ALGANT Master Thesis - 16 July 2018

The Iwasawa Main Conjecture: an approach via Euler Systems

Alessandro Biagi

Advised by

Prof. Dr. Massimo Bertolini

Università degli Studi di Padova

Universität Duisburg – Essen

Essener Seminar für Algebraische
Geometrie und Arithmetik

Fakültat für Mathematik
Universität Duisburg-Essen
Thea-Leymann-Str. 9, 45141 Essen

Introduction

The Iwasawa Main Conjecture gives relations between some algebraically defined Iwasawa modules and the analytically defined p-adic L-functions. It was proved for abelian Number Fields by Mazur and Wiles in 1984 using deep techniques from Algebraic Geometry. Therefore it is also known as "The Mazur-Wiles theorem".

In 1990, Karl Rubin found a simpler proof using a particular example of the so-called *Kolyvagin's Euler Systems*. The aim of this thesis is to give a detailed exposition of Rubin's proof of "The Main Conjecture" of Iwasawa theory for $\mathbb{Q}(\zeta_{p^\infty})$, with p odd prime, providing the necessary background to understand it.
The thesis is divided into 5 chapters as follows.

In **chapter 1** we give some basic results about the arithmeticity of Cyclotomic fields (with a special focus on $\mathbb{Q}(\zeta_{p^m})$) and we introduce CM-fields and their maximal real subfields. Moreover we discuss the Cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$ to deduce properties of the Cyclotomic units of $\mathbb{Q}(\zeta_{p^m})$ itself, such as some facts about their corresponding class numbers. The main reference for this is [**Wa**].

In **chapter 2** we study Dirichlet characters (in particular the Teichmüller character ω), Dirichlet L-series and p-adic L-functions. We follow basically [**Con1**], [**Wa**] and [**Iw**], but also some notes taken during a course held by Professor Massimo Bertolini regarding Modular forms.

In **chapter 3**, we describe the algebraic properties of the Iwasawa algebra $\Lambda = \mathbb{Z}_p[|T|]$, with special attention to the Structure theorem for finitely generated Λ-modules given in terms of a *pseudo-isomorphism*. This is done referring to [**Neu2**] and to some notes taken during a course on Iwasawa theory held by Professor Andreas Nickel. Then, following again [**Wa**] and [**Iw**], we conclude the chapter applying some of the previous results to describe another way to construct p-adic L-functions. The most important result about this section is that we can find a power series $f(T, \omega^j)$ such that $L_p(s, \omega^j) = f((1+p)^s - 1, \omega^j)$. This turns out to be fundamental for stating The Main Conjecture.

In **chapter 4** we treat the theory of $\mathbb{Z}_p$-extensions. Following [**Wa**] and [**Wi**] we give an introduction to Infinite Galois theory and the corresponding Ramification theory. Next, we show how to prove the Iwasawa's theorem about ideal class groups in $\mathbb{Z}_p$-extensions, using the approaches of [**Wa**] and [**Bro**]. Furthermore, we define the orthogonal idempotents and we study some consequences of the decomposition that they produce on Λ-modules, following [**Sa3**]. Finally, as an important application, we discuss in the setting of $\mathbb{Q}(\zeta_{p^m})$ the behavior of the local units modulo Cyclotomic units and the Maximal Abelian p-extension unramified outside p. For this we refer to [**Wa**] and [**Lan1**].

In **chapter 5**, we finally prove The Iwasawa Main Conjecture. We introduce the *Euler Systems of Cyclotomic units* that we need in order to study the problem in detail.

Besides, we discuss the cardinality of the ideal class group of $\mathbb{Q}(\zeta_p)^+$ using the basic properties of the previously defined Euler systems. The proof of the most important result of this section gives an idea of the strategy that is used to prove the Mazur-Wiles theorem. After this, we give three equivalent statements of The Iwasawa Main Conjecture. In order to prove the equivalence, we develop a small part of the theory of Adjoints. Finally, we need to discuss other important techniques of Iwasawa theory which allow us to conclude the proof. The main reference for this chapter is [**Wa**].

Contents

Chapter 1

Basic results on Cyclotomic fields and Cyclotomic units

The aim of this chapter is to give the basic background about Cyclotomic fields, CM-fields and Cyclotomic units.

1.1 Some facts on Cyclotomic fields

Let ζ_n be a primitive n-th root of unity for every $n \geq 1$. We start proving some useful arithmetic properties of $\mathbb{Q}(\zeta_n)$. In order to do this, we recall some results that we take for granted.

Facts.

1. Remind that the n-th cyclotomic polynomial is defined to be $\Phi_n(X) = \prod_{\zeta \in S_n}(X - \zeta)$ where S_n is the set of the primitive n-th roots of unity. One can prove that $\Phi_n(x) \in \mathbb{Z}[X]$ and that it is irreducible for every $n \geq 1$. If $n = p^m$ where p is a prime number, then we have

   - $\Phi_n(X) = \Phi_p(X) = \dfrac{X^p - 1}{X - 1} = X^{p-1} + \ldots + X + 1$ if $m = 1$
   - $\Phi_n(X) = \Phi_{p^m}(X) = \dfrac{X^{p^m} - 1}{X^{p^{m-1}} - 1} = X^{p^{m-1}(p-1)} + \ldots + X^{p^{m-1}} + 1$ if $m \geq 2$

2. Recall also that if $\zeta \in S_n$ then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ where ϕ is the Euler function.

3. Let K be a number field. We will denote by $\mathcal{O}_K$ its ring of integers. Then it is known that for $K = \mathbb{Q}(\zeta_n)$ we have $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

4. A prime number p ramifies in $\mathbb{Q}(\zeta_n)$ if and only if $p \mid n$.

5. A prime number p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \mod n$.

Lemma 1.1.1. *Let $n \geq 1$ and $K = \mathbb{Q}(\zeta_n)$. If ζ and ζ' are two primitive n-th roots of unity, then $\frac{1-\zeta'}{1-\zeta}$ is a unit in $\mathcal{O}_K$.*

Proof. We know by elementary group theory that there must be an integer s relatively prime to n such that $\zeta' = \zeta^s$. Now notice that

$$\frac{1 - \zeta^s}{1 - \zeta} = 1 + \zeta + \ldots + \zeta^{s-1} \in \mathcal{O}_K = \mathbb{Z}[\zeta_n].$$

Since we can interchange the roles of ζ and ζ', arguing as above we also find that $\frac{1-\zeta}{1-\zeta'} \in \mathcal{O}_K$. This implies the statement.

□

Proposition 1.1.2. *Suppose that n is not a prime power. Then $1-\zeta_n$ is a unit of $\mathbb{Z}[\zeta_n]$ and $\prod_{\substack{0<j<n \\ (j,n)=1}}(1-\zeta_n^j) = 1$.*

Proof. From fact number 1 above we get that $X^{n-1}+X^{n-2}+\ldots+X+1 = \prod_{j=1}^{n-1}(X-\zeta_n^j)$. Setting $X = 1$ follows that $n = \prod_{j=1}^{n-1}(1-\zeta_n^j)$. Now let q be a prime dividing n and say that q^a is the biggest power of q that divides n. Since j runs trough the multiples of n/q^a lesser or equal than $n-1$, we deduce that the above product has $\prod_{j=1}^{q^a-1}(1-\zeta_{q^a}^j) = q^a$ between its factors. Removing this product and applying this reasoning to every prime that divides n, it follows that $1 = \prod_j(1-\zeta_n^j)$ where the product is over those j 's such that ζ_n^j has not a prime power order. Since n has at least two distinct prime factors we must have that $1-\zeta_n$ appears in the previous product. Therefore it is a unit. This proves the first part of the proposition. For the second one, notice that $\mathcal{N}_{\mathbb{Q}(\zeta_n)|\mathbb{Q}}(1-\zeta_n) = \prod_{(j,n)=1}(1-\zeta_n^j) = \pm 1$. However since in this case the complex conjugation is in $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, the norm of every element can be written in the form $\alpha\overline{\alpha}$ for some α. Hence we deduce that previous norm must be 1, i.e. $\prod_{(j,n)=1}(1-\zeta_n^j) = 1$. Thus the proof is complete. □

Proposition 1.1.3. *Let p be a prime number and let $K = \mathbb{Q}(\zeta_{p^m})$. Then the principal ideal $(1-\zeta)\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ and $p\mathcal{O}_K = (1-\zeta)^{\phi(p^m)}\mathcal{O}_K$. In particular, p is totally ramified in $\mathcal{O}_K$.*

Proof. Firstly, notice that by the previous remark one finds that $\Phi_{p^m}(1) = p$ but also

$$\Phi_{p^m}(1) = \prod_{\zeta' \in S_{p^m}}(1-\zeta') = (1-\zeta)^{\phi(p^m)} \prod_{\zeta' \in S_{p^m}} \frac{1-\zeta'}{1-\zeta}$$

Now by the previous lemma, we have that $\epsilon \overset{\text{def}}{=} \prod_{\zeta' \in S_{p^m}} \frac{1-\zeta'}{1-\zeta}$ is a unit in $\mathcal{O}_K$. Putting all together we get $p = \epsilon(1-\zeta)^{\phi(p^m)}$ and so $p\mathcal{O}_K = (1-\zeta)^{\phi(p^m)}\mathcal{O}_K$. Now let $(1-\zeta)\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ be the factorization of $(1-\zeta)\mathcal{O}_K$ into prime ideals. Thus we deduce that

$$p\mathcal{O}_K = (1-\zeta)^{\phi(n)}\mathcal{O}_K = \mathfrak{p}_1^{\phi(n)e_1}\cdots\mathfrak{p}_r^{\phi(n)e_r}$$

Comparing this to the fundamental equation about the degrees, we find that

$$[\mathbb{Q}(\zeta_{p^m}):\mathbb{Q}] = \phi(n) = \sum_{1\le i\le r} e_i f_i \phi(n)$$

Hence we deduce that $r = e_1 = f_1 = 1$. This implies the statement. □

Lemma 1.1.4. *Let m and n be two positive integers. Then $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)})$. In particular, if $(m,n) = 1$ then $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = 1$.*

Proof. Clearly we have that $\mathbb{Q}(\zeta_{(m,n)}) \subseteq \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Now we show that actually the equality holds proving that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_{(m,n)})$ have the same degree over $\mathbb{Q}$. We indicate by $[m,n]$ the least common multiple of m and n. Notice that

$$[\mathbb{Q}(\zeta_{[m,n]}):\mathbb{Q}]\cdot[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}] = [\mathbb{Q}(\zeta_m):\mathbb{Q}]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}]$$

Then using Fact 2 above follows that

$$[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}] = \frac{\phi(m)\phi(n)}{\phi([m,n])}$$

Next, recalling that $mn/[m,n] = (m,n)$ and applying the known formulas for ϕ (see [**Con2**]) we deduce that $[\mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi((m,n))$. However this is the degree of $\mathbb{Q}(\zeta_{(m,n)})$ over $\mathbb{Q}$. This concludes the proof. □

Remark 1. Let m and n two positive integers such that $(m,n)=1$ as before. Since $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ and $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ are two Galois extensions, then the previous lemma implies that $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_n)$ are linearly disjoint over $\mathbb{Q}$ (one can look at [**Cla**] for more details about the notion of linear disjointness).

Lemma 1.1.5. *If an algebraic integer is such that its conjugates have absolute value 1, then it is a root of unity.*

Proof. First of all, consider any polynomial in $\mathbb{Q}[X]$ of degree n such that all its roots have absolute value equal to 1. Then if we consider the coefficient of this polynomial related to the power X^t, we have that it is bounded by $\binom{n}{t}$. Then set $m=[K:\mathbb{Q}]$ and let $f(X)$ be the minimal polynomial of α over $\mathbb{Q}$ where α is an algebraic integer whose conjugates have absolute value 1. Then we know that actually the coefficients of $f(X)$ are in $\mathbb{Z}$. Thus using the previous bound and the fact that the coefficients of $f(X)$ are integers we can deduce that there only finitely many algebraic integers as α. Now consider a power of α, say α^t. This is clearly an algebraic integer and its degree over $\mathbb{Q}$ is at most m. Moreover, if $\alpha_1=\alpha,\alpha_2,\dots,\alpha_m$ are the conjugates of α then $\alpha_1^r,\dots,\alpha_m^r$ are the conjugates of α^r. Hence, by the above argument, we deduce that the set of powers of α form a finite multiplicative group. This concludes the lemma. □

Proposition 1.1.6. *Let ϵ be a unit of $\mathbb{Z}[\zeta_p]$. Then there exist $\epsilon_1\in\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ and $r\in\mathbb{Z}$ such that $\epsilon=\zeta_p^r\epsilon_1$.*

Proof. Let $\alpha=\epsilon/\overline{\epsilon}$. Notice that the complex conjugation ρ is such that $\rho(\mathbb{Z}[\zeta_p])=\mathbb{Z}[\zeta_p]$ (just let ρ act on the $\mathbb{Z}$-basis $\{1,\zeta_p,\dots,\zeta_p^{p-2}\}$). Hence also $\overline{\epsilon}$ is a unit of $\mathbb{Z}[\zeta_p]$. This implies that α is an algebraic integer. Moreover, since ρ commutes with every element of $Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ we have that all conjugates of α have absolute value 1. By lemma 1.1.5, we deduce that α is a root of unity and therefore $\epsilon/\overline{\epsilon}=\pm\zeta_p^a$ for some integer a (recall that the only roots of unity in $\mathbb{Q}(\zeta_p)$ are of this form). Suppose then that $\alpha=-\zeta_p^a$ and write $\epsilon=b_0+b_1\zeta_p+\dots+b_{p-2}\zeta^{p-2}$ with $b_i\in\mathbb{Z}$ for every i. Then $\epsilon\equiv b_0+b_1+\dots+b_{p-2}$ mod $(1-\zeta_p)$. Moreover $\overline{\epsilon}=b_0+b_i\zeta_p^{-1}+\dots\equiv b_0+b_1+\dots+b_{p-2}\equiv\epsilon=-\zeta_p^a\overline{\epsilon}\equiv-\overline{\epsilon}$ mod $(1-\zeta_p)$. Hence $2\overline{\epsilon}\equiv 0 \mod (1-\zeta_p)$. However $2\notin(1-\zeta_p)$. Since $(1-\zeta_p)$ is a prime ideal, we deduce that $\overline{\epsilon}\in(1-\zeta_p)$ and this is a contradiction because $\overline{\epsilon}$ is a unit. Therefore we have that $\epsilon/\overline{\epsilon}=+\zeta_p^a$, i.e. $\overline{\epsilon}=\zeta_p^{-a}\epsilon$. Let $r\in\mathbb{Z}$ such that $2r\equiv a$ mod p and let $\epsilon_1=\zeta_p^{-r}\epsilon$ (notice that such r exists because p is odd). Then $\epsilon=\zeta_p^r\epsilon_1$ and $\overline{\epsilon}_1=\zeta_p^r\overline{\epsilon}=\zeta_p^{r-a}\epsilon=\epsilon_1$. This proves the proposition since $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ is the fixed field of ρ. □

Lemma 1.1.7. *The roots of unity in $\mathbb{Q}(\zeta_m)$ are of the form $\pm\zeta_m^j$ for $j\in\mathbb{Z}$. The plus sign holds if m is even, the minus if m is odd.*

Proof. Let ζ_n be a primitive n-th root of unity in $\mathbb{Q}(\zeta_m)$. Suppose that m is even and write $m = 2k$ with $k \geq 1$. Then $\mathbb{Q}(\zeta_m)$ contains a primitive r-th root of unity where r is the least common multiple of n and m. This implies that $\mathbb{Q}(\zeta_r) \subseteq \mathbb{Q}(\zeta_m)$ and so considering the degrees over $\mathbb{Q}$ we obtain that $\phi(r) \mid \phi(2k)$, where ϕ is the Euler function. Since $2k$ is even, using the known formulas for ϕ (see [**Con2**]) one can prove that this implies $r = 2k = m$. Hence $n \mid m$ and so ζ_n is an m-th root of unity. Now suppose that m is odd. Notice that then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$. Arguing as above we obtain that ζ_n is a $2m$-th root of unity. Since $\zeta_{2m} = -\zeta_m$, we can conclude the proof. □

Remark 2. Now we discuss an important subfield of $\mathbb{Q}(\zeta_n)$ for $n \geq 3$. In particular, we consider $\mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Notice that $\zeta_n + \zeta_n^{-1}$ is real. Then one can show that $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. This is the maximal real subfield of $\mathbb{Q}(\zeta_n)$ and is denoted by $\mathbb{Q}(\zeta_n)^+$. It is important to point out that the extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is of degree 2 since ζ_n is a root of $X^2 - (\zeta_n + \zeta_n^{-1})X + 1$. More in general, if K is a number field we denote by K^+ its maximal real subfield.

Lemma 1.1.8. *Let $n = p^m$ and consider the extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n)^+$. This is ramified at a finite prime $\mathfrak{p}$ if and only if $\mathfrak{p}$ lies above p.*

Proof. Keep on mind that by lemma 1.1.3 we know that p is totally ramified in $\mathbb{Q}(\zeta_n)$. Moreover, by fact number 4 at the beginning of the chapter, we know that p is the only prime number that ramifies in $\mathbb{Q}(\zeta_n)$.
Now let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_n)^+$ that ramifies. Say that $\mathfrak{q}$ is a prime of $\mathbb{Q}(\zeta_n)$ that lies above $\mathfrak{p}$ and that appears in its factorization with exponent $e \geq 2$. Say $q = \mathfrak{p} \cap \mathbb{Z}$ is the prime of $\mathbb{Z}$ under $\mathfrak{p}$. Then q lies also under $\mathfrak{q}$ and so it ramifies in $\mathbb{Q}(\zeta_n)$. This implies $q = p$.
On the other hand, if $\mathfrak{p}$ is a prime of $\mathbb{Q}(\zeta_n)^+$ that lies above p then $(1 - \zeta_n)\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ is necessarily the only prime ideal above $\mathfrak{p}$. Using that p is totally ramified, the previous remark and the known formulas for the degrees, one finds that the ramification index of $(1 - \zeta_n)\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ at $\mathfrak{p}$ is equal to 2. This implies the statement. □

Remark 3. Consider again $n = p^m$ and the extension $\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n)^+$. Let $\pi = (1 - \zeta_n)\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ and v_π be the π-valuation. Now notice that one can give a shorter proof of the previous lemma using the ramification indices. However, we decided not to use this argument since the previous proof shows an interesting property of v_π. If J is an ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_n)^+}$ then $v_\pi(J)$ is necessarily even. To see this, is enough to consider the factorization on J and to use that a prime in its factorization has valuation equal to 2, as showed in the above proof.

We conclude this section just stating the following interesting proposition. We refer to [**Wa**] for a proof.

Proposition 1.1.9. *Let $n \in \mathbb{N}$ and $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.*

1.2 CM-fields

In this section we are going to study some properties of the CM-fields so that we can deduce some results about the ideal class group of $\mathbb{Q}(\zeta_n)$.

Definition 1.2.1. - A number field is called *totally real* if all its embeddings into $\mathbb{C}$ lie in $\mathbb{R}$. On the other hand, a number field is called *totally imaginary* if none of its embeddings lie in $\mathbb{R}$.

- A *CM-field* is a totally imaginary quadratic extension of a totally real number field.

Example 1. let $n \geq 1$. Recalling that the maximal real subfield of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, one finds that $\mathbb{Q}(\zeta_n)$ is a CM-field.

We decided to omit the proof of the following theorem since it follows applying a result of Class field theory whose proof has nothing to do with cyclotomic units. A proof can be found in [**Lan1**] or [**Wa**].

Theorem 1.2.1. *Let K be a CM-field, K^+ its maximal real subfield, and let h and h^+ be the respective class numbers. Then h^+ divides h. The ratio $h^- \overset{\text{def}}{=} \frac{h}{h^+}$ is called the relative class number.*

Theorem 1.2.2. *Let K be a CM-field and let E be its unit group. Let E^+ be the unit group of K^+ and let W be the group of roots of unity in K. Then $Q \overset{\text{def}}{=} [E : WE^+] = 1$ or 2.*

Proof. Define $\phi : E \to W$ by $\phi(\epsilon) = \epsilon/\overline{\epsilon}$. Since K is a CM-field, we have that $\overline{\epsilon^\sigma} = (\overline{\epsilon})^\sigma$ for all embeddings σ of K into $\mathbb{C}$. Hence $|\phi(\epsilon)^\sigma| = 1$ for every σ. By lemma 1.1.5, we deduce that $\phi(\epsilon) \in W$. Denote by $\psi : E \to W/W^2$ the natural map induced by ϕ. Now we want to show that $Ker(\psi) = WE^+$. Firstly, notice that $|W/W^2| = 2$ (we have just the cosets of 1 and of a suitable primitive root of unity). Thus, consider $\epsilon = \zeta\epsilon_1$ with $\zeta \in W$ and $\epsilon_1 \in E^+$. Then $\phi(\epsilon) = \zeta^2 \in W^2$ (recall that $\overline{\zeta} = \zeta^{-1}$) and so $\epsilon \in Ker(\psi)$. Conversely, suppose $\phi(\epsilon) = \zeta^2 \in W^2$. Notice that it follows that $\epsilon_1 = \zeta^{-1}\epsilon$ is real since $\epsilon/\overline{\epsilon} = \zeta^2$ implies $\epsilon_1 = \zeta^{-1}\epsilon = \zeta\overline{\epsilon}$ and so $\overline{\epsilon}_1 = \overline{\zeta\overline{\epsilon}} = \zeta^{-1}\epsilon = \epsilon_1$. Thus also the other inclusion holds and we get that $Ker(\psi) = WE^+$. Since $|W/W^2| = 2$, we can conclude. □

Remark 4. With the notation as in the previous theorem, notice that we have $Q = 2$ if $\phi(E) = W$ and $Q = 1$ if $\phi(E) = W^2$.

For completeness, we state an interesting corollary. For a proof see [**Wa**] again.

Corollary 1.2.3. *Let $K = \mathbb{Q}(\zeta_n)$. Then $Q = 1$ if n is a prime power and $Q = 2$ if n is not a prime power.*

Notation: From now on, given a number field K, we will denote by $Cl(K)$ its ideal class group.

Theorem 1.2.4. *The natural map $Cl(\mathbb{Q}(\zeta_n)^+) \to Cl(\mathbb{Q}(\zeta_n))$ is injective.*

Proof. Suppose that I is an ideal of $\mathbb{Q}(\zeta_n)^+$ such that its lift to $\mathbb{Q}(\zeta_n)$ is a principal ideal, namely I is in the kernel of the natural map. Then for proving the claim is enough to show that actually I is principal. Now let $I \cdot \mathbb{Q}(\zeta_n) = (\alpha)$ with $\alpha \in \mathbb{Q}(\zeta_n)$. Then $(\overline{\alpha}/\alpha) = (1)$ since $I \subseteq \mathbb{R}$. This implies that $\overline{\alpha}/\alpha$ is a unit. Moreover notice that it has absolute value equal to 1. By lemma 1.1.5, we obtain that $\overline{\alpha}/\alpha$ is a root of unity. Now if n is not a prime power, then $Q = 2$. Therefore by the proof of the previous theorem we have that there exists a unit ϵ of $\mathbb{Q}(\zeta_n)$ such that $\epsilon/\overline{\epsilon} = \overline{\alpha}/\alpha$. Hence $\alpha\epsilon = \overline{\alpha\epsilon}$ is real and $I \cdot \mathbb{Q}(\zeta_n) = (\alpha) = (\alpha\epsilon)$. By the unique factorization of ideals we deduce that $I = (\alpha\epsilon)$, so that I is principal in $\mathbb{Q}(\zeta_n)^+$.

Now suppose that $n = p^m$. By proposition 1.1.3 we know that $\pi \overset{\text{def}}{=} \zeta_{p^m} - 1$ is a prime element. Observe that we have $\pi/\overline{\pi} = -\zeta_{p^m}$, which generates the roots of unity in $\mathbb{Q}(\zeta_{p^m})$ by lemma. Hence, there exists $d \in \mathbb{Z}$ such that $\overline{\alpha}/\alpha = (\pi/\overline{\pi})^d$. Now consider the π-valuation ν_π. By remark 3 we know that $\nu_\pi(\mathbb{Q}(\zeta_n)^+) \subseteq 2\mathbb{Z}$ and recalling that $\alpha\pi^d$ and I is real, we get that $d = \nu_\pi(\alpha\pi^d) - \nu_\pi(\alpha) = \nu_\pi(\alpha\pi^d) - \nu_\pi(I)$ is even. This implies $\overline{\alpha}/\alpha = (-\zeta_{p^m})^d \in W^2$. It follows that $\overline{\alpha}/\alpha = \gamma/\overline{\gamma}$ for some root of unity γ and that $\alpha\gamma$ is real. Arguing as in the previous case, we deduce that $I = (\alpha\gamma)$. Hence I is actually principal and we can conclude the proof.

□

Moreover, as a consequence of a general result of Class field theory about norms map, one has the following theorem. For details about it, we refer to [**Lan1**].

Theorem 1.2.5. *Consider $Cl(\mathbb{Q}(\zeta_n))$ and let K be an imaginary abelian extension of $\mathbb{Q}$. Then the norm map*

$$N_{K|K^+} : Cl(\mathbb{Q}(\zeta_n)) \to Cl(\mathbb{Q}(\zeta_n)^+) \text{ is surjective.}$$

1.3 Cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$

Definition 1.3.1. - Let $n \not\equiv 2 \mod 4$. Define V_n as the multiplicative group generated by

$$\{\pm\zeta_n, 1 - \zeta_n^a | 1 \leq a \leq n-1\}$$

- Let E_n be the group of units of $\mathbb{Q}(\zeta_n)$ and define $C_n = E_n \cap V_n$. Then C_n is called *the group of cyclotomic units of* $\mathbb{Q}(\zeta_n)$.
- If K is an abelian number field, we define the cyclotomic units of K by letting $K \subseteq \mathbb{Q}(\zeta_n)$ with n minimal and setting $C_K \overset{\text{def}}{=} E_K \cap C_n$ where E_K is the group of units of K (notice that this definition is suitable for $\mathbb{Q}(\zeta_n)^+$).

Lemma 1.3.1. *Let p be a prime and $m \geq 1$.*

1. *The cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$ are generated by -1 and the units:*

$$\xi_a = \zeta_{p^m}^{(1-a)/2} \frac{1 - \zeta_{p^m}^a}{1 - \zeta_{p^m}}$$

with $1 < a < \frac{p^m}{2}$ and $(a, p) = 1$.

2. *The cyclotomic units of $\mathbb{Q}(\zeta_{p^m})$ are generated by ζ_{p^m} and the cyclotomic units of $\mathbb{Q}(\zeta_{p^m})^+$.*

Proof. For simplicity about the notation, write $\zeta = \zeta_{p^m}$. Recall that the definition of the cyclotomic units involves $1 - \zeta^a$ with $a \not\equiv 0 \mod p^m$. Now let $k < m$ and $(b, p) = 1$. Then using the relation $1 - X^{pk} = \prod_{j=0}^{p^k-1}(1 - \zeta^{jp^{m-k}}X)$, we get that

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

Since $(p, b + jp^{m-k}) = 1$, we can deduce that it is enough to consider those a with $(a, p) = 1$. Moreover, $1 - \zeta^a$ and $1 - \zeta^{-a}$ differ only by the factor $-\zeta^a$, so similarly we can consider only those a with $1 \leq a < \frac{p^m}{2}$. Suppose now that

$$\xi \overset{\text{def}}{=} \pm\zeta^d \prod_{\substack{1 \leq a < \frac{p^m}{2} \\ (a,p)=1}} (1 - \zeta^a)^{c_a}$$

with d, $c_a \in \mathbb{Z}$ for all a, is a unit of $\mathbb{Q}(\zeta)$. Since by lemma 1.1.1 the ideals $(1 - \zeta^a)$ are all the same, it follows that $\sum_a c_a = 0$. Therefore

$$\xi = \pm\zeta^d \prod_{\substack{1 \leq a < \frac{p^m}{2} \\ (a,p)=1}} \left(\frac{1 - \zeta^a}{1 - \zeta}\right)^{c_a} = \pm\zeta^e \prod_{\substack{1 < a < \frac{p^m}{2} \\ (a,p)=1}} \xi_a^{c_a}$$

where $e \overset{\text{def}}{=} d + \frac{1}{2}\sum_{1 \leq a < \frac{p^m}{2}, (a,p)=1} c_a(a - 1)$. If $\xi \in \mathbb{Q}(\zeta)^+$ then since each factor in the above product is real, $\pm\zeta^e$ must be real, hence equal to ±1. This proves 1. Now if $p = 2$ then $(a, p) = 1$ implies that a is odd, so that ζ^e is in $\mathbb{Q}(\zeta)$ in all cases. This completes the proof of 2. □

For completeness we give the following statement. The proof involves the theory of regulators, and so we decided not to give the details. If one is interested, we suggest to look at [**Wa**], again.

Theorem 1.3.2. *Let p be a prime and $m \geq 1$. The cyclotomic units $C^+_{p^m}$ of $\mathbb{Q}(\zeta_{p^m})^+$ are of finite index in the full unit group $E^+_{p^m}$, then*

$$h^+_{p^m} = [E^+_{p^m} : C^+_{p^m}]$$

where $h^+_{p^m}$ is the class number of $\mathbb{Q}(\zeta_{p^m})^+$.

We conclude the section with a proposition that provide us a particular cyclotomic unit that will be used in the proof of The Iwasawa Main conjecture.

Proposition 1.3.3. *Let g be a primitive root modulo p^n. Then*

$$\zeta_{p^n}^{(1-g)/2}\frac{1 - \zeta_{p^n}^g}{1 - \zeta_{p^n}}$$

generates $C^+_{p^n}/\{\pm1\}$ as a module over $\mathbb{Z}[Gal(\mathbb{Q}(\zeta_{p^n})^+|\mathbb{Q})]$.

Proof. For simplicity of the notation, write $\zeta = \zeta_{p^n}$. Let $(a, p) = 1$. Then $a \equiv g^r \mod p^n$ for some $r > 0$ by definition of primitive root. Hence

$$\zeta^{(1-a)/2}.\frac{1 - \zeta^a}{1 - \zeta} = \zeta^{(1-g^r)/2}.\frac{1 - \zeta^{g^r}}{1 - \zeta} = \prod_{i=0}^{r-1} \zeta^{(g^i - g^{(i+1)})/2}.\frac{1 - \zeta^{g^{i+1}}}{1 - \zeta^{g^i}} = \prod_{i=0}^{r-1} \left(\zeta^{(1-g)/2}.\frac{1 - \zeta^g}{1 - \zeta}\right)^{\sigma_g^i}$$

Then we can conclude the proof using lemma 1.3.1. □

Chapter 2

Characters and L-functions

The aim of this chapter is to give the analytic background for studying The Iwasawa Main Conjecture. We start discussing Dirichlet characters, and then we pass to the classical L-functions and to their analogous for the p-adic setting.

2.1 Dirichlet characters

Definition 2.1.1. Let $n \geq 1$. A *Dirichlet character modulo* n is a multiplicative homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. When it will be clear from the context we will say only "character" to indicate a Dirichlet character.

Remark 5. Notice that if $n|m$ then a Dirichlet character $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ induces a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ by composition with the natural map $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. In this way, one can regard χ as being defined modulo m or modulo n. This leads us to the following

Definition 2.1.2. Let the notation be as in the above remark. If n is minimal, then it is called *the conductor of* χ and it is denoted by f_χ. When a Dirichlet character is defined modulo its conductor then it is called *primitive*.

Remark 6. - Notice that $1 = \chi(1) = \chi((-1) \cdot (-1)) = \chi(-1)^2$. This implies that $\chi(-1) = \pm 1$.

- Recall that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$ where ϕ is the Euler function. Thus for every $a \mod n \in (\mathbb{Z}/n\mathbb{Z})^\times$ we have $1 = \chi(1) = \chi(a^{\phi(n)} \mod n) = \chi(a \mod n)^{\phi(n)}$. This means that the image of χ is contained in the set of the $\phi(n)$-th root of unity.
- It is common to extend a Dirichlet character χ to a map $\widetilde{\chi} : \mathbb{Z} \to \mathbb{C}$ in the following way: we set $\widetilde{\chi}(a) = 0$ if $(a, f_\chi) \neq 1$, otherwise we set $\widetilde{\chi}(a) = \chi(a \mod n)$. When it will be clear on the context, we will write just χ instead of $\widetilde{\chi}$.

Definition 2.1.3. A Dirichlet character such that $\chi(-1) = 1$ is said to be *even*; if $\chi(-1) = -1$ then χ is said to be *odd*.

Remark 7. Here are some useful properties about Dirichlet characters:

- Let χ be any character modulo n and let $\psi = \overline{\chi}$ where the bar indicates the complex conjugation. Then $\psi(a \mod n) = \chi(a \mod n)^{-1}$. It follows that $\chi\overline{\chi}(a$

mod n) = 1 for every a coprime with n. Thus the set of characters of conductor n is actually a multiplicative group with multiplication defined pointwise. The identity element is called *the trivial character* and clearly it is the character that maps everything to 1. By convention, we say that the trivial character has conductor 1.

- If $(f_\chi, f_\psi) = 1$ then $f_{\chi\psi} = f_\chi f_\psi$.

For our purposes will be useful to be able to define a product of primitive characters with different conductors. We give the following:

Definition 2.1.4. Let χ and ψ be primitive Dirichlet characters of conductors respectively f_χ and f_ψ. We define the product $\chi\psi$ as follows. Consider the homomorphism

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

defined by $\gamma(a) = \chi(a)\psi(a)$. Then $\chi\psi$ is the primitive character associated to γ.

Now we are going to generalize the notion of characters.

Definition 2.1.5. Let G be a finite abelian group and let $\widehat{G}$ be the group of the multiplicative homomorphisms from G to $\mathbb{C}^\times$ (the group law is the pointwise multiplication). We call it the group of the Dirichlet characters of G.

Proposition 2.1.1. *Let G be a finite cyclic group of size n with a fixed generator γ. Then there are exactly n characters of G.*

Proof. First of all notice that since γ generates G then the values of a character χ are determined by its value on γ. By the above remark, we know that $\chi(\gamma)$ is an n-th root of unity. Hence there are at most n characters. Now we show that there are at least n characters, so that the statement holds. Let $\zeta_1, ..., \zeta_n$ be all the n-th roots of unity and for every i define $\chi_i(\gamma) = \zeta_i$. We have that $\chi_1, ..., \chi_n$ are characters and they are all distinct since they have different values on the generator γ. This concludes the proof.

□

Even if the next result is important, its proof requires some space and so we decided to omit it. The interested reader can find a proof in [**Con1**].

Lemma 2.1.2. *Let G be a finite abelian group and let H be a subgroup of G. Then any character of H can be extended to a character of G in $[G : H]$ ways.*

Lemma 2.1.3. *Let G be a finite abelian group and let $g \in G$ a non-trivial element. Then $\chi(g) \neq 1$ for some character χ of G. Moreover we have $|G| = \widehat{G}$.*

Proof. Consider the cyclic group $\langle g \rangle$ and say that $|\langle g \rangle| = m$. Since $\langle g \rangle$ is non-trivial then $m > 1$. Now also the group of the m-th roots of unity μ_m is cyclic and has cardinality equal to m. Therefore we have $\langle g \rangle \simeq \mu_m$. Notice that this isomorphism gives us a character χ of the group $\langle g \rangle$ such that $\chi(g) \neq 1$. By lemma 2.1.2, we have that χ extends to at least one character $\widetilde{\chi}$ of G. This proves the first part of the lemma. For the second part, call $H = \{1_G\}$ and $\widehat{H} = \{\psi\}$. Now we apply lemma 2.1.2 to H. In this way, we find that ψ extends to $|G|$ distinct elements of $|\widehat{G}|$ and so $|G| \leq |\widehat{G}|$. On the other hand, an element of $\widehat{G}$ when restricted becomes a character of H and so it must be one of the extensions of ψ. This proves that $|\widehat{G}| \leq |G|$ and concludes the proof.

□

Lemma 2.1.4. *If G is a finite cyclic group then $G \simeq \widehat{G}$.*

Proof. We have to show only that also $\widehat{G}$ is a cyclic group. This will imply the statement since by lemma 2.1.3 we have $|\widehat{G}| = |G|$. Let $|G| = n$ and let γ be a generator of G. Now choose ζ a primitive n-th root of unity and define $\chi \in \widehat{G}$ by $\chi(\gamma) = \zeta$. Notice that if ψ is another element of $\widehat{G}$ then $\psi(\gamma) = \zeta^k$ for some integer k. Hence $\psi = \chi^k$ and this proves that χ generates $\widehat{G}$.

□

Proposition 2.1.5. *If G_1 and G_2 are finite abelian groups then $\widehat{G_1 \times G_2} \simeq \widehat{G}_1 \times \widehat{G}_2$.*

Proof. Let χ be a character of $G_1 \times G_2$. Let χ_{G_1} and χ_{G_2} be the restrictions of χ to G_1 and G_2 respectively, i.e. $\chi_{G_1}(g) = \chi(g,1)$ and $\chi_{G_2}(h) = \chi(1,h)$. Then χ_{G_1} and χ_{G_2} are characters of G_1 and G_2 respectively and $\chi(g,h) = \chi((g,1)(1,h)) = \chi(g,1)\chi(1,h) = \chi_{G_1}(g)\chi_{G_2}(h)$. Hence we get a map

$$\begin{aligned} \phi : \widehat{G_1 \times G_2} &\to \widehat{G}_1 \times \widehat{G}_2, \\ \chi &\mapsto (\chi_{G_1}, \chi_{G_2}) \end{aligned}$$

Notice that ϕ is a group homomorphism and moreover its kernel is trivial since if χ is in the kernel then χ_{G_1} and χ_{G_2} are trivial characters and so $\chi(g,h) = \chi_{G_1}(g)\chi_{G_2}(h) = 1$, i.e. also χ is trivial. By lemma 2.1.3 the domain and codomain of ϕ have same cardinality and so we conclude the proof.

□

Lemma 2.1.6. *If G is a finite abelian group, then $G \simeq \widehat{G}$ (non-canonically).*

Proof. By hypothesis G is isomorphic to the direct product of several finite cyclic groups, say $G \simeq H_1 \times ... \times H_t$ with H_i finite cyclic for every i. As a consequence of the previous lemma, we have that $(\widehat{H_1 \times ... \times H_t}) \simeq \widehat{H}_1 \times ... \times \widehat{H}_t$. However H_i is finite and cyclic for every i and so $\widehat{H}_i \simeq H_i$. This proves that $\widehat{G} \simeq (\widehat{H_1 \times ... \times H_t}) \simeq H_1 \times ... \times H_t \simeq G$ and so we are done.

□

Corollary 2.1.7. *We have $\widehat{\widehat{G}} \simeq G$ (canonically).*

Proof. Let $g \in G$ and define $\widetilde{g} : \widehat{G} \to \mathbb{C}^\times$ by $\chi \mapsto \chi(g)$. Consider the homomorphism of groups $\phi : G \to \widehat{\widehat{G}}$ defined by $g \mapsto \widetilde{g}$. We prove that ϕ is an isomorphism. Then let $g \in Ker(\phi)$, i.e. suppose that $\chi(g) = 1$ for all $\chi \in \widehat{G}$. By lemma 2.1.3 we deduce that $g = 1$, so that ϕ is injective. Still by lemma 2.1.3 we have that $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$ and this proves the corollary.

□

Remark 8. It is usually convenient to identify $\widehat{\widehat{G}}$ with G thanks to the previous corollary. Moreover notice that we have a natural pairing

$$\begin{aligned} G \times \widehat{G} &\to \mathbb{C}^\times \\ (g, \chi) &\mapsto \chi(g) \end{aligned}$$

The interesting fact is that this pairing is non-degenerate, i.e. if $\chi(g) = 1$ for all $\chi \in \widehat{G}$ then $g = 1$ by the argument in the previous proof and if $\chi(g) = 1$ for all $g \in G$ then by definition of the trivial character we get $\chi = 1$.

