A Journey Through Iwasawa Theory

Ketelaars, Niels

Niels Ketelaars

A Journey Through Iwasawa Theory

Master thesis

July 3, 2023

Thesis supervisor: dr. Jan B. Vonk

Leiden University
Mathematical Institute

Contents

Notation

Throughout this thesis, there are certain fields, groups and modules which occur time and time again. For the convenience of the reader, we have collected the notations used for these in this chapter.

We work with an *odd* prime p. Associated to this prime, we consider the following fields:

$$\begin{aligned} F_n &= \mathbf{Q}(\zeta_{p^{n+1}}), & F_n^+ &= \mathbf{Q}(\zeta_{p^{n+1}} + \zeta_{p^{n+1}}^{-1}) \\ K_n &= \mathbf{Q}_p(\zeta_{p^{n+1}}), & K_n^+ &= \mathbf{Q}_p(\zeta_{p^{n+1}} + \zeta_{p^{n+1}}^{-1}) \end{aligned}$$

$$\begin{aligned} F_\infty &= \textstyle\bigcup_{n\geq 0} F_n, & F_\infty^+ &= \textstyle\bigcup_{n\geq 0} F_n^+ \\ K_\infty &= \textstyle\bigcup_{n\geq 0} K_n, & K_\infty^+ &= \textstyle\bigcup_{n\geq 0} K_n^+ \end{aligned}$$

The various Galois groups of these fields are the following:

$$\Gamma_n = \mathrm{Gal}(F_\infty/F_n) = \mathrm{Gal}(F_\infty^+/F_n^+)$$
$$\Gamma = \Gamma_0$$

$$G_n = \mathrm{Gal}(F_n/\mathbf{Q}) = \mathrm{Gal}(K_n/\mathbf{Q}_p), \quad G_n^+ = \mathrm{Gal}(F_n^+/\mathbf{Q}) = \mathrm{Gal}(K_n^+/\mathbf{Q}_p)$$

A p-extension of a field is one whose Galois group is a pro-p-group. We will encounter the following p-extensions of the above fields (we allow $n = \infty$ as well):

$$\begin{aligned} L_n &= \text{maximal abelian unramified } p\text{-extension of } F_n \\ L_n^+ &= \text{maximal abelian unramified } p\text{-extension of } F_n^+ \\ M_n &= \text{maximal abelian } p\text{-extension of } F_n \text{ unramified away from } p \\ M_n^+ &= \text{maximal abelian } p\text{-extension of } F_n^+ \text{ unramified away from } p \end{aligned}$$

Their Galois groups are denoted as follows:

$$\begin{aligned} \mathscr{Y}_n &= \mathrm{Gal}(L_n/F_n), & \mathscr{Y}_n^+ &= \mathrm{Gal}(L_n^+/F_n^+) \\ \mathscr{X}_n &= \mathrm{Gal}(M_n/F_n), & \mathscr{X}_n^+ &= \mathrm{Gal}(M_n^+/F_n^+) \end{aligned}$$

Lastly, we also frequently encounter various groups of units.

$$\begin{gathered}\mathscr{U}_n = \mathcal{O}_{K_n}^\times \\ \mathscr{V}_n = \mathcal{O}_{F_n}^\times \\ \mathscr{E}_n = \text{closure of } \mathscr{V}_n \text{ in } \mathscr{U}_n \\ \mathscr{D}_n = \text{cyclotomic units of } F_n \\ \mathscr{C}_n = \text{closure of } \mathscr{D}_n \text{ in } \mathscr{U}_n\end{gathered}$$

A superscript + on any of these groups denotes the intersection with K_n^+, and a subscript 1 denotes those units which are $\equiv 1$ modulo the unique prime above p. Lastly, we write

$$\mathscr{U}_\infty = \varprojlim \mathscr{U}_n,$$

where the limit is with respect to the norm maps. The same holds for all above subgroups of $\mathscr{U}_n$.

Introduction

The class group of the field $\mathbf{Q}(\zeta_p)$ has been a central object of study in algebraic number theory since its early beginnings in the 19th century. One of the most notable early figures studying this group was Ernst Kummer, who famously proved in 1850 that the Fermat equation $x^p + y^p = z^p$ has no non-trivial integer solutions whenever p is a *regular* prime, i.e. when it does not divide the class number of the field $\mathbf{Q}(\zeta_p)$. He simultaneously gave a simple criterion for regularity, proving that p is regular if and only if p divides none of the *Bernoulli numbers* $B_2, B_4, \ldots, B_{p-3}$.

In the 1950's, Kenkichi Iwasawa quite literally took the study of this field to the next level, when he started studying the whole cyclotomic tower $\mathbf{Q}(\zeta_p) \subset \mathbf{Q}(\zeta_{p^2}) \subset \cdots$. By working with the whole tower at once instead of only focussing on the individual fields, he was able to prove [Iwa59] a growth theorem regarding the class numbers of these fields. It states that for large n, the p-valuation of the class number of $\mathbf{Q}(\zeta_{p^n})$ is equal to $\mu p^n + \lambda n + \nu$ for integers μ, λ, ν independent of n. After this, Iwasawa dedicated most of his time to the study of this tower of fields and their class groups, proving numerous results that nowadays fall under the umbrella of *Iwasawa theory*. Another major breakthrough occurred in 1964 when Iwasawa observed [Iwa64] that under a simple hypothesis on p, a certain 'characteristic polynomial' associated to the class groups $\mathrm{Cl}(\mathbf{Q}(\zeta_{p^n}))$ was essentially just the *p-adic L-function*, which was constructed around the same time by Kubota and Leopoldt [KL64]. This observation allowed him to deduce many detailed statements about the structure of the class group, including a long sought after refinement of Kummer's criterion for regularity. The belief that this relationship between the p-adic L-function and the class group held true even without any hypothesis on p became known as the *Main Conjecture of Iwasawa theory*.

In 1976, Ken Ribet [Rib76] was able to prove the aforementioned refinement of Kummer's criterion using the theory of modular forms, sidestepping the Main Conjecture. However, his techniques were later successfully adapted by Barry Mazur and Andrew Wiles [MW84] to prove the full Main Conjecture. In 1990, Victor Kolyvagin [Kol90] developed the theory of *Euler systems* based on a new approach by Francisco Thaine

[Tha88] to studying class groups. Not long after, Karl Rubin [Lan90, Appendix] successfully used Euler systems to give a new proof of the Main Conjecture, which was much simpler and shorter than that of Mazur–Wiles.

This finally brings us to this thesis. There are many books exploring in detail the results mentioned above. However, these books often lack examples, motivations, and are riddled with long and arduous technical arguments. Our goal is to focus on the main ideas present in the construction of the p-adic L-function, Iwasawa's growth theorem, and Rubin's proof of the Main Conjecture. Also among our contribution is to prove a more 'effective' version of the growth theorem, providing explicit values for μ, λ and ν and quantifying how large n needs to be for the formula to hold. We furthermore give an algorithm and implementation for computing p-adic L-functions, and use it to provide numerous examples.

In Chapter 1 the construction of the p-adic L-function is carried out. We also introduce the Iwasawa algebra and study its finitely generated modules, which will turn out to be the key to understanding many of the results in Iwasawa theory.

In Chapter 2 we look at Iwasawa's growth theorem. The version of this theorem typically found in the literature gives a formula for the class number of $\mathbf{Q}(\zeta_{p^n})$ that holds for 'large enough n'. We will make explicit how large we need n to be, and provide details on how to find the invariants present in this formula from p-adic L-functions. We also provide an algorithm for calculating these L-functions, and give many explicit examples. At the end we explain how the results thus far motivate the statement of the Main Conjecture, whose proof covers the remaining chapters.

Chapter 3 covers the theory of the unit groups of $\mathbf{Q}_p(\zeta_{p^n})$ and their connection to power series. The most important result is Coleman's theorem, which allows to construct power series which interpolate certain systems of units. This leads to a generalization of the construction of the p-adic L-function in Chapter 1.

In Chapter 4 we study the group of cyclotomic units. Using the results from the previous chapter we prove Iwasawa's theorem, which relates the cyclotomic units to the p-adic L-function. This result in fact allows us to prove the Main Conjecture for all *Vandiver* primes.

Chapter 5 is concerned with the theory of Euler systems. For us, Euler systems are collections of elements in cyclotomic extensions, which can be factored to obtain relations in class groups and bounds on class numbers.

At last, we finish the proof of the Main Conjecture in Chapter 6. We will see how Euler systems can be exploited to yield information on class groups, while leaving some of the more technical details aside.

1 Measures and Iwasawa algebras

In 1964, Kubota and Leopoldt [KL64] constructed the p-adic L-function, a p-adic analytic function that interpolates certain values of the usual Dirichlet L-function. In this chapter we carry out this construction using the theory of p-adic measures. We also discuss the Iwasawa algebra and the theory of its finitely generated modules. We do all of this rather quickly, with most proofs being omitted. The interested reader can consult [RW] for a more detailed exposition.

§1.1 p-adic measures

In the entirety of this thesis, p will be an *odd* prime. We fix once and for all algebraic closures $\overline{\mathbf{Q}}$ and $\overline{\mathbf{Q}}_p$, and an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. Throughout this chapter, we let L denote a finite extension of $\mathbf{Q}_p$. Let G be a profinite abelian group, which will usually be $\mathbf{Z}_p$ or $\mathbf{Z}_p^\times$. We denote by $C(G,L)$ the L-vector space of continuous functions $G \to L$. This space comes equipped with a norm $\|f\| := \sup_{x\in G} |f(x)|$, and with this norm $C(G,L)$ becomes a p-adic Banach space. The continuous dual space $C(G,L)^\vee$ (consisting of all continuous linear functionals $C(G,L) \to L$) is called the space of *L-valued measures* on G, and also denoted by $M(G,L)$. If $\mu \in M(G,L)$ and $f \in C(G,L)$, we also write $\int_G f \cdot \mu$ or $\int_G f(x)\cdot\mu(x)$ for $\mu(f)$.

So far we have not yet utilized the group structure of G, and the above definitions indeed make sense for any topological space. But using the group operation, we can endow the space of measures with the structure of a (commutative) algebra, if we define the multiplication to be *convolution* of measures: given $\mu, \nu \in M(G,L)$, their convolution is the measure $\mu\nu$ defined by

$$\int_G f\cdot(\mu\nu) = \int_G \left(\int_G f(xy)\cdot\mu(x)\right)\cdot\nu(y).$$

Example 1.1.1. For $g \in G$, the *dirac measure* δ_g or $[g]$ is defined by $\int f\cdot[g] = f(g)$. If μ is any measure, the convolution $[g]\mu$ is the measure given by $\int_G f\cdot([g]\mu) = \int_G f(gx)\cdot\mu(x)$.

Any measure is bounded in the sense that for $\mu \in M(G,L)$, there is a constant C such that $|\mu(f)| \leq C\|f\|$ for all $f \in C(G,L)$. In particular this implies that any measure can be scaled so that $\mu(f) \in \mathcal{O}_L$ for all $f \in C(G,\mathcal{O}_L)$. Note that also any continuous map $G \to L$ can be scaled to take values in $\mathcal{O}_L$. Thus there is no harm in restricting ourselves to only studying the spaces $C(G,\mathcal{O}_L)$ of $\mathcal{O}_L$-valued functions and its dual $M(G,\mathcal{O}_L)$ of $\mathcal{O}_L$-valued measures.

To get a better idea of what the space $M(G,\mathcal{O}_L)$ looks like, we start by analyzing the space $C(G,\mathcal{O}_L)$. In the case that $G = \mathbf{Z}_p$, this space has a very simple description. For $x \in \mathbf{Z}_p$, define the generalized binomial coefficient $\binom{x}{n}$ by

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

Proposition 1.1.2 (Mahler's Theorem). If $f \in C(\mathbf{Z}_p,\mathcal{O}_L)$, then there are unique elements $a_1, a_2, \cdots \in \mathcal{O}_L$ such that

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

for all $x \in \mathbf{Z}_p$.

Proof. The idea is to construct the coefficients a_n as the finite differences $\Delta^n f(0)$, where $\Delta f(x) = f(x+1) - f(x)$. For the details, see [Col10, Théorème I.2.3]. □

The theorem implies that a measure on $\mathbf{Z}_p$ is uniquely determined by its values on the functions $\binom{x}{n}$. Given a measure μ, it would therefore be instructive to consider the generating function $\sum_{n\geq 0}\left(\int \binom{x}{n} \cdot \mu(x)\right) T^n = \int (1+T)^x \cdot \mu(x)$. We call this power series the *Amice transform* of μ, and denote it by $\mathscr{A}_\mu(T)$.

Proposition 1.1.3. The Amice transform is an $\mathcal{O}_L$-algebra isomorphism

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

Proof. See [Col10, Théorème II.2.2]. □

Example 1.1.4. The Amice transform of the dirac measure $[a]$ is simply $(1+T)^a$.

Remark 1.1.5. Note that we have an inclusion $\mathbf{Z}_p[\![T]\!] \subset \mathcal{O}_L[\![T]\!]$. By the above isomorphism, this means that we can integrate $\mathcal{O}_L$-valued functions against $\mathbf{Z}_p$-valued measures, which was not clear from the definition of $M(G,\mathcal{O}_L)$. For this reason, we will from now on specialize to the case $L = \mathbf{Q}_p$. In this case we also denote the spaces $C(G,\mathbf{Z}_p)$ and $M(G,\mathbf{Z}_p)$ simply by $C(G)$ and $M(G)$.

The ring $\mathbf{Z}_p[\![T]\!]$ is a particularly nice ring; it is a 2-dimensional complete regular local ring, with maximal ideal (p,T). Later we will study modules over this ring, which in the finitely generated case turn out to have a very simple description.

§1.2 Operations on measures

If $f \in C(\mathbf{Z}_p)$, $\mu \in M(\mathbf{Z}_p)$, we can define a new measure $f\mu$, which is defined by $\int_{\mathbf{Z}_p} g \cdot (f\mu) = \int_{\mathbf{Z}_p} fg \cdot \mu$. We will focus our attention on three special cases, and look at how the Amice transform of a measure transforms under the multiplication.

- *Multiplication by x.* First consider the measure $x\mu$. From the identity
$$x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n},$$
it follows that $\mathscr{A}_{x\mu}(T) = (1+T)\frac{\mathrm{d}}{\mathrm{d}T}\mathscr{A}_\mu(T)$. The differential operator $(1+T)\frac{\mathrm{d}}{\mathrm{d}T}$ occurs frequently enough that we shorten it to ∂.

  From this, we see that the *k-th moment* of the measure μ, which is defined to be $\int_{\mathbf{Z}_p} x^k \cdot \mu(x)$, is given by $\partial^k \mathscr{A}_\mu(0)$.

- *Multiplication by z^x.* If $z \in 1 + p\mathbf{Z}_p$, we can make sense of z^x for any $x \in \mathbf{Z}_p$, and the Amice transform of $z^x\mu$ is equal to $\mathscr{A}_\mu((1+T)z - 1)$.

- *Multiplication by $\mathbf{1}_X$.* If $X \subset \mathbf{Z}_p$ is a compact open subset, the indicator function $\mathbf{1}_X$ is continuous, and the measure $\mathbf{1}_X\mu$ is called the *restriction* of μ to X. It is denoted $\mathrm{Res}_X(\mu)$ or $\mu|_X$. Note that we have a natural inclusion of $\mathbf{Z}_p$-modules $M(X) \to M(\mathbf{Z}_p)$, by letting
$$\int_{\mathbf{Z}_p} f \cdot \mu := \int_X f|_X \cdot \mu$$
for μ a measure on X. Clearly the restriction of a measure to X lies in the image of this map, so we also view Res_X as a map $M(\mathbf{Z}_p) \to M(X)$.

  In the case that $X = a + p^n\mathbf{Z}_p$, we can use the identity
$$\mathbf{1}_{a+p^n\mathbf{Z}_p}(x) = p^{-n} \sum_{\eta^{p^n}=1} \eta^{x-a}$$

in combination with the previous point to see that

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

It then also immediately follows that

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

Lastly, we come to the most important operations on measures: the *Frobenius* and *trace* operators.

For $\mu \in M(\mathbf{Z}_p)$, the measures $\varphi(\mu)$ and $\psi(\mu)$ are given by

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

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

The maps φ and ψ are respectively known as the *Frobenius* and *trace* map. Via the Amice transform we can also view them as maps on $\mathbf{Z}_p[\![T]\!]$. The Frobenius is easily described on power series: $\varphi(f) = f((1+T)^p - 1)$. The trace operator is more mysterious, and has no explicit direct description in terms of power series. The best we can do is the following proposition.

Proposition 1.2.1. We have that $\psi \circ \varphi = \mathrm{Id}$ and $\varphi \circ \psi = \mathrm{Res}_{p\mathbf{Z}_p}$. In particular, φ is injective, and for $f \in \mathbf{Z}_p[\![T]\!]$,

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

Proof. Clear by writing out definitions. □

If $X \subset \mathbf{Z}_p$, we say that a measure μ is *supported on* X if $\mu|_X = \mu$.

Lemma 1.2.2. A measure μ is supported on $\mathbf{Z}_p^\times$ if and only if $\psi(\mu) = 0$.

Proof. This is immediate from the fact that $\varphi \circ \psi = \mathrm{Res}_{p\mathbf{Z}_p} = \mathrm{Id} - \mathrm{Res}_{\mathbf{Z}_p^\times}$ and that φ is injective. □

§1.3 Iwasawa algebras

Let G again be any profinite abelian group. If $U \subset G$ is compact and open, we write $\mu(U) := \mu(\mathbf{1}_U)$, $\mu \in M(G)$. The resulting function $\{U \subset G \text{ compact open}\} \to \mathbf{Q}_p$ is reminiscent of the more familiar idea of a measure one encounters in real analysis. This gives us another way of thinking about the space of measures as follows: the set of locally constant functions is dense in $C(G)$, and any locally constant function is a linear combination of indicator functions of sets of the form gH, where $g \in G$ and H is an open subgroup. Thus a measure is uniquely determined by the values $\mu(gH)$. This motivates the following definition and proposition.

Definition 1.3.1. The *Iwasawa algebra* of G is

$$\Lambda(G) = \varprojlim \mathbf{Z}_p[G/H],$$

where the inverse limit runs over all open subgroups of G, with respect to the obvious maps.

Proposition 1.3.2. The collection of maps $M(G) \to \mathbf{Z}_p[G/H]$, H an open subgroup, given by

$$\mu \mapsto \sum_{gH \in G/H} \mu(gH)[gH]$$

induces a map $M(G) \to \Lambda(G)$, and this map is a $\mathbf{Z}_p$-algebra isomorphism.

Proof. This is proved by explicitly constructing an inverse map, see [RW, Proposition 2.3] for the details. □

We have a natural inclusion $\mathbf{Z}_p[G] \to \Lambda(G)$, which has dense image ($\Lambda(G)$ is equipped with the standard inverse limit topology). For this reason the Iwasawa algebra is also often called the completed group algebra, and modules over it naturally arise in the following way: suppose we have an inverse system of $\mathbf{Z}_p[G]$-modules $(M_H, f_{H,H'})$ indexed by the open subgroups of G, such that H acts trivially on M_H. Then $\varprojlim M_H$ has a natural continuous $\Lambda(G)$-module structure.

In what follows we will study some properties of $\Lambda(G)$-modules (which are all assumed to have a Hausdorff topology with respect to which the action is continuous), paying special attention to the case $G = \mathbf{Z}_p$. In this case, combining Propositions 1.1.3 and 1.3.2, we see that $\Lambda(G)$ is isomorphic to $\mathbf{Z}_p[\![T]\!]$. Recall that the latter was a local ring with maximal ideal (p, T), and that it is complete with respect to the (p, T)-adic topology. It turns out (see the proof of [Was97, Theorem 7.1]) that the isomorphism

between $\Lambda(G)$ and $\mathbf{Z}_p[\![T]\!]$ also identifies the inverse limit topology on the former with the (p, T)-adic topology on the latter.

Remark 1.3.3. One may wonder if the topology also has a natural description directly on $M(G)$. It turns out to be the *weak* topology: a sequence $(\mu_n)_n$ of measures converges to μ if and only if $\mu_n(f)$ converges to $\mu(f)$ for all $f \in C(G)$.

We start with a version of Nakayama's lemma that works for general compact modules over local rings.

Proposition 1.3.4 (Nakayama's lemma). Suppose R is a local ring with maximal ideal $\mathfrak{m}$, equipped with the $\mathfrak{m}$-adic topology, and let X be a compact R-module. Then X is finitely generated over R if and only $X/\mathfrak{m}X$ is finitely generated over $R/\mathfrak{m}$, in which case a set of elements $x_1, \ldots, x_n$ generate X if and only if their images generate $X/\mathfrak{m}X$.

Proof. We first show that we have that $\bigcap_{n\geq 1} \mathfrak{m}^n X = 0$. Indeed, let $y \in X$ be non-zero and U an open neighborhood of 0 not containing y. Then for any $x \in X$, we can find n and a neighborhood U_x of x such that $\mathfrak{m}^n U_x \subset U$. Choosing finitely many of the U_x that cover X, we find that there exists n such that $\mathfrak{m}^n X \subset U$, and consequently $y \notin \mathfrak{m}^n X$.

Now, the forward direction of the proposition is clear. Conversely, suppose the quotient is finitely generated by the images of $x_1, \ldots, x_n$. Consider $Y = Rx_1 + \cdots + Rx_n$, which is a compact, hence closed, submodule of X. Then $X = \mathfrak{m}X + Y$, so that

$$\mathfrak{m}(X/Y) = \frac{\mathfrak{m}X + Y}{Y} = X/Y.$$

Applying this repeatedly yields that $\mathfrak{m}^n(X/Y) = X/Y$ for all n, and thus $X/Y = 0$. □

The following structure theorem will be our most important tool in the study of finitely generated $\mathbf{Z}_p[\![T]\!]$-modules. It classifies such modules up to so called *pseudo-isomorphism*, which is a homomorphism with finite kernel and cokernel.

Let us call a polynomial over $\mathbf{Z}_p$ *distinguished* if it is monic and every non-leading coefficient is divisible by p.

