Cyclotomic Fields and p-adic L-functions

A thesis submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

Thesis Supervisor: Dr. Baskar Balsubramanyam

by
Mihir Dilip Sheth
April, 2014

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road, Pashan, Pune 411008, India.

This is to certify that this thesis entitled "Cyclotomic Fields and p-adic L-functions" submitted towards the partial fulfillment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research Pune, represents work carried out by Mihir Dilip Sheth under the supervision of Dr. Baskar Balsubramanyam.

Professor A. Raghuram, Coordinator of Mathematics Faculty

Committee:

Dr. Baskar Balsubramanyam
Prof. A. Raghuram

Acknowledgments

I would like to express my sincere thanks to my thesis supervisor Dr. Baskar Balsubramanyam for the incredible amount of time he spent regularly guiding and advising me; from teaching me underlying concepts to helping me out with the number of proofs. I am also grateful to all faculty members of the Department of Mathematics at IISER Pune who have helped me directly or indirectly; in particular Prof. A. Raghuram for the invaluable advice I received from him at many points during the course of this thesis, and Dr. Chandrasheel Bhagwat for answering many queries related to my project and mathematics in general. Many thanks also go to my friends and my parents for their support and encouragement.

Abstract

Cyclotomic Fields and p-adic L-functions

by Mihir Dilip Sheth

This is an expository thesis exploring various arithmetical properties of cyclotomic fields and their relation to the p-adic L-functions. The primary objective is to study two different methods of constructing p-adic L-functions (one by interpolation and another by module theory), and Iwasawa's Main Conjecture which is a deep relationship between p-adic L-functions and ideal class groups of cyclotomic fields.

Contents

Chapter 1

Introduction

Cyclotomic extensions arise naturally in the study of number fields. The n-th cyclotomic extension $\mathbb{Q}(\zeta_n)$ is obtained by adjoining primitive n-th root of unity; $\zeta_n = e^{\frac{2\pi i a}{n}}, (a,n) = 1$; to the field of rational numbers $\mathbb{Q}$. Motivated by Fermat's Last Theorem and higher reciprocity laws, Kummer worked extensively on the arithmetic of cyclotomic fields in 1850's and paved the way for the development of algebraic number theory. He factored the equation $x^p + y^p = z^p$ in $\mathbb{Q}(\zeta_p)$ as follows:

$$\prod_{i=0}^{p-1}(x + \zeta_p^i y) = z^p$$

and instead of looking at each factor as just a number, he introduced the notion of "ideal numbers"(principal ideals generated by those numbers in $\mathbb{Z}[\zeta_p]$). He showed that unique factorization in $\mathbb{Q}(\zeta_p)$ could be recovered by the introduction of ideal numbers. With the assumption $(xyz, p) = 1$, Kummer proved that Fermat's Last Theorem holds true for all primes p which do not divide the class number of $\mathbb{Q}(\zeta_p)$ (such primes are known as *regular primes*). Kummer also found the remarkable relation between Bernoulli numbers B_k and the primes that divide the class number h_p of $\mathbb{Q}(\zeta_p)$: p divides $h_p \iff p$ divides the numerator of some B_k, $k = 2, 4, 6, \ldots p-3$.

The basic foundations laid by the Kummer remained the main part of the theory of cyclotomic fields for around a century. Meanwhile the mathematicians such as Kronecker, Weber, Hilbert, Takagi, Artin, Hasse etc. made fundamental contributions to the study of abelian extensions of number fields and developed class field theory. Kronecker-Weber Theorem, one of the most profound applications of class field theory, says that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

In the mid 1950's, the theory of cyclotomic fields was revisited by Iwasawa and Leopoldt. Iwasawa considered towers of cyclotomic fields and investigated Galois extensions of number fields whose Galois group is isomorphic to additive group of p-adic integers which led him to develop his theory of $\mathbb{Z}_p$-extensions. This approach was suggested by the theory of curves over finite fields. Leopoldt concentrated on a fixed cyclotomic field and established, with Kubota, "p-adic L-function"which is nothing but the p-adic analogue of classical Dirichlet L-function. Finally, in 1969, Iwasawa made the fundamental discovery that there was a close connection between his work on towers of cyclotomic fields and these p-adic L-functions of Kubota-Leopoldt. Today, this result is known as the Main Conjecture of Iwasawa Theory or Mazur-Wiles theorem.

This thesis is expected to provide an overview of the cyclotomic theory and its connection to the p-adic L-functions. The second chapter is devoted to the class field theory and its consequences such as Kronecker-Weber Theorem, Chebotarev Density Theorem. In particular, we derive some useful results on the class groups of cyclotomic fields using class field theory in Section 2.3. The second chapter forms a background for later chapters.

Construction of the p-adic L-functions is the main theme of the third chapter. The interesting fact is that Bernoulli numbers and their generalizations appear as values of Dirichlet L-functions at negative integers and Kubota-Leopoldt showed how these values can be interpolated by a function of $\mathbb{Z}_p$, denoted by $L_p(s, \chi)$ and known as the p-adic L-function. As a consequence of Kubota-Leopoldt's construction of p-adic L-functions, we obtain Kummer's criterion for irregularity of primes. The second section of this chapter presents another construction of p-adic L-functions due to Iwasawa which is closely related to the arithmetic of cyclotomic fields.

The final chapter of the thesis studies two important theorems: Iwasawa's theorem and the Main Conjecture. The ideal class group C_K of a number field K is an object of central importance in number theory. In general, the explicit determination of the class number h_K , let alone the structure of C_K as a finite abelian group, can be a difficult and computationally intensive task. But if we concentrate on a p-part of the ideal class groups of K_n's in a $\mathbb{Z}_p$-extension K_∞/K_0, we have an interesting theorem due to Iwasawa that describes the growth of this p-part as a function of n. We prove this theorem in Section 4.1.

Finally we discuss the Main Conjecture of Iwasawa theory, its equivalent formulations and the motivation behind it. Our account on the Main Conjecture surveys the important results and the recent developments in this area.

Chapter 2

Cyclotomic Fields

The present chapter provides a brief review of basic results on cyclotomic fields and their class groups. We also discuss the important theorems of global and local class field theory which will be needed often. The exposition in this chapter is based on the book by Lawrence C. Washington [13], while the part of class field theory is based on the book by Janusz [4] and the notes by J. S. Milne [9].

2.1 Basic results on cyclotomic fields

In this section, we state some basic arithmetical properties of cyclotomic fields which will lay the groundwork for later sections and chapters (see Chapter 2, [13] for the proofs of these results or any standard book on algebraic number theory).

Theorem 2.1. *$\mathbb{Q}(\zeta_n)$ is an abelian extension of $\mathbb{Q}$ of degree $\phi(n)$. More precisely, there is an isomorphism:*

$$(\mathbb{Z}/n\mathbb{Z})^{\times} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

$$a \pmod{n} \mapsto \sigma_a$$

where $\sigma_a(\zeta_n) = \zeta_n^a$

Theorem 2.2. *$\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta_n)$.*

Theorem 2.3. *The discriminant of $\mathbb{Q}(\zeta_n)$, $d(\mathbb{Q}(\zeta_n))$, is given by the following formula:*

$$d(\mathbb{Q}(\zeta_n)) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}$$

Therefore p ramifies in $\mathbb{Q}(\zeta_n)$, $n \not\equiv 2 \pmod 4$ if and only if p divides n. ($\mathbb{Q}(\zeta_{n/2}) = \mathbb{Q}(\zeta_n)$ if $n \equiv 2 \pmod 4$)

Theorem 2.4. *Suppose $p \nmid n$ and let f be the smallest positive integer such that $p^f \equiv 1 \pmod{n}$. Then p splits into $g = \phi(n)/f$ distinct primes in $\mathbb{Q}(\zeta_n)$, each of which has residue class degree f. In particular, p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \pmod{n}$.*

Theorem 2.5. *p is totally ramified in $\mathbb{Q}(\zeta_{p^n})$ for all $n \geq 1$.*

Theorem 2.6. *Suppose n has atleast two distinct factors. Then $1 - \zeta_n$ is a unit of $\mathbb{Z}[\zeta_n]$ and $\prod_{\substack{0<j<n \\ (j,n)=1}} (1 - \zeta_n^j) = 1$*

2.2 Class field theory

Class field theory describes the abelian extensions of a local or global field in terms of the arithmetic of the field itself. This section consists of two subsections. The first treats global class field theory from the classical viewpoint of ideal class groups. The second discusses local class field theory.

2.2.1 Global class field theory

Given a number field K, a modulus in K is a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ over all primes $\mathfrak{p}$, finite or infinite, of K where the exponents must satisfy:
(i) $n_{\mathfrak{p}} \geq 0$ and at most finitely many are nonzero.
(ii) $n_{\mathfrak{p}} = 0$ if $\mathfrak{p}$ is a complex infinite prime.
(iii) $n_{\mathfrak{p}} \leq 1$ if $\mathfrak{p}$ is a real infinite prime.
A modulus $\mathfrak{m}$ may thus be written as $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an $\mathcal{O}_K$-ideal and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. We set $\mathfrak{m} = 1$ if all the exponents $n_{\mathfrak{p}} = 0$. Note that for a purely imaginary K, a modulus may be regarded simply as an ideal in $\mathcal{O}_K$.

Given a modulus $\mathfrak{m}$, let $I_K(\mathfrak{m})$ be the group of all fractional ideals in $\mathcal{O}_K$ relatively prime to $\mathfrak{m}$ (i.e. relatively prime to $\mathfrak{m}_0$), and let $P_{K,1}(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}_K$ satisfies: $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and $\sigma(\alpha) > 0$ for every real infinite prime σ dividing $\mathfrak{m}_\infty$. $P_{K,1}(\mathfrak{m})$ has finite index in $I_K(\mathfrak{m})$ (Chapter IV.1, [4]). A subgroup $H \subset I_K(\mathfrak{m})$ is called a congruence subgroup for $\mathfrak{m}$ if it satisfies $P_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$ and the quotient is called a generalized ideal class group for $\mathfrak{m}$. The basic idea of class field theory is that the generalized ideal class groups are the Galois groups of abelian extensions of K, and the link between these two is provided by the *Artin map.*

Let $\mathfrak{m}$ be a modulus divisible by all ramified primes of an abelian extension L/K. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in L and let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ above $\mathfrak{p}$. We define Artin symbol $(\frac{L/K}{\mathfrak{p}})$ for $\mathfrak{p}$ as the Frobenius automorphism of $\mathfrak{P}$ over $\mathfrak{p}$ (It depends only on $\mathfrak{p}$ since L/K is abelian). It is the unique element in $\mathrm{Gal}(L/K)$ such that $(\frac{L/K}{\mathfrak{p}})(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{P}}$ for all $\alpha \in \mathcal{O}_L$ (see pp. 108-110, [8] for more details). We extend the definition of

Artin symbol to all the elements in $I_K(\mathfrak{m})$ by multiplicativity to give us the homomorphism $\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ which is called the Artin map for L/K and $\mathfrak{m}$.

Theorem 2.7 (Artin Reciprocity Theorem)**.** (i) *The Artin map is surjective.*
(ii) *If the exponents of finite primes dividing* $\mathfrak{m}$ *are sufficiently large, then* $\ker(\Phi_{L/K,\mathfrak{m}})$ *is a congruence subgroup for* $\mathfrak{m}$*, and consequently the isomorphism* $I_K(\mathfrak{m})/\ker(\Phi_{L/K,\mathfrak{m}}) \cong \mathrm{Gal}(L/K)$ *shows that* $\mathrm{Gal}(L/K)$ *is a generalized ideal class group for the modulus* $\mathfrak{m}$*.*

Proof. See Chapter V, Theorem 5.7, [4]. □

Let's apply Theorem 2.7 to the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Let $\mathfrak{m} = n\infty$. Using Theorem 2.3, we see that the Artin map

$$\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$$

is defined. For $a, b \in \mathbb{Z}, (a, n) = (b, n) = 1$,

$$\Phi_{\mathfrak{m}}\Big(\frac{a}{b}\mathbb{Z}\Big) = ab^{-1} \pmod{n}$$

It follows easily that $\ker(\Phi_{\mathfrak{m}}) = P_{\mathbb{Q},1}(\mathfrak{m})$.

For $\mathfrak{m} \mid \mathfrak{n}$, we claim that:

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \Longrightarrow P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}) \tag{2.1}$$

Suppose $\alpha\mathcal{O} = \prod_i \mathfrak{p}_i^{r_i} \in P_{K,1}(\mathfrak{n})$. Then $\alpha \equiv 1 \pmod{\mathfrak{n}_0}$ and $\sigma(\alpha) > 0$ for every real infinite prime σ dividing $\mathfrak{n}_\infty$. Since $\mathfrak{m} \mid \mathfrak{n}$, $\alpha\mathcal{O} \in P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}})$. Hence $\Phi_{\mathfrak{m}}(\alpha\mathcal{O}) = \prod_i (\frac{L/K}{p_i})^{r_i} = 1$. We see that the definition of Artin symbol for $\alpha\mathcal{O}$ depends only on the primes dividing $\alpha\mathcal{O}$. Since these primes $\mathfrak{p}_i$'s are relatively prime to $\mathfrak{n}$, $\Phi_{\mathfrak{n}}(\alpha\mathcal{O}) = \prod_i (\frac{L/K}{p_i})^{r_i} = 1$. Therefore $\alpha\mathcal{O} \in \ker(\Phi_{\mathfrak{n}})$.

(2.1) implies that $\mathrm{Gal}(L/K)$ is a generalized ideal class group for infinitely many moduli. However, there exists a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that
(i) A prime of K, finite or infinite, ramifies in L if and only if it divides $\mathfrak{f}$.
(ii) Let $\mathfrak{m}$ be a modulus divisible by all primes of K which ramify in L. Then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if a and only if $\mathfrak{f} \mid \mathfrak{m}$.

The modulus $\mathfrak{f}(L/K)$ is uniquely determined by L/K and is called the conductor of the extension.

Theorem 2.8 (Existence Theorem)**.** *Let* $\mathfrak{m}$ *be a modulus of* K *and let* H *be a congruence subgroup for* $\mathfrak{m}$*. Then there exists a unique abelian extension* L *of* K*, all of whose ramified primes, finite or infinite, divide* $\mathfrak{m}$*, such that if* $\Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ *is the Artin map of* L/K*, then* $H = \ker(\Phi_{\mathfrak{m}})$*.*

Proof. See Chapter V, Theorem 9.16, [4]. □

This theorem asserts that every generalized ideal class group is the Galois group of some abelian extension.

Corollary 2.1. *Let L and M be abelian extensions of K. Then $L \subset M$ if and only if there is a modulus $\mathfrak{m}$, divisible by all primes of K ramified in either L or M, such that $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$.*

Proof. Assume $L \subset M$. Let $r : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ be the restriction map. We first show that $r \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$. It is enough to prove that $r(\Phi_{M/K,\mathfrak{m}}(\mathfrak{p})) = \Phi_{L/K,\mathfrak{m}}(\mathfrak{p})$ for the primes $\mathfrak{p}$ in $\mathcal{O}_K$ that are relatively prime to $\mathfrak{m}$. So we have to show that the restriction of $(\frac{M/K}{\mathfrak{p}})$ to $L = (\frac{L/K}{\mathfrak{p}})$. In other words, we have to show that $(\frac{M/K}{\mathfrak{p}})(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|}$ $(\mathrm{mod}\ \mathfrak{P})$ for all $\alpha \in \mathcal{O}_L$ where $\mathfrak{P}$ is the prime in $\mathcal{O}_L$ above $\mathfrak{p}$. But, since $\alpha \in \mathcal{O}_L \subset \mathcal{O}_M$, $(\frac{M/K}{\mathfrak{p}})(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|}$ $(\mathrm{mod}\ \mathfrak{P}')$ where $\mathfrak{P}'$ is the prime in $\mathcal{O}_M$ above $\mathfrak{P}$, hence above $\mathfrak{p}$, i.e. $(\frac{M/K}{\mathfrak{p}})(\alpha) - \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \in \mathfrak{P}'$. Also $(\frac{M/K}{\mathfrak{p}})(\alpha) \in \mathcal{O}_L$ by restriction. Thus $(\frac{M/K}{\mathfrak{p}})(\alpha) - \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \in \mathcal{O}_L \cap \mathfrak{P}' = \mathfrak{P}$ and we are done.

Now by Theorem 2.7 and (2.1), there is a modulus $\mathfrak{m}$ for which $\ker(\Phi_{L/K,\mathfrak{m}})$ and $\ker(\Phi_{M/K,\mathfrak{m}})$ are both congruence subgroups for $\mathfrak{m}$. Hence $r \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$ implies $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$ immediately.

Now assume that $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$. Then under the map $\Phi_{M/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(M/K)$, the subgroup $\ker(\Phi_{L/K,\mathfrak{m}}) \subset I_K(\mathfrak{m})$ maps to a subgroup $H \subset \mathrm{Gal}(M/K)$. By Galois theory, H corresponds to an intermediate field $K \subset \tilde{L} \subset M$. The first part of the proof, applied to $\tilde{L} \subset M$, shows that $\ker(\Phi_{\tilde{L}/K,\mathfrak{m}}) = \ker(\Phi_{L/K,\mathfrak{m}})$. Then the uniqueness part of the Existence Theorem shows that $L = \tilde{L} \subset M$. □

Theorem 2.9 (Kronecker-Weber Theorem)**.** *Let L be an abelian extension of $\mathbb{Q}$. Then there exists a positive integer n such that $L \subset \mathbb{Q}(\zeta_n)$.*

Proof. By the Artin Reciprocity Theorem, there exists a modulus $\mathfrak{m}$ such that $P_{\mathbb{Q},1}(\mathfrak{m}) \subset \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$. By (2.1), we may take $\mathfrak{m} = n\infty$ for some n (n must be divisible by all ramified primes in $L/\mathbb{Q}$). Then $P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q},\mathfrak{m}}) \subset \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$. Therefore $L \subset \mathbb{Q}(\zeta_n)$ follows from Corollary 2.1. □

Now let modulus $\mathfrak{m} = 1$ of K. Then $I_K(1)/P_{K,1}(1) := C_K$ is an ideal class group of K. Applying the Existence Theorem to this modulus and the subgroup $P_{K,1}(1)$, we have a unique abelian extension H of K, unramified at all primes of K since $\mathfrak{m} = 1$, such that the Artin map induces an isomorphism

$$C_K \cong \mathrm{Gal}(H/K) \tag{2.2}$$

H is the *Hilbert class field* of K and its main property is the following:

Theorem 2.10. *The Hilbert class field H is the maximal unramified abelian extension of K.*

Proof. We already know that H is unramified and abelian. Let L be another unramified abelian extension. Then $\mathfrak{f}(L/K) = 1$ since prime ramifies if and only if it divides the conductor. Also $\ker(\Phi_{L/K,1})$ is a congruence subgroup for the modulus 1. Therefore $P_{K,1}(1) \subset \ker(\Phi_{L/K,1})$. By the definition of Hilbert class field, $P_{K,1}(1) = \ker(\Phi_{H/K,1}) \subset \ker(\Phi_{L/K,1})$. Therefore $L \subset H$ follows from Corollary 2.1. □

Theorem 2.11. *Suppose the extension of number fields L/K contains no unramified abelian subextension F/K with $F \neq K$. Then the norm map from C_L to C_K is surjective.*

Proof. Let H_L and H_K be the Hilbert class fields of L and K respectively. Then because of the assumption on L/K, we have $L \cap H_K = K$. Therefore $\mathrm{Gal}(H_K L/L) \cong \mathrm{Gal}(H_K/K)$. It follows that $H_K L \subset H_L$ since $H_K L/L$ is unramified and abelian. So we have a restriction map from $\mathrm{Gal}(H_L/L)$ to $\mathrm{Gal}(H_K L/L)$ which is surjective. Now we have the following diagram:

$$\begin{tikzcd}
C_L \arrow[r, "\sim"] \arrow[d, "\text{Norm}"'] & \mathrm{Gal}(H_L/L) \arrow[d, "\text{Restriction}"] \\
C_K \arrow[r, "\sim"] & \mathrm{Gal}(H_K/K)
\end{tikzcd}$$

The horizontal maps are the Artin maps. Let $\mathfrak{P}$ be a prime ideal of L and $\tilde{\mathfrak{P}}$ lie above $\mathfrak{P}$ in H_L. Similarly, let $\mathfrak{p}$ and $\tilde{\mathfrak{p}}$ be the primes of K and H_K lying below $\mathfrak{P}$ and $\tilde{\mathfrak{P}}$ respectively. Let $f = f(\mathfrak{P}/\mathfrak{p})$. Then $\mathrm{Norm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$. Since $\mathcal{O}_{H_K} \subseteq \mathcal{O}_{H_L}$, we have

$$\left(\frac{H_L/L}{\mathfrak{P}}\right)\Big|_{H_K}(x) \equiv x^{|\mathcal{O}_L/\mathfrak{P}|} \pmod{\tilde{\mathfrak{p}}}$$

for all $x \in \mathcal{O}_{H_K}$. But

$$\left(\frac{H_K/K}{\mathfrak{p}^f}\right)(x) = \left(\frac{H_K/K}{\mathfrak{p}}\right)^f(x) \equiv x^{|\mathcal{O}_K/\mathfrak{p}|^f} = x^{|\mathcal{O}_L/\mathfrak{P}|} \pmod{\tilde{\mathfrak{p}}}$$

Therefore

$$\left(\frac{H_L/L}{\mathfrak{P}}\right)\Big|_{H_K} = \left(\frac{H_K/K}{\mathrm{Norm}_{L/K}(\mathfrak{P})}\right)$$

Hence the above diagram is commutative and the norm map is surjective. □

We now give one more application of class field theory: Chebotarev Density Theorem. It provides very useful information about the surjectivity of Artin map. Let $\mathcal{P}_K$ be the set of all finite primes of K. Given a subset $\mathcal{S} \subset \mathcal{P}_K$, the *Dirichlet density* of $\mathcal{S}$ is defined to be

$$d(\mathcal{S}) = \lim_{s \to +1} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{-\log(s-1)}$$

provided the limit exists ($N(\mathfrak{p}) = |\frac{\mathcal{O}_K}{\mathfrak{p}}|$). We state the basic properties of Dirichlet density that follow directly from the definition and the basic analytic properties of Dedekind zeta function $\zeta_K(s)$ of K (see Section 5, Chapter VII, [10] for proofs):

1. $d(\mathcal{P}_K) = 1$.