Now we give a fundamental example of character that we will use heavily in the proof of the Main Conjecture. The notation that we are going to introduce will be used in the rest of the treatment.

Example 2 (**The Teichmüller character**). First of all, we review some basic facts of p-adic analysis. Recall that $(\mathbb{Q}_p, |\cdot|_p)$ is the completion of $(\mathbb{Q}, |\cdot|_p)$ where $|\cdot|_p$ is the p-adic norm. Moreover $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is a subring of $\mathbb{Q}_p$ and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Furthermore, $\mathbb{Z}_p$ is a DVR with maximal ideal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$ and so $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}$. It is known (see [**Gou**] for example) that $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$. From now on, we will identify them.
Now consider the natural surjective map $\pi : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ which induces a map $\widetilde{\pi} : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ still surjective. Consider also the equation $x^{p-1} - 1 = 0$ in $\mathbb{F}_p$. Its roots are exactly the elements of $\mathbb{F}_p^\times$ and so in particular they are simple. By the Hensel Lemma, if δ is a root then it lifts through $\widetilde{\pi}$ to a unique element β of $\mathbb{Z}_p^\times$ such that $\beta \mod p = \delta$ and $\beta^{p-1} - 1 = 0$ in $\mathbb{Z}_p$. This implies that μ_{p-1}= group of $(p-1)$-st roots of unity is isomorphic to a subgroup of $\mathbb{Z}_p^\times$. In particular one obtains a decomposition $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ where notice that $1 + p\mathbb{Z}_p = Ker(\widetilde{\pi})$ (for details about the decomposition, see [**Gou**]). Since $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, one finds that $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times = p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. Therefore, any $\alpha \in \mathbb{Q}_p^\times$ can be written uniquely as $\alpha = p^n \cdot \zeta \cdot (1 + p\beta)$ for $n \in \mathbb{Z}$, $\zeta \in \mu_{p-1}$, $\beta \in \mathbb{Z}_p$. Notice that $n = v_p(\alpha)$, $\langle \alpha \rangle = (1 + \beta)$ and denote ζ by $\omega(\alpha)$. Hence we have just defined a map

$$\omega : \mathbb{Z}_p^\times \to \mu_{p-1}, \, \alpha \mapsto \omega(\alpha)$$

The above function is called *the Teichmüller map*. From the fact that every $\alpha \in \mathbb{Z}_p^\times$ can be written in a unique way as $\omega(\alpha) \cdot (1 + p\beta)$ we also have the fundamental property that $\omega(\alpha) \equiv \alpha \mod p$.
Now notice that ω induces an isomorphism

$$\begin{aligned} (\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}_p/p\mathbb{Z}_p)^\times &\to \mu_{p-1}, \\ \alpha \mod p &\mapsto \omega(\alpha) \end{aligned}$$

Fixing once and for all embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$ and into $\mathbb{C}$ we may view μ_{p-1} contained either in $\mathbb{C}_p$ or $\mathbb{C}$ according to our needs. In particular, in this way we have just defined a Dirichlet character $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ that we will still denote by ω and that is called *the Teichmüller character*. One can show that ω is an odd character.

2.2 p-adic L-functions

In this section we firstly recall the basic notion of L-function. After that, we are going to define its analogous for the p-adic case and to study some of its properties which will be very important in what follows.

Convention: In what follows, including also the next chapters, by saying "Dirichlet character", we actually mean "primitive Dirichlet character".

Definition 2.2.1. Let χ be a Dirichlet character of conductor f. The *L-function* attached to χ is the series defined by

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

for $Re(s) > 1$.

Remark 9. - Notice that for $\chi = 1$ the L-series is nothing but the Riemann zeta function. It is well known that $L(s,\chi)$ may be continued analytically to the whole complex plane, except for a simple pole at $s = 1$ when $\chi = 1$ (see [**Fr**] for example).

- Let $\mathbb{P}$ be the set of all prime numbers. Then $L(s,\chi)$ has the following convergent "Euler" product expansion:

$$L(s,\chi) = \textstyle\prod_{q\in\mathbb{P}}(1-\chi(q)q^{-s})^{-1} = \prod_{q\nmid f}(1-\chi(q)q^{-s})^{-1}$$

with $Re(s) > 1$. For a reference, see [**Fr**] again. Notice that using the above formula is clear that $L(s,\chi) \neq 0$ for $Re(s) > 1$, since $\chi(q)q^s \neq 0$ for every prime q (see the remark on page 198 in [**Fr**]).

Definition 2.2.2. Recall that the *Bernoulli numbers* B_n are defined as those rational numbers such that

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

Remark 10. Let $\mathbb{Q}[|t|]$ be the ring of formal power series with coefficients in $\mathbb{Q}$. The previous definition makes sense since $e^t = \sum_{n=0}^{\infty} \frac{t^n}{n!}$ implies that $e^t - 1 = \sum_{n=1}^{\infty} \frac{t^n}{n!} \in \mathbb{Q}[|t|]^{\times}$. In particular we get that

$$\frac{t}{e^t-1} = \frac{1}{1+\frac{t}{2}+\frac{t^2}{3!}+\ldots} = \left(\sum_{n=0}^{\infty}\frac{t^n}{(n+1)!}\right)^{-1} \in \mathbb{Q}[|t|]^{\times}$$

Definition 2.2.3. Let χ be a Dirichlet character of conductor f as before and denote by $\mathbb{Q}(\chi)$ the field generated over $\mathbb{Q}$ by $\chi(a)$ with $a \in \mathbb{Z}$. The *generalized Bernoulli numbers* $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!} \in \mathbb{Q}(\chi)[|t|]$$

Remark 11. - Also this definition makes sense since arguing as above we get $e^{ft} - 1 \in \mathbb{Q}(\chi)[[t]]^{\times}$.

- Notice that we always have $\chi(f) = 0$ unless χ is the trivial character. If this is the case, we have $f = 1$.

- When $\chi = 1$ we obtain

$$\sum_{n=0}^{\infty} B_{n,1}\frac{t^n}{n!} = \frac{te^t}{e^t-1} = \frac{t}{e^t-1} + t$$

so that $B_{n,1} = B_n$ except for $n = 1$ when we have $B_{1,1} = \frac{1}{2}, B_1 = -\frac{1}{2}$. Observe also that if $\chi \neq 1$ then $B_{0,\chi} = 0$ since $\sum_{a=1}^{f} \chi(a) = 0$.

Definition 2.2.4. We define the Bernoulli polynomials $B_n(X)$ as those polynomials such that

$$\frac{te^{Xt}}{e^t-1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}$$

Remark 12. - By a direct computation one finds that $B_n(1-X) = (-1)^n B_n(X)$.

- Since the generating function is the product of $\frac{t}{e^t-1} = \sum B_n \frac{t^n}{n!}$ and $e^{Xt} = \sum X^n \frac{t^n}{n!}$ it follows that $B_n(X) = \sum_{i=0}^{n} \binom{n}{i}(B_i)X^{n-i}$.

Proposition 2.2.1. *Let F be any multiple of f. Then*

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

Proof. Notice that

$$\sum_{n=0}^{\infty}[F^{n-1}\frac{t^n}{n!}\sum_{a=1}^{F}\chi(a)B_n(\frac{a}{F})] = \sum_{a=1}^{F}\chi(a)\frac{te^{(a/F)Ft}}{e^{Ft}-1} \overset{\text{def}}{=} (\star)$$

since

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

by definition of Bernoulli polynomials.
Let $g = F/f$ and $a = b + cf$. Then we have:

$$\begin{aligned}(\star) = \sum_{b+cf=1}^{gf}\chi(b+cf)\frac{te^{(\frac{b+cf}{gf})gft}}{e^{gft}-1} &= \sum_{b=1}^{f}[\sum_{c=0}^{g-1}\chi(b)\frac{te^{(b+cf)t}}{e^{fgt}-1}] = \sum_{b=1}^{f}[\chi(b)\frac{te^{bt}}{e^{fgt}-1}\sum_{c=0}^{g-1}e^{cft}] = \\ &= \sum_{b=1}^{f}[\chi(b)\frac{te^{bt}}{e^{fgt}-1}\cdot\frac{e^{fgt}-1}{e^{ft}-1}] = \sum_{b=1}^{f}\chi(b)\frac{te^{bt}}{e^{ft}-1} = \\ &= \sum_{n=0}^{\infty}B_{n,\chi}\frac{t^n}{n!}\end{aligned}$$

and so looking at the definition of $(\star)$ and at the last expression that we obtained, we can conclude the proof.

□

Definition 2.2.5. For a complex variable s with $Re(s) > 1$ and for a real number b with $0 < b \leq 1$ we define the *Hurwitz zeta function*

$$\zeta(s,b) = \sum_{n=0}^{\infty} \frac{1}{(b+n)^s}$$

Now let

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

where a and F are integers with $0 < a < F$. Then

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

where $n \geq 1$. Hence H has a simple pole at $s = 1$ with residue $1/F$.

Definition 2.2.6. Let $\mathbb{C}_p$ be the completion of $(\overline{\mathbb{Q}}_p, |\cdot|_p)$ and consider $B(r) = \{s \in \mathbb{C}_p : |s| \leq 1\}$. A function $f : B(r) \to \mathbb{C}_p$ is said to be *p-adic analytic on $B(r)$* if f is represented by a power series $\sum_{n=0}^{\infty} a_n s^n$ with $a_n \in \mathbb{C}_p$ converging on $B(r)$.

Definition 2.2.7. Let $B(r)$ as above. A function $g : B(r) \to \mathbb{C}_p$ is said to be *p-adic analytic on $B(r)$ except for a simple pole with residue ρ at $s_0 \in B(r)$* if

1. $(s-s_0)g(s)$ is p-adic analytic on $B(r)$;
2. $\lim_{s\to s_0} g(s) = \rho$.

Definition 2.2.8. For every $n \in \mathbb{N}_{>0}$ let $\mathbb{Q}[X]_n$ be the set of all polynomials of $\mathbb{Q}[X]$ of degree n. Define

$$\binom{X}{n} = \frac{X(X-1)\cdot\ldots\cdot(X-n+1)}{n!} \in \mathbb{Q}[X]_n$$

If $n = 0$, we set $\binom{X}{0} = 1$.

Remark 13. We indicate always by $\binom{X}{n}$ the following function on $\mathbb{N}$ associated to $\binom{X}{n}$: for $m, n \in \mathbb{N}$ if $m \geq n$ we set $\binom{X}{n}(m) = \binom{m}{n}$ while if $m < n$ we put $\binom{X}{n}(m) = 0$. Hence $\binom{X}{n}$ take values in $\mathbb{N} \cup \{0\}$. Since $\mathbb{N}$ is dense in $\mathbb{Z}_p$ and $\binom{X}{n}$ is p-adically continuous we obtain that $\binom{X}{n}$ extends uniquely to a function $\binom{X}{n} : \mathbb{Z}_p \to \mathbb{Z}_p$ (see [**Gou**] for more details about this).

Notation: From now on, we will write $|\cdot|$ to indicate the p-adic norm $|\cdot|_p$. Moreover, p will always be an odd prime.

Lemma 2.2.2. *The expression $f(X) = \sum_{n=0}^{\infty} a_n\binom{X}{n}$ for $a_n \in \mathbb{Q}_p$ such that $a_n \to 0$ p-adically defines a continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$.*

Sketch of proof. Clearly we have pointwise convergence. Indeed: $|a_n\binom{x}{n}| = |a_n| \cdot |\binom{x}{n}| \leq |a_n|$ since $|\binom{x}{n}| \leq 1$. However one can deduce that the same estimate shows the uniform convergence. Hence the p-adically continuos function $\sum_{k=1}^{n} a_k\binom{X}{k}$ converges (as $n \to \infty$) to a p-adically continuous function as in the statement. □

Remark 14. Notice that if $a_n \in \mathbb{Z}_p$ for every n then $f : \mathbb{Z}_p \to \mathbb{Z}_p$.

Proposition 2.2.3. *Suppose $r < p^{-1/(p-1)} < 1$ and*

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n}$$

with $|a_n| \leq Mr^n$ for some M. Then $f(X)$ may be expressed as a power series with radius of convergence at least $r = (rp^{1/(p-1)})^{-1} > 1$.

Proof. First of all recall that $f(X)$ is continuos on $\mathbb{Z}_p$ since $a_n \to 0$ as $n \to \infty$. For every $k \in \mathbb{N}_{>0}$ define $P_k(X) = \sum_{n \leq k} a_n \binom{X}{n} = \sum_{n \leq k} a_{n,k} X^n$. Then

$$a_{n,k} = a_n \frac{integer}{n!} + a_{n+1} \frac{integer}{(n+1)!} + \ldots + a_k \frac{integer}{k!}$$

and so

$$|a_{n,k}| \leq max_{n \leq j \leq k} \{ \left| \frac{a_j \cdot (integer)}{j!} \right| \} \leq max_{n \leq j \leq k} \left| \frac{a_j}{j!} \right|$$

Now since $\frac{1}{j!} < p^{\frac{j}{p-1}}$ we have that $|\frac{a_j}{j!}| < M(rp^{\frac{1}{p-1}})^j = MR^{-j}$. Hence $|a_{n,k}| < MR^{-n}$. Moreover, the same computation shows that

$$|a_{n,k} - a_{n,k+h}| = \left| a_{k+1} \frac{integer}{(k+1)!} + \ldots + a_{k+h} \frac{integer}{(k+h)!} \right| \leq MR^{-(k+1)} \to 0 \text{ as } k \to \infty$$

Therefore $\{a_{n,k}\}_{k=1}^{\infty}$ is a Cauchy sequence. Let $a_{n,\infty} = \lim_{k \to \infty} a_{n,k}$. Then $|a_{n,\infty}| \leq MR^{-n}$. Define $P_\infty(X) = \sum_{n=0}^{\infty} a_{n,\infty} X^n$. Hence P_∞ converges in $D = \{x \in \mathbb{C}_p : |x| < R\}$. Of course also the polynomials $P_1, P_2, \ldots$ converge in D. Finally, if $x \in D$ then

$$|\sum_{n \leq n_0} a_{n,k} x^n| \leq max_{n \leq n_0} \{MR^{-n}|x|^n\} \to 0 \text{ as } n_0 \to \infty, \text{ uniformly in } k$$

Thus $f(x) = \lim_{k \to \infty} P_k(x) = P_\infty(x)$ and so f is analytic in D as we wanted.

□

Theorem 2.2.4 (Von Staudt-Clausen)**.** *Let n be even and positive. Then*

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

Proof. We want to show that for each prime p we have $B_n = -1/p$ or 0 modulo $\mathbb{Z}_p$, depending on wether $p-1$ does or does not divide n. We proceed by induction. Thus assume that the statement holds for $m < n$. It follows that $pB_m \in \mathbb{Z}_p$ for $m < n$. Notice that the claim is clearly true for $m = 0, 1$ and so we can assume that $n \geq 2$ is even. By remark 12 and proposition 2.2.1 we get that

$$B_n = B_{n,1} = p^{n-1} \sum_{a=1}^{p} B_n(\frac{a}{p}) = p^{n-1} \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} (B_j) \left(\frac{a}{p}\right)^{n-j} =$$

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

$$\equiv \sum_{a=1}^{p} (pB_0 a^n p^{-2} + npB_1 a^{n-1} p^{-1} + pB_n p^{n-2}) \mod \mathbb{Z}_p$$

Now notice that if $p \neq 2$, then $B_1 = -\frac{1}{2} \in \mathbb{Z}_p$. Moreover, being n even, we also have that $nB_1 \in \mathbb{Z}_2$. Therefore we may omit the term with B_1 in the above congruence. Recalling that $B_0 = 1$ and looking respectively at the first and last terms of the above expression, we obtain:

$$(1 - p^n)B_n \equiv \tfrac{1}{p}\textstyle\sum_{a=1}^{p} a^n \equiv \tfrac{p-1}{p} \text{ if } (p-1)|n \text{ or } \equiv 0 \text{ if } (p-1) \nmid n.$$

Since $1 - p^n \equiv 1 \mod p$, we deduce that $B_n \equiv -\frac{1}{p}$ or $\equiv 0$ modulo $\mathbb{Z}_p$. Now consider $B_n + \sum_{\substack{p \in \mathbb{P} \\ (p-1)|n}} \frac{1}{p}$. By the above line, we deduce that this is a rational number which lies in $\mathbb{Z}_p$ for every $p \in \mathbb{P}$. This implies that there are no prime numbers in its denominator and so it is actually an integer. This concludes the proof.

□

Now we state a theorem which will give us an important formula about the Hurwitz zeta function that we will use later. The proof is entirely analytical and uses a contour argument, so we decided to omit it. The interested reader can find a proof in [**Wa**].

Theorem 2.2.5 (proof omitted). *$L(1-n,\chi) = -B_{n,\chi}/n$ with $n \geq 1$. More generally, $\zeta(1-n,b) = -B_n(b)/n$ with $0 < b \leq 1$.*

Theorem 2.2.6. *Suppose that $1 \leq a \leq F$ and p is an odd prime such that $p|F$, $p \nmid a$ and ω denotes the Teichmüller character. Then there exists a p-adic analytic function $H_p(a,F,s)$ on $B(r) = \{x \in \mathbb{C}_p\}$ for $r > 1$ except for a simple pole at $s = 1$ with residue $\frac{1}{F}$ such that*

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

for all $n \geq 1$.

Proof. First of all, since p does not divide a then $a \in \mathbb{Z}_p^\times$ and $\langle a \rangle$ is defined in $1 + p\mathbb{Z}_p$. Now set

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

and assume the convergence for the moment. Then

$$\begin{aligned} H_p(1-n,a,F) &= \frac{-1}{nF}\langle a \rangle^n \sum_{j=0}^{n}\binom{n}{j}(B_j)\left(\frac{F}{a}\right)^j = \\ &= \frac{-1}{nF}\langle a \rangle^n (\frac{a}{F})^{-n} \sum_{j=0}^{n}\binom{n}{j}(B_n)\left(\frac{a}{F}\right)^{n-j} = \\ &= \frac{-F^{n-1}\omega^{-n}(a)}{n}B_n\left(\frac{a}{F}\right) = \omega^{-n}(a)H(1-n,a,F) \end{aligned}$$

where in the second equality we used the fact $a = \omega(a)\langle a \rangle$, in the third remark 12 and in the last one $H(1-n,a,F) = F^{n-1}\zeta(1-n,\frac{a}{F}) = F^{n-1}\frac{-B_n(\frac{a}{F})}{n}$ (this holds by theorem 2.2.5).

At $s = 1$, we have residue:

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

It remains to prove the convergence. We know that $\langle a\rangle^s \overset{\text{def}}{=} exp_p(s \cdot log_p\langle a\rangle)$ is analytic on $B(p^{\frac{p-2}{p-1}})$ since $exp_p(s \cdot log_p\langle a\rangle)$ converges if and only if $|s \cdot log_p\langle a\rangle| < p^{-1/(p-1)}$. Moreover notice that $|s| < r$ with $r > 1$ if and only if $|1 - s| < r$ with $r > 1$. We deduce that $\langle a\rangle^{1-s}$ converges on $B(r)$ with $r > 1$. Now we study the analiticity of $\sum_{j=0}^{\infty} \binom{1-s}{j}(B_j)(\frac{F}{a})^j$. We have that $|B_j(\frac{F}{a})^j| \leq |B_j| \cdot |F|^j$ and by theorem 2.2.4 we know that $pB_j \in \mathbb{Z}_p$. Thus $|pB_j| \leq 1$. This implies that $|B_j| \leq \frac{1}{|p|} = p$. On the other hand, by hypothesis $p|F$. Say $n = \nu_p(F) \geq 1$ where ν_p is the p-adic valuation. Hence $|F|^j = p^{-n_j} \leq p^j$. Therefore $|B_j \cdot (\frac{F}{a})^j)| \leq p \cdot p^{-j}$. Then we apply proposition 2.2.3 with $M = p$, $r = p^{-1<p^{-1/(p.1)}}$. We get that $r = p^{\frac{p-2}{p-1}} > 1$. Thus $H_p(s, a, F)$ is p-adic analytic on $B(r)$ except for a simple pole at $s = 1$ with residue $1/F$.

□

Theorem 2.2.7. *Let χ be a Dirichlet character of conductor $f \geq 1$. Then there exists a p-adic analytic function $L_p(s, \chi)$ on $B(r)$ with $r > 1$, except for a simple pole at $s = 1$ with residue $1 - \frac{1}{p}$ if $\chi = 1$ satisfying*

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

with $n \geq 1$.
Furthermore, we have the formula:

$$L_p(s, \chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1 \\ p\nmid a}}^{F}\left[\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\left(\frac{F}{a}\right)^j\right] \tag{2.1}$$

Proof. Fix F such that $f|F$ and $p|F$. In particular say $F = pt$ with $t \geq 1$. We show that the formula 2.1 gives the desired function. By the definition of $H_p(s, a, F)$ that we gave in the previous proof, we have that $L_p(\chi, s) = \sum_{a=1, p\nmid a}^{F} \chi(a)H_p(a, F, s)$. This implies that $L_p(\chi, s)$ is p-adic analytic on $B(r)$ with $r > 1$ except possibly for a simple pole at $s = 1$. Now by the previous theorem we have that, at $s = 1$, $L_p(s, \chi)$ has residue $\sum_{a=1,p\nmid a}^{F} \chi(a)\frac{1}{F}$. Suppose now $\chi = 1$. Then this sum is equal to $1 - \frac{1}{p}$. Indeed, first of all recall that by our notation on characters, we have that $f = 1$ and so $p \nmid f$. Then notice that a runs through exactly $(p - 1)t$ values such that p does not divide a. Thus the sum is clearly equal to $(p - 1)t \cdot \frac{1}{pt} = 1 - \frac{1}{p}$. Suppose then that χ is not trivial, then the same sum is equal to:

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

However the first sum is 0 since $\sum_{a=1}^{f} \chi(a) = 0$ and χ is periodic of period f. Moreover, if $p|f$ then $\chi(pb) = 0$ for all b. If p does not divide f then $f|(F/p)$, so also the second sum is always 0 by the previous argument. Hence $L_p(s, \chi)$ has no pole at $s = 1$ if χ is not trivial. If $n \geq 1$ then:

$$\begin{aligned}
L_p(1-n,\chi) &= \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)H_p(1-n,a,F) = \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)\omega^{-n}(a)H(1-n,a,F) = \\
&= \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a)\omega^{-n}(a)\left(\frac{-F^{n-1}B_n(\frac{a}{F})}{n}\right) = -\frac{1}{n}F^{n-1}\sum_{\substack{a=1\\ p\nmid a}}^{F} \chi\omega^{-n}(a)B_n\left(\frac{a}{F}\right) = \\
&= -\frac{1}{n}F^{n-1}\sum_{a=1}^{F}\chi\omega^{-n}(a)B_n\left(\frac{a}{F}\right) + \frac{1}{n}p^{n-1}\left(\frac{F}{p}\right)^{n-1}\sum_{b=1}^{F/p}\chi\omega^{-n}(pb)B_n\left(\frac{b}{F/p}\right) = \\
&\overset{\text{def}}{=} (\star)
\end{aligned}$$

where in the third equality we used the fact that if χ_1, χ_2 are two characters then $\chi_1(a)\chi_2(a) = (\chi_1\chi_2)(a)$ unless $\chi_1(a) = \chi_2(a) = 0$. Now by proposition 2.2.1 we have that the first sum is equal to $-\frac{1}{n}B_{n,\chi\omega^{-n}}$. Now if $p|f_{\chi\omega^{-n}}$ then $\chi\omega^{-n}(pb) = 0$ and so we obtain directly the formula of the statement. Otherwise $f_{\chi\omega^{-n}}$ divides F/p. Again by proposition 2.2.1 we have that the second sum is equal to $\frac{1}{n}\chi\omega^{-n}(p)p^{n-1}B_{n,\chi\omega^{-n}}$. In other words, we obtain:

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

This completes the proof.

□

Remark 15. Notice that if χ is odd then n and $\chi\omega^{-n}$ have different parities and so $B_{n,\chi\omega^{-n}} = 0$. Therefore, $L_p(s,\chi)$ is identically zero for odd χ.

Theorem 2.2.8. .

Suppose $\chi \neq 1$ and $p^2 \nmid f_\chi$. Then

$$L_p(s,\chi) = \sum_{n=0}^{\infty} a_n(s-n)^n$$

with $|a_0| \leq 1$ and with $p|a_i$ for all $i \geq 1$.

Remark 16. Notice that since $L_p(s,\chi)$ has radius of convergence greater than 1, $a_i \to 0$ as $i \to \infty$; therefore a priori we have $p|a_i$ for large i.

Proof. If χ is odd, then by remark 15 the theorem holds. Hence we may assume that χ is even by remark 15. We choose F as in the previous theorem so that $p|F$ but $p^2 \nmid F$. We need to consider formula 2.1:

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

Notice that from this formula it is clear that $L_p(s,\chi)$ may be expressed in the form $\sum_{n=0}^{\infty} a_n(s-1)^n$. Hence we need to focus our attention on the divisibility property of the coefficients stated in the theorem. Now, by our choice of F, we have that $|F| = \frac{1}{p}$. Moreover in the previous proof we observed that $|B_j \cdot (\frac{F}{a})^j| \leq \frac{1}{p^{j-1}}$. We claim that $|\frac{1}{j!}| \leq p^{\frac{j}{p-1}}$. Indeed, since there are $[\frac{j}{p^i}]$ multiples of p^i less than or equal to n, we can deduce that the exponent of p in $j!$ is

$$\left[\frac{j}{p}\right] + \left[\frac{j}{p^2}\right] + ... < \frac{j}{p-1}$$

From the above we get that:

$$\left|\frac{B_j \cdot F^{j-1}}{j! \cdot a^j}\right| \leq p^{j/(p-1)} \cdot p \cdot \frac{1}{p^{j-1}} = p^{\frac{2(p+j)-jp}{p-1}} \leq \frac{1}{p}$$

for $j \geq 3$. Therefore the coefficients in the power series expansion of

$$\frac{1}{F}\sum_{j\geq 3}\binom{1-s}{j}B_j \cdot \left(\frac{F}{a}\right)^j$$

are divisible by p. Similarly

$$\langle a\rangle^{1-s} = exp((1-s)log_p\langle a\rangle) = \textstyle\sum_{j=0}^{\infty}\frac{1}{j!}(1-s)^j(log_p\langle a\rangle)^j$$

has all coefficients in $\mathbb{Z}_p$, and moreover they are divisible by p^2 for $j \geq 2$. Indeed: we know that $p|log_p\langle a\rangle$ and so $|log_p\langle a\rangle| \leq \frac{1}{p}$. Recalling that $|\frac{1}{j!}| \leq p^{\frac{j}{p-1}}$ we obtain that $|\frac{1}{j!}log_p\langle a\rangle| \leq p^{2j-jp} \leq \frac{1}{p^2}$ for $j \geq 2$. Therefore it remains to consider

$$\frac{1}{s-1}\sum_{a=1,p\nmid a}^{F}\chi(a)(1+(1-s)log_p\langle a\rangle)\Big(\frac{1}{F} - \frac{1-s}{2a} + \frac{(1-s)(1-s-1)F}{12a^2}\Big)$$

From this expression we deduce that

$$a_0 \equiv -\sum_{a=1,p\nmid a}^{F}\chi(a)\Big(\frac{1}{F}\cdot log_p\langle a\rangle - \frac{1}{2a} - \frac{F}{12a^2}\Big) \mod p$$

Clearly $(1/F)log_p\langle a\rangle$ and $F/12$ are in $\mathbb{Z}_p$. Since $a \equiv \omega(a) \mod p$ and $p|F$, we get:

$$\sum_{a=1,p\nmid a}^{F}\chi(a)\frac{1}{a} \equiv \sum_{a=1,p\nmid a}^{F}\chi\omega^{-1}(a) \equiv 0 \mod p$$

This implies that $|a_0| \leq 1$ (use also the fact that every root of unity has norm equal to 1).
Next, we observe that

$$a_1 \equiv -\sum_{p\nmid a}\chi(a)\Big(\frac{F}{12a^2} - \frac{log_p\langle a\rangle}{2a} - \frac{F\cdot log_p\langle a\rangle}{12a^2}\Big) \mod p$$

It is also clear that $F\cdot log_p\langle a\rangle/(12a^2)$ and $log_p\langle a\rangle/(2a)$ are divisible by p. If $p \geq 5$ then $F/12 \in p\mathbb{Z}_p$, so $p|a_1$. Now if $p = 3$, we have $F/12 \in \mathbb{Z}_p^\times$. However, if $p \nmid a$ then

$a^2 \equiv 1 \mod p$ and so $\sum_{p\nmid a} \chi(a)a^{-2} \equiv \sum_{p\nmid a} \chi(a) \equiv 0$. Again we obtain $p|a_1$. Finally, we have

$$a_2 \equiv -\sum_{p\nmid a} (log_p\langle a\rangle)\frac{F}{12a^2} \equiv 0 \mod p$$

Since we showed at the beginning of the proof that all the coefficients a_n with $n \geq 3$ are divisible by p, the theorem is proved.

□

Remark 17. It is important to point out that one can prove that as a p-adic analytic function on $B(r)$ (with a simple pole if $\chi = 1$) $L_p(s, \chi)$ is uniquely characterized by theorems 2.2.7 and 2.2.8. This fact will be used later. For the details about it, see [**Iw**].

We conclude the section with a useful lemma whose proof involve the theory of p-adic regulators. Details can be found in [**Wa**].

Lemma 2.2.9. *Let $\chi \neq 1$ be an even Dirichlet character. Then $L_p(1, \chi) \neq 0$.*

Chapter 3

Iwasawa Algebra and Λ-modules

The aim of this chapter is to introduce and study the Iwasawa Algebra Λ. We start with group rings and then we pass to define Λ and to prove the Structure theorem for finitely generated Λ-modules. We will conclude the chapter applying what we will have learnt to find a new way to construct p-adic L-functions. All of this plays a key role for The Iwasawa Main Conjecture.

3.1 Group rings

We start this section with recalling some facts on topological groups.

Definition 3.1.1. A *topological group* is a triple $(G, \tau, \cdot)$ where (G, τ) is a topological space and $(G, \cdot)$ is a group such that the maps $(\cdot) : G \times G \to G$, $(x, y) \mapsto xy$ and $(-1) : G \to G$, $x \mapsto x^{-1}$ are continuous with respect to τ and the product topology $\tau \times \tau$.

The following are basic properties that follow directly from the definition of topological group.

Proposition 3.1.1. *Let $(G, \tau, \cdot)$ be a topological group. Then*

1. *If H is a subgroup of G which is open (respectively closed of finite index) then H is closed (resp. open).*

2. *If (G, τ) is compact and H is an open subgroup of G, then $[G : H] < \infty$.*

Proof.

1. Denote by T a set of representatives for the right cosets of H in G. Thus we have that $G = \bigcup_{x \in T} Hx$. This implies that $H = G \setminus \bigcup_{1 \neq x \in T} Hx$. Notice that for each $g \in G$ the map $z \mapsto zg$ from G to G is an homeomorphism. We deduce that $\bigcup 1 \neq x \in THx$ is open (resp. closed). Hence we get the first statement.

2. As above, we have that $G = \bigcup_{x \in T} Hx$ where each Hx is open. Since G is compact, it follows that it is the union of finitely many cosets. This concludes the proof.

□

Definition 3.1.2. A topological space is said to be *totally disconnected* if its only connected subsets are the empty set and the one-point sets.

Definition 3.1.3. We say that a topological group $(G, \tau, \cdot)$ is a *profinite group* if and only if G is Hausdorff, compact and totally disconnected.

Example 3. The most important example of profinite group for us is the additive group of $\mathbb{Z}_p$.

Lemma 3.1.2. *Let G be a profinite group. Then*

$$G \simeq \varprojlim_N G/N$$
$$g \mapsto (g \mod N)_N$$

where N runs through the open normal subgroups of G ordered by reverse inclusion, and all the G/N's are finite groups equipped with the discrete topology.

Sketch of proof. Notice that by proposition 3.1.1 (2.) since G is compact we deduce that G/N is a finite group for every N as in the statement. Consider $\iota : G \to \varprojlim_N G/N$, $g \mapsto (g \mod N)_N$. This is a continuous map with dense image (see [**Wi**]). Now notice that $\varprojlim_N G/N$ is Hausdorff and so ι is also a closed map since G is compact. Therefore the map is surjective. However ι is injective too. Indeed, if $g \in Ker(\iota)$ then $g \in \bigcap_N N$ where N runs as in the statement. Since G is Hausdorff, we have $\bigcap_{U \in \mathcal{U}_1} U = \{1\}$ where $\mathcal{U}_1$ is the set of all the open neighborhoods of 1. Since G is compact and totally disconnected, the open normal subgroups of G form a basis of neighborhoods at 1 (see [**Wi**] again for details). Hence every U as above is the union of some N's as in the statement. This implies that $\bigcap_N N = \{1\}$. Thus we deduce that it is an isomorphism of topological groups. □

Remark 18. Actually one can prove also a converse of the previous proposition: if a group is a projective limit of finite groups, then it is a profinite group. This gives us an equivalent definition of profinite groups (look at [**Wi**] for this).

Lemma 3.1.3. *If $\{0\} \neq H$ is a closed subgroup of $\mathbb{Z}_p$ then $H = p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$.*

Proof. Let ν_p be the p-adic valuation. Choose $x \in H$ such that $n = \nu_p(x)$ is minimal. Thinking of x as a power series we deduce that we can write $x = p^n\epsilon$ with $\epsilon \in \mathbb{Z}_p^\times$. Clearly $x\mathbb{Z} \subseteq H$ but H is closed and so $x\mathbb{Z}_p \subseteq H$ because $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. However if there exists $y \in H \setminus p^n\mathbb{Z}_p$ n then $\nu_p(y) < n$, contradicting the minimality of n. Hence we deduce that $H = x\mathbb{Z}_p = p^n\mathbb{Z}_p$.

□

Definition 3.1.4. Let R be a commutative ring and let G be a finite group. We define the *group ring of G over R* as $R[G] = \{\sum_{\sigma \in G}(r_\sigma \cdot \sigma) : r_\sigma \in R\}$ where:

- $\sum_\sigma(r_\sigma \cdot \sigma) \overset{\text{def}}{=} \sum_\sigma(\gamma_\sigma \cdot \sigma)$ if and only if $r_\sigma = \gamma_\sigma$,

- $\sum_\sigma(r_\sigma \cdot \sigma) + \sum_\sigma(\gamma_\sigma \cdot \sigma) \overset{\text{def}}{=} \sum_\sigma[(r_\sigma + \gamma_\sigma) \cdot \sigma]$,

- $[\sum_\sigma(r_\sigma \cdot \sigma)] \cdot [\sum_\sigma(\gamma_\sigma \cdot \sigma)] \overset{\text{def}}{=} \sum_\sigma[(\sum_{\tau \in G} r_\tau\gamma_{\tau^{-1}\sigma}) \cdot \sigma]$

Now we are going to consider $R[G]$-modules. Of course, if G is not abelian then we have to distinguish between left and right $R[G]$-modules. Wlog, we can focus our attention on the firsts.

Examples 1. 1. $M = R$ with trivial G-action. Let $r \in M = R$. Then $(\sum_\sigma r_\sigma \cdot \sigma) \cdot r \overset{\text{def}}{=} (\sum_\sigma r_\sigma) \cdot r$.

2. The map

$$aug : R[G] \to R, \sum_\sigma (r_\sigma \cdot \sigma) \mapsto \sum_\sigma r_\sigma$$

is an $R[G]$-homomorphism and is called *the augmentation map*. The kernel of this map $Ker(aug) = \{\sum_\sigma (r_\sigma \cdot \sigma) \in R[G] : \sum_\sigma r_\sigma = 0\}$ is clearly $R[G]$-submodule and is called the *augmentation ideal*.

3. If M_1 and M_2 are $R[G]$-modules, so are

- $Hom_R(M_1, M_2)$ via $(\sigma \cdot \phi) : M_1 \to M_2, m_1 \mapsto \sigma\phi(\sigma^{-1} m_1)$ with $\phi \in Hom_R(M_1, M_2)$, $\sigma \in G$.
- $M_1 \otimes_R M_2$ via $\sigma \cdot (m_1 \otimes m_2) \overset{\text{def}}{=} \sigma m_1 \otimes \sigma m_2$.

4. Let $L|K$ be a finite Galois extension and let $G = Gal(L|K)$. Then:

- L is a $K[G]$-module: let $\sum_\sigma (r_\sigma \cdot \sigma) \in K[G]$ and $y \in L$; set $[\sum_\sigma (r_\sigma \cdot \sigma)] \cdot y \overset{\text{def}}{=} \sum_\sigma (r_\sigma \cdot \sigma(y))$
- $L^\times$ is a $\mathbb{Z}[G]$-module: let $\sum_\sigma z_\sigma \sigma \in \mathbb{Z}[G]$ and let $y \in L^\times$; set $\sum_\sigma (z_\sigma \cdot \sigma) \cdot y \overset{\text{def}}{=} \prod_\sigma \sigma(y)^{z_\sigma} \in L^\times$
- Suppose $L|K$ are number fields, then $Cl(L)$ is a $\mathbb{Z}[G]$-module: let $\sum_\sigma (z_\sigma \cdot \sigma) \in \mathbb{Z}[G]$ and let $[\mathcal{I}] \in Cl(L)$ with $\mathcal{I}$ a fractional ideal of $\mathcal{O}_L$; set $[\sum_\sigma (z_\sigma \cdot \sigma)] \cdot [\mathcal{I}] \overset{\text{def}}{=} \prod_{\sigma \in G} [\sigma(\mathcal{I})]^{z_\sigma} \in Cl(L)$

3.2 The Iwasawa Algebra

Notation: From now on, let G be a profinite group and let $\mathcal{O}$ be a commutative noetherian local ring with finite residue field of characteristic p. We call $\mathfrak{p}$ its maximal ideal. We assume also that $\mathcal{O}$ is complete in its $\mathfrak{p}$-adic topology.

Example 4. The most important situations that one has to keep on mind are when $\mathcal{O} = \mathbb{Z}_p$ or more in general $\mathcal{O} = \mathcal{O}_F$ with $F|\mathbb{Q}_p$ a finite extension.

Definition 3.2.1. - *The complete group algebra of G over $\mathcal{O}$ is the inverse limit $\mathcal{O}[|G|] \overset{\text{def}}{=} \varprojlim_N \mathcal{O}[G/N]$ where N runs through the open normal subgroups of G ordered by reverse inclusion.*

- Let Γ be a multiplicative topological group isomorphic to $(\mathbb{Z}_p, +)$. We call $\Lambda \overset{\text{def}}{=} \mathbb{Z}_p[|\Gamma|]$ *the Iwasawa Algebra.*

- The surjective augmentation map $\mathcal{O}[G/N] \twoheadrightarrow \mathcal{O}$ with N as above induces a surjective map $\mathcal{O}[|G|] \twoheadrightarrow \mathcal{O}$ which is still called the *augmentation map*. Its kernel is denoted by $\Delta(G)$ or $\Delta_{\mathcal{O}}(G)$ and its called again the *augmentation ideal.*

Example 5. Considering the second definition above, one can take into account $1 + p\mathbb{Z}_p$. This is clearly a multiplicative group and one can show that it is isomorphic to the additive group $(\mathbb{Z}_p, +)$. See [**Sa3**] for more details about this.