Theorem 1.3.5. Let M be a finitely generated $\Lambda = \mathbf{Z}_p[\![T]\!]$-module. Then there is a pseudo-isomorphism from M to a module of the form

$$\Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j^{n_j}),$$

where the f_j are irreducible distinguished polynomials. Furthermore, such a decomposition is unique.

Proof. See [Was97, Theorem 13.12] for a direct proof using matrices, similar to the use of Smith normal form over PID's. Alternatively, the proposition is a special case of a more general structure theorem for Noetherian integrally closed domains, see [Ser60, Théorème 7] and [Bou89, Ch. VII, §4, Theorems 4 & 5]. □

It is important to note that pseudo-isomorphism is not in general an equivalence relation. This is however the case if we are dealing with torsion modules, which are precisely the modules for which $r = 0$ in the above decomposition. In this case, let us write $\mu = \sum_i m_i$. We call the ideal generated by $p^\mu \prod_{j=1}^t f_j^{n_j}$ in Λ the *characteristic ideal* of M, and denote it by $\mathrm{ch}(M)$. It is an important invariant of M, and has the property of being multiplicative in exact sequences ([Bou89, Ch. VII, §5, Proposition 10]).

We now work a little more abstractly, and denote by Γ any group isomorphic to $\mathbf{Z}_p$, and let G be a group of the form $\omega \times \Gamma$, where ω is a finite cyclic group of order k dividing $p-1$. Then any character χ of ω takes values in the $(p-1)$-st roots of unity $\mu_{p-1} \subset \mathbf{Z}_p$, and we define $e_\chi := \frac{1}{k} \sum_{a \in \omega} \chi(a)[a^{-1}] \in \mathbf{Z}_p[\omega]$. The collection of elements e_χ form a complete orthogonal system of idempotents. It follows that for any $\Lambda(G)$-module M, we have a decomposition $M = \bigoplus_\chi e_\chi M$. Note that $e_\chi M$ is the largest $\Lambda(\Gamma)$-submodule on which ω acts via χ.

Applying this to $\Lambda(G)$ itself, we obtain a decomposition $\Lambda(G) = \prod_\chi e_\chi \Lambda(G)$. Clearly $e_\chi \Lambda(G)$ is a ring, and $e_\chi M$ is a $e_\chi \Lambda(G)$-submodule of M.

Lemma 1.3.6. The restriction map $\mathrm{Res}_\Gamma \colon \Lambda(G) \to \Lambda(\Gamma)$ gives an isomorphism $e_\chi \Lambda(G) \to \Lambda(\Gamma)$.

Proof. Let $\Gamma_n \subset \Gamma$ be the unique subgroup of index p^n. Take $a \in e_\chi \mathbf{Z}_p[\omega \times \Gamma/\Gamma_n] = e_\chi \mathbf{Z}_p[\Gamma/\Gamma_n][\omega]$, which we can write as $\sum_{g \in A} a_g[g]$ with $a_g \in \mathbf{Z}_p[\Gamma/\Gamma_n]$. Because ω acts via χ, the element is completely determined by a_1, as $a_g = \chi^{-1}(g) a_1$. It follows that the

projection map

$$\begin{aligned} \mathbf{Z}_p[\omega \times \Gamma/\Gamma_n] &\to \mathbf{Z}_p[\Gamma/\Gamma_n] \\ \sum_{g \in A} a_g[g] &\mapsto a_1 \end{aligned}$$

restricts to an isomorphism on $e_\chi \mathbf{Z}_p[\omega \times \Gamma/\Gamma_n]$.

The inverse limit of the projection maps is precisely the restriction map Res_Γ, which is then an isomorphism $e_\chi \Lambda(G) \to \Lambda(\Gamma)$. □

§1.4 The p-adic zeta measure

Let us denote by ζ the Riemann zeta function, which is defined and analytic on the whole complex plane except for a simple pole at 1. Recall that it has the special values $\zeta(1-k) = (-1)^{k+1}\frac{B_k}{k}$, where the B_k are the Bernoulli numbers, defined by their exponential generating function $\frac{t}{e^t-1} = \sum_{k\geq 0} \frac{B_k}{k!} t^k$. In fact, $B_k = 0$ if $k > 1$ is odd, so as long as $k \neq 1$, we may replace $(-1)^{k+1}$ by -1 in the special value. In this section, we will construct the p-adic analogue of the ζ function, which actually turns out to be a measure instead of a function.

Let $a \in \mathbf{Z}$ be coprime to p and define $F_a(T) := \frac{a}{(1+T)^a - 1} - \frac{1}{T}$. It is easily shown that F_a is in fact a power series with p-adic integral coefficients. Let μ_a be the measure on $\mathbf{Z}_p$ it corresponds to under the Amice transform.

Lemma 1.4.1. The moments of μ_a are given by

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

Proof. If we make the change of variables $T = e^t - 1$, then

$$\begin{aligned} F_a(T) &= \frac{a}{e^{at} - 1} - \frac{1}{e^t - 1} \\ &= -\sum_{k \geq 0} (1 - a^{k+1}) \frac{B_{k+1}}{k+1} \frac{t^k}{k!}. \end{aligned}$$

The result now follows from the fact that the moments are given by $\partial^k F_a(0)$, and that under the above change of variables, $\partial = \frac{\mathrm{d}}{\mathrm{d}t}$. □

There are a few problems with the measure we have obtained. First off, there is of course the factor of $(1 - a^{k+1})$ that we want to rid ourselves of. Second, we would ideally have the k-th moment of our measure be related to B_k instead of B_{k+1}. We will deal with these problems now.

LEMMA 1.4.2. $\psi(\mu_a) = \mu_a$.

A direct proof involving power series computations is possible, but a more conceptual proof uses some of the theory of Chapter 3. Namely, we shall see that F_a is the *logarithmic derivative* of a *norm invariant* power series, and that this implies that it is equal to its own trace.

The above lemma implies that $\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_a) = \mu_a - \varphi(\psi(\mu_a)) = \mu_a - \varphi(\mu_a)$, and consequently

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

If we now consider the measure $\lambda_a := x^{-1}\,\mathrm{Res}_{\mathbf{Z}_p^\times}(\mu_a)$ on $\mathbf{Z}_p^\times$, then it satisfies

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \lambda_a(x) = -(1-p^{k-1})(1-a^k)\frac{B_k}{k}. \tag{1.1}$$

The restriction to $\mathbf{Z}_p^\times$ has allowed us to multiply by x^{-1}, shifting the moments to now interpolate the correct Bernoulli numbers. However, this has introduced a new factor of $(1-p^{k-1})$. Luckily this factor is not a problem; it now allows us to write $-(1-p^{k-1})\frac{B_k}{k} = (1-p^{k-1})\zeta(1-k)$, which would not have been true for $k=1$ without the extra factor. Moreover, the new factor cancels out the corresponding Euler factor in the product $\zeta(s) = \prod_p (1-p^{-s})^{-1}$, which is necessary to make the zeta function p-adically continuous.

This leaves us with the final task of getting rid of the factor depending on our choice of a. To do this, we want to 'divide' our measure by the measure $[1]-[a]$.

Definition 1.4.3. A *pseudo-measure* on $\mathbf{Z}_p^\times$ is an element μ of the total ring of fractions of $\Lambda(\mathbf{Z}_p^\times)$ (i.e. the localization at the non-zero-divisors) with the property that $([1]-[g])\mu \in \Lambda(\mathbf{Z}_p^\times)$ for all $g \in \mathbf{Z}_p^\times$.

We can no longer integrate arbitrary functions against pseudo-measures. We can, however, integrate non-trivial group homomorphisms $\mathbf{Z}_p^\times \to L^\times$. This is because we have that

$$\int_{\mathbf{Z}_p^\times} f(x)\cdot(\mu_1\mu_2)(x) = \left(\int_{\mathbf{Z}_p^\times} f(x)\cdot\mu_1(x)\right)\left(\int_{\mathbf{Z}_p^\times} f(x)\cdot\mu_2(x)\right)$$

whenever f is a homomorphism. Hence for a pseudo-measure μ, we may define

$$\int_{\mathbf{Z}_p^\times} f \cdot \mu := \frac{\int_{\mathbf{Z}_p^\times} f \cdot ([1]-[g])\mu}{1-f(g)}$$

where $g \in \mathbf{Z}_p^\times$ is chosen such that $f(g) \neq 1$, and this will be independent of the choice of such g. In particular, this means that we can still make sense of the moments of a pseudo measure.

Lemma 1.4.4. Let $\mu \in \Lambda(\mathbf{Z}_p^\times)$.

1. We have $\mu = 0$ if and only if $\int_{\mathbf{Z}_p^\times} x^k \cdot \mu(x) = 0$ for all $k > 0$. The analogous assertion holds for pseudo-measures.
2. If $\int_{\mathbf{Z}_p^\times} x^k \cdot \mu(x) \neq 0$ for all $k > 0$, then μ is not a zero-divisor.

Proof. See [RW, Lemma 3.8]. □

The second point shows that $[1]-[a]$ is not a zero-divisor. Furthermore, if we choose a such that it is a topological generator for $\mathbf{Z}_p^\times$, then for any $g \in \mathbf{Z}_p^\times$, the element $[1]-[a]$ divides $[1]-[g]$ in the group rings $\mathbf{Z}_p[(\mathbf{Z}/p^n\mathbf{Z})^\times]$. This implies that in fact $\frac{[1]-[g]}{[1]-[a]} \in \Lambda(\mathbf{Z}_p^\times)$, so that $1/([1]-[a])$ is a pseudo-measure. This finally gets us our desired result.

Theorem 1.4.5. There is a unique pseudo-measure ζ_p on $\mathbf{Z}_p^\times$ such that

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

for all $k \geq 1$.

Proof. Choose $a \in \mathbf{Z}$ to be a topological generator of $\mathbf{Z}_p^\times$, and define λ_a as before. We can take $\zeta_p = \frac{\lambda_a}{[1]-[a]}$ by (1.1). Uniqueness follows from the previous lemma. □

§1.5 The Kubota–Leopoldt p-adic L-function

In the previous section we have constructed a pseudo-measure, whose moments are given by interpolating values of the zeta function. What we would really like however, is to turn ζ_p into an actual (analytic) function on $\mathbf{Z}_p$. We will do this now.

Recall that there is a decomposition $\mathbf{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbf{Z}_p)$. The projection onto the first factor is called the Teichmüller character, and is denoted ω. The projection onto the second factor is denoted $x \mapsto \langle x \rangle$. Hence any p-adic unit x may be written as $x = \omega(x)\langle x \rangle$.

If $\chi\colon (\mathbf{Z}/p^n\mathbf{Z})^\times \to \overline{\mathbf{Q}} \subset \overline{\mathbf{Q}}_p$ is a primitive Dirichlet character of p-power conductor, we may view it as a homomorphism on $\mathbf{Z}_p^\times$. By the decomposition above, we can uniquely write χ as the product of a character which is trivial on $1+p\mathbf{Z}_p$ (which must be a power of ω), and a character trivial on μ_{p-1}.

When necessary, we can also view a character as a function on $\mathbf{Z}_p$ by setting it equal to 0 outside $\mathbf{Z}_p^\times$, unless χ is the trivial character, in which case we let it be constant 1 on all of $\mathbf{Z}_p$.

Definition 1.5.1. The *p-adic L-function* of χ is defined as

$$L_p(\chi, s) := \int_{\mathbf{Z}_p^\times} \chi(x)\langle x \rangle^{1-s} \cdot \zeta_p.$$

Theorem 1.5.2. For $k \geq 1$, the p-adic L-function satisfies

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

Proof. In the case that $\chi = \omega^k$, this is exactly Theorem 1.4.5, since

$$L_p(\omega^k, 1-k) = \int_{\mathbf{Z}_p^\times} \omega^k(x)\langle x \rangle^k \cdot \zeta_p = \int_{\mathbf{Z}_p^\times} x^k \cdot \zeta_p.$$

The general case is a little more tedious, see for instance [RW, Theorem 4.1]. □

Just as the Riemann zeta function, the special values of Dirichlet L-functions can be expressed using the the so-called *generalized Bernoulli numbers* $B_{k,\chi}$, which are defined using generating functions similar to $\frac{t}{e^t-1}$ for the regular Bernoulli numbers. The special values are then given by $L(\chi, 1-k) = -\frac{B_{k,\chi}}{k}$.

Next, we would like to see that the functions $L_p(\chi, s)$ are in fact analytic, meaning that they can be represented by a power series in $\mathbf{C}_p[\![s]\!]$.

Every character of μ_{p-1} is given by raising to the i-th power for some $i \in \mathbf{Z}/(p-1)\mathbf{Z}$. Recall from Section 1.3 that we have a complete system of idempotents $e_i = \sum_{\tau \in \mu_{p-1}} \tau^i[\tau^{-1}] \in \Lambda(\mathbf{Z}_p^\times)$. The results from that section tell us that a measure $\mu \in \Lambda(\mathbf{Z}_p^\times)$ is completely determined by the measures $\mathrm{Res}_{1+p\mathbf{Z}_p}(e_i\mu) \in \Lambda(1 + p\mathbf{Z}_p)$. We can use the

isomorphism

$$1 + p\mathbf{Z}_p \to \mathbf{Z}_p, \quad x \mapsto \frac{\log(x)}{\log(1+p)}$$

to view the resulting measure on $1+p\mathbf{Z}_p$ as a measure on $\mathbf{Z}_p$. The measure constructed this way is called the i-th Leopoldt transform of μ, and is denoted by $\Gamma^i(\mu)$.

Proposition 1.5.3. Let $\chi = \theta\omega^i$ be a Dirichlet character of p-power conductor (where θ is trivial on μ_{p-1}) and $\mu \in \Lambda(\mathbf{Z}_p^\times)$. Then with $g_i := \mathscr{A}_{\Gamma^i(\mu)}(T)$, we have that

$$g_i(\zeta_\theta(1+p)^s - 1) = \int_{\mathbf{Z}_p^\times} \chi(x)\langle x\rangle^s \cdot \mu$$

where $\zeta_\theta = \theta(1+p)$.

Proof. We directly calculate that

$$\begin{aligned}
g_i(\zeta_\theta(1+p)^s - 1) &= \int_{\mathbf{Z}_p} \zeta_\theta^y (1+p)^{sy} \cdot \Gamma^i(\mu)(y) \\
&= \int_{1+p\mathbf{Z}_p} \theta(x)x^s \cdot (e_i\mu)(x) \\
&= \sum_{\tau\in\mu_{p-1}} \int_{\mathbf{Z}_p} \theta(x)\tau^i(\tau^{-1}x)^s \mathbf{1}_{1+p\mathbf{Z}_p}(\tau^{-1}x) \cdot \mu(x) \\
&= \sum_{\tau\in\mu_{p-1}} \int_{\mathbf{Z}_p} \theta(x)\omega^i(x)\langle x\rangle^s \mathbf{1}_{\tau+p\mathbf{Z}_p}(x) \cdot \mu(x) \\
&= \int_{\mathbf{Z}_p^\times} \chi(x)\langle x\rangle^s \cdot \mu(x),
\end{aligned}$$

where we used the substitution $y = \frac{\log(x)}{\log(1+p)}$, and the fact that if $x \in \tau + p\mathbf{Z}_p$, we have $\langle x\rangle = \tau^{-1}x$ and $\omega(x) = \tau$. □

Theorem 1.5.4. Let $i \not\equiv 0 \bmod p-1$. There is a power series $f_i \in \mathbf{Z}_p[\![T]\!]$ such that for any character θ of $1+p\mathbf{Z}_p$, we have

$$f_i(\zeta_\theta(1+p)^{1-s} - 1) = L_p(\theta\omega^i, s),$$

where $\zeta_\theta = \theta(1+p)$. In particular, $L_p(\theta\omega^i, s)$ is a p-adic analytic function.

Proof. Choose $a \in \mathbf{Z}$ such that $\omega^i(a) \neq 1$. By the previous result, there are power series g_i and h_i such that we may write

$$L_p(\chi, s) = \frac{\int_{\mathbf{Z}_p^\times} \chi(x)\langle x\rangle^{1-s} \cdot \lambda_a}{\int_{\mathbf{Z}_p^\times} \chi(x)\langle x\rangle^{1-s} \cdot ([1]-[a])} = \frac{g_i(\zeta_\theta(1+p)^{1-s}-1)}{h_i(\zeta_\theta(1+p)^{1-s}-1)}.$$

Because $h_i(0) = 1-\omega^i(a)$ is a p-adic unit, $h_i \in \mathbf{Z}_p[\![T]\!]^\times$, so that we may take $f_i = g_i/h_i$. □

The power series from this theorem are sometimes called the *Iwasawa power series* of the L-functions, but it is also common to refer to these power series as the p-adic L-functions themselves.

Remark 1.5.5. Even though to define the pseudo-measure $\zeta_p = \frac{\lambda_a}{[1]-[a]}$ we needed to take a to be a topological generator of $\mathbf{Z}_p^\times$, the expression

$$L_p(\chi, s) = \frac{\int_{\mathbf{Z}_p^\times} \chi(x)\langle x\rangle^{1-s} \cdot \lambda_a}{\int_{\mathbf{Z}_p^\times} \chi(x)\langle x\rangle^{1-s} \cdot ([1]-[a])}$$

still holds true for any $a \in \mathbf{Z}$ coprime to p with the property that $\omega^i(a) \neq 1$.

Finally, let us record the following well-known result about p-adic analytic functions, known as the *Weierstrass preparation theorem*. Recall that a polynomial is said to be *distinguished* if it is monic and its non-leading coefficients are all divisible by p.

Theorem 1.5.6. Let $f \in \mathbf{Z}_p[\![T]\!]$. Then f can be uniquely written as $p^\mu P(T)U(T)$ where P is a distinguished polynomial, and U is a unit of $\mathbf{Z}_p[\![T]\!]$.

Proof. See [Was97, Theorem 7.3]. □

As a consequence, a non-zero element of $\mathbf{Z}_p[\![T]\!]$ can have only finitely many zeros in $\overline{\mathbf{Z}}_p$. In particular this holds for the Iwasawa power series of the p-adic L-functions. In the next chapter, we see how these zeros relate to the class numbers of p-power cyclotomic extensions of $\mathbf{Q}$.

2 Cyclotomic class numbers and p-adic L-functions

In this chapter we focus our attention on a theorem of Iwasawa [Iwa59], which states that for large enough n, the p-valuation of the class number of $\mathbf{Q}(\zeta_{p^n})$ is equal to $\mu p^n + \lambda n + \nu$ for some constants μ, λ, ν independent of n. The usual proof of this theorem however gives us no indication on how to find these constants, or on how large n needs to be for the formula to hold. In Section 1 we will study this proof. In Section 2 we will prove an 'effective' version of the theorem, where we now make explicit both how large n needs to be, and what the invariants μ, λ and ν are. It will turn out that both of these questions are answered by looking at p-adic L-functions. In Section 3 we will look at some explicit calculations and examples (something that is typically absent in the established literature). Section 4 discusses some heuristics on the size of the invariant λ. Lastly, we discuss how the results from this chapter motivate the *Main Conjecture* of Iwasawa theory.

From this point onward, we make repeated use of the basics of class field theory. The necessary results can be found in the Appendix.

§2.1 Class numbers in $\mathbf{Z}_p$-extensions

Let F_0 be a number field and F_∞/F_0 a $\mathbf{Z}_p$-extension, meaning a Galois extension such that $\Gamma := \mathrm{Gal}(F_\infty/F_0)$ is isomorphic to $\mathbf{Z}_p$. Then Γ has a unique subgroup of index p^n for each n which we denote by Γ_n, and we let F_n be the corresponding field.

Example 2.1.1. The most important examples of $\mathbf{Z}_p$-extensions are the cyclotomic extension $F_n = \mathbf{Q}(\zeta_{p^{n+1}})$ and its maximal real subfield $F_n = \mathbf{Q}(\zeta_{p^{n+1}})^+$. More generally, if F_0 is any number field and $F_0(\zeta_{p^\infty})$ is the field obtained by adjoining all p-power roots of unity, then the fixed field of the torsion subgroup of $\mathrm{Gal}(F_0(\zeta_{p^\infty})/F_0)$ is a $\mathbf{Z}_p$-extension of F_0, called the cyclotomic extension of F_0.

Let h_n be the class number of F_n. In this section, we prove a remarkable theorem of Iwasawa regarding these class numbers.

THEOREM 2.1.2. There exist positive integers μ, λ, ν, n_0 such that

$$\operatorname{ord}_p(h_n) = \mu p^n + \lambda n + \nu$$

for all $n \geq n_0$.

We will prove the theorem under the following additional hypothesis:

There is a unique prime $\mathfrak{p}_0 \subset F_0$ above p, and it ramifies completely in F_∞.

Note that both our examples of $\mathbf{Q}(\zeta_{p^{n+1}})$ and $\mathbf{Q}(\zeta_{p^{n+1}})^+$ satisfy this assumption. From now on we will assume that this hypothesis is satisfied. The general case can be reduced to this special one (see [Was97, Theorem 13.13]).

For each n, let L_n/F_n be the maximal abelian unramified p-extension (meaning the Galois group is pro-p). We let $\mathscr{Y}_n = \operatorname{Gal}(L_n/F_n)$. Additionally, let $L_\infty = \bigcup_{n\geq 0} L_n$ be the maximal abelian unramified p-extension of F_∞, and $\mathscr{Y}_\infty = \varprojlim \mathscr{Y}_n = \operatorname{Gal}(L_\infty/F_\infty)$. Class field theory shows that the Artin map yields an isomorphism between the Sylow p-subgroup of $\operatorname{Cl}(F_n)$ and $\mathscr{Y}_n$.

