Universidad Nacional de Colombia
Sede Medellín
Facultad de Ciencias

Posgrados en Matemáticas

Master's Thesis

On arithmetic equivalence and Iwasawa invariants

Thesis presented as a partial requirement to qualify for the title of
M. Sc. in Mathematics

By: Carlos Alberto Pérez López

Advisor: Ph.D Guillermo Mantilla-Soler
Co-advisor: Ph.D Juan Diego Vélez

October 2024

Universidad Nacional de Colombia
Sede Medellín
Facultad de Ciencias

Posgrados en Matemáticas

Tesis de Maestría

Sobre la equivalencia aritmética y los invariantes de Iwasawa

Tesis presentada como requisito parcial para optar al título de:
Magister en Matemáticas

Por: Carlos Alberto Pérez López

Director: Ph.D Guillermo Mantilla-Soler
Co-director: Ph.D Juan Diego Vélez

Octubre, 2024

Acknowledgements

I would like to express my thanks to my advisor, Professor Guillermo Mantilla-Soler. His enthusiasm for number theory has been so inspiring to me, and I am deeply grateful for the trust he placed in me despite numerous setbacks and inconveniences along the way.

Another word of gratitude is due to Liliana, she embodies the best qualities of humanity that the Faculty of Sciences has to offer.

Words cannot express my gratitude to my sisters, Angelica, Luisa, and Valentina. Their love and unconditional support gave me the strength to keep fighting for my life and my dreams. I know our mother would be very proud of you.

I would also like to extend my gratitude to my girlfriend, Juliana. Your love, as well as your moral and physical support, gave me the encouragement I needed to complete this work.

Abstract

In the mid-20th century, number theory experienced a significant evolution through the development of Iwasawa theory, initiated by Kenkichi Iwasawa. His pioneering approach provided new tools to study the growth of the p-part of the ideal class group in cyclotomic $\mathbb{Z}_p$-extensions of number fields. Central to this theory is the concept of Iwasawa modules and their relationship to p-adic L-functions, culminating in the Main Conjecture of Iwasawa theory. This abstract framework has profoundly influenced our understanding of arithmetic in infinite towers of number fields.

Parallel to this development, the study of Dedekind zeta functions and arithmetic equivalence—principally advanced by Ronald Perlis—introduced a framework for comparing number fields based on their zeta functions. Fields with identical Dedekind zeta functions, though not necessarily isomorphic, exhibit identical prime ideal behavior, a phenomenon explained through Gassmann equivalence of subgroups in the Galois group of a common Galois closure.

This thesis explores the deep and subtle connections between Iwasawa theory and arithmetic equivalence. Specifically, it investigates how Iwasawa modules can inform the structure of Dedekind zeta functions for totally real number fields and analyzes the relationships among Iwasawa modules associated with arithmetically equivalent fields. The exposition begins with the historical development of Iwasawa theory and the role of p-adic methods in class field theory, continues through the foundational theorems and analytic tools involving L-functions, and culminates in a synthesis that connects these algebraic and analytic structures within a unified framework.

Keywords: Iwasawa theory, arithmetic equivalence, Dedekind zeta function, Iwasawa module, L-functions, cyclotomic extensions, class groups, Gassmann equivalence, algebraic number theory.

Resumen

A mediados del siglo XX, la teoría de números experimentó una evolución significativa con el desarrollo de la teoría de Iwasawa, iniciada por Kenkichi Iwasawa. Su enfoque pionero proporcionó nuevas herramientas para estudiar el crecimiento de la parte p-ádica del grupo de clases ideales en extensiones ciclotómicas $\mathbb{Z}_p$ de cuerpos numéricos. En el centro de esta teoría se encuentran los módulos de Iwasawa y su relación con las L-funciones p-ádicas, culminando en la Conjetura Principal de la teoría de Iwasawa. Este marco abstracto ha influido profundamente en nuestra comprensión de la aritmética en torres infinitas de cuerpos numéricos.

En paralelo, el estudio de las funciones zeta de Dedekind y la equivalencia aritmética —desarrollado principalmente por Ronald Perlis— introdujo un enfoque para comparar cuerpos numéricos a partir de sus funciones zeta. Los cuerpos con funciones zeta de Dedekind idénticas, aunque no necesariamente isomorfos, exhiben un comportamiento idéntico respecto a la factorización de ideales primos, fenómeno explicado mediante la equivalencia de Gassmann entre subgrupos del grupo de Galois de una clausura de Galois común.

Esta tesis explora las conexiones profundas y sutiles entre la teoría de Iwasawa y la equivalencia aritmética. En particular, se investiga cómo los módulos de Iwasawa pueden informar sobre la estructura de las funciones zeta de Dedekind en cuerpos totalmente reales, y se analizan las relaciones entre los módulos de Iwasawa asociados a cuerpos numéricos aritméticamente equivalentes. La exposición comienza con el desarrollo histórico de la teoría de Iwasawa y el papel de los métodos p-ádicos en la teoría de cuerpos de clases, continúa con los teoremas fundamentales y las herramientas analíticas asociadas a las funciones L, y culmina en una síntesis que conecta estas estructuras algebraicas y analíticas dentro de un marco unificado.

Palabras clave: Teoría de Iwasawa, equivalencia aritmética, función zeta de Dedekind, módulo de Iwasawa, L-funciones, extensiones ciclotómicas, grupos de clases, equivalencia de Gassmann, teoría algebraica de números.

Introduction

In the 1950s and 1960s, number theory was deeply focused on class field theory, which describes abelian extensions of number fields. Number theorists were particularly interested in understanding the ideal class groups of number fields, especially in towers of fields where each field is an extension of the previous one, such as $\mathbb{Q}(\zeta_{p^n})$, where ζ_{p^n} is a primitive p^n-th root of unity. This type of tower is called a cyclotomic $\mathbb{Z}_p$-extension because it is constructed by adjoining roots of unity, and it has a Galois group isomorphic to $\mathbb{Z}_p^\times$, the group of units of the p-adic integers. The Japanese Kenkichi Iwasawa introduced an entirely new way to study the behavior of class groups in these towers of number fields. He was interested in understanding how the p-part of the class group grows in a cyclotomic $\mathbb{Z}_p$-extension. His idea was to create a systematic approach using p-adic methods and group theory to study the growth of the class numbers in these extensions. Specifically, he showed that the structure of the ideal class group in these extensions could be described in terms of an algebraic object called an Iwasawa module. Iwasawa's theorem eventually led to the formulation of the Iwasawa Main Conjecture, which relates the characteristic power series of the Iwasawa module (essentially, the structure of the p-adic class group) to the p-adic L-function of a number field. This conjecture was famously proved for cyclotomic fields by Barry Mazur and Andrew Wiles in the 1980s, providing a landmark result that connected Iwasawa theory with the behavior of p-adic L-functions.

On the other hand, the Dedekind zeta function $\zeta_K(s)$ of a number field is a fundamental object in algebraic number theory that generalizes the Riemann zeta function to arbitrary number fields. It encodes deep arithmetic information about these fields, including the distribution of prime ideals, the class number, and other important invariants. The concept of arithmetic equivalence in number theory, primarily developed by Ronald Perlis in the 1970s, deals with the question of when two number fields have the same Dedekind zeta function. This equivalence has deep implications for understanding the structure of number fields and their invariants. More explicitly, two number fields K and K' are said to be arithmetically equivalent if they have the same Dedekind zeta function, i.e.,

$$\zeta_K(s) = \zeta_{K'}(s).$$

This implies that K and K' have the same prime ideal factorization structure in terms of norms, decomposition types, and inertial degrees, although the fields themselves might not be isomorphic. Perlis showed that for two fields to be arithmetically equivalent, their Galois closures must have subgroups of the Galois group that are Gassmann equivalent. Gassmann equivalence, a concept introduced by Fritz Gassmann in the 1920s, refers to two subgroups of a Galois group that induce the same permutation character on the group, meaning they have the same fixed field behavior for prime ideals. Perlis's work established that Gassmann-equivalent subgroups in the Galois group of a common Galois closure can produce non-isomorphic fields that are arithmetically equivalent. Therefore, the Dedekind zeta function, while a powerful invariant, is not a complete invariant for determining the isomorphism class of a number field. This has implications for class field theory and the study of zeta functions in general.

The works of Perlis, Keiichi Komatsu, Jangheon Oh, and others have developed connections between Iwasawa Theory and Arithmetic Equivalence, which constitute the main focus of this thesis.

Specifically, this thesis is an exposition of certain connections that exist between these two theories, such as how knowing certain Iwasawa modules can help determine the Dedekind zeta function for totally real number fields, and what can be said about the relationships between certain Iwasawa modules of arithmetically equivalent number fields. Chapter 2 provides historical motivation, exploring the origins of the study of the p-part of the ideal class group, an area that enabled Ernst Kummer to solve a specific case of Fermat's Last Theorem through novel techniques in number theory.

Chapter 3 focuses on presenting a proof of the foundational theorem that inaugurated Iwasawa theory. As mentioned earlier, this theorem examines the growth of the p-part of the ideal class group in certain infinite extensions of fields, particularly $\mathbb{Z}_p$-extensions.

Chapter 4 is dedicated to reviewing L-functions, which play a crucial role throughout this work. We discuss how specific critical values of these functions interpolate to their analogous p-adic L-functions, creating a framework for the analytical connections developed in the final chapter.

In Chapter 5, we delve into various forms of arithmetic equivalence, with a special focus on quasi-conjugates, particularly Gassmann equivalence. Additionally, we explicitly examine the types of data that can be derived from a field via its Dedekind zeta function, shedding light on the structure and properties encoded within.

Chapter 6 revisits p-adic L-functions, the p-adic analogs of classical L-functions, and explores how these functions interpolate at certain values. This chapter also examines the profound connection between arithmetic objects, such as Iwasawa modules, and analytic objects, specifically p-adic L-functions. Known as the Main Conjecture of Iwasawa theory, this relationship forms a bridge between Iwasawa theory and arithmetic equivalence, providing new insights into their interdependence.

Contents

Chapter 1

Preliminaries

In this thesis, for simplicity, we adopt the following convention.

Convention. Let p be a prime number. Unless otherwise stated, p is always assumed to be odd.

1 Basic Algebraic Number Theory

In this section, we present a review of the basic notions and results of algebraic number theory. For basic notation, definitions, and proofs of the statements, the reader is referred to [12].

Let K be a number field, i.e., a finite extension of $\mathbb{Q}$. *The ring of integers* of K, denoted by $\mathcal{O}_K$, is defined as:

$$\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(x) \in \mathbb{Z}[x]\}.$$

We have that K is the field of fractions of $\mathcal{O}_K$. The ring of integers generalizes the notion of integers to more general number fields, with the following properties:

- $\mathcal{O}_K$ is a *Dedekind domain*, meaning it is Noetherian, integrally closed, and every nonzero prime ideal is a maximal ideal.
- $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is an *integral basis* of the ring of integers $\mathcal{O}_K$ of K (i.e., each element of $\mathcal{O}_K$ can be expressed uniquely as a $\mathbb{Z}$-linear combination of these α_i), the *discriminant* of K is defined as:

$$d_K = \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)_{1\le i,j\le n},$$

Here, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ denotes the *trace map*, which is the trace of the linear operator multiplication by α. Since $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j) \in \mathbb{Z}$, ensuring that $d_K \in \mathbb{Z}$. Moreover, d_K is independent of the choice of integral basis.

Let L/K be a finite extension of number fields, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then, $\mathfrak{p}$ factors into prime ideals of $\mathcal{O}_L$ as:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where:

- $\mathfrak{P}_i$ are prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$, meaning $\mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_K$ for every i.

- g is the number of distinct prime ideals in the factorization.
- e_i is the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Each prime ideal $\mathfrak{P}_i$ corresponds to an extension of the residue field:

$$f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}],$$

where f_i is the *inertia degree* measuring the degree of the extension of residue fields. The degree of the field extension $[L : K]$ is related to the ramification indices and inertia degrees through the $fundamental\ equality$:

$$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

Special cases:

- *Ramified Prime:* If there is a prime $\mathfrak{P}_i$ over $\mathfrak{p}$ with $e_i > 1$, the extension is ramified at $\mathfrak{p}$.
- *Unramified Prime:* If all $e_i = 1$, the extension is unramified at $\mathfrak{p}$.
- *Totally Ramified Prime:* If $g = 1$, the prime ideal $\mathfrak{p}$ stays as a single prime ideal $\mathfrak{P}_1$ with $e_1 = [L : K]$.
- *Split Prime:* If all $e_i = 1$ and $f_i = 1$, the prime $\mathfrak{p}$ splits completely into $[L : K]$ distinct prime ideals.
- *Inert Prime:* If $g = e = 1$, the prime $\mathfrak{p}$ remains a prime ideal in the extension.

There are only finitely many prime ideals of K which are ramified in L. In Particular, if p is a rational integer then p ramifies in K if and only if p divides d_K.

Suppose that K is a number field of degree $n = [K : \mathbb{Q}]$. An *embedding* of a number field K into the complex numbers $\mathbb{C}$ is an injective field homomorphism $\psi : K \hookrightarrow \mathbb{C}$. If the image of the embedding lies entirely within the real numbers $\mathbb{R} \subset \mathbb{C}$, the embedding is called a *real embedding*. If the image is not entirely contained in $\mathbb{R}$, it is called a *complex embedding*. Each complex embedding comes in conjugate pairs: if $\psi : K \hookrightarrow \mathbb{C}$ is a complex embedding, then its complex conjugate $\overline{\psi}$ is another distinct embedding. Let r_1 and r_2 be the number of real embeddings of K and the number of pairs of complex embeddings of K, respectively. Then, the degree n satisfies:

$$n = r_1 + 2r_2.$$

The embeddings of a number field are also referred to as $infinite\ primes$. If a real embedding $\psi : K \hookrightarrow \mathbb{R}$ extends to $\tilde{\psi} : L \hookrightarrow \mathbb{C}$, the prime is said to be *ramified* at infinity. In that case, we will say that $\tilde{\psi}$ is lying above ψ. Conversely, if this embedding remains real in the extension field L, the prime is said to be *unramified* at infinity. The usual prime ideals are known as $finite\ primes$.

Dirichlet's Unit Theorem states that the group of units $\mathcal{O}_K^\times$ (the invertible elements) of the ring of integers $\mathcal{O}_K$ is isomorphic to:

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1},$$

where $\mu(K)$ is the finite cyclic group of roots of unity contained in K and $\mathbb{Z}^{r_1+r_2-1}$ represents the free abelian part. In other words, there exist units $\varepsilon_1, ..., \varepsilon_{r_1+r_2+1}$ called fundamental units, such that any $\varepsilon \in \mathcal{O}_K^\times$ can be written uniquely as a product

$$\varepsilon = \zeta \cdot \varepsilon_1^{k_1} \cdots \varepsilon_{r_1+r_2-1}^{k_{r_1+r_2-1}}$$

with ζ a root of unity and integers k_i. We define $W(K) := |\mu(K)|$.