Now we fix Γ a generic multiplicative topological group isomorphic to $(\mathbb{Z}_p, +)$ and we also choose $\gamma \in \Gamma$ a topological generator (e.g. γ may corresponds to 1 through the chosen isomorphism, since $1\mathbb{Z} = \mathbb{Z}$ and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$). For $n \in \mathbb{N}$ we set $\Gamma_n \overset{\text{def}}{=} \Gamma/\Gamma^{p^n} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$. Observe that this is a cyclic group of order p^n and that we have natural maps $\Gamma_n \to \Gamma_m$ if $m \leq n$. Moreover, notice that $\mathcal{O}[\Gamma_n] \simeq \mathcal{O}[T]/\omega_n(T)$ as rings through the map

$$\gamma \mod \Gamma^{p^n} \mapsto (1 + T) \mod \omega_n(T)$$

where $\omega_n(T) \overset{\text{def}}{=} P_n \overset{\text{def}}{=} (1+T)^{p^n} - 1$. Comparing the roots, we deduce that for $m \leq n$ we have $\omega_m(T)|\omega_n(T)$ and that the following diagram

$$\begin{tikzcd}
\mathcal{O}[\Gamma_n] \arrow[r, "\simeq"] \arrow[d, "\Gamma_n \to \Gamma_m"] & \mathcal{O}[T]/\omega_n(T) \arrow[d, "\omega_m|\omega_n"] \\
\mathcal{O}[\Gamma_m] \arrow[r, "\simeq"] & \mathcal{O}[T]/\omega_m(T)
\end{tikzcd}$$

commutes. Therefore $\mathcal{O}[|\Gamma|] \overset{\star}{=} \varprojlim_n \mathcal{O}[\Gamma_n] \simeq \varprojlim_n \mathcal{O}[T]/\omega_n(T)$.

Remark 19 $(\star)$. By lemma 3.1.3 we know that all non-trivial closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$. This implies that also every open subgroup has this form since we know by lemma 3.1.1 that an open subgroup is closed too. On the other hand, since multiplication by p is an homeomorphism, every subgroup $p^k\mathbb{Z}_p$ is open. This implies that the limit $\varprojlim_n \mathcal{O}[\Gamma/\Gamma^{p^n}]$ really is the complete group algebra of Γ over $\mathcal{O}$.

Lemma 3.2.1. *Let R be a commutative ring. Then $R[|T|]^\times = \{\sum_{i=0}^\infty a_i T^i : a_i \in R, a_0 \in R^\times\}$. In particular, if R is a local ring with maximal ideal $\mathfrak{q}$, also $R[|T|]$ is local and its maximal ideal is generated by T and $\mathfrak{q}$.*

Proof. Let $f = \sum_{i=0}^\infty a_i T^i, g = \sum_{i=0}^\infty b_i T^i \in R[|T|]$ and suppose $fg = \sum_{i=0}^\infty (\sum_{j=0}^i a_j b_{i-j}) T^i = 1$. Then looking at the coefficients we deduce that $a_0 b_0 = 1$ and so $a_0 \in R^\times$. On the other hand, if $a_0 \in R^\times$ then set $b_0 = a_0^{-1}$ and inductively define $b_i = -a_0^{-1}(a_1 b_{i-1} + ... + a_i b_0) \in R$. This produces an inverse element. For the rest of the statement, just notice that $R[|T|]^\times = (T, \mathfrak{q})R[|T|]$.

□

Proposition 3.2.2 (Division with remainder)**.** *Let $\mathfrak{p}$ be the maximal ideal in $\mathcal{O}$ and let $f, g \in \mathcal{O}[|T|]$ such that $f = \sum_{i=0}^\infty a_i T^i \neq 0$ and $a_0, ..., a_{n-1} \in \mathfrak{p}, a_n \notin \mathfrak{p}$ for some $n \in \mathbb{N}$. Then there exists a unique $q \in \mathcal{O}[|T|]$ and a unique $r \in \mathcal{O}[T]$ such that $r = 0$ or deg$(r) < n$ and $g = qf + r$.*

Proof. **Existence**: We define a shift-operator $\tau = \tau_n : \mathcal{O}[|T|] \to \mathcal{O}[|T|], \sum_{i=0}^\infty b_i T^i) \mapsto \sum_{i=n}^\infty b_i T^{i-n}$. This map have the following properties (that one can check directly by computations):

- τ is $\mathcal{O}$-linear

- $\tau(T^n h) = h$ for all $h \in \mathcal{O}[|T|]$

- $\tau(h) = 0$ if and only if $h \in \mathcal{O}[T]$ and $deg(h) < n$ or $h = 0$

Notice we can write $f = P + T^n U$ where $P \overset{\text{def}}{=} \sum_{i=0}^{n-1} a_i T^i$ and $U \overset{\text{def}}{=} a_n + a_{n+1}T + ... = \tau(f) \in \mathcal{O}[|T|]^\times$. Set $q \overset{\text{def}}{=} \frac{1}{U} \cdot \sum_{j=0}^{\infty}(-1)^j(\tau \circ \frac{P}{U})^j \circ \tau(g) \in \mathcal{O}[|T|]$ where for every $x \in \mathcal{O}[|T|]$ we define inductively $(\tau \circ \frac{P}{U})^j \circ x$ by $(\tau \circ \frac{P}{U}) \circ x = \tau(\frac{P}{U}x)$ and $(\tau \circ \frac{P}{U})^2 \circ x = \tau(\frac{P}{U}\tau(\frac{P}{U}x))$. Now notice that $qf = qP + T^n qU$ and so using the above properties we get $\tau(qf) = \tau(qP) + \tau(T^n qU) = \tau(qP) + qU = [(\tau \circ \frac{P}{U}) \circ \sum_{j=0}^{\infty}(-1)^j(\tau \circ \frac{P}{U})^j \circ \tau(g)] + qU = [-\sum_{j=1}^{\infty}(\tau \circ \frac{P}{U})^j \circ \tau(g)] + qU = -qU + \tau(g) + qU = \tau(g)$. Therefore, we have shown that $\tau(gf) = \tau(g)$. Then the first and the third properties above imply that $g - qf$ belongs to $\mathcal{O}[T]$ and either $deg(g - qf) < n$ or $g - qf = 0$. Setting $r \overset{\text{def}}{=} g - qf$ we can conclude this part of the proof.

Uniqueness: Suppose we can write g in two ways such as in the statement: $qf + r = g = \widetilde{q}f + \widetilde{r}$. Then $(q - \widetilde{q})f + (r - \widetilde{r}) = 0$ and so wlog we may consider $qf + r = 0$ and prove that $q = 0$ (notice that this implies $r = 0$). Let $q = \sum_{k=0}^{\infty} b_k T^k \in \mathcal{O}[|T|]$. We show that $b_k \in \mathfrak{p}^m$ for every $k, m \geq 0$. This will imply that $b_k \in \bigcap_m \mathfrak{p}^m = \{0\}$. If $m = 0$ the statement follows. Now we proceed by double induction on m and k. Assume $b_i \in \mathfrak{p}^{m-1}$ for every $i \geq 0$ and $b_i \in \mathfrak{p}^m$ for $i < k$. We compare the coefficients of T^{n+k} in $qf + r = 0$, i.e. we consider

$$(b_0 a_{n+k} + ... + b_{k-1}a_{n+1}) + b_k a_n + (b_{k+1}a_{n-1} + ... + b_{k+n}a_0) = 0$$

Since both the terms in the parenthesis lie in $\mathfrak{p}^m$ we deduce that $b_k a_n \in \mathfrak{p}^m$ and so $b_k \in \mathfrak{p}^m$ since $a_n \notin \mathfrak{p}$ by hypothesis.

□

Definition 3.2.2. An element $p(T) \in \mathcal{O}[T]$ is called distinguished or a Weierstrass polynomial if $p(T) = T^n + a_{n-1}T^{n-1} + ... + a_0$ for some $n > 0$ and $a_0, ..., a_{n-1} \in \mathfrak{p}$.

Example 6. The polynomial $\omega_n(T) = (1 + T)^{p^n} - 1 \in \mathbb{Z}_p[T]$ is distinguished.

Theorem 3.2.3 (p-adic Weierstrass Preparation theorem). *Let $0 \neq f = \sum_{i=0}^{\infty} a_i T^i \in \mathcal{O}[|T|]$ such that $a_0, ..., a_{n-1} \in \mathfrak{p}, a_n \notin \mathfrak{p}$ for some $n \in \mathbb{N}$. Then there is a unique decomposition of $f = P \cdot U$ where P is a Weierstrass polynomial of degree n and $U \in \mathcal{O}[|T|]^\times$. In particular, if $\mathcal{O}$ is a DVR with $\mathfrak{p} = (\pi)$ then every $f \neq 0$ may be uniquely written as $f = \pi^s PU$ for some $s \geq 0$.*

Proof. **Existence**: Applying proposition 3.2.2 with $g = T^n$ we obtain that $T^n = qf + r$ with $r = 0$ or $deg(r) < n$. Now looking at this expression modulo $\mathfrak{p}$ we obtain $T^n \equiv q \cdot \sum_{i=n}^{\infty} a_i T^i + r \mod \mathfrak{p}$. Therefore $r \equiv 0 \mod \mathfrak{p}$ since $deg(r) < n$. Thus we set $P \overset{\text{def}}{=} T^n - r$ which is a distinguished polynomial. We claim that $q \in \mathcal{O}[|T|]^\times$. If this holds, then set $U \overset{\text{def}}{=} q^{-1}$. Now we prove the claim: let $q = \sum_{i=0}^{\infty} q_i T^i$ and recall that $T^n \equiv (q_0 + q_1 T + ...) \cdot (a_n T^n + ...) \mod \mathfrak{p}$ where the q_i's are the coefficients of q. Looking at the coefficient of T^n we get $1 \equiv q_0 a_n \mod \mathfrak{p}$. This implies that $q_0 a_n = 1 + y$ for some $y \in \mathfrak{p}$. Since $\mathcal{O}$ is local, then it follows that $q_0 \in \mathcal{O}^\times$ and so $q \in \mathcal{O}[|T|]^\times$ by lemma 3.2.1.

Uniqueness: Suppose $f = \widetilde{P}\widetilde{U}$. Clearly $\widetilde{P}$ can be written in the form $\widetilde{P} = T^n - \widetilde{r}$ as above. Then we deduce that $T^n = \widetilde{U}^{-1}f + \widetilde{r} = U^{-1}f + r$. However division with remainder is unique, and so we can conclude the proof of the first part. The second part follows directly collecting a power of π from the coefficients of f.

□

Corollary 3.2.4. *Let $\mathcal{O} = \mathcal{O}_F$ where $F|\mathbb{Q}_p$ is a finite extension. Assume $0 \neq f \in \mathcal{O}[|T|]$. Then there are only finitely many $x \in \mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ with $|x| < 1$ such that $f(x) = 0$.*

Proof. Write $f = \pi^s PU$ where $U = u_0 + u_1 T + \dots$ with $u_0 \notin \mathfrak{p}$, i.e. $|u_0| = 1$. Notice we can write $U(x) = u_0 + xh(x)$ with x as in the statement. Since u_0 has norm equal to 1 and $xh(x)$ has norm lesser than 1 we deduce that $|U(x)| = 1$ and so $U(x) \neq 0$. This implies that $P(x) = 0$. However P is a polynomial and therefore it has only finitely many zeros.

□

Lemma 3.2.5. *Let $P, g \in \mathcal{O}[T]$ with P distinguished. If $\frac{g}{P} \in \mathcal{O}[|T|]$ then $\frac{g}{P} \in \mathcal{O}[T]$.*

Proof. Let $n = deg(P)$. Then we can write $g \equiv r \mod (P \cdot \mathcal{O}[T])$ with $r \in \mathcal{O}[T]$ and $deg(r) < n$. Hence $g = qP + r$ with $q \in \mathcal{O}[T]$. On the other hand $g = \frac{g}{P} \cdot P$, so proposition 3.2.2 implies that $r = 0$ and $\frac{g}{P} = q$.

□

Now we have all the tools to prove the main result of this section.

Theorem 3.2.6. $\mathcal{O}[|\Gamma|] \simeq \mathcal{O}[|T|]$, $\gamma \mapsto 1 + T$ *(non-canonical since we chose γ).*

Proof. We showed that $\mathcal{O}[|\Gamma|] \simeq \varprojlim_n \frac{\mathcal{O}[T]}{\omega_n(T)}$ thanks to the isomorphism $\mathcal{O}[\Gamma_n] \simeq \frac{\mathcal{O}[T]}{\omega_n(T)}, \gamma \mod \Gamma_n \mapsto (1+T) \mod \omega_n(T)$. Moreover recall that for every $n \in \mathbb{N}$ there is a natural map $\mathcal{O}[|T|] \to \mathcal{O}[T] \mod \omega_n(T)$ given by $f = q_n\omega_n + f_n$ with $deg(f_n) < p^n = deg(\omega_n)$. Hence proving the theorem is equivalent to prove that the map $\mathcal{O}[|T|] \to \varprojlim_n \frac{\mathcal{O}[T]}{\omega_n(T)}$, $f \mapsto (f_n)_n$ is an isomorphism. We need to prove that this is well-defined, injective and surjective.

Well-defined: For $m \geq n \geq 0$ we have $f_m - f_n = (f - q_m\omega_m) - (f - q_n\omega_n) = \omega_n(q_n - q_m \cdot \frac{\omega_m}{\omega_n})$. Notice that $\frac{\omega_m}{\omega_n} \in \mathcal{O}[T]$ and so $\frac{f_m - f_n}{\omega_n} \in \mathcal{O}[|T|]$ and therefore it lies in $\mathcal{O}[T]$ by the previous lemma. Hence $f_m \equiv f_n \mod \omega_n$.

Injective: Let $f_n \equiv 0 \mod \omega_n$ for every n. Then $f_n \equiv 0 \mod \omega_n$ for every n. We claim that $\omega_n \in (p, T)^{n+1}$. If this holds then $f \in \bigcap_{n=1}^{\infty} (p, T)^n = \{0\}$. We prove the claim by induction on n. If $n = 0$ then $\omega_0 = T \in (p, T)$. Now suppose the claim holds for n, we prove it for $n+1$. Notice that $\frac{\omega_{n+1}}{\omega_n} = 1 + (1+T)^{p^n} + \dots + (1+T)^{p^n(p-1)} = p + Tr \in (p, T)$ for some polynomial r, using the inductive hypothesis.

Surjective: Let $(f_n)_n \in \varprojlim_n \mathcal{O}[T]/\omega_n(T)$. For every n we write $f_n(T) = \sum_{j=0}^{\infty} a_{nj}T^j$ with $a_{nj} \in \mathcal{O}, a_{nj} = 0$ for j sufficiently large. Now for every $m \geq n \geq 0$ notice that $f_m \equiv f_n \mod \omega_n(T)$ implies $f_m \equiv f_n \mod (p, T)^{n+1}$. Therefore the constant terms are congruent modulo p^{n+1}, the linear terms modulo p^n and so on. In particular, one finds that for fixed j the $(a_{nj})_{n\geq 0}$ is a Cauchy sequence in $\mathcal{O}$. Set $a_j \overset{\text{def}}{=} \lim_{n\to\infty} a_{nj} \in \mathcal{O}$. Thus $f(T) \overset{\text{def}}{=} \lim_{n\to\infty} f_n(T) = \sum_{j=0}^{\infty} a_j T^j \in \mathcal{O}[|T|]$ is a preimage of $(f_n)_n$ by construction.

□

Theorem 3.2.7. *Let $\mathcal{O}$ as before and set $\mathfrak{m} \overset{\text{def}}{=} \mathfrak{p} + (T) \subseteq \mathcal{O}[|T|]$. Then $\mathcal{O}[|T|]$ is a noetherian local ring with maximal ideal $\mathfrak{m}$ and $\mathcal{O}[|T|]/\mathfrak{m} \simeq \mathcal{O}/\mathfrak{p}$. If $\mathcal{O}$ is a DVR with $\mathfrak{p} = (\pi)$ then:*

1. *the irreducible elements (up to units) of $\mathcal{O}[|T|]$ are π and the irreducible distinguished polynomials*

2. *$\mathcal{O}[|T|]$ is a UFD*

3. *the prime ideals of $\mathcal{O}[|T|]$ are $\{0\}, (\pi), \mathfrak{m} = (\pi, T)$ and (P) where P is irreducible distinguished.*

Proof. By lemma 3.2.1 we know that $\mathfrak{m} = \mathcal{O}[|T|] \setminus \mathcal{O}[|T|]^\times$ and so $\mathcal{O}[|T|]$ is a local ring with maximal ideal $\mathfrak{m}$. Let $Z \overset{\text{def}}{=} \langle f_i : i \in I \rangle \mathcal{O}[|T|]$ be a generic ideal of $\mathcal{O}[|T|]$. Using proposition 3.2.3 wlog we may assume $f_i \in \mathcal{O}[T]$ for every $i \in I$. Let $J \overset{\text{def}}{=} \langle f_i : i \in I \rangle \mathcal{O}[T]$. Now we know by the Hilbert's basis theorem that $\mathcal{O}[T]$ is noetherian and so $J = \langle f_1, ..., f_s \rangle \mathcal{O}[T]$ for some $s \geq 1$. Then $Z = J\mathcal{O}[|T|] = \langle f_1, ..., f_s \rangle \mathcal{O}[|T|]$ and so $\mathcal{O}[|T|]$ is noetherian.
In the rest of the proof assume also that $\mathcal{O}$ is a DVR.

1. Let $0 \neq f \in \mathcal{O}[|T|]$ be an irreducible element. Now the second part of proposition 3.2.3 implies that $f = \pi^n P U$ with $U \in \mathcal{O}[|T|]^\times$ and some $n \geq 0$. Since π^n and P cannot be invertibles, this implies that, up to units, f is equal either π or P with P irreducible distinguished polynomial.

2. We need to show that being irreducible implies being a prime element. Now π is prime since $\mathcal{O}[|T|]/(\pi) = \mathcal{O}/(\pi)[|T|]$ is an integral domain. Let P be an irreducible distinguished polynomial and assume $P|fg$. By proposition 3.2.3 we have decompositions $f = \pi^{n_1} P_1 U_1$ and $g = \pi^{n_2} P_2 U_2$ for some $n_1, n_2 \geq 0$. This implies that P divides $\pi^{n_1+n_2} P_1 P_2$ in $\mathcal{O}[|T|]$. Now lemma 3.2.5 tells us that $P|\pi^{n_1+n_2} P_1 P_2$ in $\mathcal{O}[T]$ and so $P|P_1P_2$ in $\mathcal{O}[T]$ since $\mathcal{O}[T]$ is a UFD. This implies that $P|P_1$ or $P|P_2$ since P is a prime element of $\mathcal{O}[T]$, i.e. $P|f$ or $P|g$. By the previous point, this suffices to prove that $\mathcal{O}[|T|]$ is a UFD.

3. Since every irreducible element is prime, part 1. implies that all the stated ideals are prime. Let $\{0\} \neq \mathfrak{q}$ be prime. Choose $0 \neq f \in \mathfrak{q}$ a polynomial of minimal degree (notice that it exists by proposition 3.2.3); wlog, we may assume $f = \pi^s P$ where $P = 1$ or P distinguished polynomial. However, $\mathfrak{q}$ is prime and therefore either $\pi^s \in \mathfrak{q}$ (so that $\pi \in \mathfrak{q}$) or $P \in \mathfrak{q}$ (so that P is irreducible since f has minimal degree and $\mathfrak{q}$ is prime). Thus $(f) \subseteq \mathfrak{q}$ where $f = \pi$ or f is irreducible distinguished. Suppose now that (f) is contained properly in $\mathfrak{q}$. We claim that $\mathfrak{q} = (\pi, T)$. Indeed, choose $g \in \mathfrak{q} \setminus (f)$. In particular, f does not divide g. If f is irreducible distinguished we can write $g = qf + r$ with $0 \neq r \in \mathfrak{q}$ and $deg(r) < deg(f)$. However, this is a contradiction since $deg(f)$ is minimal. Hence we must have $(f) = (\pi)$. As (π) is properly contained in $\mathfrak{q}$ there exists $\widetilde{P} \in \mathfrak{q}$ distinguished. Since $\widetilde{P} \equiv T^n \mod (\pi)$ we obtain $T^n \in \mathfrak{q}$ and this implies $T \in \mathfrak{q}$. Therefore $(\pi, T) \subseteq \mathfrak{q}$. On the other hand, (π, T) is maximal and so $(\pi, T) = \mathfrak{q}$.

□

Remark 20. One can also show that if $\mathcal{O}[|T|]$ is as in the previous theorem, then it is also a complete topological ring with respect to the $(\mathfrak{p}, T)$-adic topology.

Observe that using theorem 3.2.6 and arguing inductively one deduces that:

Corollary 3.2.8. *For every $n \in \mathbb{N}$ we have:*

1. $\mathcal{O}[|T_1, ..., T_n|]$ *is a noetherian complete local ring*
2. *if* $\Gamma \simeq \mathbb{Z}_p^n$ *as profinite groups then* $\mathcal{O}[|\Gamma|] \simeq \mathcal{O}[|T_1, ..., T_n|]$.

We end the section with a couple of easy but still interesting lemmas.

Lemma 3.2.9. *Consider* $\Lambda = \mathbb{Z}_p[|T|]$ *as above. Suppose that* $f, g \in \Lambda$ *are relatively prime. Then the ideal* (f, g) *is of finite index in* Λ.

Proof. Take $h \in (f, g)$ an element of minimal degree. Then h must be of the form $p^s H$ with $H = 1$ or H distinguished polynomial. Say that $H \neq 1$. Since f and g are relatively prime by hypothesis, we may assume that H does not divide f. However using proposition 3.2.2 we can write

$$f = Hq + r$$

with $deg(r) < deg(H) = deg(h)$, so that $p^s f = hq + p^s r$. Therefore, since $deg(p^s r) < deg(h)$ and $p^s r \in (f, g)$, we obtain a contradiction. Hence $H = 1$ and so $h = p^s$. Notice that wlog we may assume that f is not divisible by p and moreover that it is a distinguished polynomial (otherwise we could use g or divide by a unit). Thus we deduce that $(f, g) \supseteq (p^s, f)$. Notice that proposition 3.2.2 implies that any element of Λ is congruent modulo f to a polynomial of degree less than $deg(f)$. Since there are only finitely many such polynomials modulo p^s, we deduce that the ideal (p^s, f) must have finite index. Thus we can conclude the proof. □

Lemma 3.2.10. *Let* $f \in \Lambda$ *with* $f \notin \Lambda^\times$. *Then* $\Lambda/(f)$ *is infinite.*

Clearly we may assume that $f \neq 0$. By theorem 3.2.7 it is enough to consider the cases where f is either p or a distinguished polynomial. If $f = p$, then just notice that $\Lambda/(p) \simeq \mathbb{Z}/p\mathbb{Z}[|T|]$. In the second case, the statement follows applying the division algorithm (prop 3.2.2).

3.3 The Structure theorem for finitely generated Λ-modules

Definition 3.3.1. - Let R be a commutative ring and let $\mathfrak{p} \in Spec(R)$ a prime ideal. Then we define $ht(\mathfrak{p})$ as the supremum in $\mathbb{N} \cup \{\infty\}$ of the lengths of the chains of the form $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ where every $\mathfrak{p}_i$ is a prime ideal of R. Then $ht(\mathfrak{p})$ is called the *height* of $\mathfrak{p}$.

- We say that $dim(R) \overset{\text{def}}{=} \sup_{\mathfrak{p} \in Spec(R)} \{ht(\mathfrak{p})\} = \sup_{\mathfrak{p} \in Max(R)} \{ht(\mathfrak{p})\}$ is the *Krull dimension* of R.
- We set $P(R) \overset{\text{def}}{=} \{\mathfrak{p} \in Spec(R) : ht(\mathfrak{p}) = 1\}$.

Remark 21. - R noetherian $\Rightarrow ht(\mathfrak{p}) < \infty$ for every $\mathfrak{p} \in Spec(R)$.

- Let R be a noetherian domain. Then R is a Dedekind domain if and only if R is integrally closed and $dim(R) = 1$.

- A DVR is a local PID of dimension 1.

- If $\mathcal{O}$ is a DVR and $R = \mathcal{O}[|T|]$ then $dim(R) = 2$ (this follows from theorem 3.2.7).

Now we are going to state or assume some facts whose proofs come from commutative algebra and linear algebra. Therefore we consider them not so interesting for our purposes. For the proofs look at [**Neu2**] and [**Bou1**].

In what follows, assume that R is a commutative noetherian integrally closed domain.

Proposition 3.3.1. *1. For every $\mathfrak{p} \in P(R)$, we have that $R_\mathfrak{p}$ is a DVR.*

2. $R = \bigcap_{\mathfrak{p}\in P(R)} R_\mathfrak{p}$ where the intersection is taken in $Frac(R)$.

Definition 3.3.2. Let M be an R-module.

1. The module $M^+ \overset{\text{def}}{=} Hom_R(M, R)$ is called the R-dual of M. Moreover we will denote by V the K-vector space $M_{(0)} = M \oplus_R K$ where $K = Frac(R)$.

2. M is called *reflexive* if the canonical map $\phi_M : M \to M^{++}$, $m \mapsto [\phi_M(m) : f \mapsto f(m)]$ is an isomorphism.

Example 7. Put $M = R$. If M_1, M_2 are reflexive then $M_1 \oplus M_2$ is reflexive. Hence in particular R^n is reflexive for every $n \in \mathbb{N}$.

Lemma 3.3.2. *We have that M^+ is a torsion-free module. In particular, if M is reflexive then it is also torsion-free.*

Lemma 3.3.3. *Let M be a finitely generated torsion-free R-module. Then*

1. *$M^+ = \bigcap_{\mathfrak{p}\in P(R)} M_\mathfrak{p}^+$ where the intersection is taken in V^*.*

2. *$M^{++} = \bigcap_{\mathfrak{p}\in P(R)} M_\mathfrak{p}$ where the intersection is taken in $(V^*)^*$.*

3. *$M = \bigcap_{\mathfrak{p}\in P(R)} M_\mathfrak{p}$ if and only if M is reflexive.*

Corollary 3.3.4. *If M is a finitely generated torsion-free R-module then M^+ is reflexive.*

Lemma 3.3.5. *Let M be a finitely generated R-module. TFAE:*

1. *$M_\mathfrak{p} = 0$ for every prime ideal $\mathfrak{p}$ such that $ht(\mathfrak{p}) \leq 1$.*

2. *Set $\mathfrak{a} \overset{\text{def}}{=} Ann_R(M)$. Say that $\mathfrak{p}$ is a prime ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then $ht(\mathfrak{p}) \geq 2$.*

Proof. Let $\mathfrak{p} \in Spec(R)$ and notice that $M_\mathfrak{p} = 0$ if and only if there exists $s \in R \setminus \mathfrak{p}$: $sM = 0$. However this is true if and only if $\mathfrak{a} \not\subseteq \mathfrak{p}$. This shows the above equivalence. □

Definition 3.3.3. Let M be a finitely generated R-module. Then M is said to be *pseudo-null* if and only if M satisfies the equivalent conditions of the previous lemma.

Definition 3.3.4. The set $supp(M) \overset{\text{def}}{=} \{\mathfrak{p} \in Spec(R) : M_\mathfrak{p} \neq 0\} = \{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p}\}$ is called *the support of M.*

Remark 22. It is useful to recall that in any short exact sequence of groups, modules, rings $0 \to A \to B \to C \to 0$ one has that B is finite if and only if A and B are finite. Moreover, if this is the case, we also have that $|B| = |A| \cdot |C|$.

Proposition 3.3.6. *Let M be a finitely generated R-module.*

1. *If M is pseudo-null then it is a torsion-module.*
2. *If R is a Dedekind domain then: M is pseudo-null if and only if $M = 0$.*
3. *If R is local with maximal ideal $\mathfrak{m}$, $|R/\mathfrak{m}| < \infty$ and $dim(R) = 2$, then M is pseudo-null if and only if $|M| < \infty$.*

Proof. 1. Set $S = R \setminus \{0\}$. Then notice that $S^{-1}R \otimes_R M = M_{(0)} = S^{-1}M = 0$. This means that $0 = \frac{m}{1} \in S^{-1}M$ for every $m \in M$. Hence M is a torsion-module.

2. Assume that M is pseudo-null. Then by the previous point we can choose $s \in R$ such that $sM = 0$. Now consider the factorization of $sR = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$. Thus, for every i by hypothesis we have $M_{\mathfrak{p}_i} = 0$ and so there exists $s_i \in R \setminus \mathfrak{p}_i$ such that $s_i \in \mathfrak{p}_j$ for every $j \neq i$ and $s_iM = 0$. Indeed, if s_i is an element of $R \setminus \mathfrak{p}_i$ such that $s_iM = 0$ and $s_i \notin \mathfrak{p}_j$ for some $j \neq i$, then choose $x_j \in \mathfrak{p}_j \setminus \mathfrak{p}_i$ and replace s_i by x_js_i. Set $\widetilde{s} \overset{\text{def}}{=} s_1 + ... + s_r$. It follows that $\widetilde{s} \in \mathfrak{a}$. Therefore $\widetilde{s} \notin \mathfrak{p}_i$ for every $1 \leq i \leq r$. In fact, if this is not true then $s_i \in \mathfrak{p}_i$ for some i, contradiction. Now notice that s and $\widetilde{s}$ are relatively prime (otherwise there is a non-zero prime ideal which contains $(\widetilde{s}, s)$. This implies that $\widetilde{s} \subseteq \mathfrak{p}_i$ for some i, contradiction). Thus $R = (s, \widetilde{s}) \subseteq \mathfrak{a}$ and so $M = 0$.

3. Assume that $|M| < \infty$. Notice that $M \supseteq \mathfrak{m}M \supseteq \mathfrak{m}^2M \supseteq ...$ Being M finite, then there exists $r \in \mathbb{N}$ such that $\mathfrak{m}^rM = \mathfrak{m}^{r+1}M$. Thus Nakayama's lemma implies that $\mathfrak{m}^rM = 0$. Hence $\mathfrak{m}^r \subseteq \mathfrak{a}$. Let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$. Therefore $\mathfrak{m}^r \subseteq \mathfrak{p}$ implies that $\mathfrak{m} \subseteq \mathfrak{p}$ and so $\mathfrak{m} = \mathfrak{p}$. Then $ht(\mathfrak{p}) = 2$, namely M is pseudo-null.

   Conversely, for the rest of the proof we need the following lemma of commutative algebra:

   Lemma 3.3.7. *Only for this lemma, let R be a commutative ring. Moreover let $0 \neq M$ be an R-module. Then*

   - *For $0 \neq m \in M$ consider the ideals $I_m \overset{\text{def}}{=} Ann_R(m)$ and say that $I \overset{\text{def}}{=} I_{m_0}$ is a maximal element of the set of the I_m' s ordered with respect to the inclusion. Then I is a prime ideal.*
   - *Suppose also that R is a noetherian ring and that M is a finitely generated R-module. Then there exists a filtration $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ of M such that $M_{i+1}/M_i \simeq R/\mathfrak{p}_i$ where $\mathfrak{p}_i$ is a prime ideal for every i.*

   proof of part 1. First of all observe that $Ann_R(M) \subseteq I_m$ for every $m \in M$. Suppose now that $rs \in I$ but $s \notin I$. This implies that $rsm_0 = 0$ and $sm_0 \neq 0$. Therefore $I \subseteq (r) + I \subseteq Ann_R(sm_0)$. However by the maximality of I we must have $(r) + I = I$, i.e. $r \in I$. Thus we can conclude. □

Applying part 1. of the above lemma, we can choose $m_1 \in M$ such that $Ann_R(m_1)$ is a prime ideal. Being M pseudo-null, we deduce that $ann_r(M) \subseteq ann_R(m_1)$. Since R is a local ring with $dim(R) = 2$, it follows that $ann_R(m_1) = \mathfrak{m}$. Now set $M_1 \overset{\text{def}}{=} R/\mathfrak{m}$ and consider the injective map $M_1 \hookrightarrow M$ given by $1 \mapsto m_1$ and the natural surjection $M \twoheadrightarrow M/M_1$. Since M/M_1 is again pseudo-null, we can repeat the above argument and we can construct a sequence $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ such that $M_{i+1}/M_i \simeq R/\mathfrak{m}$. Then for every i there exists an exact sequence $0 \to M_i \to M_{i+1} \to R/\mathfrak{m} \to 0$. Being $R/\mathfrak{m}$ and $M_0 = 0$ finite and arguing by induction on i, it follows that also $M_n = M$ has finite cardinality.

□

Definition 3.3.5. A morphism $f : M \to N$ of finitely generated R-modules is called a *pseudo-isomorphism* if $Ker(f)$ and $Coker(f)$ are pseudo-null, i.e. $f_\mathfrak{p} : M_\mathfrak{p} \xrightarrow{\simeq} N_\mathfrak{p}$ for every prime $\mathfrak{p}$ with $ht(\mathfrak{p}) \leq 1$. We write in this case $f : M \sim N$.

Remark 23. - Suppose that $R = \mathcal{O}[|T|]$ where $\mathcal{O}$ is a DVR and let M and N be two R-modules. Then in this case $M \sim N$ if and only if there exists an exact sequence:

$$0 \to F_1 \to M \to N \to F_2 \to 0$$

where F_1 and F_2 are finite R-modules (look at proposition 3.3.6).

- It is interesting to point out that in general $M \sim N$ does not imply that $N \sim M$. Indeed, let $R = \Lambda = \mathbb{Z}_p[|T|]$ and consider the exact sequence $0 \to \mathfrak{m} = (p, T) \to \Lambda \to \Lambda/\mathfrak{m} = \mathbb{F}_p \to 0$. This implies that $\mathfrak{m} \sim \Lambda$. However, if we take the map $\Lambda \to \mathfrak{m}$ given by $1 \mapsto g$ where g is any element of $\mathfrak{m}$, then $|\mathfrak{m}/(g)| = \infty$ since $|\Lambda/(g)| = \infty$ by lemma 3.2.10. Therefore $\Lambda \not\sim \mathfrak{m}$.

Lemma 3.3.8. *Let M be a finitely generated R-module and let $0 \neq \alpha \in R$ such that $supp(R/\alpha) \cap supp(M) \cap P(R) = \emptyset$. Then the multiplication map $M \xrightarrow{\alpha\cdot} M$ is a pseudo-isomorphism.*

Proof. Let $\mathfrak{p} \in P(R) \cap supp(M)$. Then $\mathfrak{p} \notin supp(R/\alpha)$ and so $\alpha \notin \mathfrak{p}$, i.e. $\alpha \in R_\mathfrak{p}^\times$. This implies that the map $M_\mathfrak{p} \xrightarrow{\alpha\cdot} M_\mathfrak{p}$ is an isomorphism. Moreover, if $\mathfrak{p} \in P(R)$ and $\mathfrak{p} \notin supp(M)$, then $M_\mathfrak{p} = 0$ by definition of support. This concludes the proof.

□

Lemma 3.3.9. *Let M be a finitely generated R-torsion module. Then $supp(M) \cap P(R)$ is a finite set.*

Proof. By part 2. of lemma 3.3.7, there exists a filtration $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that $M_{i+1}/M_i \simeq R/\mathfrak{p}_i$ for some $\mathfrak{p}_i$ prime ideals. Now since M is torsion, then M_{i+1}/M_i is torsion for every i. We deduce that $\mathfrak{p}_i \neq 0$. Now let $\mathfrak{p} \in supp(M) \cap P(R)$. Then $M_\mathfrak{p} \neq 0$ and so there must be an i such that $(R/\mathfrak{p}_i)_\mathfrak{p} \neq 0$ (otherwise we localize the exact sequences $0 \to M_i \to M_{i+1} \to R/\mathfrak{p}_i \to 0$ at $\mathfrak{p}$ and by induction we find that $(M_i)_\mathfrak{p} = 0$ for every i, contradiction). Hence $\mathfrak{p} \in supp(R/\mathfrak{p}_i) = \{\mathfrak{q} \in Spec(R) : Ann_R(R/\mathfrak{p}_i) \subseteq \mathfrak{q}\}$. It follows that $0 \subset \mathfrak{p}_i \subseteq \mathfrak{p}$. However $ht(\mathfrak{p}) = 1$ and so $\mathfrak{p}_i = \mathfrak{p}$. Since there are only finitely many such $\mathfrak{p}_i$'s, this ends the proof.

□

Theorem 3.3.10. *Let M be a finitely generated R-module and set $T(M) \overset{\text{def}}{=}$ the torsion submodule of M and $F(M) \overset{\text{def}}{=} M/T(M)$, Then:*

1. *There exists a pseudo-isomorphism $f : M \to F(M) \oplus T(M)$.*
2. *There exist a finite set I, $\mathfrak{p}_i \in P(R)$, $n_i \in \mathbb{N}$ for $i \in I$ and a pseudo-isomorphism*
$$g : T(M) \to \oplus_{i\in I} R/\mathfrak{p}_i^{n_i}$$
Moreover the $\mathfrak{p}_i$'s and the n_i's are uniquely determined by $T(M)$.

Proof. 1. **Case 1**: Suppose that $supp(T(M)) \cap P(R) = \emptyset$, i.e. $T(M)_{\mathfrak{p}} = 0$ for every $\mathfrak{p} \in P(R)$. Then, not only $g : T(M) \to 0$ is a pseudo-isomorphism but also the projection map $f : M \to F(M)$ since for every $\mathfrak{p} \in P(R)$ we have $(M/T(M))_{\mathfrak{p}} = M_{\mathfrak{p}}/T(M)_{\mathfrak{p}} = M_{\mathfrak{p}}/\{0\}$.

Case 2: Suppose that $supp(T(M)) \cap P(R) \neq \emptyset$. Then by lemma 3.3.9 we deduce that it must be a finite set. Say that it is equal to $\{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$. Set $S \overset{\text{def}}{=} R \setminus \bigcup_{i=1}^{h} \mathfrak{p}_i$. Recall that the prime ideals in $S^{-1}R$ are exactly the ideals of the form $S^{-1}P$ where P is a prime ideal of R and $P \cap S = \emptyset$. However, this is equivalent to say that a such P is contained in $\bigcup_{i=1}^{h} \mathfrak{p}_i$. By the well known lemma of commutative algebra "Prime avoidance", this is true if and only if either $P = \mathfrak{p}_i$ for some i or $P = 0$ (recall that every $\mathfrak{p}_i$ has height 1). Thus $S^{-1}R$ is a Dedekind domain with finitely many prime ideals, hence it is a *PID*. Moreover, $S^{-1}T(M)$ is the $S^{-1}R$-torsion submodule of $S^{-1}M$. By the Structure theorem of modules over a PID (see [**Du**]), we deduce that $S^{-1}M \simeq F \oplus S^{-1}T(M)$ where F is a free $S^{-1}R$-module of finite rank. Moreover by commutative algebra we know that:

$$Hom_{S^{-1}R}(S^{-1}M, S^{-1}T(M)) = S^{-1}Hom_R(M, T(M))$$

Therefore there exist $f_0 \in Hom_R(M, T(M))$ and $s_0 \in S$ such that $\frac{f_0}{s_0}$=projection map $S^{-1}(M) \to S^{-1}(T(M))$. In particular, notice that $\frac{f_0}{s_0} \restriction_{S^{-1}T(M)} = id_{S^{-1}T(M)}$. It follows that $f_0 \restriction_{T(M)} = s_0 \cdot id_{T(M)}$.

Now set $f \overset{\text{def}}{=} (proj, f_0) : M \to F(M) \oplus T(M)$ and consider the following commutative diagram (it exists by the Snake lemma):

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & Ker(f_0) \arrow[r, "\simeq"] \arrow[d] & Ker(f) \arrow[d] & & \\
0 \arrow[r] & T(M) \arrow[r] \arrow[d, "f_0 = s_0 \cdot id"] & M \arrow[r] \arrow[d, "f"] & F(M) \arrow[r] \arrow[d, "id"] & 0 \\
0 \arrow[r] & T(M) \arrow[r] \arrow[d] & F(M) \oplus T(M) \arrow[r] \arrow[d] & F(M) \arrow[r] & 0 \\
 & Coker(f_0) \arrow[r, "\simeq"] \arrow[d] & Coker(f) \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

Being $s_0 \in S$, we get that $s_0 \notin \mathfrak{p}_i$ for $1 \leq i \leq h$ and so $\mathfrak{p}_i \notin V(Ann_R(R/s_0)) = supp(R/s_0)$. By lemma 3.3.8 follows that f_0 is a pseudo-isomorphism and so looking at the diagram we deduce that also f is a pseudo-isomorphism.

