefore have

$$\mathrm{Gal}(\mathscr{H}_K/K) = \mathbf{A}_K^\times / K^\times \widetilde{\mathscr{U}_K}.$$

As usual, there is a natural map $\mathbf{A}_K^\times \to \{\text{ideals of } K\}$, sending $(x_v)_v$ to $\prod_{\mathfrak{l}\text{ finite}} \mathfrak{l}^{v_\mathfrak{l}(x_\mathfrak{l})}$, which is surjective and whose kernel is exactly $\widetilde{\mathscr{U}_K}$, and hence induces an isomorphism $\mathbf{C}_K/\widetilde{\mathscr{U}_K} \cong \mathrm{Cl}(K)$ between the quotient of the idèle class group and the ideal class group of K. We conclude that

$$\mathrm{Gal}(\mathscr{H}_K/K) \cong \mathrm{Cl}(K).$$

Let now

$$\mathscr{M}_K = \text{maximal abelian } p\text{-extension of } K \text{ unramified outside every prime } \mathfrak{p} \mid p;$$

$$\mathscr{L}_K = \text{maximal unramified abelian } p\text{-extension of } K.$$

Note that $\mathscr{L}_K/K$ is a subextension of the finite extension $\mathscr{H}_K/K$, and by definition, we have

$$\begin{aligned}\mathrm{Gal}(\mathscr{L}_K/K) &= \mathrm{Gal}(\mathscr{H}_K/K)\otimes \mathbf{Z}_p \\ &\cong \mathrm{Cl}(K)\otimes \mathbf{Z}_p = p\text{-Sylow subgroup of } \mathrm{Cl}(K).\end{aligned}$$

Let $\mathscr{U}_K = (\mathscr{O}\otimes\mathbf{Z}_p)^\times = \prod_{\mathfrak{p}|p}\mathscr{O}_\mathfrak{p}^\times$ be the local units of K at p and let $\mathscr{E}_K$ be the p-adic closure of the image $\mathscr{V}_K$ of $\mathscr{O}^\times$ inside $\mathscr{U}_K$ (diagonally embedded).

Proposition 10.5. — *We have*

$$\mathrm{Gal}(\mathscr{M}_K/\mathscr{L}_K) = \mathscr{U}_K/\mathscr{E}_K.$$

Proof. — Define

$$\mathscr{U}_K^{(p)} = \prod_{v\nmid p}\mathscr{O}_v^\times, \quad \widetilde{\mathscr{U}_K} = \mathscr{U}_K\times\mathscr{U}_K^{(p)},$$

(where $\mathscr{O}_v^\times = K_v^\times$ if v is an archimedean place). By class field theory, we have

$$\mathrm{Gal}(\mathscr{M}_K/K) = \mathbf{A}_K^\times/H,$$

where $H = \overline{K^\times\mathscr{U}_K^{(p)}}$, and the subgroup of $\mathrm{Gal}(\mathscr{M}_K/K)$ corresponding to $\mathscr{L}_K$ is

$$\begin{aligned}J'' = K^\times\widetilde{\mathscr{U}_K}/H &\cong \mathscr{U}_K H/H \\ &\cong \mathscr{U}_K/(\mathscr{U}_K\cap H).\end{aligned}$$

Observe that we are considering all the modules inside the idèle class group and that the inclusion of $\mathscr{E}_K$ inside $\mathbf{A}_K^\times$ is not the inclusion induced by $K^\times\subseteq\mathbf{A}_K^\times$: the first inclusion has trivial components at places away from p, while the last inclusion is the diagonal one. For the sake of clarity, we will note

$$\iota : \mathscr{V}_K \to \mathbf{A}_K^\times$$

the inclusion induced by $\mathscr{V}_K\subseteq\mathscr{E}_K\subseteq\mathscr{U}_K\subseteq\mathbf{A}_K^\times$ and we are going to see any global unit inside the idèles by the diagonal embedding.