Now, we generalize the notion of an ideal in the ring of integers to include *fractional ideals*, which are nonzero finitely generated $\mathcal{O}_K-$submodule of K. The fractional ideals form an abelian group, the *ideal group* J_K of K. The identity element is $(1) = \mathcal{O}_K$, and the inverse of a fractional ideal $\mathfrak{a}$ is $\mathfrak{a}^{-1} = \{x \in K \big| x\mathfrak{a} \subseteq \mathcal{O}_K\}$. The fractional principal ideals $(a) = a\mathcal{O}_K$, $a \in K^*$, form a subgroup of J_K, which will be denoted by P_K. The quotient group

$$Cl(K) = J_K/P_K$$

is called the *ideal class group,* or *class group* for short, of K.

The class group is a measure of the extent to which unique factorization fails in the ring of integers of K. The order of the group, which is finite, is called the *class number* of K, denoted by

$$h_K = |\mathrm{Cl}(K)|.$$

We will make considerable use of the following result from class field theory.

Theorem 1.1 (Hilbert Class Field)**.** *Let K be a number field. There exists a maximal extension H/K with respect to the following properties:*

- *H/K is an abelian extension.*
- *H/K is unramified.*

Moreover, H/K is a finite extension with

$$\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K),$$

This extension is called the maximal abelian unramified extension of K or the Hilbert class field of K.

Next, we examine the theory of ramification for the case when L/K is a Galois extension. The prime ideals are then subject to the action of the group $G = \mathrm{Gal}(L/K)$, as follows. Let

$$\Sigma_{\mathfrak{p}} := \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$$

be the set of prime ideals of $\mathcal{O}_L$ lying above the prime $\mathfrak{p}$, then

$$\sigma(\mathfrak{P}_i) \in \Sigma_{\mathfrak{p}} \quad \text{for each } \sigma \in G.$$

Therefore G acts on $\Sigma_{\mathfrak{p}}$. In fact, G acts transitively on $\Sigma_{\mathfrak{p}}$.

The *decomposition group* of $\mathfrak{P}_i$ is the stabilizer subgroup of G with respect to $\mathfrak{P}_i$:

$$D(\mathfrak{P}_i \mid \mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}.$$

The decomposition group encodes in group-theoretic language the number of different prime ideals into which a prime ideal $\mathfrak{p}$ decomposes in $\mathcal{O}_L$, more precisely, the index $(G : D(\mathfrak{P}_i \mid \mathfrak{p}))$ is equal to g. Moreover,

$$\begin{aligned} D(\mathfrak{P}_i \mid \mathfrak{p}) = 1 &\iff \mathfrak{p} \text{ is totally split.} \\ D(\mathfrak{P}_i \mid \mathfrak{p}) = G &\iff \mathfrak{p} \text{ is nonsplit.} \end{aligned}$$

Let $\sigma \in G$. Let $x + \mathfrak{P}_i$ be an element of the residue field $\mathcal{O}_L/\mathfrak{P}_i$. We define $\tilde{\sigma}$ as: $\tilde{\sigma}(x + \mathfrak{P}_i) = \sigma(x) + \mathfrak{P}_i$. The homomorphism described below is surjective.

$$\begin{aligned} \pi : D(\mathfrak{P}_i \mid \mathfrak{p}) &\to \mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})\right) \\ \sigma \quad &\mapsto \quad \pi(\sigma) = \bar{\sigma} \end{aligned}$$

The *inertia group* $I(\mathfrak{P}_i \mid \mathfrak{p})$ is the kernel of π. Therefore, it consists of all elements of the decomposition group that act trivially on the residue field $\mathcal{O}_L/\mathfrak{P}_i$:

$$I(\mathfrak{P}_i \mid \mathfrak{p}) = \{\sigma \in D(\mathfrak{P}_i \mid \mathfrak{p}) \mid \sigma(x) \equiv x \pmod{\mathfrak{P}_i} \text{ for all } x \in \mathcal{O}_L\}.$$

Therefore $D(\mathfrak{P}_i \mid \mathfrak{p})/I(\mathfrak{P}_i \mid \mathfrak{p}) \cong \mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})\right)$.

The inertia group measures the part of the Galois action that only affects higher powers of $\mathfrak{P}_i$ without changing the residue field, more precisely, $|I(\mathfrak{P}_i \mid \mathfrak{p})| = e_i$. Thus, $|D(\mathfrak{P}_i \mid \mathfrak{p})| = e_i f_i$. We note that if the inertia group is trivial, $I(\mathfrak{P} \mid \mathfrak{p}_i) = 1$, then the extension L/K is unramified at $\mathfrak{p}$.

In the Galois case, the inertia degrees are equal, namely, $f_1 = \cdots = f_g = f$. The same applies to the ramification indices: $e_1 = \cdots = e_g = e$. By fundamental equality we have

$$[L : K] = efg.$$

Let $K_1 \subseteq K_2 \subseteq K_3$ be number fields with K_2/K_1 and K_3/K_1 being Galois, and let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \mathfrak{p}_3$ be primes of K_1, K_2, and K_3, respectively. Consider the restriction homomorphism

$$\mathrm{res} : \mathrm{Gal}(K_3/K_1) \to \mathrm{Gal}(K_2/K_1).$$

Then:

- $\mathrm{res}\,|_{D(\mathfrak{p}_3|\mathfrak{p}_1)}$: $D(\mathfrak{p}_3 \mid \mathfrak{p}_1) \to D(\mathfrak{p}_2 \mid \mathfrak{p}_1)$ is surjective.
- $\mathrm{res}\,|_{I(\mathfrak{p}_3|\mathfrak{p}_1)}$: $I(\mathfrak{p}_3 \mid \mathfrak{p}_1) \to I(\mathfrak{p}_2 \mid \mathfrak{p}_1)$ is surjective.

Now, we extend the previous notions to the concept of infinite primes. Let L/K be a Galois extension of number fields and let Ψ be an infinite prime of L lying above the infinite prime ψ of K. The decomposition and inertia subgroups for the pair $\Psi \mid \psi$ are equal and are defined by:

$$D(\Psi \mid \psi) = T(\Psi \mid \psi) = \{\sigma \in \mathrm{Gal}(L/K) : \Psi \circ \sigma = \Psi\}.$$

2 Basic results on cyclotomic fields

In this section, we review the basic notions and results of cyclotomic fields, one of the main objects of interest in this thesis. The reader is referred to Chapters 1 and 2 of [18], for basic notation, definitions, and proofs of the statements.

For $n \geq 1$, let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$; this is a primitive nth root of unity. Then the nth cyclotomic field is the extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ generated by ζ_n. The conjugates of ζ_n in $\mathbb{C}$ are, therefore, the other primitive nth roots of unity: ζ_n^k for $1 \leq k \leq n$ with $(k, n) = 1$. The degree of $\mathbb{Q}(\zeta_n)$ is therefore $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, where ϕ is Euler's totient function. The roots of $x^n - 1$ are the powers of ζ_n, so $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$. Therefore $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$.

Theorem 1.2. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

The isomorphism sends each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ to $a \mod n$, where a is an integer such that $\sigma(\zeta_n) = \zeta_n^a$ and $(a, n) = 1$.

Theorem 1.3. *The ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.*

Proposition 1.1. *For $n > 2$, the discriminant of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is*

$$(-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

In particular, the discriminant of $\mathbb{Q}(\zeta_{p^n})$ is

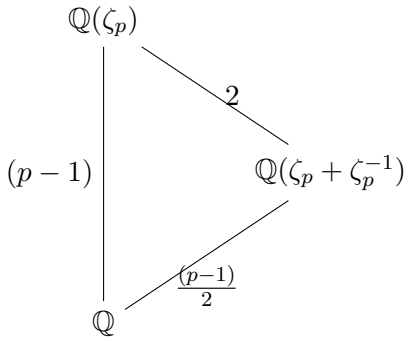
$$\epsilon \cdot p^{p^n - 1(p^n - n - 1)}, \quad \epsilon = \begin{cases} -1 & \text{if } p^n = 4 \text{ or } \text{ if } p \equiv 3 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Proposition 1.2. *Let K be a number field with r_2 pairs of complex embeddings. Then d_K has sign $(-1)^{r_2}$.*

Corollary 1.3.1. *p ramifies in $\mathbb{Q}(\zeta_n) \iff p$ divides n.*

Proposition 1.3. *If n is a power of a prime p, then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is totally ramified above p.*

Take any embedding of $\mathbb{Q}(\zeta_p)$ into the complex numbers. Complex conjugation acts as an automorphism sending ζ_p to ζ_p^{-1}. The fixed field is $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\cos(2\pi/p))$ and is called the maximal real subfield of $\mathbb{Q}(\zeta_p)$, denoted by $\mathbb{Q}(\zeta_p)^+$.



Proposition 1.4. *If $n = p^n$ then $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is ramified at the prime above p and at the infinite primes, and unramified at the other primes.*

Proposition 1.5. *The ring of integers of $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.*

Proposition 1.6. *The only roots of unity in $\mathbb{Q}(\zeta_n)$ are of the form $\pm\zeta_n^m$.*

Proposition 1.7. *Let u be a unit of $\mathbb{Z}[\zeta_p]$. Then there exist $u_1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $r \in \mathbb{Z}$ such that $u = \zeta_p^r u_1$.*

In the next chapter, we will motivate the study of the p-part of the class group and its historical relevance in solving a particular case of Fermat's Last Theorem.

Chapter 2

Fermat's Last Theorem for Regular primes

One of the most famous problems in mathematics states that

Theorem 2.1 (Fermat's Last Theorem)**.** *Let $n > 2$ be an integer number. Then*

$$x^n + y^n = z^n, \qquad with \quad xyz \neq 0,$$

has no integer solutions.

Pierre de Fermat proved it for the case $n = 4$, therefore, it suffices to consider the case where $n = p$ is an odd prime number. The case where p does not divide x,y, and z is called the first case of Fermat's Last Theorem, the second case, where p divides one of x,y,z.

In this chapter, we first discuss Fermat's Last Theorem for the first two odd primes, which will allow us to see how the need for Kummer's Lemma arises. Finally, we discuss a sufficient condition for Fermat's Last Theorem to be true.

1 Fermat's Last Theorem for the cases $p = 3$ and $p = 5$

Let us consider the case $p = 3$ of Fermat's last theorem, namely

Theorem 2.2. *The equation*

$$x^3 + y^3 = z^3, \qquad with \quad xyz \neq 0,$$

has no integer solutions.

Proof. For the sake of contradiction, let us assume there is a nontrivial solution (x, y, z) of $x^3 + y^3 = z^3$. We may assume that x, y and z are pairwise coprime in $\mathbb{Z}$, since otherwise, if, for example $(x, y) = d \neq 1$, then each factor prime of d divides z. Therefore d divides z and then we cancel out d from the equation. We proceed similarly in other cases.

Also we may assume that $3|xyz$ since otherwise if $3 \nmid x$ then $x^3 \equiv \pm 1 \pmod 9$ and similarly for y and z. Therefore $x^3 + y^3 \equiv -2, 0$, or $+2 \pmod 9$ but $z^3 \equiv \pm 1 \pmod 9$, therefore $x^3 + y^3 \neq z^3$. Since we assume that x, y and z are pairwise relatively prime then 3 divides only one of them. Without loss of generality, we may assume that $3|z$ because if for example $3|y$ we may rewrite the equation (as $x^3 + (-z)^3 = (-y)^3$), similarly in the case where $3|x$. Hence, from now on, we will assume that $3|z$ but $3 \nmid x, y$.

Let ζ_3 be a primitive 3th root of unity, ζ_3 satisfies the equation $\zeta_3^2+\zeta_3+1=0$. In the ring $\mathbb{Z}[\zeta_3]$ the above equation is factored as follows

$$(x+y)(x+\zeta_3 y)(x+\zeta_3^2 y)=z^3,$$

$\mathbb{Z}[\zeta_3]$ is known as the ring of Eisenstein integers, which forms a Euclidean domain whose norm N is given by the square modulus:

$$N(a+b\zeta_3)=a^2-ab+b^2.$$

Using that

$$a^2-ab+b^2=\left(a-\frac{b}{2}\right)^2+\frac{3b^2}{4},$$

we can find out that the units group of $\mathbb{Z}[\zeta_3]$ is $\mathbb{Z}[\zeta_3]^\times=\{\pm 1,\pm\zeta_3,\pm\zeta_3^2\}$. We define

$$\begin{aligned}\eta&=x+y,\\ \mu&=x+\zeta_3 y,\\ \chi&=x+\zeta_3^2 y,\\ \pi&=1-\zeta_3.\end{aligned}$$

Since $(-\zeta_3^2)(1-\zeta_3)^2=3$ then $\pi|z$ and therefore $\pi|\eta\mu\chi$. Due to the fact that π is a prime number in $\mathbb{Z}[\zeta_3]$, π divides one of η,μ,χ. Because the equalities

$$\begin{aligned}\eta-\mu&=y(1-\zeta_3)\quad\text{and}\\ \mu-\chi&=y\zeta_3(1-\zeta_3),\end{aligned}$$

we obtain that π divides η,μ and χ, therefore they are not pairwise relatively prime in $\mathbb{Z}[\zeta_3]$, in that case, note that the equation

$$-\zeta_3(x+\zeta_3 y)-\zeta_3^2(x+\zeta_3^2 y)=x+y$$

implies that any common divisor of two among η, μ, and χ in $\mathbb{Z}[\zeta_3]$ also divides the third. Let $\pi'\in\mathbb{Z}[\zeta_3]$ be a prime common divisor of η,μ and χ, let us see that π' and π are associate elements in $\mathbb{Z}[\zeta_3]$. If $\pi'|y$ and $\pi'|x$ in $\mathbb{Z}[\zeta_3]$ so $N(\pi')|y^2$ and $N(\pi')|x^2$ in $\mathbb{Z}$ which is not possible since x and y are relatively prime in $\mathbb{Z}$ and $N(\pi')\neq\pm1$, therefore without loss of generality assume that $\pi'\nmid y$, since $\pi'|(x+y)$ then also $\pi'\nmid x$. Since $\pi'|\eta$ and $\pi'|\mu$ so $\pi'|\eta-\mu$ namely $\pi'|y\pi$ and since $\pi'\nmid y$ so $\pi'|\pi$, but π is a prime number in $\mathbb{Z}[\zeta_3]$, then $\pi'=u\pi$ where u is a unit of $\mathbb{Z}[\zeta_3]$.