2. From the above and from the Structure theorem for modules over a PID, we deduce that there exists an isomorphism $g_0 : S^{-1}T(M) \xrightarrow{\simeq} S^{-1}E$ where $E \overset{\text{def}}{=} \oplus_{i=1}^{h} \oplus_{j=1}^{r} R/\mathfrak{p}_i^{n_{ij}}$. As before we get that there are $g \in Hom_R(T(M), E)$ and $s \in S$ such that $g_0 = \frac{g}{s}$. Notice that $s \in R_{\mathfrak{p}_i}^{\times}$ for every i and that g is a pseudo-isomorphism. Indeed $g_{\mathfrak{p}_i} = s \cdot (g_0)_{\mathfrak{p}_i}$ is an isomorphism for $1 \leq i \leq h$ and if $\mathfrak{p} \in P(R) \setminus \{\mathfrak{p}_1, ..., \mathfrak{p}_h\}$ then $T(M)_{\mathfrak{p}} = 0 = E_{\mathfrak{p}}$.

□

Remark 24. One can prove that being pseudo-isomorphic is an equivalence relation on finitely generated R-torsion module.

Proposition 3.3.11. *Let M be a finitely generated R-module and assume that M is torsion-free. Then there is an injective pseudo-isomorphism $M \hookrightarrow M'$ where M' is a reflexive module. In particular, the statement holds for $M' = M^{++}$.*

Definition 3.3.6. Let $(R, \mathfrak{m})$ be a Noetherian local ring with $dim(R) = n$. Then R is said to be a *regular local ring* if there exist $p_1, ..., p_n \in R$ such that $\mathfrak{m} = (p_1, ..., p_n)$.

Example 8. Let $\mathcal{O}$ be a DVR and let π be a uniformizer. Then $\mathcal{O}[|T|]$ is a 2-dimensional regular local ring with maximal ideal $\mathfrak{m} = (\pi, T)$.

Remark 25. Using some arguments of commutative algebra, one can prove that a regular local ring is an integrally closed domain (see [**Bou2**] or [**Mat**]).

Theorem 3.3.12. *If M is a reflexive finitely generated R-module M over a 2-dimensional regular local ring, then M is free.*

Proof. First of all, let $\mathfrak{m} = (p_1, p_2)$ with $p_1, p_2 \in R$. Thus $R/(p_1)$ is a regular local ring of dimension 1. This means that $R/(p_1)$ is a DVR.
Now since M is reflexive then it is torsion-free and so the multiplication map $M \xrightarrow{p_i \cdot} M$ is injective. Choose a surjective morphism $\phi : R^r \twoheadrightarrow M$ with r minimal. Now consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & R^r \arrow[r, "p_i \cdot"] \arrow[d, "\phi"] & R^r \arrow[r] \arrow[d, "\phi"] & (R/p_iR)^r \arrow[r] \arrow[d, "\overline{\phi}"] & 0 \\
0 \arrow[r] & M \arrow[r, "p_i \cdot"] & M \arrow[r] & M/p_iM \arrow[r] & 0
\end{tikzcd}$$

We claim that M/p_1M is a free $R/(p_1)$-module. Indeed: $R/(p_1)$ is an integral domain and so $Hom_R(M, R/(p_1))$ is torsion-free as $R/(p_1)$-module. Consider the map $M^{++} \to Hom_R(M^+, R/(p_1))$ given by $f \mapsto [g \mapsto f(g) \mod (p_1)]$. Now we study its kernel: suppose that $f(g) \equiv 0 \mod (p_1)$ for every $g \in M^+$. Then, since p_1 is not a zero-divisor, follows that for every $g \in M^+$ there exists a unique $x_g \in R$ such that $f(g) = p_1 x_g$. This means that there is a function $h \in M^{++}$ such that $f(g) = p_1 h(g)$ for every $g \in M^+$. Therefore, the kernel is equal to $p_1 M^{++}$. Being M reflexive, we deduce that $M/p_1M \simeq M^{++}/p_1M^{++}$ injects into the torsion-free module $Hom_R(M^+, R/(p_1))$. It follows that M/p_1M is torsion-free too and so it is a free module since $R/(p_1)$ is

a PID. Hence $\overline{\phi}$ is an isomorphism, otherwise $M/p_1M \simeq ((R/p_1R)^r/Ker(\overline{\phi}))$ is a free $R/(p_1)$-module of rank $s < r$. Since $p_1 \in \mathfrak{m}$, then by Nakayama's lemma we get that there exists a surjective map $R^r \twoheadrightarrow M$, contradicting the minimality of r.
Now by the Snake lemma applied to the above diagram, we have that $Ker(\phi) \xrightarrow{p_1\cdot} Ker(\phi)$ is an isomorphism. This implies that $p_1 \cdot Ker(\phi) = Ker(\phi)$ so that $Ker(\phi) = 0$ again by Nakayama's lemma. Therefore $M \simeq R^r$ and we can conclude the proof. □

Thus we can finally prove the most important result of this section.

Corollary 3.3.13 (The Structure theorem for finitely generated Λ-modules)**.** *Let R be a 2-dimensional regular local ring and let M be a finitely generated R-module. Then there exist finitely many prime ideals $\mathfrak{p}_i$ with $i \in I$ of height 1, a nonnegative integer r, natural numbers $n_i \in \mathbb{N}$ and a pseudo-isomorphism:*

$$M \sim R^r \oplus \bigoplus_{i\in I} R/\mathfrak{p}_i^{n_i}$$

Moreover, the prime ideals $\mathfrak{p}_i$ and the numbers r, n_i are uniquely determined by M:

$$r = dim_K(M \otimes_R K), \quad \{\mathfrak{p}_i : i \in I\} = supp(M) \cap P(R)$$

with $K = Frac(R)$.

Proof. By theorem 3.3.10 and remark 25, we already know that $M \sim F(M) \oplus T(M) \sim F(M) \oplus \bigoplus_{i\in I} R/\mathfrak{p}_i$ with I, n_i and the $\mathfrak{p}_i$'s as in the above statement. Thus applying proposition 3.3.11 we also find that $M \sim F(M)^{++} \oplus \bigoplus_{i\in I} R/\mathfrak{p}_i^{n_i}$. However, the previous theorem tells us that $F(M)^{++}$ is a free R-module. This implies that there exists r such that $M \sim R^r \oplus \bigoplus_{i\in I} R/\mathfrak{p}_i^{n_i}$. Looking at the previous proofs, one deduces that r and the $\mathfrak{p}_i$'s satisfy the requested properties. This concludes the corollary. □

We conclude the section applying the corollary to the most importante case for us. This leads us to some important definitions.

Definition 3.3.7. Applying the previous corollary with $R = \mathbb{Z}_p[|T|]$ and M a finitely generated Λ-module we get that

$$M \sim \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p_i^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/(P_j^{n_j})$$

where $s, t, m_i, n_j \in \mathbb{N}$ and the P_j's are irreducible distinguished polynomials. Then we can define:

- $r_\Lambda(M) = r$ the *Λ-rank of M*
- $\mu(M) = \sum_{i=1}^{s} m_i$ the *Iwasawa μ-invariant of M*
- $\lambda(M) = \sum_{j=1}^{t} n_j \cdot deg(P_j)$ the *Iwasawa λ-invariant of M*
- $char(M) = p^{\mu(M)} \cdot \prod_{j=1}^{t} P_j^{n_j}$ the *characteristic polynomial of M*
- $char_\Lambda(M) = char(M)\Lambda$ the *characteristic ideal of M*

Furthermore, we call a finitely generated Λ-module of the form

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

an *elementary* Λ*-module.*

Remark 26. 1. By definition, we have $deg(char(M)) = \lambda(M)$.

2. Observe that the invariants defined above depend on M only up to pseudo-isomorphism and $r_\Lambda(M), \mu(M)$ and $\lambda(M)$ are independent of the chosen generator γ. This is not true for the characteristic polynomial, so that we should write $char^\gamma(M)$ to be more precise. Moreover, notice that $char^\gamma(M) = char^\gamma(T_\Lambda(M))$ where $T_\Lambda(M)$ is the Λ-torsion submodule of M.

3.4 Application: another way to construct p-adic L-functions

In this section we want to present another method to construct p-adic L-functions that will provide us an important tool for stating The Iwasawa Main conjecture. In particular, we are going to show that there exists a power series $f(T, \omega^j)$ such that $L_p(s, \omega^j) = f((1 + p)^s - 1, \omega^j)$.

Let p be an odd prime as usual. It is known that $Gal(\mathbb{Q}(\zeta_{p^{n+1}})|\mathbb{Q}) \simeq (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. If we let

$$\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n\geq 0} \mathbb{Q}(\zeta_{p^{n+1}}),$$

then it follows that $Gal(\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q}) \simeq \varprojlim_{n\geq 0}(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times$. More explicitly, let $a = \sum_i a_i p^i \in \mathbb{Z}_p^\times$ and let $\zeta = \zeta_{p^n}$ for some n. Then we set

$$\sigma_a(\zeta) \overset{\text{def}}{=} \zeta^a \overset{\text{def}}{=} \prod_i \zeta^{a_i p^i}$$

which is a finite product since $\zeta^{p^i} = 1$ for $i \geq n$. Clearly σ_a gives an element of $Gal(\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q})$. However notice that every automorphism must be of this form, since it is known what happens at each finite n-level. Now for what we said in the example 2 we have a decomposition

$$\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$$

and one can see that they are given by the isomorphisms

$$a \mapsto (\omega(a) \mod p, \langle a\rangle) \mapsto (\omega(a) \mod p, \frac{log_p\langle a\rangle}{log_p(1 + p)})$$

Now observe that $1 + p$ is a topological generator for $1 + p\mathbb{Z}_p$ since $(1 + p)^{\mathbb{Z}_p} = 1 + p\mathbb{Z}_p$.

Let d be a positive integer with $(p, d) = 1$ and let $q_n = p^{n+1}d, K_n = \mathbb{Q}(\zeta_{q_n})$, and $K_\infty = \bigcup_{n\geq 0} \mathbb{Q}(\zeta_{q_n})$. Then $K_n = K_0(\zeta_{p^{n+1}})$ and $K_\infty = K_0(\zeta_{p^\infty})$. It follows that

$$\begin{aligned} Gal(K_\infty|\mathbb{Q}) &= \varprojlim_n Gal(K_n|\mathbb{Q}) \simeq \varprojlim_n (\mathbb{Z}/q_n\mathbb{Z})^\times \simeq \\ &\simeq \varprojlim_n ((\mathbb{Z}/d\mathbb{Z})^\times \times (\mathbb{Z}/p^{n+1})^\times) \simeq (\mathbb{Z}/d\mathbb{Z})^\times \times \mathbb{Z}_p^\times \end{aligned}$$

However by the above we have $\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$ and so

$$Gal(K_\infty|\mathbb{Q}) \simeq \Delta \times \Gamma$$

where $\Delta = Gal(K_0|\mathbb{Q}) \simeq (\mathbb{Z}/pd\mathbb{Z})^\times$ and $\Gamma = Gal(K_\infty|K_0) \simeq (1 + p\mathbb{Z}_p, \cdot) \simeq (\mathbb{Z}_p, +)$. In particular, identifying Γ with $1 + p\mathbb{Z}_p$, we have $\Gamma = 1 + q_0\mathbb{Z}_p = (1 + q_0)^{\mathbb{Z}_p}$ since $(p, d) = 1$ and so also $1 + q_0$ gives a topological generator.
The elements of Γ which fix K_n can be clearly identified with the elements of $1 + q_n\mathbb{Z}_p = (1 + q_0)^{p^n\mathbb{Z}_p} = \Gamma^{p^n}$. Therefore by Galois theory we deduce that $Gal(K_n|K_0) \simeq \Gamma/\Gamma^{p^n} \overset{\text{def}}{=} \Gamma_n$. Furthermore, notice that arguing as before we get that

$$Gal(K_n|\mathbb{Q}) \simeq \Delta \times \Gamma_n.$$

Using this isomorphism, for $a = \sum_i a_i p^i \in \mathbb{Z}_p^\times$ as above, we write:

$$\sigma_a = \delta(a)\gamma_n(a)$$

with $\delta(a) \in \Delta, \gamma_n(a) \in \Gamma_n$. In particular observe that by our writing we have $\gamma_n(1 + q_0) = 1 + q_0 \mod \Gamma^{p^n}$.

Now let χ be a Dirichlet character whose conductor is of the form p^jd for some $j \geq 0$. Clearly, we may regard χ as a character of $Gal(K_n|\mathbb{Q})$ so that we can uniquely write $\chi = \theta\psi$ where $\theta \in \widehat{\Delta}, \psi \in \widehat{\Gamma}_n$. Then θ is a character with conductor d or pd (hence $p^2 \nmid f_\theta$), while ψ is a character of Γ_n, so ψ has p-power order and is either trivial or has conductor equal to p^j and $j \geq 1$.

Definition 3.4.1. Let $\chi = \theta\psi$ a character of conductor dp^j with $j \geq 1$ as above. Then we call θ a character of *the first kind* and ψ a character of *the second kind.*

Remark 27. One can show that ψ is an even character since the fixed field of its kernel is a real field (see [**Wa**] for the details). Thus, if χ is even then θ is even.

Now assume $\chi = \theta\psi$ is an even character and let $\theta^* = \omega\theta^{-1}$ (thus θ^* is odd). Moreover, define

$$\xi_n = -\frac{1}{q_n} \cdot \sum_{\substack{0<a<q_n \\ (a,q_0)=1}} a\delta(a)^{-1}\gamma_n(a)^{-1} \in \mathbb{Q}_p[\Delta \times \Gamma_n]$$

and

$$\begin{aligned}\eta_n &= (1 - (1 + q_0)\gamma_n(1 + q_0)^{-1})\xi_n = \\ &= -\sum_{\substack{0<a<q_n \\ (a,q_0)=1}} \left(\frac{a(1 + q_0)}{q_n} - (1 + q_0)\frac{a}{q_n}\right) \delta(a)^{-1}\gamma_n(a)^{-1}\gamma_n(1 + q_0)^{-1} \in \mathbb{Z}_p[\Delta \times \Gamma_n].\end{aligned}$$

Let $K_\theta = \mathbb{Q}_p(\theta)$, $\mathcal{O}_\theta = \mathbb{Z}_p[\theta]$ (the notation has the similar meaning of $\mathbb{Q}(\chi)$) and

$$\epsilon_{\theta^*} \overset{\text{def}}{=} \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \theta^*(\delta)\delta^{-1}$$

The above ϵ_{θ^*} is called the idempotent for θ^*. There is a more general theory about idempotents that we will treat in the following sections.
Notice that $\epsilon_{\theta^*}\xi_n = \xi_n(\theta)\epsilon_{\theta^*}$ and $\epsilon_{\theta^*}\eta_n = \eta_n(\theta)\epsilon_{\theta^*}$, where

$$\xi_n(\theta) \overset{\text{def}}{=} -\frac{1}{q_n} \cdot \sum_{\substack{0<a<q_n \\ (a,q_0)=1}} a\theta\omega^{-1}(a)\gamma_n(a)^{-1} \in K_\theta[\Gamma_n]$$

and

$$\begin{aligned}\eta_n(\theta) &\overset{\text{def}}{=} (1-(1+q_0)\gamma_n(1+q_0)^{-1})\xi_n(\theta) = \\ &= \sum_{\substack{0<a<q_n \\ (a,q_0)=1}} \left((1+q_0)\frac{a}{q_n} - \frac{a(1+q_0)}{q_n}\right) \cdot \theta\omega^{-1}(a)\gamma_n(a)^{-1}\gamma_n(1+q_0)^{-1} \in \mathcal{O}_\theta[\Gamma_n]\end{aligned}$$

Proposition 3.4.1. *1. $\frac{1}{2}\eta_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$*

2. if $\theta \neq 1$ then $\frac{1}{2}\xi_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$

3. if $m \geq n \geq 0$ then $\eta_m(\theta) \mapsto \eta_n(\theta)$ and $\xi_m(\theta) \mapsto \xi_n(\theta)$ under the natural map from $K_\theta[\Gamma_m]$ to $K_\theta[\Gamma_n]$.

Partial proof. We give complete proofs of 1. and 3. Since the proof of 2. involves a lot of computations, we decided not to present it. However, we will state some important formulas that arise from its proof. This can be find with all the details in [**Wa**].

1. By definition, $\eta_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$. Now since p is odd we have that $|\frac{1}{2}| = 1$ and so $\frac{1}{2} \in \mathbb{Z}_p$. Therefore multiplying $\eta_n(\theta)$ by $\frac{1}{2}$ we still obtain an element of $\mathcal{O}_\theta[\Gamma_n]$.

3. Notice that under the natural map $\Gamma_{n+1} \to \Gamma_n$ we have $\gamma_{n+1}(a) \mapsto \gamma_n(a)$. Therefore

$$\xi_{n+1}(\theta) \mapsto \xi'_n(\theta) = -\frac{1}{q_{n+1}} \sum_{\substack{0<a<q_{n+1}, \\ (a,q_0)=1}} a\theta\omega^{-1}(a)\gamma_n(a)^{-1}.$$

Notice that for every a in the sum we can write $a = b + iq_n$ with $0 \leq b < q_n, (b, q_0) = 1$, and $0 \leq i < p$. Then $a \equiv b \mod q_n$ implies $\gamma_n(a) = \gamma_n(b)$ (this follows from the fact that $Gal(K_n\mathbb{Q}) \simeq (\mathbb{Z}/q_n\mathbb{Z})^\times$ and by its decomposition as $\Delta \times \Gamma_n$). Now $f_\theta = d$ or pd and $f_\omega = p$, therefore $f_{\theta\omega^{-1}}$ divides $q_0 = pd = lcm(p, d, pd)$. Thus $f_{\theta\omega^{-1}}$ divides q_n and so $a \equiv b \mod q_n$ implies also that $\theta\omega^{-1}(a) = \theta\omega^{-1}(b)$. It follows that

$$\begin{aligned}\xi'_n(\theta) &= -\frac{1}{q_{n+1}} \sum_{\substack{0\leq b<q_n \\ (b,q_0)=1}} \left(\theta\omega^{-1}(b)\gamma_n(b)^{-1}\sum_{i=0}^{p-1}(b+iq_n)\right) = \\ &= -\frac{p}{q_{n+1}} \sum_{\substack{0\leq b<q_n \\ (b,q_0)=1}} \left(\theta\omega^{-1}(b)\gamma_n(b)^{-1}\sum_{i=0}^{p-1} b\right) - \frac{q_n}{q_{n+1}} \sum_{\substack{0\leq b<q_n \\ (b,q_0)=1}} \theta\omega^{-1}(b)\gamma_n(b)^{-1}\sum_{i=1}^{p-1} i = \\ &= \xi_n - \frac{p-1}{2} \sum_{\substack{0\leq b<q_n \\ (b,q_0)=1}} \theta\omega^{-1}(b)\gamma_n(b)^{-1}.\end{aligned}$$

Now observe that

$$\sum_{\substack{0\le b<q_n\\(b,q_0)=1}} \theta\omega^{-1}(b)\gamma_n(b)^{-1} = \sum_{\substack{0\le b<\frac{q_n}{2}\\(b,q_0)=1}} (\theta\omega^{-1}(b)\gamma_n(b)^{-1} + \theta\omega^{-1}(q_n-b)\gamma_n(q_n-b)^{-1})$$

However: since $\theta\omega^{-1} = \theta(-1)\omega(-1) = -1$ then $\theta\omega^{-1}(q_n - b) = \theta\omega^{-1}(-b) = \theta\omega^{-1}(b)$; similarly $\gamma_n(q_n - b) = \gamma_n(-b) = \gamma_n(-1)\gamma_n(b) = \gamma_n(b)$. Hence

$$\sum_{\substack{0\le b<q_n\\(b,q_0)=1}} \theta\omega^{-1}(b)\gamma_n^{-1}(b) = 0$$

This implies that $\xi'_n(\theta) = \xi_n(\theta)$. Noticing that $\gamma_m(a) \mapsto \gamma_n(a)$ through $\Gamma_m \to \Gamma_n$, also the general case follows.

□

As promised in the previous proof, we will state some important formulas that one can find in proving part 2. of the previous proposition.

Proposition 3.4.2. *Assume $\theta \neq 1$. Let R denote the set of $(p-1)$-st roots of unity and R' be a set of representatives for R modulo ± 1. Moreover let T denote a set of representatives of elements of $(\mathbb{Z}/q_n\mathbb{Z})^\times$ such that $\Gamma_n = \{\gamma_n(b) : b \in T\}$. Hence:*

1. *If $f_\theta = p$, then*

$$\frac{1}{2}\xi_n(\theta) = -\frac{1}{2p^{n+1}}\sum_{b\in T}\sum_{\alpha\in R} s_n(b\alpha)\theta\omega^{-1}(b\alpha)\gamma_n(b)^{-1}$$

2. *If $f_\theta \neq p$, then*

$$\frac{1}{2}\xi(\theta) = -\frac{1}{d}\sum_{b\in T}\sum_{\alpha\in R'}\sum_{i=0}^{d-1} i\theta\omega^{-1}(s_n(b\alpha) + iqp^n)\gamma_n(b)^{-1}$$

Using proposition 3.4.1 and the fact that $\mathcal{O}_\theta[|\Gamma|] \simeq \mathcal{O}_\theta[|T|]$, we deduce that there are power series $f, g, h \in \mathcal{O}_\theta[[T]]$ with the following correspondences:

$$\varprojlim_n \xi_n(\theta) \leftrightarrow f(T,\theta), if \theta \neq 1$$
$$\varprojlim_n \eta_n(\theta) \leftrightarrow g(T,\theta)$$
$$\varprojlim_n (1-(1+q_0)\gamma_n(1+q_0)^{-1}) \leftrightarrow h(T,\theta)$$

Moreover one can show that $h(T,\theta) = 1 - \dfrac{1+q_0}{1+T}$ and that $f(T,\theta) = \dfrac{g(T,\theta)}{h(T,\theta)}$ (if $\theta = 1$, we take this as definition of $f(T,\theta)$).

The following lemma will be useful to prove the main result of this chapter. The proof is just a matter of computations and so we decided to omit it. The interested reader can look at [[**Wa**]] for the details.

Lemma 3.4.3.

$$\lim_{n\to\infty}\Big(\frac{1}{q_n}\cdot\sum_{\substack{0<a<q_n\\(a,q_0)=1}}\chi\omega^{-m}(a)a^m\Big) = (1-\chi\omega^{-m}(p)p^{m-1})B_{m,\chi\omega^{-m}}$$

Theorem 3.4.4. *Let $\chi = \theta\psi$ be an even Dirichlet character of conductor dp^j with $j \geq 1$ as above (θ of first kind, ψ of second kind). Moreover let $\zeta_\psi \overset{\text{def}}{=} \psi(1+q_0)^{-1} = \chi(1+q_0)^{-1}$. Then*

$$L_p(s,\chi) = f(\zeta_\psi(1+q_0)^s - 1, \theta).$$

Proof. First of all notice that ζ_ψ is a p^k-th root of unity for some $k \geq 1$. Moreover observe that if $|s| < p^{\frac{p-2}{p-1}}$ then

$$|(1+q_0)^s - 1| = |exp_p(s\cdot log_p(1+q_0)) - 1| < 1$$

and so also $|\zeta_\psi(1+q_0)^s - 1| = |exp_p(log_p(\zeta_\psi)) + exp_p(s\cdot log_p(1+q_0))| < 1$. Therefore the RHS of the statement converges and is an analytic function of s. Consequently, by the uniqueness discussed in remark 17, we only need to prove the above equality for $s = 1-m$, where m is a positive integer. Let $i(a) \overset{\text{def}}{=} log_p\langle a\rangle / log_p(1+q_0)$. Since $\gamma_n(1+q_0)$ generates Γ_n then it corresponds to $\big((1+T) \mod ((1+T)^{p^n}-1)\big) \in \mathbb{Z}_p[|T|]/(\omega_n(T)\mathbb{Z}_p[|T|])$. It follows that $\gamma_n(a) = \gamma_n(1+q_0)^{i(a)}$ corresponds to $(1+T)^{i(a)}$ mod $((1+T)^{p^n}-1)$. From the definition of $\eta_n(\theta)$ we have

$$g(T,\theta) \equiv \sum_{\substack{0<a<q_n\\(a,q_0)=1}}\Big(((1+q_0)\frac{a}{q_n} - \frac{(1+q_0)a}{q_n})\cdot\theta\omega^{-1}(a)(1+T)^{-i(a)-1}\Big) \mod ((1+T)^{p^n}-1).$$

Let $(1+q_0)a = a_1 + a_2q_n$ with $0 \leq a_1 < q_n$. By definition of log_p we have that $i(a)+1 = i((1+q_0)a)$. Moreover notice that $(1+q_0)a \equiv a_1 \mod q_n$ implies:

- $\omega((1+q_0)a) = \omega(a_1)$;
- $\theta((1+q_0)a) = \theta(a_1)$;
- $\gamma_n((1+q_0)a) = \gamma_n(a_1)$;
- $\langle(1+q_0)a\rangle = \omega((1+q_0)a)^{-1}(1+q_0)a = \omega(a_1)^{-1}(a_1+a_2q_n) = \langle a_1\rangle + \omega(a_1)^{-1}a_2q_n$.

So in particular we get $i(a)+1 = i((1+q_0)a) \equiv i(a_1)$ modulo p^n. Thus

$$g(T,\theta) \equiv \sum_{\substack{0<a<q_n\\(a,q_0)=1}} a_2\theta\omega^{-1}(a_1)(1+T)^{-i(a_1)} \mod ((1+T)^{p^n}-1).$$

Now if m is a positive integer and n is sufficiently large we have:

$$(\zeta_\psi(1+q_0)^{1-m})^{p^n} - 1 = (1+q_0)^{(1-m)p^n} - 1 \equiv 0 \mod q_n$$

Then:

$$g(\zeta_\psi(1+q_0)^{1-m}-1,\theta) \equiv \sum_{\substack{0<a<q_n\\(a,q_0)=1}} a_2\theta\omega^{-1}(a_1)(\zeta_\psi^{-1}(1+q_0)^{m-1})^{i(a_1)} \mod q_n.$$

However $\zeta_\psi^{-i(a_1)} = \psi(1+q_0)^{i(a_1)} = \psi(a_1)$ and $(1+q_0)^{i(a_1)} = \langle a_1\rangle$. Therefore

$$\begin{aligned} g(\zeta_\psi(1+q_0)^{1-m}-1,\theta) &\equiv \sum_{\substack{0<a<q_n\\(a,q_0)=1}} a_2\theta\omega^{-1}(a_1)\psi(a_1)\langle a_1\rangle^{m-1} \\ &\equiv \sum_{\substack{0<a<q_n\\(a,q_0)=1}} a_2\chi\omega^{-m}(a_1)a_1^{m-1} \mod q_n. \end{aligned}$$

If n is large enough that f_ψ divides q_n, then $\chi\omega^{-m}((1+q_0)a) = \chi\omega^{-m}(a_1)$. Moreover,

$$((1+q_0)a)^m = (a_1+a_2q_n)^m \equiv a_1^m + ma_1^{m-1}q_na_2 \mod q_n^2,$$

and so

$$\begin{aligned} \chi\omega^{-m}(1+q_0)(1+q_0)^m \sum_{\substack{0<a<q_n\\(a,q_0)=1}} \chi\omega^{-m}(a)a^m &\equiv \sum_{\substack{0<a<q_n\\(a,q_0)=1}} \chi\omega^{-m}(a_1)a_1^m + \\ + mq_n \sum_{\substack{0<a<q_n\\(a,q_0)=1}} a_2\chi\omega^{-m}(a_1)a_1^{m-1} \mod q_n^2. \end{aligned}$$

This implies

$$g(\zeta_\psi(1+q_0)^{1-m}-1,\theta) \equiv (\chi\omega^{-m}(1+q_0)(1+q_0)^m-1)\frac{1}{mq_n}\sum_{\substack{0<a<q_n\\(a,q_0)=1}} \chi\omega^{-m}(a)a^m \mod q_n$$

Now observe that as a runs from 1 to q_n, so does a_1 and furthermore that $\chi\omega^{-m}(1+q_0) = \chi(1+q_0)$. Hence, recalling the definitions of q_n and of p-adic limit, and using also the previous lemma, we obtain:

$$\begin{aligned} g(\zeta_\psi(1+q_0)^{1-m}-1,\theta) &= ((1+q_0)^m\chi(1+q_0)-1)\frac{1}{m}\lim_{n\to\infty}\left(\frac{1}{q_n}\sum_{\substack{0<a<q_n\\(a,q_0)=1}} \chi\omega^{-m}(a)a^m\right) = \\ &= -h(\zeta_\psi(1+q_0)^{1-m}-1,\theta)\frac{1}{m}\lim_{n\to\infty}\left(\frac{1}{q_n}\sum_{\substack{0<a<q_n\\(a,q_0)=1}} \chi\omega^{-m}(a)a^m\right) = \\ &= -h(\zeta_\psi(1+q_0)^{1-m}-1,\theta)\frac{1}{m}(1-\chi\omega^{-m}(p)p^{m-1})B_{m,\chi\omega^{-m}}. \end{aligned}$$

Therefore dividing $g(\zeta_\psi(1+q_0)^{1-m},\theta)$ by $h(\zeta_\psi(1+q_0)^{1-m}-1,\theta)$ and recalling the formulas for $f(T,\theta)$ and $L_p(1-m,\chi)$ we can conclude the proof. □

Chapter 4

Iwasawa's theory of $\mathbb{Z}_p$-extensions

The aim of this chapter is to give other necessary background on Iwasawa theory in order to start the study of the proof of The Iwasawa Main Conjecture. We start with some remarks in infinite Galois theory and then we pass to study the Iwasawa's theorem for ideal class groups in $\mathbb{Z}_p$-extensions. Next we discuss Modules decomposition with respect to orthogonal idempotents. We conclude the chapter with a brief discussion on cyclotomic units and on the maximal unramified abelian p-extension unramified outside p.

4.1 Infinite Galois theory and Ramification theory

In this section we want just to collect the key properties of infinite Galois extensions and their corresponding Ramification theory in order to prove the Iwasawa's theorem. Thus, we are not going to prove most of the claims. For the proofs, see [**Wi**] and [**Wa**].

Let $L|K$ be an algebraic field extension. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}_L$ and let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, which is a prime ideal of $\mathcal{O}_K$, as it is known by commutative algebra. In particular, one says that $\mathfrak{P}$ *lies above* $\mathfrak{p}$.

Clearly these rings of integers are not Dedekind domains in general, but one can show anyway that $\mathcal{O}_L/\mathfrak{P}$ is a field extension of $\mathcal{O}_K/\mathfrak{p}$. In particular it is an abelian extension since one can prove that $\mathcal{O}_L|\mathbb{F}_p$ is a Galois extension. On the other hand, by commutative algebra we know that given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ there exists a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$.
As in the finite case, if $L|K$ is Galois then $Gal(L|K)$ indicates the group of automorphisms of L which fix K pointwise. Now let F be a field such that $K \subseteq F \subseteq L$ and $F|K$ is finite. Set $G_F \overset{\text{def}}{=} Gal(L|F)$. Notice that by our assumption this has finite index in $Gal(L|K)$. Then we give a topology on $Gal(L|K)$ letting such G_F form a basis for the neighborhoods of the identity in $Gal(L|K)$. Consider now two fields F_1 and F_2 with the same just mentioned properties of F and such that $F_1 \subseteq F_2$. Then we have natural maps $Gal(F_2|K) \to Gal(F_1|K)$. Hence we get that $Gal(L|K)$ is a profinite group and

$$Gal(L|K) \simeq \varprojlim G/G_F \simeq \varprojlim Gal(F|K)$$

where the limit is taken with respect to: F runs through the normal finite subextensions $F|K$, the order on the indices is given via inclusion and the maps are the natural ones defined above. Thus now we can state the Galois correspondence also for infinite extensions:

Theorem 4.1.1. *Let $L|K$ be a Galois extension. Then the map Φ defined by $\Phi(M) = Gal(L|M)$ is an inclusion-reversing bijection from the set of the intermediate fields of $L|K$ to the set of subgroups of $Gal(L|K)$. Its inverse Φ^{-1} maps each subgroup H to the field K^H of all elements fixed by H.*

Proposition 4.1.2. *Let $L|K$ be a Galois extension and let M be an intermediate field. Then*

- *$Gal(L|M)$ is open in $Gal(L|K)$ if and only if $[M : K]$ is finite. If this is the case then $[Gal(L|K) : Gal(L|M)] = [M : K]$.*
- *$Gal(L|M) \trianglelefteq Gal(L|K)$ if and only if $M|K$ is a Galois extension. If this is the case then the restriction map $Gal(L|K) \to Gal(M|K)$ is surjective and its kernel is $Gal(L|M)$. Consequently*

$$Gal(M|K) \simeq Gal(L|K)/Gal(L|M)$$

One can also show that, as for finite extensions, if $L|K$ is Galois then the action of $Gal(L|K)$ on the primes above $\mathfrak{p}$ is transitive. In other words:

Lemma 4.1.3. *Suppose $L|K$ is a Galois extension and let $\mathfrak{P}$ and $\mathfrak{P}'$ be primes of K lying above $\mathfrak{p}$. Then there exists $\sigma \in Gal(L|K)$ such that $\sigma\mathfrak{P} = \mathfrak{P}'$.*

Similarly to the finite case, one defines

Definition 4.1.1. Let $L|K$ be a Galois extension and let $\mathfrak{P}$ lie above $\mathfrak{p}$. We define the *decomposition group* as

$$D = D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in Gal(L|K) : \sigma\mathfrak{P} = \mathfrak{P}\}$$

Definition 4.1.2. Let $L|K$ be a Galois extension and let $\mathfrak{P}$ lie above $\mathfrak{p}$. We define the *inertia group* as

$$I = I(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) : \sigma(\alpha) \equiv \alpha \mod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\}$$

Remark 28.

- It can be shown also that D is a closed group of $Gal(L|K)$ and moreover I is a closed group of D itself.
- As in the finite case, we still have the exact sequence

$$1 \to I \to D \to Gal((\mathcal{O}_L/\mathfrak{P})|(\mathcal{O}_K|\mathfrak{p})) \to 1$$

Now assume for the moment that the extension $L|K$ is just algebraic, that $\mathbb{Q} \subseteq K$ and let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Then clearly $\overline{\mathbb{Q}}|L$ and $\overline{\mathbb{Q}}|K$ are Galois extensions. As usual, let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ that lies above a prime $\mathfrak{p}$ of $\mathcal{O}_K$. Choose a prime ideal $\mathfrak{Q}$ of $\mathcal{O}_{\overline{\mathbb{Q}}}$ lying above $\mathfrak{P}$. We obtain

$$I(\mathfrak{Q}|\mathfrak{p}) \subseteq Gal(\overline{\mathbb{Q}}|K)$$
$$I(\mathfrak{Q}|\mathfrak{P}) \subseteq Gal(\overline{\mathbb{Q}}|L) \subseteq Gal(\overline{\mathbb{Q}}|K)$$
$$I(\mathfrak{Q}|\mathfrak{P}) = I(\mathfrak{Q}|\mathfrak{p}) \cap Gal(\overline{\mathbb{Q}}|L)$$

These observations allow us to define the *ramification index* as

$$e(\mathfrak{P}|\mathfrak{p}) = [I(\mathfrak{Q}|\mathfrak{p}) : I(\mathfrak{Q}|\mathfrak{P})]$$

which clearly could be infinite.

If $\mathfrak{Q}'$ is another prime lying above $\mathfrak{P}$ then by lemma 4.1.1 there exists some $\sigma \in Gal(\overline{\mathbb{Q}})$ such that $\mathfrak{Q}' = \sigma\mathfrak{Q}$. Moreover one has

$$I(\mathfrak{Q}'|\mathfrak{p}) = \sigma I(\mathfrak{Q}|\mathfrak{p})\sigma^{-1}$$
$$I(\mathfrak{Q}'|\mathfrak{P}) = \sigma I(\mathfrak{Q}|\mathfrak{P})\sigma^{-1}$$

Therefore, the ramification index $e(\mathfrak{P}|\mathfrak{p})$ does not depend on the choice of $\mathfrak{Q}$. This shows also that if the extension $L|K$ is abelian, then the definition of inertia group does not depend on the particular prime above $\mathfrak{p}$. Similarly, one finds that this last fact holds also for the definition of decomposition group.

Now re-add the hypothesis that the extension $L|K$ is Galois. Then there is a natural restriction map

$$Gal(\overline{\mathbb{Q}}|K) \to Gal(L|K)$$

with kernel equal to $Gal(\overline{\mathbb{Q}}|K)$. Furthermore, one can show that the induced map $I(\mathfrak{Q}|\mathfrak{p}) \to I(\mathfrak{P}|\mathfrak{p})$ is surjective, with kernel equal to $I(\mathfrak{Q}|\mathfrak{P})$. Hence we deduce

$$I(\mathfrak{Q}|\mathfrak{p})/I(\mathfrak{Q}|\mathfrak{P}) \simeq I(\mathfrak{P}|\mathfrak{p})$$

and so

$$e(\mathfrak{P}|\mathfrak{p}) = |I(\mathfrak{P}|\mathfrak{p})|$$

.

Clearly this is coherent with the definitions given in the finite case.

Remark 29. Let $L|K$ be a Galois extension and let $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Notice that by the definition of the decomposition group and the transitive action of $Gal(L|K)$ follows that the numbers of prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}$ is equal to $[Gal(L|K) : D(\mathfrak{P}|\mathfrak{p})]$, which clearly can be infinite and does not depend on the prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$.

Now we give some definitions that will generalize the ones for the finite case.

Definition 4.1.3. Let $L|K$ be a Galois extension and let $\mathfrak{p}$ a prime of $\mathcal{O}_K$. We say that:

- $L|K$ is *ramified at* $\mathfrak{p}$ if there exists a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$ such that $I(\mathfrak{P}|\mathfrak{p}) \neq \{1\}$.
- $L|K$ is *unramified at* $\mathfrak{p}$ if for every prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$ one has $I(\mathfrak{P}|\mathfrak{p}) = \{1\}$.
- $L|K$ is *unramified* if the extension is unramified at every prime of $\mathcal{O}_K$.
- $L|K$ is *totally ramified at* $\mathfrak{p}$ if there exists a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$ such that $I(\mathfrak{P}|\mathfrak{p}) = Gal(L|K)$.
- $L|K$ is *totally ramified* if every prime in $\mathcal{O}_K$ is totally ramified in $L|K$.

Remark 30. One can prove that $\mathfrak{p}$ is unramified or totally ramified if so is in every finite normal subextension $F|K$ with $K \subseteq F \subseteq L$.

We conclude the section with a couple of easy lemmas that will play an important role during the proof of the Iwasawa's theorem. The first follows just by definition of inertia group and arguing by double inclusion. The second one is a consequence of the Galois correspondence.

Lemma 4.1.4. *Let $L|K$ and $M|K$ be Galois extensions with $M \subseteq L$. Suppose that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_L$. Then*

$$I_{L|M}(\mathfrak{p}|\mathfrak{p} \cap \mathcal{O}_M) = I_{L|K}(\mathfrak{p}|\mathfrak{p} \cap \mathcal{O}_K) \cap Gal(L|M)$$

Lemma 4.1.5. *Let $L|K$ and $M|K$ be finite Galois extensions. Then*

$$Gal(LM|M) \simeq Gal(L|L \cap M).$$

4.2 Iwasawa's theorem

Definition 4.2.1. A *$\mathbb{Z}_p$-extension* of a number field K is a Galois extension $K_\infty|K$ such that $Gal(K_\infty|K) \simeq (\mathbb{Z}_p, +)$.