Note that since each $\mathscr{Y}_n$ is a p-group, they are also $\mathbf{Z}_p$-modules. Furthermore, $\mathscr{Y}_n$ is equipped with an action of Γ as follows: for $\gamma \in \Gamma$, $y \in \mathscr{Y}_n$, let $\tilde{\gamma} \in \operatorname{Gal}(L_\infty/F_0)$ denote any lift of γ. Then the action is defined by $\gamma \cdot y := \tilde{\gamma} y \tilde{\gamma}^{-1}$. It is easily checked that this is well defined and gives a group action. Furthermore, under the aforementioned isomorphism of $\mathscr{Y}_n$ with the Sylow p-subgroup of the class group, this action is simply the one induced from the natural action of Γ on the group of fractional ideals of F_n. Consequently, $\mathscr{Y}_\infty$ becomes a $\mathbf{Z}_p[\Gamma]$-module. Iwasawa proved his theorem by using rather ad-hoc arguments regarding the structure of $\mathscr{Y}_\infty$ as an $\mathbf{Z}_p[\Gamma]$-module. Not long after, Serre [Ser60] was able to simplify Iwasawa's proof by realizing that because $\Gamma_n = \operatorname{Gal}(F_\infty/F_n)$ acts trivially on $\mathscr{Y}_n$, the inverse limit $\mathscr{Y}_\infty$ is even a (finitely generated) $\Lambda(\Gamma)$-module (as is described just after Proposition 1.3.2). The theorem now follows by exploiting the established structure theory for such modules. This insight cannot be understated: from this point on, almost all of the key results in Iwasawa theory are most naturally stated in terms $\Lambda(\Gamma)$-modules.

From now on, fix a topological generator γ_0 for Γ, which yields an isomorphism $\Gamma \to \mathbf{Z}_p$. This allows us to identity $\Lambda(G)$ with $\Lambda = \mathbf{Z}_p[\![T]\!]$ via the Amice transform. Under this identification, $\gamma_0 \in \Lambda(G)$ corresponds to $1 + T \in \mathbf{Z}_p[\![T]\!]$. If M is any $\Lambda(\Gamma)$-module, we denote by

$$M_{\Gamma_n} = M/(\gamma_0^{p^n} - 1)M$$

the set of Γ_n-*coinvariants*.

Lemma 2.1.3. Let $H = \mathrm{Gal}(L_\infty/F_0)$ and let $I \subset H$ be the inertia subgroup of any prime above $\mathfrak{p}_0$.

1. $H = I\mathscr{Y}_\infty$ and $I \cap \mathscr{Y}_\infty = 1$;
2. $[H,H] = (\gamma_0 - 1)\mathscr{Y}_\infty = T\mathscr{Y}_\infty$, where $[H,H]$ denotes the closed subgroup generated by the commutators $[a,b]$;
3. $\mathscr{Y}_n = (\mathscr{Y}_\infty)_{\Gamma_n}$.

Proof. The first assertion follows since F_∞/F_0 is totally ramified above $\mathfrak{p}_0$ and L_∞/F_∞ is unramified.

This implies that the natural map $I \to H/\mathscr{Y}_\infty = \Gamma$ is an isomorphism. Under this isomorphism, the action of Γ corresponds to I acting on $\mathscr{Y}_\infty$ by conjugation. Let $\sigma_0 \in I$ be the element mapping to γ_0. To lessen the risk of confusion, let us denote the action exponentially. Thus it remains to show that $[H,H] = \mathscr{Y}_\infty^{(\sigma_0-1)}$. If $y \in \mathscr{Y}_\infty$, we have $y^{\sigma_0-1} = \sigma_0 y \sigma_0^{-1} y^{-1} = [\sigma_0, y]$. Conversely, let $a,b \in H$. Writing $a = \alpha x, b = \beta y$ with $\alpha,\beta \in I, x,y \in \mathscr{Y}_\infty$, a straightforward calculation shows that $[a,b] = (x^\alpha)^{1-\beta}(y^\beta)^{\alpha-1}$. Because σ_0 topologically generates I, $1-\beta$ and $\alpha - 1$ are divisible by $\sigma_0 - 1$ in the Iwasawa algebra $\Lambda(I)$. Thus $[a,b] \in \mathscr{Y}_\infty^{\sigma_0-1}$.

Write $H_n = \mathrm{Gal}(L_\infty/F_n)$ and $I_n = H_n \cap I$. One deduces from the previous points that

$$I_n = I^{p^n}, H_n = I_n\mathscr{Y}_\infty \text{ and } [H_n,H_n] = \mathscr{Y}_\infty^{(\sigma_0^{p^n}-1)}.$$

Because L_n is the maximal abelian unramified subextension of L_∞/F_n, we deduce that

$$\mathscr{Y}_n = \frac{\mathrm{Gal}(L_\infty/F_n)}{\mathrm{Gal}(L_\infty/L_n)} = \frac{H_n}{[H_n,H_n]I^{p^n}} = \frac{I^{p^n}\mathscr{Y}_\infty}{I^{p^n}\mathscr{Y}_\infty^{(\sigma_0^{p^n}-1)}} = \mathscr{Y}_\infty/\mathscr{Y}_\infty^{(\sigma_0^{p^n}-1)}. \qquad \square$$

Lemma 2.1.4. The group $\mathscr{Y}_\infty$ is a finitely generated Λ-module.

Proof. As $T \in (p,T)$, $\mathscr{Y}_\infty/(p,T)\mathscr{Y}_\infty$ is a quotient of $\mathscr{Y}_0 = \mathscr{Y}_\infty/T\mathscr{Y}_\infty$, hence finite. The result now follows from Nakayama's lemma 1.3.4. $\square$

Remark 2.1.5. Note that the application of Nakayama's lemma yields something else interesting: namely, $\mathscr{Y}_\infty = 0$ if and only if $\mathscr{Y}_n = 0$ for some n. In particular, we see that $p \mid h_n$ for some n if and only if $p \mid h_n$ for all n.

Proof of Theorem 2.1.2. By the structure theorem and the previous lemma, there is a module of the form

$$A = \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j^{n_j})$$

and a pseudo-isomorphism $\phi\colon \mathscr{Y}_\infty \to A$. Writing $A_n = A/\varphi^n(T)A$, we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \varphi^n(T)\mathscr{Y}_\infty & \longrightarrow & \mathscr{Y}_\infty & \longrightarrow & \mathscr{Y}_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & \varphi^n(T)A & \longrightarrow & A & \longrightarrow & A_n & \longrightarrow & 0 \end{array}$$

Applying the snake lemma immediately yields the following:

(i) $\#\ker(\phi'_n) \le \#\ker(\phi)$

(ii) $\#\operatorname{coker}(\phi''_n) \le \#\operatorname{coker}(\phi)$

(iii) $\#\operatorname{coker}(\phi'_n) \le \#\operatorname{coker}(\phi)$

(iv) $\#\ker(\phi''_n) \le \#\ker(\phi)\#\operatorname{coker}(\phi)$

(v) $\#\operatorname{coker}(\phi_n)\#\ker(\phi'_n)\ker(\phi''_n) = \#\ker(\phi_n)\#\operatorname{coker}(\phi'_n)\operatorname{coker}(\phi''_n)$

Additionally, if $m \ge n \ge 0$, we have

(a) $\#\ker(\phi'_n) \ge \#\ker(\phi'_m)$

(b) $\#\operatorname{coker}(\phi'_n) \ge \#\operatorname{coker}(\phi'_m)$

(c) $\#\operatorname{coker}(\phi''_n) \le \#\operatorname{coker}(\phi''_m)$

All of these taken together imply that as n grows, the sizes of $\ker(\phi''_n)$ and $\operatorname{coker}(\phi''_n)$ eventually stabilize. We conclude that $\#\mathscr{Y}_n = \#A_n \cdot \frac{\#\ker(\phi''_n)}{\#\operatorname{coker}(\phi''_n)} = \#A_n \cdot p^c$ for some constant c and large enough n. We are therefore reduced to showing that $\#A_n = \mu p^n + \lambda n + \nu$ for some μ, λ, ν and large enough n. In fact, still writing

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

we will show that we can take $\mu = \sum_{i=1}^{s} m_i$ and $\lambda = \sum_{j=1}^{t} n_j \deg(f_j)$. We first state the following lemma, which tells us that we can divide with remainder by distinguished polynomials.

Lemma 2.1.6. Let $f \in \Lambda$ be a distinguished polynomial of degree d. Then for any $g \in \Lambda$, there exist unique $q, r \in \Lambda$ with r a polynomial of degree $< d$, such that $g = qf + r$.

The proof can be found in [Was97, Proposition 7.2]. Now, the lemma immediately implies that $\Lambda/(\varphi^n(T))$ is infinite, so that we must have $r = 0$ in the decomposition. Furthermore, it is clear that $\#\Lambda/(\varphi^n(T), p^m) = p^{mp^n}$. It remains to show that for g a distinguished polynomial of degree d, we have that $\#\Lambda/(g(T), \varphi^n(T)) = p^{dn+c}$ for large enough n. This turns out to be a bit technical, but the idea is to use the division algorithm to show that when $p^{n-1} \geq d$, we have $\#\Lambda/(g(T), \varphi^{n+1}(T)) = p^d \#\Lambda/(g(T), \varphi^n(T))$. The details are in [Lan90, Chapter 5, Theorem 1.2]. □

Note that while the proof above shows that μ, λ, ν and n_0 as in the theorem exist, it does not give us any way to find them. There is no way to find n_0, and to find the other invariants it seems we would need to have complete knowledge of the structure of all the class groups $\mathscr{Y}_n$. One might think we could look at the proof of the structure theorem to see how m_i, f_j and n_j are obtained from the module. Alas, we would see that we need an explicit finite presentation of $\mathscr{Y}_\infty$, something which is of course again unrealistic to ask for given limited knowledge of the class groups. In the next section we will focus our attention to the case $F_n = \mathbf{Q}(\mu_{p^{n+1}})$, and prove an *effective* version of the theorem. We will see how in this case μ, λ and n_0 are connected to p-adic L-functions.

§2.2 An effective version of the growth theorem

For the rest of this chapter, let $F_n = \mathbf{Q}(\zeta_{p^{n+1}})$ and $F_\infty = \mathbf{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} F_n$. Then F_∞/F_0 is a $\mathbf{Z}_p$-extension. Indeed, there is an isomorphism

$$\varkappa \colon \mathrm{Gal}(F_\infty/\mathbf{Q}) \to \mathbf{Z}_p^\times$$

characterized by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\varkappa(\sigma)}$, called the *cyclotomic character*. We have a decomposition $\mathbf{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbf{Z}_p)$, the latter factor being isomorphic to $\mathbf{Z}_p$. The fixed field of the this subgroup is then exactly F_0. Similarly, we have that F_∞^+/F_0^+ is a $\mathbf{Z}_p$-extension as well, where the $+$ indicates the maximal real subfield.

We write h_n and h_n^+ for the class numbers of F_n and F_n^+, respectively. By class field theory, h_n^+ divides h_n, and we denote the quotient by h_n^-, which is called the *relative class number*. Why would we be interested in this number? There are two main reasons. Firstly, the relative class number is much easier to handle than the individual class numbers h_n and h_n^+. Part of the reason that class groups are hard to study, is because they are intimately related to unit groups. For instance, the analytic class number

formula allows us to compute the product of the class number and the regulator with relative ease, but gives no way to separate the two. However, the unit groups of F_n and F_n^+ have the same rank, and most of the complications introduced by them disappear upon dividing the class numbers. Secondly, it is conjectured that p never divides h_0^+. A prime with this property is called a *Vandiver prime*, so that conjecturally, every prime is a Vandiver prime. This is known as the Kummer–Vandiver conjecture. Remark 2.1.5 implies that a Vandiver prime does not divide h_n^+ for any n. Since we are interested in studying $\mathrm{ord}_p(h_n)$, it therefore makes sense to study $\mathrm{ord}_p(h_n^-)$, since we expect these to be the same. While there is virtually no progress towards a proof of the conjecture, it has been confirmed for all primes $< 2^{31}$ by Hart, Harvey & Ong [HHO17]. In this sense, for all practical applications of Theorem 2.1.2, we can simply work with h_n^- instead.

Now that we have motivated the study of h_n^-, we will prove the following effective version of Iwasawa's theorem.

Theorem 2.2.1. For $i = 2, 4, \cdots, p-3$, let $f_i \in \mathbf{Z}_p[\![T]\!]$ be the power series from Theorem 1.5.4. Write $f_i = p^{\mu_i} P_i(T) U_i(T)$ with P_i distinguished of degree λ_i and U_i a unit, and write P for the product of the P_i. Let n_0 be such that $\max_i \lambda_i < p^{n_0} - p^{n_0-1}$. Then for all $n \geq n_0$, we have that

$$\mathrm{ord}_p(h_n^-) = \mu p^n + \lambda n + \nu,$$

where

$$\mu = \sum_i \mu_i,$$

$$\lambda = \sum_i \lambda_i,$$

$$\nu = \sum_{\substack{\zeta^{p^{n_0-1}}=1 \\ \zeta \neq 1}} \mathrm{ord}_p\left(\frac{P(\zeta(1+p)-1)}{\zeta - 1}\right) - \mu + \mathrm{ord}_p(h_0^-).$$

Proof. From the analytic class number formula for F_n and F_n^+, it follows that

$$h_n^- = 2p^{n+1} \prod_{\chi \text{ odd}} \left(-\frac{1}{2} B_{1,\chi}\right) = 2p^{n+1} \prod_{\chi \text{ even}} \left(-\frac{1}{2} B_{1,\chi\omega^{-1}}\right),$$

where the product runs over Dirichlet characters of conductor dividing p^{n+1}. As before, we may write any such character as a product of some ω^i and a character θ of $1 + p\mathbf{Z}_p$ vanishing on $1 + p^{n+1}\mathbf{Z}_p$. Thus, up to multiplication by a p-adic unit, this

product becomes

$$p^{n+1} \prod_{i \text{ even}} B_{1,\omega^{i-1}} \prod_{\theta \neq 1} B_{1,\theta\omega^{-1}} \prod_{\substack{\theta,\omega^i \neq 1 \\ i \text{ even}}} B_{1,\theta\omega^{i-1}}.$$

Here the middle product runs over the characters of $1 + p\mathbf{Z}_p$ that are trivial on $1 + p^{n+1}\mathbf{Z}_p$. Let us first analyze this middle product. It is (up to a unit) equal to

$$\prod_{\theta \neq 1} L_p(\theta, 0) = \prod_{\theta \neq 1} \frac{\int_{\mathbf{Z}_p^\times} \theta(x)\langle x \rangle x^{-1} \cdot \mu_a}{1 - \theta(a)\langle a \rangle}$$

where we can take $a = 1 + p$. Write $\zeta_\theta = \theta(a)$. Then ζ_θ is a p^n-th root of unity. Hence $\mathrm{ord}_p(1 - \zeta_\theta) < 1$, so that $\mathrm{ord}_p(1 - \theta(a)\langle a \rangle) = \mathrm{ord}_p(1 - \zeta_\theta + \zeta_\theta p) = \mathrm{ord}_p(1 - \zeta_\theta)$. As θ runs through the characters trivial on $1 + p^{n+1}\mathbf{Z}_p$, ζ_θ runs through all p^n-th roots of unity. We therefore have that

$$\prod_{\theta \neq 1} \frac{1}{1 - \theta(a)\langle a \rangle} \sim \prod_{\substack{\zeta^{p^n} = 1 \\ \zeta \neq 1}} \frac{1}{1 - \zeta} = p^{-n},$$

where $\sim$ means equality up to a p-adic unit.

Let us now turn to the integral $\int_{\mathbf{Z}_p^\times} \theta(x)\langle x \rangle x^{-1} \cdot \mu_a$. We claim that it is a p-adic unit. As $\theta(x)$ is a power of ζ_θ, we have $\theta(x) \equiv 1 \bmod 1 - \zeta_\theta$, and of course $\langle x \rangle \equiv 1 \bmod p$, so that $\theta(x)\langle x \rangle \equiv 1 \bmod 1 - \zeta_\theta$. Thus it suffices to show that $\int_{\mathbf{Z}_p^\times} x^{-1} \cdot \mu_a$ is a unit.

Note that for $x, y \in \mathbf{Z}_p^\times$, we have $|x^{-1} - y^{-1}| = \frac{|x-y|}{|xy|} = |x - y|$. It follows that the locally constant function $\sum_{r=1}^{p-1} r^{-1} \mathbf{1}_{r+p\mathbf{Z}_p}$ approximates x^{-1} 'up to order p' in the sense that

$$x^{-1} \equiv \sum_{r=1}^{p-1} r^{-1} \mathbf{1}_{r+p\mathbf{Z}_p}(x) \bmod p$$

for all $x \in \mathbf{Z}_p$. Thus $\int_{\mathbf{Z}_p^\times} x^{-1} \cdot \mu_a \equiv \sum_{r=1}^{p-1} r^{-1} \int_{r+p\mathbf{Z}_p} \mu_a \bmod p$. We now calculate that

$$\begin{aligned}
\int_{r+p\mathbf{Z}_p} \mu_a &= \mathscr{A}_{\mathrm{Res}_{r+p\mathbf{Z}_p}\mu_a}(0) \\
&= p^{-1} \sum_{\zeta^p=1} \zeta^r \mathscr{A}_{\mu_a}(\zeta - 1) \\
&= p^{-1}\mathscr{A}_{\mu_a}(0) + p^{-1} \sum_{\substack{\zeta^p=1 \\ \zeta\neq 1}} \zeta^r \left(\frac{a}{\zeta^a - 1} - \frac{1}{\zeta - 1} \right) \\
&= -\frac{1}{2} + \sum_{\substack{\zeta^p=1 \\ \zeta\neq 1}} \frac{\zeta^r}{1-\zeta}
\end{aligned}$$

We claim that this last sum is equal to $r - \frac{p+1}{2}$. It suffices to show that this holds for $r = 1$ and that the difference between the sums for $r+1$ and r is 1. The case $r = 1$ is simple: it becomes

$$\sum_{\substack{\zeta^p=1 \\ \zeta\neq 1}} \left(\frac{1}{1-\zeta} - 1 \right) = \frac{\Phi_p'(1)}{\Phi_p(1)} - (p-1) = \frac{(1-p)}{2},$$

where Φ_p is the p-th cyclotomic polynomial. Next, for $r = 1, \ldots, p-2$, we have that

$$\begin{aligned}
\sum_{\substack{\zeta^p=1 \\ \zeta\neq 1}} \frac{\zeta^{r+1}}{1-\zeta} - \frac{\zeta^r}{1-\zeta} &= \sum_{\substack{\zeta^p=1 \\ \zeta\neq 1}} \frac{1-\zeta^r}{1-\zeta} - \frac{1-\zeta^{r+1}}{1-\zeta} \\
&= -\sum_{\substack{\zeta^p=1 \\ \zeta\neq 1}} \zeta^r = 1
\end{aligned}$$

as was to be shown.

All in all we find that $\int_{r+p\mathbf{Z}_p} \mu_a = r - \frac{p}{2}$, so that

$$\begin{aligned}
\int_{\mathbf{Z}_p^\times} x^{-1} \cdot \mu_a &\equiv \sum_{r=1}^{p-1} r^{-1} \int_{r+p\mathbf{Z}_p} \mu_a \\
&\equiv \sum_{r=1}^{p-1} 1 \equiv -1 \bmod p
\end{aligned}$$

In particular, it is a unit as claimed.

We have shown thus far that

$$\frac{h_n^-}{h_0^-} \sim \prod_{\substack{\theta,\omega^i\neq 1\\ i \text{ even}}} B_{1,\theta\omega^{i-1}} \sim \prod_{\theta\neq 1}\prod_{\substack{i\neq 0\\ i \text{ even}}} L_p(\theta\omega^i, 0) = \prod_{\substack{\zeta^{p^n}=1\\ \zeta\neq 1}}\prod_{\substack{i\neq 0\\ i \text{ even}}} f_i(\zeta_\theta(1+p)-1).$$

Write $f_i(T) = p^{\mu_i} P_i(T) U_i(T)$ with P_i distinguished of degree λ_i, and U_i a unit. Choose n_0 such that $\lambda_i < p^{n_0} - p^{n_0-1}$ for all i. If ζ is root of unity of order p^k, then $\operatorname{ord}_p(\zeta(1+p)-1) = \operatorname{ord}_p(\zeta-1) = \frac{1}{p^k - p^{k-1}}$. Thus for $k \geq n_0$, we have

$$\operatorname{ord}_p(P_i(\zeta(1+p)-1)) = \lambda_i \operatorname{ord}_p(\zeta-1).$$

It follows that for $n \geq n_0$,

$$\begin{aligned}\operatorname{ord}_p\left(\frac{h_n^-}{h_0^-}\right) &= \mu(p^n-1) + \sum_{\substack{\zeta^{p^n}=1\\ \zeta\neq 1}} \operatorname{ord}_p(P(\zeta(1+p-1)))\\ &= \mu(p^n-1) + \lambda \sum_{\substack{\zeta^{p^n}=1\\ \zeta\neq 1}} \operatorname{ord}_p(\zeta-1) + C\\ &= \mu p^n + \lambda n + (C-\mu),\end{aligned}$$

where

$$C = \sum_{\substack{\zeta^{p^{n_0-1}}=1\\ \zeta\neq 1}} \operatorname{ord}_p(P(\zeta(1+p)-1)) - \operatorname{ord}_p(\zeta-1).$$

Thus we have shown that

$$\operatorname{ord}_p(h_n^-) = \mu p^n + \lambda n + \nu$$

for $n \geq n_0$, with $\nu = C - \mu + \operatorname{ord}_p(h_0^-)$. □

It would be remiss not to mention the following remarkable result of Ferrero and Washington regarding the μ-invariant, that actually holds true for more general number fields.

Theorem 2.2.2 (Ferrero–Washington). Let F_0 be an abelian number field. Then the μ-invariant of the cyclotomic $\mathbf{Z}_p$-extension of F_0 vanishes.

Proof. See [Was97, Theorem 7.15]. □

As mentioned, so far the equality $\operatorname{ord}_p h_n = \operatorname{ord}_p h_n^+$ has been verified for all $p < 2^{31}$ in [HHO17]. The same paper also verified for all these primes that $\mu = 0$ (which we also know to be true by the Ferrero–Washington theorem) and $\lambda = \nu = i_p$, where i_p is the number of L-functions $f_2, \ldots, f_{p-3}$ which have a zero, known as the *irregularity index* of p. Note that we always have $i_p \leq \lambda$, with equality if and only if all L-functions have at most one zero. In particular, we can take $n_0 = 1$ in the preceding theorem. Lastly, by the interpolation formula $f_k((1+p)^k - 1) = L_p(\omega^k, 1-k) = -(1-p^{k-1})\frac{B_k}{k}$ and the Weierstrass preparation theorem, f_k has a zero if and only if B_k is divisible by p. Combining all of this, we get the following practical result.