Since π^2 and 3 are associates, $\pi^2|z$ and therefore there exist $m\in\mathbb{Z}_{\geq 2}$ such that $z=\pi^m z'$ and $\pi\nmid z'$, where $z'\in\mathbb{Z}[\zeta_3]$. Let $\eta',\mu',\chi'\in\mathbb{Z}[\zeta_3]$ such that $\eta=\pi\eta',\mu=\pi\mu'$ and $\chi=\pi\chi'$, then

$$-\zeta_3(\pi\mu')-\zeta_3^2(\pi\chi')=\pi\eta',$$

so

$$-\zeta_3(\mu')-\zeta_3^2(\chi')=\eta'. \tag{2.1}$$

Let us see that η' and μ' are relatively prime in $\mathbb{Z}[\zeta_3]$, then by equation (2.1) it follows that η',μ' and χ' are pairwise relatively prime in $\mathbb{Z}[\zeta_3]$. Since $(\pi\eta')-(\pi\mu')=\pi y$ and $(\pi\mu')-\zeta_3(\pi\eta')=\pi x$ then

$$\begin{aligned}\eta'-\mu'&=y\\ \mu'-\zeta_3\eta'&=x\end{aligned}$$

thus, if there were a prime element $\delta\in\mathbb{Z}[\zeta_3]$ such that $\delta|\eta',\mu'$ so $\delta|y,x$ and therefore $N(\delta)|y^2,x^2$ in $\mathbb{Z}$ which is impossible since x and y are relatively prime and $N(\delta)\neq\pm1$. Now note that as $\eta\in\mathbb{Z}$ and $\pi|\eta$ then $N(\pi)|\eta^2$ namely $3|\eta$, then $\pi^2|\eta$ and therefore $\pi|\eta'$. Since η', μ' and χ' are pairwise relatively prime,

$$(\pi^{3m-2}\eta'')(\pi\mu')(\pi\chi') = \pi^{3m}(z')^3 \qquad \text{for some} \quad \eta'' \in \mathbb{Z}[\zeta_3]$$

so

$$\eta''\mu'\chi' = (z')^3.$$

Moreover η'', μ' and χ' are pairwise relatively prime and $\mathbb{Z}[\zeta_3]$ is a unique factorization domain, then

$$\begin{aligned}\eta'' &= u_1\alpha_1^3\\ \mu' &= u_2\alpha_2^3\\ \chi' &= u_3\alpha_3^3\end{aligned}$$

such that $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}[\zeta_3]$ and $u_1, u_2, u_3 \in \mathbb{Z}[\zeta_3]^\times$. Therefore

$$\begin{aligned}\eta = x + y \quad &= \pi^{3m-2}u_1\alpha_1^3\\ \mu = x + \zeta_3 y \ &= \pi u_2\alpha_2^3\\ \chi = x + \zeta_3^2 y \ &= \pi u_3\alpha_3^3,\end{aligned}$$

hence

$$-\zeta_3(\pi u_2\alpha_2^3) - \zeta_3^2(\pi u_3\alpha_3^3) = \pi^{3m-2}u_1\alpha_1^3,$$

thus,

$$\alpha_2^3 + u_4\alpha_3^3 = \pi^{3(m-1)}u_5\alpha_1^3, \tag{2.2}$$

where u_4 and u_5 are units. let us recall that $m \geq 2$ and $3|\pi^2$, then

$$\alpha_2^3 + u_4\alpha_3^3 \equiv 0 \pmod{3\mathbb{Z}[\zeta_3]}$$

since π and α_3 are relatively prime in $\mathbb{Z}[\zeta_3]$, there exist $\theta, \beta \in \mathbb{Z}[\zeta_3]$ such that $3\theta + \alpha_3\beta = 1$, therefore

$$\alpha_3\beta \equiv 1 \pmod{3\mathbb{Z}[\zeta_3]}$$

thus,

$$u_4 \equiv u_4\alpha_3^3\beta^3 \equiv (-\alpha_2)^3\beta^3 (\text{mod } 3\mathbb{Z}[\zeta_3]),$$

if $-\alpha_2\beta = c + d\zeta_3$, then

$$(-\alpha_2)^3\beta^3 = (c^3 - 3cd^2 + d^3) + \zeta_3(3c^2d - 3cd^2),$$

then

$$u_4 \equiv c^3 + d^3 \pmod{3\mathbb{Z}[\zeta_3]}$$

now comes an important step that will eventually generalize to some special primes, if $u \in \mathbb{Z}[\zeta_3]^\times$ and $u \equiv a \pmod{3\mathbb{Z}[\zeta_3]}$ for some rational integer a, then $u = v^3$ for some $v \in \mathbb{Z}[\zeta_3]^\times$, this result can be easily verified because there are few units. Therefore the equation (2.2) becomes

$$\alpha_2^3 + (\alpha_3')^3 = \pi^{3(m-1)}u_5\alpha_1^3.$$

Thus, the equation

$$X^3 + Y^3 = \pi^{3k}UZ^3$$

with $U \in \mathbb{Z}[\zeta_3]^\times, (X, Y) = (X, Z) = (Y, Z) = 1, \pi \nmid X, Y, Z$ and $k \in \mathbb{Z}^+$, has solution in $\mathbb{Z}[\zeta_3]$.

Let us see that it suffices to consider the case $k = 1$. Suppose that $k \geq 2$ is a positive integer for which the equation is satisfied. Again, the above equation is factored as follows

$$(X + Y)(X + \zeta_3 Y)(X + \zeta_3^2 Y) = \pi^{3k}UZ^3$$

since π divides one of $\eta = X + Y$, $\mu = X + \zeta_3 Y$,$\chi = X + \zeta_3^2 Y$; π divides all of them since $\pi|(\mu - \chi)$ and $\pi|(\eta - \mu)$. Let $\eta', \mu', \chi' \in \mathbb{Z}[\zeta_3]$ such that $\eta = \pi\eta', \mu = \pi\mu'$ and $\chi = \pi\chi'$. Similarly to the above facts, we can prove that η', μ', and χ' are pairwise relatively prime. Furthermore, without loss of generality, we may assume $\eta = \pi^{3k-2}\eta''$ for some $\eta'' \in \mathbb{Z}[\zeta_3]$, since if for example $\pi|\mu'$ then we make the change to the associated element $Y^* = \zeta_3 Y$ and so $\mu = (X + Y^*) = \pi^{3k-2}\mu''$, similarly in the case $\pi|\chi$. Proceeding similarly to the previous arguments, we can find an equation of the form

$$(X')^3 + (Y')^3 = \pi^{3(k-1)} U'(Z')^3$$

so we can iteratively decrease to $k = 2$ and find a solution to the equation

$$(X + Y)(X + \zeta_3 Y)(X + \zeta_3^2 Y) = \pi^3 U Z^3$$

such that $U \in \mathbb{Z}[\zeta_3]^\times, (X, Y) = (X, Z) = (Y, Z) = 1$ and $\pi \nmid X, Y, Z$. We claim that this cannot happen. Proceeding similarly to the previous arguments $(X + Y), (X + \zeta_3 Y)$ and $(X + \zeta_3^2 Y)$ are multiples of π, in fact, π divides each of them exactly once. Since $(a + b\zeta_3)(1 - \zeta_3) = (a + b)(1 - \zeta_3) - b(1 - \zeta_3)^2$, $a + b \equiv 0, 1,$ or 2 (mod 3) and 3 and π^2 are associates, there are 2 distinct nonzero multiples of π module π^2, so we must have

$$X + Y \equiv X + \zeta_3 Y \pmod{\pi^2}, \quad X + Y \equiv X + \zeta_3^2 Y \pmod{\pi^2}, \quad \text{or} \quad X + \zeta_3 Y \equiv X + \zeta_3^2 Y \pmod{\pi^2}$$

therefore

$$(1 - \zeta_3)Y \equiv 0 \pmod{\pi^2}, \quad (-\zeta_3^2)(1 - \zeta_3)Y \equiv 0 \pmod{\pi^2}, \quad \text{or} \quad (\zeta_3)(1 - \zeta_3)Y \equiv 0 \pmod{\pi^2}$$

this congruences forces π to divide Y, contradiction. The theorem is proved. □

Now, let us consider the case $p = 5$ of Fermat's last theorem,

Theorem 2.3. *The equation*

$$x^5 + y^5 = z^5, \qquad \textit{with} \quad xyz \neq 0,$$

has no integer solutions.

Proof. For the sake of contradiction, let us assume there is a nontrivial solution (x, y, z) of $x^5 + y^5 = z^5$. Again, we may assume $x, y,$ and z are relatively prime. Similarly, we may assume that $5|xyz$ since otherwise if $5 \nmid x$ then $x^5 \equiv \pm 1, \pm 7 \pmod{25}$ and similarly for y and z. Consequently $x^5 + y^5 \equiv 2, 0, -2, 14, -14, 6, -6, 8$ or $-8 \pmod{25}$ but $z^5 \equiv \pm 1, \pm 7 \pmod{25}$, therefore $x^5 + y^5 \neq z^5$. However, we must stop at $p = 7$ since $1^7 + 30^7 \equiv 31^7 \pmod{49}$, then this method cannot be generalized.

Similarly, as in the case $n = 3$ without loss of generality we may assume $5|z$, therefore, from now on we will assume that $5|z$ but $5 \nmid x, y$.

Let ζ_5 be a primitive 5th root of unity, ζ_5 satisfies the equation $\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$. Let us try something more general, namely, the equation

$$X^5 + Y^5 = \pi^{5k} U Z^5, \qquad U \in \mathbb{Z}[\zeta_5]^\times, \quad \pi = 1 - \zeta_5, \quad \pi \nmid Z \quad \text{and} \quad k \in \mathbb{Z}^+$$

has no solutions in the ring $\mathbb{Z}[\zeta_5]$.

Let us see that it suffices to consider the case $k = 1$. Assume a solution such that $k \geq 2$. Similarly to the case $p = 3$, in the ring $\mathbb{Z}[\zeta_5]$ the above equation is factored as follows

$$(X + Y)(X + \zeta_5 Y)(X + \zeta_5^2 Y)(X + \zeta_5^3 Y)(X + \zeta_5^4 Y) = \pi^{5k} U Z^5. \tag{2.3}$$

Let $\alpha = a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3$ be a general element of $\mathbb{Z}[\zeta_5]$ and $\sigma_i : \zeta_5 \mapsto \zeta_5^i \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, the norm $N(\alpha) = \prod_{i=1}^4 \sigma_i(\alpha)$ is equal to the expression

$$\frac{1}{4}\left[\left[(ad+ca+db)+(ab+cb+dc)-2(a^2+b^2+c^2+d^2)\right]^2 - 5\left[(ad+ca+db)-(ab+cb+dc)\right]^2\right]$$

$\mathbb{Z}[\zeta_5]$ is a Euclidean Domain with the norm N (see page 15 in [1]). Therefore, as in the case $p = 3$, $\mathbb{Z}[\zeta_5]$ is endowed with a very important quality, that of being a unique factorization domain.

If $a = b = 0$ and $c = d = -1$ in the above expression then $N(\alpha) = 1$, by choosing $\zeta_5 = \frac{\sqrt{5}-1}{4} + i\sqrt{\frac{5+\sqrt{5}}{8}}$ we have

$$\varepsilon = -\zeta_5^2 - \zeta_5^3 = \frac{1+\sqrt{5}}{2}$$

is a unity such that $\varepsilon \neq \pm\zeta_5^r$. $\mathbb{Q}(\zeta_5)$ is a totally imaginary number field with $r_1 = 0$ real embedding and $r_2 = 2$ pairs of complex embeddings, since $\mathbb{Z}[\zeta_5]$ is the ring of integers of $\mathbb{Q}(\zeta_5)$ then by Dirichlet's unit theorem there is exactly $1 = r_1 + r_2 - 1$ fundamental unity, therefore

$$\mathbb{Z}[\zeta_5]^\times = \left\{ \pm\zeta_5^r \left(\frac{1+\sqrt{5}}{2}\right)^t : r, t \in \mathbb{Z} \right\}.$$

We may assume that X, Y and Z are pairwise relatively prime in $\mathbb{Z}[\zeta_5]$. Since $N(1-\zeta_5) = 5$ then π is a prime in $\mathbb{Z}[\zeta_5]$. Suppose that the equation (2.3) has solution for some $k \geq 2$, then, of course, π divides one of $\theta_0 = X + Y$, $\theta_1 = X + \zeta_5 Y$, $\theta_2 = X + \zeta_5^2 Y$, $\theta_3 = X + \zeta_5^3 Y$, $\theta_4 = X + \zeta_5^4 Y$. If $i > j$ then

$$\theta_j - \theta_i = \zeta_5^j(1 - \zeta_5^{i-j})Y$$
$$\zeta_5^j\theta_i - \zeta_5^i\theta_j = \zeta_5^j(1 - \zeta_5^{i-j})X$$

since π and $1 - \zeta_5^{i-j}$ are associates then π divides $\theta_0, \theta_1, \theta_2, \theta_3$ and θ_4. Let $\theta_0', \theta_1', \theta_2', \theta_3', \theta_4' \in \mathbb{Z}[\zeta_3]$ such that $\theta_0 = \pi\theta_0', \theta_1 = \pi\theta_1', \theta_2 = \pi\theta_2', \theta_3' = \pi\theta_3'$ and $\theta_4 = \pi\theta_4'$. Because

$$(\theta_j' - \theta_i')\pi = \zeta^j(1 - \zeta_5^{i-j})Y$$
$$(\zeta_5^j\theta_i' - \zeta_5^i\theta_j')\pi = \zeta_5^j(1 - \zeta_5^{i-j})X$$

the elements $\theta_0', \theta_1', \theta_2', \theta_3'$ and θ_4' are pairwise relatively prime, since otherwise X and Y are not relatively prime, which contradicts the choice of X and Y. Similarly to the case $p = 3$, without loss of generality, we may assume $\theta_0 = \pi^{5k-4}\theta_0''$ for some $\theta_0'' \in \mathbb{Z}[\zeta_5]$; since

$$\theta_0''\theta_1'\theta_2'\theta_3'\theta_4' = UZ^5$$

then

$$\theta_0'' = u_1\alpha_1^5$$
$$\theta_1' = u_2\alpha_2^5$$
$$\theta_4' = u_3\alpha_3^5$$

such that $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}[\zeta_5]$ and $u_1, u_2, u_3 \in \mathbb{Z}[\zeta_5]^\times$. Since $\theta_1 + \zeta_5\theta_4 = (1+\zeta_5)\theta_0$, then

$$(u_2\alpha_2^5\pi) + \zeta_5(u_3\alpha_3^5\pi) = (1+\zeta_5)\pi^{5k-4}u_1\alpha_1^5$$