2. If $\mathcal{S} \subset \mathcal{T}$ and $d(\mathcal{S})$ and $d(\mathcal{T})$ exist, then $d(\mathcal{S}) \leq d(\mathcal{T})$.

3. If $d(\mathcal{S})$ exists, then $0 \leq d(\mathcal{S}) \leq 1$.

4. If $\mathcal{S}$ and $\mathcal{T}$ are disjoint and $d(\mathcal{S})$ and $d(\mathcal{T})$ exist, then $d(\mathcal{S} \cup \mathcal{T}) = d(\mathcal{S}) + d(\mathcal{T})$.

5. If $\mathcal{S}$ is finite, then $d(\mathcal{S}) = 0$.

6. If $d(\mathcal{S})$ exists and $\mathcal{T}$ differs from $\mathcal{S}$ by finitely many elements, then $d(\mathcal{T}) = d(\mathcal{S})$.

Let L/K be Galois extension (possibly non-abelian) and $\mathfrak{p}$ be a prime of K unramified in L. Then different primes $\mathfrak{P}$ of L above $\mathfrak{p}$ may give us different Artin symbols $(\frac{L/K}{\mathfrak{P}})$, but all of the $(\frac{L/K}{\mathfrak{P}})$ are conjugate of each other and in fact they form a complete conjugacy class in $\mathrm{Gal}(L/K)$. So we can define Artin symbol $(\frac{L/K}{\mathfrak{p}})$ for $\mathfrak{p}$ to be this conjugacy class in $\mathrm{Gal}(L/K)$.

Theorem 2.12 (Chebotarev Density Theorem)**.** *Let L/K be Galois, and let $\langle\sigma\rangle$ be the conjugacy class of an element $\sigma \in \mathrm{Gal}(L/K)$. Then the set*

$$\mathcal{S} = \left\{ \mathfrak{p} \in \mathcal{P}_K \mid \mathfrak{p} \text{ is unramified in } L \text{ and } \left(\frac{L/K}{\mathfrak{p}}\right) = \langle\sigma\rangle \right\}$$

has Dirichlet density

$$d(\mathcal{S}) = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal}(L/K)|} = \frac{|\langle\sigma\rangle|}{[L:K]}$$

Proof. See Chapter V, Theorem 10.4, [4]. □

We now prove the classic theorem in number theory using Chebotarev Density Theorem:

Corollary 2.2 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Let $(a, m) = 1$. Then the arithmetic progression $\{a + nm \mid n \in \mathbb{Z}\}$ contains infinitely many prime numbers.*

Proof. Let $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}$, so L/K is abelian. Hence $(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p})$ is a single element in $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. For all the primes p of the form of $a + nm$, $p \equiv a \pmod{m}$. Thus $(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}) = \sigma_a$. Therefore the density of the set of such primes is $1/[L : K] = 1/\phi(m) > 0$ which implies that there are infinitely many such primes. □

Now let L/K be abelian and $\mathfrak{p}$ be a prime of K which splits completely in L. Then $f(\mathfrak{P}/\mathfrak{p}) = 1$ for all the primes $\mathfrak{P}$ of L above $\mathfrak{p}$. Since $f(\mathfrak{P}/\mathfrak{p})$ is the order of the Frobenius map of $\mathfrak{P}$ over $\mathfrak{p}$, we have $(\frac{L/K}{\mathfrak{p}}) = 1 \iff \mathfrak{p}$ splits completely in L. From Chebotarev Density Theorem, we see that the splitting primes have Dirichlet density $1/[L : K]$, and in particular there are infinitely many of them. The surprising fact is that these primes characterize the extension L/K uniquely.

2.2.2 Local class field theory

Local field is a field K which is locally compact with respect to a nontrivial valuation, e.g. a finite extension of $\mathbb{Q}_p$ is a nonarchimedean local field while $\mathbb{R}$ or $\mathbb{C}$ is an archimedean local field. Local class field theory classifies the abelian extensions of a local field. The composite of two finite abelian extensions of K is again a finite abelian extension of K. We denote the union of all finite abelian extensions of K by K^{ab} which is an infinite abelian extension of K.

Theorem 2.13 (Local Reciprocity Law). *For every nonarchimedean local field K, there exists a unique homomorphism $\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that for every finite abelian extension L of K, $\mathrm{Norm}_{L/K}(L^\times)$ is contained in the kernel of $a \mapsto \phi_K(a)|_L$, and ϕ_K induces an isomorphism*

$$\phi_{L/K} : K^\times/\mathrm{Norm}_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$$

Let T denote the inertia subgroup of $\mathrm{Gal}(L/K)$ and U_K and U_L the groups of units in K and L respectively. Then

$$U_K/\mathrm{Norm}_{L/K}(U_L) \cong T$$

Proof. See Chapter I, Section 2-4, [9]. □

The maps ϕ_K and $\phi_{L/K}$ are called the *local Artin maps* for K and L/K, and the subgroups of $K^\times$ of the form of $\mathrm{Norm}_{L/K}(L^\times)$ for some finite abelian extension L/K are called the *norm groups* in $K^\times$. We denote $\mathrm{Norm}_{L/K}(L^\times)$ by $\mathrm{Nm}(L^\times)$.

Corollary 2.3. (a) *The map $L \mapsto \mathrm{Nm}(L^\times)$ is a bijection from the set of finite abelian extensions of K onto the set of norm groups in $K^\times$.*
(b) *$L \subset L'$ if and only if $\mathrm{Nm}(L'^\times) \subset \mathrm{Nm}(L^\times)$.*
(c) *$\mathrm{Nm}((L.L')^\times) = \mathrm{Nm}(L^\times) \cap \mathrm{Nm}(L'^\times)$.*

(d) $\mathrm{Nm}(L \cap L')^\times) = \mathrm{Nm}(L^\times).\mathrm{Nm}(L'^\times)$.

(e) *Every subgroup of $K^\times$ containing a norm group is itself a norm group.*

Proof. The transitivity of norms, $\mathrm{Norm}_{L'/K} = \mathrm{Norm}_{L/K} \circ \mathrm{Norm}_{L'/L}$, shows that $L \subset L' \Rightarrow \mathrm{Nm}(L'^\times) \subset \mathrm{Nm}(L^\times)$. Hence $\mathrm{Nm}((L.L')^\times) \subset \mathrm{Nm}(L^\times) \cap \mathrm{Nm}(L'^\times)$. Conversely, if $a \in \mathrm{Nm}(L^\times) \cap \mathrm{Nm}(L'^\times)$, then $\phi_{L/K}(a) = \phi_{L'/K}(a) = 1$. But, $\phi_{LL'/K}(a)|_L = \phi_{L/K}(a)$ and $\phi_{LL'/K}(a)|_{L'} = \phi_{L'/K}(a)$. As the map $\sigma \mapsto (\sigma|_L, \sigma|_{L'}) : \mathrm{Gal}(LL'/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$ is injective, it follows that $\phi_{LL'/K}(a) = 1$ and thus $a \in \mathrm{Nm}((L.L')^\times)$. This proves (c).

Now if $\mathrm{Nm}(L'^\times) \subset \mathrm{Nm}(L^\times)$, statement (c) becomes $\mathrm{Nm}((L.L')^\times) = \mathrm{Nm}(L'^\times)$. Since the index of a norm group os the degree of the abelian extension defining it and $L' \subset LL'$, this implies that $LL' = L'$. Hence $L \subset L'$. This proves (b).

Now by definition, the map $L \mapsto \mathrm{Nm}(L^\times)$ is surjective and it follows from (b) that it is injective. This proves (a).

We next prove (e). Let $N = \mathrm{Nm}(L^\times)$ be a norm group and let $N \subset I \subset K^\times$. Let M be the fixed field of $\phi_{L/K}(I)$, so that $\phi_{L/K}$ maps I/N isomorphically onto $\mathrm{Gal}(L/M)$. Consider the following commutative diagram:

$$\begin{tikzcd}
K^\times \arrow[r, "\phi_{L/K}"] \arrow[d, equal] & \mathrm{Gal}(L/K) \arrow[d] \\
K^\times \arrow[r, "\phi_{M/K}"] & \mathrm{Gal}(M/K)
\end{tikzcd}$$

The kernel $\phi_{M/K}$ is $\mathrm{Nm}(M^\times)$. On the other hand, the kernel of $K^\times \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ is $\phi_{L/K}^{-1}(\mathrm{Gal}(L/M))$, which equals I.

Finally, we prove (d). Since $L \cap L'$ is the largest extension of K contained in both L and L', from (a), we have $\mathrm{Nm}(L^\times).\mathrm{Nm}(L'^\times)$ is the smallest subgroup containing both $\mathrm{Nm}(L^\times)$ and $\mathrm{Nm}(L'^\times)$ which is itself a norm group by (e). Therefore the two must correspond. □

Lemma 2.1. *Let L be an extension K. If $\mathrm{Nm}(L^\times)$ is of finite index in $K^\times$, then it is open.*

Proof. The group U_L of units in L is compact, and so $\mathrm{Nm}(U_L)$ is closed in $K^\times$. Since $\mathrm{Nm}(U_L) = \mathrm{Nm}(L^\times) \cap U_K$, $U_K/\mathrm{Nm}(U_L) \hookrightarrow K^\times/\mathrm{Nm}(L^\times)$. Therefore, $\mathrm{Nm}(U_L)$ is closed of finite index in U_K, and hence is open in U_K, which itself is open in $K^\times$. Therefore the group $\mathrm{Nm}(L^\times)$ contains an open subgroup of $K^\times$, and so is itself open. □

Theorem 2.14 (Local Existence Theorem). *The norm groups in $K^\times$ are exactly the open subgroups of finite index.*

Proof. See Chapter I, Section 2-4, [9]. □

From Local Existence Theorem, we see that the Corollary 2.3 holds with "norm group" replaced by "open subgroup of finite index". Therefore the finite abelian extensions of a local field K are classified in terms of the open subgroups of finite index of $K^\times$. As an application, we prove Local Kronecker-Weber Theorem.

Theorem 2.15 (Local Kronecker-Weber Theorem)**.** *Let L be an abelian extension of $\mathbb{Q}_p$. Then there exists a positive integer n such that $L \subset \mathbb{Q}_p(\zeta_n)$.*

Proof. Consider $\mathbb{Q}_p(\zeta_k)$ where $p \nmid k$. Let π and U be the uniformizing parameter and the group of units of $\mathbb{Q}_p(\zeta_k)$. As $\mathbb{Q}_p(\zeta_k)$ is unramified and $\mathbb{Q}_p(\zeta_k)^\times = \pi^{\mathbb{Z}} \times U$, local class field theory tells us that,

$$\mathrm{Norm}_{\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_k)^\times) \cong \pi^{[\mathbb{Q}_p(\zeta_k):\mathbb{Q}_p]\mathbb{Z}} \times U$$

Now consider $\mathbb{Q}_p(\zeta_{p^m})$, which is totally ramified of degree $p^{m-1}(p-1)$ over $\mathbb{Q}_p$. Local Reciprocity Law gives

$$\mathbb{Q}_p^\times/\mathrm{Norm}_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_{p^m})^\times) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$$

Since $\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}/(p-1)\mathbb{Z} \times (1 + p\mathbb{Z}_p)$ (see (3.7)), we must have

$$\mathrm{Norm}_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_{p^m})^\times) = p^{\mathbb{Z}}(1 + p^m\mathbb{Z}_p)$$

Now since $L/\mathbb{Q}_p$ is an abelian extension, its corresponding norm group N is open of finite index in $\mathbb{Q}_p^\times$, so contains $p^{n'\mathbb{Z}}(1 + p^m\mathbb{Z}_p)$ for some n', m. Choosing large k enough, we may suppose that $n' \mid [\mathbb{Q}_p(\zeta_{p^k}) : \mathbb{Q}_p]$. Then using Corollary 2.3, we have

$$N \supseteq \mathrm{Nm}(\mathbb{Q}_p(\zeta_{n'})^\times) \cap \mathrm{Nm}(\mathbb{Q}_p(\zeta_{p^m})^\times) = \mathrm{Nm}(\mathbb{Q}_p(\zeta_{n'p^m})^\times)$$

and therefore $L \subseteq \mathbb{Q}_p(\zeta_{n'p^m}) = \mathbb{Q}_p(\zeta_n)$. □

We now prove that Theorem 2.15 (Local Kronecker-Weber Theorem) for all $p \Longrightarrow$ Theorem 2.9 (Kronecker-Weber Theorem). Assume $K/\mathbb{Q}$ is abelian. Let p be a prime which ramifies in this extension. Let K_p be the completion at a prime above p. Then $K_p/\mathbb{Q}_p$ is abelian, so by Theorem 2.15, $K_p \subseteq \mathbb{Q}_p(n_p)$ for some n_p. Let p^{e_p} be the exact power of p dividing n_p and let

$$n = \prod_{p \text{ ramifies in } K} p^{e_p}$$

We claim $K \subseteq \mathbb{Q}(\zeta_n)$. Let $L = K(\zeta_n)$, so $L/\mathbb{Q}$ (composite of K and $\mathbb{Q}(\zeta_n)$) is abelian and p ramifies in $L/\mathbb{Q}$ then p ramifies in $K/\mathbb{Q}$. Also, if L_p denotes the completion at a suitable prime of L above p, then $L_p = K_p(\zeta_n) \subseteq \mathbb{Q}_p(\zeta_{n'p^{e_p}})$ with $(n', p) = 1$. Let I_p be the inertia subgroup for p in $L/\mathbb{Q}$. Then $I_p \cong \text{Gal}(\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p)$. Let $I \subseteq \text{Gal}(L/\mathbb{Q})$ be the subgroup generated by all I_p with p finite and ramified. Since $L.\mathbb{Q}$ is abelian,

$$|I| \leq \prod |I_p| = \prod \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

Let F be the fixed field of I. Then $F/\mathbb{Q}$ is unramified at all finite primes, so $F = \mathbb{Q}$. Therefore $I = \text{Gal}(L/\mathbb{Q})$. Hence $[L : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, But $\mathbb{Q}(\zeta_n) \subseteq K(\zeta_n) = L$, so we have $L = \mathbb{Q}(\zeta_n)$ and $K \subseteq \mathbb{Q}(\zeta_n)$. Thus we deduce the global result from the corresponding result of local fields. This "local-to-global"technique is often used in algebraic number theory.

2.3 Some results on the class groups of cyclotomic fields

A CM-field is a totally imaginary quadratic extension of a totally real number field. Such a field may be obtained by starting with a totally real number field and adjoining the square root of a number all of whose conjugates are negative. All cyclotomic fields are CM-fields. One can obtain $\mathbb{Q}(\zeta_n)$ from $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ by adjoining the square root of $\zeta_n^2 + \zeta_n^{-2} - 2$ which is totally negative. So $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is a maximal real subfield of $\mathbb{Q}(\zeta_n)$.

Let K be a CM-field and K^+ be the real subfield. Let $\phi, \psi : K \to \mathbb{C}$ be two embeddings. We claim that $\phi^{-1}(\overline{\phi(\alpha)}) = \psi^{-1}(\overline{\psi(\alpha)})$ for all $\alpha \in K$. Since $\phi(K)/\phi(K^+)$ is quadratic, it is normal, and complex conjugation fixes $\phi(K^+)$. Therefore $\overline{\phi}(K) = \phi(K)$. In particular, $\phi^{-1}(\overline{\phi})$ is defined. Hence both $\phi^{-1}(\overline{\phi})$ and $\psi^{-1}(\overline{\psi})$ are automorphisms of K and both fix K^+ since it is totally real. Since K is totally imaginary, neither automorphism can be identity. Therefore they must be equal since $\text{Gal}(K/K^+)$ has order 2. Thus complex conjugation induces an automorphism on the CM-field which is independent of the embedding into $\mathbb{C}$.

Theorem 2.16. *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 $Q := [E : WE^+] = 1$ or 2.*

Proof. Define $\phi : E \to W$ by $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon}$ (all conjugates of $\varepsilon/\bar{\varepsilon}$ have absolute value 1, hence $\varepsilon/\bar{\varepsilon}$ is a root of unity). Let $\psi : E \to W/W^2$ be the map induced by ϕ. Suppose $\varepsilon = \zeta\varepsilon_1$ where $\zeta \in W, \varepsilon_1 \in E^+$. Then $\phi(\varepsilon) = \zeta^2 \in W^2$, so $\varepsilon \in \text{Ker}(\psi)$. Conversely, suppose $\phi(\varepsilon) = \zeta^2 \in W^2$. Then $\varepsilon_1 = \zeta^{-1}\varepsilon = \zeta^{-1}\zeta^2\bar{\varepsilon} = \zeta\bar{\varepsilon} = \bar{\varepsilon_1}$. Therefore, $\varepsilon_1 \in E^+$. It follows that $\text{Ker}(\psi) = WE^+$. Since $|W/W^2| = 2$, we are done. Note that if $\phi(E) = W$ then $Q = 2$; if $\phi(E) = W^2$ then $Q = 1$. □

Corollary 2.4. *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.*

Proof. We first consider the case: $n = p^k, p > 2$. Let $\varepsilon \in E$. We know that $\varepsilon/\bar{\varepsilon}$ is a root of unity, therefore $\varepsilon/\bar{\varepsilon} = \pm\zeta_n^a$ for some a (all the roots of unity in $\mathbb{Q}(\zeta_n)$ are of this form). Suppose $\varepsilon/\bar{\varepsilon} = -\zeta_n^a$. We write $\varepsilon = b_0 + b_1\zeta_n + \ldots + b_{\phi(n)-1}\zeta_n^{\phi(n)-1}$. Then $\varepsilon \equiv b_0 + b_1 + \ldots + b_{\phi(n)-1} \pmod{1-\zeta_n}$. Also $\bar{\varepsilon} = b_0 + b_1\zeta_n^{-1} + \ldots + b_{\phi(n)-1}\zeta_n^{-(\phi(n)-1)} \equiv b_0 + b_1 + \ldots + b_{\phi(n)-1} \equiv \varepsilon = -\zeta^a\bar{\varepsilon} \equiv -\bar{\varepsilon} \pmod{1-\zeta_n}$. Therefore $2\bar{\varepsilon} \equiv 0 \pmod{1-\zeta_n}$. But $2 \notin (1-\zeta_n)$. Since $(1-\zeta_n)$ is a prime ideal, $\bar{\varepsilon} \in (1-\zeta_n)$ which is impossible since $\bar{\varepsilon}$ is a unit. Therefore $\varepsilon/\bar{\varepsilon} = +\zeta_n^a$. Let $2r \equiv a \pmod{n}$ (2 is invertible since $(2, p^k) = 1$), and let $\varepsilon_1 = \zeta_n^{-r}\varepsilon$. Then $\varepsilon = \zeta_n^r\varepsilon_1$ and $\varepsilon_1 \in E^+$ as $\bar{\varepsilon_1} = \varepsilon_1$. This proves that $Q = 1$ for $n = p^k, p > 2$.