Theorem 2.2.3. If $p < 2^{31}$, we have that

$$\operatorname{ord}_p(\#\mathrm{Cl}(\mathbf{Q}(\zeta_{p^n}))) = \lambda n$$

for all $n \geq 1$, where λ is the number of Bernoulli numbers $B_2, B_4, \cdots, B_{p-3}$ that are divisible by p.

§2.3 Examples of p-adic L-functions

The results from the previous chapter motivate us to look at how one might compute the λ-invariant for a prime by considering their p-adic L-functions. By the Weierstrass preparation theorem and the Ferrero–Washington theorem 2.2.2, the number of zeros of a power series $\sum_{n\geq 0} a_n T^n$ is equal to the smallest index n for which a_n is not divisible by p. Thus to find the λ invariant, it suffices to find an approximation of the L-functions that is accurate modulo p.

Lemma 2.3.1. Let $f \in \mathbf{Z}_p[\![T]\!]$ be a power series, and let $g \in \mathbf{Z}_p[T]$ be a polynomial that agrees with f in at least n points. Then $f \equiv g \bmod (p, T^n)$.

Proof. By the Weierstrass preparation theorem, we may write $f(T) - g(T) = p^\mu P(T)U(T)$ with P a distinguished polynomial of degree at least n, so that $P \equiv 0 \bmod (p, T^n)$. □

Consequently, to find our modulo p approximation up to a certain number of terms, we only need to find a polynomial that agrees with f_i in a certain number of points. But this is easy: after all, we know that $f_i((1+p)^k - 1) = -(1-p^{k-1})\frac{B_k}{k}$ for all $k \equiv i \bmod p-1$. We do however need to be careful that the resulting interpolating polynomial is actually a polynomial over $\mathbf{Z}_p$, otherwise we cannot apply the above lemma. Using this method, we find for instance that for $p = 5$, the power series f_2 is given by

$$f_2(T) \equiv 2 + T + T^3 + T^4 \bmod (p, T^5).$$

Note that f_2 is in this case the only interesting power series, since f_0 is not a power series, and f_1, f_3 are identically zero.

As an another example, the Iwasawa power series for $p = 11$ are given by

$$\begin{aligned}
f_2(T) &\equiv 10 + \ \ 5T + 6T^2 + 7T^3 + \ \ T^4 \bmod (p, T^5) \\
f_4(T) &\equiv 10 + 10T + 8T^2 + 3T^3 + 8T^4 \bmod (p, T^5) \\
f_6(T) &\equiv 1 \ \ + \ \ 9T + 5T^2 + 7T^3 + 6T^4 \bmod (p, T^5) \\
f_8(T) &\equiv 5 \ \ + 10T + 8T^2 + 8T^3 + 4T^4 \bmod (p, T^5)
\end{aligned}$$

We can see that none of these series so far have constant terms which are divisible by p, which is to be expected, since 5 and 11 are regular primes. The smallest irregular prime is $p = 37$, for which the 32nd series has a zero:

$$f_{32}(T) \equiv 21T + 8T^2 + 35T^3 + 15T^4 \bmod (p, T^5).$$

This agrees with the fact that $B_{32} = -37 \times \frac{214147806700}{510}$ is divisible by 37, and that the class number of $\mathbf{Q}(\zeta_{37})$ is 37.

The smallest prime for which multiple series have a zero is $p = 157$, and it concerns the following series:

$$\begin{aligned}
f_{62}(T) &\equiv 48T + \ \ 65T^2 + 28T^3 + 142T^4 \bmod (p, T^5) \\
f_{110}(T) &\equiv 51T + 128T^2 + 16T^3 + 139T^4 \bmod (p, T^5)
\end{aligned}$$

A remarkable class number computation has shown that the class number of $\mathbf{Q}(\zeta_{157})$ is equal to

$$5 \cdot 13^2 \cdot 157^2 \cdot 1093 \cdot 1873 \cdot 418861 \cdot 3148601.$$

Note the factor of 157^2, which agrees with what we expect from looking at the L-functions. The next few primes for which two series have a zero are $p = 353, 379, 467$. Not long after, we find the first prime for which three of the power series have a zero, namely $p = 491$:

$$\begin{aligned}
f_{292}(T) &= 456T + 189T^2 + 268T^3 + 282T^4 \bmod (p, T^5) \\
f_{336}(T) &= 103T + 240T^2 + 233T^3 + 232T^4 \bmod (p, T^5) \\
f_{338}(T) &= 475T + \ \ 98T^2 + 342T^3 + 296T^4 \bmod (p, T^5)
\end{aligned}$$

Even though we have no idea what the class number of $\mathbf{Q}(\zeta_{491})$ is, this definitively shows not only that this number is exactly divisible by 491^3, but also that the class number of $\mathbf{Q}(\zeta_{491^2})$ is divisible by 491^6, that of $\mathbf{Q}(\zeta_{491^3})$ is divisible by 491^9, etc, even though we will probably never know what these class numbers are.

Now, what if we are interested in finding more accurate approximations of p-adic L-functions? We can still do this by finding a polynomial that interpolates certain values of the L-function, except that the points have to be chosen more carefully to guarantee a higher p-adic accuracy.

Proposition 2.3.2. Let μ be a measure on $\mathbf{Z}_p^\times$, and let $P_{n,i}$ be the polynomial

$$P_{n,i}(T) = \sum_{k=1}^{p-1} \sum_{j=0}^{p^n-1} \omega^i(k)\mu(\omega(k)(1+p)^j + p^{n+1}\mathbf{Z}_p)(1+T)^j.$$

Then if ζ is a p^n-th root of unity, and $\theta\colon \mathbf{Z}_p^\times \to \overline{\mathbf{Q}}_p^\times$ is the character trivial on μ_{p-1} with $\theta(1+p) = \zeta$, we have that

$$P_{n,i}(\zeta - 1) = \int_{\mathbf{Z}_p^\times} \theta\omega^i \cdot \mu.$$

Proof. This follows immediately upon noting that $\mathbf{Z}_p^\times$ is the disjoint union of the sets $\omega(k)(1+p)^j + p^{n+1}\mathbf{Z}_p$, and that on such a set, $\theta\omega^i$ is constant with value $\omega^i(k)\zeta^j$. □

In particular, applying this to the measures λ_a and $[1]-[a]$ from Chapter 1, we get polynomials that agree with the power series g_i and h_i from Theorem 1.5.4 in the values $\zeta - 1$. Thus the difference between our approximation and the true power series will be divisible by $\varphi^n(T) = (1+T)^{p^n} - 1$. The coefficients of this polynomial are of course the binomial coefficients $\binom{p^n}{k}$, which become more and more divisible by p as n increases. For instance, for $k = 0, \ldots, p-1$ they are divisible by p^n, so that the first p terms of our approximation are accurate modulo p^n.

Proposition 2.3.2 appears in [SW13] (though with $i = 0$) as a way to compute p-adic L-functions of elliptic curves. It is also the basis for SageMath's built-in algorithm for computing these L-functions. Curiously, Sage has no built-in methods to compute the Kubota–Leopoldt p-adic L-functions discussed in this thesis. Luckily, the techniques described above are easy enough to implement.[1] This way, we can for instance compute the 32nd L-function for $p = 37$ that is accurate modulo p^3:

$$\begin{aligned} f_{32}(T) = {} & (30 \cdot 37 + 31 \cdot 37^2) + (21 + 30 \cdot 37 + 25 \cdot 37^2)T \\ & + (8 + 6 \cdot 37)T^2 + (35 + 6 \cdot 37 + 6 \cdot 37^2)T^3 \\ & + (15 + 4 \cdot 37 + 3 \cdot 37^2)T^4 \bmod (p^3, T^5) \end{aligned}$$

[1] For example, see https://gitlab.com/niels-ketelaars/iwasawa

Using the mentioned code to do this already reveals a big weakness: computing the above series already takes almost 5 minutes on standard hardware. Trying to compute a series for $p = 157$ with a similar accuracy is already infeasible.

§2.4 Heuristics for Iwasawa invariants

From the examples we have seen, it appears that the λ-invariant of a prime is usually not that large. It is almost always 0, and was shown in [HHO17], it is always smaller than 10 for all $p < 2^{31}$. Furthermore, for all these primes there is actually no L-function which has more than a single zero. This suggests that we can always take $n_0 = 1$ in Theorem 2.2.1. In this section we analyze some heuristics for why this might be the case.

Let us denote by i_p the *irregularity index* of p, which is defined to be the number of p-adic L-functions $f_2, \dots, f_{p-3}$ which have a zero. We have remarked that $i_p = \lambda$ for all primes below 2^{31}. Is this what we expect to happen in general?

We will make the following assumption:

> The coefficients of each Iwasawa power series are independently, uniformly distributed modulo p.

We will show that we expect that for all but finitely many primes, $\lambda \leq i_p + 1$. There are two ways in which this inequality can fail to be true. The first is that one of the L-functions has three zeros, or equivalently, has its first three coefficients divisible by p. Under our assumption, the probability that for a given series at least one of its first three coefficients is not divisible by p is $1 - p^{-3}$. Thus, the probability that this holds for all $(p-3)/2$ series is $(1-p^{-3})^{(p-3)/2}$. Consequently, we have with probability $1-(1-p^{-3})^{(p-3)/2}$ that some series has its first three coefficients divisible by p. Because

$$1 - (1-p^{-3})^{(p-3)/2} \leq \frac{p-3}{2} p^{-3} = O(p^{-2}),$$

the sum of these probabilities over all p converges. This implies (for instance, via the Borel-Cantelli lemma from probability theory) that with probability 1, it happens only finitely often that some L-function has three zeros.

The second way in which it can happen that $\lambda > i_p + 1$ is if at least two series have their first two coefficients divisible by p. Using the same reasoning as above, we have a probability of $(1-p^{-2})^{(p-3)/2}$ that no power series has its first two coefficients divisible by p. Similarly, the probability of exactly one series having this property is

$$\binom{(p-3)/2}{1} \left(1-p^{-2}\right)^{(p-3)/2-1} p^{-2}.$$

Thus the probability that at least two power series have their first two coefficients divisible by p comes down to

$$1 - \left((1-p^{-2})^{(p-3)/2} + \binom{(p-3)/2}{1} \left(1-p^{-2}\right)^{(p-3)/2-1} p^{-2} \right) = O(p^{-2}).$$

Thus we should also expect this to only happen finitely often. It should therefore hold that $\lambda \leq i_p + 1$ for almost all p. In particular, we see that most of the time, an L-function has at most 1 zero. If it does happen to have 2 zeros, then it is most likely the only L-function for that prime to have multiple zeros.

§2.5 Towards the Main Conjecture

Looking at the proof of Theorem 2.1.2, we see that the λ-invariant is precisely the number of zeros of a generator of the characteristic ideal $\mathrm{ch}(\mathscr{Y}_\infty)$. On the other hand, Theorem 2.2.1 tells us it is the number of zeros of the product $f = \prod_{i \text{ even}} f_i$ of the p-adic L-functions. This begs the question: is this product perhaps a generator for the characteristic ideal of $\mathscr{Y}_\infty$?

First note that the λ from Theorem 2.1.2 is different from the one in 2.2.1. The first has to do with the class numbers h_n, while the latter contributes only to the relative class number h_n^-. Thus the above conjecture on the characteristic ideal is certainly stronger than the Kummer–Vandiver conjecture that $\mathrm{ord}_p h_n = \mathrm{ord}_p h_n^-$. It seems that we cannot reasonably hope to answer our question. We could of course assume the Kummer–Vandiver conjecture (and we even know that is true for all $p < 2^{31}$) and see if that leads to a proof, but we can actually refine our question on the characteristic ideal in a way that it is independent from Kummer–Vandiver.

Let $G_n = \mathrm{Gal}(F_n/\mathbf{Q})$, $G_n^+ = \mathrm{Gal}(F_n^+/\mathbf{Q})$ and similarly define $G = \mathrm{Gal}(F_\infty/\mathbf{Q}) \cong \Gamma \times G_0$ and $G^+ = \mathrm{Gal}(F_\infty^+/\mathbf{Q}) \cong \Gamma \times G_0^+$. Note that our action of Γ on $\mathscr{Y}_\infty$ extends in an obvious way to an action of G. We may identify G_0 with $(\mathbf{Z}/p\mathbf{Z})^\times$, in which case every character of G_0 is given by a power of the Teichmüller character ω. Recall that we have idempotents $e_i = \frac{1}{p-1} \sum_{a \in G_0} \omega^i(a)[a^{-1}] \in \mathbf{Z}_p[G_0]$, which allow us to decompose $\mathscr{Y}_\infty = \bigoplus_i e_i \mathscr{Y}_\infty$. Let $e_+ = \sum_{i \text{ even}} e_i$ and $e_- = 1 - e_+$. Then in fact $e_+\mathscr{Y}_\infty$ is naturally isomorphic to $\mathscr{Y}_\infty^+ = \mathrm{Gal}(L_\infty^+/F_\infty^+)$. It follows that $e_+\mathscr{Y}_n$ has order $\mathrm{ord}_p h_n^+$, and hence $e_-\mathscr{Y}_\infty$ has order $\mathrm{ord}_p h_n^-$.

Thus we can now ask, is the characteristic ideal of $e_-\mathscr{Y}_\infty$ generated by the product of the L-functions? If the Kummer–Vandiver conjecture is true, we have $e_+\mathscr{Y}_\infty = 0$, and this question therefore reduces to the previous one. But we can try to be even more precise. We still have a decomposition $e_-\mathscr{Y}_\infty = \bigoplus_{i \text{ odd}} e_i \mathscr{Y}_\infty$, and so we could even ask if the characteristic ideal of $e_i\mathscr{Y}_\infty$ is generated by some individual L-function. It

cannot of course be generated by f_i, since this power series is identically 0 for i odd. The correct answer turns out to be the following:

Theorem 2.5.1. For $i \not\equiv 1 \bmod p-1$ odd, we have that

$$\mathrm{ch}(e_i\mathscr{Y}_\infty) = f_{p-i}\left(\frac{1+p}{1+T} - 1\right)\Lambda.$$

This is known as the *Main Conjecture of Iwasawa theory* (even though it is a theorem nowadays, the name has stuck). It was first proven by Mazur and Wiles [MW84] using modular forms. Later a simpler proof was found by Karl Rubin [Lan90, Appendix] using what are now known as *Euler systems*. The rest of this thesis will be dedicated to studying this proof.

We first mention that the version of the Main Conjecture mentioned here is slightly different from the version that is usually encountered, which is also the version we will prove. Let M_n be the maximal abelian p-extension of F_n that is unramified away from p, and let $\mathscr{X}_n = \mathrm{Gal}(M_n/F_n)$. Define M_∞ and $\mathscr{X}_\infty$ analogously. In the same way as $\mathscr{Y}_\infty$, $\mathscr{X}_\infty$ is $\Lambda(G)$-module, which is in fact finitely generated. Furthermore, if V is any $\Lambda(G)$-module, let V' denote the $\Lambda(G)$-module with the same underlying group, but where the action of G is now defined as $g \cdot v := \varkappa(g)g^{-1}v$, where the latter expression is taken to mean the original action of G on V. Iwasawa [Iwa73] showed that for each even $i \not\equiv 0 \bmod p-1$, the Λ-module $e_i\mathscr{X}_\infty$ is pseudo-isomorphic to $e_{p-i}\mathscr{Y}'_\infty$. On the level of characteristic ideals it is seen that this implies that the Main Conjecture can be equivalently stated as follows:

Theorem 2.5.2. For $i \not\equiv 0 \bmod p-1$ even, we have that

$$\mathrm{ch}(e_i\mathscr{X}_\infty) = f_i\Lambda.$$

3 Local units and power series

Since the Main Conjecture concerns certain modules over the Iwasawa algebra $\Lambda = \mathbf{Z}_p[\![T]\!]$, it makes sense to start with a more thorough study of this ring itself. We do this by introducing two important operations: the norm and the logarithmic derivative. We start by studying the norm map, and use it to prove a theorem of Coleman, which relates certain power series in Λ to units in completions of cyclotomic fields. After this, we turn to the logarithmic derivative, which gives us a way to relate the norm map to the trace map from Chapter 1. As a result we will be able to derive multiple exact sequences giving us insight into the structure of the Iwasawa algebra.

The presentation of this material is heavily inspired by [CS06, Chapter 2], though we have tried to be more clear and give simpler proofs in a number of places.

§3.1 The norm map

Our goal in this section if to prove the following proposition, which asserts the existence of a multiplicative analogue of the trace map ψ. Recall that the Frobenius map $\varphi\colon \Lambda \to \Lambda$ was defined by $\varphi(f) = f((1+T)^p - 1)$.

Proposition 3.1.1. There exists a unique multiplicative map $\mathcal{N}\colon \Lambda \to \Lambda$ such that

$$(\varphi \circ \mathcal{N})(f) = \prod_{\eta^p = 1} f((1+T)\eta - 1)$$

Proof. Uniqueness follows from injectivity of φ. For existence, we first show that a power series f is in the image of φ if and only if it satisfies $f((1+T)\eta - 1) = f(T)$ for all $\eta \in \mu_p$. Indeed, suppose f has this property. Then $f(\eta - 1) = f(0)$ for all $\eta \in \mu_p$, and by the Weierstrass preparation theorem, $f(T) - f(0)$ must be divisible by $\prod_{\eta^p=1}(T - \eta) = \varphi(T)$. If we write $f(T) - f(0) = \varphi(T)f_1(T)$, we see that f_1 also has the property that $f_1((1+T)\eta - 1) = f_1(T)$. Thus we may write $f_1(T) - f_1(0) = \varphi(T)f_2(T)$. Continuing this

indefinitely, we obtain a sequence $\alpha_1, \alpha_2, \dots$ such that $f(T) - \sum_{k=0}^{n} \alpha_k \varphi(T)^k \in \varphi(T)^{n+1}\Lambda$ (where $\alpha_0 = f(0), \alpha_1 = f_1(0), \dots$). Since $\varphi(T) \in (p, T)$, we may take $n \to \infty$ to obtain that $f(T) = \varphi(\sum_{k \geq 0} \alpha_k T^k)$.

Now, for any $f \in \Lambda$, the power series $h(T) = \prod_{\eta^p = 1} f((1+T)\eta - 1)$ satisfies the hypothesis that $h((1+T)\eta - 1) = h(T)$ for all η, so it lies in the image of φ. Therefore we may define

$$\mathcal{N}(f) := \varphi^{-1}\left(\prod_{\eta^p = 1} f((1+T)\eta - 1) \right),$$

which satisfies the desired relation. □

Note the similarity of this result with Proposition 1.2.1. Being the multiplicative analogue of the trace map, it is aptly named the *norm* map. The next proposition tells us that the procedure of iterating the norm map enjoys some nice convergence properties.

Proposition 3.1.2. The norm map has the following properties:

1. If $f \in \Lambda^\times$, we have $\mathcal{N}(f) \equiv f \bmod p\Lambda$.
2. If $f \equiv 1 \bmod p^k\Lambda$, then $\mathcal{N}(f) \equiv 1 \bmod p^{k+1}\Lambda$.
3. If $f \in \Lambda^\times$, $k_2 \geq k_1 \geq 0$, then $\mathcal{N}^{k_2}(f) \equiv \mathcal{N}^{k_1}(f) \bmod p^{k_1+1}\Lambda$.

In particular, point 3 implies the sequence $\mathcal{N}^n(f)$ is Cauchy, and hence convergent. To prove the proposition, we need a lemma.

Lemma 3.1.3. Let $f \in \Lambda$. If $\varphi(f) \equiv 1 \bmod p^k\Lambda$, then $f \equiv 1 \bmod p^k\Lambda$.

Proof. Note that $\varphi(T) \equiv T^p \bmod p\Lambda$, and therefore $\varphi(h) \equiv h(T^p) \bmod p\Lambda$ for $h \in \Lambda$. In particular, $p \mid h$ if and only if $p \mid \varphi(h)$.

Now suppose $f \in \Lambda$ is such that $\varphi(f) \equiv 1 \bmod p^k\Lambda$. Write $f - 1 = p^m h$, with $h \in \Lambda$, $p \nmid h$. We wish to show that $m \geq k$. We have that $\varphi(f) - 1 = p^m \varphi(h)$, and by the above, $p \nmid \varphi(h)$. Therefore $m \geq k$, as desired. □

Proof of Proposition 3.1.2. Denote by $\mathfrak{p}_0$ the maximal ideal of $\mathbf{Z}_p[\mu_p]$. Suppose that $f \in \Lambda^\times$ satisfies $f \equiv 1 \bmod p^k\Lambda$. Since for $\eta \in \mu_p$ we have $(1+T)\eta - 1 \equiv T \bmod \mathfrak{p}_0\Lambda$, we find that $f((1+T)\eta - 1) \equiv f(T) \bmod \mathfrak{p}_0 p^k \Lambda$. Hence, $\varphi(\mathcal{N}(f)) \equiv f(T)^p \bmod \mathfrak{p}_0 p^k \Lambda$. Because $\varphi(\mathcal{N}(f)) - f(T)^p \in \Lambda$, this is in fact a congruence mod $\Lambda \cap \mathfrak{p}_0 p^k \Lambda = p^{k+1}\Lambda$.

Taking $k = 0$, we see that any $f \in \Lambda^\times$ satisfies $\varphi(\mathcal{N}(f)) \equiv f(T)^p \equiv \varphi(f) \bmod p\Lambda$. Applying Lemma 3.1.3 to $\mathcal{N}(f)/f$ then yields that $\mathcal{N}(f) \equiv f \bmod p\Lambda$. If $k \geq 1$, then

any $f \equiv 1 \bmod p^k\Lambda$ satisfies $\varphi(\mathcal{N}(f)) \equiv f(T)^p \equiv 1 \bmod p^{k+1}\Lambda$, and again Lemma 3.1.3 yields that $\mathcal{N}(f) \equiv 1 \bmod p^{k+1}\Lambda$. This takes care of the first two assertions.