since $1 + \zeta_5 = \frac{1-\zeta_5^2}{1-\zeta_5}$ is a unit, then

$$\alpha_2^5 + u_4\alpha_3^5 = \pi^{5(k-1)}u_5\alpha_1^5, \tag{2.4}$$

where u_4 and u_5 are units. Since π^4 and 5 are associates and $k \geq 2$, then

$$\alpha_2^5 + u_4\alpha_3^5 \equiv 0 \pmod{5\mathbb{Z}[\zeta_5]},$$

since π and α_3 are relatively prime in $\mathbb{Z}[\zeta_5]$, since $5 = \varepsilon\pi^4$, for some unit $\varepsilon \in \mathbb{Z}[\zeta_5])$, then 5 and α_3 are relatively prime, thus, there do exist $\gamma, \beta \in \mathbb{Z}[\zeta_5]$ such that $5\gamma + \alpha_3\beta = 1$, therefore

$$\alpha_3\beta \equiv 1 \pmod{5\mathbb{Z}[\zeta_5]},$$

thus,

$$u_4 \equiv u_4\alpha_3^5\beta^5 \equiv (-\alpha_2)^5\beta^5 \pmod{5\mathbb{Z}[\zeta_5]},$$

if $-\alpha_2\beta = c + d\zeta_5$, then

$$(-\alpha_2)^5\beta^5 \equiv c^5 + d^5 \pmod{5\mathbb{Z}[\zeta_5]},$$

then $u_4 \equiv a \pmod{5\mathbb{Z}[\zeta_5]}$ for some rational integer a. Again, now comes the big step, let us see that if $u \in \mathbb{Z}[\zeta_5]^\times$ and $u \equiv a \pmod{5\mathbb{Z}[\zeta_5]}$ for some rational integer a then $u = v^5$ for some $v \in \mathbb{Z}[\zeta_5]^\times$. We know that if $u \in \mathbb{Z}[\zeta_5]^\times$ then $u = \pm\zeta_5^r\varphi^t$ for some $r, t \in \mathbb{Z}$ and $\varphi = \frac{1+\sqrt{5}}{2}$, then $u \cdot \overline{u}^{-1} = \zeta_5^{2r}$, if $u \equiv a \pmod{5\mathbb{Z}[\zeta_5]}$ for some rational integer a then $\overline{u} \equiv a \pmod{5\mathbb{Z}[\zeta_5]}$ and consequently $\overline{u} \equiv u \pmod{5\mathbb{Z}[\zeta_5]}$, hence $1 \equiv u \cdot \overline{u}^{-1} \equiv \zeta_5^{2r} \pmod{5\mathbb{Z}[\zeta_5]}$, namely $1 - \zeta_5^{2r} \equiv 0 \pmod{5\mathbb{Z}[\zeta_5]}$, if $r \equiv 1, 2, 3, 4 \pmod 5$ then $1 - \zeta_5^{2r}$ and π are associates, therefore $1 - \zeta_5^{2r} \equiv 0 \pmod{5\mathbb{Z}[\zeta_5]}$ if and only if $r \equiv 0 \pmod 5$, so $u = \pm\varphi^t$, namely u is a real unit. The number φ is known as the golden ratio and satisfies $\varphi^2 = \varphi + 1$, note that

$$\begin{aligned}
\varphi^3 &= \varphi(\varphi + 1) = 2\varphi + 1,\\
\varphi^4 &= \varphi(2\varphi + 1) = 3\varphi + 2,\\
\varphi^5 &= \varphi(3\varphi + 2) = 5\varphi + 3,\\
\varphi^6 &= \varphi(5\varphi + 3) = 8\varphi + 5,
\end{aligned}$$

inductively, it can be shown that if $t \geq 1$ then $\varphi^t = F_t\varphi + F_{t-1}$ where $\{F_n\}_n$ is the Fibonacci Sequence, note that

$$-\varphi^{-1} = \frac{1-\sqrt{5}}{2} = -\zeta_5 - \zeta_5^4 = \sigma_3(-\zeta_5^2 - \zeta_5^3) = \sigma_3(\varphi),$$

therefore if $\left(\frac{1+\sqrt{5}}{2}\right)^t \equiv A \pmod{5\mathbb{Z}[\zeta_5]}$ for some rational integer A, then $\left(\frac{1-\sqrt{5}}{2}\right)^t \equiv A \pmod{5\mathbb{Z}[\zeta_5]}$, hence

$$\sqrt{5}F_t = \left(\frac{1+\sqrt{5}}{2}\right)^t - \left(\frac{1-\sqrt{5}}{2}\right)^t \equiv 0 \pmod{5\mathbb{Z}[\zeta_5]},$$

and then $\sqrt{5} = -1+2\varphi$ divides F_t, then $N(\sqrt{5}) = 5^2$ divides F_t^4, so 5 divides F_t in $\mathbb{Z}$. Using the recurrence relation for the Fibonacci numbers, it can be shown that $F_{t+5} = 5F_{t+1} + 3F_t$, then $F_{t+5} \equiv 3F_t \pmod 5$ and therefore $F_{20+j} \equiv 3F_{15+j} \equiv 3^2F_{10+j} \equiv 3^3F_{5+j} \equiv 3^4F_j \equiv F_j \pmod 5$, if $F_j \equiv 0 \pmod 5$ for $0 \leq j \leq 19$ then $j = 0, 5, 10, 15$. Therefore if $F_t \equiv 0 \pmod 5$ then $t \equiv 0 \pmod 5$, thus, $u = \pm\varphi^t = (\pm\varphi^l)^5$ for some non-negative integer l. For the case of a negative power of φ, we note that if $t \geq 1$

$$\left(\frac{1+\sqrt{5}}{2}\right)^t = (-1)^t\varphi^{-t},$$

then if φ^{-t} is congruent to a rational integer module 5, again, we can conclude that $t \equiv 0 \pmod 5$.

Therefore, continuing backwards through the above, the Equation (2.4) becomes

$$\alpha_2^5 + (\alpha_3')^5 = \pi^{5(k-1)}u_5\alpha_1^5.$$

Again, we can iteratively decrease to $k = 2$ and find a solution to the equation

$$(X+Y)(X+\zeta_5 Y)(X+\zeta_5^2 Y)(X+\zeta_5^3 Y)(X+\zeta_5^4 Y) = \pi^5 U Z^5$$

such that $U \in \mathbb{Z}[\zeta_5]^\times, (X,Y) = (X,Z) = (Y,Z) = 1$ and $\pi \nmid X, Y, Z$. We claim that this cannot happen. Proceeding similarly to the previous arguments, we find that $(X+Y), (X+\zeta_5 Y), (X+\zeta_5^2 Y), (X+\zeta_5^3 Y)$ and $(X+\zeta_5^4 Y)$ are multiples of π exactly once. Since

$$a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3 = a+b+c+d+[-b-c(1+\zeta_5)-d(1+\zeta_5+\zeta_5^2)](1-\zeta_5)$$

then $(a+b\zeta_5+c\zeta_5^2+d\zeta_5^3)(1-\zeta_5) \equiv (a+b+c+d)(1-\zeta_5) \pmod{(1-\zeta_5)^2}$, since $a+b+c+d \equiv 0, 1, 2, 3$ or $4 \pmod 5$, then, there are 4 distinct nonzero multiples of π module π^2, so we must have

$$X + \zeta_5^i Y \equiv X + \zeta_5^{i'} Y \pmod{\pi^2}$$

for some $0 \leq i < i' \leq 4$. Therefore $(1-\zeta_5^{i-i'})Y \equiv 0 \pmod{\pi^2}$. Since $1-\zeta_5^{i-i'}$ is a unit multiple of π, this congruence forces π to divide Y, this is a contradiction. The theorem is proved. □

These two proofs of Fermat's theorem for the primes 3 and 5 lead us to ask two important questions

I. Is $\mathbb{Z}[\zeta_p]$ always a unique factorization domain?

II. If $u \in \mathbb{Z}[\zeta_p]^\times$ is such that $u \equiv a \pmod p$ for some integer a, is u always a pth power?

Kummer answered these questions quite nicely. He proved that $\mathbb{Z}[\zeta_{23}]$ is not a unique factorization domain, in fact, Montgomery and Uchida proved (independently) that $\mathbb{Z}[\zeta_p]$ is a unique factorization domain exactly when $p \leq 19$, (see [11]). The purpose of the next section is to show that II is true for a special kind of prime number, which is due to Kummer.

2 Kummer's Lemma

Ernst Eduard Kummer made several contributions to mathematics in different areas, particularly his pioneering work on Fermat's Last Theorem. Specifically, Kummer developed in the 1840s a powerful theory of ideal factorization and used to prove Fermat's Last Theorem for the following special kind of prime number.

Definition 2.1 (Regular Prime)**.** *For a prime number p, we call p regular when the class number $h_p = h(\mathbb{Q}(\zeta_p))$ is not divisible by p.*

A prime p is called irregular if p divides h_p. We define the Bernoulli number B_n by the formula

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

In chapter 6 we shall prove Kummer's criterion, which states that p is irregular if and only if p divides the numerator of some B_k, $k = 2, 4, 6, ..., p-3$. The first few irregular primes are 37,59,67,101,103,131,149 and 157. It is known there are infinitely many irregular primes (see [18]), however, is still an open problem to show there are infinitely many regular primes. The purpose of this section is to present a proof by class field theory of the following property of the units of $\mathbb{Q}(\zeta_p)$ when p is regular.

Theorem 2.4 (Kummer's Lemma)**.** *Let p be a regular prime and $u \in \mathbb{Z}[\zeta_p]^\times$ with $u \equiv a \pmod p$ for some rational intenger a. Then $u = v^p$ for some $v \in \mathbb{Z}[\zeta_p]^\times$.*

Proof. Since $u^p \cdot (u^{p-1})^{-1} = u$ then u is a pth power if and only if u^{p-1} a pth power, note that $u^{p-1} \equiv a^{p-1} \equiv 1 \pmod{p}$, therefore we may assume without loss of generality that $u \equiv 1 \pmod{p}$.

Let $K = \mathbb{Q}(\zeta_p)$ and let $L = K(\sqrt[p]{u})$. Suppose $[L : K] > 1$. The polynomial $f(x) = x^p - u \in K[x]$ is factored as follows

$$f(x) = \prod_{i=0}^{p-1}(x - \zeta_p^i \sqrt[p]{u}),$$

therefore L is the splitting field of $f(x)$ over K, also L/K is an abelian extension of degree p. Let us see that L/K is unramified. Since K is a totally imaginary number field then L/K is unramified at all infinite primes. Let $i < j$, since the factors of discriminant of $f(x)$ are

$$\sqrt[p]{u}\zeta_p^i - \sqrt[p]{u}\zeta_p^j = \sqrt[p]{u}\zeta_p^i(1 - \zeta_p^{j-i}),$$

so the only prime which can possibly be ramified is $(1-\zeta_p)$, let us see that $(1-\zeta_p)$ is not ramified. We have that $u = 1 + p\beta$ for some $\beta \in \mathbb{Z}[\zeta_p]$, remember that $(1 - \zeta_p)^{p-1} = p\mathbb{Z}[\zeta_p]$ and $[\mathbb{Z}[\zeta_p]/(1 - \zeta_p) : \mathbb{Z}/p\mathbb{Z}] = 1$, hence $\beta = k + (1 - \zeta_p)\gamma$ for some integer k, for some $\gamma \in \mathbb{Z}[\zeta_p]$, therefore

$$u \equiv 1 + pk \pmod{p(1 - \zeta_p)},$$

so

$$\pm 1 = N_{K/\mathbb{Q}}(u) \equiv (1 + pk)^{p-1} \equiv 1 + \binom{p-1}{1} pk \equiv 1 - pk \pmod{p(1 - \zeta_p)}.$$

Note that if $N_{K/\mathbb{Q}}(u) = -1$ then $1 - \zeta_p$ divides -2, which is a contradiction, consequently $N_{K/\mathbb{Q}}(u) = 1$, then $1 - \zeta_p$ divides k, hence

$$u \equiv 1 \pmod{p(1 - \zeta_p)}$$

therefore $(1 - \zeta_p)^p$ divides $u - 1$, note that

$$u - 1 = \prod_{i=0}^{p-1}(\sqrt[p]{u} - \zeta_p^i)$$

then $(1 - \zeta_p)^p\mathcal{O}_L$ divides the product of ideals $\prod_{i=0}^{p-1}(\sqrt[p]{u} - \zeta_p^i)$. Suppose that $(1 - \zeta_p)$ is ramified in L, since L/K is Galois and $[L : K] = p$ then $(1-\zeta_p)$ must be totally ramified. Let $\mathfrak{P}$ be the prime of L lying above $(1 - \zeta_p)$, then $\mathfrak{P}^{p^2}$ divides $\prod_{i=0}^{p-1}(\sqrt[p]{u} - \zeta_p^i)$, by a combinatorial argument $\mathfrak{P}^p = (1 - \zeta_p)\mathcal{O}_L$ divides $(\sqrt[p]{u} - \zeta_p^{i_0})$ for some $0 \leq i_0 \leq p - 1$, since if $i \neq j$

$$(\sqrt[p]{u} - \zeta_p^j) - (\sqrt[p]{u} - \zeta_p^i) = -\zeta_p^j(1 - \zeta_p^{i-j})$$

then $(1 - \zeta_p)\mathcal{O}_L$ divides $(\sqrt[p]{u} - \zeta_p^i)$ for all i, therefore $\alpha = \frac{1-\sqrt[p]{u}}{1-\zeta_p} \in \mathcal{O}_L$, note that $L = K(\alpha)$ and α is a root of

$$F(x) = \frac{((1 - \zeta_p)x - 1)^p + u}{(1 - \zeta_p)^p}$$

its other roots are

$$\frac{1 - \zeta_p^i \sqrt[p]{u}}{1 - \zeta_p} = \frac{1 - \zeta_p^i}{1 - \zeta_p} + \zeta_p^i \cdot \frac{1 - \sqrt[p]{u}}{1 - \zeta_p} \in \mathcal{O}_L$$

Let $0 \leq n \leq p-1$, since $(1-\zeta_p)^p$ divides $\binom{p}{n}(1-\zeta_p)^{p-n}$ and $u-1$ in $\mathbb{Z}[\zeta_p]$, it is clear that L is the splitting field of $F(x)$ over K, note that if $i < j$ then

$$\frac{1 - \zeta_p^i \sqrt[p]{u}}{1 - \zeta_p} - \frac{1 - \zeta_p^j \sqrt[p]{u}}{1 - \zeta_p} = -\zeta_p^i \sqrt[p]{u} \cdot \frac{1 - \zeta_p^{j-i}}{1 - \zeta_p} \in \mathcal{O}_L^\times$$

so $(1 - \zeta_p)$ is not ramified in L, contradiction. Therefore L/K is unramified. Then $L \subseteq H$ where H is the Hilbert class field of K. By Theorem 1.1, $h_p = \#\mathrm{Gal}(H/K) = [H : K] = [H : L][L : K] = [H : L] \cdot p$, since p is regular, we have a contradiction. Therefore $[L : K] = 1$. The theorem is proved. □

3 First Case of Fermat's Last Theorem for regular primes

As mentioned in the previous section, Fermat's Last Theorem is true for regular primes. Let us recall that the case where p does not divide x,y, and z is called the first case of Fermat's Last Theorem, the second case, where p divides one of x,y,z. The greatest difference between the proofs of the first case and the second case for regular primes is the use of Kummer's Lemma in the second case.