Now let ε be a unit in $\mathbb{Q}(\zeta_{2^k})$ such that $\varepsilon/\bar{\varepsilon} \notin W^2$. Then $\varepsilon/\bar{\varepsilon} = \xi =$ a primitive 2^k-th root of unity. Let N denote the norm from $\mathbb{Q}(\zeta_{2^k})$ to $\mathbb{Q}(i)$. Then $N(\xi) = \xi^a$, where

$$a = \sum_{\substack{0<b<2^k \\ b\equiv 1 \pmod{4}}} b = 2^{k-2} + 2^{k-1}(2^{k-2}-1) \equiv 2^{k-2} \pmod{2^{k-1}}$$

Therefore ξ^a is a primitive 4-th root of unity i.e. $\xi^a = N(\varepsilon)/\overline{N(\varepsilon)} = \pm i$. But $N(\varepsilon)$ is a unit of $\mathbb{Q}(i)$, therefore ± 1 or $\pm i$. None of these possibilities works, so we have a contradiction. So $Q = 1$ for $\mathbb{Q}(\zeta_{2^k})$.

Now assume n is not a prime power. By Theorem 2.6, $1 - \zeta_n$ is a unit. But $(1-\zeta_n)/(1-\bar{\zeta_n}) = -\zeta_n$. Suppose $-\zeta_n \in W^2$. Then $-\zeta_n = (\pm\zeta_n^r)^2 = \zeta_n^{2r}$ so $-1 = \zeta_n^{2r-1}$. Clearly n must be even, so $n \equiv 0 \pmod{4}$. Since $\zeta_n^{n/2} = -1$, we have $n/2 \equiv 2r - 1 \pmod{n}$, therefore $n/2 \equiv -1 \pmod{2}$, which is impossible. It follows that $-\zeta_n \notin W^2$, so $Q = 2$. This completes the proof. □

We denote the class number of $\mathbb{Q}(\zeta_n)$ by h_n and that of the maximal real subfield of $\mathbb{Q}(\zeta_n)$ by h_n^+. Define $h_n^- := h_n/h_n^+$.

Theorem 2.17. *Let C_n be the ideal class group of $\mathbb{Q}(\zeta_n)$ and C_n^+ the ideal class group of the real subfield $\mathbb{Q}(\zeta_n)^+$. Then the natural map $C_n^+ \to C_n$ is an injection. Therefore h_n^+ divides h_n.*

Proof. Let I be an ideal in $\mathbb{Q}(\zeta_n)^+$ which becomes principal when lifted to $\mathbb{Q}(\zeta_n)$. We have to show that I is principal in $\mathbb{Q}(\zeta_n)^+$. Let $I = (\alpha)$ with $\alpha \in \mathbb{Q}(\zeta_n)$. Then $(\bar{\alpha}/\alpha) = (\bar{I}/I) = (1)$, since I is real. Therefore $\bar{\alpha}/\alpha$ is a unit and has absolute value 1. Hence $\bar{\alpha}/\alpha$ is a root of unity.

If n is not a prime power, $Q = 2$; so the map $\phi : E \to W$ in the proof of Theorem 2.16 is surjective which implies that there exists a unit $\varepsilon \in \mathbb{Q}(\zeta_n)$ such that $\varepsilon/\bar{\varepsilon} = \bar{\alpha}/\alpha$. Thus $\alpha\varepsilon$ is real and $I = (\alpha) = (\alpha\varepsilon)$. It follows from the unique factorization of ideals that $I = (\alpha\varepsilon)$ is principal in $\mathbb{Q}(\zeta_n)^+$.

Now suppose $n = p^k$. Let $\pi = \zeta_{p^k} - 1$. We have $\pi/\bar{\pi} = -\zeta_{p^k}$ which generates roots of unity in $\mathbb{Q}(\zeta_{p^k})$. Therefore $\bar{\alpha}/\alpha = (\pi/\bar{\pi})^d$ for some d. Since the π-adic valuation takes on only even values on $\mathbb{Q}(\zeta_{p^k})^+$ and since $\alpha\pi^d$ and I are real, $d = v_\pi(\alpha\pi^d) - v_\pi(\alpha) = v_\pi(\alpha\pi^d) - v_\pi(I)$ is even. Hence $\bar{\alpha}/\alpha = (-\zeta_{p^k})^d \in W^2$. In particular, $\bar{\alpha}/\alpha = \zeta^2 = \zeta/\bar{\zeta}$ for some root of unity ζ, and $\alpha\zeta$ is real. As before, $I = (\alpha\zeta)$ is principal in $\mathbb{Q}(\zeta_n)^+$. The second part of the theorem follows from the finiteness of ideal class groups. □

Theorem 2.18. *Suppose the extension of number fields L/K contains no unramified abelian subextension F/K with $F \neq K$. Then h_K divides h_L. In fact the norm map the norm map from the class group of L to the class group of K is surjective.*

Proof. Let H be the maximal unramified abelian extension (Hilbert class field) of K. By the assumption on L/K, we have $H \cap L = K$. Therefore $[HL : L] = [H : K]$. Since HL/L is unramified abelian, it is contained in the Hilbert class field of L. By class field theory, the Galois group of the Hilbert class field is isomorphic to the ideal class group. Hence $h_K = [H : K] = [HL : L]$ divides h_L. The second part is proved in the section on class field theory. □

Note that the above theorem is usually used in the case that L/K is totally ramified at some prime. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is totally ramified at the archimedean primes, we can apply the previous theorem and we get the result of Theorem 2.17 again i.e. h_n^+ divides h_n. Also we can use the above theorem for $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})$ where p is prime; since p is totally ramified and the class numbers of quadratic extensions can be computed easily using class number formula. e.g. $3 \mid h(\mathbb{Q}(\sqrt{-23})) \implies 3 \mid h_{23}$.

Corollary 2.5. *h_{p^m} divides h_{p^n} for $n \geq m$.*

Proof. Theorem 2.5 implies that the prime above p in $\mathbb{Q}(\zeta_{p^m})$ is totally ramified in $\mathbb{Q}(\zeta_{p^n})$. So we use Theorem 2.18 to get the result. □

Corollary 2.6. *If $m \mid n$ then $h_m \mid h_n$.*

Proof. Let $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ and $n = p_1^{e_1'} p_2^{e_2'} \dots p_r^{e_r'} q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$ where $q_i \nmid m, e_j' \geq e_j$ and $f_k \geq 0$. Let $\tilde{\mathfrak{p}_i}$ and $\tilde{\mathfrak{q}_j}$ be some primes above p_i and q_j resp. in $\mathbb{Q}(\zeta_m)$. Let K be an arbitrary subextension of $\mathbb{Q}(\zeta_n)$ containing $\mathbb{Q}(\zeta_m)$. Since $e_j' \geq e_j$ and $f_k \geq 0$, atleast one of $\tilde{\mathfrak{p}_i}$'s or $\tilde{\mathfrak{q}_j}$'s is ramified in K. So it follows from Theorem 2.18 that h_m divides h_n. □

Theorem 2.19. *Suppose L/K is a Galois extension* $\mathrm{Gal}(L/K)$ *is a p-group. Assume that there is at most one prime (finite or infinite) which ramifies L/K. If $p \mid h_L$ then $p \mid h_K$.*

Proof. Assume $p \mid h_L$. Let H be the maximal unramified abelian p-extension of L and $\mathrm{Gal}(H/L)$ is isomorphic to the p-Sylow subgroup of L. Since L/K is Galois, the maximality of H implies that H/K is Galois. Let G=$\mathrm{Gal}(H/K)$. As $|G| = |\mathrm{Gal}(H/L)||\mathrm{Gal}(L/K)|$, G is also a p-group. Let $\mathfrak{p}$ be the prime (if it exists) of K which ramifies in L, let $\tilde{\mathfrak{p}}$ be a prime of H above $\mathfrak{p}$. Let $I \subseteq G$ be the inertia group for $\tilde{\mathfrak{p}}$. Since H/L is unramified, $|I| \leq \deg(L/K) < |G|$. Now by a well-known result in the theory p-groups, there exists a normal subgroup G_1 of G, of index p, with $I \subseteq G_1 \subset G$. The inertia subgroups of other primes of H above $\mathfrak{p}$ are conjugates of I, hence lie in G_1. Since $\mathfrak{p}$ is the only ramified prime, no other prime of K ramifies in the fixed field of G_1. But the fixed field of G_1 is Galois of degree p over K, so K has unramified abelian extension of degree p. Class field theory implies that p divides h_K. □

Observe that if we take $K = \mathbb{Q}$ in the above theorem, then $h_K = 1$. So $p \nmid h_K$ implies that $p \nmid h_L$. Thus we have the following corollary:

Corollary 2.7. *If $L/\mathbb{Q}$ is Galois, $\mathrm{Gal}(L/\mathbb{Q})$ is a p-group, and exactly one finite prime ramifies, then $p \nmid h_L$.*

Corollary 2.8. *$p \mid h_p$ if and only if $p \mid h_{p^n}$ for $n \geq 1$.*

Proof. Corollary 2.6 implies the statement in the forward direction.
Since $|\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p))| = p^{n-1}$ and $(1-\zeta_p)$ is the only ramified prime in $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)$, Theorem 2.19 implies the statement in the backward direction. □

Theorem 2.20. *Let $n \not\equiv 2 \pmod 4$ be arbitrary. If $2 \mid h_n^+$ then $2 \mid h_n^-$.*

Proof. $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is totally ramified at infinity, so Theorem 2.18 implies that the norm map on the ideal class groups $N : C \to C^+$ is surjective. So $h_n^+ = |\ker(N)|$. Now if $2 \mid h_n^+$, then there exists a nontrivial ideal class $\alpha \in C^+$ such that $\alpha^2 = 1$. We lift α to C. Since $N(\alpha) = \alpha^2 = 1$, $\alpha \in \ker(N)$. Since the map $C^+ \to C$ is injective by Theorem 2.17, $\alpha \neq 1$ in C, but $\alpha^2 = 1$. Therefore $\ker(N)$ has even order, so $2 \mid h_n^-$. □

Let A be a finite abelian p-group. Then $A \cong \bigoplus \mathbb{Z}/p^{a_i}\mathbb{Z}$ for some integers a_i. Let n_a= number of i with $a_i = a$ and r_a= number of i with $a_i \geq a$. Then $r_1 = p$-rank of $A = \dim_{\mathbb{Z}/p\mathbb{Z}}(A/A^p)$. More generally, $r_a = \dim_{\mathbb{Z}/p\mathbb{Z}}(A^{p^{a-1}}/A^{p^a})$.

Theorem 2.21. *Let L/K be cyclic of degree n. Let p be prime, $p \nmid n$, and assume all fields E with $K \subseteq E \subset L$ satisfy $p \nmid h_E$. Let A be the p-Sylow subgroup of the ideal class group of L, and let f be the order of $p \pmod n$. Then $r_a(A) \equiv n_a(A) \equiv 0 \pmod f$ for all a. In particular, if $p \mid h_L$ then p-rank of A is atleast f and $p^f \mid h_L$.*

Proof. Let $V = A^{p^{a-1}}/A^{p^a}$, so V has p^{r_a} elements. Let $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Then σ acts on V. Let $v \in V, v \neq 0$, and suppose the orbit of v has less than n elements. Then $\sigma^i(v) = v$ for $i < n, i \mid n$. Therefore, $(\frac{n}{i})v = (1 + \sigma^i + \ldots + \sigma^{((n/i)-1)i})v = \mathrm{Norm}(v)$ where the norm is induced by the norm form L to the subfield of degree i over K. Since p does not divide the class number of this subfield, we have $(\frac{n}{i})v = 0$. But $p \nmid n$ so $v = 0$, contradiction. It follows that the orbit of $v \neq 0$ has n elements, so $p^{r_a} \equiv 1 \pmod{n}$. Therefore $f \mid r_a$. Since $n_a = r_a - r_{a+1}$, we obtain $f \mid n_a$. □

We use the above result to explicitly find the class group of $\mathbb{Q}(\zeta_{29})$ given that $h_{29} = 8$. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_{29})/\mathbb{Q}) = (\mathbb{Z}/29\mathbb{Z})^{\times} = \mathbb{Z}/28\mathbb{Z}$. Let K be the fixed field of $\mathbb{Z}/7\mathbb{Z}$. K is Galois of degree 4 over $\mathbb{Q}$ since $\mathbb{Z}/28\mathbb{Z} = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. The only prime that ramifies in $\mathbb{Q}(\zeta_{29})/\mathbb{Q}$ is 29 and it is totally ramified. So by Corollary 2.7, $2 \nmid h_K$. Now $\mathbb{Q}(\zeta_{29})/K$ is cyclic of order 7, $2 \nmid 7$ and $2 \nmid h_K$, also there are no nontrivial intermediate fields between $\mathbb{Q}(\zeta_{29})$ and K. So we can apply Theorem 2.21. The order f of $2 \pmod 7$ is 3, so the rank of the class group is atleast 3. Therefore the class group is $(\mathbb{Z}/2\mathbb{Z})^3$ since $h_{29} = 8$.

Chapter 3

p-adic L-functions

The present chapter describes two different methods of constructing p-adic L-functions, one given by Kubota-Leopoldt and another given by Kenkichi Iwasawa. The exposition given in this chapter is mainly based on the book by Iwasawa [3].

3.1 Kubota-Leopoldt's construction

In this section, we construct a p-adic meromorphic function defined on a sufficiently large domain in $\overline{\mathbb{Q}}_p$ and which takes the values of classical Dirichlet L-function $L(s, \chi)$ at the negative integers. These values, being algebraic integers (see Theorem (2.9), Chapter VII, [10]), can be considered as the elements in $\overline{\mathbb{Q}}_p$. Hence the p-adic function, so obtained, can be thought as a p-adic analogue of the classical Dirichlet L-function or p-adic L-function. In the following, we first study p-adic holomorphic functions which are defined by convergent power series and which take pre-assigned values at the negative integers. Using the results thus obtained, we then prove the existence and the uniqueness of the p-adic L-function mentioned above.

3.1.1 Generalized Bernoulli numbers and their properties

Ordinary Bernoulli numbers B_n and ordinary Bernoulli polynomials $B_n(x)$ are defined by following functions:

$$F(t) = \frac{te^t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}, F(t, x) = \frac{te^{(1+x)t}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}$$

We generalize these definitions as follows:

Definition 3.1. *Let χ be a Dirichlet character with conductor f and let*

$$F_\chi(t) = \sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}$$

$$F_\chi(t,x) = F_\chi(t)e^{xt} = \sum_{a=1}^{f} \frac{\chi(a)te^{(a+x)t}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi}(x)\frac{t^n}{n!}$$

the coefficients $B_{n,\chi}$, $B_{n,\chi}(x)$ in the power series expansions are called as generalized Bernoulli numbers and generalized Bernoulli polynomials respectively, belonging to the Dirichlet character χ .

We now mention some simple properties of generalized Bernoulli numbers that follow directly from the definition:

1. For $\chi = \chi^0$, principal character, $B_{n,\chi^0} = B_n$ and $B_{n,\chi^0}(x) = B_n(x)$.

2. $$B_{n,\chi}(x) = \sum_{i=1}^{n} \binom{n}{i} B_{i,\chi}x^{n-i}$$

3. $B_{n,\chi}(0) = B_{n,\chi}$

4. For $\chi \neq \chi^0$ $B_{0,\chi}$ = constant term in the power series expansion = constant term in $\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{ft}-1} = \frac{1}{f}\sum_{a=1}^{f}\chi(a) = 0$ and $B_{0,\chi^0} = 1$.

5. For $\chi \neq \chi^0$,

$$\begin{aligned} F_\chi(-t,-x) = \sum_{a=1}^{f} \frac{\chi(a)(-t)e^{-(a-x)t}}{e^{-ft}-1} &= \sum_{a=1}^{f} \frac{\chi(-1)\chi(f-a)(-t)e^{(f-a+x)t}}{e^{ft}-1} \\ &= \chi(-1)F_\chi(t,x) \end{aligned}$$

Therefore we have

$$(-1)^n B_{n,\chi}(-x) = \chi(-1)B_{n,\chi}(x)$$

Putting $x = 0$, we see that if $\chi \neq \chi^0$ and χ and n have different parities then $B_{n,\chi} = 0$ for all $n \geq 0$ from property 3.

6. Similarly

$$F_\chi(t,x) = \frac{1}{f}\sum_{a=1}^{f} \chi(a)F\Big(ft, \frac{a-f+x}{f}\Big)$$

implies

$$B_{n,\chi}(x) = \frac{1}{f}\sum_{a=1}^{f}\chi(a)f^n B_n\Big(\frac{a-f+x}{f}\Big)$$

In particular at $x = 0$,

$$B_{n,\chi} = \frac{1}{f}\sum_{a=1}^{f}\chi(a)f^n B_n\Big(\frac{a-f}{f}\Big)$$

7. For any integer $k \geq 0$ and $n \geq 0$, let

$$S_{n,\chi}(k) := \sum_{a=1}^{k}\chi(a)a^n$$

and let $S_n(k) := S_{n,\chi^0}(k)$. Now

$$F_\chi(t,x) - F_\chi(t,x-f) = \sum_{a=1}^{f}\chi(a)te^{(a+x-f)t}$$

implies

$$B_{n,\chi}(x) - B_{n,\chi}(x-f) = n\sum_{a=1}^{f}\chi(a)(a+x-f)^{n-1}$$

Replacing n by $n+1$ in the above and adding the equalities for $x = f, 2f, 3f, ..., kf$, we obtain

$$S_{n,\chi}(kf) = \frac{1}{n+1}(B_{n+1,\chi}(kf) - B_{n+1,\chi}(0)) \tag{3.1}$$

In particular, for $\chi = \chi^0, f = 1$, we have

$$S_n(k) = \frac{1}{n+1}(B_{n+1}(k) - B_{n+1}(0))$$

Lemma 3.1. *Let $\mathbb{Q}_p(\chi)$ denote the field generated by $\chi(a), a \in \mathbb{Z}$ over $\mathbb{Q}_p$. In $\mathbb{Q}_p(\chi)$*

$$B_{n,\chi} = \lim_{h\to\infty}\frac{S_{n,\chi}(p^h f)}{p^h f}$$

Proof. Using property 2, we have

$$B_{n+1,\chi}(x) - B_{n+1,\chi}(0) = (n+1)B_{n,\chi}x + A(x)$$

where all the terms in $A(x)$ have degree ≥ 2 in x. Putting $x = p^h f$ and from 3.1, we get

$$\frac{S_{n,\chi}(p^h f)}{p^h f} = B_{n,\chi} + \frac{A(p^h f)}{p^h f}$$

Taking $\lim_{h\to\infty}$ on both sides, we get the result because $\lim_{h\to\infty} \frac{A(p^h f)}{p^h f} = 0$ in $\mathbb{Q}_p(\chi)$. □

For $\chi = \chi^0, f = 1$, the above lemma states

$$B_n = \lim_{h\to\infty} \frac{S_n(p^h)}{p^h} \tag{3.2}$$

Lemma 3.2. *The power of any prime p dividing the denominator of any Bernoulli number B_n is at most 1.*

Proof. By 3.2, it is sufficient to show that $S_n(p^h) \equiv 0 \pmod{p^{h-1}}$. This is trivial for $h = 1$. Let $h > 1$. Since every integer a, $1 \leq a \leq p^h$ can be written uniquely in the form of $a = b + cp^{h-1}$ where $1 \leq b \leq p^{h-1}$ and $1 \leq c < p$, we have

$$S_n(p^h) = \sum_{a=1}^{p^h} a^n \equiv p \sum_{b=1}^{p^{h-1}} = pS_n(p^{h-1}) \pmod{p^{h-1}}$$

Hence the lemma is proved by induction on h. □

3.1.2 p-adic holomorphic functions as convergent power series

Let K be a finite extension of $\mathbb{Q}_p$ contained in $\overline{\mathbb{Q}}_p$ and $K[[x]]$ be the ring of all formal power series in x. K is a locally compact field (see Proposition 1 and 3, Chapter II, [11]) and $A(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ converges at $x = x_0$ in $\overline{\mathbb{Q}}_p$ if and only if $|a_n x_0^n| \to 0$ as $n \to \infty$. Hence if $A(x_0) < \infty$ then $A(x) < \infty$ for all $x \in \overline{\mathbb{Q}}_p$ with $|x| < |x_0|$.