Finally, the first part shows that $\mathcal{N}^{k_2-k_1}(f)/f \equiv 1 \bmod p\Lambda$ for $f \in \Lambda^\times$. The last part then follows from the second upon applying $\mathcal{N}^{k_1}$ to both sides. □

§3.2 Coleman's interpolating power series

Denote by $\mathscr{U}_n$ the unit group of the ring of integers of $K_n = \mathbf{Q}_p(\mu_{p^{n+1}})$. Let us fix a system $\{\eta_n\}_n$ where $\eta_n \in K_n$ is a primitive p^{n+1}-th root of unity, with the property that $\eta_{n+1}^p = \eta_n$. Also write $\pi_n = \eta_n - 1$, which is a uniformizer for K_n.

Because K_n is totally ramified over $\mathbf{Q}_p$, we can write any element in its ring of integers as a power series in π_n with coefficients in $\{1, \cdots, p-1\}$. In particular, we find that for each n and $u_n \in \mathscr{U}_n$, there is a power series $f_n \in \Lambda$ such that $f_n(\pi_n) = u_n$.

Let $\mathscr{U}_\infty = \varprojlim \mathscr{U}_n$, where the limit is with respect to the norm maps. It was the amazing insight of Coleman [Col79] that if we choose $u = (u_n)_n \in \mathscr{U}_\infty$, then there is a *unique* power series f such that $f(\pi_n) = u_n$ for all n. Our goal in this section is to prove this theorem.

To see how we might find this power series, let us remark the following: if $f \in \Lambda^\times$ satisfies $\mathcal{N}(f) = f$, then $(f(\pi_n))_n \in \mathscr{U}_\infty$. This is because in general, we have

$$(\mathcal{N}f)(\pi_{n-1}) = (\varphi \circ \mathcal{N})(f)(\pi_n) = \prod_{\eta \in \mu_p} f(\eta\eta_n - 1) = N_{F_n/F_{n-1}}(f(\pi_n)).$$

Thus to find an interpolating power series for a system of units $u \in \mathscr{U}_\infty$, it seems like a good idea to consider norm invariant power series. If we denote by $(\Lambda^\times)^{\mathcal{N}=1}$ the set of $f \in \Lambda^\times$ with $\mathcal{N}(f) = f$, we will prove the following theorem:

> Theorem 3.2.1. For $u = (u_n)_n \in \mathscr{U}_\infty$, there is a unique $f_u \in (\Lambda^\times)^{\mathcal{N}=1}$ such that $f_u(\pi_n) = u_n$, and the map $u \mapsto f_u$ is an isomorphism $\mathscr{U}_\infty \xrightarrow{\sim} (\Lambda^\times)^{\mathcal{N}=1}$.

Proof. By the Weierstrass preparation theorem, an non-zero integral power series has only finitely many zeros in $\mathbf{Z}_p$, from which the uniqueness follows at once.

Let $u = (u_n)_n \in \mathscr{U}_\infty$. Choose a power series $f_n \in \Lambda$ with $f_n(\pi_n) = u_n$. Consider the sequence $g_m = \mathcal{N}^m(f_{2m})$. Because Λ is compact, this sequence has a convergent subsequence, whose limit we denote by g. We claim that this g is our desired f_u.

Recall that for general $f \in \Lambda^\times$ we have that

$$(\mathcal{N}f)(\pi_{n-1}) = N_{F_n/F_{n-1}}(f(\pi_n)).$$

In particular, $u_{n-k} = \mathcal{N}^k(f_n)(\pi_{n-k})$ for $k \le n$. Consequently, we find that for $m \ge n$, $u_n = \mathcal{N}^{2m-n}(f_{2m})(\pi_n)$. By Proposition 3.1.2, $\mathcal{N}^{2m-n}(f_{2m}) \equiv \mathcal{N}^m(f_{2m}) \bmod p^{m+1}\Lambda$. In particular, $u_n \equiv g_m(\pi_n) \bmod p^{m+1}$ and therefore $g_m(\pi_n) \to u_n$ as $m \to \infty$. Thus $g(\pi_n) = u_n$.

Because the power series $f = \mathcal{N}(g)$ also satisfies $f(\pi_n) = u_n$, the uniqueness implies that $\mathcal{N}(g) = g$, so $g \in (\Lambda^\times)^{\mathcal{N}=1}$. □

In fact, a little more is true. As before, let us write $G = \mathrm{Gal}(F_\infty/\mathbf{Q}) = \mathrm{Gal}(K_\infty/\mathbf{Q}_p)$. Then G acts naturally on $\mathscr{U}_\infty$. It also acts on Λ by $\sigma f = f((1+T)^{\varkappa(\sigma)} - 1)$, where $\varkappa\colon G \to \mathbf{Z}_p^\times$ is the cyclotomic character. Then we can see that the isomorphism $\mathscr{U}_\infty \to (\Lambda^\times)^{\mathcal{N}=1}$ is in fact G-invariant as well.

Example 3.2.2. Of course the Coleman power series for the units $(\eta_n)_n$ is simply $1+T$. A more interesting example is given by the *cyclotomic units*

$$\xi_{n,a} = \frac{\eta_n^{a/2} - \eta_n^{-a/2}}{\eta_n^{1/2} - \eta_n^{-1/2}} = \eta_n^{(1-a)/2}\frac{\eta_n^a - 1}{\eta_n - 1},$$

where $a \in \mathbf{Z}$ is coprime to p. It is a nice exercise to show that $\xi_a = (\xi_{n,a})_n \in \mathscr{U}_\infty$. Its Coleman series is

$$\frac{(1+T)^{a/2} - (1+T)^{-a/2}}{(1+T)^{1/2} - (1+T)^{-1/2}} = (1+T)^{(1-a)/2}\frac{(1+T)^a - 1}{T}.$$

The cyclotomic units will be studied in more detail in the next chapter, and play an important role in the proof of the Main Conjecture.

§3.3 The logarithmic derivative

Given a unit power series $f \in \Lambda^\times$, define its *logarithmic derivative* to be

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

It's clear that $\Delta\colon \Lambda^\times \to \Lambda$ is a group homomorphism. Furthermore, the identity

$$\Delta \circ \mathcal{N} = \psi \circ \Delta \tag{3.1}$$

is easily verified. Thus Δ acts as a bridge between the multiplicative norm and additive trace map. In particular, we see that $\Delta((\Lambda^\times)^{\mathcal{N}=1}) \subset \Lambda^{\psi=1}$, where $(\Lambda^\times)^{\mathcal{N}=1}$ as before denotes the unit power series satisfying $\mathcal{N}(f) = f$, and $\Lambda^{\psi=1}$ those power series satisfying $\psi(f) = f$.

Remark 3.3.1. Let

$$f = (1+T)^{(1-a)/2}\frac{(1+T)^a - 1}{T}$$

be the Coleman power series of the cyclotomic units ξ_a. Its logarithmic derivative is equal to

$$\frac{a-1}{2} + \frac{a}{(1+T)^a - 1} - \frac{1}{T},$$

which we recognize as being (up to a constant term) the power series used to construct the pseudo-measure ζ_p in the first chapter. By the above, this power series is equal to its own trace, from which Lemma 1.4.2 follows immediately.

The rest of this section will be devoted to showing that the inclusion $\Delta((\Lambda^\times)^{\mathcal{N}=1}) \subset \Lambda^{\psi=1}$ is in fact an equality.

Proposition 3.3.2. We have that $\Delta((\Lambda^\times)^{\mathcal{N}=1}) = \Lambda^{\psi=1}$.

Before we begin the proof, we need the following auxillary lemma.

Lemma 3.3.3. For $n \geq 1$, we have that

$$\psi\left(\frac{1+T}{T}\varphi(T)^n\right) = \frac{1+T}{T}T^n.$$

Proof. Note that while we defined Δ only on $\Lambda^\times$, its defining expression of course makes sense for any non-zero power series (as an element of the field of fractions of Λ). Applying Δ to both sides of the equation

$$\varphi(T) = \prod_{\eta^p=1}((1+T)\eta - 1)$$

we obtain that

$$p\varphi\left(\frac{1+T}{T}\right) = \sum_{\eta^p=1}\frac{\eta(1+T)}{\eta(1+T)-1}.$$

Multiplying by $\frac{1}{p}\varphi(T)^n$ yields that

$$\varphi\left(\frac{1+T}{T}T^n\right) = \varphi\circ\psi\left(\frac{1+T}{T}\varphi(T)^n\right).$$

Injectivity of φ then gives the desired result. □

Proof of Proposition 3.3.2. We have already remarked that $\Delta((\Lambda^\times)^{\mathcal{N}=1}) \subset \Lambda^{\psi=1}$. The hard part lies in showing the reverse inclusion. If $A \subset \Lambda$, we write $\overline{A}$ for its image

in $\mathbf{F}_p[\![T]\!]$. The idea will be to first show that $\overline{\Delta((\Lambda^\times)^{\mathcal{N}=1})} = \overline{\Lambda^{\psi=1}}$, and then that this implies the proposition. The proof proceeds in several steps.

$$\textbf{Step 1: } \overline{(\Lambda^\times)^{\mathcal{N}=1}} = \mathbf{F}_p[\![T]\!]^\times.$$

Let $f \in \Lambda^\times$. Then by the last part of Proposition 3.1.2, the sequence $\mathcal{N}^n(f)$ is Cauchy. It therefore converges to some power series g, which must satisfy $\mathcal{N}(g) = g$ (so $g \in (\Lambda^\times)^{\mathcal{N}=1}$) and $\overline{g} = \overline{f}$ (by the first part of the same proposition).

$$\textbf{Step 2: } \mathbf{F}_p[\![T]\!] = \Delta(\mathbf{F}_p[\![T]\!]^\times) + \frac{T+1}{T} T^p \mathbf{F}_p[\![T^p]\!].$$

Suppose $g \in \mathbf{F}_p[\![T]\!]$. Write $\frac{T}{1+T} g = \sum_{n \geq 0} a_n T^n$, and define a new power series

$$h = \sum_{(m,p)=1} a_m \sum_{k \geq 0} T^{mp^k}.$$

Then $\frac{T}{1+T} g - h \in T^p \mathbf{F}_p[\![T^p]\!]$, so it suffices to show that $\frac{1+T}{T} h \in \Delta(\mathbf{F}_p[\![T]\!]^\times)$. We will inductively construct a sequence $\alpha_i \in \mathbf{F}_p$ such that for all m,

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

The case $m = 0$ is vacuous. Now suppose we have found $\alpha_1, \ldots, \alpha_{m-1}$. Write $h_{m-1} = \frac{1+T}{T} \sum_{k \geq m} d_k T^k$. Observe that

$$\Delta(1 - \alpha_i T^i) = -\frac{1+T}{T} \sum_{k \geq 1} i \alpha_i^k T^{ik}.$$

From this and the definition of h, it follows that $d_k = d_{pk}$ for all k.

Now, if $d_m = 0$, we may take $\alpha_m = 0$. Otherwise, by the previous remark m is not divisible by p, and we may take $\alpha_m = -m^{-1} d_m$.

By construction, $h_m \to 0$ (in the T-adic topology), so we have $\frac{1+T}{T} h = \sum_{i \geq 1} \Delta(1 - \alpha_i T^i)$. Thus we see that $\Delta(\prod_{i \geq 1} (1 - \alpha_i T^i)) = \frac{T+1}{T} h$.

$$\textbf{Step 3: } \overline{\Lambda^{\psi=1}} = \Delta(\mathbf{F}_p[\![T]\!]^\times) = \overline{\Delta((\Lambda^\times)^{\mathcal{N}=1})}.$$

Let $f \in \Lambda^{\psi=1}$. By the previous steps we may write $f \equiv \Delta(a) + b \bmod p\Lambda$ for some $a \in (\Lambda^\times)^{\mathcal{N}=1}, b \in \Lambda$, with b of the form $\frac{1+T}{T} \sum_{m \geq 1} d_m T^{pm}$. Because Δ maps $(\Lambda^\times)^{\mathcal{N}=1}$ to $\Lambda^{\psi=1}$, we see that $\psi(b) \equiv b \bmod p\Lambda$. From Lemma 3.3.3 it now follows that

$$b \equiv \psi(b) \equiv \psi\left(\frac{1+T}{T} \varphi\left(\sum_{m \geq 1} d_m T^m \right) \right) = \frac{1+T}{T} \sum_{m \geq 1} d_m T^m \bmod p\Lambda.$$

Thus $d_m \equiv 0 \bmod p$, and $f \equiv \Delta(a) \bmod p\Lambda$.

Step 4: $\Lambda^{\psi=1} = \Delta((\Lambda^\times)^{\mathcal{N}=1})$.

Let $f_0 \in \Lambda^{\psi=1}$. By the previous step, there exists a $g_1 \in (\Lambda^\times)^{\mathcal{N}=1}$ such that $\Delta(g_1) = f_0 - pf_1$ for some $f_1 \in \Lambda$. Since Δ maps $(\Lambda^\times)^{\mathcal{N}=1}$ to $\Lambda^{\psi=1}$, it follows that we must also have $f_1 \in \Lambda^{\psi=1}$. Hence there exists a $g_2 \in (\Lambda^\times)^{\mathcal{N}=1}$ such that we can write $\Delta(g_2) = f_1 - pf_2$ for some $f_2 \in \Lambda$. We may continue this indefinitely to obtain a sequence of power series $g_i \in (\Lambda^\times)^{\mathcal{N}=1}$, $f_i \in \Lambda$ with the property that $\Delta(g_i) = f_{i-1} - pf_i$. Define

$$h_n = \prod_{i=1}^{n} g_i^{p^{i-1}} \in (\Lambda^\times)^{\mathcal{N}=1}.$$

Then $\Delta(h_n) = \sum_{i=1}^{n} p^{i-1}\Delta(g_i) = f_0 - p^n f_n$, so $\Delta(h_n) \to f_0$. Hence any limit point h of the sequence h_n satisfies $\Delta(h) = f_0$. □

§3.4 Some exact sequences

In this section we will construct a number of exact sequences using the maps $\varphi, \psi, \mathcal{N}$ and Δ. We will see that these sequences give us more insight into the process from Chapter 1 where we constructed the ζ measure. Especially the last sequence will play in important role in the next chapter in connecting the ζ measure to the units $\mathscr{U}_\infty$.

One important step in the construction in Chapter 1 was restricting the measure μ_a on $\mathbf{Z}_p$ to $\mathbf{Z}_p^\times$. Because $\psi(\mu_a) = \mu_a$, restricting to $\mathbf{Z}_p^\times$ was the same as applying the map $1 - \varphi$. Our first exact sequence describes the kernel and cokernel of this map.

Proposition 3.4.1. There is an exact sequence

$$0 \longrightarrow \mathbf{Z}_p \longrightarrow \Lambda^{\psi=1} \xrightarrow{1-\varphi} \Lambda^{\psi=0} \longrightarrow \mathbf{Z}_p \longrightarrow 0$$

where the map $\Lambda^{\psi=0} \to \mathbf{Z}_p$ is evaluation at 0.

Proof. First note that since $\psi \circ \varphi = \mathrm{Id}$, $(1 - \varphi)$ indeed maps $\Lambda^{\psi=1}$ to $\Lambda^{\psi=0}$. Also, we have $\psi(1 + T) = 0$, which shows surjectivity of the last map.

The only remaining non-obvious parts are the exactness at the middle two terms. For the first, suppose $f \in \Lambda$ is non-constant. Write $f = a_0 + a_r T^r + \dots$ with $a_r \neq 0$. Then $\varphi(f) = a_0 + p^r a_r T^r + \dots \neq f$, and hence we have exactness at $\Lambda^{\psi=1}$.

Lastly, we need to check exactness at $\Lambda^{\psi=1}$. It is clear that $f(0) - \varphi(f)(0) = 0$. Suppose $f \in \Lambda^{\psi=0}$ satisfies $f(0) = 0$. A straightforward induction shows that $\varphi^n(T) \in (p, T)^n$, and hence $\varphi^n(T)$ converges to 0. As f is divisible by T, we also get that $\varphi^n(f) \to 0$. Consequently, the series $\sum_{n\geq 0} \varphi^n(f)$ converges to an element h, which satisfies $\psi(h) = h$ and $(1 - \varphi)(h) = f$. □

We now define the so called *canonical map*.

Lemma 3.4.2. If $f \in \Lambda^\times$, the expression

$$\mathcal{L}(f) = \frac{1}{p} \log\left(\frac{f(T)^p}{\varphi(f)(T)}\right)$$

defines an element of Λ, and $\mathcal{L}(f) \in \Lambda^{\psi=0}$ if $f \in (\Lambda^\times)^{\mathcal{N}=1}$.

Proof. Here log is defined by its usual power series $\log(x) = \sum_{m\geq 1}(-1)^{m-1}\frac{(x-1)^m}{m}$. It is immediately seen that for $h \in 1 + p\Lambda$, $\log(h)$ converges to an element of $p\Lambda$. Because $\varphi(f) \equiv f(T)^p \bmod p\Lambda$, it follows that $\mathcal{L}(f) \in \Lambda$.

Now suppose $f \in (\Lambda^\times)^{\mathcal{N}=1}$. This means that

$$\varphi(f) = \prod_{\eta \in \mu_p} f(\eta(1 + T) - 1).$$

From this it readily follows that

$$\varphi \circ \psi(\mathcal{L}(f)) = \frac{1}{p} \sum_{\eta \in \mu_p} \mathcal{L}(f)(\eta(1 + T) - 1) = 0. \qquad \square$$

The canonical map is defined this way precisely to make the following square commute:

$$\begin{array}{ccc} (\Lambda^\times)^{\mathcal{N}=1} & \xrightarrow{\mathcal{L}} & \Lambda^{\psi=0} \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \partial} \\ \Lambda^{\psi=1} & \xrightarrow[1-\varphi]{} & \Lambda^{\psi=0} \end{array}$$

Note that in our original construction of ζ_p, we started with a power series in $\Lambda^{\psi=1}$ corresponding to a measure μ_a. We restricted this measure to $\mathbf{Z}_p^\times$ (which is the same as applying $1-\varphi$) and divided it by x^{-1} (which in terms of power series is the same as applying the inverse of ∂, since multiplication by x corresponds to applying ∂). By now

we have also seen that our original power series is the logarithmic derivative of an element of $(\Lambda^\times)^{\mathcal{N}=1}$, so our entire construction in Chapter 1 is essentially an application of the canonical map. This can be summarized by the following proposition.

LEMMA 3.4.3. Suppose $f \in (\Lambda^\times)^{\mathcal{N}=1}$. If μ is the measure associated to $\mathcal{L}(f)$ under the Amice transform, then μ is supported in $\mathbf{Z}_p^\times$, and

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \mu(x) = (1 - p^{k-1}) \cdot (\partial^{k-1} \circ \Delta)(f)(0).$$

Proof. By Lemma 3.4.2 we have $\psi(\mu) = 0$, so that μ is supported in $\mathbf{Z}_p^\times$ by Lemma 1.2.2. Hence

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \mu(x) = \int_{\mathbf{Z}_p} x^k \cdot \mu(x).$$

The last integral is exactly $\partial^k \mathcal{L}(f)(0)$. From the commutative square above and the additional identity $\partial \circ \varphi = p(\varphi \circ \partial)$, the desired expression for the integral follows. □

Example 3.4.4. Let us once and for all hammer home how the canonical map gives us the measure from Chapter 1. Let

$$f = (1+T)^{(1-a)/2} \frac{(1+T)^a - 1}{T}.$$

It is an element of $(\Lambda^\times)^{\mathcal{N}=1}$ because it is the Coleman series for the cyclotomic units ξ_a. We have seen that its logarithmic derivative is

$$\frac{a-1}{2} + \frac{a}{(1+T)^a - 1} - \frac{1}{T}.$$

By the previous lemma, letting μ be the measure associated to $\mathcal{L}(f)$, we have

$$\int_{\mathbf{Z}_p^\times} x^k \cdot \mu(x) = -(1 - p^{k-1})(1 - a^k)\frac{B_k}{k}.$$

We of course already know a measure with these exact moments, namely $\lambda_a = ([1] - [a])\zeta_p$. Thus by Lemma 1.4.4, we have $\mu = \lambda_a$.

The following proposition determines the kernel and cokernel of the canonical map.

Proposition 3.4.5. Let $A = \{\eta(1+T)^a \mid \eta \in \mu_{p-1}, a \in \mathbf{Z}_p\}$. Then we have an exact sequence

$$0 \longrightarrow A \longrightarrow (\Lambda^\times)^{\mathcal{N}=1} \xrightarrow{\mathcal{L}} \Lambda^{\psi=0} \longrightarrow \mathbf{Z}_p \longrightarrow 0$$

where the last map is given by $f \mapsto (\partial f)(0)$.

Proof. It is easily checked that $\mathcal{L}$ maps A to 0. Conversely, if $\mathcal{L}(f) = 0$, then by injectivity of log we have $f(T)^p = f((1+T)^p - 1)$. Writing $f = f_u$, we then have $u_n^p = u_{n-1}$ and $\eta = f(0) \in \mu_{p-1}$. Hence $\eta^{-1}u \in \varprojlim \mu_{p^n}$, so we can write it as $(\eta_n^a)_n$ for some $a \in \mathbf{Z}_p$. Then $f = \eta(1+T)^a \in A$.

Finally, exactness at $\Lambda^{\psi=0}$ follows from a simple diagram chase in the following commutative diagram,

$$\begin{array}{ccccc} (\Lambda^\times)^{\mathcal{N}=1} & \xrightarrow{\mathcal{L}} & \Lambda^{\psi=0} & \longrightarrow & \mathbf{Z}_p \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \partial} & & \| \\ \Lambda^{\psi=1} & \xrightarrow[1-\varphi]{} & \Lambda^{\psi=0} & \longrightarrow & \mathbf{Z}_p \end{array}$$

using that ∂ is injective on $\Lambda^{\psi=0}$, Δ is surjective (Proposition 3.3.2) and the bottom row is exact (Proposition 3.4.1). □

Let $T_p(\mathbf{G}_m) = \varprojlim \mu_{p^n} \subset \mathscr{U}_\infty$. As before, we let $G = \mathrm{Gal}(F_\infty/\mathbf{Q}) = \mathrm{Gal}(K_\infty/\mathbf{Q})$. Using the Coleman isomorphism we may identify $\mathscr{U}_\infty$ with $(\Lambda^\times)^{\mathcal{N}=1}$, and via the cyclotomic character we identity G and $\mathbf{Z}_p^\times$. This way we may view the canonical map as a way of constructing measures on G from compatible systems of local units.