Proposition 4.2.1. *Let $K_\infty|K$ be a $\mathbb{Z}_p$-extension. Then, for each $n \geq 0$, there is a unique field K_n of degree p^n over K, and these K_n, plus K_∞, are the only fields between K and K_∞.*

Proof. By infinite Galois theory and by the definition of $\mathbb{Z}_p$-extension, we know that the intermediate fields of $K_\infty|K$ correspond to the closed subgroups of $\mathbb{Z}_p$. By lemma 3.1.3, we know that they have the form $p^n\mathbb{Z}_p$ for some n. Since $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$, by the correspondence of Galois theory we can conclude the proof.

□

The consequence of the previous proposition is that to give a $\mathbb{Z}_p$-extension $K_\infty|K$ is the same to give a sequence of fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_\infty = \bigcup_{n\geq 0} K_n$$

such that $Gal(K_n|K) \simeq \mathbb{Z}/p^n\mathbb{Z}$ for every $n \geq 0$.

Remark 31. Every number field K has at least one particular $\mathbb{Z}_p$-extension, called *the cyclotomic $\mathbb{Z}_p$-extension* of K. Indeed, let p be an odd prime and set $q = p$ if p is odd or $q = 4$ otherwise. Then notice that we have an isomorphism $(\mathbb{Z}/qp^n\mathbb{Z})^\times \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times$ (cyclic group of order p^n). Thus for every $n \geq 1$ there exists a unique (unless $p = 2$ and $n = 1$) subfield of $\mathbb{Q}(\zeta_{qp^n})$ which is cyclic of degree p^n over $\mathbb{Q}$ (it is the fixed field by $(\mathbb{Z}/q\mathbb{Z})^\times$). Call them $\mathbb{B}_n$ for every $n \geq 1$. Therefore setting $\mathbb{B}_0 = \mathbb{Q}$ and $\mathbb{B}_\infty = \bigcup_{n\geq 0} \mathbb{B}_n$ we deduce that $\mathbb{B}_\infty|\mathbb{Q}$ is a $\mathbb{Z}_p$-extension. Now let K be any number field and let $K_\infty = K\mathbb{B}_\infty$. We now prove that $K_\infty|K$ is a $\mathbb{Z}_p$-extension. Say that $e \geq 0$ is such that $\mathbb{B}_e = K \cap \mathbb{B}_\infty$. Thus, by lemma 4.1.5 we have $Gal(K_\infty|K) \simeq Gal(\mathbb{B}_\infty|\mathbb{B}_\infty \cap K) \simeq p^e\mathbb{Z}_p \simeq \mathbb{Z}_p$, as we wanted. Moreover notice that if K contains $\mathbb{Q}(\zeta_q)$ then the extension is obtained by simply adjoining all p^n-th roots of unity for all $n \geq 1$.

Example 9. Let p be an odd prime. The most important example of $\mathbb{Z}_p$-extension for us is $\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q}(\zeta_p)$ where $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n\geq 0} \mathbb{Q}(\zeta_{p^{n+1}})$ (this is actually the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\zeta_p)$ by the above remark).

The following proposition will play an important role for proving the Iwasawa's theorem. The arguments involved to prove it are completely about class field theory, so we decided to omit the proof. For the details, see [**Wa**] or [**Lan1**].

Proposition 4.2.2. *Let $K_\infty|K$ be a $\mathbb{Z}_p$-extension and let $\widetilde{l}$ be a prime of K (finite or infinite) which does not lie above p. Then $K_\infty|K$ is unramified at $\widetilde{l}$.*

The meaning of the previous proposition is that $\mathbb{Z}_p$-extensions are "unramified outside p".

Lemma 4.2.3. *Let $K_\infty|K$ be a $\mathbb{Z}_p$-extension. At least one prime ramifies in this extension, and there exists $n \geq 0$ such that every prime which ramifies in $K_\infty|K_n$ is totally ramified.*

Proof. By a classical result in algebraic number theory (see [**Sam**] for example) we know that the class number of K is finite. This implies that also the maximal abelian unramified extension H of K is finite since by class field theory we know that $Gal(H|K) \simeq Cl(K)$. Hence since $K_\infty|K$ is an infinite extension, we can deduce that at least one prime ramifies in $K_\infty|K$. By the previous proposition, we get that the only primes that may ramify are those of K above p. We know that there are only finitely many such primes since K is a number field and we call them $\mathfrak{p}_1, ..., \mathfrak{p}_s$. Let $I_1, ..., I_s$ be the corresponding inertia groups for the extension $K_\infty|K$. These are closed subgroups of $Gal(K_\infty|K) = \mathbb{Z}_p$ and so also $\bigcap_{j=1}^s I_j$ is closed. Thus there exists $n \geq 0$ such that $\bigcap_{j=1}^s I_j = p^n\mathbb{Z}_p$. Now the corresponding Galois group is $Gal(K_\infty|K_n) = p^n\mathbb{Z}_p$ which is clearly contained in each inertia group I_j. We have to show that this implies that all the primes of K_n above $\mathfrak{p}_j$ are totally ramified. Fix a j and let $\mathfrak{P}$ a prime above $\mathfrak{p}_j$ and consider its inertia group $I_{K_\infty|K_n}$ for the extension $K_\infty|K_n$. Notice that

$$I_{K_\infty|K_n} = I_j \cap Gal(K_\infty|K_n) = Gal(K_\infty|K_n)$$

where the first equality holds since in this cases the Galois groups are abelian and the second one because $Gal(K_\infty|K_n) \subseteq I_j$. Therefore, we have just show that all the primes of K_n above each $\mathfrak{p}_j$ are totally ramified in $K_\infty|K_n$. Noticing that a prime of K_n that ramifies in $K_\infty|K_n$ is necessary above some $\mathfrak{p}_j$, we can conclude the proof. □

We are now arrived to the most important result of this chapter. Given a $\mathbb{Z}_p$-extension $K_\infty|K$, denote by $\Gamma = Gal(K_\infty|K) \simeq \mathbb{Z}_p$ and let γ_0 be a topological generator of Γ. Let L_n be the maximal unramified abelian p-extension of K_n and let A_n = p-Sylow of the ideal class group of K_n. Moreover let $L_\infty = \bigcup_{n\geq 0} L_n$, $X_n = Gal(L_n|K_n)$ and $X = Gal(L_\infty|K_\infty)$.

Theorem 4.2.4 (Iwasawa's theorem)**.** *Let $K_\infty|K$ be a $\mathbb{Z}_p$-extension. Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exist integers $\lambda \geq 0, \mu \geq 0$ and ν, all independent of n, and an integer n_0 such that*

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

for all $n \geq n_0$.

Proof. First of all notice that by our notation and by class field theory we have that $X_n \simeq A_n$ (look at [**Sa2**] and [**Sa3**]). More precisely, for $m > n$ we have a commutative diagram:

$$\begin{tikzcd} A_m \arrow[r, "\simeq"] \arrow[d, "N"] & X_m \arrow[d, "\iota"] \\ A_n \arrow[r, "\simeq"] & X_n \end{tikzcd}$$

where N is the norm map and ι is defined by $\sigma \mapsto \sigma \restriction_{L_n}$. Moreover, each L_n is Galois over K since L_n is maximal and so $L_\infty|K$ is a Galois extension too. Let $G \overset{\text{def}}{=} Gal(L_\infty|K)$. Now we are going to make some observations and to prove some statements under a further assumption that we will be able to remove at a certain point thanks to lemma 4.2.3.

Iwasawa's assumption: All primes which are ramified in $K_\infty|K$ are totally ramified.

By this assumption, notice that for every n we get $K_{n+1} \cap L_n = K_n$. Indeed, as we discussed before, since by class field theory the maximal unramified abelian extension is finite, we must have a prime $\mathfrak{p}$ of K that ramifies in $K_\infty|K$. The assumption implies that $\mathfrak{p}$ is totally ramified in $K_\infty|K$ and then by remark 30 so is in any finite subextension $F|K$ with $K \subseteq F \subseteq K_\infty$. From this we deduce that $\mathfrak{p}$ totally ramifies also in the abelian extension $(K_{n+1} \cap L_n)|K$. Now let $\mathfrak{P}$ a prime of K_n lying over $\mathfrak{p}$. Denote by $I(\mathfrak{P})$ the inertia group of $\mathfrak{p}$ for the extension $(K_{n+1} \cap L_n)|K_n$ and by $I(\mathfrak{p})$ the inertia group of $\mathfrak{p}$ for the extension $(L_n \cap K_{n+1})|K$. Since $I(\mathfrak{P}) = I(\mathfrak{q}) \cap Gal((K_{n+1} \cap L_n)|K_n)$ we deduce that $\mathfrak{P}$ is totally ramified too in the extension $(K_{n+1} \cap L_n)|K_n$. However, $L_n|K_n$ is unramified and so also $(K_{n+1} \cap L_n)|K_n$ must be unramified. This is impossible unless $L_n \cap K_{n+1} = K_n$.

Using lemma 4.1.5, we obtain that $Gal(L_nK_{n+1}|K_{n+1}) \simeq Gal(L_n|L_n \cap K_{n+1}) = Gal(L_n|K_n)$, which is isomorphic to a quotient of X_{n+1} by Galois theory. Notice that to the norm map $A_{n+1} \to A_n$ corresponds a natural map $X_{n+1} \to X_n$ and moreover we have $X_n \simeq Gal(L_nK_\infty|K_\infty)$. Hence

$$\varprojlim_n X_n = \varprojlim_n Gal(L_n|K_n) \simeq \varprojlim_n Gal(L_nK_\infty|K_\infty) \simeq$$
$$\simeq Gal((\bigcup L_nK_\infty)|K_\infty) = Gal(L_\infty|K_\infty) = X$$

Now recall that $\Gamma_n = \Gamma/\Gamma^{p^n} \simeq \mathbb{Z}/p^n\mathbb{Z} \simeq Gal(K_n|K)$. Then if we consider $\gamma_n \in \Gamma_n$ it makes sense to extend it to an element $\widetilde{\gamma_n} \in Gal(L_n|K)$. Let $x_n \in X_n$. Then there is an action of γ_n on x_n given by

$$x_n^{\gamma_n} \overset{\text{def}}{=} \widetilde{\gamma_n} x_n \widetilde{\gamma_n}^{-1}.$$

Since $Gal(L_n|K_n)$ is abelian, $x_n^{\gamma_n}$ is well defined (moreover this action corresponds to the one on A_n). Hence we get that X_n is a $\mathbb{Z}_p[\Gamma_n]$-module. Moreover since an element of $X \simeq \varprojlim X_n$ may be viewed as a vector of the form $(x_0, x_1, ...)$ we can make $\mathbb{Z}_p[\Gamma_n]$ acting on the n-th component for every n, so that X becomes a Λ-module. Observe that using the isomorphism $\Lambda \simeq \mathbb{Z}_p[|T|]$ we obtain that $1 + T$ acts as $\gamma_0 \in \Gamma$. In particular one has that

$$x^\gamma = \widetilde{\gamma} x \widetilde{\gamma}^{-1}, \text{ for } \gamma \in \Gamma, x \in X.$$

where $\widetilde{\gamma}$ is an extension of γ to G.

Let $\mathfrak{p}_1, ..., \mathfrak{p}_s$ be the primes which ramify in $K_\infty|K$ and fix a prime $\widetilde{\mathfrak{p}_i}$ of L_∞ lying over $\mathfrak{p}_i$. Let $I_i \subseteq G$ be its inertia group. Since $L_\infty|K_\infty$ is an unramified extension, we obtain that $I_i \cap X = 1$. This implies that we have an injection $I_i \hookrightarrow G/X \simeq \Gamma$. On the other hand, since $K_\infty|K$ is totally ramified at $\mathfrak{p}_i$, we obtain that the map above is surjective too, and so is an isomorphism. Hence we deduce that

$$G = I_i X = X I_i \text{ for } i = 1, ..., s.$$

Now let $\sigma_i \in I_i$ such that it maps to γ_0 under the above bijection. Then σ_1 must be a topological generator of I_i. Using that $G = XI_1$ we have $I_i \subseteq XI_1$ for $i = 1, ..., s$. Therefore we get $\sigma_i = a_i\sigma_1$ for some $a_i \in X$. In particular notice that $a_1 = 1$.

Remark 32. Notice that the isomorphism $\mathbb{Z}_p \simeq \Gamma$ may be written as $x \mapsto \gamma_0^x$ with $x \in \mathbb{Z}_p$. This is how we are going to think of the isomorphism from now on. If we define $(1 + T)^x \overset{\text{def}}{=} \sum_{n=0}^{\infty} \binom{c}{n} T^n$, where the binomial has been discussed in chapter 2, one can prove that γ_0^x corresponds to $(1 + T)^x$ under the isomorphism of theorem 3.2.6. This fact will be used in the next lemma.

Lemma 4.2.5. *Suppose that the Iwasawa's assumption holds. Then*

$$[G, G] = X^{\gamma_0 - 1} = TX$$

Proof. Since $\Gamma \simeq I_1 \subseteq G$ maps onto $\Gamma \simeq G/X$, we identify Γ with I_1 and define the action of Γ on X via this identification, so that $x^\gamma = \gamma x \gamma^{-1}$. Consider now $g_1, g_2 \in G$. Recalling that $G = \Gamma X$, there are $\gamma_1, \gamma_2 \in \Gamma$ and $x_1, x_2 \in X$ such that $g_1 = \gamma_1 x_1$ and $g_2 = \gamma_2 x_2$. Using the fact that Γ is abelian we get that

$$\begin{aligned} g_1 g_2 g_1^{-1} g_2^{-1} &= \gamma_1 x_1 \gamma_2 x_2 x_1^{-1} \gamma_1^{-1} x_2^{-1} \gamma_2^{-1} = \\ &= x_1^{\gamma_1} \gamma_1 \gamma_2 x_2 x_1^{-1} \gamma_1^{-1} x_2^{-1} \gamma_2^{-1} = x_1^{\gamma_1} (x_2 x_1^{-1})^{\gamma_1 \gamma_2} (x_2^{-1})^{\gamma_2} \end{aligned}$$

Using also that X is abelian we obtain

$$\begin{aligned} x_1^{(1-\gamma_2)\gamma_1} x_2^{(\gamma_1 - 1)\gamma_2} &= (\gamma_1 x_1 \gamma_1^{-1})^{(1-\gamma_2)} (\gamma_2 x_2 \gamma_2^{-1})^{(\gamma_1 - 1)} = \\ &= \gamma_1 x_1 \gamma_1^{-1} \gamma_2 \gamma_1 x_1^{-1} \gamma_1^{-1} \gamma_2^{-1} \gamma_1 \gamma_2 x_2 \gamma_2^{-1} \gamma_1^{-1} \gamma_2 x_2^{-1} \gamma_2^{-1} = \\ &= x_1^{\gamma_1} (x_2 x_1^{-1})^{\gamma_1 \gamma_2} (x_2^{-1})^{\gamma_2} \end{aligned}$$

Putting altogether one has

$$g_1 g_2 g_1^{-1} g_2^{-1} = x_1^{(1-\gamma_2)\gamma_1} x_2^{(\gamma_1 - 1)\gamma_2}$$

In particular, setting $\gamma_2 = 1$ and $\gamma_1 = \gamma_0$, we find that $x_2^{(\gamma_0 - 1)} \in [G, G]$. Hence $X^{(\gamma_0 - 1)} \subseteq [G, G]$.

Now let $\gamma \in \Gamma$ be arbitrary. By the previous remark, there must be $c \in \mathbb{Z}_p$ such that $\gamma = \gamma_0^c$. Moreover, remark implies also that

$$1 - \gamma = 1 - \gamma_0^c = 1 - (1 + T)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Lambda.$$

In particular we obtain that $x_1^{(1-\gamma_2)\gamma_1} \in X^{(\gamma_0 - 1)}$ and $x_2^{(1-\gamma_1)\gamma_2} \in X^{(\gamma_0 - 1)}$. Therefore $[G, G] \subseteq X^{(\gamma_0 - 1)}$. This concludes the proof. □

Remark 33. Notice that TX is closed since it is the image of the compact set X. This implies that also $[G, G]$ is closed.

Lemma 4.2.6. *Suppose again that the Iwasawa's assumption holds. Let Y_0 be the $\mathbb{Z}_p$-submodule of X generated by $\{a_i : 2 \leq i \leq s\}$ and by $X^{\gamma_0-1} = TX$. Let $Y_n \overset{\text{def}}{=} \nu_n Y_0 \overset{\text{def}}{=} Y_0^{\nu_n}$, where*

$$\nu_n \overset{\text{def}}{=} 1 + \gamma_0 + \gamma_0^2 + \ldots + \gamma_0^{p^n-1} = \frac{\gamma_0^{p^n} - 1}{\gamma_0 - 1} = \frac{(1+T)^{p^n} - 1}{T}$$

Then we have $X_n \simeq X/Y_n$ for $n \geq 0$.

Proof. **Notation:** In this proof, if M is a submodule of X, we will write $\nu_n M$ to indicate M^{ν_n}.

First of all consider $n = 0$. We have $K \subseteq L_0 \subseteq L_\infty$ and moreover L_0 is the maximal abelian unramified p-extension of K. Since $L|K$ is a p-extension too, then $L_0|K$ is the maximal unramified abelian p-subextension of $L|K$. Therefore $Gal(L_\infty|L_0)$ must be the closed subgroup of G generated by $\overline{[G, G]}$ and all the inertia groups I_i for $1 \leq i \leq s$. In particular we have that $Gal(L_\infty|L_0)$ is the closure of the group generated by X^{γ_0-1}, I_1, and $a_2, \ldots, a_s$. Thus

$$\begin{aligned} X_0 = Gal(L_0|K) = G/Gal(L_\infty|L_0) = XI_1/\overline{\langle X^{(\gamma_0-1)}, a_2, \ldots, a_s, I_1\rangle} \simeq \\ \simeq X/\overline{\langle X^{(\gamma_0-1)}, a_2, \ldots, a_s\rangle} = X/Y_0 \end{aligned}$$

This concludes the case $n = 0$.

Now, suppose that $n \geq 1$. The idea is to argue as above. Replace K by K_n and so γ_0 is replaced by $\gamma_0^{p^n}$ because $Gal(K_\infty|K_n) \simeq \Gamma^{p^n}$. In particular, this makes σ_1 become $\sigma_i^{p^n}$. Observe that

$$\begin{aligned} \sigma_i^{k+1} &= (a_i\sigma_1)^{k+1} = a_i\sigma_1 a_i \sigma_1^{-1}\sigma_1^2 a_i \sigma_1^{-2} \cdots \sigma_1^k a_i \sigma_1^{-k}\sigma_1^{k+1} = \\ &= a_i^{1+\sigma_1+\ldots+\sigma_1^k}\sigma_1^{k+1} \end{aligned}$$

Therefore we get $\sigma_i^{p^n} = (\nu_n a_i)\sigma_1^{p^n}$, so we need to replace a_i by $\nu_n a_i$. Finally, we replace X^{γ_0-1} by $X^{(\gamma_0^{p^n}-1)} = \nu_n X^{(\gamma_0-1)}$. Therefore Y_0 becomes $\nu_n Y_0 = Y_n$. This completes the proof.

□

The above result will play a key role since it allows us to recover information about X_n from information about X.

Lemma 4.2.7 (Nakayama's Lemma for compact Λ-modules)**.** *Let M be a compact Λ-module. Then the following are equivalent:*

(1) M is a finitely generated Λ-module

(2) M/TM is a finitely generated $\mathbb{Z}_p$-module

(3) $M/(p, T)M$ is a finitely dimensional $\mathbb{F}_p$-vector space

Proof. Notice that passing to the proper quotients we deduce immediately the implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3). Thus we assume (3) and we now prove (1). let U be a neighborhood of 0 in M. Since $(p,T)^n \to 0$ in Λ, each $x \in M$ has a neighborhood U_x such that $(p,T)^{n_x} U_x \subseteq U$ for some n_x (we shrink U if necessary). Since M is compact it follows that we can find finitely many U_x's covering M. Therefore $(p,T)^n M \subseteq U$ for a large n. This implies that $\bigcap_m ((p,T)^m M) = 0$ for *any* compact Λ-module M. Now by hypothesis, there exist elements $m_1, \dots, m_n \in M$ whose residue classes generate $M/(p,T)M$ as $\mathbb{F}_p$-vector space. Consider then the compact Λ-module $N \overset{\text{def}}{=} \Lambda m_1 + \dots + \Lambda m_n \subseteq M$ (it is the image of Λ^n). We have that $M = N + (p,T)M$ and so

$$\frac{M}{N} = \frac{N + (p,T)M}{N} = (p,T)\frac{M}{N}$$

Iterating this equality we get that $M/N = (p,T)^k M/N$ for all $k > 0$. Notice that N is also closed and so M/N is a compact Λ-module. Therefore we can apply the above argument to deduce that $M/N = \bigcap_m (p,T)^m M/N = 0$, i.e. $M = N$. Since N is a finitely generated Λ-module by definition, this concludes the proof. □

We state as a corollary the following trivial (but interesting) consequence:

Corollary 4.2.8. *Let M be a compact Λ-module. Then $M = 0 \Leftrightarrow M/TM = 0 \Leftrightarrow M/(p,T)M = 0$.*

Lemma 4.2.9. *Continue to assume that the Iwasawa's assumption holds. Then $X = Gal(L_\infty|K_\infty)$ is a finitely generated Λ-module.*

Proof. Clearly $\nu_1 = \frac{(1+T)^p - 1}{T} \in (p,T)$ and so $Y_0/(p,T)Y_0$ is isomorphic to a quotient of $Y_0/\nu_1 Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$. We know that X_1 is a finite set and so we deduce that also $Y_0/(p,T)Y_0$ is finite. By the previous lemma, it follows that Y_0 is finitely generated. Since $X/Y_0 = X_0$ is finite, this implies that X must be finitely generated too. This concludes the proof.

□

Removing the Iwasawa's assumption: Now we indicate how to remove the Iwasawa's assumption wlog. Let $K_\infty|K$ be a $\mathbb{Z}_p$-extension. By lemma 4.2.3 we can choose $e \geq 0$ such that in $K_\infty|K_e$ all ramified primes are totally ramified. Then lemmas 4.2.6 and 4.2.9 apply to $K_\infty|K_e$. In particular X, which is the same for K_e and K, is a finitely generated Λ-module. For $n \geq e$, noticing that $Gal(K_\infty|K_e) \simeq \Gamma^{p^e}$ is generated by $\gamma_0^{p^e}$, we replace ν_n by $\nu_{n,e}$ where

$$\nu_{n,e} \overset{\text{def}}{=} \frac{\nu_n}{\nu_e} = 1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \dots + \gamma_0^{p^n - p^e}.$$

Let Y_e replace Y_0 in lemma 4.2.6. Then we get

$$Y_n = \nu_{n,e} Y_e, \text{ and } X_n \simeq X/Y_n \text{ for } n \geq e.$$

Notice that with these observations we have proved the following

Lemma 4.2.10. *Let $K_\infty|K$ be a $\mathbb{Z}_p$-extension. Then X is a finitely generated Λ-module, and there exists $e \geq 0$ such that*

$$X_n \simeq X/\nu_{n,e} Y_e \textit{ for all } n \geq e.$$

We can now apply theorem 3.3.13 to X. We can also apply it to Y_e with the same answer, since X/Y_e is finite and the theorem is given in terms of pseudo-isomorphisms. So we have

$$Y_e \sim X \sim \Lambda^r \oplus (\bigoplus \Lambda/(p^{k_i})) \oplus (\bigoplus \Lambda/(f_j(T)^{m_j})).$$

Now we want to study the summands that appear on the right side. In particular, our next step is to compute $M/\nu_{n,e}M$ for each summand M on the RHS. Doing this, we will be able to obtain the desired bounds on $|X_n|$.

1. Consider $M = \Lambda$. Notice that $\nu_{n,e}$ is not a unit in Λ since it is a distinguished polynomial. By lemma 3.2.10, we know that $\Lambda/(\nu_{n,e})$ is infinite. Since $Y_e/\nu_{n,e}Y_e$ is finite, it follows that Λ does not occur as a summand, i.e. $r = 0$.

2. Consider $M = \Lambda/(p^k)$ with $k > 0$. In this case, we have $M/\nu_{n,e}M \simeq \Lambda/(p^k, \nu_{n,e})$. One can show that if the ratio of two distinguished polynomials is a polynomial, then it is distinguished or constant. Therefore

$$\nu_{n,e} = \frac{\nu_n}{\nu_e} = \frac{((1+T)^{p^n} - 1)/T}{((1+T)^{p^e} - 1)/T}$$

is distinguished. Applying the division algorithm, one finds that every element of $\Lambda/(p^k, \nu_{n,e})$ is represented uniquely by a polynomial $\mod p^k$ of degree less than $deg(\nu_{n,e}) = p^n - p^e$. Hence

$$|M/\nu_{n,e}M| = p^k(p^n - p^e) = p^{kp^n + c},$$

where $c = -kp^e$ is a constant depending on K.

3. Consider $M = \Lambda/(f(T)^m)$ and let $g(T) \overset{\text{def}}{=} f(T)^m$. Say that g has degree d. Since f is distinguished, so is g. Thus

$$T^d \equiv p \cdot (poly) \mod g$$

where by $'poly'$, we mean a polynomial. In what follows, we are going to use the term $'poly'$ not necessarily to indicate the same polynomial at each step. Therefore

$$T^k \equiv (p) \cdot (poly) \mod g \text{ for } k \geq d.$$

If $p^n \geq d$ then

$$(1+T)^{p^n} = 1 + (p) \cdot (poly) + T^{p^n} \equiv 1 + (p) \cdot (poly) \mod g.$$

In particular notice that

$$\begin{aligned}(1+T)^{p^{n+1}} &= ((1+T)^{p^n})^p \equiv (1+p\cdot(poly))^p \mod g \equiv \\ &\equiv 1+p^2\cdot(poly) \mod g\end{aligned}$$

Now for every $n \in \mathbb{N}$ set $P_n(T) \overset{\text{def}}{=} (1+T)^{p^n} - 1$. It follows that

$$\begin{aligned}P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 = ((1+T)^{p^{n+1}} - 1)(1 + (1+T)^{p^{n+1}} + \ldots + (1+T)^{p^{n+1}(p-1)}) = \\ &= P_{n+1}(T)(1 + (1+T)^{p^{n+1}} + \ldots + (1+T)^{p^{n+1}(p-1)} \equiv \\ &\equiv P_{n+1}(T)(1 + \ldots + 1 + p^2\cdot(poly) \mod g \equiv \\ &\equiv P_{n+1}(T)(p + p^2\cdot(poly)) \mod g \equiv p(1+p\cdot(poly))P_{n+1}(T) \mod g\end{aligned}$$

Since $1 + (p)(polynomial) \in \Lambda^\times$, we see that

$$\tfrac{P_{n+2}}{P_{n+1}} \text{ acts on } \Lambda/(g) \text{ as } (p)\cdot(unit)$$

as long as $p^n \geq d$.
Now assume that $n_0 > e, p^{n_0} \geq d$, and $n \geq n_0$. Then

$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}}{P_{n+1}}$$

and so

$$\nu_{n+2,e}M = \frac{P_{n+2}}{P_{n+1}}(\nu_{n+1,e}M) = p\nu_{n+1,e}M$$

Therefore

$$|M/\nu_{n+2,e}M| = |M/pM|\cdot|pM/p\nu_{n+1,e}M|$$

for $n \geq n_0$. Now since g is a distinguished polynomial, we have $(g,p) = 1$. This implies that multiplication by p is injective, so that

$$|pM/p\nu_{n+1,e}M| = |M/\nu_{n+1,e}M|$$

Since $M/pM \simeq \Lambda/(p,g) = \Lambda/(p,T^d)$, we obtain $|M/pM| = p^d$. By induction, one finds that

$$|M/\nu_{n,e}M| = p^{d(n-n_0-1)}\cdot|M/\nu_{n_0+1,e}M|$$

for $n \geq n_0{+}1$. Therefore, if $|M/\nu_{n,e}M|$ is finite for all n, then we get $|M/\nu_{n,.e}M| = p^{dn+c}$ for some constant c depending on K and $n \geq n_0+1$. If $M/\nu_{n,e}M$ is infinite for some n, then M cannot occur as summand on the RHS, as observed in the first case, because this happens only when $(\nu_{n,e}, f) \neq 1$ by lemma 3.2.10.

Putting all these observations together, we deduce the following

Proposition 4.2.11. *Suppose that*

$$E \overset{\text{def}}{=} \Lambda^r \oplus (\textstyle\bigoplus_{i=1}^s \Lambda/(p^{k_i})) \oplus (\bigoplus_{j=1}^t \Lambda/(g_j(T))),$$

where each $g_j(T)$ is distinguished. Let $m = \sum_i k_i$ and $l = \sum_j deg(g_j)$. If $E/\nu_{n,e}E$ is finite for all n, then $r = 0$ and there exist n_0 and c such that

$$|E/\nu_{n,e}E| = p^{mp^n+nl+c}$$

for all $n > n_0$.

Now consider E as in the previous proposition. Then we saw that $Y_e \sim E$ and so, equivalently, we have an exact sequence

$$0 \to A \to Y_e \to E \to B \to 0$$

where A and B are finite Λ-modules. We know the cardinality of $E/\nu_{n,e}E$ for all $n > n_0$. It remains to obtain similar information for Y_e. At the moment, we only know that $E_n = mp^n + nl + c_n$ where c_n is bounded. The following lemma solves this problem. The proof is not particularly enlightning, so we decided to omit it. The main idea is that it follows by applying the Snake lemma to the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \nu_{n,e}Y \arrow[r] \arrow[d] & Y \arrow[r] \arrow[d] & Y/\nu_{n,e}Y \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \nu_{n,e}E \arrow[r] & E \arrow[r] & E/\nu_{n,e}E \arrow[r] & 0
\end{tikzcd}$$

Lemma 4.2.12. *Suppose Y and E are Λ-modules with $Y \sim E$ such that $Y/\nu_{n,e}Y$ is finite for all $n \geq e$. Then, for some constant c and some n_0 we have*

$$|Y/\nu_{n,e}Y| = p^c \cdot |E/\nu_{n,e}E|$$

for all $n \geq n_0$.

Therefore, considering this lemma and E as in the previous proposition, we deduce that there exist integers $n_0, \nu, \lambda \geq 0$ and $\mu \geq 0$ such that

$$p^{e_n} = |X_n| = |X/Y_e| \cdot |Y_e/\nu_{n,e}Y_e| = (constant) \cdot |E/\nu_{n,e}E| = p^{\lambda n+\mu p^n+\nu}$$

for all $n > n_0$.
This concludes the proof of Iwasawa's theorem. □

Remark 34. An important fact that can be shown in detail, is that λ and μ actually are such that $\lambda = \lambda(X)$, $\mu = \mu(X)$. This can be found in [**Neu2**] and it will be used later.

Now we look immediately at a consequence that will be useful later.

Corollary 4.2.13. *Suppose $K_\infty|K$ is a $\mathbb{Z}_p$-extension in which exactly one prime is ramified, and assume it is totally ramified. Then*

$$A_n \simeq X_n \simeq X/((1+T)^{p^n} - 1)X$$

Moreover, $p \nmid h_0$ if and only if $p \nmid h_n$ for all $n \geq 0$.

Proof. Since $K_\infty|K$ satisfies the Iwasawa's assumption, we can apply lemma 4.2.6. We obtain $s = 1$, and so $Y_0 = TX$. Thus

$$Y_n = \nu_n TX = (\tfrac{(1+T)^{p^n}-1)}{T} TX$$

This proves the first part.

For the second one, if $p \nmid h_0$, then $X_0 = 0$, namely $X/TX = 0$. This implies also that $X/(p,T)X = 0$. By Nakayama's lemma 4.2.7, we get $X = 0$. Thus we can conclude. □

Even if we have already proved using explicitly the topological Nakayama's lemma that X is a finitely generated Λ-module, it can be proved that it is also a torsion module using the following more algebraic lemma. A proof can be found in [**Sa3**].

Lemma 4.2.14. *Let $\mathfrak{m}$ be the maximal ideal of Λ. Let M be a profinite Λ-module, i.e. a Λ-module of the form $M = \varprojlim_i M_i$ where M_i is a finite Λ-module and the canonical maps $M \to M_i$ are surjective for every i. Moreover, suppose that for some element $f \in \mathfrak{m}$ we have that M/fM is a finite Λ-module. Then M is a finitely generated torsion Λ-module.*

Corollary 4.2.15. *Let X be as above. Then X is a finitely generated torsion Λ-module.*

Proof. Once again, given our $\mathbb{Z}_p$-extension $K_\infty|K$, we choose $e \geq 0$ such that in $K_\infty|K_e$ all ramified primes are totally ramified. Moreover we fix $n \geq e$. Since we have $X \simeq Gal(L_\infty|K_\infty)$ and $A_n \simeq Gal(L_n|K_n) \simeq Gal(L_nK_\infty|K_\infty)$ we deduce that the natural map $X \to A_n$ is surjective. Let $\widetilde{Y_n} \overset{\text{def}}{=} Ker(X \to A_n)$. As above, let γ_0 be a generator of $\Gamma = Gal(K_\infty|K_n)$ as a $\mathbb{Z}_p$-module. Then one can show that $\widetilde{Y_n} = Y_n$ and that the natural map $X \to A_{n+1}$ induces an isomorphism $Y_n/\nu_1 Y \simeq Ker(A_{n+1} \xrightarrow{norm} A_n)$ (see [**Sa3**] for more details). Since the RHS of this isomorphism is finite and kernels of abelian groups commute with projective limits, it follows by the previous lemma that Y_n is a finitely generated torsion Λ-module. Finally, we know that $A_n \simeq X_n \simeq X/Y_n$. Thus X and Y_n differ only by a finite group. This implies that also X is a finitely generated torsion Λ-module.

□

We end the section stating an important theorem due by Washington that will be very important in the next chapters. The proof is very long and so we are forced to omit it. The interested reader can look at [**Wa**].

Theorem 4.2.16. *Let K be an abelian extension of $\mathbb{Q}$, let p be any prime, and let $K_\infty|K$ be the cyclotomic $\mathbb{Z}_p$-extension of K. Then $\mu = 0$.*

Remark 35. For our purposes, the most important application of this theorem is when $K = \mathbb{Q}(\zeta_p)$ and p is an odd prime number.

4.3 Modules decomposition

Proposition 4.3.1. *Let R be a commutative ring and G an abelian group of order n. Suppose that R contains $\frac{1}{n}$ and a primitive n-th primitive root of unity. Moreover let $\widehat{G} \overset{\text{def}}{=} Hom(G, R^\times)$ (this is a harmless abuse of notation). Then:*

1. *For $\chi \in \widehat{G}$, set $\epsilon_\chi \overset{\text{def}}{=} \frac{1}{n}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1} \in R[G]$. Thus we have:*

   - $\epsilon_\chi^2 = \epsilon_\chi$
   - $\epsilon_\chi \sigma = \chi(\sigma)\epsilon_\chi$
   - $\sum_{\chi\in G}\epsilon_\chi = 1$
   - $\epsilon_\chi \cdot \epsilon_{\chi'} = 0$ *when* $\chi \neq \chi'$

2. *If M is an $R[G]$-module, then M decomposes into $M = \oplus_{\chi\in\widehat{G}}\epsilon_\chi M$.*

Proof. The proof of 1. follows from direct computations so we focus on the proof of 2. Since by 1. we know that $1 = \sum_\chi \epsilon_\chi$, we deduce that for every $x \in M$ one has $x = \sum_\chi \epsilon_\chi x$. Now suppose that $\sum_\chi \epsilon_\chi a_\chi = 0$, with $a_\chi \in M$. Then $\epsilon_{\chi'}(\sum_\chi a_\chi) = \epsilon_{\chi'}0 = 0$ and so $\epsilon_{\chi'}a_\chi = 0$. By the generality of χ' we can deduce that $\epsilon_\chi a_\chi = 0$ for every χ. Thus, we obtain that the above sum is direct. □

Remark 36. Let M be an $R[G]$-module. Then, using the just given definitions and properties, one has the two following easy but still interesting observations:

- If N is another $R[G]$-module such that $M \simeq N$, then $\epsilon_\chi M \simeq \epsilon_\chi N$ for every $\chi \in \widehat{G}$.
- For every $\chi \in \widehat{G}$ we have that $\epsilon_\chi M = \{x \in M : \sigma(x) = \chi(\sigma)x \text{ for all } \sigma \in G\}$

Now let p be an odd prime and let ρ be the complex conjugation. Set $G \overset{\text{def}}{=} Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and notice that $\widehat{G} = \{\omega^i : 0 \leq i \leq p-2\}$ where ω is the Teichmüller character. For a $\mathbb{Z}_p$-module M on which the complex conjugation ρ acts, set $M^+ \overset{\text{def}}{=} \{x \in M : \rho(x) = x\}$ and $M^- \overset{\text{def}}{=} \{x \in M : \rho(x) = -x\}$. Since p is odd, applying the previous proposition properly we get that

$$M = M^+ \oplus M^-$$

Moreover, if M is also a $\mathbb{Z}_p[G]$-module, we deduce that

$$M^+ = \frac{1+\rho}{2}M = \sum_{\substack{\chi\in\widehat{G}\\ \chi \text{ even}}} \epsilon_\chi M$$
$$M^- = \frac{1-\rho}{2}M = \sum_{\substack{\chi\in\widehat{G}\\ \chi \text{ odd}}} \epsilon_\chi M$$

Now for every $n \geq 1$ set $C_n \overset{\text{def}}{=} Cl(\mathbb{Q}(\zeta_n))$. Since ρ still acts on C_n then we can define C_n^- as before. Now we prove an interesting result about class numbers.

Proposition 4.3.2. *The sequence*

$$1 \to C_n^- \to C_n \xrightarrow{N_{K|K^+}} Cl(\mathbb{Q}(\zeta_n)^+) \to 1$$

is exact. In particular, we have that $Cl(\mathbb{Q}(\zeta_n)^+) \simeq C_n/C_n^-$.

Proof. Consider theorems 1.2.4 and 1.2.5. In particular, we look at the composition of maps

$$C_n \xrightarrow{norm} Cl(\mathbb{Q}(\zeta_n)^+) \xrightarrow{inj} C_n$$

By definition, one finds that the kernel of this composition is C_n^-. Since $Ker(inj \circ norm) = Ker(norm)$, the claims follow. □

Clearly one deduces the following

Corollary 4.3.3. $h_n^- = \frac{h_n}{h_n^+} = |C_n^-|$.

Remark 37. Let A_0 be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. Notice that there exists $n \geq 0$ such that $p^n \cdot A_0 = 0$, and so we can make A_0 into a $\mathbb{Z}_p$-module by defining $(\sum_{j=0}^{\infty} b_j p^j) \cdot a \overset{\text{def}}{=} \sum_{j=0}^{\infty}(b_j p^j a)$, with $a \in A_0$, since the latter sum is finite. Furthermore, G also acts naturally on A_0, so that A_0 is actually a $\mathbb{Z}_p[G]$-module. Moreover, since ρ acts on A_0, by lemma 4.3.1 we have a decomposition $A_0 = A_0^+ \oplus A_0^-$. Denote by $A_0(\mathbb{Q}(\zeta_p)^+)$ the p-Sylow subgroup of $Cl(\mathbb{Q}(\zeta_p)^+)$. Applying the previous proposition one deduces that $A_0(\mathbb{Q}(\zeta_p)^+) \simeq A_0/A_0^- \simeq A_0^+$.