Lemma 3.3. *Let $A(x)$ and $B(x)$ be power series in $K[[x]]$, convergent in a neighbourhood of 0 in $\overline{\mathbb{Q}}_p$. Suppose that $A(\xi_i) = B(\xi_i)$ for some sequence of elements $\xi_i \in \overline{\mathbb{Q}}_p$ such that $\xi_i \neq 0$ for all i and $\lim_{i\to\infty} \xi_i = 0$. Then $A(x) = B(x)$.*

Proof. Let $A(x) - B(x) = \sum_{n=0}^{\infty} c_n x^n \in K[[x]]$. Assume that $A(x) \neq B(x)$. Then there exists minimum n_0 such that $c_{n_0} \neq 0$. Thus $A(x) - B(x) = \sum_{n \geq c_{n_o}} c_n x^n$. Hence

$$0 = A(\xi_i) - B(\xi_i) = \xi_i^{n_0}\Big(c_{n_0} + \sum_{n>n_o} c_n \xi_i^{n-n_o}\Big)$$

Since $\xi_i \neq 0$ for all i, we get

$$-c_{n_0} = \sum_{n>n_o} c_n \xi_i^{n-n_o} = \xi_i \Big(\sum_{k=1}^{\infty} c_{n_0+k} \xi_i^{k-1} \Big)$$

Taking $\lim_{i\to\infty}$ on both sides, we see that $\xi_i \to 0$ and the sum remains bounded. Therefore we get the contradiction $c_{n_0} = 0$. □

For a power series $A = A(x) = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$, we define $\|A\| := \sup_n |a_n|$ and $P_K := \{A \in K[[x]] \mid \|A\| < \infty\}$. Note that $K[x] \subseteq P_K \subseteq K[[x]]$. One can easily verify that $\|A\|$ defines norm on P_K.

Lemma 3.4. *P_K is complete with respect to the norm $\|A\|$, so it is a Banach algebra over a local field K.*

Proof. Let $A_k = \sum_{n=0}^{\infty} a_n^k x^n$ be a cauchy sequence in P_K. Then given $\epsilon > 0$, there exists $N > 0$ such that $\|A_{k_1} - A_{k_2}\| = \sup_n |a_n^{k_1} - a_n^{k_2}| < \epsilon$ for all $k_1, k_2 > N$. So, for each $n \geq 0$, $|a_n^{k_1} - a_n^{k_2}| \leq \sup_n |a_n^{k_1} - a_n^{k_2}| < \epsilon$. Therefore a_n^k is cauchy for each n and thus converges in K. Let $\lim_{k\to\infty} a_n^k = a_n$ and $A = \sum_{n=0}^{\infty} a_n x^n$. We'd like to show that A_k converges to A.

By replacing ϵ by $\epsilon/2$ in the previous paragraph, we can find an $N' > 0$ such that $|a_n^{k_1} - a_n^{k_2}| < \epsilon/2$ for all $n \geq 0$ and $k_1, k_2 > N'$. Taking limits as $k_2 \to \infty$, we obtain $|a_n^k - a_n| \leq \epsilon/2$ for all $n \geq 0$ and $k > N'$. Taking supremum in n, we get $\sup_n |a_n^k - a_n| = \|A_k - A\| \leq \epsilon/2 < \epsilon$ for all $k > N'$. This implies A_k converges to A and we are done. □

For each $n \geq 0$, we define a polynomial $\binom{x}{n} \in K[x]$ by

$$\binom{x}{n} = \frac{x(x-1)(x-2)....(x-n+1)}{n!} \qquad \binom{x}{0} = 1, \binom{x}{1} = x$$

It is obvious that

$$\Big\| \binom{x}{n} \Big\| \leq \Big| \Big(\frac{1}{n!} \Big) \Big| \tag{3.3}$$

Lemma 3.5. *For $n \geq 1$,*

$$|p|^{\frac{n}{p-1}} \leq |n!| \leq np|p|^{\frac{n}{p-1}}$$

Proof. Write n in a prime p-basis: $n = \sum_{i=1}^{N} a_i p^i$ ($a_N \neq 0, 1 \leq a_i < p$). Let $s = \sum_{i=1}^{N} a_i$. Then it can be easily shown that the highest power of p dividing $n!$ is $\frac{n-s}{p-1}$. Hence $|n!| = |p|^{\frac{n-s}{p-1}} \geq |p|^{\frac{n}{p-1}}$. As $a_N \geq 1$, $n \geq p^N$. Therefore $N \leq \frac{\log n}{\log p}$.

Now $s \leq (p-1)(N+1) \leq (p-1)(\frac{\log n}{\log p} + 1)$ thus $\frac{s}{p-1} \leq \frac{\log{(np)}}{\log p}$. So $|n!| = |p|^{\frac{n-s}{p-1}} = |p|^{\frac{n}{p-1}} p^{\frac{s}{p-1}} \leq np|p|^{\frac{n}{p-1}}$ ($|p| = p^{-1}$). □

Note that $|p|^{\frac{n}{p-1}} \leq |n!|$ holds for $n = 0$. Hence 3.3 and Lemma 3.5 give us for all $n \geq 0$

$$\left\| \binom{x}{n} \right\| \leq |p|^{\frac{-n}{p-1}} \tag{3.4}$$

Now let $b_n (n \geq 0)$ be a sequence of elements in K and let

$$c_n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} b_i$$

so that

$$e^{-t} \sum_{n=0}^{\infty} b_n \frac{t^n}{n!} = \sum_{n=0}^{\infty} c_n \frac{t^n}{n!}$$

and

$$b_n = \sum_{i=0}^{n} \binom{n}{i} c_i$$

Theorem 3.1. *Let r be a real number such that $0 < r < |p|^{\frac{1}{p-1}}$. Suppose $|c_n| \leq Cr^n$ for all $n \geq 0$ with some $C > 0$. Then there exists a unique power series $A(x)$ in P_K satisfying following properties:*

1. *$A(x)$ converges at every ξ in $\overline{\mathbb{Q}}_p$ such that $|\xi| < |p|^{\frac{1}{p-1}} r^{-1}$.*

2. *$A(n) = b_n$ for every $n \geq 0$.*

Proof. Since $|p|^{\frac{1}{p-1}} r^{-1} > 1$, property 1 implies $A(x)$ converges for all $\xi \in \overline{\mathbb{Q}}_p$ with $|\xi| \leq 1$ so that $A(n)$ mentioned in property 2 are well-defined. Now let

$$A_k(x) = \sum_{n=0}^{\infty} a_n^k x^n = \sum_{i=0}^{k} c_i \binom{x}{i} \qquad (a_n^k \in K)$$

As $A_k(x)$ is a polynomial of degree $\leq k$, $a_n^k = 0$ for $n > k$. By the assumption on c_n,

$$\left\| c_n \binom{x}{n} \right\| \leq |c_n| |p|^{\frac{-n}{p-1}} \leq Cr_1^n$$

where $r_1 = r|p|^{\frac{-1}{p-1}} < 1$. Hence

$$\|A_l - A_k\| \leq \max_{k<i\leq l} \left\| c_i \binom{x}{i} \right\| \leq Cr_1^{k+1} \qquad (k < l)$$

It follows from Lemma 3.4 that $\lim_{k\to\infty} A_k = A$ exists in P_K and we have $\|A - A_k\| \leq Cr_1^{k+1}$.

Let $A = \sum_{n=0}^{\infty} a_n x^n$. Then $\lim_{k\to\infty} a_n^k = a_n$. Now

$$|a_n^k| = |a_n^k - a_n^{n-1}| \leq \|A_k - A_{n-1}\| \leq Cr_1^n \qquad (k \geq n)$$

Hence $|a_n| < Cr_1^n$ fo all $n \geq 0$. Therefore $A(x)$ converges at ξ in $\overline{\mathbb{Q}}_p$ with $|\xi| < r_1^{-1} = |p|^{\frac{1}{p-1}} r^{-1}$ because $|a_n \xi^n| \leq C\delta^n$ for some δ such that $0 < \delta < 1$.

Now fix $\xi, |\xi| < r_1^{-1}$ and consider

$$A(\xi) - A_k(\xi) = \sum_{n=0}^{\infty} (a_n - a_n^k)\xi^n$$

If $k < n$, then

$$|(a_n - a_n^k)\xi^n| = |a_n \xi^n| \leq Cr_1^n |\xi^n| \leq C(r_1\xi)^k$$

and if $k \geq n$, then

$$|(a_n - a_n^k)\xi^n| = \|A - A_k\| |\xi^n| \leq Cr_1^{k+1}|\xi^n|$$

where $Cr_1^{k+1}|\xi^n| \leq Cr_1^k$ if $|\xi| \leq 1$ and $Cr_1^{k+1}|\xi^n| \leq C(r_1|\xi|)^k$ if $|\xi| \geq 1$. Therefore

$$|A(\xi) - A_k(\xi)| \leq \max(Cr_1^k, C(r_1|\xi|)^k).$$

Thus we see that $A(\xi) = \lim_{k\to\infty} A_k(\xi)$. For each integer $n \leq k$,

$$A_k(n) = \sum_{i=0}^{k} c_i \binom{n}{i} = \sum_{i=0}^{n} c_i \binom{n}{i} = b_n$$

Hence it follows from the above that $A(n) = b_n$. This proves the existence of $A(x)$ having properties 1 and 2. The uniqueness of $A(x)$ is an immediate consequence of Lemma 3.3. □

We restate the formula proved above as the following:

Corollary 3.1. *Let $A(x)$ be the power series in Theorem 3.1. For each $\xi \in \overline{\mathbb{Q}}_p$ with $|\xi| < |p|^{\frac{1}{p-1}} r^{-1}$,*

$$A(\xi) = \lim_{k\to\infty} \sum_{i=0}^{k} c_i \binom{\xi}{i} = \sum_{i=0}^{\infty} c_i \binom{\xi}{i}$$

3.1.3 Construction of the p-adic L-function

Let $q = p$ for all $p > 2$ and $q = 4$ for $p = 2$. Let $U = \mathbb{Z}_p^{\times}, D = 1 + q\mathbb{Z}_p$ and V be the cyclic group of order $p-1$ consisting $(p-1)$ roots of unity in $\mathbb{Q}_p$. Then we have the following isomorphism:

$$U \cong V \times D$$

Each $a \in U$ can be uniquely written in the form $a = \omega(a)\langle a\rangle$ where $\omega(a) \in V$ and $\langle a\rangle \in D$. Note that $\omega(a)$ is a p-adic Dirichlet character of conductor q and order $\phi(q)$.

Let χ be a Dirichlet character with conductor f and ω be a character introduced above. For each integer n, define the product $\chi_n := \chi\omega^{-n}$. Then the conductor f_n of χ_n divides fq and since $\chi = \chi_n\omega^n$, f divides f_nq. Therefore f and f_n differ only by a power of p. Thus if $a \in \mathbb{Z}, (a,p) = 1$ then $(a,f) = (a,f_n)$ and $\chi_n(a) = \chi(a)\omega(a)^{-n}$.

Now, let $K = \mathbb{Q}_p(\chi)$= the field generated by the values of $\chi(a), a \in \mathbb{Z}$ over $\mathbb{Q}_p$. As $\chi(a)$ are algebraic integers, $\chi(a) \in \overline{\mathbb{Q}}_p$. Therefore K is a finite extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$. We now define a sequence of elements in K for $n \geq 0$:

$$b_n = (1 - \chi_n(p)p^{n-1})B_{n,\chi_n}$$

Note that $\chi_n(a) \in K$ for all $a \geq 0$. As before,

$$c_n = \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}b_i$$

Lemma 3.6. $|c_n| < |q^2f|^{-1}|q|^n$ *for all* $n \geq 0$.

Proof. From Lemma 3.1, we have

$$B_{n,\chi_n} = \lim_{h\to\infty}\frac{S_{n,\chi_n}(p^hf_n)}{p^hf_n}$$

Since f and f_n differ only by a power of p,

$$\begin{aligned} B_{n,\chi_n} &= \lim_{h\to\infty}\frac{S_{n,\chi_n}(p^hf)}{p^hf} \\ &= \lim_{h\to\infty}\frac{\sum_{a=1}^{p^hf}\chi_n(a)a^n}{p^hf} \end{aligned}$$

Hence

$$\begin{aligned} b_n &= \lim_{h\to\infty}\frac{\sum_{a=1}^{p^hf}\chi_n(a)a^n}{p^hf} - \lim_{h\to\infty}\frac{\chi_n(p)p^{n-1}\sum_{a=1}^{p^{h-1}f}\chi_n(a)a^n}{p^{h-1}f} \\ &= \lim_{h\to\infty}\frac{\sum_{a=1}^{p^hf}\chi_n(a)a^n - \sum_{a=1}^{p^{h-1}f}\chi_n(pa)(pa)^n}{p^hf} \end{aligned}$$

$$\begin{aligned} b_n &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1\\ p\nmid a}}^{p^h f} \chi_n(a) a^n \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1\\ (a,p)=1}}^{p^h f} \chi(a)\omega(a)^{-n}\omega(a)^n \langle a\rangle^n \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1\\ (a,p)=1}}^{p^h f} \chi(a)\langle a\rangle^n \\ &= \lim_{h\to\infty} \frac{1}{q^h f} \sum_{\substack{a=1\\ p\nmid a}}^{g^h f} \chi(a)\langle a\rangle^n \end{aligned}$$

Therefore

$$c_n = \lim_{h\to\infty} \frac{c_{n,h}}{q^h f}$$

where

$$c_{n,h} = \sum_{\substack{a=1\\ p\nmid a}}^{g^h f} \sum_{i=0}^{n} \binom{n}{i} \chi(a)\langle a\rangle^i (-1)^{n-i} = \sum_{\substack{a=1\\ p\nmid a}}^{g^h f} \chi(a)(\langle a\rangle - 1)^n$$

We next prove that $\frac{c_{n,h}}{q^h f} \equiv 0 \pmod{\frac{q^n}{q^2 f}}$ in K for $h \geq 1$ by induction. This is trivial for $h = 1$ as $\langle a\rangle \equiv 1 \pmod{q}$. Let $h > 1$ and let $1 \leq a \leq q^{h+1}f, (a,p) = 1$. Write a in the form

$$a = u + q^h f v \qquad\qquad (1 \leq u \leq q^h f, 0 \leq q < v)$$

Since $a \equiv u \pmod{q}$, we have $\omega(a) = \omega(u)$. Thus

$$\langle a\rangle = \langle u\rangle + \omega(u)^{-1} q^h f v$$

Hence

$$(\langle a\rangle - 1)^n = \sum_{i=0}^{n} \binom{n}{i} (\langle u\rangle - 1)^i (\omega(u)^{-1} q^h f v)^{n-i}$$

where the i-th term in the sum on the right is divisible $q^{i+h(n-i)}$. If $n - i \geq 1$ then $i + h(n-i) = n + (h-1)(n-i) \geq n + h - 1$. Therefore

$$\chi(a)(\langle a\rangle - 1)^n \equiv \chi(u)(\langle u\rangle - 1)^n \pmod{q^{n+h-1}}$$

Taking the sum over a, we see that

$$c_{n,h+1} \equiv q c_{n,h} \pmod{q^{n+h-1}}$$

so that

$$\frac{c_{n,h+1}}{q^{h+1}f} \equiv \frac{c_{n,h}}{q^h f} \pmod{\frac{q^n}{q^2 f}}$$

Therefore by induction, we see that $\frac{c_{n,h}}{q^h f} \equiv 0 \pmod{\frac{q^n}{q^2 f}}$ for $h \geq 1$. Taking $\lim_{h\to\infty}$, we have $\frac{c_n q^2 f}{q^n} \in \mathbb{Z}_p$ and hence the lemma is proved. □

We now apply Theorem 3.1 for the above sequences b_n and c_n and for $r = |q| < |p|^{\frac{1}{p-1}}$. The theorem gives us the unique power series $A_\chi(x)$ in $K[[x]]$ which converges at every ξ in $\overline{\mathbb{Q}}_p$ with $|\xi| < |p|^{\frac{1}{p-1}}|q|^{-1}$ and satisfies

$$A_\chi(n) = (1 - \chi_n(p)p^{n-1})B_{n,\chi_n} \qquad (n \geq 0)$$

In particular, by Property 4 of the generalized Bernoulli numbers, we have for $\chi = \chi^0$

$$A_\chi(0) = (1 - \chi(p)p^{-1})B_{0,\chi} = 1 - \frac{1}{p}$$

and 0 for non-principal characters.

Theorem 3.2. *There exists a p-adic meromorphic function $L_p(s,\chi)$ with the following properties:*

1. *It is given by*

$$L_p(s,\chi) = \frac{a_{-1}}{s-1} + \sum_{n=0}^{\infty} a_n(s-1)^n \qquad a_n \in K = \mathbb{Q}_p(\chi)$$

where $a_{-1} = 1 - \frac{1}{p}$ if $\chi = \chi^0$ and 0 otherwise. Also the power series converges in the domain $\mathfrak{D} = \{s \mid s \in \overline{\mathbb{Q}}_p, |s-1| < r\}$, $r = |p|^{\frac{1}{p-1}}|q|^{-1} > 1$.

2. *For $n = 1, 2, 3, ...$, we have*

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

Furthermore, $L_p(s,\chi)$ is uniquely characterized by the above two properties as a p-adic meromorphic function on the domain $\mathfrak{D}$.

Proof. Let $L_p(s,\chi) = \frac{A_\chi(1-s)}{s-1}$ where $A_\chi(x)$ is mentioned above. As $L(1-n,\chi_n) = \frac{-B_{n,\chi_n}}{n}$, both properties 1 and 2 follow immediately from the corresponding properties of $A_\chi(x)$. The uniqueness of $L_p(s,\chi)$ is a consequence of Lemma 3.3. □

The Theorem 3.2 gives us the p-adic meromorphic $L_p(s,\chi)$ function which agrees with the Dirichlet L-function $L(s,\chi)$ at negative integers with Euler factor at prime p removed.

As already mentioned in the beginning, we call $L_p(s,\chi)$ the p-adic L-function.

We now give a brief outline of the proof of Kummer's criterion for irregularity of primes. First we mention some useful theorems which are required to prove the criterion. The proofs of these results can be found in Chapter 4, [13].

Theorem 3.3 (Conductor-Discriminant Formula)**.** *Let K be the number field associated to the group X of Dirichlet characters. Then the discriminant of K is given by*

$$d(K) = (-1)^{r_2} \prod_{\chi\in X} f_\chi$$

where r_1, r_2 are the number of real and complex embeddings of K into $\mathbb{C}$ resp. and f_χ is a conductor of χ.

Theorem 3.4 (Class Number Formula)**.** *Let h be the class number of K, R be the regulator and w be the number of roots of unity in K. Then*

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|d(K)|}} = \prod_{\chi\in X,\chi\neq 1} L(1,\chi)$$

If K is a CM-field, K^+ is its maximum real subfield and h and h^+ are the respective class numbers then from the class field theory; we know that h^+ divides h. The quotient h^- is called the relative class number. Using the class number formula for K and K^+, the conductor-discriminant formula and the expression of $L(1,\chi)$ for odd characters in terms of Bernoulli numbers, we obtain

Theorem 3.5.

$$h^-(K) = Qw \prod_{\chi \text{ odd}} (-\frac{1}{2}B_{1,\chi})$$

where Q (= 1 or 2) is the index of a subgroup of the units in K^+ in a group of the units in K.

Coming back to p-adic L-functions, if $\chi \neq \chi^0$ and $pq \nmid f_\chi$, then one can show that p divides all the coefficients a_i's (except possibly a_0) in the power series expression of $L_p(s,\chi)$ (see Theorem 5.12, [13]).

Corollary 3.2. *Suppose $\chi \neq 1, pq \nmid f$. Let $m, n \in \mathbb{Z}$. Then $L_p(m,\chi) \equiv L_p(n,\chi) \pmod{p}$.*

Proof. Both sides are congruent to a_0. □

Corollary 3.3 (Kummer's Congruences)**.** *Suppose $m \equiv n \pmod{p-1}, (p-1) \nmid n$ are positive even integers. Then*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}$$

More generally, if m and n are positive even integers with $m \equiv n \pmod{(p-1)p^a}$ and $(p-1) \nmid n$ then

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

Proof. Here p is assumed to be odd. Since $m \equiv n \pmod{p-1}$, $\omega^m = \omega^n$, and so $L_p(s, \omega^m) = L_p(s, \omega^n)$. We have $L_p(1-m, \omega^m) = -(1-p^{m-1})(B_m/m)$ and similarly for n. Also

$$\begin{aligned} L_p(1-m, \omega^m) &= a_0 + a_1(-m) + a_2(-m)^2 \dots \\ &\equiv a_0 + a_1(-n) + a_2(-n)^2 \dots \pmod{p^{a+1}} \\ &\equiv L_p(1-n, \omega^n) \pmod{p^{a+1}} \end{aligned}$$

Hence the result follows. □

Corollary 3.4. *Suppose n is odd, $(p-1) \nmid (n+1)$. Then*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \pmod{p}$$

and both sides are p-integral.