Corollary 3.4.6. There is an exact sequence of G-modules

$$0 \longrightarrow \mu_{p-1} \times T_p(\mathbf{G}_m) \longrightarrow \mathscr{U}_\infty \longrightarrow \Lambda(G) \longrightarrow T_p(\mathbf{G}_m) \longrightarrow 0.$$

Proof. This is simply the sequence in Proposition 3.4.5, where we have identified $(\Lambda^\times)^{\mathcal{N}=1}$ with $\mathscr{U}_\infty$ using Proposition 3.2.1, and $\Lambda^{\psi=0}$ with $\Lambda(\mathbf{Z}_p^\times) \cong \Lambda(G)$ using Lemma 1.2.2 and the cyclotomic character. □

4 Global and cyclotomic units

In the previous chapter, we saw the relation between local units and measures. Example 3.4.4 in particular showed us the connection between the units

$$\xi_{n,a} = \frac{\eta_n^{a/2} - \eta_n^{-a/2}}{\eta_n^{1/2} - \eta_n^{-1/2}} = \eta_n^{(1-a)/2} \frac{\eta_n^a - 1}{\eta_n - 1}$$

and the pseudo-measure ζ_p. In this chapter we explore this connection further, and use it to prove a theorem of Iwasawa [Iwa64], which describes the characteristic ideal of a certain Λ-module arising from these local units in terms of p-adic L-functions. We then use class field theory to relate this module to $\mathscr{X}_\infty$, thereby getting us closer to a proof the Main Conjecture.

§4.1 The group of cyclotomic units

Definition 4.1.1. We define the group of *cyclotomic units* of F_n, denoted $\mathscr{D}_n$, to be the intersection of $\mathcal{O}_{F_n}^\times$ with the subgroup of $F_n^\times$ generated by

$$\left\{ \pm\eta_n, \eta_n^a - 1 \,\middle|\, 1 \le a \le \frac{p^{n+1}-1}{2} \right\}.$$

We will also denote by $\mathscr{C}_n$ the closure of $\mathscr{D}_n$ inside of K_n.

The group of cyclotomic units certainly contains the aforementioned $\xi_{n,a}$. By the Dirichlet unit theorem, the group of cyclotomic units $\mathscr{D}_n$ (as well as its real counterpart $\mathscr{D}_n^+ = \mathscr{D}_n \cap F_n^+$) has rank at most $\frac{p^n(p-1)}{2} - 1$. The following proposition provides us with an explicit set of of $\frac{p^n(p-1)}{2} - 1$ many generators for the free part of the group of cyclotomic units.

Proposition 4.1.2. The following hold:

1. The group of real cyclotomic units $\mathscr{D}_n^+$ is generated by -1 and
$$\{\xi_{n,a} \mid 1 < a < \tfrac{p^n}{2}, (a,p) = 1\}.$$
2. The group of cyclotomic units $\mathscr{D}_n$ is generated by η_n and $\mathscr{D}_n^+$.
3. If a generates $(\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$, then $\xi_{n,a}$ generates $\mathscr{D}_n^+/\{\pm 1\}$ as a $\mathbf{Z}[G_n^+]$-module.

Proof. From the fact that for $k \leq n$ we have $X^{p^k} - 1 = \prod_{j=0}^{p^k-1}(X\eta_n^{jp^{n+1-k}} - 1)$, we get that

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

This implies that in our original generating set for $\mathscr{D}_n$, we may restrict to a coprime to p.

Now suppose we have an arbitrary cyclotomic unit $\xi \in \mathscr{D}_n$. By the above, we may write

$$\xi = \pm\eta_n^d \prod_{(a,p)=1} (\eta_n^a - 1)^{e_a},$$

where the product runs over all a coprime to p from 1 to $\frac{p^{n+1}-1}{2}$. All the factors $\eta_n^a - 1$ have the same p-adic absolute value, while the left hand side has absolute value 1, so that $\sum e_a = 0$. Therefore we can write

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

Point 1 and 2 now follow upon noting that $\xi_{n,a}$ is real, so that $\xi \in \mathscr{D}_n^+$ if and only if $e = 0$.

The last point follows by observing that

$$\xi_{n,a^r} = \prod_{j=0}^{r-1} \eta_n^{(a^j - a^{j+1})/2} \frac{\eta_n^{a^{j+1}} - 1}{\eta_n^{a^j} - 1}$$

and that all the factors in the product are Galois conjugates of $\xi_{n,a}$. □

Remark 4.1.3. It is in fact even true that the group of cyclotomic units has finite index in the full unit group. In other words, it has maximal rank and the set of generators provided above are actually a basis for the free part. Explicitly, it can be shown using the analytic class number formula that

$$[\mathcal{O}_{F_n}^\times : \mathscr{D}_n] = [\mathcal{O}_{F_n^+}^\times : \mathscr{D}_n^+] = h_n^+.$$

This equation is one of the key ingredients in connecting the cyclotomic units to the class group. To get an idea for why it is true, note that the class number formula for the field F_n^+ says that the product $\prod L(\chi, 1)$ over the non-trivial even characters of conductor dividing p^{n+1} is essentially equal to $\mathrm{Reg}(\mathcal{O}_{F_n^+}^\times)h_n^+$. Furthermore, we have the classical formula that $L(\chi, 1)$ is essentially given by

$$\sum_{a \in (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times} \chi(a)^{-1} \log|1 - \eta_n^a|.$$

Some (elementary, though non-trivial) algebraic manipulations show then that the product $\prod L(\chi, 1)$ is exactly equal to the regulator $\mathrm{Reg}(\mathscr{D}_n^+)$ of the cyclotomic units. We obtain the formula since the quotient of the regulators of the full unit group and the cyclotomic units is precisely the index $[\mathcal{O}_{F_n^+}^\times : \mathscr{D}_n^+]$. For details see [Lan90, Chapter 3, Theorem 5.1].

Denote by $\mathscr{U}_{n,1}$ the subgroup of $\mathscr{U}_n$ consisting of units which are $\equiv 1$ modulo the maximal ideal. If $H \subset \mathscr{U}_n$ is any subgroup, we let $H_1 = H \cap \mathscr{U}_{n,1}$. The reason for restricting to only these units is because $\mathscr{U}_{n,1}$ is a pro-p-group, and so has a natural action of $\mathbf{Z}_p$. Combined with its Galois action, this means that $\mathscr{U}_{\infty,1}$ is a $\Lambda(G)$-module.

Corollary 4.1.4. The group $\mathscr{C}_{\infty,1}^+$ is a cyclic $\Lambda(G^+)$-module. It is generated by $\omega^{-1}(a)\xi_a = (\omega^{-1}(a)\xi_{n,a})_n$, where $a \in \mathbf{Z}$ is a topological generator of $\mathbf{Z}_p^\times$.

Proof. The Coleman power series of ξ_a is $(1+T)^{(1-a)/2}\frac{(1+T)^a-1}{T}$, which has constant term a. Therefore $\xi_{n,a} \equiv a \bmod \pi_n$, so $\omega^{-1}(a)\xi_{n,a} \in \mathscr{U}_{n,1}^+$. Because $\mathscr{U}_{n,1}$ is a $\mathbf{Z}_p$-module and $p-1$ a p-adic unit, we can write

$$\omega^{-1}(a)\xi_{n,a} = ((\omega^{-1}(a)\xi_{n,a})^{p-1})^{1/(p-1)}$$

with $(\omega^{-1}(a)\xi_{n,a})^{p-1} = \xi_{n,a}^{p-1} \in \mathscr{D}_n^+$. This shows that $\omega^{-1}(a)\xi_{n,a} \in \mathscr{C}_{n,1}^+$.

To see that this element generates $\mathscr{C}_{\infty,1}^+$, it suffices to show that $\omega^{-1}(a)\xi_{n,a}$ generates $\mathscr{C}_{n,1}^+$ as a $\mathbf{Z}_p[G_n^+]$-module. Any element of $\mathscr{C}_{n,1}^+$ may be written as ξ^d, with $\xi \in \mathscr{D}_{n,1}^+$ and

$d \in \mathbf{Z}_p$. By the previous proposition, we may write $\xi = \prod_{\sigma \in G_n^+} \sigma(\xi_{n,a})^{e_\sigma}$, in which case

$$\xi = \left(\prod_{\sigma \in G_n^+} \sigma(\omega^{-1}(a)\xi_{n,a})^{e_\sigma (p-1)} \right)^{1/(p-1)} \in \mathbf{Z}_p[G_n^+]\omega^{-1}(a)\xi_{n,a}. \qquad \square$$

§4.2 Iwasawa's theorem

Recall that any $\Lambda(G)$-module M could be decomposed as $e_+M \oplus e_-M$. In particular, we can write $\Lambda(G) = e_+\Lambda(G) \times e_-\Lambda(G)$. Similarly as in Lemma 1.3.6, we can show that $e_+\Lambda(G)$ is naturally isomorphic to $\Lambda(G^+)$. The isomorphism $G \to \mathbf{Z}_p^\times$ allows us to view the pseudo-measure ζ_p as a measure on G. In fact, because all odd moments of ζ_p are 0, this means that it actually descends to a pseudo-measure on G^+. To remove the hassle of having only a pseudo-measure instead of a bonafide measure, we introduce the augmentation ideal.

Definition 4.2.1. The *augmentation ideal* $I(G)$ of $\Lambda(G)$ is the closure in $\Lambda(G)$ of the regular augmentation ideal $\{\sum_{g\in G} a_g[g] \mid \sum_{g\in G} a_g = 0\} \subset \mathbf{Z}_p[G]$. Equivalently, it is the inverse limit of the augmentation ideals of $\mathbf{Z}_p[G_n]$.

We know if K is a cyclic group generated by k, the augmentation ideal of $\mathbf{Z}_p[K]$ is generated by $[1]-[k]$. It readily follows that $I(G)$ is generated by $[1]-[\sigma_a]$, where a topologically generates $\mathbf{Z}_p^\times$ and σ_a satisfies $\varkappa(\sigma_a) = a$. From the definition of a pseudo-measure, it is now immediate that $I(G)\zeta_p$ is an ideal of $\Lambda(G)$.

The following theorem of Iwasawa makes very explicit the relation we have been observing between cyclotomic units and the pseudo-measure ζ_p.

Theorem 4.2.2. There is a canonical isomorphism of $\Lambda(G^+)$-modules

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

Proof. Consider the exact sequence

$$0 \longrightarrow \mu_{p-1} \times T_p(\mathbf{G}_m) \longrightarrow \mathscr{U}_\infty \longrightarrow \Lambda(G) \longrightarrow T_p(\mathbf{G}_m) \longrightarrow 0$$

from Corollary 3.4.6. Because $\mathscr{U}_\infty = \mu_{p-1} \times \mathscr{U}_{\infty,1}$, we also get an exact sequence

$$0 \longrightarrow T_p(\mathbf{G}_m) \longrightarrow \mathscr{U}_{\infty,1} \longrightarrow \Lambda(G) \longrightarrow T_p(\mathbf{G}_m) \longrightarrow 0.$$

Multiplying this sequence by the idempotent e_+ yields an isomorphism $\mathscr{U}_{\infty,1}^+ \xrightarrow{\sim} \Lambda(G^+)$. Thus it now suffices to calculate the image of $\mathscr{C}_{\infty,1}^+$, which by Corollary 4.1.4 will be

generated by the image of $u = \omega^{-1}(a)\xi_a$. But by Example 3.4.4, this image is $\lambda_a = ([1]-[\sigma_a])^+\zeta_p$, where $([1]-[\sigma_a])^+$ denotes the image of $[1]-[\sigma_a]$ in $\Lambda(G^+)$. As $([1]-[\sigma_a])^+$ generates $I(G^+)$, we find that the image is indeed $I(G^+)\zeta_p$. □

§4.3 An equivalent statement of the Main Conjecture

Let us denote by $\mathscr{V}_n$ the group of global units $\mathcal{O}_{F_n}^\times$, and by $\mathscr{E}_n$ its closure inside $K_n = \mathbf{Q}_p(\mu_{p^{n+1}})$. Furthermore, recall that M_∞ denoted the maximal abelian p-extension of F_∞ that is unramified away from p, and L_∞ its the maximal subextension that is everywhere unramified over F_∞. Just as we related the Galois group of L_∞ to the class groups of the fields F_n, we would like to have a similar description for the Galois group $\mathscr{X}_\infty = \mathrm{Gal}(M_\infty/F_\infty)$. The statement of class field theory in the Appendix is insufficient for this, since that only deals with unramified extensions. However, more intricate statements of class field theory can relate Galois groups to subgroups of the *idèle class group*. In particular, we have the following result for our field M_∞.

Lemma 4.3.1. There is an isomorphism

$$\mathscr{U}_{\infty,1}/\mathscr{E}_{\infty,1} \xrightarrow{\sim} \mathrm{Gal}(M_\infty/L_\infty)$$

Proof. By class field theory (see [RW, Proposition 10.5]) we have for all n an exact sequence $0 \to \mathscr{E}_{n,1} \to \mathscr{U}_{n,1} \to \mathrm{Gal}(M_n/L_n) \to 0$. A compactness argument shows that the sequence stays exact when passing to the inverse limit. □

Theorem 4.3.2. There is an exact sequence

$$0 \longrightarrow \mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1} \longrightarrow \mathscr{U}_{\infty,1}/\mathscr{C}_{\infty,1} \longrightarrow \mathscr{X}_\infty \longrightarrow \mathscr{Y}_\infty \longrightarrow 0.$$

Proof. Follows immediately from the preceding lemma. □

Let $i \not\equiv 0 \bmod p-1$ be even. By multiplying the above sequence by e_i and taking characteristic ideals, we find that

$$\mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1}))\,\mathrm{ch}(e_i\mathscr{X}_\infty) = \mathrm{ch}(e_i(\mathscr{U}_{\infty,1}/\mathscr{C}_{\infty,1}))\,\mathrm{ch}(e_i\mathscr{Y}_\infty).$$

The proofs of Proposition 1.5.3 and Theorem 1.5.4 shows that under the identification of $e_i\Lambda(G)$ with $\Lambda = \mathbf{Z}_p[\![T]\!]$, the ideal $e_iI(G)\zeta_p$ corresponds to the ideal of Λ generated by the Iwasawa power series f_i. In particular, combining this with Iwasawa's theorem, we have that

$$\mathrm{ch}(e_i(\mathscr{U}_{\infty,1}/\mathscr{C}_{\infty,1})) = f_i\Lambda.$$

The Main Conjecture states that this is also the characteristic ideal of $e_i\mathscr{X}_\infty$. Thus to show the Main Conjecture, it actually suffices to show that

$$\mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1})) = \mathrm{ch}(e_i\mathscr{Y}_\infty). \tag{4.1}$$

In fact, this already allows to prove the Main Conjecture for all practical cases.

Corollary 4.3.3. If p is Vandiver prime, the Main Conjecture holds.

Proof. We will show that $\mathscr{E}^+_{\infty,1}/\mathscr{C}^+_{\infty,1} = \mathscr{Y}^+_\infty = 0$. That $\mathscr{Y}^+_\infty = 0$ follows from Remark 2.1.5. Next, notice that by tensoring the exact sequence

$$0 \to \mathscr{V}^+_{n,1} \to \mathscr{V}^+_n \to \mathbf{F}_p^\times$$

with $\mathbf{Z}_p$ we obtain that $\mathscr{V}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p = \mathscr{V}^+_n \otimes_{\mathbf{Z}} \mathbf{Z}_p$. The same holds for $\mathscr{D}^+_n$. Therefore, we find that the Sylow p-subgroup of $\mathscr{V}^+_n/\mathscr{D}^+_n$ is

$$\begin{aligned}(\mathscr{V}^+_n/\mathscr{D}^+_n) \otimes_{\mathbf{Z}} \mathbf{Z}_p &\cong (\mathscr{V}^+_n \otimes_{\mathbf{Z}} \mathbf{Z}_p)/(\mathscr{D}^+_n \otimes_{\mathbf{Z}} \mathbf{Z}_p) \\ &\cong (\mathscr{V}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p)/(\mathscr{D}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p).\end{aligned}$$

Remark 4.1.3 states that $h^+_n = [\mathscr{V}^+_n : \mathscr{D}^+_n]$, so the Sylow p-subgroup of $\mathscr{V}^+_n/\mathscr{D}^+_n$ is trivial. Hence $\mathscr{D}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p = \mathscr{V}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p$. From the commutative diagram

$$\begin{array}{ccc} \mathscr{D}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p & = & \mathscr{V}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p \\ \downarrow & & \downarrow \\ \mathscr{C}^+_{n,1} & \longrightarrow & \mathscr{E}^+_{n,1} \end{array}$$

where the vertical arrows are surjective, we find that the bottom arrow is surjective as well, showing that $\mathscr{E}^+_{n,1} = \mathscr{C}^+_{n,1}$. □

Remark 4.3.4. A theorem of Brumer [Bru67] says that $\mathscr{V}^+_{n,1} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ and $\mathscr{E}^+_{n,1}$ in fact have the same $\mathbf{Z}_p$-rank. Consequently, the vertical maps are isomorphisms, and we see that we actually always have that $\#(\mathscr{E}^+_{n,1}/\mathscr{C}^+_{n,1}) = \#\mathscr{Y}^+_n$. This is of course still a much weaker statement than (4.1), but nevertheless it will turn out to be relevant for the proof.

The equivalent form (4.1) is the one we will prove in Chapter 6. We make clear the strategy for this in the next chapter.

We end with a final lemma regarding the characteristic ideal of $e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1})$.

Lemma 4.3.5. Suppose that $i \not\equiv 0$ is even, and let $h \in \Lambda(\Gamma)$ be a generator for the ideal $\mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1}))$. Then for all n, there is a positive integer C such that for all $c > C$, there is a map $\theta\colon e_i\mathscr{E}_{n,1} \to \mathbf{Z}_p[\Gamma/\Gamma_n]$ such that the image of $e_i\mathscr{C}_{\infty,1}$ is $p^c h\mathbf{Z}_p[\Gamma/\Gamma_n]$.

Proof. Since the proof is rather technical, we omit some details, which can be found in [Lan90, Appendix, Corollary 6.4]. The idea is that since $e_i\mathscr{U}_{\infty,1}$ is a torsion-free $\Lambda(\Gamma)$-module of rank one (as was shown in the proof of Theorem 4.2.2), the same holds true for $e_i\mathscr{E}_{\infty,1}$. Thus there is an injective map $\theta'\colon e_i\mathscr{E}_{\infty,1} \to \Lambda(\Gamma)$ with finite cokernel. Because it induces a pseudo-isomorphism $e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1}) \to \Lambda(\Gamma)/\theta'(\mathscr{C}_{\infty,1})$, we must have that

$$\theta'(\mathscr{C}_{\infty,1}) = \mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1})).$$

We can tensor with $\Lambda(\Gamma)/(\gamma_0^{p^n} - 1) = \mathbf{Z}_p[\Gamma/\Gamma_n]$ to obtain a map $\theta_n\colon (e_i\mathscr{E}_{\infty,1})_{\Gamma_n} \to \mathbf{Z}_p[\Gamma/\Gamma_n]$. However, the module $(e_i\mathscr{E}_{\infty,1})_{\Gamma_n}$ is not isomorphic to $e_i\mathscr{E}_{n,1}$ (which *was* true for the module $\mathscr{Y}_\infty$ for instance). Instead, we only have a map $\pi_n\colon (e_i\mathscr{E}_{\infty,1})_{\Gamma_n} \to e_i\mathscr{E}_{n,1}$ with $\ker\pi_n \subset \ker\theta_n$, and $\operatorname{coker}\pi_n$ is finite with order bounded independently of n. So if we choose c such that p^c annihilates this cokernel, we can let $\theta(u) = \theta''(\pi_n^{-1}(p^c u))$. This has the correct image because it *is* true that $(e_i\mathscr{C}_{\infty,1})_{\Gamma_n} = e_i\mathscr{C}_{n,1}$. □

5 Euler systems

In this chapter we develop the theory of *Euler systems* in the context of the Main Conjecture. In their most basic form, they were introduced by Thaine [Tha88], who used them to construct annihilators of class groups of cyclotomic fields. Kolyvagin [Kol90] expanded the theory, using it to prove more detailed statements about the structure of the class group. Not long after, Rubin [Lan90, Appendix] managed to find a much simpler proof of the Main Conjecture using Euler systems.

For us, an Euler system is a collection of elements of certain extensions of a field F, that are norm-compatible in a sense to be defined. Factoring these elements allows us to obtain relations in the class group of the field, which will help us understand the characteristic ideal of the class group and ultimately lead us to a proof of the Main Conjecture.

Throughout this chapter, we utilize some basic results regarding group cohomology. All the necessary definitions and theorems can be found in the Appendix.

§5.1 Cyclotomic Euler systems

For the rest of this chapter, let m be a power of p and fix one of the fields $F = \mathbf{Q}(\mu_m)^+$. Let t be a power of p larger than m. Denote by S_t the set of positive squarefree integers which are divisible only by primes $q \equiv 1 \bmod t$. Note that this condition implies that q splits completely in F.

For any $r \in S_t$ and q a prime not dividing r, denote by $\mathrm{Fr}_q \in \mathrm{Gal}(F(\mu_r)/\mathbf{Q})$ the Frobenius of q, characterized by $\mathrm{Fr}_q(\zeta_r) = \zeta_r^q$.

Definition 5.1.1. An *Euler system* is a collection $\{\xi_r\}_{r \in S_t}$ with $\xi_r \in F(\mu_r)^\times$ satisfying the following properties:

1. ξ_r is an integral unit of $F(\mu_r)$ if $r > 1$;

2. $N_{F(\mu_r)/F(\mu_{r/q})}(\xi_r) = (\mathrm{Fr}_q - 1)\xi_{r/q}$ whenever $q \mid r$;

3. $\xi_r \equiv \xi_{r/q}$ modulo any prime above $q \mid r$.

Henceforth we will refer to these properties as **ES1**, **ES2** and **ES3**.