We note the importance of a prime p being regular. Let $\mathfrak{a}$ be an ideal of $\mathbb{Z}[\zeta_p]$, if $\mathfrak{a}^p$ is principal, since p does not divide h_p then the class group of $\mathbb{Q}(\zeta_p)$ has no nontrivial elements of order p, this means $\mathfrak{a}$ is trivial in the class group, so $\mathfrak{a}$ is a principal ideal.

The purpose of this section is to prove the following fact.

Theorem 2.5. *Let p a regular prime. The equation*

$$x^p + y^p = z^p, \qquad (xyz, p) = 1$$

has no integer solutions.

Proof. Let us assume that there is a nontrivial solution (x, y, z) of $x^p + y^p = z^p$, with $(xyz, p) = 1$. The case $p = 3$ we have already verified, then we may assume that $p \geq 5$. Suppose $x \equiv y \equiv -z \pmod{p}$, then

$$x^p \equiv (-z)^p \pmod{p}$$
$$y^p \equiv (-z)^p \pmod{p}$$

so $3z^p = x^p + y^p + 2z^p \equiv 0 \pmod{p}$, which is a contradiction, hence $x \not\equiv -z \pmod{p}$ or $y \not\equiv -z \pmod{p}$. Therefore we may rewrite the equation if necessary (as $x^p + (-z)^p = (-y)^p$) to obtain $x \not\equiv y \pmod{p}$. We shall need this assumption later on. Also, we may assume x, y, and z are relatively prime, otherwise divide by the greatest common divisor.

In the ring $\mathbb{Z}[\zeta_p]$, the left-hand side of the above equation is factored as $\prod_{i=0}^{p-1}(x + \zeta_p^i y)$, considered the equation

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

as equality of ideals in $\mathbb{Z}[\zeta_p]$.

Lemma 2.1. *The ideals $(x + \zeta_p^i y)$, $i = 0, 1, ..., p - 1$, are pairwise relatively prime.*

Proof. Suppose $\mathfrak{p}$ is a prime ideal with $\mathfrak{p}|(x + \zeta_p^i y)$ and $\mathfrak{p}|(x + \zeta_p^j y)$, where $i \neq j$. Then $\mathfrak{p}|y\zeta_p^i(1 - \zeta_p^{j-i})$. Therefore $\mathfrak{p} = (1 - \zeta_p)$ or $\mathfrak{p}|y$, Similarly, $\mathfrak{p}$ divides $\zeta_p^j(x + \zeta_p^i y) - \zeta_p^i(x + \zeta_p^j y) = x\zeta_p^j(1 - \zeta_p^{i-j})$, so $\mathfrak{p} = (1 - \zeta_p)$ or $\mathfrak{p}|x$. If $\mathfrak{p} \neq (1 - \zeta_p)$ then $\mathfrak{p}|x$ and $\mathfrak{p}|y$, therefore $x, y \in \mathfrak{p} \cap \mathbb{Z}$, which is impossible since $(x, y) = 1$. Therefore $\mathfrak{p} = (1 - \zeta_p)$. In that case, $(1 - \zeta_p)$ is a factor of (z), so $z \in (1 - \zeta_p) \cap \mathbb{Z} = p\mathbb{Z}$, this leads to a contradiction, since we are assuming that $(p, z) = 1$. The result follows. □

Lemma 2.1 implies that $(x + \zeta_p^i y)$ must be the pth power of an ideal:

$$(x + \zeta_p^i y) = \mathfrak{a}_i^p, \qquad 0 \leq i \leq p - 1.$$

Since p is regular and $\mathfrak{a}_i^p$ is principal then $\mathfrak{a}_i$ is principal. Particularly, $\mathfrak{a}_1 = (\alpha)$ for some $\alpha \in \mathbb{Z}[\zeta_p]$, so $x + \zeta_p y = u\alpha^p$ for some unit u. Proposition 1.7 says that $u = \zeta_p^r u_1$ for some $r \in \mathbb{Z}$ and where u_1 is a real unit, so $\overline{u_1} = u_1$. It is easy to see that $\alpha^p \equiv a \pmod{p}$ for some rational integer a, therefore

$x + \zeta_p y = \zeta_p^r u_1 \alpha^p \equiv \zeta_p^r u_1 a \pmod{p}$. Taking complex conjugates we find that $x + \zeta_p^{-1} y \equiv \zeta_p^{-r} u_1 a \pmod{p}$, hence

$$\zeta_p^{-r}(x + \zeta_p y) \equiv u_1 a \equiv \zeta_p^r (x + \zeta_p^{-1} y) \pmod{p}$$

thus

$$x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \pmod{p}. \tag{2.5}$$

Now, we need the following lemma

Lemma 2.2. *Suppose $\beta = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$ with $a_i \in \mathbb{Z}$ and at least one $a_i = 0$. If $n \in \mathbb{Z}$ and n divides β then n divides each a_j.*

Proof. Let $a_{j_0} \in \{a_1, ..., a_{p-1}\}$ such that $a_{j_0} = 0$, then $\mathcal{B} = \{1, \zeta_p, ..., \zeta_p^{p-1}\} \backslash \{\zeta_p^{j_0}\}$ is a basis for $\mathbb{Z}[\zeta_p]$ as a $\mathbb{Z}-$module, so the other $a_j's$ give the coefficients with respect to $\mathcal{B}$. □

Since $p \geq 5$, if $1, \zeta_p, \zeta_p^{2r}, \zeta_p^{2r-1}$ are distinct, then by Lemma 2.2 p divides x and y, which is contrary to our original assumptions. Therefore, they are not distinct. Since $\zeta_p \neq 1$ and $\zeta_p^{2r} \neq \zeta_p^{2r-1}$, we have the following cases:

- $(\zeta_p^{2r} = 1)$. We have from (2.5) that

  $$\zeta_p y - \zeta_p^{p-1} y = \zeta_p y - \zeta_p^{-1} y \equiv 0 \pmod{p},$$

  by Lemma 2.2 p divides y, contradiction.

- $(\zeta_p^{2r-1} = 1$ or $\zeta_p^{2r} = \zeta_p)$. We have from (2.5) that

  $$(x - y) + \zeta_p(y - x) = x + \zeta_p y - \zeta_p x - y \equiv 0 \pmod{p},$$

  by Lemma 2.2 p divides $x - y$, which contradicts the choice of x and y made at the beginning of the proof.

- $(\zeta_p^{2r-1} = \zeta_p)$. We have from (2.5) that

  $$x - \zeta_p^2 x = x - \zeta_p^{2r} x \equiv 0 \pmod{p},$$

  again, by Lemma 2.2 p divides x, contradiction. The theorem is proved.

□

4 Second Case of Fermat's Last Theorem for regular primes

Assume that the equation $x^p + y^p = z^p$ has a solution in nonzero integers x, y, z with at least one number divisible by p. Again, we may assume that $(x, y) = (x, z) = (y, z) = 1$. Therefore we may rewrite the equation if necessary to obtain $p|z$ and $p \nmid x, y$. Writing $z = p^n z_0$, with $(z, z_o) = 1$ and $n \geq 1$, we have

$$x^p + y^p = u(1 - \zeta_p)^{(p-1)pn} z_0^p$$

for some $u \in \mathbb{Z}[\zeta_p]^\times$ and p not dividing xyz_o. Therefore $(1 - \zeta_p)$ does not divides xyz_o. As the proof of Fermat's Last Theorem for the cases $p = 3$ and $p = 5$ suggests, it is more convenient to prove a stronger result.

Theorem 2.6. *Let p be a regular prime. There do not exist $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_p]$, all nonzero, such that*

$$\alpha^p + \beta^p = u(1-\zeta_p)^{pk}\gamma^p$$

for some $u \in \mathbb{Z}[\zeta_p]^\times$, $n \in \mathbb{Z}^+$, $(1-\zeta_p)$ does not divide $\alpha\beta\gamma$, and $(\alpha), (\beta), (\gamma)$ pairwise comaximal ideals.

Proof. Let us see that it suffices to consider the case $k = 1$. Assume a solution such that $k \geq 2$. Consider the ideal equation

$$\prod_{i=0}^{p-1}(\alpha + \zeta_p^i\beta) = (1-\zeta_p)^{pk}(\gamma)^p.$$

Let $\theta_i = \alpha + \zeta_p^i\beta$, $\pi = 1-\zeta_p$. Since $k \in \mathbb{Z}^+$ then (π) divides at least one of the factors (θ_i). Let $i \neq j$, since π divides $\theta_i - \theta_j = (\alpha + \zeta_p^i\beta) - (\alpha + \zeta_p^j\beta)$ then (π) divides (θ_i), $0 \leq i \leq p-1$. Therefore $\theta_i = \theta_i'\pi$ for some $\theta_i' \in \mathbb{Z}[\zeta_p]$. Since

$$(\theta_j' - \theta_i')\pi = \zeta^j(1-\zeta_p^{i-j})\beta = (\text{unit})\pi\beta$$
$$(\zeta_p^j\theta_i' - \zeta_p^i\theta_j')\pi = \zeta_p^j(1-\zeta_p^{i-j})\alpha = (\text{unit})\pi\alpha$$

the ideals $(\theta_0'), ..., (\theta_{p-1}')$ are pairwise comaximal, since otherwise (β) and (α) are not pairwise comaximal ideals. Changing β to $\zeta_p^{i_0}\beta$ does not affect Fermat's equation, then without loss of generality, we may assume $(\theta_0) = (\pi)^{pk-(p-1)}(\theta_0'')$ for some $\theta_0'' \in \mathbb{Z}[\zeta_p]$, then

$$[(\pi)^{pk-(p-1)}(\theta_0'')][(\pi)(\theta_1')]\cdots[(\pi)(\theta_{p-1}')] = (\pi)^{pk}(\gamma)^p$$

so

$$(\theta_0'')(\theta_1')\cdots(\theta_{p-1}') = (\gamma)^p$$

the ideals $(\theta_0''), (\theta_1'), ..., (\theta_{p-1}')$ are pairwise comaximal, hence each one must be the pth power of an ideal:

$$\theta_0'' = \mathfrak{a}_0^p, \;\; \theta_1' = \mathfrak{a}_1^p, \;\ldots,\; \theta_{p-1}' = \mathfrak{a}_{p-1}^p$$

since p is regular, the ideal $\mathfrak{a}_i$ must be principal, in particular, $\mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_{p-1}$ are principal, therefore

$$\theta_0'' = u_1\gamma_*^p$$
$$\theta_1' = u_2\alpha_*^p$$
$$\theta_{p-1}' = u_3\beta_*^p$$

such that $\gamma_*, \alpha_*, \beta_* \in \mathbb{Z}[\zeta_5]$ and $u_1, u_2, u_3 \in \mathbb{Z}[\zeta_p]^\times$, note that

$$(\alpha + \zeta_p\beta) + \zeta_p(\alpha + \zeta_p^{p-1}\beta) = (1+\zeta_p)(\alpha+\beta)$$

where $1 + \zeta_p = \frac{1-\zeta_p^2}{1-\zeta_p}$ is a unity, then

$$(u_2\alpha_*^p\pi) + \zeta_p(u_3\beta_*^p\pi) = \pi^{pk-(p-1)}u_1'\gamma_*^p$$

so

$$\alpha_*^p + u_4\beta_*^p = \pi^{p(k-1)}u_5\gamma_*^p \tag{2.6}$$

where u_4 and u_5 are units. Since π^{p-1} and p are associates and $k \geq 2$, then

$$\alpha_*^p + u_4\beta_*^p \equiv 0 \pmod{p}.$$

As (π) and (β_*) are comaximal ideals, then the ideals $(p) = (\pi)^{p-1}$ and (β_*) are comaximal, thus, there do exist $\omega \in (p)$ and $\beta_*\lambda \in (\beta_*)$ such that $\omega + \beta_*\lambda = 1$, therefore

$$\beta_*\lambda \equiv 1 \pmod{p}$$

thus,

$$u_4 \equiv u_4\beta_*^p\lambda^p \equiv (-\alpha_*)^p\lambda^p \pmod{5}$$

since $(-\alpha_*\lambda)^p \equiv a \pmod 5$ for some rational integer a then $u_4 \equiv a \pmod 5$, by Kummer's Lemma $u_4 = v^p$ for some unit v, therefore, the Equation (2.6) becomes

$$\alpha_*^p + (\beta'_*)^p = \pi^{p(k-1)}u_5\gamma_*^p.$$

Again, we can iteratively decrease to $k = 2$ and find a solution to the equation

$$\prod_{i=0}^{p-1}(\alpha + \zeta_p^i\beta) = \alpha^p + \beta^p = u\pi^p\gamma^p$$

such that $u \in \mathbb{Z}[\zeta_p]^\times$, π does not divide $\alpha\beta\gamma$, and $(\alpha), (\beta), (\gamma)$ pairwise comaximal ideals. Let us see that cannot happen.

Proceeding similarly to the previous arguments, we find that the ideals $(\alpha + \zeta_p^i\beta)$, $0 \le i \le p-1$ are multiples of (π), however, in this case, are in fact multiples of (π) exactly once. Let

$$\xi = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$$

be a general element of $\mathbb{Z}[\zeta_p]$, note that

$$\xi = \overbrace{a_0 + a_1 + a_2 + \cdots + a_{p-1}}^{a} - a_1(1-\zeta_p) - a_2(1-\zeta_p^2) - \cdots - a_{p-2}(1-\zeta_p^{p-2}).$$

Let $1 \le i \le p-1$, remember that $1 - \zeta_p^i$ is a unit multiple of $1 - \zeta_p$, then

$$\xi\pi \equiv a\pi \pmod{\pi^2}$$

Since $|\mathbb{Z}[\zeta_p]/(1-\zeta_p)| = p$, there are $p-1$ distinct nonzero residues module π, therefore there are $p-1$ distinct nonzero multiples of π module π^2, so we must have

$$\alpha + \zeta_p^i\beta \equiv \alpha + \zeta_p^j\beta \pmod{\pi^2}$$

for some $0 \le i < j \le p-1$. Therefore $(1 - \zeta^{j-i})\beta \equiv 0 \pmod{\pi^2}$, namely (π) divides (β), contradiction. The theorem follows. □

Kummer revived Lamé's original approach to attempt solving Fermat's Last Theorem, proving it in the case when p is a regular prime by considering the p-part of the ideal class group. This p-part of the ideal class group lies at the heart of Iwasawa's theory, which we will explore in the next chapter.