Proof. We have $\omega^{n+1} \neq \chi^0$ and $\omega^n(p) = 0$. Therefore by Corollary 3.2,

$$\begin{aligned} B_{1,\omega^n} &= (1-\omega^n(p))B_{1,\omega^n} \\ &= -L_p(0, \omega^{n+1}) \equiv -L_p(1-(n+1), \omega^{n+1}) \pmod{p} \\ &= (1-p^n)\frac{B_{n+1}}{n+1} \equiv \frac{B_{n+1}}{n+1} \pmod{p} \end{aligned}$$

The p-integrality also follows from Corollary 3.2. □

Theorem 3.6. *Let p be an odd prime and let h_p^- be the relative class number of $\mathbb{Q}(\zeta_p)$. Then $p|h_p^-$ if and only if p divides the numerator of some $B_j, j = 2, 4, 6, ..., p-3$.*

Proof. The odd characters corresponding to $\mathbb{Q}(\zeta_p)$ are $\omega, \omega^3, \dots, \omega^{p-2}$. Therefore, by Theorem 3.5,

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-2} \Big(-\frac{1}{2}B_{1,\omega^j}\Big)$$

($Q = 1$ by Corollary 2.4, $w = 2p$). Note that

$$B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv \frac{p-1}{p} \pmod{\mathbb{Z}_p}$$

Therefore $(2p)(-\frac{1}{2}B_{1,\omega^{p-2}}) \equiv 1 \pmod{p}$, so we have

$$h_p^- = \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \Big(-\frac{1}{2}B_{1,\omega^j}\Big) \pmod{p}$$

Hence by Corollary 3.4,

$$h_p^- = \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} \Big(-\frac{1}{2}\frac{B_{j+1}}{j+1}\Big) \pmod{p}$$

The theorem follows immediately. □

Next we show that $p \mid h_p \iff p \mid h_p^-$. We know that $L_p(1,\chi)$ has no pole if $\chi \neq \chi^0$.

Theorem 3.7 (p-adic Class Number Formula)**.** *Let K be a totally real abelian number field of degree n corresponding to a group X of Dirichlet characters. Then*

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{d(K)}} = \prod_{\substack{\chi\in X \\ \chi\neq 1}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1,\chi)$$

Proof. See Theorem 5.24, [13]. □

Proposition 3.1. *Suppose K is totally real Galois number field. If there is only one prime of K above p, and if the ramification of p is at most $p-1$, then*

$$\left|\frac{[K:\mathbb{Q}]R_p(K)}{\sqrt{d(K)}}\right|_p \leq 1.$$

Proof. See Proposition 5.33, [13]. □

Theorem 3.8. *If $p \mid h_p^+$ then $p \mid h_p^-$. Therefore $p \mid h_p \iff p$ divides the numerator B_j for some $j = 2, 4, 6, ..., p-3$.*

Proof. The characters corresponding to $\mathbb{Q}(\zeta_p)^+$ are $1, \omega^2, ..., \omega^{p-3}$. Let $n = (p-1)/2$. Then

$$\frac{2^{n-1}h^+R_p^+}{\sqrt{d^+}} = \prod_{\substack{j=2 \\ j \text{ even}}}^{p-3} L_p(1,\omega^j)$$

Since $\mathbb{Q}(\zeta_p)^+$ satisfies the hypotheses of proposition 1, we have $|R_p^+/\sqrt{d^+}| \leq 1$. Thus $p \mid h^+ \Longrightarrow p \mid L_p(1,\omega^j)$ for some j. By Corollary 3.2,

$$0 \equiv L_p(1,\omega^j) \equiv L_p(0,\omega^j) = -(1-\omega^{j-1}(p))B_{1,\omega^{j-1}} = -B_{1,\omega^{j-1}} \pmod{p}$$

Since by Theorem 3.6,

$$h^- = \prod_{\substack{i=1 \\ i \text{ odd}}}^{p-4} (-\frac{1}{2}B_{1,\omega^i}) \pmod p$$

we have $p \mid h^-$, as desired. □

This completes the proof of Kummer's criterion for the irregularity of prime numbers.

3.2 Iwasawa's construction

In this section, we give another construction of p-adic L-functions which is closely related to the arithmetic of cyclotomic extensions. This construction was given by Iwasawa in 1969.

3.2.1 Group rings and power series

As before, let $q = 4$ or $q = p$ according to $p = 2$ or $p > 2$. Let $(d, p) = 1$. Now, a Dirichlet character χ is called a character of the first kind if its conductor $f_\chi = d$ or $f_\chi = dq$ and it is called a character of the second kind if $f_\chi = 1$ or $f_\chi = qp^n, n \geq 0$ (power of p). Using the natural isomorphisms

$$(\mathbb{Z}/dqp^n\mathbb{Z})^\times \cong (\mathbb{Z}/d\mathbb{Z})^\times \times (\mathbb{Z}/qp^n\mathbb{Z})^\times \tag{3.5}$$

$$(\mathbb{Z}/qp^n\mathbb{Z})^\times \cong (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z}) \tag{3.6}$$

we see that any Dirichlet character χ can be uniquely decomposed into a product of a character of the first kind θ and a character of the second kind ψ: $\chi = \theta\psi$.

Define $q_n = dqp^n$, then $(a, q_0) = 1$ if and only if $(a, q_n) = 1$. Let $\sigma_n(a)$= residue class of a modulo q_n. These $\sigma_n(a), (a, q_0) = 1$ the multiplicative group $G_n = (\mathbb{Z}/q_n\mathbb{Z})^\times$. For $m \geq n \geq 0$, we have a natural surjective homomorphism from $G_m \to G_n$: $\sigma_m(a) \mapsto \sigma_n(a)$. Let Γ_n denote the kernel of $G_n \to G_0$ that is

$$\Gamma_n = \{\sigma_n(a) \mid a \equiv 1 \pmod{q_o}\}$$

This is a cyclic group of order p^n. Define another subgroup of Δ_n of G_n by

$$\Delta_n = \{\sigma_n(a) \mid a^{p-1} \equiv \pm 1 \pmod{qp^n}\}$$

Note that for $p > 2$, there exists no integer a such that $a^{p-1} \equiv -1 \pmod{qp^n}$. Therefore the above condition is same as $a^{p-1} \equiv 1 \pmod{qp^n}$. The natural isomorphism mentioned in 3.5 and 3.6 implies that

$$G_n = \Delta_n \times \Gamma_n$$

Furthermore, $m \geq n \geq 0$, a homomorphism $G_m \to G_n$ induces

$$\Gamma_m \to \Gamma_n \quad , \quad \Delta_m \cong \Delta_n$$

Now, let

$$G = \varprojlim G_n \quad , \quad \Gamma = \varprojlim \Gamma_n \quad , \quad \Delta = \varprojlim \Delta_n$$

with respect to the above homomorphisms. These are profinite abelian groups and

$$G = \Delta \times \Gamma$$

where $\Delta \cong \Delta_0 = G_0$. For $a \in \mathbb{Z}, (a, q_0) = 1$, let

$$\sigma_n(a) = \delta_n(a)\gamma_n(a) \qquad \delta_n(a) \in \Delta_n, \gamma_n(a) \in \Gamma_n$$

Let $\sigma(a), \delta(a)$ and $\gamma(a)$ be the inverse limits of $\sigma_n(a), \delta_n(a)$ and $\gamma_n(a)$ respectively. Then we have

$$\sigma(a) = \delta(a)\gamma(a)$$

Let $a, b \in \mathbb{Z}$, $(a, q_0) = (b, q_0) = 1$. then the following isomorphism

$$(\mathbb{Z}/p^n\mathbb{Z}) \cong (\mathbb{Z}_p/p^n\mathbb{Z}_p) \cong (1 + q\mathbb{Z}_p)/(1 + qp^n\mathbb{Z}_p) \tag{3.7}$$

implies $\gamma_n(a) = \gamma_n(b)$ if and only if $\langle a \rangle \equiv \langle b \rangle \bmod qp^n\mathbb{Z}_p$ (The last isomorphism is given by $\mathbb{Z}_p \mapsto (1+q)^{\mathbb{Z}_p} = 1 + q\mathbb{Z}_p$). Therefore,

$$\Gamma_n \cong (1 + q\mathbb{Z}_p)/(1 + qp^n\mathbb{Z}_p)$$

$$\gamma_n(a) \mapsto \langle a \rangle (1 + qp^n\mathbb{Z}_p)$$

Taking inverse limits, it follows that $\gamma(a) = \gamma(b)$ if and only if $\langle a \rangle = \langle b \rangle$ and

$$\Gamma \cong (1 + q\mathbb{Z}_p)$$

$$\gamma(a) \mapsto \langle a \rangle$$

Let K be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}$ be the ring of local integers in K and $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$. Let $\Lambda = \mathcal{O}[[x]]$. Λ is a local ring and its maximal ideal $\mathfrak{m}$ is generated by x and $\mathfrak{p}$ (see Proposition 13.9 [13]). $\mathfrak{m}$ defines $\mathfrak{m}$-adic topology on Λ which makes it into a compact topological ring. Let $\mathcal{O}[\Gamma_n]$ denote the group ring. For $m \geq n \geq 0$, the group homomorphism $\Gamma_m \to \Gamma_n$ induces a natural morphism of group rings $\mathcal{O}[\Gamma_m] \to \mathcal{O}[\Gamma_n]$. Let

$$\mathcal{O}[[\Gamma]] = \varprojlim \mathcal{O}[\Gamma_n]$$

Note that $\mathcal{O}[\Gamma] \subseteq \mathcal{O}[[\Gamma]]$. In fact, we shall see that this inclusion is proper. The $\mathfrak{p}$-adic topology on $\mathcal{O}$ defines a natural compact topology on each free $\mathcal{O}$-module $\mathcal{O}[\Gamma_n]$. Hence $\mathcal{O}[[\Gamma]]$ is a profinite group ring of Γ.

Lemma 3.7. $\Lambda = \mathcal{O}[[x]] \cong \mathcal{O}[[\Gamma]]$, *the isomorphism being induced by* $1 + x \mapsto \gamma(1 + q_0)$. *Moreover, the isomorphism is unique.*

Proof. Since $\mathcal{O}[x]$ is everywhere dense in $\mathcal{O}[[x]]$, the uniqueness is obvious. It is easy to see that, for each $n \geq 0$, there is an isomorphism

$$\mathcal{O}[x]/((1+x)^{p^n} - 1) \cong \mathcal{O}[\Gamma_n]$$

given by $1 + x \bmod ((1+x)^{p^n} - 1) \mapsto \gamma_n(1 + q_0)$. The limit of these isomorphisms gives us the required isomorphism in the lemma. □

Now, let ψ be a Dirichlet character of the second kind and we choose a field K that contains all the values of $\psi(a), a \in \mathbb{Z}$. We denote by n_0 the smallest integer such that $f_\psi \mid q_n$ for all $n \geq n_0$. Now fix integer t and consider residue class of $\psi(a)^{-1}\langle a\rangle^{-t} \pmod{q_n\mathcal{O}}$ where $(a, q_0) = 1$. This residue class depends only on $\gamma_n(a)$ for $n \geq n_0$. Therefore we have a homomorphism of $\mathcal{O}$-algebras for $n \geq n_0$:

$$\phi_{t,n}^{\psi} : \mathcal{O}[\Gamma_n] \to \mathcal{O}/q_n\mathcal{O}$$

$$\gamma_n(a) \mapsto \psi(a)^{-1}\langle a\rangle^{-t} \pmod{q_n\mathcal{O}} \tag{3.8}$$

Since the following diagram is commutative for $m \geq n \geq n_0$,

$$\begin{tikzcd}
\mathcal{O}[\Gamma_m] \arrow[r] \arrow[d] & \mathcal{O}/q_m\mathcal{O} \arrow[d] \\
\mathcal{O}[\Gamma_n] \arrow[r] & \mathcal{O}/q_n\mathcal{O}
\end{tikzcd}$$

we have a continuous morphism of $\mathcal{O}$-algebras

$$\phi_t = \phi_t^{\psi} = \lim \phi_{t,n}^{\psi} : \mathcal{O}[[\Gamma]] \to \mathcal{O}$$

$$\gamma(a) \mapsto \psi(a)^{-1}\langle a\rangle^{-t}$$

In particular, $\phi_t(\gamma(1+q_0)) = \psi(1+q_0)^{-1}(1+q_0)^{-t} = \zeta_\psi(1+q_0)^{-t}$ where $\zeta_\psi = \psi(1+q_0)^{-1}$

is a root of unity in K of order a power of prime. As $\zeta_\psi \equiv (1+q_0) \equiv 1 \pmod{p}$, we have $\zeta_\psi(1+q_0)^{-t} \equiv 1 \pmod{\mathfrak{p}}$. Hence if $f(x) \in \mathcal{O}[[x]]$, then $f(\zeta_\psi(1+q_0)^{-t}-1)$ is well defined in $\mathcal{O}$.

Lemma 3.8. *Let $f(x) \mapsto \xi$ under the isomorphism in Lemma 3.7. Then $\phi_t^\psi(\xi) = f(\zeta_\psi(1+q_0)^{-t}-1)$.*

Proof. For $f(x) = 1+x$, $\xi = \gamma(1+q_0)$. Thus $\phi_t^\psi(\xi) = \phi_t^\psi(\gamma(1+q_0)) = \psi(1+q_0)^{-1}(1+q_0)^{-t} = \zeta_\psi(1+q_0)^{-t} = f(\zeta_\psi(1+q_0)^{-t}-1)$. This implies that the same formula works for any arbitrary $f(x) \in \mathcal{O}[x]$ and hence for $f(x) \in \mathcal{O}[[x]]$. □

Let θ be a Dirichlet character of the first kind with $\theta(-1) = 1$. Hence $f_\theta = d$ or $f_\theta = dq$. Fix a finite extension K_θ of $\mathbb{Q}_p$ containing all the values of $\theta(a), a \in \mathbb{Z}$. Let $\mathcal{O}_\theta$ be the ring local integers in K_θ. Define, for $n \geq 0$,

$$\begin{aligned}\xi_n = \xi_n^\theta &= -\frac{1}{2q_n}\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} \langle a\rangle\theta(a)\gamma_n(a)^{-1}\\ &= -\frac{1}{2q_n}\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} a\theta_1(a)\gamma_n(a)^{-1} \quad , \quad \theta_1 = \theta\omega^{-1}\end{aligned}$$

and let

$$\eta_n = \eta_n^\theta = (1-(1+q_0)\gamma_n(1+q_0)^{-1})\xi_n$$

Both $\xi_n, \eta_n \in K_\theta[\Gamma_n]$.

We now show that, under the morphism $K_\theta[\Gamma_{n+1}] \to K_\theta[\Gamma_n]$, $\xi_{n+1} \mapsto \xi_n$. Let ξ'_{n+1} be the image of ξ_{n+1} under the given morphism.

$$\xi'_{n+1} = -\frac{1}{2q_{n+1}}\sum_{\substack{b=0\\(b,q_0)=1}}^{q_{n+1}} b\theta_1(b)\gamma_n(b)^{-1}$$

We write $b = a + iq_n, 0 \leq a < q_n, (a,q_0) = 1, 0 \leq i < p$. Then $b \equiv a \pmod{q_n}$ implies $\gamma_n(b) = \gamma_n(a)$. Since f_θ and $f_\omega(=q)$ divide q_0, f_{θ_1} also divides q_0. Hence $b \equiv a \pmod{q_n}$ implies $\theta_1(b) = \theta_1(a)$. Therefore

$$\begin{aligned}\xi'_{n+1} &= -\frac{1}{2q_{n+1}}\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} \theta_1(a)\gamma_n(a)^{-1}\sum_{a=0}^{p-1}(a+iq_n)\\ &= \xi_n - \left(\frac{p-1}{4}\right)\sum_{\substack{a=0\\(a,q_o)=1}}^{q_n/2}(\theta_1(a)\gamma_n(a)^{-1} + \theta_1(q_n-a)\gamma_n(q_n-a)^{-1})\end{aligned}$$

However, $\theta_1(-1) = \theta(-1)\omega^{-1}(-1) = -1$. Thus $\theta_1(q_n - a) = \theta_1(-a) = -\theta_1(a)$ and $\gamma_n(q_n - a) = \gamma_n(-a) = \gamma_n(-1)\gamma_n(a) = \gamma_n(a)$. Therefore the sum in the above expression is 0. Hence $\xi'_{n+1} = \xi_n$. In general, for $m \geq n \geq 0$, $\xi_m \mapsto \xi_n$ and $\eta_m \mapsto \eta_n$ under $K_\theta[\Gamma_m] \to K_\theta[\Gamma_n]$.

We next show that η_n is in fact contained in $\mathcal{O}_\theta[\Gamma_n]$. As $\langle 1+q_0\rangle = 1+q_0$ and $\theta(1+q_0) = 1$,

$$\eta_n = \xi_n + \frac{1}{2q_n} \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} \langle(1+q_o)a\rangle\theta((1+q_o)a)\gamma_n((1+q_o)a)^{-1}$$

For each integer $a, 0 \leq a < q_n, (a, q_0) = 1$, define a' and a'' by $(1+q_0)a = a' + a''q_n$, $0 \leq a' < q_n$. Since $(1+q_0)a \equiv a' \pmod{q_n}$, $\omega((1+q_0)a) = \omega(a')$, $\theta((1+q_0)a) = \theta(a')$ and $\gamma_n((1+q_0)a) = \gamma_n(a')$. Thus $\langle(1+q_0)a\rangle = \omega((1+q_0)a)^{-1}(1+q_0)a = \omega(a')^{-1}(1+q_0)a = \omega(a')^{-1}(a'+a''q_n) = \langle a'\rangle + \omega(a')^{-1}a''q_n$. Furthermore, if a ranges through 0 to q_n such that $(a, q_0) = 1$, then so does a'. Hence

$$\eta_n = \xi_n + \frac{1}{2q_n} \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} (\langle a'\rangle + \omega(a')^{-1}a''q_n)\theta(a')\gamma_n(a')^{-1} = \frac{1}{2} \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} a''\theta_1(a')\gamma_n(a')^{-1} \quad (3.9)$$

Since $(1+q_0)(q_n - a) = q_n - a' + (q_0 - a'')q_n$, $\theta_1(q_n - a') = \theta_1(-a')$ and $\gamma_n(q_n - a') = \gamma_n(a')$, it follows that

$$\begin{aligned}\eta_n &= \frac{1}{2} \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n/2} (a''\theta_1(a')\gamma_n(a')^{-1} + (q_n - a'')\theta_1(q_n - a')\gamma_n(q_n - a')^{-1}) \\ &= \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n/2} (a'' - \frac{q_0}{2})(\theta_1(a')\gamma_n(a')^{-1})\end{aligned}$$

For $p \neq 2$, $(a'' - \frac{q_0}{2}) \in \mathbb{Z}_p$, hence $\eta_n \in \mathcal{O}_\theta[\Gamma_n]$ and for $p = 2$, q_0 is even. This shows that $\eta_n \in \mathcal{O}_\theta[\Gamma_n]$.

Now, since $\eta_m \mapsto \eta_n$ under $\mathcal{O}_\theta[\Gamma_m] \to \mathcal{O}_\theta[\Gamma_n]$, $m \geq n \geq 0$, let

$$\eta_\infty = \eta_\infty^\theta = \varprojlim \eta_n \qquad , \qquad \eta_\infty \in \mathcal{O}_\theta[[\Gamma]]$$

and

$$g(x,\theta) \mapsto \eta_\infty \qquad , \qquad g(x,\theta) \in \mathcal{O}_\theta[[x]]$$

under the isomorphism $\mathcal{O}_\theta[\Gamma] \cong \mathcal{O}_\theta[x]$ mentioned in Lemma 3.7.