For any prime $q \in S_t$, fix a primitive q-th root of unity ζ_q, and for $r \in S_t$, let $\zeta_r = \prod_{q|r} \zeta_q$. Also fix a primitive m-th root of unity ζ_m. Our most important example of an Euler system is given by

$$\xi_r = \prod_{j=0}^{m-1} (\zeta_m^j \zeta_r - 1)^{n_j} (\zeta_m^{-j} \zeta_r - 1)^{n_j},$$

with $n_j \geq 0$. To see that **ES1** is satisfied, observe first that $\zeta_m^j \zeta_r - 1 \in \mathbf{Z}[\zeta_m, \zeta_r]^\times$, which follows from the fact that

$$\prod_{\substack{0<k<l \\ (k,l)=1}} (1 - \zeta_l^k) = 1$$

whenever l is not a prime power. Now simply note that

$$(\zeta_m^j \zeta_r - 1)(\zeta_m^{-j} \zeta_r - 1) = N_{\mathbf{Q}(\zeta_m, \zeta_r)/F(\mu_r)}(\zeta_m^j \zeta_r - 1).$$

For **ES2**, note that the conjugates of ζ_q over $F(\mu_{r/q})$ are given by $\eta\zeta_q$ with η a q-th root of unity different from ζ_q^{-1}, and that $\prod_{\eta^q=1}(X\eta - 1) = X^q - 1$. Lastly, **ES3** is clear, since $\zeta_q \equiv 1$ modulo any prime above q.

The reason for the importance of this Euler system is as follows. Let $a, b, c \in \mathbf{Z}_{\geq 1}$ denote respectively a generator of $(\mathbf{Z}/m\mathbf{Z})^\times$, an inverse of 2 mod t, and an inverse of -2 mod t. Then taking

$$\xi_r = (\zeta_m^a \zeta_r - 1)^b (\zeta_m^{-a} \zeta_r - 1)^b (\zeta_m \zeta_r - 1)^c (\zeta_m^{-1} \zeta_r - 1)^c,$$

we see that

$$\xi_1 \equiv \left(\frac{(\zeta_m^a - 1)(\zeta_m^{-a} - 1)}{(\zeta_m - 1)(\zeta_m^{-1} - 1)} \right)^{1/2} = \zeta_m^{(1-a)/2} \frac{\zeta_m^a - 1}{\zeta_m - 1} \bmod F^{\times t}.$$

This last unit is of course the one occurring in Corollary 4.1.4.

As mentioned previously, the Euler systems are used to give relations in the class group of F. Presently it is not at all clear how this will work. After all, the elements ξ_r are units, so they do not generate interesting ideals. Furthermore, they are not even elements of the field we are interested in, which is F. The rest of this section is devoted to using the Euler system to construct elements of F which do have interesting factorizations.

Let $r \in S_t$, and define

$$\mathbf{N}_r = \sum_{\sigma \in \mathrm{Gal}(F(\mu_r)/F)} \sigma \in \mathbf{Z}[\mathrm{Gal}(F(\mu_r)/F)].$$

Note that there is a natural isomorphism $\mathrm{Gal}(F(\mu_r)/F) = \prod_{q|r} \mathrm{Gal}(F(\mu_q)/F)$, which allows us to identify $\mathbf{N}_r$ and $\prod_{q|r} \mathbf{N}_q$. Furthermore, because we can also identify $\mathrm{Gal}(F(\mu_q)/F)$ and $\mathrm{Gal}(F(\mu_r)/F(\mu_{r/q}))$ for $q \mid r$, we can write $N_{F(\mu_r)/F(\mu_{r/q})}(x)$ for $x \in F(\mu_r)$ as $\mathbf{N}_q x$.

Each $\mathrm{Gal}(F(\mu_q)/F)$ for q prime is cyclic. For each of these groups, choose a generator σ_q. Define another operator

$$\mathbf{D}_q = \sum_{i=1}^{q-1} i\sigma_q^i \in \mathbf{Z}[\mathrm{Gal}(F(\mu_q)/F)].$$

Note that this depends on the choice of generator. For arbitrary $r \in S_t$, let $\mathbf{D}_r = \prod_{q|r} \mathbf{D}_q$. The identity

$$(\sigma_q - 1)\mathbf{D}_q = q - 1 - \mathbf{N}_q \tag{5.1}$$

is straightforward to verify. Even though in what follows we consider the multiplicative groups $F(\mu_r)^\times$, we will write the action of Galois additively.

Lemma 5.1.2. For $r \in S_t$, we have $\mathbf{D}_r \xi_r \in (F(\mu_r)^\times / F(\mu_r)^{\times t})^{\mathrm{Gal}(F(\mu_r)/F)}$.

Proof. We will use induction on the number of prime factors of r. If $r = 1$ there is nothing to prove. Otherwise, suppose $q \mid r$. Then

$$(\sigma_q - 1)\mathbf{D}_r \xi_r = (q - 1 - \mathbf{N}_q)\mathbf{D}_{r/q}\xi_r \equiv (1 - \mathrm{Fr}_q)\mathbf{D}_{r/q}\xi_{r/q} \bmod F(\mu_r)^{\times t}.$$

By the induction hypothesis, the element $\mathbf{D}_{r/q}\xi_{r/q}$ is fixed by Fr_q modulo $F(\mu_{r/q})^{\times t}$, and it follows that $\sigma_q \mathbf{D}_r \xi_r \equiv \mathbf{D}_r \xi_r \bmod F(\mu_r)^{\times t}$. Since $\mathrm{Gal}(F(\mu_r)/F)$ is generated by the σ_q for $q \mid r$, the lemma follows. □

Lemma 5.1.3. The natural map

$$F^\times / F^{\times t} \to (F(\mu_r)^\times / F(\mu_r)^{\times t})^{\mathrm{Gal}(F(\mu_r)/F)}$$

is an isomorphism.

Proof. First note that $\mu_t \cap F^\times = 1$, and as r is coprime to t, a ramification argument shows that $\mu_t \cap F(\mu_r)^\times = 1$ as well. Hence we have an exact sequence

$$0 \longrightarrow F(\mu_r)^\times \xrightarrow{a \mapsto a^t} F(\mu_r)^\times \longrightarrow F(\mu_r)^\times / F(\mu_r)^{\times t} \longrightarrow 0,$$

and taking $\mathrm{Gal}(F(\mu_r)/F)$ invariants we obtain an exact sequence

$$0 \longrightarrow F^\times \longrightarrow F^\times \longrightarrow (F(\mu_r)^\times / F(\mu_r)^{\times t})^{\mathrm{Gal}(F(\mu_r)/F)} \longrightarrow H^1(F(\mu_r)/F).$$

But $H^1(F(\mu_r)/F) = 0$ by Hilbert 90, yielding the result. □

By the previous lemmas, we see that there exists a unique element $\kappa_r \in F^\times/F^{\times t}$ such that $\kappa_r \equiv \mathbf{D}_r\xi_r \bmod F(\mu_r)^{\times t}$. It is these elements that we will factor to gain knowledge of the class group of F.

Remark 5.1.4. Recall that the map

$$(F(\mu_r)^\times/F(\mu_r)^{\times t})^{\mathrm{Gal}(F(\mu_r)/F)} \to H^1(F(\mu_r)/F)$$

is defined as follows: let $c \in (F(\mu_r)^\times/F(\mu_r)^{\times t})^{\mathrm{Gal}(F(\mu_r)/F)}$. Choose a representative $b \in F(\mu_r)^\times$. Then for all $\sigma \in \mathrm{Gal}(F(\mu_r)/F)$, the element $(\sigma-1)b = \sigma(b)/b$ becomes trivial in $F(\mu_r)^\times/F(\mu_r)^{\times t}$, so that there is a unique $a_\sigma \in F(\mu_r)^\times$ with $a_\sigma^t = (\sigma-1)b$. Then our map sends c to the crossed homomorphism $\mathrm{Gal}(F(\mu_r)/F) \to F^\times$ given by $\sigma \mapsto a_\sigma$.

Applying this to $c = \mathbf{D}_r\xi_r$ and using Hilbert 90, we see that there is a $\beta \in F(\mu_r)^\times$ with

$$(\sigma-1)\beta = ((\sigma-1)\mathbf{D}_r\xi_r)^{1/t}$$

and we can then take

$$\kappa_r = \mathbf{D}_r\xi_r/\beta^t.$$

This explicit choice of κ_r will be useful later.

§5.2 The factorization theorem

In this section we prove the 'factorization theorem', which tells us how to factor the elements κ_r constructed in the previous section.

We again introduce some notation. For q a rational prime, let

$$\mathcal{I}_q = \bigoplus_{\mathfrak{q}|q} \mathbf{Z}\mathfrak{q}$$

be the free abelian group on the primes of $\mathcal{O}_F$ lying above q. Also write

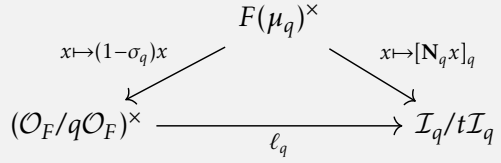
$$\mathcal{I} = \bigoplus_q \mathcal{I}_q$$

for the free abelian group on all primes, which is of course simply the group of non-zero fractional ideals of $\mathcal{O}_F$, written additively. If $y \in F$, we let $(y) \in \mathcal{I}$ be the principal ideal generated by y (i.e. $(y) = \sum_{\mathfrak{q}} \mathrm{ord}_{\mathfrak{q}}(y)\mathfrak{q}$), and $(y)_q \in \mathcal{I}_q$ denotes the projection to $\mathcal{I}_q$. Additionally, we denote by $[y] \in \mathcal{I}/t\mathcal{I}$ and $[y]_q \in \mathcal{I}_q/t\mathcal{I}_q$ the projections mod t.

Lemma 5.2.1. Suppose $q \equiv 1 \bmod t$ is prime. There is natural map of $\mathrm{Gal}(F/\mathbf{Q})$-modules

$$\ell_q \colon (\mathcal{O}_F/q\mathcal{O}_F)^\times \to \mathcal{I}_q/t\mathcal{I}_q$$

making the following diagram commute:



Furthermore, for $\mathfrak{q} \subset F$ a prime above q, we have $\mathrm{ord}_\mathfrak{q}\, \ell_q(x) = 0$ if and only if x is a t-th power modulo $\mathfrak{q}$.

The map on the left should be interpreted as follows: let $\mathfrak{q} \subset F$ be a prime above q, which is totally ramified in $F(\mu_q)$. Let $\mathfrak{Q} \subset F(\mu_q)$ be the unique prime above $\mathfrak{q}$. Then for $x \in F(\mu_r)^\times$, $\mathrm{ord}_\mathfrak{Q}((1-\sigma_q)x) = 0$, so $(1-\sigma_q)x$ is a unit in the localization of $\mathcal{O}_{F(\mu_q)}$ at $\mathfrak{Q}$. It can therefore be interpreted as an element of $(\mathcal{O}_{F(\mu_q)}/\mathfrak{Q})^\times$. Doing this for all $\mathfrak{Q}$ yields an element of

$$\prod_{\mathfrak{Q}|q} (\mathcal{O}_{F(\mu_q)}/\mathfrak{Q})^\times = \prod_{\mathfrak{q}|q} (\mathcal{O}_F/\mathfrak{q})^\times = (\mathcal{O}_F/q\mathcal{O}_F)^\times.$$

The first equality here is because every $\mathfrak{q} \mid q$ totally ramifies in $F(\mu_q)$, and the second because q is totally split in F, since $q \equiv 1 \bmod t$.

Proof. Let $\mathfrak{q} \subset F$ be a prime above q, and let $\pi_\mathfrak{q} \in F(\mu_q)$ be a uniformizer for the unique prime of $F(\mu_q)$ above $\mathfrak{q}$. Because $\mathfrak{q}$ totally, tamely ramifies in $F(\mu_q)$, ramification theory tells us that $\gamma_\mathfrak{q} = (1-\sigma_q)\pi_\mathfrak{q}$ is a generator for $(\mathcal{O}_{F(\mu_q)}/\mathfrak{Q})^\times = (\mathcal{O}_F/\mathfrak{q})^\times$ independent of the choice of uniformizer.

Any element x of $\prod_{\mathfrak{q}|q} (\mathcal{O}_F/\mathfrak{q})^\times = (\mathcal{O}_F/q\mathcal{O}_F)^\times$ can now be written as $x = (\gamma_\mathfrak{q}^{n_\mathfrak{q}})_\mathfrak{q}$. We then define $\ell_q(x) = \sum_{\mathfrak{q}|q} n_\mathfrak{q}\mathfrak{q}$. This map satisfies all the desired properties. □

Because the kernel of ℓ_q contains the t-th powers, we can make sense of $\ell_q(x)$ for all $x \in F^\times/F^{\times t}$ with $[x]_q = 0$.

Theorem 5.2.2. Suppose $r \in S_t$, and q is a rational prime. Then $[\kappa_r]_q = 0$ if $q \nmid r$, and $[\kappa_r]_q = \ell_q(\kappa_{r/q})$ otherwise.

Proof. If $q \nmid r$, then any prime $\mathfrak{q} \mid q$ of F is unramified in $F(\mu_r)$. That $[\kappa_r]_q = 0$ now follows immediately from the fact that $\kappa_r \equiv \mathbf{D}_r \xi_r \bmod F(\mu_r)^{\times t}$, and that $\mathbf{D}_r \xi_r$ is a unit of $F(\mu_r)$.

Now suppose $q \mid r$. By Remark 5.1.4, we may represent κ_r as $\kappa_r = \mathbf{D}_r \xi_r / \beta_r^t$, where $\beta_r \in F(\mu_r)^\times$ satisfies

$$(\sigma - 1)\beta_r = ((\sigma - 1)\mathbf{D}_r \xi_r)^{1/t}$$

for all $\sigma \in \mathrm{Gal}(F(\mu_r)/F)$. Define $\beta_{r/q}$ similarly. By the above, we may take $\beta_{r/q}$ to be coprime to q.

Let $\mathfrak{q} \subset F$ be a prime above q, and $\mathfrak{Q} \subset F(\mu_r)$ a prime above $\mathfrak{q}$. As the ramification index of $\mathfrak{q}$ in $F(\mu_r)$ is $q-1$, we have

$$\mathrm{ord}_{\mathfrak{Q}} \beta_r = \frac{-1}{t} \mathrm{ord}_{\mathfrak{Q}} \kappa_r = -\frac{q-1}{t} \mathrm{ord}_{\mathfrak{q}} \kappa_r,$$

so that

$$[\kappa_r]_q = \sum_{\mathfrak{q} \mid q} \left(\frac{t}{1-q} \mathrm{ord}_{\mathfrak{Q}} \beta_r \right) \mathfrak{q} \bmod t\mathcal{I}_q. \tag{5.2}$$

Let $\pi_{\mathfrak{q}} \in F(\mu_q)$ be a uniformizer for the unique prime above $\mathfrak{q}$. Because $F(\mu_r)/F(\mu_q)$ is unramified at primes above q, this is also a uniformizer at $\mathfrak{Q}$. Writing

$$\gamma = \prod_{\mathfrak{q} \mid q} \pi_{\mathfrak{q}}^{\mathrm{ord}_{\mathfrak{q}} \kappa_r},$$

we have that $\beta_r \gamma^{(q-1)/t}$ is a unit at all primes above q and $[\kappa_r]_q = [\mathbf{N}_q \gamma]_q$. It follows that modulo any prime above q, we have

$$(1 - \sigma_q)\gamma^{(q-1)/t} \equiv (\sigma_q - 1)\beta_r = ((q - 1 - \mathbf{N}_q)\mathbf{D}_{r/q} \xi_r)^{1/t}$$

$$= \frac{\mathbf{D}_{r/q} \xi_r^{(q-1)/t}}{((\mathrm{Fr}_q - 1)\mathbf{D}_{r/q} \xi_r)^{1/t}} \equiv \frac{\mathbf{D}_{r/q} \xi_{r/q}^{(q-1)/t}}{(\mathrm{Fr}_q - 1)\beta_{r/q}} \equiv \left(\frac{\mathbf{D}_{r/q} \xi_{r/q}}{\beta_{r/q}^t} \right)^{(q-1)/t} = \kappa_{r/q}^{(q-1)/t}.$$

Here we used (5.1), **ES2**, and **ES3**. The commutative diagram in Lemma 5.2.1 shows that $\frac{q-1}{t} \ell_q(\kappa_{r/q}) = \frac{q-1}{t} [\kappa_r]_q$. Writing $\ell_q(\kappa_{r/q}) = \sum_{\mathfrak{q} \mid q} a_{\mathfrak{q}} \mathfrak{q}$, we find from (5.2) that $\frac{q-1}{t} a_{\mathfrak{q}} = -\mathrm{ord}_{\mathfrak{Q}} \beta_r$, and hence

$$[\kappa_r]_q = \sum_{\mathfrak{q} \mid q} \left(\frac{t}{1-q} \mathrm{ord}_{\mathfrak{Q}} \beta_r \right) \mathfrak{q} = \ell_q(\kappa_{r/q}). \qquad \square$$

§5.3 Rubin's density theorem

Theorem 5.2.2 tells us about the factorization of κ_r above certain primes q in terms of the map ℓ_q. The final ingredient in the our study of Euler systems, will be a theorem that tells us how to find primes q for which the values $\ell_q(\kappa_{r/q})$ are 'easy' to calculate.

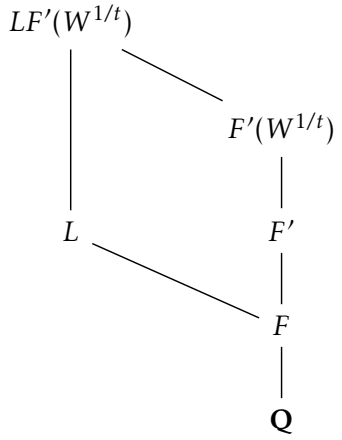
THEOREM 5.3.1. Suppose we are given a class $\mathfrak{c} \in \mathrm{Cl}(F)$ of p-power order, a finite $\mathrm{Gal}(F/\mathbf{Q})$-submodule $W \subset F^\times/F^{\times t}$ and a $\mathrm{Gal}(F/\mathbf{Q})$-homomorphism

$$\Psi\colon W \to (\mathbf{Z}/t\mathbf{Z})[\mathrm{Gal}(F/\mathbf{Q})].$$

Then there are infinitely many primes $\mathfrak{q} \in \mathfrak{c}$ such that

1. $q \equiv 1 \bmod t$, where q is the rational prime below $\mathfrak{q}$;
2. $[w]_q = 0$ for all $w \in W$;
3. there exists $u \in (\mathbf{Z}/t\mathbf{Z})^\times$ such that $\ell_q(w) = u\Psi(w)\mathfrak{q}$ for all $w \in W$.

Proof. Let L be the maximal abelian unramified p-extension of F, and let $F' = F(\mu_t)$. By class field theory, the Artin map gives an isomorphism between the Sylow p-subgroup of the class group and $\mathrm{Gal}(L/F)$. The fields we will consider are summed up in the diagram below.



First, note that $L \cap F' = F$, because F'/F is totally ramified at the unique prime above p. The proof will now proceed in several steps.

Step 1: the natural map $F^\times/F^{\times t} \to (F')^\times/(F')^{\times t}$ is injective.

We can identify $F^\times/F^{\times t}$ with $H^1(\mathrm{Gal}(\overline{F}/F), \mu_t)$, and it follows from the inflation-restriction exact sequence that

$$\begin{aligned}\ker(F^\times/F^{\times t} \to (F')^\times/(F')^{\times t}) &= \ker(H^1(\mathrm{Gal}(\overline{F}/F), \mu_t) \to H^1(\mathrm{Gal}(\overline{F}/F'), \mu_t)) \\ &= H^1(\mathrm{Gal}(F'/F), \mu_t).\end{aligned}$$

Because $\mathrm{Gal}(F'/F)$ is cyclic and μ_t finite, we have

$$\#H^1(\mathrm{Gal}(F'/F), \mu_t) = \#(\mu_t \cap F) = 1.$$

In particular, note that this allows us to interpret W as a subgroup of $(F')^\times/(F')^{\times t}$.

Step 2: $L \cap F'(W^{1/t}) = F$.

Kummer theory, combined with step 1, gives an isomorphism of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules $\mathrm{Gal}(F'(W^{1/t})/F') \to \mathrm{Hom}(W, \mu_t)$. As complex conjugation acts trivially on W and by -1 on μ_t, it acts by -1 on $\mathrm{Gal}(F'(W^{1/t})/F')$. Complex conjugation furthermore acts trivially on $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(LF'/F')$, since F is totally real and $\mathrm{Gal}(L/F)$ is abelian. It follows that complex conjugation must act both trivially and by -1 on $\mathrm{Gal}(F'(W^{1/t}) \cap LF'/F')$, and therefore $F'(W^{1/t}) \cap LF' = F'$. Intersecting this with L then yields that $F'(W^{1/t}) \cap L = F$.

Step 3: constructing the primes.

Fix a primitive t-th root of unity ζ_t, and define a $\mathbf{Z}/t\mathbf{Z}$-linear map

$$\iota\colon (\mathbf{Z}/t\mathbf{Z})[\mathrm{Gal}(F/\mathbf{Q})] \to \mu_t$$

by $\iota(\mathrm{Id}_F) = \zeta_t$ and $\iota(g) = 1$ for $\mathrm{Id}_F \neq g \in \mathrm{Gal}(F/\mathbf{Q})$. Let $\gamma \in \mathrm{Gal}(F'(W^{1/t})/F')$ be the element corresponding to $\iota \circ \Psi \in \mathrm{Hom}(W, \mu_t)$ via the Kummer isomorphism. By definition, this means that $\iota \circ \Psi(w) = \gamma(\sqrt[t]{w})/\sqrt[t]{w}$. Also let $\delta \in \mathrm{Gal}(L/F)$ be the element corresponding to $\mathfrak{c} \in \mathrm{Cl}(F)$ via the Artin map.