Chapter 3

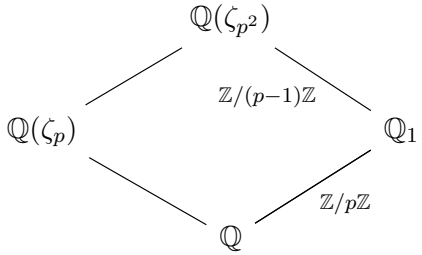
Iwasawa's Theory of $\mathbb{Z}_p$-extensions

Generalizing Kummer's ideas, the Japanese mathematician Kenkichi Iwasawa decided to study, instead of only the p-part of the class group of a number field K, the p-part of certain infinite tower extensions of it. Let us look at a prototype example of this, given by Iwasawa.

The fields $\mathbb{Q}(\zeta_{p^n})$, for every $n \geq 1$, form the following tower of number fields:

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_{p^2}) \subseteq \cdots \subseteq \mathbb{Q}(\zeta_{p^n}) \subseteq \cdots$$

The field $\mathbb{Q}(\zeta_{p^\infty}) := \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^n})$ is an example of an infinite extension of $\mathbb{Q}$, but it is not the "certain infinite tower extensions" we referred to previously. It is an infinite tower of extensions of certain subfields of $\mathbb{Q}(\zeta_{p^\infty})$, specifically, let $\mathbb{Q}_1$ be the subfield of $\mathbb{Q}(\zeta_{p^2})$ fixed by the unique normal subgroup $H \subset \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}) \cong \mathbb{Z}/(p-1)p\mathbb{Z}$ such that $|H| = p-1$, i.e., $\mathbb{Q}_1 = \mathbb{Q}(\zeta_{p^2})^H$. Therefore, $\mathbb{Q}_1/\mathbb{Q}$ is an abelian extension of degree p.



Now, let us generalize this construction as follows. Given that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \cong \mathbb{Z}/(p-1)p^n\mathbb{Z}$, we define $\mathbb{Q}_n$ as the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ fixed by the unique normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ of order $p-1$. Therefore, $\mathbb{Q}_n/\mathbb{Q}$ is such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$ and

$$\mathbb{Q} \subsetneq \mathbb{Q}_1 \subsetneq \mathbb{Q}_2 \subsetneq \cdots \subsetneq \mathbb{Q}_n \subsetneq \cdots \subsetneq \bigcup_{n\geq 1} \mathbb{Q}_n \subsetneq \mathbb{Q}(\zeta_{p^\infty}).$$

The extension $\mathbb{Q}_\infty := \bigcup_{n\geq 1} \mathbb{Q}_n$ of $\mathbb{Q}$ is an example of what we will refer to as a $\mathbb{Z}_p$-extension. One of the main purpose of this chapter is to prove a generalization of the following result.

Theorem 3.1 (Iwasawa, 1956)**.** *Let p^{e_n} be the exact power of p dividing the class number of $\mathbb{Q}_n$. Then there exist non-negative integers λ, μ and ν, all independent of n, and an integer n_0 such that*

$$e_n = \lambda n + \mu p^n + \nu \quad \textit{for all } n \geq n_0.$$

The Iwasawa theory has had a profound impact on our understanding of the arithmetic of number fields. This chapter is a brief review of this theory.

1 Infinite Galois Theory and Ramification Theory

It is well known that there are infinite Galois extensions in which some subgroups of the Galois group do not correspond to any intermediate subfield. To formulate a version of the fundamental theorem of Galois theory for the infinite case, it is necessary to equip the Galois group with an appropriate topology.

Let L/K be an algebraic extension of fields that is not necessarily finite, and assume it is also Galois (normal and generated by roots of separable polynomials). As usual, $G = \mathrm{Gal}(L/K)$ is the group of automorphisms of L which fix K pointwise. Suppose $K \subseteq F \subseteq L$ with F/K finite. Then $G_F = \mathrm{Gal}(L/F)$ is of finite index in G. The topology on G is defined by letting such G_F form a basis for the neighborhoods of the identity in G. Then G is profinite, and

$$G \cong \varprojlim G/G_F \cong \varprojlim \mathrm{Gal}(F/K),$$

where F runs through the normal finite subextensions F/K, or through any subsequence of such F such that $\bigcup F = L$. The ordering on the indices F is via inclusion ($F_1 \subseteq F_2$), and the maps used to obtain the inverse limit are the natural maps $\mathrm{Gal}(F_2/K) \to \mathrm{Gal}(F_1/K)$. The fundamental theorem of Galois theory now reads as follows:

There is a one-to-one correspondence between closed subgroups H of G and fields M with $K \subseteq M \subseteq L$:

$$\begin{aligned} \mathrm{Gal}(L/M) &\leftrightarrow M \\ H &\leftrightarrow \text{fixed field of } H. \end{aligned}$$

Open subgroups correspond to finite extensions, normal subgroups correspond to normal extensions, etc.

Example 3.1. Consider $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$. An element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is determined by its action on ζ_{p^n} for all $n \geq 1$. For each n, we have $\sigma\zeta_{p^n} = \zeta_{p^n}^{a_n}$ for some $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, and clearly $a_n \equiv a_{n-1} \mod p^{n-1}$. So, we obtain an element of

$$\mathbb{Z}_p^\times \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}).$$

Conversely, if $a \in \mathbb{Z}_p^\times$, then $\sigma_{\zeta_{p^n}} = \zeta_{p^n}^a$ defines an automorphism. The closed (and open) subgroup $1+p^n\mathbb{Z}_p$ corresponds to its fixed field $\mathbb{Q}(\zeta_{p^n})$.

Now, suppose that K is an algebraic extension of $\mathbb{Q}$, not necessarily of finite degree. Let $\mathcal{O}_K$ be the ring of all algebraic integers in K, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p. Therefore,

$$\mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z} + \mathfrak{p})/\mathfrak{p} \subseteq \mathcal{O}_K/\mathfrak{p}.$$

It can be shown that $\mathcal{O}_K/\mathfrak{p}$ is a field and is an algebraic extension of $\mathbb{Z}/p\mathbb{Z}$ (since $\mathcal{O}_K$ is integral over $\mathbb{Z}$). In fact, $\mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z}))$ is abelian since any finite extension of a finite field is cyclic, and an inverse limit of abelian groups is clearly abelian.

Let L/K be an algebraic extension, again not necessarily finite. Let $\mathfrak{P}$ be a nonzero prime ideal of $\mathcal{O}_L$, and let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, which is a prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_L/\mathfrak{P}$ is an extension of $\mathcal{O}_K/\mathfrak{p}$; in fact, it is an abelian extension since $\mathcal{O}_L/\mathfrak{P}$ is abelian over $\mathbb{Z}/p\mathbb{Z}$. Conversely, suppose we are given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. As in the finite case, there exists $\mathfrak{P}$ in $\mathcal{O}_L$ lying above $\mathfrak{p}$; that is, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

Proposition 3.1. *Suppose L/K is a Galois extension. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be primes of L lying above $\mathfrak{p}$. Then there exists $\sigma \in Gal(L/K)$ such that $\sigma\mathfrak{P} = \mathfrak{P}'$.*

We now want to discuss the ramification. However, $\mathcal{O}_K$ and $\mathcal{O}_L$ are not necessarily Dedekind domains, as they may fail to be Noetherian. This means that we cannot define ramification via factorization of primes. Instead, we use inertia groups. Let L/K be a Galois extension, as above, and let $\mathfrak{P}$ lie above $\mathfrak{p}$. Define the *decomposition group* by

$$Z = Z(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma\mathfrak{P} = \mathfrak{P}\}.$$

We have that Z is a closed subgroup. Now define the *inertia group* by

$$T = T(\mathfrak{P} \mid \mathfrak{p}) = \{\sigma \in Z \mid \sigma(\alpha) \equiv \alpha \mod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

We have that T is a closed subgroup. As with the case of finite extensions, we have an exact sequence

$$1 \to T \to Z \to \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) \to 1.$$

The surjectivity may be proved by using the fact that we have surjectivity for finite extensions.

Suppose now that L/K is an algebraic extension but not necessarily Galois. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Then $\overline{\mathbb{Q}}/L$ and $\overline{\mathbb{Q}}/K$ are Galois extensions. Let $\mathfrak{P}$ be a prime of L lying over the prime $\mathfrak{p}$ of K. Choose a prime ideal $\mathfrak{D}$ of $\mathcal{O}_{\overline{\mathbb{Q}}}$ lying above $\mathfrak{P}$. We have

$$\begin{aligned} T(\mathfrak{D} \mid \mathfrak{p}) &\subseteq \mathrm{Gal}(\overline{K}/K), \\ T(\mathfrak{D} \mid \mathfrak{P}) \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/L) &\subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/K), \\ T(\mathfrak{D} \mid \mathfrak{P}) &= T(\mathfrak{D} \mid \mathfrak{p}) \cap \mathrm{Gal}(\overline{\mathbb{Q}}/K). \end{aligned}$$

Define the *ramification index* by

$$e(\mathfrak{P} \mid \mathfrak{p}) = [T(\mathfrak{D} \mid \mathfrak{p}) : T(\mathfrak{D} \mid \mathfrak{P})],$$

which is possibly infinite. If $\mathfrak{D}'$ is another prime lying above $\mathfrak{P}$, then $\mathfrak{D}' = \sigma\mathfrak{D}$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, and

$$\begin{aligned} T(\mathfrak{D}' \mid \mathfrak{p}) &= \sigma T(\mathfrak{D} \mid \mathfrak{p})\sigma^{-1}, \\ T(\mathfrak{D}' \mid \mathfrak{P}) &= \sigma T(\mathfrak{D} \mid \mathfrak{P})\sigma^{-1}. \end{aligned}$$

Therefore the index $e(\mathfrak{P} \mid \mathfrak{p})$ does not depend on the choice of $\mathfrak{D}$. If L/K is Galois then there is the natural restriction map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Gal}(L/K),$$

with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$. The induced map $T(\mathfrak{D} \mid \mathfrak{p}) \to T(\mathfrak{P} \mid \mathfrak{p})$ is surjective, with kernel equal to $T(\mathfrak{D} \mid \mathfrak{P})$. Therefore

$$T(\mathfrak{D} \mid \mathfrak{p})/T(\mathfrak{D} \mid \mathfrak{P}) \cong T(\mathfrak{P} \mid \mathfrak{p}),$$

and

$$e(\mathfrak{P} \mid \mathfrak{p}) = |T(\mathfrak{P} \mid \mathfrak{p})|.$$

So the ramification index equals the order of the inertia group, for Galois extensions. It follows that the definition agrees with the usual one for finite extensions.

To consider infinite primes, we proceed slightly differently. Remember that an infinite prime of K is either an embedding $\phi : K \to \mathbb{R}$ or a pair of complex-conjugate embeddings $(\psi, \overline{\psi})$, with $\overline{\psi} \neq \psi$ and $\psi : K \to \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, any embedding ϕ or ψ may be extended to an embedding

$\overline{\mathbb{Q}} \to \mathbb{C}$ (use Zorn's lemma). In particular, we can extend to L. If L/K is Galois and ϕ_1 and ϕ_2 are two extensions of ϕ, then $\phi_2^{-1}\phi_1 \in \mathrm{Gal}(L/K)$. Hence $\phi_1 = \phi_2\sigma$ for some σ. If $(\psi_1, \overline{\psi_1})$ and $(\psi_2, \overline{\psi_2})$ extend ϕ, we have $\psi_1 = \psi_2\sigma$, hence $(\psi_1, \overline{\psi_1}) = (\psi_2, \overline{\psi_2})\sigma$, for some σ. A similar result holds for extensions of complex infinite primes, so the Galois group acts transitively on the extensions of a given infinite prime.

If L/K is Galois, w is an infinite prime of L, and v is an infinite prime of K below w, then we define

$$T(w \mid v) = Z(w \mid v) = \{\sigma \in \mathrm{Gal}(L/K) \mid w\sigma = w\}.$$

It is easy to see that T is nontrivial only when v is real, $w = (\psi, \overline{\psi})$ is complex, and $\sigma \neq 1$ is the "complex conjugation" $\psi^{-1}\overline{\psi}(= \overline{\psi^{-1}}\psi)$, which permutes ψ and $\overline{\psi}$ and has order 2. Therefore

$$|T(w/v)| = 1 \text{ or } 2.$$

2 Group Rings, Powers Series and the Structure of $\Lambda-$modules

The main goal of the next section is to prove Iwasawa's Theorem. Let $\Lambda = \mathbb{Z}_p[[T]]$. We first state some results about the structure of Λ and Λ-modules that are needed to prove the theorem. For the proof of these results, see sections 7.1 and 13.2, [18].

It is known that the ring of integers of $\mathbb{Q}_p$ is $\mathbb{Z}_p$. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Then $\mathcal{O}$ is a local ring. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$ and let π be a generator of $\mathfrak{p}$, so $(\pi) = \mathfrak{p}$. The ring $\mathcal{O}[[T]]$ can be endowed with the (π, T)-adic topology.

Let Γ be a multiplicative topological group isomorphic to the additive group $\mathbb{Z}_p$. Let γ be a fixed topological generator of Γ, i.e., the cyclic subgroup generated by γ is dense in Γ. Since the closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$, the closed subgroups of Γ are of the form Γ^{p^n}. Let $\Gamma_n = \Gamma/\Gamma^{p^n}$, so Γ_n is cyclic of order p^n, generated by the coset of γ.

Consider the group ring $\mathcal{O}[\Gamma_n]$. If $m \geq n \geq 0$ there is a natural map $\phi_{m,n} : \mathcal{O}[\Gamma_m] \to \mathcal{O}[\Gamma_n]$ induced by the map $\Gamma_m \to \Gamma_n$. Then

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

where the isomorphism is defined by

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

Since $(1+T)^{p^n} - 1$ divides $(1+T)^{p^m} - 1$ when $m \geq n \geq 0$, there is a natural map in the polynomial rings corresponding to $\phi_{m,n}$. If we take the inverse limit of the group rings $\mathcal{O}[\Gamma_n]$ with respect to the maps $\phi_{m,n}$, we get $\mathcal{O}[[\Gamma]]$, the so-called profinite group ring of Γ. The ring $\mathcal{O}[[\Gamma]]$ is the compactification of the profinite topological ring $\mathcal{O}[\Gamma]$ and contains certain "infinite sums" of elements of Γ. We have

$$\mathcal{O}[[\Gamma]] \cong \varprojlim \mathcal{O}[T]/((1+T)^{p^n} - 1).$$

Theorem 3.2. *$\mathcal{O}[[\Gamma]] \cong \mathcal{O}[[T]]$ as topological rings, with the isomorphism induced by $\gamma \mapsto 1 + T$.*

The case where $\mathcal{O} = \mathbb{Z}_p$ is of interest to us, and in this case, we have $\mathbb{Z}_p[[\Gamma]] \cong \Lambda$.