We now assume $\theta \neq \chi^0$. In this case we will prove that ξ_n is also contained in $\mathcal{O}_\theta[\Gamma_n]$. Since $\langle q_n - a\rangle = (q_n - a)\omega(q_n - a)^{-1} = (q_n - a)(-\omega(a)^{-1}) = \langle a\rangle - \omega(a)^{-1}q_n$ and $\theta(q_n - a) =$

$\theta(a)$. We have

$$\begin{aligned}\xi_n &= -\frac{1}{2q_n}\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n/2}(\langle a\rangle\theta(a)\gamma_n(a)^{-1}+\langle q_n-a\rangle\theta(q_n-a)\gamma_n(q_n-a)^{-1})\\ &= -\frac{1}{q_n}\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n/2}\langle a\rangle\theta(a)\gamma_n(a)^{-1}+\frac{1}{2}\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n/2}\theta_1(a)\gamma_n(a)^{-1}\end{aligned}$$

Fix an integer $a_0, (a_0, q_0) = 1$, and denote by $\sum'$ the sum taken over all integers a such that $0 \le a < q_n/2, (a, q_0) = 1, \gamma_n(a) = \gamma_n(a_0)$. Since $\langle a\rangle = \langle a_0\rangle \pmod{q_n}$ for such integers a, we have $\sum'\langle a\rangle\theta(a)\gamma_n(a)^{-1} \equiv \Big(\sum'\theta(a)\Big)\langle a_0\rangle\gamma_n(a_0)^{-1} \pmod{q_n\mathcal{O}_\theta[\Gamma_n]}$. However, we see from $G_n = \Delta_n \times \Gamma_n$ that when a takes the values as mentioned above, the elements $\delta_n(a)$ and $\delta_n(q_n - a)$ precisely fill out the group Δ_n. Since θ is essentially a non-principal character of the group Δ_n, it follows that $\sum'\theta(a) = \frac{1}{2}\Big(\sum'\theta(a) + \theta(q_n - a)\Big) = 0$. Therefore $\sum'\langle a\rangle\theta(a)\gamma_n(a)^{-1} \equiv 0 \pmod{q_n\mathcal{O}_\theta[\Gamma_n]}$. and hence

$$\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n/2}\langle a\rangle\theta(a)\gamma_n(a)^{-1}\equiv 0 \pmod{q_n\mathcal{O}_\theta[\Gamma_n]}$$

This shows that $\xi_n \in \mathcal{O}_\theta[\Gamma_n]$ for $p > 2$. For $p = 2$, $\theta_1(a) = \omega(a)^{-1}\theta(a) = \pm\theta(a) \equiv \theta(a) \pmod{2\mathcal{O}}$. Therefore, $\sum'\theta_1(a) \equiv \sum'\theta(a) \equiv 0 \pmod{2\mathcal{O}}$. Thus,

$$\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n/2}\theta_1(a)\gamma_n(a)^{-1}\equiv 0 \pmod{2\mathcal{O}_\theta[\Gamma_n]}$$

which implies that ξ_n is contained in $\mathcal{O}_\theta[\Gamma_n]$ for $p = 2$.

Now, since $\xi_m \mapsto \xi_n$ under $\mathcal{O}_\theta[\Gamma_m] \to \mathcal{O}_\theta[\Gamma_n]$, $m \ge n \ge 0$, let

$$\xi_\infty = \xi_\infty^\theta = \varprojlim \xi_n \qquad , \qquad \xi_\infty \in \mathcal{O}_\theta[[\Gamma]]$$

and

$$f(x,\theta) \mapsto \xi_\infty \qquad , \qquad f(x,\theta) \in \mathcal{O}_\theta[[x]]$$

under the isomorphism $\mathcal{O}_\theta[\Gamma] \cong \mathcal{O}_\theta[x]$ mentioned in Lemma 3.7.

Now,

$$\varprojlim(1-(1+q_0)\gamma_n(1+q_0)^{-1}) = (1-(1+q_0)\gamma(1+q_0)^{-1})$$

implies

$$\eta_\infty = (1-(1+q_0)\gamma(1+q_0)^{-1})\xi_\infty$$

Let $h(x,\theta) = 1-\frac{1+q_0}{1+x} = 1-(1+q_0)\sum_{n=0}^\infty (-x)^n$. Then $h(x,\theta) \mapsto (1-(1+q_0)\gamma(1+q_0)^{-1})$ under the isomorphism $\mathcal{O}_\theta[\Gamma] \cong \mathcal{O}_\theta[x]$. Hence

$$g(x,\theta) = h(x,\theta)f(x,\theta)$$

If $\theta = \chi^0$ then $d=1, q_0=q, K_\theta = \mathbb{Q}_p$ and $g(x,\theta) = g(x,\chi^0) \in \mathbb{Z}_p[[x]]$. Let $h(x,\chi^0) = 1-\frac{1+q}{1+x}$. We define $f(x,\chi^0) = g(x,\chi^0)h(x,\chi_o)^{-1}$. We shall see in the next section that $f(x,\chi^0)$ is not contained in $\mathbb{Z}_p[[x]]$.

3.2.2 Construction of the p-adic L-function

Let χ be an even Dirichlet character and $\chi = \theta\psi$ be the decomposition of χ into the product of the character of the first kind and the character of the second kind. Let $f_\theta = d$ or $f_\theta = dq$, $q_n = dqp^n$ and $\zeta = \chi(1+q_0)^{-1} = \psi(1+q_0)^{-1}$ as defined in the earlier section. Since $\langle -1\rangle = 1, \psi(-1) = 1$, we have $\theta(-1) = \chi(-1) = 1$. Hence $f(x,\theta)$ can be defined as mentioned in 3.2.1.

Lemma 3.9.

$$2f(\zeta(1+q_0)^{1-n}-1,\theta) = -(1-\chi_n(p)p^{n-1})\frac{B_{n,\chi_n}}{n} \qquad (\chi_n = \chi\omega^{-n})$$

for every integer $n \geq 1$.

Proof. We fix a finite extension K of $\mathbb{Q}_p$ containing all the values of $\chi(a), \theta(a), \psi(a), a \in \mathbb{Z}$. From 3.9, we have

$$2\eta_n = 2\eta_n^\theta = \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} a''\theta_1(a')\gamma_n(a')^{-1}$$

As $\eta_n \in \mathcal{O}[\Gamma_n]$, we apply the morphism $\phi_{t,n}^\psi = \phi_{t,n}$ (see 3.8) to the both sides,

$$\begin{aligned} 2\phi_{t,n}(\eta_n) &\equiv \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} a''\theta_1(a')\psi(a')\langle a'\rangle^t \pmod{q_n\mathcal{O}} \\ &\equiv \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} a''\chi_1(a')\langle a'\rangle^t \pmod{q_n\mathcal{O}} \\ &\equiv \sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} a''\chi_{t+1}(a')(a')^t \pmod{q_n\mathcal{O}} \end{aligned}$$

where $\chi_1 = \chi\omega^{-1}, \chi_{t+1} = \chi\omega^{-(t+1)}$. Now $(1+q_0)a = a' + a''q_n$ implies $(1+q_0)^{t+1}a^{t+1} \equiv (a')^{t+1} + (t+1)(a')^t a'' q_n \pmod{q_n^2}$. If n is large enough such that $f_\chi | q_n$, then $\chi_{t+1}(a') = \chi_{t+1}((1+q_0)a) = \chi_{t+1}(1+q_0)\chi_{t+1}(a)$. Hence it follows from the above congruence that

$$\begin{aligned}
&\chi_{t+1}(1+q_0)(1+q_0)^{t+1} \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \chi_{t+1}(a)a^{t+1} \\
&= \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \chi_{t+1}(1+q_0)\chi_{t+1}(a)(1+q_0)^{t+1}a^{t+1} \\
&\equiv \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \chi_{t+1}(a')(a')^{t+1} + (t+1) \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \chi_{t+1}(a')(a')^t a'' q_n \pmod{q_n^2\mathcal{O}}
\end{aligned}$$

Therefore,

$$2(t+1)\phi_{t,n}(\eta_n) \equiv -(1-\chi(1+q_0)(1+q_0))\frac{1}{q_n} \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \chi_{t+1}(a)a^{t+1} \pmod{q_n\mathcal{O}}$$

Hence by taking limit on both sides,

$$2(t+1)\phi_t(\eta_\infty) \equiv -(1-\zeta^{-1}(1+q_0)) \lim_{n\to\infty} \frac{1}{q_n} \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \chi_{t+1}(a)a^{t+1}$$

As $g(x,\theta) \mapsto \eta_\infty^\theta$ under $\mathcal{O}[[x]] \cong \mathcal{O}[[\Gamma]]$, it follows from Lemma 3.8 that $\phi_t(\eta_\infty) = g(\zeta(1+q_0)^{-t}-1,\theta)$. On the other hand, $h(\zeta(1+q_0)^{-t}-1,\theta) = 1-\zeta^{-1}(1+q_0)^{t+1} \neq 0$ for $t \geq 0$. Hence it follows form the above that

$$2f(\zeta(1+q_0)^{-t}-1,\theta) = -\frac{1}{t+1} \lim_{n\to\infty} \frac{1}{q_n} \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \chi_{t+1}(a)a^{t+1}$$

Now suppose $(a,p) = 1$ but $(a,q_0) > 1$. Since $f_{\chi_{t+1}} = dp^e$ for some $e \geq 0$, $(a, f_{\chi_{t+1}}) > 1$ and thus $\chi_{t+1}(a) = 0$.

Hence

$$\begin{aligned}\sum_{\substack{a=0\\(a,q_0)=1}}^{q_n} \chi_{t+1}(a)a^{t+1} &= \sum_{\substack{a=0\\(a,p)=1}}^{q_n} \chi_{t+1}(a)a^{t+1}\\ &= \sum_{a=0}^{q_n} \chi_{t+1}(a)a^{t+1} - \sum_{\substack{a=0\\p\mid a}}^{q_n} \chi_{t+1}(a)a^{t+1}\\ &= \sum_{a=0}^{q_n} \chi_{t+1}(a)a^{t+1} - \chi_{t+1}(p)p^{t+1}\sum_{a=0}^{q_{n-1}} \chi_{t+1}(a)a^{t+1}\\ &= s_{t+1,\chi_{t+1}}(q_n) - \chi_{t+1}(p)p^{t+1}s_{t+1,\chi_{t+1}}(q_{n-1})\end{aligned}$$

where $s_{n,\chi}(k)$ is defined in 3.1.1. Since $q_n = dqp^n = f_{\chi_{t+1}}p^{h_n}$, $h_n = n+1-e$ or $n+2-e$. So from Lemma 3.1 we have,

$$\lim_{n\to\infty} \frac{s_{t+1,\chi_{t+1}}(q_n)}{q_n} = B_{t+1,\chi_{t+1}}$$

Therefore,

$$2f(\zeta(1+q_0)^{-t}-1,\theta) = -\frac{1}{t+1}(1-\chi_{t+1}(p)p^t)B_{t+1,\chi_{t+1}}$$

Putting $n = t+1 \geq 1$, we obtain the formula in the lemma. □

Now let us consider the special case where $\chi = \theta = \psi = \chi^0$ and $n = 1$. Since $\zeta = \chi(1+q_0)^{-1} = 1$, $\chi_1(p) = \omega^{-1}(p) = 0$, it follows from Lemma 3.9 that

$$f(0,\chi^0) = -\frac{1}{2}B_{1,\omega^{-1}} = -\frac{1}{2q}\sum_{a=1}^{q}\omega^{-1}(a)a$$

(see property 6 of generalized Bernoulli numbers). If $(a,p)=1$ then $\omega^{-1}(a)a \equiv 1 \pmod{q\mathbb{Z}_p}$. Therefore

$$\begin{aligned}\sum_{a=1}^{q}\omega^{-1}(a)a &\equiv p-1 \pmod{p\mathbb{Z}_p}, \qquad (p>2)\\ &\equiv 2 \pmod{4\mathbb{Z}_2}, \qquad (p=2)\end{aligned}$$

Hence $|f(0,\chi^0)| = |\frac{1}{q}| > 1$. Thus $f(x,\chi^0) \notin \mathbb{Z}_p[[x]]$. However, since $h(0,\chi^0) = -q$, we see that $g(0,\chi^0)$ is a p-adic unit and thus $g(x,\chi^0)$ is invertible in $\mathbb{Z}_p[[x]]$.

Still in the special case, the argument in the first part of the proof of Lemma 3.9 shows that

$$2\phi_{-1,n}(\eta_n) \equiv \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} (a')^{-1}a'' \pmod{q_n\mathcal{O}}$$

Now $(1+q_0)a = a' + a''q_n$ implies $(1+q_0)\langle a\rangle = \langle a'\rangle(1+(a')^{-1}a''q_n)$ so that $\log(1+q_0) + \log\langle a\rangle = \log\langle a'\rangle + \log(1+(a')^{-1}a''q_n)$. Hence taking the sum over all integers a such that $0 \le a < q_n, (a,q_0) = 1$, we obtain

$$\begin{aligned}\Big(1-\frac{1}{p}\Big)q_n\log(1+q_0) &= \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} \log(1+(a')^{-1}a''q_n) \\ &\equiv \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} (a')^{-1}a''q_n \pmod{q_np^{n+1}\mathbb{Z}_p}\end{aligned}$$

Hence

$$\Big(1-\frac{1}{p}\Big)\log(1+q_0) \equiv \sum_{\substack{a=0 \\ (a,q_0)=1}}^{q_n} (a')^{-1}a'' \pmod{p^{n+1}\mathbb{Z}_p}$$

Therefore

$$2g(q_0,\chi^0) = 2g(1+q_0-1,\chi^0) = \varprojlim(2\phi_{-1,n}(\eta_n)) = \Big(1-\frac{1}{p}\Big)\log(1+q_0) \tag{3.10}$$

Now consider a power series $u(s-1)$ in $K[[s-1]]$ given by

$$u(s-1) = \zeta(1+q_0)\sum_{n=1}^{\infty}\frac{(\log(1+q_0))^n}{n!}(s-1)^n$$

Since q_0 is divisible by q and $|\log(1+q_0)| \le |q|$, we have, by Lemma 3.5,

$$\Big|\zeta(1+q_0)\frac{(\log(1+q_0))^n}{n!}\Big| \le |q|^n|p|^{-\frac{n}{p-1}} = r^{-n}$$

with $r = |q|^{-1}|p|^{\frac{1}{p-1}} > 1$. Hence $u(s-1)$ converges in the domain $\mathfrak{D} = \{s|s \in \overline{\mathbb{Q}}_p, |s-1| < r\}$ and $|u(s-1)| < 1$ for $s \in \mathfrak{D}$.

Let $c = \zeta(1+q_0) - 1$, then c is contained in the maximal ideal $\mathfrak{p}$ of the ring $\mathcal{O}$ of local integers in K. Let $A(x) = \sum_{n=0}^{\infty} a_nx^n$ be any power series in $\mathcal{O}[[x]]$. Since $(c+x)$ is contained in the maximal ideal $\mathfrak{m}$ of $\mathcal{O}[[x]]$, $\sum_{n=0}^{\infty} a_n(c+x)^n$ exists and let $B(x) = \sum_{n=0}^{\infty} a_n(c+x)^n$. For each $\alpha \in \overline{\mathbb{Q}}_p, |\alpha| < 1$, we then have $A(c+\alpha) = B(\alpha)$. Let $B(x) = \sum_{n=0}^{\infty} b_nx^n$. Since $u(s-1)$ is a power series in $(s-1)$ without the constant term, we obtain by a formal computation that

$$\sum_{n=0}^{\infty} b_n u(s-1)^n = \sum_{n=0}^{\infty} c_n (s-1)^n$$

It is easy to see that $|c_n| \leq r^{-n}$ because $b_n \leq 1$ for $n \geq 0$, and the coefficients of $u(s-1)$ satisfy the same condition as above. Therefore the power series $\sum_{n=0}^{\infty} c_n(s-1)^n$ converges in the domain $\mathfrak{D}$ and

$$A(c+u(s-1)) = B(u(s-1)) = \sum_{n=0}^{\infty} c_n (s-1)^n$$

for every $s \in \mathfrak{D}$. Note that $|u(s-1)| < 1$ and $|c+u(s-1)| < 1$, so that $A(c+u(s-1))$ and $B(u(s-1))$ are well-defined in $\mathfrak{D}$.

If s is an integer, $s = t \in \mathbb{Z}$. then $c + u(t-1) = c + \zeta(1+q_0)(e^{(t-1)\log(1+q_0)} - 1) = \zeta(1+q_0)^t - 1$. Hence, by continuity, we have $c + u(s-1) = \zeta(1+q_0)^s - 1$ for every $s \in \mathbb{Z}_p$ where $(1+q_0)^s := \langle 1+q_0 \rangle^s = (1 + \langle 1+q_0 \rangle - 1)^s = \sum_{n=0}^{\infty} \binom{s}{n} (\langle 1+q_0 \rangle - 1)^n$ which converges in $\mathbb{Z}_p$, $(s \in \mathbb{Z}_p)$ (see Chapter 5 of [3] for more details). Thus we have

$$A(\zeta(1+q_0)^s - 1) = \sum_{n=0}^{\infty} c_n (s-1)^n \qquad |c_n| \leq r^{-n}$$

for every $s \in \mathfrak{D}$.

We now assume that the first factor of χ is non-principal that is $\theta \neq \chi^0$. In this case, $f(x, \theta)$, defined in 3.2.1, is a power series in $\mathcal{O}[[x]]$. Hence, by the above remark, the function $F(s, \chi) = 2f(\zeta(1+q_0)^s - 1, \theta)$ is defined in the domain $\mathfrak{D}$ and is given by a power series:

$$F(s, \chi) = \sum_{n=0}^{\infty} a_{n,\chi} (s-1)^n \qquad |a_{n,\chi}| \leq r^{-n}$$

Assume next that $\theta = \chi^0, \chi = \psi$. Since $g(x, \chi^0)$ is a power series in $\mathcal{O}[[x]]$, the function $G(s, \chi) = 2g(\zeta(1+q_0)^s - 1, \chi^0)$ is again defined in $\mathfrak{D}$ and is given by a power series similar to that for $F(s, \chi)$. On the other hand,

$$\begin{aligned} h(\zeta(1+q_0)^s - 1, \chi^0) = h(c+u(s-1), \chi^0) &= 1 - \frac{1+q_0}{1+c+u(s-1)} \\ &= 1 - \zeta^{-1} \Big(\sum_{n=0}^{\infty} \frac{(\log(1+q_0))^n}{n!} (s-1)^n \Big)^{-1} \\ &= 1 - \zeta^{-1} \sum_{n=0}^{\infty} \frac{(\log(1+q_0))^n}{n!} (1-s)^n \end{aligned}$$

Suppose $\chi \neq \psi \neq \chi^0$, then $\zeta \neq 1$ and

$$h(\zeta(1+q_0)^s - 1, \chi^0) = (1-\zeta^{-1})\Big(1 + \frac{1}{1-\zeta}\sum_{n=1}^{\infty}\frac{(\log(1+q_0))^n}{n!}(1-s)^n\Big)$$

Since ζ is a root of unity with order a power of p, $|1-\zeta| \geq |p|^{\frac{1}{p-1}}$. Hence by the remark in the proof of Lemma 3.5,

$$\Big|\frac{1}{1-\zeta}\frac{(\log(1+q_0))^n}{n!}\Big| \leq |p|^{-\frac{1}{p-1}}|q|^n|p|^{-\frac{n-1}{p-1}} = r^{-n}$$

It implies that $h(\zeta(1+q_0)^s - 1, \chi^0) \neq 0$ for every $s \in \mathfrak{D}$ and

$$F(s,\chi) = 2f(\zeta(1+q_0)^s - 1, \chi^0) = \frac{2g(\zeta(1+q_0)^s - 1, \chi^0)}{h(\zeta(1+q_0)^s - 1, \chi^0)}$$

is defined in $\mathfrak{D}$ and is given by a power series in $K[[x]]$:

$$F(s,\chi) = \sum_{n=0}^{\infty} a_{n,\chi}(s-1)^n \qquad |a_{n,\chi}| \leq |1-\zeta|^{-1}r^{-n}$$

Finally let $\chi = \theta\psi = \chi^0$. In this case, $\zeta = 1$ and

$$h(\zeta(1+q_0)^s - 1, \chi^0) = \log(1+q_0)(s-1)\sum_{n=0}^{\infty}\frac{(\log(1+q_0))^n}{n!}(1-s)^n$$

where the power series converges because of the same reason as mentioned above. Therefore $h(\zeta(1+q_0)^s - 1, \chi^0)$ vanishes in $\mathfrak{D}$ only at $s = 1$ and the function $F(s,\chi^0) = 2f(\zeta(1+q_0)^s - 1, \chi^0)$ given by the following power series

$$F(s,\chi^0) = \frac{a_{-1}}{s-1} + \sum_{n=0}^{\infty} a_n(s-1)^n \qquad |a_n| \leq |1-\zeta|^{-1}r^{-n}$$

is now defined for all $s \neq 1$ in $\mathfrak{D}$. We also see that, 3.10 implies,

$$a_{-1} = \lim_{s\to 1}(s-1)F(s,\chi^0) = \frac{(1-\frac{1}{p})\log(1+q_0)}{\log(1+q_0)} = 1 - \frac{1}{p}$$

Thus, we have now obtained a function $F(s,\chi)$ for each Dirichlet character $\chi, \chi(-1) = 1$ defined in the domain $\mathfrak{D}$ excluding $s = 1$ in the case of $\chi = \chi^0$. By Lemma 3.9, it also satisfies

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

for every integer $n \geq 1$. Hence $F(s, \chi)$ possesses both the properties of Theorem 3.2 which uniquely characterize the p-adic L-function. Therefore $F(s, \chi) = L_p(s, \chi)$. Note that n and χ_n have different parities if $\chi(-1) = -1$. This implies $B_{n,\chi_n} = 0$ (property 5 of generalized Bernoulli numbers) which in turn implies $L_p(1-n, \chi) = 0$ for $n \geq 1$. Hence, by p-adic Weierstrass Preparation Theorem, $L_p(s, \chi)$ is identically 0 for odd χ.