Now we make an important consideration that will be used to state properly The Iwasawa Main Conjecture. As we saw in section 3.4 we have a decomposition

$$Gal(\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q}) = \Delta \times \Gamma$$

where $\Delta = Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ and $\Gamma = Gal(\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q}(\zeta_p))$. Because of this, follows that $\Lambda^* \overset{\text{def}}{=} \mathbb{Z}_p[|Gal(\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q})|]$ is isomorphic to $\mathbb{Z}_p[\Delta][|\Gamma|]$. Now let X denote $\varprojlim_n X_n \simeq \varprojlim_n A_n$ as above. We know that $Gal(\mathbb{Q}(\zeta_{p^\infty}|\mathbb{Q})$ acts on X, so that X is a Λ^*-module. Hence, because $\Lambda^* \simeq \mathbb{Z}_p[\Delta][|\Gamma|]$, we deduce that X is also a $\mathbb{Z}_p[\Delta][|\Gamma|]$-module. Recalling that ω generates $\widetilde{\Delta}$, by proposition 4.3.1 follows that

$$X = \bigoplus_{i=0}^{p-2} \epsilon_{\omega^i} X$$

For every $n \geq 0$, let A_n be the ideal class group of $\mathbb{Q}(\zeta_{p^{n+1}})$, as usual. Now we show that $\epsilon_{\omega^i} X$ corresponds to the projective limit of the ω^i-component of A_n, so that $\epsilon_{\omega^i} X$ becomes a Λ-module. Furthermore, still in section 3.4 we saw that $Gal(\mathbb{Q}(\zeta_{p^n})|\mathbb{Q})$ is isomorphic to $\Delta \times Gal(\mathbb{Q}(\zeta_{p^n})|\mathbb{Q}(\zeta_p))$. Hence we can make Δ acting on A_n. Again, by proposition 4.3.1, we have a decomposition $A_n = \bigoplus_{i=0}^{p-2} \epsilon_{\omega^i} A_n$. However, by remark 36 we also know that

$$\epsilon_{\omega^i} X = \{x \in X : \sigma(x) = \omega^i(\sigma)x \text{ for all } \sigma \in \Delta\}$$
$$and$$
$$\epsilon_{\omega^i} A_n = \{x \in A_n : \sigma(x) = \omega^i(\sigma)x \text{ for all } \sigma \in \Delta\}$$

Therefore we deduce that $\epsilon_{\omega^i} X \simeq \varprojlim_n \epsilon_{\omega^i} A_n$. Since every $\epsilon_{\omega^i} A_n$ is clearly a $\mathbb{Z}_p[\Gamma_n|$-module, follows that $\epsilon_{\omega^i} X$ is a $\Lambda = \varprojlim_n \mathbb{Z}_p[\Gamma_n]$-module.

Remark 38. We give some ideas about a generalization of the previous remark and further consequences of the Iwasawa's theorem, but we do not give all the details. For every $n \geq 0$ let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and set $K_\infty = \bigcup_{n\geq 0} K_n$. Then the field extension $K_\infty^+|K_0^+$ is a $\mathbb{Z}_p$-extension. Moreover, denote by A_n the p-Sylow subgroup of the ideal class group of K_n, as usual. This is a $\mathbb{Z}_p[G]$-module and the complex conjugation acts on it. In particular, it decomposes as

$$A_n = A_n^+ \oplus A_n^-$$

As above, one also has that $A(K_n^+) \simeq A_n/A_n^- \simeq A_n^+$. Moreover, for every $n \in \mathbb{N}$ we have that even X_n decomposes as

$$X_n = X_n^+ \oplus X_n^-$$

so that $X = X^+ \oplus X^-$. Proceeding as in the proof of the Iwasawa's theorem, one finds that:

$$A_n^\pm \simeq X_n^\pm \simeq X^\pm/\nu_{n,e}Y_e^\pm.$$

Furthermore, if $p^{e_n^\pm}$ is the largest power of p dividing $h_n^\pm$, then one obtains

$$e_n = e_n^+ + e_n^-$$

and that there exist non-negative integers $\lambda^\pm, \mu^\pm, \nu^\pm$ and $n_0^\pm$ such that

$$e_n^\pm = \lambda^\pm n + \mu^\pm p^n + \nu^\pm \text{ for } n \geq n_0^\pm$$

with $\lambda = \lambda^+ + \lambda^-$, $\mu = \mu^+ + \mu^-$ and $\nu = \nu^+ + \nu^-$.

4.4 Local units modulo Cyclotomic units

In this section we present a theorem that relates the Iwasawa Algebra Λ with the units of $\mathbb{Q}(\zeta_p)$. We will omit the proofs and most of the details. Anyway we believe that, as it is organized, the section still is a useful exposition of the subject. For the proofs look at [**Wa**].

Let p be an odd prime and let U_1 be the units of $\mathbb{Q}_p(\zeta_p)$ which are congruent to 1 mod $(\zeta_p - 1)$. We have the following:

Lemma 4.4.1. *Let $2 \leq i \leq p-2$ and let ϵ_i be the corresponding idempotent of $\mathbb{Z}_p[Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q}]$. Then there exists $\lambda_i \in \mathbb{Z}_p$, $\lambda_i \neq 1$ with $\lambda_i^{p-1} = 1$ such that*

$$\xi_i = \epsilon_i \left(\frac{\lambda_i - \zeta_p}{\omega(\lambda_i - 1)} \right)$$

generates $\epsilon_i U_1$ (here ω denotes the Teichmüller map).

Now we generalize the previous definition. For $n \geq 0$, let U_1^n be the units of $\mathbb{Q}_p(\zeta_{p^{n+1}})$ which are congruent to 1 mod $(\zeta_{p^{n+1}} - 1)$. One can show that the norm of the extension $\mathbb{Q}_p(\zeta_{p^{n+1}})|\mathbb{Q}_p(\zeta_{p^n})$ maps U_1^n into U_1^{n-1}. Denote by $N_{n,n-1}$ this norm. Thus we can define

$$U_1^\infty \overset{\text{def}}{=} \varprojlim_n U_1^n$$

Arguing as above, we have that U_1^∞ is a Λ-module and also a $\mathbb{Z}_p[Gal(\mathbb{Q}_p(\zeta_p)|\mathbb{Q}_p)]$-module. Notice that, wlog, we may assume that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. This assumption will hold in the rest of the section.

Let $2 \leq i \leq p-2$ and let λ_i as in corollary 4.4.1. Define more in general

$$\xi_i^n \overset{\text{def}}{=} \epsilon_i \left(\frac{\lambda_i - \zeta_{p^{n+1}}}{\omega(\lambda_i - 1)} \right)$$

Then

$$N_{n,n-1}(\xi_i^n) = \epsilon_i \Big(\prod_{\zeta \in \mu_p} \left(\frac{\lambda - \zeta\zeta_{p^{n+1}}}{\omega(\lambda_i - 1)} \right) \Big) = \epsilon_i \left(\frac{\lambda_i^p - \zeta_{p^n}}{\omega(\lambda_i - 1)^p} \right) = \xi_i^{n-1}$$

Hence

$$\xi_i^\infty \overset{\text{def}}{=} (\xi_i^n)_n \in \epsilon_i U$$

.

This definition lead us to the following

Theorem 4.4.2. *Let the notation as above. Then*

$$\Lambda \simeq \epsilon_i U_1^\infty$$

through $g \mapsto g\xi_i^\infty$ *and*

$$\Lambda/((1+T)^{p^n} - 1) \simeq \epsilon_i U_1^n$$

through $g \mapsto g\xi_i^n$.
In particular, $\epsilon_i U_1^\infty$ *is a free* Λ*-module or rank* 1.

We conclude the section with a consideration that will be used later. Let C_n denote the cyclotomic units of $\mathbb{Q}(\zeta_{p^{n+1}})$, define $C_1^n \overset{\text{def}}{=} C_n \cap U_1^n$ and let $\overline{C_1^n}$ be the closure of C_1^n in U_1^n. Then, in the usual way, $\overline{C_1^n}$ is a $\mathbb{Z}_p[Gal(\mathbb{Q}_p(\zeta_{p^{n+1}})|\mathbb{Q}_p)]$-module. Moreover, we can also define $\overline{C_1^\infty} \overset{\text{def}}{=} \varprojlim_n \overline{C_1^n}$ with respect to the norm map as above. Then we have that $\overline{C_1^\infty}$ is a Λ-module and a $Gal(\mathbb{Q}_p(\zeta_p)|\mathbb{Q}_p)$-module. Hence, similarly to the previous theorem, applying proposition 1.3.3 one can prove the following:

Theorem 4.4.3. *Let* $2 \leq i \leq p-2$. *Then*

$$\epsilon_i(\overline{C_1^\infty}/\omega_n\overline{C_1^\infty}) \simeq \epsilon_i\overline{C_1^n}$$

where $\omega_n = \gamma_0^{p^n} - 1 = (1+T)^{p^n} - 1$ *as usual.*

Now fix g a primitive root modulo p^2. Then g is a primitive root modulo p^n for all $n \geq 1$. Thus define

$$\eta_n \overset{\text{def}}{=} \left(\zeta_{p^n+1}^{(1-g)/2} \frac{\zeta_{p^{n+1}}^g - 1}{\zeta_{p^{n+1}} - 1}\right)^{p-1}$$

One can show that $N_{n,n-1}(\epsilon_i \eta_n) = \epsilon_i \eta_{n-1}$. This implies that $\epsilon_i \eta \overset{\text{def}}{=} (\epsilon_i \eta_n)_n \in \epsilon_i \overline{C_1^\infty}$. Hence we can state the important (see [**Lan1**] for this):

Proposition 4.4.4. *Let $i \neq 1$. Then $\epsilon_i(\overline{C_1^\infty}) = \Lambda \epsilon_i \eta$. In particular, $\epsilon_i(\overline{C_1^\infty})$ is a free Λ-module of rank 1.*

Finally we have:

Theorem 4.4.5. *Let $i \not\equiv 0 \mod (p-1)$ be even. Then*

$$\epsilon_i U_1^\infty / \epsilon_i \overline{C_1^\infty} \simeq \Lambda/(f_i(T))$$

where $f_i(T)$ is an element of Λ such that

$$f_i(\kappa_0^s - 1) = L_p(1-s, \omega^i)$$

and κ_0 is defined by $\gamma_0 \zeta_{p^n} = \zeta_{p^n}^{\kappa_0}$ for all $n \geq 1$. In particular, $\epsilon_i U_1^\infty / \epsilon_i \overline{C_1^\infty}$ is a finitely generated torsion Λ-module.

The above theorems will play a key role in the proof of the Main Conjecture.

4.5 The Maximal Abelian p-extension unramified outside p

This section is only a collection of some observations that we will use later. We do not give all the details. For these, we refer to [**Wa**].

Let p be an odd prime, F a totally real field (like $\mathbb{Q}$) and set $K_0 = F(\zeta_p)$. Moreover denote by $K_\infty | K_0$ the cyclotomic $\mathbb{Z}_p$-extension of K_0 and let K_n for every $n \geq 1$ be as usual. Denote by M_∞ the maximal abelian p-extension of K_∞ which is unramified outside p (it exists by class field theory) and set

$$\Sigma_\infty \overset{\text{def}}{=} Gal(M_\infty | K_\infty)$$

Notice also that Σ_∞ is a Λ-module as we expect (similar action that we put on X). Now let M_n be the maximal abelian p-extension of K_n which is unramified outside p (the existence is still guaranteed by class field theory). Observe also that $K_\infty \subseteq M_n$. Proceeding in a similar way as in the proof of lemma 4.2.6, one can find that

$$\Sigma_n \overset{\text{def}}{=} Gal(M_n | K_\infty) \simeq \Sigma_\infty / \omega_n \Sigma_\infty$$

where $\omega_n = P_n = (\gamma_0^{p^n} - 1) = (1+T)^{p^n} - 1$ as before. Then one can show that Σ_n is a finitely generated $\mathbb{Z}_p$-module (see [**Wa**] for the details); thus by lemma 4.2.7 we deduce that Σ_∞ is a finitely generated Λ-module. This implies that $\Sigma_\infty \sim \Lambda^a \oplus (torsion)$ for some $a \geq 0$. However, one can improve this result. Indeed (look at [**Wa**] for details), if $2r_2$ denotes the number of complex embeddings of K_0, then one has

$$\Sigma_\infty \sim \Lambda^{r_2} \oplus (torsion)$$

Now set $F = \mathbb{Q}$. We give an idea of the proof of an interesting proposition. For every $n \geq 0$, let $W_{p^{n+1}}$ denote the set of the p^{n+1}-st roots of unity and set $W_{p^\infty} = \bigcup_{n\geq 0} W_{p^{n+1}}$. Moreover let T be equal to $\varprojlim_n W_{p^{n+1}}$ where the inverse limit is taken with respect to the p-th power map. Then we have an isomorphism of abelian groups $T \simeq \mathbb{Z}_p$. Furthermore the Galois group $Gal(K_\infty|\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ acts on T: indeed if $a \in \mathbb{Z}_p^\times$, $t \in T$ and we write T additively, we define an action by $\sigma_a(t) = at$. Finally set $T^{(-1)} = Hom_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$. Clearly also $T^{(-1)}$ is isomorphic to $\mathbb{Z}_p$ as abelian group. Furthermore, $T^{(-1)}$ is a $Gal(K_\infty|\mathbb{Q})$-module thanks to the just defined action on T. In particular, if $f \in T^{(-1)}$ and $t \in T$ then we let the action be

$$(\sigma_a f)(t) \overset{\text{def}}{=} \sigma_a(f(\sigma_a^{-1} t)) = f(a^{-1}t) = a^{-1} f(t)$$

where we used the fact that σ_a acts trivially on $\mathbb{Z}_p$. In other words, this action is given in a such way that $\sigma_a f = a^{-1} f$. Now recall that ϵ_j indicates the idempotents of $Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ then one defines the "*twist*" of $\epsilon_j \Sigma_\infty(-1)$ as

$$\epsilon_j \Sigma_\infty(-1) \overset{\text{def}}{=} \epsilon_j \Sigma_\infty \otimes_{\mathbb{Z}_p} T^{(-1)}$$

The Galois action is now defined through $\sigma_a(x \otimes f) = \sigma_a(x) \otimes a^{-1} f = a^{-1}\sigma_a(x) \otimes f$ with $a \in \mathbb{Z}_p^\times$, $x \in \epsilon_j \Sigma_\infty$ and $f \in T^{(-1)}$. Define also $A_\infty = \varinjlim_n A_n$ where the limit is taken with respect to the natural maps $A_n \to A_{n+1}$ given by the inclusions $\mathbb{Q}(\zeta_{p^n}) \subset \mathbb{Q}(\zeta_{p^{n+1}})$. Then we have the following

Proposition 4.5.1. *$\epsilon_j \Sigma_\infty(-1) \simeq Hom_{\mathbb{Z}_p}(\epsilon_i A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ as Λ-modules, where $i + j \equiv 1$* mod $(p-1)$ *and i is odd.*

Proof. We show that

$$Hom_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p) \simeq Hom_{\mathbb{Z}_p}(B, W_{p^\infty}) \otimes_{\mathbb{Z}_p} T^{(-1)}$$

for any Λ-module B. Since there is a non-degenerate *Kummer* pairing

$$\epsilon_j \Sigma_\infty \times \epsilon_i A_\infty \to W_{p^\infty}$$

with j and i as in the statement (see [**Wa**]) we deduce that $\epsilon_j \Sigma_\infty \simeq Hom_{\mathbb{Z}_p}(\epsilon_i A_\infty, W_{p^\infty})$ (this is an isomorphism of Λ-modules when we define the action $(\sigma f)(a) = \sigma(f(\sigma^{-1} a))$ for $\sigma \in Gal(K_\infty|\mathbb{Q})$ and $f \in Hom_{\mathbb{Z}_p}(\epsilon_i A_\infty, W_{p^\infty})$). This clearly will complete the proof. First of all notice that the function $\phi : \mathbb{Q}_p/\mathbb{Z}_p \to W_{p^\infty}$, given by $\frac{a}{p^n} \mapsto \zeta_{p^n}^a$ is an isomorphism of abelian groups. Now fix t_0 a generator of $T^{(-1)}$ as $\mathbb{Z}_p$-module. Then the abelian groups of the statement are isomorphic through the map $h \xrightarrow{\psi} (\phi h) \otimes t_0$ where $h \in Hom_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$. Therefore it remains to prove that we have an isomorphism of Γ-modules too. Let $\sigma_a \in \Gamma$ for some $a \in \mathbb{Z}_p^\times$. Hence we get

$$(\sigma_a h)(b) = \sigma_a(h(\sigma_a^{-1} b)) = h(\sigma_a^{-1} b)$$

but also

$$\begin{aligned}\sigma_a(\phi h \otimes t_0) &= \sigma_a \phi h \sigma^{-1} \otimes \sigma_a t_0 = a\phi h \sigma_a^{-1} \otimes a^{-1} t_0 = \\ &= \phi h \sigma^{\cdot 1} \otimes t_0\end{aligned}$$

This implies that under the above isomorphism $\sigma_a h$ is mapped to $\sigma_a(\phi h \otimes t_0)$. Indeed: $\psi((\sigma_a h)(b)) = \psi(h(\sigma_a^{-1}b)) = (\phi h \sigma_a^{-1}(b)) \otimes t_0 = \sigma_a(\phi h(b) \otimes t_0) = \sigma_a \psi(h(b))$. However this means that we have an isomorphism of Γ-modules. Thus we also have the isomorphism of $\Lambda = \mathbb{Z}_p[|\Gamma|]$-modules of the statement and so we can conclude the proof. □

Chapter 5

The Iwasawa Main Conjecture

The aim of this chapter is to prove The Iwasawa Main Conjecture for $\mathbb{Q}(\zeta_{p^\infty})$, with p odd prime. Before giving the statement, we study some properties of the Euler Systems of Cyclotomic units. As application, we see how to use them to study the ideal class group of $\mathbb{Q}(\zeta_p)^+$. After that, we apply some definitions and results of the previous chapters to enunciate The Iwasawa Main Conjecture. In order to prove it, we will develop some theory of Adjoints and further techniques of Iwasawa theory.

5.1 Euler Systems of Cyclotomic units

Let $m \geq 3$, p an odd prime and let $F = \mathbb{Q}(\zeta_m)^+$. The setting for this section is the following:

- M = a large power of p
- $l \equiv 1 \mod mM$ with l prime
- L = a product of distinct primes, each $\equiv 1 \mod mM$
- $\zeta_L = \prod_{l|L} \zeta_l$
- $F(L) = F(\zeta_L)$
- $N_{lL|L} = N_{F(lL)|F(L)}$= the norm for the extension $F(lL)|F(L)$

Now we are ready to discuss one particular example of the so-called Kolyvagin's Euler Systems. For the general theory about them, look at [**Ru**] for example. We give the following:

Definition 5.1.1. In the above setting, an **Euler System of Cyclotomic units** is the collection of the following data:

- $\alpha = \prod_j((1-\zeta_m^j)(1-\zeta_m^{-j}))^{a_j}$ with $j, a_j \geq 1$
- $\alpha(L) = \prod_j((1-\zeta_m^j\zeta_L)(1-\zeta_m^{-j}\zeta_L))^{a_j}$ with the a_j's as above

Remark 39. We want just to point out that if m is not a prime power then α is a cyclotomic unit of F (follows from proposition 1.1.2). This is not clearly true if m is a prime power (recall proposition 1.1.3) but, with a little abuse of terminology, in a context like the one we are discussing one still says that α is a cyclotomic unit of F. On the other hand, for any m, we have that $\alpha(L)$ is a unit of $F(L)$ (to see this notice that $1-\zeta_m^j\zeta_L \in \mathbb{Z}[\zeta_m\zeta_L]^\times$ for every $j \geq 1$, again by proposition 1.1.2). Finally, observe that $[\mathbb{Q}(\zeta_m,\zeta_L):F(L)] = 2$ and $\alpha(L) = N_{\mathbb{Q}(\zeta_m,\zeta_L)|F(L)}(\prod_j(1-\zeta_m^j\zeta_L)^{a_j})$.

Notation: For typographical reasons, we will write ring actions additively, so for example $(\sigma-1)\alpha$ means the same as $\sigma\alpha/\alpha$.

Lemma 5.1.1. *We have:*

1. *Assume l does not divide L. Then $N_{lL|L}\alpha(lL) = \alpha(L)^{Frob_l - 1}$ where $Frob_l$ is the Frobenius element for l for the extension $F(L)|\mathbb{Q}$.*

2. *$\alpha(lL) \equiv \alpha(L)$ modulo all primes of $F(lL)$ above l.*

Proof. 1. For this part it is enough to observe that the norm for the extension $\mathbb{Q}(\zeta_m,\zeta_{lL})|\mathbb{Q}(\zeta_m,\zeta_L)$ of the element $1-\zeta_m^j\zeta_{lL}$ is equal to

$$\prod_{k=1}^{l-1}(1-\zeta_m^j\zeta_L\zeta_l^k) = \frac{1-\zeta_m^{jl}\zeta_L^l}{1-\zeta_m^j\zeta_L} = (1-\zeta_m^j\zeta_L)^{Frob_l-1}$$

Indeed replacing ζ_m^j with ζ_m^{-j} and using the fact (as in the above remark) that $\alpha(lL) = N_{\mathbb{Q}(\zeta_m,\zeta_{lL})|F(lL)}(\prod_j(1-\zeta_m^j\zeta_{lL})^{a_j})$, we get the first claim.

2. Notice that $\zeta_l \equiv 1$ modulo all primes above l (if $\mathfrak{p}$ is a prime of $F(lL)$ lying above l, then $\mathcal{O}_{F(lL)}/\mathfrak{p}$ is a field of characteristic l). Hence the second claim is true too. □

The two properties above 1. and 2. are fundamental to prove the Main Conjecture and they are actually taken inside the definition of Kolyvagin's Euler Systems in their general theory (see [**Ru**]).

Now for each prime l as above, fix a primitive root $s \mod l$. Define $\sigma_l \in Gal(F(l)|F)$ by $\sigma_l(\zeta_l) = \zeta_l^s$. Notice that we may extend σ_l when needed so that $\sigma_l = id$ on roots of unity of order prime to l. Then we obtain that $\langle\sigma_l\rangle = Gal(F(lL)|F(L))$. Let

$$D_l \overset{\text{def}}{=} \sum_{j=0}^{l-2} j\sigma_l^j$$

By a direct calculation one finds that

$$(\sigma_l - 1)D_l = l - 1 - N_l$$

where $N_l \overset{\text{def}}{=} \sum_{j=0}^{l-2}\sigma_l^j$ can be identified with the norm $N_{lL|L}$ defined above. Define

$$D_L = \prod_{l|L} D_l$$

Then we can prove the following proposition that gives us explicit formulas for some algebraic integers $\kappa(L)$ and β_L that will play a key role in the chapter.

Proposition 5.1.2. *There exists $\beta_L \in F(L)^\times$ and $\kappa(L) \in F^\times$ such that*

$$D_L\alpha(L) = \kappa(L)\beta_L^M$$

and $((\sigma - 1)D_l\alpha(L))^{1/M} = \beta_L^{\sigma-1}$ for all $\sigma \in Gal(F(L)|F)$.

Proof. Denote by $H = (F(L)^\times/F(L)^{\times M})^G$ the elements of $F(L)^\times/F(L)^{\times M}$ fixed by $G = Gal(F(L)|F)$. We claim that $D_L\alpha(L) \mod (F(L)^\times)^M \in H$. We prove it by induction on the number of prime factors of L. If $L = 1$ then $G = 1$ so that the claim holds. Suppose then that the claim is true for all L' with fewer prime factors than L. Let $l|L$ and let L' such that $L = lL'$. Then we have:

$$\begin{aligned}(\sigma_l - 1)D_{lL'}\alpha(lL') &= (\sigma_l - 1)D_l(D_{L'}\alpha(lL')) = (l - 1 - N_l)D_{L'}\alpha(lL') = \\ &= \frac{D_{L'}\alpha(lL'))^l}{D_{L'}\alpha(lL')} \cdot \frac{1}{N_l(D_{L'}\alpha(lL'))} = (M^{th}power)/D_{L'}N_l\alpha(lL') = \\ &= (M^{th}power)/D_L\alpha(L')^{Frob_l-1} = \\ &= (M^{th}power) \cdot (\kappa(L')\beta_{L'}^M)^{Frob_l-1} = (M^{th}power)(M^{th}power)\end{aligned}$$

where in the fourth equality we used that $l - 1 \equiv 0 \mod M$, in the fifth that l does not divide L' and in the sixth the inductive assumption. Therefore σ_l fixes $D_L\alpha(L)$ modulo M^{th} powers for each $l|L$. Since the set of σ_l with $l|L$ generates G, this proves the claim.

Now we claim that $F(L)$ contains no non-trivial p-power roots of unity. Indeed: $\mathbb{Q}(\zeta_L)$ and $\mathbb{Q}(\zeta_p, \zeta_m)$ are linearly disjoint over $\mathbb{Q}$ and then so are $F(L)$ and $F(\zeta_p)$ over F. On the other hand

$$[F(L)(\zeta_p) : F] = [F(L)(\zeta_p) : F(L)] \cdot [F(L) : F] = [F(L)(\zeta_p) : F(\zeta_p)] \cdot [F(\zeta_p) : F]$$

However by disjointness we have $[F(L)(\zeta_p) : F(\zeta_p)] = [F(L) : F]$. Thus, since F is properly contained in $F(\zeta_p)$, from the line above follows that $[F(L)(\zeta_p) : F(L)] = [F(\zeta_p) : F] \neq 1$. Therefore $\zeta_p \notin F(L)$, as we wanted.

Then by this observation we can define $c : G \to F(L)^\times$ by $c(\sigma) = ((\sigma - 1)D_L\alpha(L))^{1/M}$. Indeed this is well-defined because $F(L)$ contains no non-trivial M^{th} roots of unity by our choice of M and by the just proved claim. By a direct calculation, we find that c satisfies *the cocycle relation*:

$$c(\sigma_1\sigma_2) = c(\sigma_1)c(\sigma_2)^\sigma.$$

To conclude the proof, we need the following

Lemma 5.1.3. *There exists $\beta \in F(L)^\times$ such that $c(\sigma) = \beta^{\sigma-1}$ for all $\sigma \in G$.*

Proof. By the linear independence of characters, there exists $x \in F(L)^\times$ such that $y = \Sigma_{\sigma\in G}c(\sigma)\sigma(x) \neq 0$. Now let $\tau \in G$. The cocycle condition implies that

$$\tau y = \Sigma_\sigma c(\sigma)^\tau\sigma(x) = \Sigma_\sigma c(\tau\sigma)c(\tau)^{-1}\tau\sigma(x) = c(\tau)^{-1}\sum_\sigma c(\sigma\tau)\tau\sigma(x) = c(\tau)^{-1}y.$$

Hence $c(\tau) = y^{1-\tau}$. Setting $\beta = y^{-1}$, we conclude the lemma. □

Now we come back to the proof of the proposition: let β be as in the previous lemma and let $\kappa(L) = D_L\alpha(L)/\beta^M$. Then

$$(\sigma - 1)\kappa(L) = \frac{(\sigma - 1)D_L\alpha(L)}{(\sigma - 1)\beta^M} = \frac{c(\sigma)^M}{((\sigma - 1)\beta)^M} = 1$$

for all $\sigma \in G$, so $\kappa(L) \in F^\times$ (last equality holds by the previous lemma). This completes the proof.

□

Remark 40. Consider $\mathfrak{p}$ a prime of F such that $\mathfrak{p} \nmid L$. Notice that $F(L)$ is the compositum of F and $\mathbb{Q}(\zeta_L)$. Then looking at the ramification indices we deduce that $\mathfrak{p}$ is unramified in $F(L)|F$. Observe also that by lemma 5.1.2 follows that $(\kappa(L)) = (\beta_L^{-1})^M$ as ideals in $F(L)$. Thus we obtain that the $\mathfrak{p}$-adic valuation satisfies $\nu_\mathfrak{p}(\kappa(L)) = 0 \mod M$.

Now fix L and let $l \equiv 1 \mod (mML)$. Let λ be a prime of F above l and let $\mathcal{L}$ be a prime of $F(lL)$ above λ. We assume that $\kappa(L) \not\equiv 0 \mod \lambda$. Since $l \equiv 1 \mod (mML)$, we get that l splits completely in $F(L)|\mathbb{Q}$ and that is totally ramified in $F(lL)|F(L)$ (see again the ramification indices). This implies that if s is a primitive root modulo l, then it is also a primitive root modulo λ and modulo $\mathcal{L}$.

Proposition 5.1.4. *Suppose $\kappa(L) \equiv s^a \mod \lambda$. Then the λ-adic valuation of $\kappa(lL)$ satisfies*

$$v_\lambda(\kappa(lL)) \equiv -a \mod M$$

Proof. Using lemma 5.1.1 and proposition 5.1.2, one finds that

$$\begin{aligned}(\sigma_l - 1)\beta_{lL} &= ((\sigma_l - 1)D_{lL}\alpha(lL))^{1/M} = ((l - 1 - N_l)D_L\alpha(lL))^{1/M} = \\ &= (D_L\alpha(lL))^{(l-1)/M} \equiv (D_L\alpha(L))^{(l-1)/M} \mod \mathfrak{p}\end{aligned}$$

where $\mathfrak{p}$ is any prime above l and where the third equality holds since $l \equiv 1 \mod mML$ implies that $Frob_l = 1$ and so $N_{lL|L}\alpha(lL) = 1$ by lemma 5.1.1. Let $a' \in \mathbb{N}$ such that $D_L\alpha(L) \equiv s^{a'} \mod \mathcal{L}$. Then by proposition 5.1.2 we deduce that $a' \equiv a \mod M$. Therefore

$$(\sigma_l - 1)\beta_{lL} \equiv s^b \mod \mathcal{L},$$

where $b = a'(l-1)/M \equiv a(l-1)/M \mod (l-1)$. Now set $c = \nu_\mathcal{L}(\beta_{lL})$. Since $\nu_\mathcal{L}(1-\zeta_l) = 1$, we can write $\beta = (1 - \zeta_l)^c y$ where $\nu_\mathcal{L}(y) = 0$. Notice that

$$(1 - \zeta_l)^{\sigma_l - 1} = \frac{1 - \zeta_l^s}{1 - \zeta_l} \equiv s \mod \mathcal{L}$$

since by the binomial expansion we have $\zeta_l^s - 1 = (\zeta_l - 1 + 1)^s - 1 = -s(1 - \zeta_l) + \cdots$. Moreover, being $\mathcal{L}$ totally ramified in $F(lL)|F(L)$, σ_l belongs to the inertia group of $\mathcal{L}$, so $\sigma_l y \equiv y \mod \mathcal{L}$. Therefore

$$s^b \equiv (\sigma_l - 1)\beta_{lL} = ((1 - \zeta_l)^{\sigma_l - 1})^c y^{\sigma_l - 1} \equiv s^c \cdot 1 \equiv s^c \mod \mathcal{L}$$

Hence we deduce that $b \equiv c \mod (l-1)$. Since $\mathcal{L}^{l-1} = \lambda$, recalling the above properties of a' we have

$$\begin{aligned} \nu_\lambda(\kappa(lL)) = \frac{1}{l-1}\nu_{\mathcal{L}}(\kappa(lL)) = -\frac{1}{l-1}\nu_{\mathcal{L}}(\beta_{lL}^M) = \\ = -\frac{Mc}{l-1} \equiv -\frac{Mb}{l-1} \equiv -a \mod M \end{aligned}$$

This concludes the proof of the proposition.

□

5.2 Example: The Ideal Class Group of $\mathbb{Q}(\zeta_p)^+$

In this section we show how to use the previous results about the Euler System of Cyclotomic units in order to study the ideal class group of $\mathbb{Q}(\zeta_p)^+$. This is not needed for the proof of The Iwasawa Main Conjecture but it gives us some important strategies that will be generalized in the next sections.

The setting is the same as before with $m = p$ (with p odd prime as usual) and $M = p|A^+| \cdot |(E/C)_p| = p|A^+|^2$ where A^+ is the p-part of the ideal class group of $F = \mathbb{Q}(\zeta_p)^+$, E is the group of units of F, C is the subgroup of cyclotomic units and $(E/C)_p$ is the p-part of (E/C).

Let χ be an even p-adic valued character of $G \overset{\text{def}}{=} Gal(\mathbb{Q}(\zeta_p)^+|\mathbb{Q})$. Now recall by theorem 1.3.2 that $[E : C]$ is the class number of $\mathbb{Q}(\zeta_p)^+$. The main theorem of this section tells us that this equality holds componentwise with respect to the χ-components, namely:

Theorem 5.2.1. *Let χ be a character as above. Then $|\epsilon_\chi(A^+)| = |\epsilon_\chi(E/C)_p|$ where $\epsilon_\chi(E/C)_p$ indicates the χ-component of $(E/C)_p$.*

Proof. First of all, notice that if χ is trivial then $|\epsilon_\chi(A^+)| = 1 = |\epsilon_\chi(E/C)_p|$ (this is because in this case $\epsilon_\chi = \frac{2}{p-1}norm$). Therefore, we can consider χ to be non-trivial in the rest of the proof. Notice that by the results and remarks of section 4.3, we have:

$$\begin{aligned} \prod_{\chi \text{ even}} |\epsilon_\chi(A^+)| = p\text{-part of the class number of } \mathbb{Q}(\zeta_p)^+ = \\ = p\text{-part of } |E/C| = \prod_{\chi \text{ even}} |\epsilon_\chi(E/C)_p| \end{aligned}$$

This implies that to prove the equality $|\epsilon_\chi(A^+)| = |\epsilon_\chi(E/C)_p|$ is enough to show that $\epsilon_\chi(A^+)$ divides $|\epsilon_\chi(E/C)_p|$ for each χ as above. Notice now that for every idempotent $\epsilon_\chi \in \mathbb{Z}_p[G]$ we can define an element $\epsilon'_\chi \in \mathbb{Z}[G]$ that has the same coefficients of ϵ_χ but modulo M (this is done because $\epsilon_\chi\kappa$ is not defined in general). In this way $\epsilon'_\chi\kappa(L)$, $\epsilon'_\chi\kappa(lL)$ are defined and moreover $\epsilon_\chi(A^+) = \epsilon'_\chi(A^+)$. If $\epsilon_\chi = \sum_\sigma \chi(\sigma)\sigma^{-1}$ then we write $\epsilon'_\chi = \sum_\sigma \chi'(\sigma)\sigma^{-1}$. Now we need the following:

Lemma 5.2.2. *Let λ, l, L and s as in the previous section with $l \equiv 1 \mod mML$. Assume that the ideal class $\mathfrak{C}$ of λ is in $\epsilon_\chi(A^+)$ and also that the classes of the prime ideals of F dividing L are in $\epsilon_\chi(A^+)$. Suppose:*

1. *$\mathfrak{C}$ has order f in the quotient of $\epsilon_\chi(A^+)$ by the subgroup generated by the classes of the primes dividing L*

2. *$\epsilon'_\chi\kappa(lL) \in (F^\times)^{p^r}$ with $p^r \leq M$ and $Mp^{-r}A^+ = 0$*

3. *if $\epsilon'_\chi\kappa(L) \equiv s^a \mod \lambda$ and $p^{r'} \mid\mid a$, then $p^{r'} < M$*

Then $r' \geq r$ and $f \mid p^{r'-r}$.

Proof. Let $\sigma \in Gal(F|\mathbb{Q})$. Then s is also a primitive root modulo $\sigma\lambda$. Let

$$\kappa(L) \equiv s^{a_\sigma} \mod \sigma\lambda.$$

It follows that $\sigma^{-1}\kappa(L) \equiv s^{a_\sigma} \mod \lambda$. Therefore

$$\epsilon'_\chi\kappa(L) \equiv s^a \mod \lambda \text{ with } a \equiv \sum_\sigma \chi'(\sigma)a_\sigma \mod M$$

From now on let r and r' be as in assumptions 2. and 3. By construction then we have $p^{r'} \mid\mid a$. By proposition 5.1.4 we get that

$$\nu_{\sigma\lambda}(\kappa(lL)) \equiv -a_\sigma \mod M$$

Since $\nu_\lambda(\sigma^{-1}\kappa) = \nu_{\sigma\lambda}(\kappa)$ it follows also that

$$\nu_\lambda(\epsilon'_\chi\kappa(lL)) \equiv \sum_\sigma \chi'(\sigma)\nu_{\sigma\lambda}(\kappa(lL)) \equiv \sum_\sigma \chi'(\sigma)(-a_\sigma) \equiv -a \mod M$$

Now since we know that p^r divides $\nu_\lambda(\epsilon'_\chi\kappa(lL))$, we deduce that $p^r \mid a$, so that $r \leq r'$. Furthermore,

$$\nu_{\sigma^{-1}\lambda}(\epsilon'_\chi\kappa(lL)) = \nu_\lambda(\sigma\epsilon'_\chi\kappa(lL)) \equiv \chi(\sigma)\nu_\lambda(\epsilon'_\chi\kappa(lL)) \equiv -\chi(\sigma)a \mod M$$

Thus by remark 40 we deduce also that there is an ideal I such that

$$\begin{aligned}(\epsilon'_\chi\kappa(lL)) &= \prod_\sigma(\sigma^{-1}\lambda)^{-a\chi'(\sigma)} \cdot (\text{primes dividing } L) \cdot I^M = \\ &= \lambda^{-a\epsilon'_\chi} \cdot (\text{primes dividing } L) \cdot I^M\end{aligned}$$

Notice that le LHS is a p^r-th power. Hence the exponent of every prime ideal on the RHS is a multiple of p^r and so we may take the p^r-th root of the equation. Moreover considering the classes of the ideals in the previous expression and using again the fact that $\epsilon'_\chi\kappa(lL) \in (F^\times)^{p^r}$, it follows that the class of I lies in A^+. Since Mp^{-r} annihilates A^+ by hypothesis, we deduce that the ideal $I^{Mp^{-r}}$ is principal. By hypothesis we can also identify $\epsilon'_\chi\mathfrak{C}$ with $\mathfrak{C}$. Thus $-ap^{-r}\mathfrak{C} = -ap^{-r}\epsilon'_\chi\mathfrak{C}$ is equal to 0 in the quotient of $\epsilon_\chi(A^+)$ by the subgroup generated by the classes of the primes dividing L. Therefore $f \mid ap^{-r}$. Recalling that $p^{r'} \mid\mid a$ and observing that f must be a power of p, we can conclude the proof. □

By the Structure theorem for finite abelian groups, we can write

$$\epsilon_\chi(A^+) \simeq \mathbb{Z}/f_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/f_k\mathbb{Z}$$

for some $k \geq 1$ and some powers of prime numbers $f_1, \ldots, f_k$. Now proceeding inductively, we can choose classes $\mathfrak{C}_1, \ldots, \mathfrak{C}_k$ in $\epsilon_\chi(A^+)$ such that $\mathfrak{C}_{i+1}$ has order f_{i+1} in $\epsilon_\chi(A^+)/(\mathfrak{C}_1, \ldots, \mathfrak{C}_i)$. We also need (see [**Wa**] for details):

Proposition 5.2.3. *Let $N \geq 1$ and let i be even with $2 \leq i \leq p-3$. Set $E_{p^N} = E/E^{p^N}$ and $E^+_{p^N} = E^+/(E^+)^{p^N}$. Then*

$$\epsilon_i(E^+_{p^N}) \simeq \mathbb{Z}/p^N\mathbb{Z}$$

Applying the above proposition, it follows that $\epsilon_\chi(E/C)_p$ is cyclic. Say that it has cardinality p^{r_0}. Then we can choose $u \in E$ such that $u \notin E^p$ and $u^{p^{r_0}} \in C$. Let $\alpha \overset{\text{def}}{=} u^{p^{r_0}}$. Notice that we may assume that $\sigma u \equiv u^{\chi(\sigma)}$ modulo M^{th}-powers for all $\sigma \in G$ (if not, replace u with $u^{\epsilon'_\chi}$). Therefore we also have that $\sigma\alpha \equiv \alpha^{\chi(\sigma)}$ modulo M^{th}-powers for all $\sigma \in G$. Choose also primes $\lambda_1, \ldots, \lambda_k$ lying above rational primes $l_1, \ldots, l_k$ such that $\lambda_i \in \mathfrak{C}_i$ and $l_i \equiv 1 \mod ML_{i-1}$, where $L_{i-1} = l_1 \cdots l_{i-1}$.
Starting with α, we obtain $\kappa(L_i)$ in the same way as we did in the previous section. Then let $\epsilon'_\chi\kappa(L_i) \in F^{p^{r_i}}$ with r_i not necessarily maximal and let $\epsilon'_\chi\kappa(L_i)$ be a $p^{r'_i}$-th power modulo λ_{i+1} with r'_i maximal, so that $r'_i \geq r_i$. Now we want apply the previous lemma. Thus we need to show that all the hypothesis are satisfied. After that, we will deduce that $r'_i = r_i$ for every i and we will be able to conclude. Suppose now that we have chosen the primes $\lambda_1, \ldots, \lambda_k$ such that $r_0 \geq r_j = r'_j$ for all $j < i$. Let r_i be the largest integer less than or equal to $r_0 + 1$ such that $\epsilon'_\chi\kappa(L_i) \in F^{p^{r_i}}$. Then we obtain that $Mp^{-r_i}A^+ = 0$. Indeed, notice that $Mp^{-r_0-1}A^+ = p^{-r_0}|A^+|^2A^+ = 0$ since $p^{r_0} \mid |A^+|$ by our definition of r_0. Thus condition 2. of the previous lemma is fulfilled with $L = L_{i-1}$ and $l = l_i$. Since $r'_{i-1} = r_{i-1} \leq r_0$, we have $p^{r'_{i-1}} < M$, so that also condition 3. is satisfied. Clearly for condition 1. we consider the ideal classes $\mathfrak{C}_1, \ldots, \mathfrak{C}_k$. It follows that we can apply the previous lemma. On one hand we obtain that $r'_{i-1} \geq r_i$, so that $r_i \leq r_0$. This implies that $r_i \neq r_0 + 1$. Therefore r_i is the maximal integer such that $\epsilon'_\chi\kappa(L_i) \in F^{p^{r_i}}$. On the other hand we also get that $r'_i \geq r_{i+1}$ and

$$|\epsilon_\chi(A^+)| = f_1 \cdots f_k \mid p^{(r'_0-r_1)+(r'_1-r_2)+\cdots(r'_{k-1}-r_k)}$$

Now we take for granted another result. We refer again to [**Wa**] for a proof.