Proposition 3.2 (Division Algorithm)**.** *Let $f, g \in \mathcal{O}[[T]]$ and assume $f = a_0 + a_1T + \cdots$, with $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$, but $a_n \in \mathcal{O}^\times$. Then we may uniquely write*

$$g = qf + r,$$

where $q \in \mathcal{O}[[T]]$ and where $r \in \mathcal{O}[T]$ is a polynomial of degree at most $n-1$.

Definition 3.1. $P(T) \in \mathcal{O}[T]$ is called *distinguished* if

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

with $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$. (Note that $P(T)$ is almost an Eisenstein polynomial. But we allow $\pi^2 \mid a_0$, so we do not necessarily have irreducibility).

Theorem 3.3 (p-adic Weierstrass Preparation Theorem)**.** *Let*

$$f(T) = \sum_{i=0}^{\infty} a_i \, T^i \in \mathcal{O}[[T]],$$

and assume for some n we have $a_i \in \mathfrak{p}$, $0 \leq i \leq n-1$, but $a_n \notin \mathfrak{p}$ (so $a_n \in \mathcal{O}^\times$). Then f may be uniquely written in the form

$$f(T) = P(T)U(T),$$

where $U(T) \in \mathcal{O}[[T]]$ is a unit and $P(T)$ is a distinguished polynomial of degree n.
More generally, if $f(T) \in \mathcal{O}[[T]]$ is nonzero, then we may uniquely write

$$f(T) = \pi^\mu P(T)U(T)$$

with P and U as above and μ a non-negative integer.

Now, the following results tell us about the structure of the group ring Λ.

Lemma 3.1. *Λ is a UFD whose irreducible elements are p and the irreducible distinguished polynomials.*

Lemma 3.2. *Suppose $f, g \in \Lambda$ are relatively prime. Then the ideal (f, g) is of finite index in Λ.*

Lemma 3.3. *The prime ideals of Λ are 0, (p, T), (p) and the ideals $(P(T))$ where $P(T)$ is an irreducible distinguished polynomial. The ideal (p, T) is the unique maximal ideal.*

Lemma 3.4. *Let $f \in \Lambda$ with $f \notin \Lambda^\times$. Then $\Lambda/(f)$ is infinite.*

Definition 3.2. Two Λ-modules M and M' are said to be *pseudo-isomorphic*, written

$$M \sim M',$$

if there is a homomorphism $M \to M'$ with finite kernel and co-kernel. In other words, there is an exact sequence of Λ-modules

$$0 \to A \to M \to M' \to B \to 0$$

with A and B finite Λ-modules.

$M \sim M'$ does not imply $M' \sim M$. For example, $(p, T) \sim \Lambda$, obviously. But suppose $\Lambda \to (p, T)$. Let $f(T)$ be the image of $1 \in \Lambda$. Then the image of Λ is $(f) \subseteq (p, T)$. But $\Lambda/(f)$ is infinite, so $(p, T)/(f)$ is infinite. Hence, the cokernel is infinite. However, it can be shown that for finitely generated Λ-torsion Λ-modules, $M \sim M' \iff M' \sim M$.

We shall need to know the structure of finitely generated Λ-modules. The following theorem was first proved by Iwasawa in terms of the group ring $\mathbb{Z}_p[[\Gamma]]$. Serre was the one who noticed that the group ring is isomorphic to Λ.

Theorem 3.4 (Structure Theorem for Λ-modules)**.** *Let M be a finitely generated Λ-module. Then*

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

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

We define the *Iwasawa invariants* of the module M as

- $r(M) = \text{rank}_\Lambda(M) = r$, this is the Λ-rank of M.
- $\mu(M) = \sum n_i$, this is the *Iwasawa μ-invariant.*
- $\lambda(M) = \sum m_j \deg(f_j)$, this is the *Iwasawa λ-invariant.*

Proposition 3.3. *The Iwasawa invariants are well-defined.*

The ideal $char(M) := (\prod f_j^{m_j})(\prod p^{n_i})\Lambda$ is known as the *characteristic ideal* of M.

3 Iwasawa's Theorem

A $\mathbb{Z}_p$-extension of a number field K is an extension K_∞/K with

$$\text{Gal}(K_\infty/K) \cong \mathbb{Z}_p.$$

Let K_∞/K be a $\mathbb{Z}_p$-extension. The intermediate fields correspond to the closed subgroups of $\mathbb{Z}_p$. Since the only non-trivial closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$. Then, for each $n \geq 0$, there is a unique field K_n of degree p^n over K, and these K_n, plus K_∞, are the only fields between K and K_∞. Therefore, it is also possible to regard a $\mathbb{Z}_p$-extension as a sequence of fields

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

with

$$\text{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

We have the following results about the ramification in $\mathbb{Z}_p$-extensions.

Lemma 3.5. *Let K_∞/K be a $\mathbb{Z}_p$-extension and let l be a prime (possibly infinite) of K which does not lie above p. Then K_∞/K is unramified at l. In other words, $\mathbb{Z}_p$-extensions are "unramified outside p."*

Lemma 3.6. *Let K_∞/K be a $\mathbb{Z}_p-$extension. At least one prime ramifies in this extension, and there exist $n \geq 0$ such that every prime which ramifies in K_∞/K_n is totally ramified.*

Now we are ready to prove the following result.

Theorem 3.5 (Iwasawa, 1956)**.** *Let K_∞/K be a $\mathbb{Z}_p-$extension. Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exist non-negative integers λ, μ and ν, all independent of n, and an integer n_0 such that*

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

Proof. Let H_n be the Hilbert class field of K_n, so $\text{Gal}(H_n/K_n) \cong \text{Cl}(K_n)$. By group theory, we have $\text{Cl}(K_n) \cong A_n \oplus G_n$, where A_n is the unique p-Sylow subgroup of $\text{Cl}(K_n)$ and G_n is a subgroup of $\text{Cl}(K_n)$. Let $L_n = H_n^{G_n}$, so L_n/K_n is an unramified abelian extension of degree the exact power of p dividing the class number of K_n.

Definition 3.3 (p-extension)**.** We say that a Galois extension L/K is a p-extension if $\mathrm{Gal}(L/K)$ is a p-group, i.e., $|\mathrm{Gal}(L/K)| = p^n$ for some natural n.

Lemma 3.7. *L_n is the maximal unramified abelian p-extension of K_n.*

Proof. Let L' be an unramified abelian p-extension K_n. Let us see that $L' \subseteq L_n$. We have $L' \subseteq H_n$ and $|\mathrm{Gal}(L'/K)| = p^N$ for some N. Let $\sigma \in G_n$, for every $l \in L'$ we have that $\sigma^{p^N}(l) = (\sigma\big|_{L'})^{p^N}(l) = l$. Let a be the order of σ, since $(|G_n|, p) = 1$ then there exists an integer b such that $p^N b \equiv 1 \bmod a$. Therefore, $l = (\sigma^{p^N})^b(l) = \sigma(l)$, so $l \in H_n^{G_n} = L_n$. □

Lemma 3.8. *$L_n \subseteq L_{n+1}$ for every $n \geq 0$.*

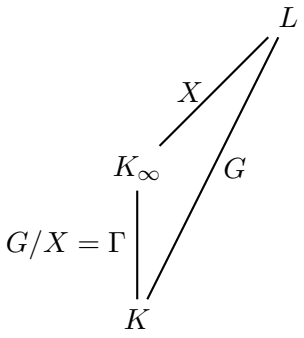
Proof. Since L_n/K_n is Galois, so $K_{n+1}L_n/K_{n+1}$ is also Galois. Since the homomorphism

$$\begin{aligned} \varphi : \mathrm{Gal}(K_{n+1}L_n/K_{n+1}) &\to \mathrm{Gal}(L_n/K_n) \\ \sigma \quad &\mapsto \quad \sigma\big|_{L_n}, \end{aligned}$$

has a trivial kernel then $K_{n+1}L_n/K_{n+1}$ is an abelian $p-$extension. Let us now see that $K_{n+1}L_n/K_{n+1}$ is unramified. Let $\mathfrak{P}$ be a finite prime of $K_{n+1}L_n$ and $\mathfrak{p} = \mathfrak{P} \cap K_{n+1}$. It is easy to see that if $\sigma \in I(\mathfrak{P}|\mathfrak{p})$ then $\sigma\big|_{L_n} \in I(\mathfrak{P} \cap L_n | \mathfrak{p} \cap K_{n+1})$. Since φ is injective and L_n/K_n is unramified then $I(\mathfrak{P}|\mathfrak{p})$ is trivial, therefore $K_{n+1}L_n/K_{n+1}$ is unramified at the finite primes. Now, let us see that $K_{n+1}L_n/K_{n+1}$ is unramified at the infinite primes. Suppose that $\phi : K_{n+1} \hookrightarrow \mathbb{R}$ is a real embedding such that ϕ ramifies in $K_{n+1}L_n$, namely, we can extend ϕ to $\tilde{\phi} : K_{n+1}L_n \hookrightarrow \mathbb{C}$. Thus, $\tilde{\phi}\big|_{K_n}$ is a real embedding, while $\tilde{\phi}\big|_{L_n}$ is a complex embedding, this is a contradiction because L_n/K_n is unramified. By Lemma 3.7, we have $K_{n+1}L_n \subseteq L_{n+1}$, therefore $L_n \subseteq L_{n+1}$.

□

Let $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Let γ_0 be a topological generator of Γ. Let $X_n = \mathrm{Gal}(L_n/K_n) \cong A_n$. Let $L = \bigcup_{n\geq 0} L_n$ and $X = \mathrm{Gal}(L/K_\infty)$. Each L_n is Galois over K, so L/K is also Galois. Let $G = \mathrm{Gal}(L/K)$. We have the following diagram:



The idea will be to make X into a Γ-module, hence a Λ-module. It will be shown to be finitely generated and Λ-torsion, hence pseudo-isomorphic to a direct sum of modules of the form $\Lambda/(p^k)$ and $\Lambda/(P(T)^k)$. We then transfer the result back to X to obtain the Iwasawa's theorem.

Remark. By Lemma 3.6, there exists an integer e such that all primes that ramify in K_∞/K_e are totally ramified. The fact that all ramified primes in K_∞/K_e are totally ramified proves to be quite convenient. Since $\mathrm{Gal}(K_\infty/K_e) \cong \Gamma^{p^e} \cong p^e\mathbb{Z}_p$ and $p^e\mathbb{Z}_p \cong \mathbb{Z}_p$ as additive groups, then K_∞/K_e is a $\mathbb{Z}_p-$extension, we can momentarily work with the extension K_∞/K_e and prove some results that apply to it.

Lemma 3.9. *Assume that all ramified primes in K_∞/K are totally ramified. Then X is a Γ-module.*

Proof. By our assumption,

$$K_{n+1} \cap L_n = K_n,$$

so

$$\mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_{n+1}/K_{n+1}),$$

which is a quotient of X_{n+1}. We have a map

$$X_{n+1} \to X_n.$$

This corresponds to the norm map $A_{n+1} \to A_n$ on ideal class groups. Observe that

$$X_n \cong \mathrm{Gal}(L_nK_\infty/K_\infty),$$

so

$$\varprojlim X_n \cong \varprojlim \mathrm{Gal}\left(\bigcup L_nK_\infty/K_\infty\right) = \mathrm{Gal}(L/K_\infty) = X.$$

Let $\gamma \in \Gamma_n = \Gamma/\Gamma^{p^n}$. Extend γ to $\tilde{\gamma} \in \mathrm{Gal}(L_n/K)$. Let $x \in X_n$. Then γ acts on x by

$$x^\gamma = \tilde{\gamma} x \tilde{\gamma}^{-1}.$$

Since $\mathrm{Gal}(L_n/K_n)$ is abelian, x^γ is well-defined. (This action corresponds to the action on A_n.) Therefore X_n becomes a $\mathbb{Z}_p[\Gamma_n]$-module. Representing an element of $X \cong \varprojlim X_n$ as a vector $(x_0, x_1, \dots)$, and letting $\mathbb{Z}_p[\Gamma_n]$ act on the n-th component, we easily find that X becomes a module over $\Lambda \cong \varprojlim \mathbb{Z}_p[\Gamma_n]$. (The only thing to be checked is that $x^\gamma \in X$, and this is easy to do.) The polynomial $1 + T \in \Lambda$ acts as $\gamma_0 \in \Gamma$. We have

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

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

□

Lemma 3.10. *Assume that all ramified primes in K_∞/K are totally ramified. Let G' be the closure of the commutator subgroup of G. Then*

$$G' = X^{\gamma_0 - 1} = TX.$$

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be the primes which ramify in K_∞/K, and fix a prime $\mathfrak{P}_i$ of L lying above $\mathfrak{p}_i$. Let $I_i \subseteq G$ be the inertia group. Since L/K_∞ is unramified,

$$I_i \cap X = 1.$$

Since K_∞/K is totally ramified at $\mathfrak{p}_i$,

$$I_i \hookrightarrow G/X = \Gamma$$

is surjective, hence bijective. So

$$G = I_iX = XI_i, \quad i = 1, \dots, s.$$

Let $\sigma_i \in I_i$ map to γ_0. Then σ_i must be a topological generator of I_i. Since

$$I_i \subseteq XI_1,$$

we have

$$\sigma_i = a_i\sigma_1$$

for some $a_i \in X$. Note that $a_1 = 1$. Since $\Gamma \cong I_1 \subseteq G$ maps onto $\Gamma = G/X$, we may lift $\gamma \in \Gamma$ to the corresponding element in I_1 in order to define the action of Γ on X. For simplicity, we identify Γ and I_1, so $x^\gamma = \gamma x \gamma^{-1}$. Let

$$a = \alpha x, \quad b = \beta y, \quad \text{with } \alpha, \beta \in \Gamma, \quad x, y \in X,$$

be arbitrary elements of $G = \Gamma X$. Then

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha (yx^{-1})^{\alpha\beta} (\alpha\beta) \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha (yx^{-1})^{\alpha\beta} (y^{-1})^\beta \quad \text{(since } \Gamma \text{ is abelian)} \\ &= (x^\alpha)^{1-\beta} (y^\beta)^{\alpha - 1}. \end{aligned}$$