We see that $L_p(s, \chi)$ is constructed by a method different from that in section 3.1. The formula

$$L_p(s, \chi) = 2f(\zeta(1+q_0)^s - 1, \theta) \tag{3.11}$$

is a very useful result and has many applications to the theory of cyclotomic fields, following theorem being one of them:

Theorem 3.9. *Let $h_n^- = \frac{h(\mathbb{Q}(\zeta_{p^{n+1}}))}{h(\mathbb{Q}(\zeta_{p^{n+1}})^+)}$ and $p^{e_n^-}$ be the exact power of p dividing h_n^-. There exists integers λ, μ and ν, all independent of n, with $\lambda \geq 0, \mu \geq 0$, such that*

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

for all n sufficiently large.

Proof. See first three sections of Chapter 7, [3]. □

The above theorem is a part of much more general theory of Iwasawa, theory of $\mathbb{Z}_p$-extensions, which we will consider in the next chapter.

Chapter 4

The Main Conjecture

We discuss Iwasawa's theory of $\mathbb{Z}_p$-extensions and the Main Conjecture of Iwasawa theory in the present chapter. The account given here is based on the book by Lawrence C. Washington [13] and on the notes by Romyar Sharifi [12]. Throughout the chapter, we assume $p > 2$ for simplicity.
Notation: Our notation is slightly different than the standard one. We denote the power series ring by $\mathbb{Z}_p[[x]]$ instead of $\mathbb{Z}_p[[T]]$ and the projective limit of ideal class groups by Y instead of X.

4.1 Iwasawa's theorem

The main goal of this section is to prove Iwasawa's theorem which is concerned with the study of sizes of class groups in $\mathbb{Z}_p$-extensions. Let $\Lambda = \mathbb{Z}_p[[x]]$. We first state some results about the structure of Λ and Λ-modules that are needed to prove the theorem. For the proofs of these results, see section 13.2, [13].

Theorem 4.1 (p-adic Weierstrass Preparation Theorem)**.** *Let $f(x) \in \Lambda$ be nonzero. Then f can be uniquely written as $f(x) = p^{\mu}P(x)U(x)$ where $P(x)$ is a distinguished polynomial, $U(x) \in \Lambda^{\times}$ and μ is a nonegative integer.*

Lemma 4.1. *Λ is a UFD whose irreducible elements are p and the irreducible distinguished polynomials.*

Lemma 4.2. *Suppose $f, g \in \Lambda$ are relatively prime. Then the ideal (f, g) is of finite index in Λ.*

Lemma 4.3. *The prime ideals of Λ are $0, (p, x), (p)$ and the ideals $(P(x))$ where $P(x)$ is an irreducible distinguished polynomial. The ideal (p, x) is the unique maximal ideal.*

Lemma 4.4. *Let $f \in \Lambda$ with $f \notin \Lambda^{\times}$. Then $\Lambda/(f)$ is infinite.*

Theorem 4.2. *(Structure Theorem for Λ-modules) Let M be a finitely generated Λ-module. Then*

$$M \sim \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(x)^{m_j})\Big)$$

where $r, s, t, n_i, m_j \in \mathbb{Z}$ and f_j is irreducible distinguished.

Now let K be a number field and K_∞/K be a $\mathbb{Z}_p$-extension such that $K = K_0 \subset K_1 \ldots \subset K_\infty$ with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ and $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Iwasawa's theorem says that

Theorem 4.3 (Iwasawa's Theorem)**.** *Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exists 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. Only finitely many primes in K (those above p) ramify in K_∞ (Proposition 13.2, [13]). We first assume that these primes are totally ramified in K_∞/K.

Let L_n be the maximal unramified abelian p-extension of K_n and A_n be the p-part of the ideal class group of K_n. Set $Y_n = \mathrm{Gal}(L_n/K_n)$. Note that, from class field theory, $p^{e_n} = |A_n| = |Y_n|$. Let $L = \bigcup_{n\geq 0} L_n$ and $Y = \mathrm{Gal}(L/K_\infty)$. Since K_n/K is Galois, the maximality of L_n over K_n implies L_n/K is Galois and hence L/K is Galois. Let $G = \mathrm{Gal}(L/K)$. Since K_{n+1}/K_n is totally ramified and L_n/K_n is unramified, $K_{n+1} \cap L_n = K_n$. Therefore $Y_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_{n+1}/K_{n+1})$. As $L_nK_{n+1} \subset L_{n+1}$, we see that Y_n is a quotient of Y_{n+1}. Thus we have an onto map $Y_{n+1} \to Y_n$. Similarly we have $Y_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$ and so we have

$$\begin{aligned}
\varprojlim Y_n &= \varprojlim \mathrm{Gal}(L_n/K_n) \\
&\cong \varprojlim \mathrm{Gal}(L_nK_\infty/K_\infty) \\
&= \mathrm{Gal}((\bigcup L_nK_\infty)/K_\infty) \\
&= \mathrm{Gal}(L/K_\infty) = Y
\end{aligned}$$

Let $\gamma_n \in \Gamma_n$. We extend γ_n to an element $\tilde{\gamma_n} \in \mathrm{Gal}(L_n/K)$. Let $y_n \in Y_n$. There is an action of γ_n on y_n given by $y_n^{\gamma_n} = \tilde{\gamma_n} y_n \tilde{\gamma_n}^{-1}$. This action is well-defined since Y_n is abelian. This implies that Y_n is a $\mathbb{Z}_p[\Gamma_n]$-module (It has a $\mathbb{Z}_p$-action because it is a p-group!). Representing an element of Y as a vector $(y_0, y_1, \ldots\ldots)$ and letting $\mathbb{Z}_p[\Gamma_n]$ act on the n-th component, we find that Y becomes a module over $\Lambda \cong \mathbb{Z}_p[[\Gamma]]$. As before, $\gamma \in \Gamma, y \in Y$ then $y^\gamma = \tilde{\gamma} y \tilde{\gamma}^{-1}$ where $\tilde{\gamma}$ is an extension of γ to G.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the primes in K that ramify in K_∞. Fix a prime $\tilde{\mathfrak{p}_i}$ of L lying over $\mathfrak{p}_i$. Let $I_i = I(\tilde{\mathfrak{p}_i}/\mathfrak{p}_i) \subset G$ be the inertia group. Since L/K_∞ is unramified, $I_i \cap Y = \{e\}$. Thus we have an injective map $I_i \hookrightarrow G/Y \cong \Gamma$. Now our assumption that K_∞/K is totally ramified at $\mathfrak{p}_i$ implies that this map is in fact surjective and thus bijective. Therefore $G = I_iY = YI_i$ for $i = 1, 2, \ldots, s$. Let $\sigma_i \in I_i$ be an element that maps to the topological generator γ_0 in Γ. Now $I_i \subset YI_1$ for $i = 1, 2, \ldots, s$, so there exists $a_i \in Y$ such that $\sigma_i = a_i\sigma_1$ for $i = 1, 2, \ldots, s$.

Lemma 4.5. $[G, G] = Y^{\gamma_0 - 1} = xY$

Proof. Let $a, b \in G$. Using $G = \Gamma Y$, we write $a = \gamma_1 y_1$ and $b = \gamma_2 y_2$. We identify Γ with I_1 and define the action of Γ on Y via this identification, i.e. $y^\gamma = \gamma y \gamma^{-1}$. Therefore

$$\begin{aligned}
aba^{-1}b^{-1} &= \gamma_1 y_1 \gamma_2 y_2 y_1^{-1} \gamma_1^{-1} y_2^{-1} \gamma_2^{-1} \\
&= (y_1^{\gamma_1})\gamma_1\gamma_2 y_2 y_1^{-1}\gamma_1^{-1} y_2^{-1}\gamma_2^{-1} \\
&= (y_1^{\gamma_1})((y_2 y_1^{-1})^{\gamma_1\gamma_2})\gamma_1\gamma_2\gamma_1^{-1} y_2^{-1}\gamma_2^{-1} \\
&= (y_1^{\gamma_1})((y_2 y_1^{-1})^{\gamma_1\gamma_2})\gamma_2 y_2^{-1}\gamma_2^{-1} \quad (\Gamma \text{ is abelian}) \\
&= (y_1^{\gamma_1})((y_2 y_1^{-1})^{\gamma_1\gamma_2})(y_2^{-1})^{\gamma_2} \\
&= (y_1^{\gamma_1})^{1-\gamma_2}(y_2^{\gamma_2})^{\gamma_1 - 1}
\end{aligned}$$

Taking $\gamma_1 = \gamma_0, \gamma_2 = 1$, we see that $Y^{\gamma_0 - 1} \subseteq [G, G]$. For γ_2 arbitrary, there exists $c \in \mathbb{Z}_p$ such that $\gamma_2 = \gamma_0^c$. so

$$1 - \gamma_2 = 1 - \gamma_0^c = 1 - (1 + x)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} x^n \in x\Lambda$$

Thus $(y_1^{\gamma_1})^{1-\gamma_2} \in xY = Y^{\gamma_0 - 1}$. Similarly $(y_2^{\gamma_2})^{\gamma_1 - 1} \in Y^{\gamma_0 - 1}$. Therefore $[G, G] \subseteq Y^{\gamma_0 - 1}$. □

Note that, as xY is closed (continuous image of the compact set Y), $[G, G]$ is also closed. Therefore the closure G' of the commutator subgroup of $G = xY = Y^{\gamma_0 - 1}$.

Lemma 4.6. *Let M_0 be the $\mathbb{Z}_p$-submodule of Y generated by $\{a_i | 2 \le i \le s\}$ and by $Y^{\gamma_0 - 1} = xY$. Let $M_n = \nu_n M_0$, where $\nu_n = 1 + \gamma_0 + \gamma_0^2 \ldots + \gamma_0^{p^n - 1} = \frac{(1+x)^{p^n} - 1}{x}$. Then $Y_n \cong Y/M_n$ for $n \ge 0$.*

Proof. First, consider $n = 0$. We have $K_0 = K \subseteq L_0 \subseteq L$. Since L_0/K is maximal abelian unramified p-extension and L/K is a p-extension, L_0/K is the maximal unramified abelian subextension of L/K. Therefore $\mathrm{Gal}(L/L_0)$ must be the closed subgroup of G generated by G' and all the inertia subgroups I_i, $1 \le i \le s$. Therefore $\mathrm{Gal}(L/L_0)$ is the closure of the group generated by $Y^{\gamma_0 - 1}, I_1$ and $a_2, \ldots, a_s$, so

$$Y_0 = \mathrm{Gal}(L_0/K) = G/\mathrm{Gal}(L/L_0) = YI_1/\mathrm{Gal}(L/L_0) \cong Y/\overline{\langle Y^{\gamma_0-1}, a_2, \ldots, a_s \rangle} = Y/M_0$$

Now for $n \geq 1$, we replace K by K_n, γ_0 by $\gamma_0^{p^n}$. Then σ_i becomes $\sigma_i^{p^n}$. But $\sigma_i^{k+1} = (a_i\sigma_1)^{k+1} = a_i\sigma_1 a_i \sigma_1^{-1}\sigma_1^2 \ldots a_i \sigma_1^{-k}\sigma_1^{k+1} = a_i^{1+\sigma_1+\ldots+\sigma_1^k}\sigma_1^{k+1}$. Therefore $\sigma_i^{p^n} = (\nu_n a_i)\sigma_1^{p^n}$, so a_i is replaced by $\nu_n a_i$. Finally, Y^{γ_0-1} is replaced by $Y^{\gamma_0^{p^n}-1} = \nu_n Y^{\gamma_0-1}$. Therefore M_0 becomes $\nu_n M_0 = M_n$, which yields the desired result. □

Lemma 4.7 (Nakayama's Lemma). *Let Y be a compact Λ-module. If $y_1, \ldots, y_n$ generate $Y/(p,x)Y$ over $\mathbb{Z}$, then they also generate Y as a Λ-module. In particular $Y/(p,x)Y = 0 \iff Y = 0$.*

Proof. Let U be a small neighbourhood of 0 in Y. Since (p,x) is a maximal ideal of Λ, $(p,x)^n \to 0$ in Λ. So each $y \in Y$ has a neighbourhood U_y such that $(p,x)^n U_y \subseteq U$ for large n. Since Y is compact, finitely many U_y's cover Y. Therefore $(p,x)^n Y \subseteq U$ for large n, so $\bigcap (p,x)^n Y = 0$ for any compact module Y.

Let $Y' = \Lambda y_1 + \ldots + \Lambda y_n \subseteq Y$. Then Y' is compact (image of Λ^n), so Y/Y' is a compact Λ-module. By assumption, $Y' + (p,x)Y = Y$. Therefore $Y/Y' = (Y' + (p,x)Y)/Y' = (p,x)Y/Y'$. Hence $(p,x)^n(Y/Y') = Y/Y'$ for all $n \geq 0$. It follows that $\bigcap (p,x)^n(Y/Y') = Y/Y' = 0$ since Y/Y' is compact, so $Y = Y'$. □

Lemma 4.8. *$Y = \mathrm{Gal}(L/K_\infty)$ is a finitely generated Λ-module.*

Proof. $\nu_1 = \frac{(1+x)^p - 1}{x} \in (p,x)$, so $M_0/(p,x)M_0$ is a quotient of $M_0/\nu_1 M_0 = M_0/M_1 \subseteq Y/M_1 = Y_1$, which is finite. Therefore M_0 is finitely generated by Lemma 4.7. Since $Y/M_0 = Y_0$ is finite, Y must also be finitely generated. □

Since there exists an integer $e \geq 0$ such that in K_∞/K_e all ramified primes are totally ramified (Lemma 13.3, [13]), we remove our first assumption. Then Lemmas 4.6 and 4.8 apply to K_∞/K_e. In particular, Y, which is the same K_e and K, is a finitely generated Λ-module. For $n \geq e, \nu_{n,e} := \frac{\nu_n}{\nu_e} = 1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \ldots + \gamma_0^{p^n - p^e}$ replaces ν_n for K_∞/K_e, since $\gamma_0^{p^e}$ generates $\mathrm{Gal}(K_\infty/K_e)$. Let M_e be "M_0 for K_e". Then $M_n = \nu_{n,e}M_e$ and $Y_n \cong Y/M_n$ for all $n \geq e$.

We now apply Theorem 4.2 to Y. We can also apply it to M_e with the same answer, since Y/M_e is finite. So we have

$$M_e \sim Y \sim \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(x)^{m_j})\Big)$$

We shall calculate $|V/\nu_{n,e}V|$ for each of the summands V on the right side.

1. $V = \Lambda$. So $V/\nu_{n,e}V = \Lambda/(\nu_{n,e})$. Since $\nu_{n,e} = \frac{((1+x)^{p^n}-1)}{((1+x)^{p^e}-1)} \in (p, x)$ for $n \geq e$, $\nu_{n,e} \notin \Lambda^\times$. Hence by Lemma 4.4, $\Lambda/(\nu_{n,e})$ is infinite. But, $M_e/\nu_{n,e}M_e$ is finite. So Λ does not occur as a summand.

2. $V = \Lambda/(p^k)$. In this case $V/\nu_{n,e}V = \Lambda/(p^k, \nu_{n,e})$. It is easy to show that $\nu_{n,e}$ is a distinguished polynomial. By the division algorithm, every element of $\Lambda/(p^k, \nu_{n,e})$ is represented uniquely by a polynomial mod p^k of degree less than $\deg(\nu_{n,e}) = p^n - p^e$. Therefore $|V/\nu_{n,e}V| = p^{k(p^n-p^e)} = p^{kp^n+c}$ for some constant c.

3. $V = \Lambda/(f(x)^m)$. Let $g(x) = f(x)^m$. Then g is also a distinguished polynomial of degree, say d. Hence $x^d \equiv p(\text{poly.}) \pmod g$, so $x^k \equiv p(\text{poly.}) \pmod g$ for $k \geq d$. If $p^n \geq d$ then

$$\begin{aligned}(1+x)^{p^n} &= 1 + p(\text{poly.}) + x^{p^n} \\ &\equiv 1 + p(\text{poly.}) \pmod g\end{aligned}$$

   Therefore $(1+x)^{p^{n+1}} \equiv 1 + p^2(\text{poly.}) \pmod g$. It follows that

$$\begin{aligned}(1+x)^{p^{n+2}} - 1 &= (1 + (1+x)^{p^{n+1}} + \ldots + (1+x)^{(p-1)p^{n+1}})((1+x)^{p^{n+1}} - 1) \\ &\equiv (1 + \ldots + 1 + p^2(\text{poly.}))((1+x)^{p^{n+1}} - 1) \pmod g \\ &\equiv p(1 + p(\text{poly.}))((1+x)^{p^{n+1}} - 1) \pmod g\end{aligned}$$

   Since $1 + p(\text{poly.}) \in \Lambda^\times$, $\frac{(1+x)^{p^{n+2}}-1}{(1+x)^{p^{n+1}}-1}$ acts as (p).(unit) on $V = \Lambda/(g)$ for $p^n \geq d$. Let $n_0 \geq e, p^{n_0} \geq d$ and $n \geq n_0$. Then

$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{(1+x)^{p^{n+2}} - 1}{(1+x)^{p^{n+1}} - 1}$$

   and thus

$$\nu_{n+2,e}V = \frac{(1+x)^{p^{n+2}} - 1}{(1+x)^{p^{n+1}} - 1}(\nu_{n+1,e}V) = p\nu_{n+1,e}V$$

   Therefore $|V/\nu_{n+2,e}V| = |V/pV||pV/p\nu_{n+1,e}V|$ for $n \geq n_0$. Since $(g, p) = 1$, multiplication by p is injective, so $|pV/p\nu_{n+1,e}V| = |V/\nu_{n+1,e}V|$. Also $|V/pV| = |\Lambda/(p, g)| = p^d$. Hence $|V/\nu_{n+2,e}V| = p^d|V/\nu_{n+1,e}V|$. Therefore, by induction, we have

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

   for $n > n_0$. If $|V/\nu_{n,e}V|$ is finite for all n, then $|V/\nu_{n,e}V| = p^{dn+c}$ for some constant c. If it is infinite then V cannot occur in our case.

Thus we have proved the following proposition:

Proposition 4.1. *Suppose*

$$E = \Lambda^r \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(g_j(x)^{m_j}) \Big)$$

where each $g_j(x)$ is distinguished (not necessarily irreducible). Let $m = \sum k_i$ and $l = \sum \deg(g_j)$. If $|E/\nu_{n,e}E|$ is finite for all n, then $r = 0$ and there exist n_0 and c such that

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

for all $n > n_0$.

Now we have an exact sequence $0 \longrightarrow A \longrightarrow M_e \longrightarrow E \longrightarrow B \longrightarrow 0$ where A and B are finite. We also know the order of $E/\nu_{n,e}E$ for all $n > n_0$. Therefore it remains to relate this order to the order of $M_e/\nu_{n,e}M_e$. The issue here is that the orders of A and B could very with n, but the following lemma shows that these orders remain constant for large enough n.