We now claim that $\mathscr{U}_K\cap H = \mathscr{E}_K$. One inclusion is clear, since clearly $\iota(\mathscr{V}_K)\subseteq\mathscr{U}_K$ and, if $x\in\mathscr{V}_K$, we can write $\iota(x) = x\,(\iota(x)/x)\in K^\times\mathscr{U}_K^{(p)}$, which shows that $\iota(\mathscr{V}_K)\subseteq K^\times\mathscr{U}_K^{(p)}$ and we conclude by taking the closure on both sides of the inclusion (recall that $\mathscr{E}_K = \overline{\iota(\mathscr{V}_K)}$ by definition). To prove that $\mathscr{U}_K\cap H\subseteq\mathscr{E}_K$, define, for every $n\geq 1$, the subgroup $\mathscr{U}_{K,n} = \prod_{\mathfrak{p}|p}1+\mathfrak{p}^n\mathscr{O}_\mathfrak{p}$. Observe that the sets $K^\times\mathscr{U}_K^{(p)}\mathscr{U}_{K,n}$ (resp. $\iota(\mathscr{V}_K)\mathscr{U}_{K,n}$), for $n\geq 1$, define a cofinal subset of closed neighbourhoods of $K^\times\mathscr{U}_K^{(p)}$ (resp. $\iota(\mathscr{V}_K)$) and that

$$\overline{K^\times\mathscr{U}_K^{(p)}} = \bigcap_{n\geq 1}K^\times\mathscr{U}_K^{(p)}\mathscr{U}_{K,n}, \quad \mathscr{E}_K = \bigcap_{n\geq 1}\iota(\mathscr{V}_K)\mathscr{U}_{K,n},$$

so it suffices to prove $K^\times\mathscr{U}_K^{(p)}\mathscr{U}_{K,n}\subseteq\iota(\mathscr{V}_K)\mathscr{U}_{K,n}$ for every n. Let $x\in K^\times, u'\in\mathscr{U}_K^{(p)}, u\in\mathscr{U}_{K,n}$ be such that $xu'u\in\mathscr{U}_K$. So in particular $xu'\in\mathscr{U}_K$. Since u' has component 1 at all primes $\mathfrak{p}\mid p$, then x must be a unit at those primes. Since any element in $\mathscr{U}_K$ has component 1 at all primes $v\nmid p$ and $xu'\in\mathscr{U}_K$, then x must be a unit at all those primes. Hence x is a global unit. Now observe that, at primes above p, we have $xu' = x\in\mathscr{V}_K$ (since it has component 1 at any place above p), and at primes outside p, $xu' = 1$, so we conclude that $xu'\in\iota(\mathscr{V}_K)$, hence $xu'u\in\iota(\mathscr{V}_K)\mathscr{U}_{K,n}$, which concludes the proof of the proposition. □

11. Power series and Iwasawa algebras

In this section we state and give references for some basic yet fundamental results on Iwasawa algebras and the structure theory of modules over $\Lambda(\mathbf{Z}_p)$.

Fix a finite extension $L/\mathbf{Q}_p$ and denote $\mathscr{O}_L$, $\mathfrak{p}|p$, $\pi = \pi_L$ and $k = k_L$ its ring of integers, its maximal ideal, a uniformizer and its fraction field respectively.

Definition 11.1. — A polynomial $P(T) \in \mathscr{O}_L[T]$ is called distinguished if $P(T) = a_0 + a_1T + \ldots + a_{n-1}T^{n-1} + T^n$ with $a_i \in \mathfrak{p}$ for every $0 \leq i \leq n-1$.

The following two results are some of the main tools in dealing with power series.

Proposition 11.2. — *Let $f(T) = \sum_{i\geq 0} a_i T^i \in \mathscr{O}_L[[T]]$ and assume that $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$ and that $a_n \in \mathscr{O}_L^\times$. Then:*

– (Division algorithm) For every $g(T) \in \mathscr{O}_L[[T]]$ there exist unique $q(T) \in \mathscr{O}_L[[T]]$ and $r(T) \in \mathscr{O}_L[T]$, where r has degree at most $n-1$, such that

$$g(T) = q(T)f(T) + r(T).$$

– (Weierstrass Preparation Theorem) The power series f may be uniquely written in the form

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

where $U(T) \in \mathscr{O}_L[[T]]$ is a unit and $P(T) \in \mathscr{O}_L[T]$ is a distinguished polynomial of degree n.