By step 2, there is a unique $\sigma \in \mathrm{Gal}(LF'(W^{1/t})/F)$ such that $\sigma|_{F'(W^{1/t})} = \gamma$ and $\sigma|_L = \delta$. The Chebotarev density theorem now guarantees the existence of infinitely many primes $\mathfrak{q} \subset F$ which are unramified in $LF'(W^{1/t})$, and whose Frobenius conjugacy class in $\mathrm{Gal}(LF'(W^{1/t})/F)$ is the conjugacy class of σ. We will show that all such $\mathfrak{q}$ satisfy the desired properties.

Step 4: proving the desired properties.

That $\mathfrak{q} \in \mathfrak{c}$ is clear from the construction. If q denotes the rational prime below $\mathfrak{q}$, then q is totally split in F' because $\sigma|_{F'} = \mathrm{Id}_{F'}$. From this we gather that $q \equiv 1 \bmod t$. The

assertion that $[w]_q = 0$ for all $w \in W$ is equally clear, following from the fact that $\mathfrak{q}$ is unramified in $F'(W^{1/t})$.

It remains only to show the final assertion. Lemma 5.2.1 says that $\mathrm{ord}_{\mathfrak{q}}(\ell_q(w)) = 0$ if and only if w is a t-th power modulo $\mathfrak{q}$. On the other hand,

$$\mathrm{ord}_{\mathfrak{q}}(\Psi(w)\mathfrak{q}) = 0 \iff \iota \circ \Psi(w) = 1 \iff \frac{\gamma(\sqrt[t]{w})}{\sqrt[t]{w}} = 1.$$

But $\gamma = \sigma|_{F'(W^{1/t})}$ is a Frobenius for $\mathfrak{q}$, so that this last statement is equivalent to saying that w is a t-th power modulo $\mathfrak{q}$. This means that the maps $W \to \mathbf{Z}/t\mathbf{Z}$ given by $w \mapsto \mathrm{ord}_{\mathfrak{q}}(\ell_q(w))$ and $w \mapsto \mathrm{ord}_{\mathfrak{q}}(\Psi(w)\mathfrak{q})$ have the same kernel and image, and hence differ by a unit $u \in (\mathbf{Z}/t\mathbf{Z})^\times$. Then the image of $w \mapsto \ell_q(w) - u\Psi(w)\mathfrak{q}$ is contained in $\bigoplus_{\mathfrak{q}' \neq \mathfrak{q}} (\mathbf{Z}/t\mathbf{Z})\mathfrak{q}'$, which has no non-zero $\mathrm{Gal}(F/\mathbf{Q})$-submodules. We conclude that $\ell_q(w) = u\Psi(w)\mathfrak{q}$ for all $w \in W$, as desired. □

6 Proof of the Main Conjecture

In this final chapter, we finish the proof of the Main Conjecture. There are plenty books which do this in detail, such as Rubin's original account [Lan90, Appendix] and [CS06]. However, in a fully detailed proof it can be easy to get overwhelmed by all the technicalities, and as a result miss the forest for the trees. Instead, we will focus on the main ideas, namely how the theory of Euler systems gives us information about the class group that allows us to conclude the theorem.

From now on, fix $i \not\equiv 0 \bmod p-1$ even. Recall that we have reduced the Main Conjecture to the statement that

$$\mathrm{ch}(e_i \mathscr{Y}_\infty) = \mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1})).$$

Let us start with a quick outline of the proof of this statement. Let ξ_r be the Euler system discussed at the beginning of the previous chapter, which was given by

$$\xi_r = (\zeta_m^a \zeta_r - 1)^b (\zeta_m^{-a} \zeta_r - 1)^b (\zeta_m \zeta_r - 1)^c (\zeta_m^{-1} \zeta_r - 1)^c,$$

where $a, b, c \in \mathbf{Z}_{\geq 1}$ denote respectively a generator of $\mathbf{Z}_p^\times$, an inverse of 2 mod t, and an inverse of -2 mod t. In particular, we have that

$$\xi_1 \equiv \zeta_m^{(1-a)/2} \frac{\zeta_m^a - 1}{\zeta_m - 1} \bmod F^{\times t}.$$

The fact that this is precisely the unit that generates $\mathscr{C}_{\infty,1}$ allows us to relate the Euler system to the characteristic ideal $\mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1}))$. Next up, by finding an appropriate map Ψ, we use Theorem 5.3.1 to find a prime $\mathfrak{q}_1$ for which we can calculate $\ell_q(\kappa_1)$ in terms of Ψ. The factorization theorem 5.2.2 then tells us about how κ_{q_1} factors, namely via $[\kappa_{q_1}]_{q_1} = \ell_{q_1}(\kappa_1)$. We now pick another Ψ, and we apply the same results to find a prime $\mathfrak{q}_2$ for which we can calculate $\ell_{q_2}(\kappa_{q_1})$ in terms of Ψ, and factor $[\kappa_{q_1 q_2}]_{q_2} = \ell_{q_2}(\kappa_{q_1})$. Repeating this enough times, we obtain information about the class group, and through κ_1 we relate the class group back to $\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1}$.

Theorem 6.0.1. For all even $i \not\equiv 0$, we have that

$$\mathrm{ch}(e_i\mathscr{Y}_\infty) = \mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1})).$$

Proof. There exists an injective map

$$\bigoplus_{j=1}^{k} \Lambda(\Gamma)/g_j\Lambda(\Gamma) \to e_i\mathscr{Y}_\infty$$

with finite cokernel. The characteristic ideal of $\mathscr{Y}_\infty$ is then generated by $g^{(i)} = \prod_{j=1}^{k} g_j$. Also, let $h^{(i)}$ be a generator of $\mathrm{ch}(e_i(\mathscr{E}_{\infty,1}/\mathscr{C}_{\infty,1}))$.

Fix now a positive integer n, and write $F = F_n^+$. From now on we will think of $\mathscr{Y}_n$ as the Sylow p-subgroup of the class group of F_n. Let $\mathfrak{c}_1,\dots,\mathfrak{c}_k,\mathfrak{c}_{k+1} \in e_i\mathscr{Y}_n$ be 'specially chosen' ideal classes. The idea is to let $\mathfrak{c}_j$ be the image in $e_i\mathscr{Y}_n$ of $1 \in \Lambda(\Gamma)/g_j\Lambda(\Gamma)$ under the above map, and $\mathfrak{c}_{k+1}$ can be any class. Furthermore, let C be as in Lemma 4.3.5, and choose $c > C$ such that p^c annihilates the cokernel of the above map. Let $\theta\colon e_i\mathscr{E}_{n,1} \to \mathbf{Z}_p[\Gamma/\Gamma_n]$ be the corresponding map from Lemma 4.3.5, chosen such that $\theta(e_i\xi_{n,a}) = p^c h^{(i)}$. Let t be a large power of p.

If $\mathfrak{q} \subset F$ is a prime lying above a rational prime q, define a map $\nu_\mathfrak{q}\colon F^\times/F^{\times t} \to (\mathbf{Z}/t\mathbf{Z})[\Gamma/\Gamma_n]$ by $\nu_\mathfrak{q}(w)e_i\mathfrak{q} = e_i[w]_q \in e_i(\mathcal{I}_q/t\mathcal{I}_q)$. Note that $e_i(\mathcal{I}_q/t\mathcal{I}_q)$ is free of rank 1 as a $(\mathbf{Z}/t\mathbf{Z})[\Gamma/\Gamma_n]$-module, so that $\nu_\mathfrak{q}$ is actually well-defined.

We will repeatedly apply Theorem 5.3.1 to construct primes $\mathfrak{q}_1,\dots,\mathfrak{q}_{k+1}$ lying above $q_1,\dots,q_{k+1}$ such that

1. $\mathfrak{q}_j \in \mathfrak{c}_j$;
2. $q_j \equiv 1 \bmod t$;
3. $\nu_{\mathfrak{q}_1}(\kappa_{q_1}) = u_1 p^c h^{(i)}$;
4. $g_{j-1}\nu_{\mathfrak{q}_j}(\kappa_{r_j}) = u_j p^c \nu_{\mathfrak{q}_{j-1}}(\kappa_{r_{j-1}})$ for $j > 1$

where $r_j = q_1 \cdots q_j$ and $u_j \in (\mathbf{Z}/t\mathbf{Z})^\times$.

For the first prime, we let $W = e_i(\mathcal{O}_F^\times/\mathcal{O}_F^{\times t})$, and define $\Psi\colon W \to (\mathbf{Z}/t\mathbf{Z})[\Gamma/\Gamma_n]$ to be the composition

$$W \longrightarrow e_i(\mathscr{E}_{n,1}/\mathscr{E}_{n,1}^t) \xrightarrow{\theta} (\mathbf{Z}/t\mathbf{Z})[\Gamma/\Gamma_n] \xrightarrow{e_i} e_i(\mathbf{Z}/t\mathbf{Z})[\Gamma/\Gamma_n]$$

Let $\mathfrak{q}_1$ be a prime satisfying the conclusion of Theorem 5.3.1, with this W, Ψ, and $\mathfrak{c} = \mathfrak{c}_1$. Then clearly conditions 1 and 2 are satisfied. Furthermore, it follows from

Theorems 5.2.2 and 5.3.1 that for some $u_1 \in (\mathbf{Z}/t\mathbf{Z})^\times$ we have

$$\nu_{\mathfrak{q}_1}(\kappa_{\mathfrak{q}_1})e_i\mathfrak{q}_1 = e_i[\kappa_{\mathfrak{q}_1}]_{q_1} = e_i\ell_{q_1}(\kappa_1) = u_1\Psi(e_i\kappa_1)e_i\mathfrak{q}_1 = u_1p^ch^{(i)}e_i\mathfrak{q}_1.$$

This proves 3.

Suppose now that we have constructed $\mathfrak{q}_1,\dots,\mathfrak{q}_{j-1}$. Let $W \subset F^\times/F^{\times t}$ be the $\mathbf{Z}_p[\Gamma/\Gamma_n]$-submodule generated by $e_i\kappa_{r_{j-1}}$. One can show now[1] that there is a map $\Psi'\colon W \to (\mathbf{Z}/t\mathbf{Z})[\Gamma/\Gamma_n]$ with the property that

$$g_{j-1}\Psi'(e_i\kappa_{r_{j-1}}) = p^c\nu_{\mathfrak{q}_{j-1}}(\kappa_{r_{j-1}}).$$

Let $\mathfrak{q}_j$ be a prime satisfying the conclusion of 5.3.1, this time with W as above, $\Psi = e_i\Psi'$, and $\mathfrak{c} = \mathfrak{c}_j$. Again conditions 1 and 2 are immediate, and condition 4 follows by a similar computation as above.

Continue this process until we have constructed $\mathfrak{q}_1,\dots,\mathfrak{q}_{k+1}$. If we now combine condition 3 and condition 4 for all $j > 1$, we get that

$$p^{c(k+1)}h^{(i)} = u\nu_{\mathfrak{q}_{k+1}}(\kappa_{r_{k+1}})g^{(i)}$$

for some unit $u \in (\mathbf{Z}/t\mathbf{Z})^\times$. In particular, we see that $g^{(i)} \mid p^{c(k+1)}h^{(i)}$ in the ring $(\mathbf{Z}/t\mathbf{Z})[\Gamma_n]$. Because this holds for all sufficiently large t and n, we get that the divisibility also holds in $\Lambda(\Gamma)$. By the Ferrero–Washington theorem, $p \nmid g^{(i)}$, and therefore $g^{(i)} \mid h^{(i)}$.

The relation $g^{(i)} \mid h^{(i)}$ is actually true as well for $i = 0$, because $g^{(0)}$ is actually a unit in $\Lambda(\Gamma)$. Let $g = \prod_{i \text{ even}} g^{(i)}$ and $h = \prod_{i \text{ even}} h^{(i)}$. Under the isomorphism of $\Lambda(\Gamma)$ with $\Lambda = \mathbf{Z}_p[\![T]\!]$, we may assume g and h are both the product of a power of p and a distinguished polynomial. It suffices to show now that this power of p is the same for both, and their degrees are equal.

Let μ be such that p^μ is the largest power of p dividing h (by Ferrero–Washington, g is not divisible by p). We know from the proof of 2.1.2 that for large enough n, we have that $\#\mathscr{Y}_n^+ = p^{\deg(g)n+\nu}$. For the other module the situation is a bit more complicated; we only have that for all n, $\#(\mathscr{E}_{n,1}^+/\mathscr{C}_{n,1}^+) = p^{\mu p^n+\deg(h)n+\nu_n'}$, where ν_n' is bounded. But Remark 4.3.4 states that $\#\mathscr{Y}_n^+ = \#(\mathscr{E}_{n,1}^+/\mathscr{C}_{n,1}^+)$, which gives the desired equality. □

[1] It is at this point in particular that we are skipping many technical details. Namely, our choice of $\mathfrak{c}_j$, c and t all come into play here.

A Appendix

§A.1 The Hilbert class field

At its most basic level, class field theory gives a way to relate Galois groups of unramified abelian extensions of number fields to the class group of the base field, through something called the *Hilbert class field*. A good reference is [Neu99].

Let F be a number field, and $\mathcal{I}$ the group of its non-zero fractional ideals. Recall that if K/F is a finite, unramified abelian extension, the Artin symbol

$$\left(\frac{K/F}{\cdot}\right): \mathcal{I} \to \mathrm{Gal}(K/F)$$

is defined by letting $\left(\frac{K/F}{\mathfrak{p}}\right) = \mathrm{Fr}_\mathfrak{p}$ for $\mathfrak{p} \subset F$ a prime, and extending multiplicatively.

Theorem A.1.1. There exists a unique field extension H/F that is abelian, everywhere unramified and is maximal with these properties among extensions of F. Furthermore, the extension is finite and its Artin map is surjective and trivial on the principal ideals. Hence it induces an isomorphism

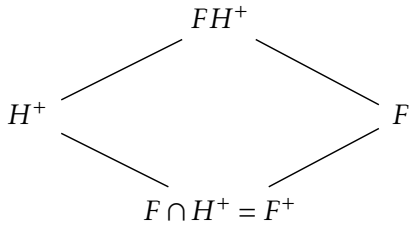
$$\left(\frac{H/F}{\cdot}\right): \mathrm{Cl}(F) \xrightarrow{\sim} \mathrm{Gal}(H/F).$$

The field H from the theorem is called the Hilbert class field of F.

Because $\mathrm{Gal}(H/F)$ is abelian, it is the direct sum of its Sylow p-subgroups. Therefore, for any prime p, $\mathrm{Gal}(H/F)$ has a unique minimal subgroup of p-power index (namely, the direct sum of the Sylow subgroups for primes different from p). Associated to this subgroup is a subfield $L \subset H$, which is then the maximal abelian unramified extension of F of p-power degree. The group $\mathrm{Gal}(L/F)$, which is the quotient of $\mathrm{Gal}(H/F)$ by the aforementioned p-power index subgroup, is naturally identified with the Sylow p-subgroup of $\mathrm{Gal}(H/F)$. The Artin map allows us to further identify it with the Sylow

p-subgroup of $\mathrm{Cl}(F)$. We will often make this identification.

Suppose now that F is a CM field, meaning that it is totally imaginary, and has a totally real subfield F^+ such that F/F^+ is quadratic. If h denotes the class number of F and h^+ that of F^+, then $h^+ \mid h$. To see this, let H and H^+ be the Hilbert class fields of F and F^+, respectively.



Because F/F^+ is totally ramified at the infinite primes, we have $F \cap H^+ = F^+$. Consequently, we have an isomorphism $\mathrm{Gal}(FH^+/F) \to \mathrm{Gal}(H^+/F^+)$. In particular, FH^+/F^+ is abelian. Furthermore, because the extension H^+/F^+ is unramified, so is the extension FH^+/F. It follows that $FH^+ \subset H$, so we have a surjection $\mathrm{Gal}(H/F) \to \mathrm{Gal}(FH^+/F) \to \mathrm{Gal}(H^+/F^+)$. By the above theorem, we find that $h^+ \mid h$.

§A.2 Group cohomology

Let G be a profinite group and and M a $\mathbf{Z}[G]$-module, such that the action of G on M is continuous if M is equipped with the discrete topology. A *crossed homomorphism* is a continuous map $f : G \to M$ such that $f(gh) = gf(h) + f(g)$. If $m \in M$ is any element, the map $g \mapsto gm - m$ is a crossed homomorphism. Any crossed homomorphism of this form is called *principal*. Let $H^1(G, M)$ denote the quotient group of all crossed homomorphisms modulo the principal crossed homomorphisms. It is called the first cohomology group of G with coefficients in M.

Example A.2.1. If G acts trivially on M, then $H^1(G, M) = \mathrm{Hom}(G, M)$.

Proposition A.2.2. Any exact sequence of $\mathbf{Z}[G]$-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

induces a long exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C).$$

Proof. If M is a $\mathbf{Z}[G]$-module, let $Z^1(G, M)$ denote the group of crossed homomorphisms $G \to M$. We have a map $M \to Z^1(G, M)$ sending m to the principal crossed

homomorphism $g \mapsto gm - m$. The proposition now follows upon applying the snake lemma to the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & Z^1(G,A) & \longrightarrow & Z^1(G,B) & \longrightarrow & Z^1(G,C) & & \end{array}$$

□

If $H \subset G$ is a closed subgroup, then there is a natural induced homomorphism $H^1(G,M) \to H^1(H,M)$ called the *restriction*. If in addition H is normal, then M^H is a $\mathbf{Z}[G/H]$-module, and there is a natural map $H^1(G/H, M^H) \to H^1(G,M)$, called the *inflation*.

Proposition A.2.3. The restriction and inflation maps fit into an exact sequence

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G,M) \xrightarrow{\text{Res}} H^1(H,M).$$

Proof. See [Ser79, Chapter VII, §6, Prop. 4]. □

We will also need the following result regarding the cohomology of finite cyclic groups.

Proposition A.2.4. If G is finite cyclic and M is finite, then

$$\#H^1(G,M) = \#(M^G/N_G M),$$

where $N_G M = \{\sum_{g\in G} gm \mid m \in M\}$.

Proof. See [Ser79, Chapter VIII, §4, Prop. 8]. □

If L/K is a Galois extension, we also write $H^1(L/K)$ for $H^1(\mathrm{Gal}(L/K), L^\times)$. The next result derives its name from the fact that it was the 90th theorem in Hilbert's famous *Zahlbericht*.

Proposition A.2.5 (Hilbert 90). If L/K is a finite Galois extension, then $H^1(L/K) = 0$.

Proof. See [Ser79, Chapter X, §1, Prop. 2]. □

Bibliography

[Bou89] Nicolas Bourbaki. *Commutative Algebra: Chapters 1-7*. 1st ed. Springer-Verlag, 1989.

[Bru67] Armand Brumer. "On the units of algebraic number fields". *Mathematika* 14.2 (1967), pp. 121–124.

[Col10] Pierre Colmez. "Fonctions d'une variable p-adique". *Représentations p-adiques de groupes p-adiques II : Représentations de* $\mathbf{GL}_2(\mathbf{Q}_p)$ *et* (φ,Γ)*-modules*. Ed. by Laurent Berger, Christophe Breuil, and Pierre Colmez. Astérisque 330. Société Mathématique de France, 2010, pp. 13–59.

[Col79] Robert Coleman. "Division Values in Local Fields." *Inventiones Mathematicae* 53 (1979), pp. 91–116.

[CS06] John Coates and Ramdorai Sujatha. *Cyclotomic fields and zeta values*. 1st ed. Springer-Verlag, 2006.

[HHO17] William Hart, David Harvey, and Wilson Ong. "Irregular primes to two billion". *Mathematics of Computation* 86.308 (2017), pp. 3031–3049.

[Iwa59] Kenkichi Iwasawa. "On Γ-extensions of algebraic number fields". *Bulletin of the American Mathematical Society* 65.4 (1959), pp. 183–226.

[Iwa64] Kenkichi Iwasawa. "On some modules in the theory of cyclotomic fields". *Journal of the Mathematical Society of Japan* 16.1 (1964), pp. 42–82.

[Iwa73] Kenkichi Iwasawa. "On $\mathbf{Z}_l$-Extensions of Algebraic Number Fields". *Annals of Mathematics* 98.2 (1973), pp. 246–326.

[KL64] Tomio Kubota and Heinrich Leopoldt. "Eine p-adische Theorie der Zetawerte. Teil I: Einführung der p-adischen Dirichletschen L-Funktionen." *Journal für die reine und angewandte Mathematik* 214-215 (1964), pp. 328–339.

[Kol90] Victor Kolyvagin. "Euler Systems". *The Grothendieck Festschrift: A Collection of Articles Written in Honor of the 60th Birthday of Alexander Grothendieck*. Ed. by Pierre Cartier et al. Birkhäuser Boston, 1990, pp. 435–483.

[Lan90] Serge Lang. *Cyclotomic fields I and II*. 2nd ed. Springer-Verlag, 1990.

[MW84] Barry Mazur and Andrew Wiles. "Class fields of abelian extensions of $\mathbf{Q}$". *Inventiones Mathematicae* 76 (1984), pp. 179–330.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. 1st ed. Springer-Verlag, 1999.

[Rib76] Kenneth Ribet. "A Modular Construction of unramified p-Extensions of $\mathbf{Q}(\mu_p)$". *Inventiones Mathematicae* 34 (1976), pp. 151–162.

[RW] Joaquín Rodrigues Jacinto and Chris Williams. *An Introduction to p-adic L-functions*. URL: https://warwick.ac.uk/fac/sci/maths/people/staff/cwilliams/lecturenotes/lecturenotes-change.pdf.

[Ser60] Jean-Pierre Serre. "Classes des corps cyclotomiques". *Séminaire Bourbaki*. Vol. 5. 174. Société Mathématique de France, 1960, pp. 83–93.

[Ser79] Jean-Pierre Serre. *Local Fields*. 1st ed. Springer-Verlag, 1979.

[SW13] William Stein and Christian Wuthrich. "Algorithms for the arithmetic of elliptic curves using Iwasawa theory". *Mathematics of Computation* 82.283 (2013), pp. 1757–1792.

[Tha88] Francisco Thaine. "On the Ideal Class Groups of Real Abelian Number Fields". *Annals of Mathematics* 128.1 (1988), pp. 1–18.

[Was97] Lawrence Washington. *Introduction to Cyclotomic Fields*. 2nd ed. Springer-Verlag, 1997.