Lemma 4.9. *Suppose F and E are Λ-modules with $F \sim E$ and $F/\nu_{n,e}F$ is finite for all $n \geq e$. Then, for some constant a and some n_0, $|F/\nu_{n,e}F| = p^a |E/\nu_{n,e}E|$ for all $n \geq n_0$.*

Proof. We have the following commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \ker(\phi'_n) \arrow[d] & \ker(\phi) \arrow[d] & \ker(\phi''_n) \arrow[d] & \\
0 \arrow[r] & \nu_{n,e}F \arrow[r] \arrow[d, "\phi'_n"] & F \arrow[r] \arrow[d, "\phi"] & F/\nu_{n,e}F \arrow[r] \arrow[d, "\phi''_n"] & 0 \\
0 \arrow[r] & \nu_{n,e}E \arrow[r] \arrow[d] & E \arrow[r] \arrow[d] & E/\nu_{n,e}E \arrow[r] \arrow[d] & 0 \\
 & \operatorname{coker}(\phi'_n) \arrow[d] & \operatorname{coker}(\phi) \arrow[d] & \operatorname{coker}(\phi''_n) \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Our goal is to prove that $|\ker(\phi''_n)|$ and $|\operatorname{coker}(\phi''_n)|$ are constant for large enough n. We prove this by showing each is bounded and decreasing. First we show that each is bounded. It is clear that $|\operatorname{coker}(\phi''_n)| \leq |\operatorname{coker}(\phi)|$ since one obtains representatives of $\operatorname{coker}(\phi''_n)$ from those of $\operatorname{coker}(\phi)$. For $\ker(\phi''_n)$, we apply the snake lemma to obtain the long exact sequence:

$$0 \longrightarrow \ker(\phi'_n) \longrightarrow \ker(\phi) \longrightarrow \ker(\phi''_n) \longrightarrow \operatorname{coker}(\phi'_n) \longrightarrow \operatorname{coker}(\phi) \longrightarrow \operatorname{coker}(\phi''_n) \longrightarrow 0$$

From this sequence, we see that $|\ker(\phi''_n)| \leq |\ker(\phi)|.|\operatorname{coker}(\phi'_n)| \leq |\ker(\phi)|.|\operatorname{coker}(\phi)|$ because one obtains representatives of $\operatorname{coker}(\phi'_n)$ by multiplying those of $\operatorname{coker}(\phi)$ by $\nu_{n,e}$. Therefore both $|\ker(\phi''_n)|$ and $|\operatorname{coker}(\phi''_n)|$ are bounded.

We now show that $|\operatorname{coker}(\phi''_n)|$ is decreasing. Let $m \geq n \geq 0$. Then we have $|\operatorname{coker}(\phi''_m)| \leq |\operatorname{coker}(\phi''_n)|$ since $\nu_{m,e}E = \nu_{n,e}\left(\frac{\nu_{m,e}}{\nu_{n,e}}\right)E \subseteq \nu_{n,e}E$. Thus $|\operatorname{coker}(\phi''_n)|$ is constant for large enough n.

Using the snake lemma, we have

$$|\ker(\phi'_n)|.|\ker(\phi''_n)|.|\operatorname{coker}(\phi)| = |\ker(\phi)|.|\operatorname{coker}(\phi'_n)|.|\operatorname{coker}(\phi''_n)|$$

So it remains to show that $|\ker(\phi'_n)|$ and $|\operatorname{coker}(\phi'_n)|$ are constant for large enough n. It is clear from the commutative diagram $|\ker(\phi'_n)| \leq |\ker(\phi)|$, so $|\ker(\phi'_n)|$ is bounded. Also $\nu_{m,e}F \subseteq \nu_{n,e}F$ implies $|\ker(\phi'_m)| \leq |\ker(\phi'_n)|$ for $m \geq n \geq 0$. Thus $|\ker(\phi'_n)|$ is decreasing, so constant for large enough n. Now we already know that $|\operatorname{coker}(\phi'_n)|$ is bounded. Let $\nu_{m,e}y \in \nu_{m,e}E$. Fix a set of representatives of $\operatorname{coker}(\phi'_n)$ and let $z \in \nu_{n,e}E$ be the representative for $\nu_{n,e}y$ in $\operatorname{coker}(\phi'_n)$. Observe that $\nu_{n,e}y - z = \phi(\nu_{n,e}x)$ for some $x \in F$ since it is necessarily in $\operatorname{Im}(\phi'_n)$ and this injects into $\operatorname{Im}(\phi)$. Thus we have $\nu_{m,e}y - \left(\frac{\nu_{m,e}}{\nu_{n,e}}\right)z = \phi(\nu_{m,e}x) = \phi'_m(\nu_{m,e}x)$. This shows that $|\operatorname{coker}(\phi'_m)| \leq |\operatorname{coker}(\phi'_n)|$, hence $|\operatorname{coker}(\phi'_n)|$ is constant for large enough n and we are done. □

Applying the above lemma to our case $M_e \sim E$, we get $|M_e/\nu_{n,e}M_e| = p^a|E/\nu_{n,e}E| = p^a p^{mp^n+ln+c}$ for all $n \geq n_0$, where E as in Proposition 4.1. It is now simple to complete the proof Iwasawa's theorem. We have shown that there exists integers $\mu \geq 0, \lambda \geq 0, \nu, n_0$ such that

$$\begin{aligned} p^{e_n} = |Y_n| &= |Y/M_e|.|M_e/\nu_{n,e}M_e| \\ &= (\text{constant})p^a p^{mp^n+ln+c} \\ &= p^{\lambda n+\mu p^n+\nu} \end{aligned}$$

for all $n \geq n_o$. □

We close this section with one application of Iwasawa'a theorem.

Proposition 4.2. *Suppose K_∞/K is a $\mathbb{Z}_p$-extension in which exactly one prime is ramified, and assume it is totally ramified. Then $Y_n = Y/((1+x)^{p^n}-1)Y$ and $p \nmid h_0 \iff p \nmid h_n$ for all $n \geq 0$, where h_i= class number of K_i.*

Proof. Since K_∞/K is totally ramified, we may use Lemma 4.6. We have $s = 1$, so $M_0 = xY$ and $M_n = ((1+x)^{p^n} - 1)Y$. This proves the first part. If $p \nmid h_0$, then $Y_0 = 0$, so $Y/xY = 0$. This implies $Y/(p,x)Y = 0$. By Nakayama's lemma, $Y = 0$. Thus $Y_n = 0$ and $p \nmid h_n$ for all $n \geq 0$. □

In particular for the $\mathbb{Z}_p$-extension $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p(\zeta_p)$, the Proposition 4.2 implies Corollary 2.8.

4.2 The Main Conjecture of Iwasawa theory

The Main Conjecture gives relations between various algebraically defined Λ-modules and the analytically defined p-adic L-functions. There are several equivalent formulations of the Main Conjecture depending on the choice of Λ-module. Here we discuss the form (first form) which relates the projective limit of the ideal class groups in a $\mathbb{Z}_p$-extension to the p-adic L-function. Mazur and Wiles proved the Main Conjecture (first form) for the abelian extensions of $\mathbb{Q}$ in 1984 using delicate techniques from algebraic geometry and the theory of modular curves. In the mid 1980s, Thaine and Kolyvagin introduced new techniques to study ideal class groups of real cyclotomic fields. Using these methods, Kolyvagin was able to determine the orders of different eigenspaces of the p-part of the ideal class group of $\mathbb{Q}(\zeta_p)$. The advantage of this method was that the proofs were much simpler than those of similar work by Mazur and Wiles. Rubin extended Kolyvagin's methods to give fairly elementary proof of the Main Conjecture (See Appendix, [7]). In 1990, Wiles proved the Main Conjecture for the abelian extensions of totally real fields.

Let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$, $K_\infty = \bigcup_{n\geq 0} K_n$. Then $K_\infty/K_0 = \mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)$ is the cyclotomic $\mathbb{Z}_p$-extension. As before, let L_n be the maximal unramified abelian p-extension of K_n and A_n be the p-Sylow subgroup of the ideal class group of K_n. Set $Y_n = \mathrm{Gal}(L_n/K_n) \cong A_n$, $L = \bigcup_{n\geq 0} L_n$ and $Y = \mathrm{Gal}(L/K_\infty)$. $\Gamma_n = \mathrm{Gal}(K_n/K_0)$ acts on A_n and makes it into a $\mathbb{Z}_p[\Gamma_n]$-module. The norm map N_n from A_n to A_{n-1} commutes with the action of the group ring. We denote the inverse limit $\varprojlim A_n$ with respect to the norm mappings by A. Using $\Lambda \cong \mathbb{Z}_p[[\Gamma]]$, A becomes Λ-module by defining the action componentwise. We also have $Y \cong \varprojlim Y_n \cong \varprojlim A_n = A$.

Now let G be a finite abelian group and $\hat{G}$ its character group. For $\chi \in \hat{G}$, define

$$\varepsilon_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in \overline{\mathbb{Q}}[G]$$

where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. The following properties of ε_χ's can be easily verified:

1. $\varepsilon_\chi^2 = \varepsilon_\chi$

2. $\varepsilon_\chi \varepsilon_\psi = 0$ if $\chi \neq \psi$

3. $\sum_{\chi \in \hat{G}} \varepsilon_\chi = 1$

4. $\varepsilon_\chi \sigma = \chi(\sigma)\varepsilon_\chi$

The ε_χ's are called the orthogonal idempotents of the group ring $\overline{\mathbb{Q}}[G]$. Let M be a module over $\overline{\mathbb{Q}}[G]$ and $M_\chi = \varepsilon_\chi M$. For $m \in M$, property 3 implies $\sum_{\chi \in \hat{G}} \varepsilon_\chi m = m$ and $\sum_{\chi \in \hat{G}} \varepsilon_\chi a_\chi = 0 \Longrightarrow \varepsilon_\chi a_\chi = 0$ using property 1 and 2. Therefore $M = \bigoplus_\chi M_\chi$. Each $\sigma \in G$ acts on M and thus M_χ is the eigenspace with eigenvalue $\chi(\sigma)$ by property 4.

In particular, let $G = \mathrm{Gal}(K_0/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Then $\hat{G} = \{\omega^i | 0 \leq i \leq p-2\}$ where ω is the p-adic Dirichlet character mentioned in 3.1.3. The idempotents in this case are:

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1} \in \mathbb{Z}_p[G]$$

Since $G \times \Gamma_n$ acts on A_n in the same way as the action of Γ_n on $A_n \cong Y_n$ was defined, G acts on A_n and thus A_n can be considered as $\mathbb{Z}_p[G]$-module. So we can decompose A_n according to the idempotents. Each $\varepsilon_i A_n$ is now a $\mathbb{Z}_p[\Gamma_n]$-module, hence $\varprojlim \varepsilon_i A_n = \varepsilon_i A \cong \varepsilon_i Y$ is a Λ-module. The following amazing result relates these Λ-modules (algebraic objects) to p-adic L-functions (analytic objects):

Theorem 4.4. *Assume $p \nmid h(\mathbb{Q}(\zeta_p)^+)$. Let $P_n(x) = (1+x)^{p^n} - 1$. Then for $i = 3, 5, \ldots, p-2$,*

$$\varepsilon_i A_n \cong \Lambda/(P_n(x), f(x, \omega^{1-i})) \quad \text{and} \quad \varepsilon_i A \cong \Lambda/(f(x, \omega^{1-i}))$$

where $f(x, \omega^{1-i})$ is the power series satisfying $f((1+p)^s - 1, \omega^{1-i}) = L_p(s, \omega^{1-i})$ (power series from Iwasawa's construction of p-adic L-functions).

Proof. See the proof of Theorem 10.16, [13]. □

We factor $f(x, \omega^{1-i}) = p^{\mu_i} g_i(x) U_i(x)$ with g_i distinguished and $U_i \in \Lambda^\times$. Therefore, by Theorem 4.4, $\varepsilon_i Y = \Lambda/(p^{\mu_i} g_i(x)) \cong \Lambda/(p^{\mu_i}) \bigoplus \Lambda/(g_i)$ which is of the form of decomposition of $\varepsilon_i Y$ as a Λ-module. It is known that $\mu_i = 0$ for cyclotomic $\mathbb{Z}_p$-extensions (Theorem 7.15, [13]). Therefore

$$\varepsilon_i Y \cong \Lambda/(f(x, \omega^{1-i})) \cong \Lambda/(g_i(x))$$

So in this case the distinguished polynomial in the decomposition of $\varepsilon_i Y$ is essentially the p-adic L-function. Iwasawa conjectured that this is true in more general situation, for totally real extensions of rationals.

Let F be totally real and let $K_0 = F(\zeta_p), K_\infty = F(\zeta_{p^\infty})$. Let $\Delta = \mathrm{Gal}(K_0/F) \subseteq$

$(\mathbb{Z}/p\mathbb{Z})^\times$. Let $\chi \in \hat{\Delta}$ be odd. Then

$$Y_\chi = \varepsilon_\chi Y \hookrightarrow \bigoplus_i \Lambda/(p^{k_i^\chi}) \oplus \bigoplus_j \Lambda/(g_j^\chi(x))$$

with finite cokernel. Let $\mu_\chi = \sum k_i^\chi$ and let $g_\chi(x) = p^{\mu_\chi} \prod_j g_j^\chi(x)$ (g_χ is called as characteristic polynomial associated to Y_χ). It has been shown by Deligne and Ribet that there exists a p-adic L-function for the even character $\omega\chi^{-1}$. Let γ_0 be the generator of $\mathrm{Gal}(K_\infty/K_0)$ corresponding to $1+x$. Define $\kappa_0 \in 1+p\mathbb{Z}$ by $\gamma_o \zeta_{p^n} = \zeta_{p^n}^{\kappa_0}$ for all $n \geq 1$. It has been shown that there exists a power series $f_\chi \in \Lambda$ such that $L_p(s, \omega\chi^{-1}) = f_\chi(\kappa_0^s - 1)$, $\chi \neq \omega$. We now state the Main Conjecture:

Theorem 4.5 (The Main Conjecture or Mazur-Wiles Theorem (first form)). *$f_\chi(x) = g_\chi(x)U_\chi(x)$ with $U_\chi(x) \in \Lambda^\times$.*

In other words, the Main Conjecture says that the power series attached to the p-adic L-function is equal to the characteristic polynomial up some unit.

We now state a slightly different form. Consider $\mathbb{C}_p$-vector space $V = Y \otimes_{\mathbb{Z}_p} \mathbb{C}_p$. Since

$$Y \sim \bigoplus_i \Lambda/(p^{k_i}) \oplus \bigoplus_j \Lambda/(g_j(x))$$

we have

$$V \cong \bigoplus_j \mathbb{C}_p[x]/(g_j(x))$$

as tensoring with $\mathbb{C}_p$ kills the finite kernel, cokernel and the $\Lambda/(p^{k_i})$'s in the decomposition of Y. V is a finite dimensional vector space and $x+1 = \gamma_0$ acts on V by multiplication. Thus Γ acts on V. Let $g(x) = \prod g_j(x)$ be the characteristic polynomial of $\gamma_0 - 1$ acting on V. The vector space V is clearly a $\overline{\mathbb{Q}}_p[\Delta]$-module, so we can decompose

$$V = \sum_\chi \varepsilon_\chi V$$

Then

$$g(x) = \prod_\chi g^\chi(x)$$

where $g^\chi(x)$ the characteristic polynomial of $\gamma_0 - 1$ acting on $\varepsilon_\chi V$. By p-adic Weierstrass Preparation Theorem, we can write $f_\chi(x) = p^{\mu_\chi}\tilde{f}_\chi(x)U_\chi(x)$.

Theorem 4.6 (The Main Conjecture (second form)). *$\tilde{f}_\chi(x) = g^\chi(x)$.*

Note that the advantage of this form is that we may consider larger class of characters, but since V is formed by tensoring Y with $\mathbb{C}_p$, we lose the information contained in μ_χ.

Proving Main Conjecture is a very difficult task. As mentioned earlier, currently there are two methods used to prove the Main Conjecture. One of them is the "geometric"method which was invented by Mazur and Wiles. In this method one uses congruences and p-adic representations coming from modular forms. The other method, which is rather different in nature and easier than the first one, uses a certain Galois cohomological tool known as "Euler system". Unfortunately, constructing an Euler system is very difficult in its own right and very few Euler systems are known.

The motivation for the Main Conjecture comes from the theory of function fields over finite fields (or curves over finite fields). Function fields have many properties that are closely related to the arithmetical properties of number fields; for example, both have zeta functions, satisfy class field theory, and have finite residue class fields at all (nonarchimedean) places. Let C be a complete, nonsingular curve of genus g over a finite field k of characteristic $l \neq p$ and let J be its Jacobian variety. Let J_p be the set of points on J of p-power order defined over the algebraic closure $\overline{k}$ of k. This is essentially the analogue of $Y \cong A = \varprojlim A_n$ for cyclotomic $\mathbb{Z}_p$-extensions. We have $J_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$ as abelian groups. Therefore $\mathrm{Hom}_{\mathbb{Z}_p}(J_p, (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}) = \mathbb{Z}_p^{2g}$, and

$$\mathrm{Hom}_{\mathbb{Z}_p}(J_p, (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathbb{Q}_p^{2g}$$

The Frobenius automorphism of $\overline{k}/k$ acts on this last space and Weil Conjecture states that the characteristic polynomial is the numerator of the zeta function of C. Extending an analogy with the Weil Conjecture, it is natural to ask whether the characteristic polynomial of the pro-p part of the class group Y of a cyclotomic $\mathbb{Z}_p$-extension is of zeta type or not. Therefore the Main Conjecture is an attempt to extend the analogy between number fields and function fields to this important situation.

We now give one application of the Main Conjecture to the sizes of class groups. Let p be an odd prime and $F/\mathbb{Q}$ be an abelian imaginary extension. Let $\chi : \mathrm{Gal}(F/\mathbb{Q}) \to \mathcal{O}_\chi^\times$ be an odd character, where $\mathcal{O}_\chi$ is the ring generated over $\mathbb{Z}_p$ by the values of χ. Set $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Let $g = [\mathcal{O}_\chi : \mathbb{Z}_p]$ and A_F be the p-Sylow subgroup of the class group of F. We write A_F^χ to denote the χ-isotypical piece of A_F, that is $A_F^\chi = A_F \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\chi$.

Theorem 4.7. *Suppose $\chi \neq \omega$, then $|A_F^\chi| = |\mathcal{O}_\chi/L_p(0, \omega\chi^{-1})|$.*

Proof. See Section 5.2, [1]. □

In particular, if $v_p(a)$ denotes the p-adic valuation of a, then Theorem 4.7 implies $v_p(|A_F^\chi|) = v_p(|\mathcal{O}_\chi/L_p(0, \omega\chi^{-1})|) = v_p(|\mathcal{O}_\chi/(L(0, \chi^{-1})(1 - \chi^{-1}(p)))|) = g v_p(L(0, \chi^{-1}))$.

We end this chapter by mentioning two of the major directions Iwasawa theory has expanded over the years. The obvious generalization is to replace the limits of class groups Y with more general objects. For example, Let E be an elliptic curve over $\mathbb{Q}$ with ordinary reduction at p, then there is a Main Conjecture for the structure of Pontryagin dual of Selmer group of E over $\mathbb{Q}_\infty$ in terms of a p-adic L-function of E. Great progress has been made on this particular Main Conjecture, due to successive work of Rubin (for CM-curves), Kato, and Skinner and Urban. In the second generalization, one allows the Galois group Γ of the tower of cyclotomic fields to be isomorphic to an open subgroup of $GL_m(\mathbb{Z}_p)$ for some $m \geq 1$. In this case, Main Conjecture becomes more difficult to formulate, as the structure theory of Λ-modules is no longer simple. Still, in the past decade, such main conjectures have been formulated using algebraic K-theory as one of the several tools. The corresponding Main Conjecture for p-adic Lie extensions of totally real number fields has recently been proved by Mahesh Kakde in a paper under review. Other possible directions for future developments could be a theory of $\hat{\mathbb{Z}}$-extensions ($\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} = \prod \mathbb{Z}_p$). Some progress has been made by E. Friedman in this direction.

Bibliography

[1] Brown J. L., *An Introduction to Iwasawa Theory*, Course Notes, Ohio State University, Autumn 2006.

[2] Coates J., Sujatha R., *Cyclotomic Fields and Zeta Values*, Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg, 2006.

[3] Iwasawa K., *Lectures on p-adic L-functions*, Annals of Mathematics Studies, 74, Princeton University Press, 1972.

[4] Janusz G., *Algebraic Number Fields*, Academic Press, New York-London, 1973.

[5] Katz N., *p-adic L-function via moduli of elliptic curves*, Proceedings of Symposia in Pure Mathematics, Volume 29, 1975.

[6] Lang S., *Algebraic Number Theory*, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994.

[7] Lang S., *Cyclotomic Fields I and II*, Graduate Texts in Mathematics, 121, Springer-Verlag, New York, 1990.

[8] Marcus D. A., *Number Fields*, Springer-Verlag, New York, 1977.

[9] Milne J. S., *Class Field Theory*, Notes version 4.02.

[10] Neukirch J., *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften, 322, Springer-Verlag, Berlin, 1999.

[11] Serre J.-P., *Local Fields*, Graduate Texts in Mathematics, 67, Springer-Verlag, New York, 1979.

[12] Sharifi R., *Notes on Iwasawa Theory*, `http://math.arizona.edu/~sharifi/iwasawa.pdf`.

[13] Washington L. C. , *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.