Proof. — See [**Was97**, Proposition 7.2; Theorem 7.3]. □

Let

$$\Lambda = \varprojlim \mathscr{O}_L[\mathbf{Z}_p/p^n\mathbf{Z}_p] \cong \mathscr{O}_L[[T]]$$

be the Iwasawa algebra (identifying $\Lambda(\mathbf{Z}_p)$ with $\mathscr{O}_L[[T]]$ using the Mahler transform and dropping $\mathbf{Z}_p$ from the notation, as is standard). As we have seen, this ring is hugely important. Most of the ideas surrounding Iwasawa theory rely on the fact that one has a structure theorem for finitely generated modules over Λ.

Proposition 11.3. — *The prime ideals of Λ are exactly 0, (π, T), (π) and ideals $(P(T))$ where $P(T)$ is an irreducible distinguished polynomial. Moreover, Λ is a local Noetherian ring with maximal ideal (π, T).*

Proof. — See [**Was97**, Proposition 13.9; Lemma 13.11] □

Let M, M' be two Λ-modules. We say that M is pseudo-isomorphic to M', and we write $M \sim M'$, if there exists a homomorphism $M \to M'$ with finite kernel and co-kernel, 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!).

Remark 11.4. — Note that $\sim$ is *not* an equivalence relation. In particular, $M \sim M'$ does not imply $M' \sim M$. For example, $(\pi, T) \sim \Lambda$, but $\Lambda \not\sim (\pi, T)$ (see [**Was97**, §13.2]). This problem goes away if we restrict to the case where M and M' are finitely generated torsion Λ-modules.

The following is the main result concerning the structure theory of finitely generated Λ-modules, and says that Λ almost behaves as if it was a principal ideal domain.

Theorem 11.5. — *Let M be a finitely generated Λ-module. Then*

$$M \sim \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}) \Big),$$

for some integers $r, s, t \geq 0$, $n_i, m_j \geq 1$ and irreducible distinguished polynomials $f_j(T) \in \mathscr{O}[T]$.

Proof. — See [**Was97**, Theorem 13.12]. □

Remark 11.6. — We do *not* have a similar result for the finite level group algebras $\mathscr{O}_L[\mathbf{Z}_p/p^n\mathbf{Z}_p]$, only for the projective limit. A fundamental concept in Iwasawa theory is the idea that it is easier to study a tower of p-extensions all in one go, and use results about the tower to deduce results at finite level, and a major reason for this is this structure theorem.

Definition 11.7. — 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

$$\mathrm{Ch}_\Lambda(M) = \prod_{i=i}^{s} (p^{n_i}) \prod_{j=1}^{t} \left(f_j^{m_j} \right) \subset \Lambda.$$

The above definition generalizes slightly to other groups other than those isomorphic to $\mathbf{Z}_p$. Let $\mathcal{G} = H \times \Gamma \cong \mathbf{Z}_p$, were H is a finite commutative group of order prime to p and $\Gamma \cong \mathbf{Z}_p$. Then we have a decomposition

$$\Lambda(\mathcal{G}) \cong \mathscr{O}_L[G] \otimes \Lambda.$$

Let M be a finitely generated torsion $\Lambda(\mathcal{G})$-module. Let $H^\wedge$ denote the group of characters of H and define, for any $\omega \in H^\wedge$,

$$e_\omega := \frac{1}{|H|} \sum_{a \in H} \omega^{-1}(a)[a] \in \mathscr{O}_L[H].$$

Lemma 11.8. — *The group H acts on $M^{(\omega)} := e_\omega M$ via multiplication by ω and we have a decomposition of $\Lambda(\mathcal{G})$-modules*

$$M = \oplus_{\omega \in H^\wedge} M^{(\omega)}.$$

Moreover, each $M^{(\omega)}$ is a finitely generated torsion Λ-module.

Proof. — See [**CS06**, A.1] or the exercises. □

In view of the above lemma, we we have the following definition.