Proposition 5.2.4. *Let $\mathfrak{C}$ be one of the ideal classes of F defined above. Let b and c be positive integers with $c \mid b$. Let $\beta \in F^\times$. Suppose that $\lambda \in \mathfrak{C}$ lies over a prime $l \equiv 1 \mod b$ and satisfies $\beta \equiv c$-th power $\mod \lambda$. Then*

$$\beta = c\text{-}th \text{ power in } F \text{ if } c \text{ is odd}$$
$$\beta = \pm\frac{c}{2}\text{-}th \text{ power in } F \text{ if } c \text{ is even}$$

By the previous proposition with $b = ML_i$ and $c = p^{r'_i}$ we deduce that $r_i \geq r'_i$ and so $r_i = r'_i$ for all i. Therefore $|\epsilon_\chi(A^+)|$ divides $p^{r_0-r_k}$ and this implies that $|\epsilon_\chi(A^+)|$ divides $p^{r_0} = |\epsilon_\chi(E/C)_p|$. This completes the proof of the theorem. □

5.3 Introduction to the problem and statement

Let p be an odd prime and let ζ_p be a primitive p-th root of unity as usual. Consider the $\mathbb{Z}_p$-extension $\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q}(\zeta_p)$ and the following notations for $n \geq 0$:

- A_n = p-part of the ideal class group of $\mathbb{Q}(\zeta_{p^{n+1}})$
- $A_\infty = \varinjlim_n A_n$ with respect to the maps $A_n \to A_{n+1}$ given by the inclusions $\mathbb{Q}(\zeta_{p^n}) \subset \mathbb{Q}(\zeta_{p^{n+1}})$
- $X = Gal(L_\infty|\mathbb{Q}(\zeta_{p^\infty}))$ where L_∞ is the maximal unramified abelian $p-$extension of $\mathbb{Q}(\zeta_{p^\infty})$
- $\Sigma_n = Gal(M_n|\mathbb{Q}(\zeta_{p^\infty}))$ where M_n is the maximal abelian p-extension of $\mathbb{Q}(\zeta_{p^{n+1}})$ unramified outside p, for $n \leq \infty$
- ϵ_i = the i^{th} idempotent for $Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ with i odd
- $L_p(s, \omega^j)$ = p-adic L-function for ω^j with j even and nonzero
- $f(T, \omega^j)$ = the power series in $\mathcal{O}_{\omega^j}[|T|]$ (where $\mathcal{O}_{\omega^j} = \mathbb{Z}_p[\omega^j]$) such that $L_p(s, \omega^j) = f((1+p)^s - 1, \omega^j)$

Let M be a finitely generated *torsion* Λ-module. Then by corollary 3.3.13 M is pseudo-isomorphic to an elementary Λ-module $E = \bigoplus_{i=1}^s \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^t \Lambda/(P_j^{n_j})$ where the P_j's are irreducible distinguished polynomials. Recall that all height one prime ideals of Λ, namely those other than 0 and (p, T) are of the form $\mathfrak{p}$ where $\mathfrak{p}$ is either p or an irreducible distinguished polynomial.

Let M as above. Recall also that at the end of section 3.3 we defined **the characteristic polynomial of** M to be $char(M) = \prod_{j=1}^t p^{\mu(M)} \cdot P_j^{n_j} = \prod_{j=1}^t P_j^{n_j}$.

Remark 41. By corollary 4.2.15, we know that X is a finitely generated torsion Λ-module. Moreover, by theorem 4.2.16 we have that $\mu(X) = 0$. This implies that $X \sim \bigoplus_{j=1}^s \Lambda/(P_j^{e_j})$ where each P_j is an irreducible distinguished polynomial. Hence the characteristic polynomial of X is $char(X) = \prod_{j=1}^s P_j^{e_j}$. Furthermore, in section 4.3 we saw that $\epsilon_i X$ is a Λ-module for every i. Then notice that actually it is also a finitely generated torsion Λ-module since so it is X and since Λ is a noetherian ring.

Now we can state:

Theorem 5.3.1 (The Iwasawa Main Conjecture)**.** *Let p be an odd prime and let i be odd, $i \not\equiv 1 \mod (p-1)$. Then $char(\epsilon_i X) = f(T, \omega^{1-i})u(T)$ with $u(T) \in \Lambda^\times$.*

There are many beautiful formulas in mathematics. Among them, this is considered one of the most fascinating: on the LHS we have an algebraic and arithmetic object, determined by the ideal class groups while on the RHS we have a p-adic analytic object, determined by the values of p-adic L-functions.

There are several equivalent forms of the Main Conjecture. Before seeing some of them, we need to prepare properly the setting. Recall the norm maps of the extensions $\mathbb{Q}_p(\zeta_{p^{n+2}})|\mathbb{Q}_p(\zeta_{p^{n+1}})$ and $\mathbb{Q}(\zeta_{p^{n+2}})|\mathbb{Q}(\zeta_{p^{n+1}})$ for every $n \geq 0$. Then, we fix other notations:

- U_1^n = units of $\mathbb{Q}_p(\zeta_{p^{n+1}})$ congruent to $1 \mod (\zeta_{p^{n+1}} - 1)$
- E_1^n = units of $\mathbb{Q}(\zeta_{p^{n+1}})$ congruent to $1 \mod (\zeta_{p^{n+1}} - 1)$
- C_n = group of cyclotomic units of $\mathbb{Q}(\zeta_{p^{n+1}})$

- $C_1^n = C_n \cap U_1^n$
- $\overline{E}_1^n$ = closure of $E_1^n \cap U_1^n$ in U_1^n
- $\overline{C}_1^n$ = closure of C_1^n in U_1^n
- $U_1^\infty = \varprojlim U_1^n$ with respect to the norm maps
- $\overline{E}_1^\infty = \varprojlim \overline{E}_1^n$ with respect to the norm maps
- $\overline{C}_1^\infty = \varprojlim \overline{C}_1^n$ with respect to the norm maps

Remark 42. For the next claim it is worth to observe that if j is even with $j \not\equiv 0 \mod (p-1)$ then theorem 4.4.5 implies that $\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty))$ is a finitely generated torsion Λ-module.

Proposition 5.3.2. *The following are equivalent:*

1. $char(\epsilon_i X) = f(T, \omega^{1-i})u_i(T)$ *for all odd* $i \not\equiv 1 \mod (p-1)$ *where* $u_i \in \Lambda^\times$*;*
2. $char(\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty)) = char(\epsilon_j X)$ *for all even* $j \not\equiv 0 \mod (p-1)$*;*
3. $char(\epsilon_j X)$ *divides* $char(\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty))$ *for all even* $j \not\equiv 0 \mod (p-1)$.

The proof is postponed at the end of section 5.5. To prove The Main Conjecture, we will prove that actually statement 3 of the previous proposition holds. To do this, we need the following corollary whose proof follows from a general result of Class field theory that relates the local units of a number field with its Hilbert Class field. For a proof, look at [**Wa**].

Corollary 5.3.3. *Let* $n \geq 0$ *and let* L_n *be the maximal unramified abelian p-extension of* $\mathbb{Q}(\zeta_{p^{n+1}})$*, as usual. Then* $U_1^n/\overline{E_1^n} \simeq Gal(M_n|L_n)$*. In particular, there is an injective map* $U_1^n/\overline{E_1^n} \hookrightarrow \Sigma_n$.

5.4 Adjoints

In this section we introduce the theory of Adjoints in order to give an idea of the proof of proposition 5.4.15.

Lemma 5.4.1. *Let* M *be a finitely generated torsion* Λ*-module.*

1. $char(M) \cdot M$ *is finite*
2. *If* M *is finite, then* $(p, T)^n M = 0$ *for* n *sufficiently large; hence, the annihilator of* X *is of finite index in* Λ
3. *If for each* $x \in M$ *there exist relatively prime* $f, g \in \Lambda$ *(depending on* x*) such that* $fx = gx = 0$*, then* M *is finite.*

Proof. 1. Since M is a finitely generated torsion Λ-module, there is an exact sequence $0 \to A \to M \to E$ with A finite contained in M and E elementary Λ-module. If $m \in M$, then $char(M)m$ maps to 0 in E (by definition of $char(M)$). Hence it lies in A.

2. If $f \in (p, T)$ and $m \in M$. Being M finite, we have that $f^i x = f^j x$ for some i, j with $0 < i < j$. Since $1 - f^{j-i} \in \Lambda^\times$, then $f^i x = 0$. In particular $p^r x = T^r x = 0$ for some r. Now notice that $(p, T)^{2n} \subseteq (p^n, T^n)$ for every n and that, being M finite, the annihilator of M contains (p^m, T^m) for m sufficiently large. Since $\Lambda/(p^m, T^m)$ is finite, the statement follows.

3. Let $x_1, ..., x_n$ be a set of generators for M and let $f_i x_i = g_i x_i = 0$, where f_i and g_i are relatively prime elements of Λ for every i. Then the finite module $\bigoplus_i \Lambda/(f_i, g_i)$ surjects onto M (consider $\lambda + (f_i, g_i) \mapsto \lambda x_i$), which is therefore finite.

□

From now on, for each height one prime ideal $\mathfrak{p} = (f)$, let $\Lambda_{\mathfrak{p}}$ be the localization of Λ at $\mathfrak{p}$.

Lemma 5.4.2. *Let $M \sim E \overset{\text{def}}{=} \bigoplus_i \Lambda/(f_i^{m_i})$. Then $M \otimes_\Lambda \Lambda_{\mathfrak{p}} = \bigoplus_{(f_i)=\mathfrak{p}} \Lambda_{\mathfrak{p}}/f_i^{m_i}\Lambda_{\mathfrak{p}}$.*

Proof. Since $M \sim E$ there exists an exact sequence of Λ-modules $0 \to A \to M \to E \to B \to 0$ with A, B finite. Recall that localization preserves exact sequences (i.e. it is an exact functor) and so we have that $0 \to A \otimes_\Lambda \Lambda_{\mathfrak{p}} \to M \otimes_\Lambda \Lambda_{\mathfrak{p}} \to E \otimes_\Lambda \Lambda_{\mathfrak{p}} \to B \otimes_\Lambda \Lambda_{\mathfrak{p}} \to 0$ is exact. Now let $g \in (p, T)$ with $g \notin \mathfrak{p}$. Since A is finite, $g^n A = 0$ for some $n > 0$. It follows that $A \otimes_\Lambda \Lambda_{\mathfrak{p}} = 0$ since $g/1$ is a unit in $\Lambda_{\mathfrak{p}}$. Similarly, $B \otimes_\Lambda \Lambda_{\mathfrak{p}} = 0$. If f is irreducible and $(f) \neq \mathfrak{p}$, then $f^m(\Lambda/(f^m)) = 0$ and again $f/1$ is a unit in $\Lambda_{\mathfrak{p}}$, so tensoring with $\Lambda_{\mathfrak{p}}$ removes these terms. Indeed: $(\bigoplus_i \Lambda/(f_i)^{m_i}) \otimes_\Lambda \Lambda_{\mathfrak{p}} = \bigoplus_i (\Lambda/(f_i^{m_i}) \otimes_\Lambda \Lambda_{\mathfrak{p}}) = \bigoplus_{(f_i)=\mathfrak{p}} (\Lambda/(f_i^{m_i}) \otimes_\Lambda \Lambda_{\mathfrak{p}}) = \bigoplus_{(f_i)=\mathfrak{p}} \Lambda_{\mathfrak{p}}/f_i^{m_i}\Lambda_{\mathfrak{p}}$. This proves the lemma.

□

Remark 43. Notice that $\Lambda_{\mathfrak{p}}$ is a PID since it is a noetherian integrally closed domain of dimension 1.

Proposition 5.4.3. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of finitely generated Λ-modules. Then $char(M_1) \cdot char(M_2) = char(M_3)$.*

Proof. This follows from the lemma above and from the structure theorem for modules over a PID.

□

Lemma 5.4.4. *The natural assignment $\psi : M \to \bigoplus_{\mathfrak{p}} (M \bigotimes_\Lambda \Lambda_{\mathfrak{p}})$ gives a well defined map. Moreover $Ker(\psi)$ is finite and is the maximal finite submodule of M.*

Proof. First of all, notice that by lemma 5.4.2 we have that $M \bigotimes_\Lambda \Lambda_{\mathfrak{p}} = 0$ if $\mathfrak{p}$ does not divide $char(M)$, so the sum over $\mathfrak{p}$ is actually finite. This gives a well defined map. Notice that every finite submodule of M is contained in $Ker(\psi)$. Since Λ is Noetherian and M is finitely generated, $Ker(\psi)$ is finitely generated. It is therefore finite by definition of Kernel.

□

Now for **any** Λ-module X define

$$\widetilde{\alpha}(X) \overset{\text{def}}{=} Hom_{\mathbb{Z}_p}(Coker(\psi), \mathbb{Q}_p/\mathbb{Z}_p).$$

Notice that we have an action of Γ on $\widetilde{\alpha}(X)$: $(\gamma f)(x) = f(\gamma^{-1}x)$ for $\gamma \in \Gamma$ and $x \in Coker(\psi)$. Now we define an action of Λ is a similar way: $(g(T)f)(x) = f(g((1+T)^{-1}-1)x)$ for $g(T) \in \Lambda$. It is convenient to twist this action. Hence $\widetilde{\alpha}(X)$ is a Λ-module. Consider the involution:

$$\tau : \Lambda \to \Lambda,\ g(T) \mapsto g((1+T)^{-1}-1) = \widetilde{g}(T)$$

If X is *any* Λ-module, let $\widetilde{X}$ be X with a new action of Λ:

$$g(T) \star x \overset{\text{def}}{=} \widetilde{g}(T)x$$

In a similar way we set $\gamma \star x = \gamma^{-1}x$ for $\gamma \in \Gamma$. In particular note that

$$\tau : \widetilde{\Lambda/(f)} \to \Lambda/(\widetilde{f})$$

is an isomorphism of Λ-modules since $g(T) \star h(T) = \widetilde{g}(T)h(T)$ maps to $g(T)\widetilde{h}(T)$.

Definition 5.4.1. Let the notation as above. Then $\alpha(X) = \widetilde{\widetilde{\alpha}(X)}$ is called the *Iwasawa-adjoint* of X.

Observe that the definition is not suitable for computations, so we need another approach. For a fixed finitely generated torsion Λ-module M as before, we define an *admissible sequence* to be a sequence $\sigma_0, \sigma_1, \ldots$ of elements of Λ such that σ_n and $char(M)$ are relatively prime, with $\sigma_n \neq 0$ (observe that this works also for finite M), and $\sigma_{n+1}/\sigma_n \in (p, T)$ for all $n \geq 0$. Note that

$$\frac{1}{\sigma_0}\Lambda \subset \frac{1}{\sigma_1}\Lambda \subseteq \frac{1}{\sigma_2}\Lambda \subset \cdots$$

and so

$$\varinjlim \frac{1}{\sigma_n}\Lambda = \bigcup \frac{1}{\sigma_n}\Lambda$$

Proposition 5.4.5. *The map*

$$\phi : M \otimes_\Lambda (\textstyle\bigcup_n \frac{1}{\sigma_n}\Lambda) \to \bigoplus_{\mathfrak{p}}(M \otimes_\Lambda \Lambda_{\mathfrak{p}}),\ x \otimes \frac{1}{\sigma_n} \mapsto (\ldots, x \otimes \frac{1}{\sigma_n}, \ldots)$$

is an isomorphism of Λ-modules (the direct sum is taken over any set of prime ideals $\mathfrak{p}$ containing all (height one) prime divisors of $char(M)$ and such that $\sigma_n \in {\Lambda_{\mathfrak{p}}}^\times$ for all n and $\mathfrak{p}$).

Proof. Note that every element on the LHS can be written in the form $x \otimes \frac{1}{\sigma_n}$. Suppose now that $\phi(x \otimes \frac{1}{\sigma_n}) = 0$. Multiplying by σ_n, we find that $x \otimes 1 = 0$ in $M \otimes_\Lambda \Lambda_{\mathfrak{p}}$ for all $\mathfrak{p}$ (since $\sigma_n \in \Lambda_{\mathfrak{p}}^\times$). Therefore $x \in Ker(\psi)$, which is finite. Lemma 5.4.1 (part 2.) implies that $(\sigma_{n+a}/\sigma_n)x = 0$ for some $a \geq 0$, so

$$x \otimes \frac{1}{\sigma_n} = \frac{\sigma_{n+a}}{\sigma_n}x \otimes \frac{1}{\sigma_{n+a}} = 0$$

Hence ϕ is injective.
Let $\mathfrak{p} = (f)$ and let $x \otimes \frac{1}{\eta} \in M \otimes_\Lambda \Lambda_{\mathfrak{p}}$. To prove that ϕ is surjective, by the linearity of the map it is enough to show that $(0, \ldots, x \otimes \frac{1}{\eta}, \ldots, 0) \in Im(\phi)$ with $\eta \in \Lambda \setminus \mathfrak{p} = S$. Let

$\lambda \in \Lambda$ be such that $\lambda M = 0$ but $\lambda \neq 0$ (for example, a suitable multiple of $char(X)$ will work by lemma 5.4.1, part 1.). Write $\lambda = f^b \lambda_1$, with f such that does not divide λ_1. Let $Y = \lambda_1 M / \lambda_1^2 \eta M$. Then $(\lambda_1 \eta, f^b) Y = 0$. Notice that $(\lambda_1 \eta, f^b)$ has finite index in Λ: indeed f is a prime element, $\eta \in S$, we choose λ_1 properly and moreover we have a previous lemma. Hence since Y is finitely generated, Y is finite. Therefore $\sigma_c Y = 0$ for some $c \geq 0$, so $\sigma_c \lambda_1 x = \lambda_1^2 \eta y$ for some $y \in M$. In $M \otimes_\Lambda \Lambda_{\mathfrak{p}}$ we have that:

$$\lambda_1 y \otimes \frac{1}{\sigma_c} = \lambda_1^2 \eta y \otimes \frac{1}{\lambda_1 \eta \sigma_c} = x \otimes \frac{1}{\eta}$$

In $M \otimes_\Lambda \Lambda_{\mathfrak{q}}$, with $\mathfrak{q} \neq \mathfrak{p}$, we get:

$$\lambda_1 y \otimes \frac{1}{\sigma_c} = f^b \lambda_1 y \otimes \frac{1}{\sigma_c f^b} = 0$$

Therefore ϕ is surjective.

□

Now applying $M \otimes_\Lambda$ (which is a right exact functor) to the exact sequence

$$0 \to \Lambda \to \bigcup_n \tfrac{1}{\sigma_n} \Lambda \to (\bigcup_n \tfrac{1}{\sigma_n} \Lambda)/\Lambda \to 0$$

we obtain:

$$X \to \bigoplus_{\mathfrak{p}} (X \bigotimes_\Lambda \Lambda_{\mathfrak{p}}) \to X \bigotimes_\Lambda (\bigcup_n \tfrac{1}{\sigma_n} \Lambda)/\Lambda \to 0$$

Therefore we deduce that

$$Coker(\psi) \simeq X \bigoplus_\Lambda (\bigcup_n \tfrac{1}{\sigma_n} \Lambda)/\Lambda$$

Now notice that if $\sigma_n = (T - \pi)^n$ with $\pi \in p\mathbb{Z}_p$ then:

$$\bigcup_n \tfrac{1}{\sigma_n} \Lambda = \Lambda[\tfrac{1}{T-\pi}] = \mathbb{Z}_p((T - \pi))$$

where the last term is the ring of Laurent series with only finitely many negative exponents (for the above line recall that $\Lambda = \mathbb{Z}_p[[T]] = \mathbb{Z}_p[[T - \pi]]$).

Proposition 5.4.6. *Assume $f \in \Lambda, \pi \in p\mathbb{Z}_p$, and $f(\pi) \neq 0$. Then*

$$\Lambda/(f) \simeq Hom_{\mathbb{Z}_p}(\Lambda/(f) \bigotimes_\Lambda \Lambda[\tfrac{1}{T-\pi}]/\Lambda, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \alpha(\Lambda/(f))$$

Corollary 5.4.7. *If E is an elementary torsion Λ-module, then $E \simeq \alpha(E)$.*

Proposition 5.4.8. *1. $\alpha(M)$ has no non-zero finite Λ-submodules*

2. If M is finite, then $\alpha(M) = 0$.

Proof. For both the claims, notice that it suffices to prove them for $\widetilde{\alpha}(M)$.

1. Choose $\pi \in p\mathbb{Z}_p \subset p\Lambda$ so that $\{(T - \pi)^n\}_n$ is an admissible sequence for M. Let ϕ lie in a finite Λ-submodule of $\widetilde{\alpha}(X) = Hom_{\mathbb{Z}_p}(M \otimes_\Lambda \Lambda[\frac{1}{T-\pi}]/\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$. Since $\widetilde{(T - \pi)} = (1 + T)^{-1} - \pi - 1 \in (p, T)$, then lemma 5.4.1 implies that $\widetilde{(T - \pi)}^n \phi = 0$ for n sufficiently large. Now consider $b \otimes c \in X \otimes_\Lambda \Lambda[\frac{1}{T-\pi}]/\Lambda$. Then we have $b \otimes c = (T - \pi)^n b \otimes c/(T - \pi)^n$ and so

$$\phi(b \otimes c) = \phi((T-\pi)^n b \otimes c/(T-\pi)^n) = (\widetilde{(T-\pi)}^n\phi)(b \otimes c/(T-\pi)^n) = 0$$

We deduce that $\phi = 0$ and so we are done.

2. If X is finite, then still by lemma 5.4.1 we have $(T-\pi)^n X = 0$ for n sufficiently large, so that $X \otimes_\Lambda [\frac{1}{T-\pi}]/\Lambda = 0$ arguing similarly to the previous claim.

□

Proposition 5.4.9. *An exact sequence $0 \to X \to Y \to Z \to 0$ of finitely generated torsion Λ-modules induces an exact sequence*

$$0 \to \alpha(Z) \to \alpha(Y) \to \alpha(X) \to \textit{some finite } \Lambda\textit{-module.}$$

Proof. Notice that also for this claim is enough to prove that it holds for $\widetilde{\alpha}(X), \widetilde{\alpha}(Y)$ and $\widetilde{\alpha}(Z)$. Consider the commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r] \arrow[d, "\psi_X"] & Y \arrow[r] \arrow[d, "\psi_Y"] & Z \arrow[r] \arrow[d, "\psi_Z"] & 0 \\
0 \arrow[r] & \oplus_{\mathfrak{p}}(X \otimes_\Lambda \Lambda_{\mathfrak{p}}) \arrow[r] & \oplus_{\mathfrak{p}}(Y \otimes_\Lambda \Lambda_{\mathfrak{p}}) \arrow[r] & \oplus_{\mathfrak{p}}(Z \otimes_\Lambda \Lambda_{\mathfrak{p}}) \arrow[r] & 0
\end{tikzcd}$$

Since localization is exact, we have that the bottom row is exact. Hence the Snake Lemma gives us an exact sequence:

$$Ker(\psi_Z) \to Coker(\psi_X) \to Coker(\psi_Y) \to Coker(\psi_Z) \to 0.$$

Since $\mathbb{Q}_p/\mathbb{Z}_p$ is an injective $\mathbb{Z}_p$-module, we have that $Hom_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ is an exact contravariant functor and applying it to the sequence above we obtain the result (using also the fact that $Ker(\psi_Z)$ is finite by lemma 5.4.4).

□

Proposition 5.4.10. *Let X and Y be finitely generated torsion Λ-modules with $X \sim Y$. Then $\alpha(Y) \sim \alpha(X)$.*

Proof. By hypothesis, there is an exact sequence:

$$0 \to A \to X \to Y \to B \to 0$$

with A and B finite Λ-modules. Of course, we may assume A contained in X and so considering $0 \to A \to X \to X/A \to 0$ and the previous proposition we obtain an exact sequence

$$0 \to \alpha(X/A) \to \alpha(X) \to \alpha(A)$$

By proposition 5.5.11, we have that $\alpha(A) = 0$ and so we deduce $\alpha(X/A) \simeq \alpha(X)$. On the other hand, notice that we have an exact sequence $0 \to X/A \to Y \to B \to 0$ and so still applying the previous proposition we get

$$0 \to \alpha(B) \to \alpha(Y) \to \alpha(X/A) \to \text{some finite } \Lambda\text{-module}$$

Again by proposition 5.5.11, we have $\alpha(B) = 0$. This implies $\alpha(Y) \sim \alpha(X/A) \simeq \alpha(X)$.

□

Corollary 5.4.11. *$X \sim \alpha(X)$ and also $\alpha(X)$ is a finitely generated torsion Λ-module.*

Proof. By the structure theorem we deduce that there is an elementary Λ-module E such that $X \sim E$. By corollary 5.4.7 and the previous proposition, we have that $X \sim E \simeq \alpha(E) \sim \alpha(X)$. Hence, since X is a finitely generated torsion Λ-module, so must be $\alpha(X)$.

□

Proposition 5.4.12. *$\varinjlim X/\sigma_n X \simeq X \bigotimes_\Lambda (\bigcup_n \frac{1}{\sigma_n}\Lambda/\Lambda)$ and so*

$$\widetilde{\alpha}(X) \simeq Hom_{\mathbb{Z}_p}(\varinjlim X/\sigma_n X, \mathbb{Q}_p/\mathbb{Z}_p)$$

Proof. By a basic property of tensor products (see [**Bou1**] or [**At**]) we have that:

$$X/\sigma_n X \simeq X \bigotimes_\Lambda (\Lambda/\sigma_n\Lambda) \simeq X \bigotimes_\Lambda (\tfrac{1}{\sigma_n}\Lambda/\Lambda)$$

Now we give $\{\frac{1}{\sigma_n}\Lambda/\Lambda\}_n$ the structure of a direct system through the natural inclusions $\frac{1}{\sigma_n}\Lambda/\Lambda \to \frac{1}{\sigma_{n+1}\Lambda/\Lambda}$. Hence using the facts that $\varinjlim$ is a functor and that direct limits commute with tensor products (see [**At**] again), we get that:

$$\varinjlim X/\sigma_n X \simeq \varinjlim (X \otimes_\Lambda (\tfrac{1}{\sigma_n}\Lambda/\Lambda)) \simeq X \otimes_\Lambda \varinjlim (\tfrac{1}{\sigma_n}\Lambda/\Lambda) \simeq X \otimes_\Lambda (\textstyle\bigcup_n \frac{1}{\sigma_n}\Lambda/\Lambda)$$

□

Now we recall some notation of chapter 4.

Let $K_\infty|K$ be a $\mathbb{Z}_p$-extension of a number field K. Let A_n be the p-part of the class group of K_n and L_n be the Hilbert p-class field of K_n, so that

$$X_n = Gal(L_n|X_n) \simeq A_n.$$

It follows that $X = \varprojlim_n X_n \simeq \varprojlim_n A_n$. By lemma 4.2.6 there is an index e and a submodule $Y_e \subseteq X$ such that

$$A_n \simeq X_n \simeq X/\nu_{n,e} Y_e$$

for all $n \geq e$, where

$$\nu_{n,e} \overset{\text{def}}{=} ((1+T)^{p^n} - 1)/((1+T)^{p^e} - 1)$$

Moreover we consider $\varinjlim_n A_n$ with respect to the natural maps $A_n \to A_{n+1}$. Then one can prove that the following diagram

$$\begin{tikzcd} A_n \arrow[r, "natural"] \arrow[d, "\simeq"] & A_{n+1} \arrow[d, "\simeq"] \\ X_n \arrow[r, "x \mapsto \nu_{n+1,n} x"] & X_{n+1} \end{tikzcd}$$

commutes for every n (see [**Wa**] for details). Using this fact, we prove the next proposition.

Proposition 5.4.13. *$\widetilde{X} \sim Hom_{\mathbb{Z}_p}(\varinjlim A_n, \mathbb{Q}_p/\mathbb{Z}_p)$*

Proof. Consider the exact sequence:

$$0 \to Y_e/\nu_{n,e}Y_e \to X/\nu_{n,e}Y_e \to X/Y_e \to 0$$

We know that $\varinjlim$ is an exact functor (see [[**Bou1**]] for example), and so using the previous observation and recalling that $A_n \simeq X_n = X/\nu_{n,e}Y_e$ we get another exact sequence

$$0 \to \varinjlim(Y_e/\nu_{n,e}Y_e) \to \varinjlim A_n \to \varinjlim X/Y_e \to 0$$

Now since $X/Y_e \simeq A_e$ is finite (by a previous proposition), by the definition of $\nu_{n,e}$ there exist $m \geq n \geq e$ such that $\nu_{m,n}X/Y_e = 0$. Notice that this implies $\varinjlim X/Y_e = 0$. Then $\varinjlim Y_e/\nu_{n,e}Y_e \simeq \varinjlim A_n$. From proposition 5.4.12 we deduce that $\widetilde{\alpha}(Y_e) = Hom(\varinjlim Y_e/\nu_{n,e}Y_e, \mathbb{Q}_p/\mathbb{Z}_p)$ (notice that $\{\nu_{n,e}\}_n$ form an admissible sequence for Y_e). Since by a previous proposition $Y_e \simeq X$, we have $\widetilde{X} \sim \widetilde{\alpha}(X) \sim \widetilde{\alpha}(Y_e)$ and so the claim holds.

□

Let the notation be as in a previous proposition. Notice that the previous proof shows also that the following fact holds:

Proposition 5.4.14. $\widetilde{\epsilon_i X} \simeq Hom_{\mathbb{Z}_p}(\varinjlim \epsilon_i A_n, \mathbb{Q}_p/\mathbb{Z}_p)$

Now we arrive to the main result of this section. A complete proof requires an additional work on Σ_∞ that we decided to omit. Therefore, we are going to sketch the proof (more details can be found in [**Wa**]).

Proposition 5.4.15. *Suppose $\epsilon_i X$ has characteristic polynomial $f(T)$. Then*

$$Hom_{\mathbb{Z}_p}(\varinjlim \epsilon_i A_n, \mathbb{Q}_p/\mathbb{Z}_p)$$

has characteristic polynomial equal to $f((1+T)^{-1}-1)$ and $\epsilon_{1-i}\Sigma_\infty$ has characteristic polynomial $f(\kappa(1+T)^{-1}-1)$ where $\kappa \in 1+p\mathbb{Z}_p$ is defined by $\gamma_0\zeta_{p^n} = \zeta_{p^n}^\kappa$ for all n.

Sketch of proof. The first part follows from the previous proposition and the definition of the action of Λ on $\widetilde{\epsilon_i X}$. For the second one, one may observe that if γ_0 acts on $\epsilon_i X$ as $(1+T)$, then it acts on $\widetilde{(\epsilon_i X)}(1) \overset{\text{def}}{=} \widetilde{\epsilon_i X} \otimes_{\mathbb{Z}_p} T \simeq \epsilon_j \Sigma_\infty$ by $\kappa(1+T)^{-1}$ (where T here is the same of proposition) . Then one may prove that this implies the statement.

□

5.5 Some techniques of Iwasawa theory

The following technical results will be fundamental to prove the Main conjecture. First of all, we need to fix other notations:

- p = an odd prime
- γ_0 = a generator of $\Gamma = Gal(\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q}(\zeta_p))$
- $P_n = \omega_n = (1+T)^{p^n} - 1 = \gamma_0^{p^n} - 1$ (we use the usual identification $\gamma_0 = 1+T$)
- Γ_n = the subgroup of Γ of index p^n

- $M^{\Gamma_n} = \{m \in M | \gamma_0^{p^n} m = m\} = Ker(M \xrightarrow{P_n} M)$ where M is a Λ-module
- $M_{\Gamma_n} = M/P_n = M/(P_n M) = Coker(M \xrightarrow{P_n} M)$
- $\chi = \omega^j = j^{th}$-power of the Teichmüller character ω for some $j > 0, j$ even (i.e. a non trivial even character of $Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q})$)

Now we summarize in a proposition some fundamental results that, more or less, we saw earlier:

Proposition 5.5.1. *Let $\overline{C}_1^n, X_n, U_1^n$ and Σ_n as in the previous sections. Then:*

1. $\epsilon_\chi(\overline{C}_1^\infty/P_n) \simeq \epsilon_\chi \overline{C}_1^n$
2. $\epsilon_\chi(X/P_n) \simeq \epsilon_\chi X_n$
3. $\epsilon_\chi(U_1^\infty/P_n) \simeq \epsilon_\chi U_1^n$
4. $\epsilon_\chi(\Sigma_\infty/P_n) \simeq \epsilon_\chi \Sigma_n$

Proof. The first statement follows by theorem 4.4.3. The second and the third ones respectively by corollary 4.2.13 and theorem 4.4.2. The last one is discussed in section 4.5.

□

Lemma 5.5.2. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of Λ-modules.*

1. *Set $\Gamma_0 \overset{\text{def}}{=} \Gamma$. Then for every $n \geq 0$ there is an exact sequence*
$$0 \to M_1^{\Gamma_n} \to M_2^{\Gamma_n} \to M_3^{\Gamma_n} \to (M_1)_{\Gamma_n} \to (M_2)_{\Gamma_n} \to (M_3)_{\Gamma_n} \to 0$$
In particular, $Ker((M_1)_{\Gamma_n} \to (M_2)_{\Gamma_n}) \simeq M_3^{\Gamma_n}/Im(M_2^{\Gamma_n})$.
2. *If M_3 is a finitely generated Λ-module and $(M_3)_{\Gamma_n}$ is finite, then $M_3^{\Gamma_n}$ is finite*

Proof. 1. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d, "P_n \cdot"] & M_2 \arrow[r] \arrow[d, "P_n \cdot"] & M_3 \arrow[r] \arrow[d, "P_n \cdot"] & 0 \\
0 \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & M_3 \arrow[r] & 0
\end{tikzcd}$$

where the vertical maps are multiplication by $P_n = \gamma_0^{p^n} - 1$. By definition we have $M_i^{\Gamma_n} = Ker(M_i \xrightarrow{P_n \cdot} M_i)$ and $(M_i)_{\Gamma_n} = Coker(M_i \xrightarrow{P_i \cdot} M_i)$. Then the Snake Lemma yields the exact sequence of the statement and we can conclude.

2. Assume that M_3/P_n is finite. Hence M_3 is a Λ-module with torsion. Now consider the exact sequence
$$0 \to M_3^{\Gamma_n} \to M_3 \xrightarrow{P_n \cdot} M_3 \to (M_3)_{\Gamma_n} \to 0.$$

We deduce that $M_3/M_3^{\Gamma_n} \simeq P_nM_3$. Therefore $char(P_nM_3) = char(M_3/M_3^{\Gamma_n})$. On the other hand if we consider the exact sequence

$$0 \to P_nM_3 \to M_3 \to (M_3)_{\Gamma_n} \to 0$$

and we use the previous lemma we get that

$$char(P_nM_3) = char(M_3) \cdot char(M_3/P_n) = char(M_3)$$

However $char(M_3) = char(M_3^{\Gamma_n}) \cdot char(M_3/M_3^{\Gamma_n})$ by

$$0 \to M_3^{\Gamma_n} \to M_3 \to M_3/M_3^{\Gamma_n} \to 0$$

Substituting, we obtain that $char(M_3^{\Gamma_n}) = 1$, hence $M_3^{\Gamma_n}$ is finite by lemma 5.4.1. □

Here is a technical result which deals only with the theory of compact groups. For more details look at [**Wa**].

Lemma 5.5.3. *For each $n \geq 1$, let $0 \longrightarrow A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n \to 0$ be an exact sequence of compact groups. Then the sequence*

$$0 \to \varprojlim_n A_n \xrightarrow{f} \varprojlim_n B_n \xrightarrow{g} \varprojlim_n C_n \to 0$$

is exact. In particular, $\varprojlim_n (B_n/A_n) \simeq \varprojlim_n B_n/\varprojlim_n A_n$.