Definition 11.9. — Let $\mathcal{G}$ be as above and let M be a finitely generated torsion $\Lambda(\mathcal{G})$-module. We define the *characteristic ideal* of M to be the ideal

$$\mathrm{Ch}_{\Lambda(\mathcal{G})}(M) := \oplus_{\omega \in H^\wedge} \mathrm{Ch}_\Lambda(M^{(\omega)}) \subseteq \Lambda(\mathcal{G}).$$

We will be using the following a basic property of characteristic ideals:

Lemma 11.10. — *The characteristic ideal is multiplicative in exact sequences.*

Proof. — See [**CS06**, A.1 Proposition 1] □

References

[Bel09] Joël Bellaïche. An introduction to the conjecture of Bloch and Kato. 2009. Unpublished.

[BSW17] Daniel Barrera Salazar and Chris Williams. Exceptional zeros and $\mathcal{L}$-invariants of Bianchi modular forms. *Trans. Amer. Math. Soc.*, 2017. To appear.

[Cas86] J. W. S. Cassels. *Local Fields*. London Mathematical Society Student Texts. Cambridge University Press, 1986.

[Col] Pierre Colmez. La fonction zeta p-adique, notes du cours de M2. Unpublished notes.

[Col00] P. Colmez. Fonctions L p-adiques. *Astérisque*, (266):Exp. No. 851, 3, 21–58, 2000. Séminaire Bourbaki, Vol. 1998/99.

[Col10a] Pierre Colmez. Fonctions d'une variable p-adique. *Asterisque*, 330:13–59, 2010.

[Col10b] Pierre Colmez. Représentations de $\mathrm{GL}_2(\mathbf{Q}_p)$ et (φ, Γ)-modules. *Asterisque*, 330:281–509, 2010.

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

[Dar01] Henri Darmon. Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications. *Ann. of Math.*, 154:589–639, 2001.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228. Graduate Studies in Mathematics, 2005.

[Gre76] Ralph Greenberg. On the Iwasawa invariants of totally realy number fields. *Amer. J. Math.*, 98(1):263–284, 1976.

[GZ86] Benedict Gross and Don Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84:225–320, 1986.

[Hid93] Haruzo Hida. *Elementary theory of L-functions and Eisenstein series*, volume 26 of *LMS Student Texts*. Cambridge University Press, 1993.

[HK03] Annette Hubber and Guido Kings. Bloch-Kato conjecture and main conjecture of Iwasawa theory for Dirichlet characters. *Duke Mat. J.*, 119, no. 3:393–464, 2003.

[Iwa52] Kenkichi Iwasawa. Some properties of L-groups. *Proceedings of the International Congress of Mathematicians, Cambridge Mass., 1950*, 1952.

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

[Kol88] Victor Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $Ш(E/\mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk. USSR ser. Matem.*, 52, 1988. In Russian.

[Lan90] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, 1990.

[Loe14] David Loeffler. P-adic integration on ray class groups and non-ordinary p-adic L-functions. In T. Bouganis and O Venjakob, editors, *Iwasawa 2012: State of the art and recent advances*, volume 7 of *Contributions in Mathematical and Computational Sciences*, pages 357 – 378. Springer, 2014.

[MM91] M. Ram Murty and V. Kumar Murty. Mean values of derivatives of modular L-series. *Ann. of Math.*, 133:447–475, 1991.

[MTT86] Barry Mazur, John Tate, and Jeremy Teitelbaum. On p-adic analogues of the Birch and Swinnerton-Dyer conjecture. *Invent. Math.*, 84:1 – 48, 1986.

[MW84] Barry Mazur and Andrew Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[NSW99] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Springer, 1999.

[PR95] B. Perrin-Riou. Fonctions L p-adiques des représentations p-adiques. *Astérisque*, (229):198, 1995.

[Rub00] Karl Rubin. *Euler Systems*. Annals of Mathematics Studies. Princeton University Press, 2000.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa Main Conjectures for GL(2). *Invent. Math.*, 195 (1):1–277, 2014.

[Tat50] John Tate. *Fourier analysis in number fields and Hecke's zeta functions*. PhD thesis, Princeton, 1950.

[Was97] Larry Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate texts in mathematics*. Springer, 1997. 2nd Edition.

Joaquín Rodrigues Jacinto, University College of London • *E-mail :* ucahrod@ucl.ac.uk

Chris Williams, Imperial College • *E-mail :* christopher.williams@imperial.ac.uk