Proposition 5.5.4. *There is an ideal $\mathfrak{U}$ of Λ of finite index such that, for all n, $\mathfrak{U}$ annihilates the kernel and cokernel of the natural map $\epsilon_\chi\overline{E}_1^\infty/P_n \to \epsilon_\chi\overline{E}_1^n$. The orders of these kernels and cokernels are bounded independently of n.*

Proof. By corollary 5.3.3, lemmas 5.5.3 and 5.5.2, we have the commutative diagram:

$$\begin{tikzcd}
\epsilon_\chi(X^{\Gamma_\infty}/Im(\Sigma_n^{\Gamma_n})) \arrow[r] & \epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)/P_n \arrow[r, "\phi_1"] \arrow[d, "\pi_1"] & \epsilon_\chi\Sigma_\infty/P_n \arrow[r] \arrow[d] & \epsilon_\chi X/P_n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \epsilon_\chi(U_1^n/\overline{E}_1^n) \arrow[r] & \epsilon_\chi\Sigma_n \arrow[r] & \epsilon_\chi X_n \arrow[r] & 0
\end{tikzcd}$$

The second and third vertical maps are isomorphisms by proposition 5.5.1. By a diagram chase, one shows that $Ker(\phi_1) = Ker(\pi_1)$. Since $\epsilon_\chi X/P_n \simeq \epsilon_\chi X_n$ is finite, lemma 5.5.2 implies that $\epsilon_\chi(X^{\Gamma_n})$ is finite too. Let $\epsilon_\chi X_{finite}$ be the maximum finite Λ-submodule of $\epsilon_\chi X$. Then of course $\epsilon_\chi(X^{\Gamma_n}) \subseteq \epsilon_\chi X_{finite}$. By lemma 5.5.2, using the top sequence we have that $Ker(\phi_1)$ is isomorphic to a submodule of a quotient of $\epsilon_\chi X_{finite}$. Therefore, the order of $Ker(\phi_1)$ is finite and bounded independently of n. Now consider the commutative diagram:

$$\begin{tikzcd}
\epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)^{\Gamma_n} \arrow[r] & \epsilon_\chi\overline{E}_1^\infty/P_n \arrow[r, "\phi_2"] \arrow[d, "\pi_2"] & \epsilon_\chi U_1^\infty/P_n \arrow[r] \arrow[d] & \epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)/P_n \arrow[r] \arrow[d, "\pi_1"] & 0 \\
0 \arrow[r] & \epsilon_\chi(\overline{E}_1^n) \arrow[r] & \epsilon_\chi U_1^n \arrow[r] & \epsilon_\chi(U_1^n/\overline{E}_1^n) \arrow[r] & 0
\end{tikzcd}$$

By a diagram chase we deduce that $Ker(\pi_2) \simeq Ker(\phi_2)$. We claim that $\epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)/P_n$ is finite. For the moment we assume that this claim is true and we postpone its proof until the end of the main proof. Hence by reasoning as above we find that $Ker(\phi_2)$ is isomorphic to a quotient of $\epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)_{finite}$. Now we replace $\epsilon_\chi\overline{E}_1^\infty$ by $\epsilon_\chi(\overline{E}_1^\infty)/Ker(\phi_2)$ in the above diagram so that we can apply the Snake Lemma. We deduce that $Ker(\pi_1) = Ker(\phi_1) \simeq Coker(\pi_2)$. Now by lemma 5.4.1 (point 2) we have ideals $\mathfrak{U}_1, \mathfrak{U}_2$ of finite index in Λ which annihilate respectively $\epsilon_\chi X_{finite}$ and $\epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)_{finite}$. Considering $\mathfrak{U}_1 + \mathfrak{U}_2$ we deduce that there exists an ideal $\mathfrak{U}$ (for example $\mathfrak{U}_1 + \mathfrak{U}_2$ itself) of finite index in Λ that annihilates:

$$\epsilon_\chi X_{finite} \bigoplus \epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)_{finite}$$

Now since $Ker(\phi_1)$ and $Ker(\phi_2)$ are isomorphic to submodules of quotients respectively of $\epsilon_\chi X_{finite}$ and $\epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)_{finite}$, we deduce that $\mathfrak{U}$ annihilates $Ker(\pi_2) \bigoplus Coker(\pi_2)$ as we wanted.

Now we prove the claim as promised. First of all notice, that we have a surjection

$$\epsilon_\chi(U_1^\infty/\overline{C}_1^\infty)/P_n \twoheadrightarrow \epsilon_\chi(U_1^\infty/\overline{E}_1^\infty)/P_n$$

By theorem 4.4.5, we have $\epsilon_\chi(U_1^\infty/\overline{C}_1^\infty) \simeq \Lambda/(f_\chi)$ where $f_\chi = f((1+p)\cdot(1+T)^{-1}-1, \chi)$ and $f(T, \chi)$ is the power series that gives the p-adic L-function. Therefore $\epsilon_\chi(U_1^\infty/\overline{C}_1^\infty)/P_n \simeq \Lambda/(f_\chi, P_n)$. Now the roots of P_n are $\zeta_{p^n}^j - 1$ with $0 \leq j < p^n$. Theorem 3.4.4 says that

$$f(\zeta_{p^n}^j(1+p)^s - 1, \chi) = L_p(s, \chi\psi_n^j)$$

where $\psi_n(1+p) = \zeta_{p^n}$ is a primitive p^n-th root of unity. Hence by lemma 2.2.9 we get:

$$f_\chi(\zeta_{p^n}^j - 1) = f(\zeta_{p^n}^{-j}(1+p) - 1, \chi) = L_p(1, \chi\psi_n^{-j}) \neq 0$$

Therefore f_χ and P_n have no common roots, i.e. they are relatively prime. By lemma 3.2.9, we also have that $\Lambda/(f_\chi, P_n)$ is finite. This proves the claim and consequently even the proposition.

□

Lemma 5.5.5. *There is an exact sequence*

$$0 \to \epsilon_\chi\overline{E}_1^\infty \xrightarrow{\theta} \Lambda \to \textit{some finite } \Lambda\textit{-module} \to 0$$

Proof. By theorem 4.4.2, we know that $\epsilon_\chi U_1^\infty \simeq \Lambda$. Since Λ is a noetherian integral domain, we have that $\epsilon_\chi\overline{E}_1^\infty \subseteq \epsilon_\chi U_1^\infty$ is a finitely generated torsion-free Λ-module. By the classification of finitely generated Λ-modules, we deduce that there is a pseudo-isomorphism $\epsilon_\chi\overline{E}_1^\infty \sim \Lambda$. Therefore there exists an exact sequence $0 \to A \to \epsilon_\chi\overline{E}_1^\infty \xrightarrow{\theta} \Lambda \to B \to 0$ with A, B finite Λ-modules. However, since $\epsilon_\chi\overline{E}_1^\infty$ is torsion-free, it has no finite Λ-submodules, namely $A = 0$ and so θ must be an injection.

□

Proposition 5.5.6. *Let $\mathfrak{U}$ be as in the previous proposition and let $\alpha \in \mathfrak{U}$. Let $h_\chi = char(\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty))$. For each $n \geq 0$ there is a map*

$$\theta_\alpha^n : \epsilon_\chi\overline{E}_1^n \to \Lambda_n = \Lambda/P_n$$

such that

$$\theta_\alpha^n(\epsilon_\chi\overline{C}_1^n) = \alpha h_\chi\Lambda_n$$

Proof. The map θ of the previous lemma induces an exact sequence

$$0 \to \epsilon_\chi(\overline{E}_1^\infty/C_1^\infty) \xrightarrow{\widetilde{\theta}} \Lambda/\theta(\epsilon_\chi\overline{C}_1^\infty) \to \text{some finite } \Lambda\text{-module} \to 0$$

By abuse of notation, we still write θ instead of $\widetilde{\theta}$. Let η be as in lemma 4.4.4. Then, by construction of η, we have $\epsilon_\chi\overline{C}_1^\infty = \epsilon_\chi(\eta)\Lambda$, so $\theta(\epsilon_\chi\overline{C}_1^\infty)$ is the principal ideal generated by $\theta(\epsilon_\chi\eta)$. In particular, $\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)$ is pseudo-isomorphic to $\Lambda/\theta(\epsilon_\chi\eta)$ (just take 0 as finite module on the left). Hence by definition of characteristic polynomial, h_χ and $\theta(\epsilon_\chi\eta)$ differ by a unit of Λ.

Now let $\pi_n : \epsilon_\chi(\overline{E}_1^\infty/P_n) \to \epsilon_\chi\overline{E}_1^n$ be the natural map. By the choice of α, we have $\alpha Ker(\pi_n) = 0 = \alpha Coker(\pi_n) = 0$. Let $\theta_n : \epsilon_\chi(\overline{E}_1^\infty/P_n) \to \Lambda_n$ be induced by θ. Now notice that Λ_n has no $\mathbb{Z}_p$-torsion and so in particular it has no $\mathbb{Z}$-torsion. Moreover $Ker(\pi_n)$ is finite by the previous lemma. Hence we get:

$$Ker(\pi_n) \subseteq (\epsilon_\chi(\overline{E}_1^\infty/P_n))_{finite} \subseteq Ker(\theta_n)$$

Let $u \in \epsilon_\chi\overline{E}_1^n$. Define

$$\theta_\alpha^n(u) = \theta_n(\pi_n^{-1}(\alpha u)) \in \Lambda_n$$

Since $\alpha Coker\pi_n = 0$, we have $\alpha u \in Im(\pi_n)$, so there exists $v \in \epsilon_\chi(\overline{E}_1^\infty/P_n)$ with $\pi_n(v) = \alpha u$. Since $Ker(\pi_n) \subseteq Ker(\theta_n)$, $\theta_n(v)$ depends only on αu, so θ_α^n is well defined. Indeed if $v', v'' \in \pi_n^{-1}(\alpha u)$ then $\theta_n(v') = \theta_n(v'')$.

Moreover, since $\alpha\pi_n : \alpha\epsilon_\chi(\overline{C}_1^\infty/P_n) \to \alpha\epsilon_\chi\overline{C}_1^n$ is surjective (the kernel is 0 and the image is everything by our choice of α), we have:

$$\theta_\alpha^n(\epsilon_\chi\overline{C}_1^n) = \theta_n(\alpha\epsilon_\chi(\overline{C}_1^\infty/P_n)) = \alpha h_\chi\Lambda_n$$

as we wanted.

□

Remark 44. Notice that by the previous proposition and 5.3.2 we can now rewrite the statement of the Main conjecture as: $char(\epsilon_\chi X) = char(h_\chi)$

Remark 45. It is useful in what follows to recall that in any exact sequence of finite groups, finite modules and finite rings with finite length we have that the product of the cardinalities of the terms in even positions is equal to the product of the cardinalities of terms in odd positions.

Proposition 5.5.7. *Let χ be arbitrary (including $\chi = 1$). There exists a constant $c > 0$ such that:*

$$c^{-1}[\epsilon_\chi\overline{E}_1^n : \epsilon_\chi\overline{C}_1^n] \leq |\Lambda/(P_n, h_\chi)| \leq c[\epsilon_\chi\overline{E}_1^n : \epsilon_\chi\overline{C}_1^n] < \infty$$

for all $n < \infty$

Proof. The case where $\chi = 1$ follows from the previous proposition. Assume now that $\chi \neq 1$. From the proof of proposition 5.5.6, we have an exact sequence

$$0 \to \epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty) \to \Lambda/(h_\chi) \to F \to 0$$

where F is finite.
This yields another exact sequence:

$$F^{\Gamma_n} \to \epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n \to \Lambda/(h_\chi, P_n) \to F/P_n \to 0$$

Indeed: lemma 5.5.2 implies that $Ker(\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n \to \Lambda/(h_\chi, P_n)) \simeq F^{\Gamma_n}/Im(\Lambda/h_\chi^{\Gamma_n})$; thus we can define a map $F^{\Gamma_n} \to F^{\Gamma_n}/Im(\Lambda/h_\chi^{\Gamma_n}) \subseteq \epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n$ that gives us the above sequence.

From this we deduce that

$$|F/P_n| \cdot |\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty| = |F^{\Gamma_n}| \cdot |\Lambda/(h_\chi, P_n)|$$

On one hand we have:

$$\begin{aligned}|\Lambda/(h_\chi, P_n)| &= |F/P_n|/|F^{\Gamma_n}| \cdot |\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n| \leq \\ &\leq |F|/|F^{\Gamma_n}| \cdot |\epsilon_\chi(...)/P_n| \leq |F| \cdot |\epsilon_\chi(...)/P_n|\end{aligned}$$

On the other:

$$|\Lambda/(h_\chi, P_n)| \geq 1/|F^{\Gamma_n}| \cdot |\epsilon_\chi(...)/P_n| \geq 1/|F| \cdot |\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n|$$

Hence, there is a constant $c_1 > 0$ (for example, $c_1 = |F|$) such that

$$c_1^{-1}|\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n| \leq |\Lambda/(h_\chi, P_n)| \leq c_1|\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n|$$

Now applying the Snake Lemma to the exact sequence

$$1 \to \epsilon_\chi\overline{C}_1^\infty \to \epsilon_\chi\overline{E}_1^\infty \to \epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty) \to 1$$

we obtain the top row of the following commutative diagram:

$$\begin{tikzcd}
 & \epsilon_\chi(\overline{C}_1^\infty/P_n) \arrow[r] \arrow[d] & \epsilon_\chi(\overline{E}_1^\infty/P_n) \arrow[r] \arrow[d] & \epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \epsilon_\chi\overline{C}_1^n \arrow[r] & \epsilon_\chi\overline{E}_1^n \arrow[r] & \epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n) \arrow[r] & 1
\end{tikzcd}$$

The first vertical map is an isomorphism by proposition 5.5.1. By a diagram chase, one finds that the kernel and cokernel of the third vertical map are isomorphic to those of the second vertical map, which have order bounded independently of n by proposition 5.5.4.

Now call ϕ the third vertical map and consider the exact sequence

$$0 \to Ker(\phi) \to \epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n \xrightarrow{\phi} \epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n) \to Coker(\phi) \to 0$$

As in one of the previous propositions, we have that

$$|Ker(\phi)| \cdot |\epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n)| = |Coker(\phi)| \cdot |\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n|$$

Now let $c_2 = \max\{|Ker(\phi)|, |Coker(\phi)|\} + 1$. It follows that $c_2 > 0$ is such that

$$c_2^{-1}|\epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n| \leq |\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n| \leq c_2|\epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n| < \infty$$

Indeed, say $c_2 = Ker(\phi) + 1$. Then

$$|\epsilon_\chi(\overline{E}_1^\infty/\overline{C}_1^\infty)/P_n| = |Ker(\phi)|/|Coker(\phi)| \cdot |\epsilon_\chi(\overline{C}_1^n/\overline{C}_1^n|.$$

Hence on one hand we have $|\epsilon_\chi(...)| \leq c_2|\epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n)|$. On the other

$$|\epsilon_\chi(...)| \geq |\epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n)| \geq 1/c_2 \cdot |\epsilon_\chi(\overline{E}_1^n/\overline{C}_1^n)|$$

The case where $c_2 = Coker(\phi) + 1$ is similar. Therefore, setting $c = c_1c_2$ we obtain the statement.

□

Proposition 5.5.8. *Let χ arbitrary and let $\epsilon_\chi X \simeq \varprojlim \epsilon_\chi A_n \sim \bigoplus_{i=1}^k \Lambda/(f_i)$ with $f_i \in \Lambda$. Then there is an ideal $\mathfrak{B}$ of Λ of finite index with the following property: for each $\alpha \in \mathfrak{B}$ and for each n, there are ideal classes $\mathfrak{C}_1, ..., \mathfrak{C}_k \in \epsilon_\chi A_n$ such that the annihilator $Ann(\mathfrak{C}_j) \subseteq \Lambda_n$ of $\mathfrak{C}_j$ in $\epsilon_\chi A_n/(\Lambda_n\mathfrak{C}_1 + ... + \Lambda_n\mathfrak{C}_{j-1})$ satisfies $\alpha Ann(\mathfrak{C}_j) \subseteq f_j\Lambda_n$.*

Proof. By hypothesis, there is an exact sequence

$$\epsilon_\chi X \to \bigoplus_{i=1}^k \Lambda/(f_i) \to F \to 0$$

with F finite Λ-module. Since the tensor is a right exact functor, tensoring with $\Lambda_n = \Lambda/P_n$ we get

$$\epsilon_\chi(X/P_n) \to \bigoplus_{i=1}^k \Lambda_n/(f_i) \to F/P_n \to 0$$

Let $\mathfrak{B}$ be the annihilator of F. By lemma 5.4.1 (part 2.) we have that $\mathfrak{B}$ has finite index in Λ. Now let $\alpha \in \mathfrak{B}$ and consider the element $y = (0, ..., class\ of\ \alpha, ..., 0) \in \bigoplus_i \Lambda_n/(f_i)$ with the class of α in the j-th place. Since in the above sequence y goes to an element of $\alpha(F/P_n) = 0$, we have that y belongs to the image of $\epsilon_\chi(X/P_n) \to \bigoplus_i \Lambda_n/(f_i)$. Hence there is an ideal class $\mathfrak{C}_j \in \epsilon_\chi A_n \simeq \epsilon_\chi(X/P_n)$ such that it maps to y under the previous isomorphism and the map of the upper sequence. Now let $g \in Ann(\mathfrak{C}_j)$ where $Ann(\mathfrak{C}_j) \subseteq \Lambda_n$ is the annihilator of the class of $\mathfrak{C}_j$ in the Λ_n-module $\epsilon_\chi A_n/(\Lambda_n\mathfrak{C}_1 + ... + \Lambda_n\mathfrak{C}_{j-1})$. Then $g\cdot$ (class of $\mathfrak{C}_j$) $= 0$, i.e. $g\mathfrak{C}_j \in \Lambda_n\mathfrak{C}_1 + ... + \Lambda_n\mathfrak{C}_{j-1}$. However, by the construction of $\mathfrak{C}_k$ with $1 \leq k \leq j-1$, under the above composition of maps we have that

$$\Lambda_n\mathfrak{C}_1 + ... + \Lambda_n\mathfrak{C}_{j-1} \mapsto \Lambda_n(\alpha, 0, 0, ...) + ... + \Lambda_n(0, ..., \alpha, ..., 0) =$$
$$= \Lambda_n(\alpha, \alpha, \alpha, ..., 0, 0, 0, ...) \overset{\text{def}}{=} Y$$

where the last α is in $(j-1)$-st position, so that on one hand $g\mathfrak{C}_j \mapsto g \cdot y$, on the other $g\mathfrak{C}_j$ maps in Y. In other words:

$$g \cdot y = g \cdot (0, ..., \alpha, ..., 0) = (0, ..., \text{class of } (g \cdot \alpha), ..., 0) \in Y$$

This implies that the class of $(g \cdot \alpha)$ in $\Lambda_n/f_j\Lambda_n$ is 0, i.e. $g \cdot \alpha \in f_j\Lambda_n$. This concludes the proof.

□

Now suppose that F is a Galois extension of $\mathbb{Q}$ and let $G = Gal(F|\mathbb{Q})$. Let l be a rational prime that splits completely in $F|\mathbb{Q}$. Moreover fix a prime λ of F above l and a primitive root s modulo l. Then notice that s is also a primitive root modulo $\sigma\lambda$ for each $\sigma \in G$. Let $\kappa \in F^\times$ be relatively prime to l and let $\sigma \in G$.

Definition 5.5.1. Let κ, l, σ as above.

1. Define $a_\sigma = ind_{\sigma\lambda}(\kappa) \in \mathbb{Z}/(l-1)\mathbb{Z}$ by
$$\kappa \equiv s^{a_\sigma} \mod (\sigma\lambda)$$

2. Let $M|(l-1)$ and define $\overline{ind}_\lambda(\kappa) = \Sigma_{\sigma\in G} ind_{\sigma\lambda}(\kappa)\sigma \in \mathbb{Z}/M\mathbb{Z}[G]$. This definition depends clearly on the choices of l, λ and s.

3. Similarly, for arbitrary κ, define $b_\sigma = v_{\sigma\lambda}(\kappa)$ =the $\sigma\lambda$-valuation of κ and
$$\overline{v}_\lambda(\kappa) = \Sigma_{\sigma\in G} b_\sigma\sigma \in \mathbb{Z}[G]$$

Lemma 5.5.9. *$\overline{ind}_\lambda$ and $\overline{v}_\lambda$ are $\mathbb{Z}[G]$-homomorphisms.*

The following result (due to Rubin) will play a key role in the proof of the Main Conjecture. Its proof relies on Class field theory and is very technical; we decided then to omit it. For details look at [**Lan1**] or [**Wa**].

Proposition 5.5.10. *Let p be an odd prime. Let $m \geq 1, F = \mathbb{Q}(\zeta_m)^+$ and $G = Gal(F|\mathbb{Q})$. Let $\mathfrak{C}$ be an ideal class of F of order a power of p, let M be a power of p, and let $L \geq 1$. Suppose we have a finite $\mathbb{Z}[G]$-module*
$$W \subset F^\times/(F^\times)^M$$
and a $\mathbb{Z}[G]$-homomorphism
$$\psi : W \to \mathbb{Z}/M\mathbb{Z}[G]$$
Then there are infinitely many primes λ of F such that:

1. *$\lambda \in \mathfrak{C}$;*

2. *$l \equiv 1 \mod ML$ and l splits completely in F;*

3. *the λ-adic valuation of each $w \in W$ is congruent to $0 \mod M$,*

4. *there exists $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that*
$$\overline{ind}_\lambda(w) = u\psi(w)$$
for all $w \in W$.

In order to prove proposition 5.3.2, we are going to assume a fact that follows from some considerations regarding the theory of the ideal class groups. For a proof see [**Wa**].

Proposition 5.5.11. *Let $\chi = 1$ (i.e. $\epsilon_\chi = \epsilon_0$). Then $\epsilon_0(\overline{E}_1^n/\overline{C}_1^n) = 1$ for all $n \leq \infty$. Moreover, $\epsilon_0 X_n = 0$ for all $n \leq \infty$ (we set $X_\infty = X$ in this case).*

Here is the proof of proposition 5.3.2:

Proof. By theorem 4.4.5 and lemma 5.5.3, we know that for even $j \not\equiv 0 \mod (p-1)$ we have

$$\epsilon_j(U_1^\infty/\overline{C}_1^\infty) \simeq \varprojlim \epsilon_j(U_1^n/\overline{C}_1^n) \simeq \Lambda/(f(\frac{1+p}{1+T}-1,\omega^j)) \qquad (5.1)$$

Now let L_n be the maximal unramified abelian p-extension of $\mathbb{Q}(\zeta_{p^{n+1}})$ and let M_n be the maximal abelian p-extension of $\mathbb{Q}(\zeta_{p^{n+1}})$ unramified outside p. Moreover recall that $X_n = Gal(L_n|\mathbb{Q}(\zeta_{p^{n+1}}))$ and $\Sigma_n = Gal(M_n|\mathbb{Q}(\zeta_{p^{n+1}}))$. From corollary 5.3.3 we have an injection

$$U_1^n/\overline{E}_1^n \hookrightarrow \Sigma_n$$

and so $U_1^\infty/\overline{E}_1^\infty \hookrightarrow \Sigma_\infty$.

Consider now the following two exact sequences:

1. $0 \to \epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty) \to \epsilon_j(U_1^\infty/\overline{C}_1^\infty) \to \epsilon_j(U_1^\infty/\overline{E}_1^\infty) \to 0$
2. $0 \to \epsilon_j X \to \epsilon_j\Sigma_\infty \to \epsilon_j(U_1^\infty/\overline{E}_1^\infty) \to 0$

By proposition 5.4.3 we get:

- $char(\epsilon_j(U_1^\infty/\overline{C}_1^\infty) = char(\epsilon_j(U_1^\infty/\overline{E}_1^\infty)) \cdot char(\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty))$
- $char(\epsilon_j\Sigma_\infty) = char(\epsilon_j X) \cdot char(\epsilon_j(U_1^\infty/\overline{E}_1^\infty))$

Hence dividing the first expression by the second one we obtain:

$$\frac{char(\epsilon_j(U_1^\infty/\overline{C}_1^\infty))}{char(\epsilon_j\Sigma_\infty)} = \frac{char(\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty))}{char(\epsilon_j X)}$$

Therefore by the above expression and by expression 5.1 we deduce that: $char(\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty)) = char(\epsilon_j X)$ *if and only if* $f(\frac{1+p}{1+T}-1,\omega^j)$ *differs from* $char(\epsilon_j\Sigma_\infty)$ *by a unit of* Λ.

By proposition 5.4.15, this is equivalent to $f(T,\omega^j)$ and $char(\epsilon_{1-j}X)$ differing by a unit of Λ. This proves the equivalence of 1. and 2.

Suppose now that $char(\epsilon_j X)$ divides $char(\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty))$ for all even $j \not\equiv 0 \mod (p-1)$. By proposition 5.5.11 we have that both groups are trivial for $j = 0$, so we may assume this divisibility happens for all j. Set $\epsilon_+ = \sum_j \epsilon_j$ with j even and $0 \leq j \leq p-3$. Then $char(\epsilon_+ X)$ divides $char(\epsilon_+(\overline{E}_1^\infty/\overline{C}_1^\infty))$ and we have equality if and only if there is equality for each j.

Notice that:

$$\prod_j |\epsilon_j(\overline{E}_1^n/\overline{C}_1^n)| = |\overline{E}_1^n/\overline{C}_1^n| = p\text{-part of } [E^n : C^n] = |\epsilon_+ X_n| = p^{\lambda^+ n+\mu^+ p^n+\nu^+}$$

for all n sufficiently large. Observe that $\lambda^+ = deg(char(\epsilon_+ X))$, proceeding as in the proof of theorem 4.2.4. Now set $h_j = char(\epsilon_j(\overline{E}_1^\infty/\overline{C}_1^\infty))$. By proposition 5.5.7 we know that there is a constant $c > 0$ such that

$$c^{-1}|\epsilon_j(\overline{E}_1^n/\overline{C}_1^n)| \leq |\Lambda/(P_n, h_j)| \leq c|\epsilon_j(\overline{E}_1^n/\overline{C}_1^n)|$$

for all n. Reasoning as in the proof of theorem 4.2.4, we deduce that there exist $\lambda_j = deg(h_j)$ and μ_j, ν_j such that $|\Lambda/(P_n, h_j)| = p^{\lambda_j n + \mu_j p^n + \nu_j}$ for all n sufficiently large. Let $\lambda = \sum_l \lambda_j$ and similarly define μ and ν. Then:

$$c^{-(p-3)/2} p^{\lambda^+ n + \mu^+ p^n + \nu^+} \leq p^{\lambda n + \mu p^n + \nu} \leq c^{(p-3)/2} p^{\lambda^+ n + \mu^+ p^n + \nu^+}$$

for all n sufficiently large. It follows that $\mu^+ = \mu$ and $\lambda^+ = \lambda$. Therefore $h_2 h_4 \cdots h_{p-3} = char(\epsilon_+ X) = \prod_j char(\epsilon_j X)$, since one polynomial divides the other and they are monic of same degree. Hence $h_j = char(\epsilon_j X)$ for every j. Then we can deduce that 2. and 3. are equivalent.

□

5.6 The Proof

Finally it is time to prove The Main Conjecture.

Proof. Fix $n \geq 0$. We are going to use the techniques of the previous chapters to study

$$F_n = \mathbb{Q}(\zeta_{p^{n+1}})^+$$

Set

$$G_n = Gal(F_n|\mathbb{Q})$$

and let M and L be respectively a large power of p and a product of primes, as in section 5.1.

Roughly speaking, the idea is to choose an appropriate $\kappa(1) \in C^+_{p^n+1}$ and to apply inductively some procedures of the previous sections to produce some elements $\kappa(L) \in F_n^\times$. In this way we will obtain information on the structure of the class group of F_n. Before doing that, we need some remarks.

First of all: κ, l, and λ will have the same meanings of the previous paragraphs with respect to the above F_n. Now let χ a character as before: since $\epsilon_\chi \kappa$ is not defined in general, we choose $\epsilon'_\chi \in \mathbb{Z}[Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q})]$ such that $\epsilon_\chi \equiv \epsilon'_\chi \mod M$. Notice that $\epsilon_\chi \mathbb{Z}_p[G_n] = \epsilon_\chi \Lambda_n$ with $\Lambda_n = \Lambda/P_n$ as usual. In particular, $\overline{ind}(\epsilon'_\chi \kappa) \in \epsilon_\chi(\Lambda_n/M\Lambda_n)$ and $\overline{\nu}(\epsilon'_\chi \kappa) \mod M$ may be regarded as an element of $\epsilon_\chi(\Lambda_n/M\Lambda_n)$.

Proposition 5.6.1. *Let $\kappa(lL)$ and $\kappa(L)$ as in the previous sections. Then:*

$$\overline{\nu}(\epsilon'_\chi \kappa(lL)) \equiv -\overline{ind}_\lambda(\epsilon'_\chi(\kappa(L)) \mod (M\Lambda_n)$$

Proof. By proposition 5.1.4 we have that $\nu_{\sigma\lambda}(\kappa(lL)) \equiv ind_{\sigma\lambda}(\kappa(L)) \mod M$. Then using the definitions of $\overline{\nu}$ and $\overline{ind}$ we obtain the claim.

□

Let h_χ as in proposition 5.5.6 and let $f_1, ..., f_k$ and $\mathfrak{C}_1, ..., \mathfrak{C}_k$ as in proposition 5.5.8. Choose $\alpha \in \mathfrak{U} \cap \mathfrak{B}$ where $\mathfrak{U}$ is as in proposition 5.5.4 and $\mathfrak{B}$ still as in proposition 5.5.8. Notice that wlog we may assume that α is chosen relatively prime to P_m for all m, so that $\Lambda_m/\alpha\Lambda_m$ is finite for every m. We know that $\Lambda/(h_\chi, P_n) \simeq \Lambda_n/h_\chi\Lambda_n$ is finite by proposition 5.5.7. Choose $h_0 \in \mathbb{N}$ such that p^{h_0} annihilates both $\Lambda_n/\alpha\Lambda_n$ and $\Lambda_n/h_\chi\Lambda_n$. Therefore $p^{h_0}\Lambda_n = \alpha\Lambda_n$ and $p^{h_0}\Lambda_n = h_\chi\Lambda_n$, which implies that $\alpha|p^{h_0}$ and

$h_\chi | p^{h_0}$ in Λ_n. Now we set $M = |A_n| p^{n+(k+1)h_0}$ where A_n is the class group of $\mathbb{Q}(\zeta_{p^{n+1}})$ as in the previous sections.
Let $\kappa(1) \in C^+_{p^{n+1}}$ be the unit of proposition 1.3.3 (where we replace n by $n+1$). Let $\mathfrak{C}_1, ..., \mathfrak{C}_k$ be as above and let $\mathfrak{C}_{k+1}$ be any ideal class.
We want to find primes $\lambda_1, ..., \lambda_{k+1} \in F_n$ lying respectively above rational primes $l_1, ..., l_{k+1}$ such that for every $1 \leq i \leq k+1$ we have:

1. $\lambda_i \in \mathfrak{C}_i$
2. $l_i \equiv 1 \mod ML_{i-1}$ where $L_{i-1} = l_1 \cdots l_{i-1}$
3. $\overline{ind}_{\lambda_i}(\epsilon_\chi \kappa(L_{i-1}))(\prod_{j<i} f_j)$ divides $\epsilon_\chi \alpha^i h_\chi$ in $\epsilon_\chi(\Lambda_n / M\Lambda_n)$

We start by choosing λ_1. The function θ^n_α in proposition 5.5.6 induces a map

$$\psi : \epsilon_\chi(E^n_1/(\overline{E}^n_1)^M) \to \Lambda_n/M\Lambda_n \xrightarrow{\epsilon_\chi} \epsilon_\chi \mathbb{Z}/M\mathbb{Z}[G_n]$$

Proposition 5.5.10 implies that there are a prime $\lambda_1 \in \mathfrak{C}_1$ and a $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that $l_1 \equiv 1 \mod M$ and $\psi(\epsilon'_\chi \kappa(1)) \equiv u \cdot \overline{ind}_{\lambda_1}(\epsilon'_\chi \kappa(1)) \mod (\epsilon_\chi M\mathbb{Z}[G_n])$.

Since $\epsilon_\chi M\mathbb{Z}[G_n] \subset \epsilon_\chi M\mathbb{Z}_p[G_n] = \epsilon_\chi M\Lambda_n$ we read the last congruence modulo $\epsilon_\chi M\Lambda_n$.
However, by proposition 4.4.4 we know that $\epsilon_\chi \kappa(1)$ generates $\epsilon_\chi \overline{C^n_1}$ and so proposition 5.5.6 implies that

$$\theta^n_\alpha(\epsilon'_\chi \kappa(1)) = \alpha h_\chi v$$

for some $v \in \Lambda^\times_n$. Therefore recalling how ψ is induced by θ^n_α we get:

$$\epsilon_\chi \alpha h_\chi \equiv v^{-1} u \cdot \overline{ind}_{\lambda_1}(\epsilon'_\chi \kappa(1)) \mod (\epsilon_\chi M\Lambda_n)$$

This proves 3. for $i = 1$. To prove the general case, we proceed by induction: suppose $i \geq 1$ and that we have found primes $\lambda_1, ..., \lambda_i$ satisfying 1., 2. and 3. Then we have the following (see [**Wa**] for a proof):

Lemma 5.6.2. *Let $W = \epsilon'_\chi(\kappa(L_i)\Lambda_n/M\Lambda_n) \subset F^\times_n/(F^\times_n)^M$ be the multiplicative group generated by $\epsilon'_\chi \kappa(L_i)$ and its Galois conjugates and let $\rho \in \Lambda_n$. Then the map*

$$\psi : W \to \epsilon'_\chi(\Lambda_n/M\Lambda_n)$$
$$\rho\epsilon'_\chi \kappa(L_i) \mapsto \rho \frac{\alpha \overline{v}_{\lambda_i}(\epsilon'_\chi \kappa(L_i))}{f_i}$$

is a well-defined Λ-homomorphism.

Let W and ψ as in the previous lemma. Then lemma 5.5.10 states that there exist $\lambda_{i+1} \in \mathfrak{C}_{i+1}$, with $l_{i+1} \equiv 1 \mod (ML_i)$ and $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that

$$\psi(\epsilon'_\chi(\kappa(L_i)) \equiv u \cdot \overline{ind}_{\lambda_{i+1}}(\epsilon'_\chi(\kappa(L_i)) \mod (\epsilon_\chi M\Lambda_n)$$

Therefore

$$-\alpha \cdot \overline{ind}_{\lambda_i}(\epsilon'_\chi \kappa(L_{i-1})) \equiv \alpha \overline{v}_{\lambda_i}(\epsilon'_\chi \kappa(L_i)) \equiv f_i \psi(\epsilon'_\chi \kappa(L_i)) \equiv f_i u \cdot \overline{ind}_{\lambda_{i+1}}(\epsilon'_\chi \kappa(L_i))$$

modulo $(M\Lambda_n)$.
Now by the inductive hypothesis, we have that

$$\epsilon_\chi \alpha^i h_\chi = \overline{ind}_{\lambda_i}(\epsilon'_\chi \kappa(L_{i-1}))(\textstyle\prod_{j<i} f_j)\cdot \text{ (an element of } \epsilon'_\chi(\Lambda_n/M\Lambda_n)).$$

Multiplying this equality by α and using the just found congruence, we get that 3. holds also for $i+1$.

Still by induction, we deduce that $char(\epsilon_\chi X) = \prod_{i=1}^k f_i$ divides $\alpha^{k+1}h_\chi$ in $\Lambda_n/M\Lambda_n$. Indeed, if $k=1$ then consider 3. as above: we have that f_1 divides $\prod_{j<2} f_j = f_1$ which divides $\epsilon_\chi \alpha^2 h_\chi$ in $\epsilon_\chi(\Lambda_n/M\Lambda_n)$. Assuming that the result holds for k and using the same argument of the previous line, one shows that the result holds also for $k+1$. Now by our choice of M, we can view $\Lambda_n/M\Lambda_n$ contained in $\Lambda_n/p^n\Lambda_n$, and so we can say that $char(\epsilon_\chi X)$ divides $\alpha^{k+1}h_\chi$ also in $\Lambda_n/p^n\Lambda_n$. However this implies that for every n there exists $g_n \in \Lambda$ such that

$$(\textstyle\prod_{i=1}^k f_i)g_n \equiv \alpha^{k+1}h_\chi \mod (p^n, P_n)$$

Since Λ is compact, there exists a convergent subsequence g_{n_j} converging to some $g \in \Lambda$. Since $\bigcap_{j\geq 0}(p^{n_j}, P_{n_j}) \subseteq \bigcap_{j\geq 0}(p, T)^{n_j} = 0$, it follows that $char(\epsilon_\chi X)g = \alpha^{k+1}h_\chi$. In other words, for any $\alpha \in \mathfrak{U} \cap \mathfrak{B}$ relatively prime to P_m for all m, we have that $char(\epsilon_\chi X)$ divides $\alpha^{k+1}h_\chi$. Since $\mathfrak{U} \cap \mathfrak{B}$ has finite index in Λ, both T^c and p^c are in $\mathfrak{U} \cap \mathfrak{B}$ for some $c \geq 1$. Notice then that the polynomials $\alpha_1 = T^c - p^{2c}$ and $\alpha_2 = T^c - p^{3c}$ are relatively prime to each other and to $(1+T)^{p^m} - 1$ for all m because they have no common roots. So in particular we obtain that $char(\epsilon_\chi X)$ divides $\alpha_1^{k+1}h_\chi$ and $\alpha_2^{k+1}h_\chi$. Since Λ is a UFD, we deduce that $char(\epsilon_\chi X)$ divides h_χ. Then we can conclude the prove of The Iwasawa Main Conjecture by proposition 5.3.2.

□

Bibliography

[**Lan1**] Serge Lang: *Cyclotomic Fields I and II*, Springer-Verlag, Combined Second Edition (1990)

[**Lan2**] Serge Lang: *Algebraic Number Theory*, Springer, Second Edition (1994)

[**Wa**] Lawrence C. Washington: *Introduction to Cyclotomic Fields*, Springer, Second Edition (1997)

[**Sa2**] Takeshi Saito et al.: *Number Theory 2: Introduction to Class Field Theory*, American Mathematical Society, (2011)

[**Sa3**] Takeshi Saito et al.: *Number Theory 3: Iwasawa Theory and Modular Forms*, American Mathematical Society (2012)

[**Iw**] Kenkichi Iwasawa: *Lectures on p-adic L-functions*, Annals of Mathematics Studies, Princeton University press (1972)

[**Bro**] Jim L. Brown: *An Introduction to Iwasawa Theory*, Notes by Jim L. Brown

[**Gou**] Fernando Q. Gouvea: *p-adic Numbers: An Introduction*, Springer, Second Edition (2003)

[**Neu1**] Juergen Neukirch: *Algebraic Number Theory*, Springer, (1999)

[**Neu2**] Juergen Neukirch et al.: *Cohomology of Number Fields*, Springer, Second Edition (2008)

[**Ko**] Neal Koblitz: *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer, (1984)

[**Sam**] Pierre Samuel: *Algebraic Theory of Numbers*, Dover Publications, (2008)

[**Con1**] Keith Conrad: *Characters of finite Abelian Groups*, Notes by Keith Conrad

[**Con2**] Keith Conrad: *Cyclotomic Extensions*, Notes by Keith Conrad

[**Wi**] John S. Wilson: *Profinite Groups*, Clarendon Press, London Mathematical Society Monographs (1998)

[**Bou1**] N. Bourbaki: *Commutative Algebra, Chapters* 1-7, Springer (1972)

[**Bou2**] N. Bourbaki: *Algèbre commutative, Chapitres 8 et 9*, Springer (1983)

[**El**] Geir Ellingsrud: *Cyclotomic fields*, Notes by Geir Ellingsrud

[**Fr**] Eberhard Freitag and Rolf Busam: *Complex Analysis*, Springer, Second Edition (2009)

[**Ru**] Karl Rubin: *Euler Systems*, Annals of Mathematics Studies, Princeton University press (2000)

[**Coa**] J. Coates and R. Sujatha: *Cyclotomic Fields and Zeta Values*, Springer, (2006)

[**Ou**] Yi Ouyang: *Introduction to Iwasawa Theory*, Notes by Yi Ouyang

[**At**] M. F. Atiyah and I. G. MacDonald: *Introduction to Commutative Algebra*, CRC Press (1994)

[**Mar**] Daniel A. Marcus: *Number Fields*, Springer (1977)

[**Du**] David S. Dummit and Richard M. Foote: *Abstract Algebra*, John Wiley and Sons Inc., Third Edition (2003)

[**Cla**] Pete L. Clark: *Field theory*, Notes by Pete L. Clark

[**Se**] Soogil Seo: *Circular Distributions and Euler Systems*, Journal of Number Theory 88, 366-379 (2001)

[**Mat**] Hideyuki Matsumura: *Commutative Ring Theory*, Cambridge University Press (1987)

[**Sha**] Romyar Sharifi: *Iwasawa Theory*, Notes by Romyar Sharifi