Let $\beta = 1$, $\alpha = \gamma_0$. We find that $y^{\gamma_0 - 1} \in G'$, so

$$X^{\gamma_0 - 1} \subseteq G'.$$

For β arbitrary, there exists $c \in \mathbb{Z}_p$ with $\beta = \gamma_0^c$, so

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

Since $\gamma_0 - 1 = T$, $(x^\alpha)^{1-\beta} \in X^{\gamma_0 - 1}$. Similarly, $(y^\beta)^{1-\alpha} \in X^{\gamma_0 - 1}$. Since $X^{\gamma_0 - 1} = TX$ is closed (it is the image of the compact set X), $G' \subseteq X^{\gamma_0 - 1}$. This proves the lemma. □

Lemma 3.11. *Assume that all ramified primes in K_∞/K are totally ramified. Let Y_0 be the $\mathbb{Z}_p$-submodule of X generated by $\{a_i \mid 2 \le i \le s\}$ and by $X^{\gamma_0 - 1} = TX$. Let $Y_n = \nu_n Y_0$, where*

$$\nu_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1+T)^{p^n} - 1}{T}.$$

Then

$$X_n \cong X/Y_n \quad \text{for } n \ge 0.$$

Proof. First, consider $n = 0$. We have $K \subseteq L_0 \subseteq L$. Since L_0 is the maximal abelian unramified p-extension of K, and since 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 groups $I_i, 1 \le i \le s$. Therefore $\mathrm{Gal}(L/L_0)$ is the closure of the group generated by $X^{\gamma_0 - 1}, I_1,$ and $a_2, \ldots, a_s,$ so

$$X_0 = \mathrm{Gal}(L_0/K) = G/\mathrm{Gal}(L/L_0) = XI_1/\mathrm{Gal}(L/L_0) \cong X/\overline{\langle X^{\gamma_0 - 1}, a_2, \ldots, a_s \rangle} = X/Y_0.$$

Now, suppose $n \ge 1$. Replace K by K_n and γ_0 by $\gamma_0^{p^n}$. Then σ_i becomes $\sigma_i^{p^n}$. Observe that

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

Therefore

$$\sigma_i^{p^n} = (\nu_n a_i) \sigma_1^{p^n},$$

so a_i is replaced by $\nu_n a_i$. Finally, $X^{\gamma_0 - 1}$ is replaced by $(\gamma_0^{p^n} - 1)X = \nu_n X^{\gamma_0 - 1}$. Therefore Y_0 becomes $\nu_n Y_0$, which yields the desired result. This completes the proof.

□

The above result is a very crucial step since it allows us to retrieve information about X_n from information about X.

Lemma 3.12 (Nakayama's Lemma)**.** *Let X be a compact Λ-module. Then*

$$X \text{ is finitely generated over } \Lambda \iff X/(p,T)X \text{ is finite.}$$

If $x_1, \ldots, x_n$ generate $X/(p,T)X$ over $\mathbb{Z}$, then they also generate X as a Λ-module. A special case:

$$X/(p,T)X = 0 \iff X = 0.$$

Proof. Consider a small neighborhood U of 0 in X. Since $(p,T)^n \to 0$ in Λ, each $z \in X$ has a neighborhood U_z such that $(p,T)^n U_z \subseteq U$ for large n. Since X is compact, finitely many U_z cover X. Therefore $(p,T)^n X \subseteq U$ for large n, so $\bigcap((p,T)^n X) = 0$ for any compact Λ-module X.

Now assume $x_1, \ldots, x_n$ generate $X/(p,T)X$. Let $Y = \Lambda x_1 + \cdots + \Lambda x_n \subseteq X$. Then Y is compact (image of Λ^n), hence closed, so X/Y is a compact Λ-module. By assumption, $Y + (p,T)X = X$. Therefore

$$(p,T)(X/Y) = (Y + (p,T)X)/Y = X/Y,$$

hence

$$(p,T)^n(X/Y) = X/Y \quad \text{for all } n \geq 0.$$

It follows from the above that $X/Y = 0$, so $X = Y$ and $\{x_i\}$ generates X (this could also be proved more explicitly by successively considering $x \in X \mod (p,T)$, then $\mod (p,T)^2$, etc.). The other parts of the lemma follow easily.

□

Lemma 3.13. *Assume that all ramified primes in K_∞/K are totally ramified. $X = Gal(L/K_\infty)$ is a finitely generated Λ-module.*

Proof. Clearly $\nu_1 \in (p,T)$, so $Y_0/(p,T)Y_0$ is a quotient of $Y_0/\nu_1 Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$, which is finite. Therefore, Y_0 is finitely generated. Since $X/Y_0 = X_0$ is finite, X must also be finitely generated. This proves the lemma. □

Arbitrary K. We now remove the assumption. The Lemmas 3.11 and 3.13 apply to K_∞/K_e. In particular, X, which is the same for K_e and K, is a finitely generated Λ-module. For $n \geq e$,

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

This replaces ν_n for K_∞/K_e, since $\gamma_0^{p^e}$ generates $\mathrm{Gal}(K_\infty/K_e)$. Let Y_e be "Y_0 for K_e." Then

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

We have proved the following.

Lemma 3.14. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then X is a finitely generated Λ-module, and there exists $e \geq 0$ such that*

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

We can now apply the structure theorem of $\Lambda-$modules to X. We can also apply it to Y_e with the same answer, since X/Y_e is finite. So we have

$$Y_e \sim X \sim \Lambda^r \oplus \left(\bigoplus \Lambda/(p^{k_i})\right) \oplus \left(\bigoplus \Lambda/(f_i(T)^{m_i})\right).$$

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

1. $V = \Lambda$. By Lemma 3.4, $\Lambda/(\nu_{n,e})$ is infinite. Since $Y_e/\nu_{n,e}Y_e$ is finite, it follows easily that Λ does not occur as a summand.

2. $V = \Lambda/(p^k)$. In this case,
$$V/\nu_{n,e}V \simeq \Lambda/(p^k, \nu_{n,e}).$$
It is easy to show that if the quotient of two distinguished polynomials is a polynomial, then it is distinguished (or constant). Therefore
$$\nu_{n,e} = \frac{\nu_n}{\nu_e} = \frac{((1+T)^{p^n}-1)/T}{((1+T)^{p^e}-1)/T}.$$
is distinguished. 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. $V = \Lambda/(f(T)^m)$. Let $g(T) = f(T)^m$. Then g is also distinguished, say of degree d. Hence
$$T^d \equiv pQ(T) \mod g$$
for some polynomial $Q(T)$, so
$$T^k \equiv (p)(\text{polynomial}) \mod g \quad \text{for } k \geq d.$$
If $p^n \geq d$, then
$$(1+T)^{p^n} = 1 + (p)(\text{poly.}) + T^{p^n} \equiv 1 + (p)(\text{poly.}) \mod g.$$
Therefore,
$$(1+T)^{p^{n+1}} \equiv 1 + p^2(\text{poly.}) \mod g.$$
It follows that
$$\begin{aligned} P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 \\ &= ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}+1})((1+T)^{p^{n+1}} - 1) \\ &\equiv (1 + \cdots + 1 + (p^2)(\text{poly.}))(P_{n+1}(T)) \\ &= p(1 + (p)(\text{poly.}))P_{n+1}(T) \mod g. \end{aligned}$$
Since $1 + (p)(\text{poly.}) \in \Lambda^\times$,
$$\frac{P_{n+2}}{P_{n+1}} \quad \text{acts as } (p)(\text{unit}) \text{ on } V = \Lambda/(g),$$
for $p^n \geq d$. Assume $n_0 > e, p_0 > d$, and $n \geq n_0$. Then
$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}}{P_{n+1}},$$
and
$$\nu_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(\nu_{n+1,e}V) = p\nu_{n+1,e}V.$$

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

$$|pV/p\nu_{n+1,e}V| = |V/\nu_{n+1,e}V|.$$

Since

$$V/pV \simeq \Lambda/(p,g) = \Lambda/(p,T^d),$$

we have

$$|V/pV| = p^d.$$

By induction,

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

for $n \geq n_0 + 1$. If $V/\nu_{n,e}V$ is finite for all n, then

$$|V/\nu_{n,e}V| = p^{dn+c}, \quad n \geq n_0 + 1.$$

for some constant c. If $V/\nu_{n,e}V$ is infinite, then V cannot occur in our case. This happens only when $(\nu_n, e, f) \neq 1$.
Putting everything together, we obtain the following.

Proposition 3.4. *Suppose*

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

where each $g_j(T)$ 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

$$|E/\nu_{n,e}E| = p^{mp^n+ln+c}, \quad \textit{for all } n > n_0.$$

We have an exact sequence

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

where A and B are finite. We know the order of $E/\nu_{n,e}E$ for all $n > n_0$. It remains to obtain similar information about Y_e. At the moment, all we can conclude is that $e_n = mp^n + ln + c_n$, where c_n is bounded. The following lemma solves our problem.

Lemma 3.15. *Suppose Y and E are Λ-modules with $Y \sim E$ such that $Y/\nu_{n,e}Y$ is finite for all $n \geq e$. Then, for some constant c and some n_0,*

$$|Y/\nu_{n,e}Y| = p^c|E/\nu_{n,e}E| \quad \textit{for all } n \geq n_0.$$

Proof. We hace the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{n,e}Y & \longrightarrow & Y & \longrightarrow & Y/\nu_{n,e}Y & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & \nu_{n,e}E & \longrightarrow & E & \longrightarrow & E/\nu_{n,e}E & \longrightarrow & 0 \end{array}$$

There are the following inequalities.

(i) $|\ker \phi'_n| \leq |\ker \phi|$

(ii) $|\text{Coker } \phi'_n| \leq |\text{Coker } \phi|$

(iii) $|\text{Coker } \phi''_n| \leq |\text{Coker } \phi|$

(iv) $|\ker \phi'_n| \leq |\ker \phi| \cdot |\text{Coker } \phi|$

Inequality (i) is obvious. (iii) holds because representatives of Coker ϕ give representatives for Coker ϕ''_n. For (ii), multiply the representatives of Coker ϕ by $\nu_{n,e}$.
By the Snake Lemma, there is a long exact sequence

$$0 \to \ker \phi'_n \to \ker \phi \to \ker \phi''_n \to \text{Coker } \phi'_n \to \text{Coker } \phi \to \text{Coker } \phi''_n \to 0.$$

Everything is straightforward except the map $\ker \phi''_n \to \text{Coker } \phi'_n$. Let $x \in \ker \phi''_n$. There exists $y \in Y$ which maps to x. Since $\phi(y)$ maps to 0 in $E/\nu_{n,e}E$ by the commutativity of the diagram, we must have $\phi(y) \in \nu_{n,e}E$. One checks that $\phi(y) \mod \phi'_n(\nu_{n,e}Y)$ depends only on x. The map $x \mapsto \phi(y)$ is the desired one. It remains to check exactness. It follows that

$$|\ker \phi''_n| \leq |\ker \phi||\text{Coker } \phi'_n| \leq |\ker \phi||\text{Coker } \phi|,$$

by (ii). This proves (iv).
Now suppose $m \geq n \geq 0$. We have the following inequalities.

(a) $|\ker \phi'_n| \geq |\ker \phi'_m|$,

(b) $|\text{Coker } \phi'_n| \geq |\text{Coker } \phi'_m|$,

(c) $|\text{Coker } \phi''_n| \leq |\text{Coker } \phi''_m|$.

For (a), observe that $\nu_{m,e} = (\nu_{m,e}/\nu_{n,e})\nu_{n,e}$. Therefore $\nu_{m,e}Y \subseteq \nu_{n,e}Y$, so $\ker \phi'_m \subseteq \ker \phi'_n$. For (b), let $\nu_{m,e}y \in \nu_{m,e}E$. Let $z \in \nu_{n,e}E$ be a representative for $\nu_{n,e}y$ in Coker ϕ'_n. Then

$$\nu_{n,e}y - z = \phi(\nu_{n,e}x) \quad \text{for some } x \in Y.$$

Multiply by $\nu_{m,e}/\nu_{n,e}$ to obtain

$$\nu_{m,e}y - \left(\frac{\nu_{m,e}}{\nu_{n,e}}\right) z = \phi(\nu_{m,e}x) = \phi'_m(\nu_{m,e}x).$$

So $(\nu_{m,e}/\nu_{n,e})$ times representatives for Coker ϕ'_n gives representatives for Coker ϕ'_m. This proves (b). Since $\nu_{n,e}E \subseteq \nu_{n,e}E$, inequality (c) follows easily.
By (i), (ii), (iii), (a), (b), (c), the orders of $\ker \phi'_n$, Coker ϕ'_n, and Coker ϕ''_n are constant for $n \geq n_0$, for some n_0. It remains to treat $\ker \phi''_n$. By the Snake Lemma,

$$|\ker \phi'_n||\ker \phi''_n||\text{Coker } \phi| = |\ker \phi||\text{Coker } \phi'_n||\text{Coker } \phi''_n|.$$

(In any exact sequence, the alternating product of the orders is 1; proof: replace $0 \to A \to B \to \cdots$ by $0 \to B/A \to \cdots$ and use induction on the length of the sequence.) It follows that $|\ker \phi''_n|$ must be constant for $n \geq n_0$. □

We therefore have E, integers $\lambda \geq 0$, $\mu \geq 0$, and v, and an integer n_0 such that

$$\begin{aligned} p^{e_n} = |X_n| &= |X/Y_e||Y_e/\nu_{n,e}Y_e| \\ &= (\text{const.})|E/\nu_{n,e}E| \\ &= p^{\lambda n + \mu p^n + v}, \quad \text{for all } n > n_0. \end{aligned}$$

This completes the proof of the Iwasawa's Theorem. □

Chapter 4

Dedekind zeta function and $L-$functions

In 1837, Peter Gustav Lejeune Dirichlet proved the following result:

Theorem 4.1. *Let $(a, n) = 1$. Then there are infinitely many primes $p \equiv a \pmod{n}$.*

This theorem marked a significant milestone in number theory and is considered one of the first major results in analytic number theory. Dirichlet used analytic methods, including what are now called Dirichlet L-functions, to prove it.

In the present chapter, we shall introduce one of the most interesting algebraic invariants attached to a number field: the Dedekind zeta function, which encodes arithmetic data of the associated number field and plays a fundamental role in this thesis. Finally, we briefly review the L-functions, mainly because we will need to construct their p-adic analogues later on, and discuss how the p-adic L-functions are interpolated with the usual L-functions.

1 Class Number Formulas

Let K be an algebraic number field. The Dedekind zeta function $\zeta_K(s)$ is defined for complex numbers s with $\mathrm{Re}(s) > 1$ by the series:

$$\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{\|I\|^s},$$

where I ranges through the non-zero ideals of the ring of integers $\mathcal{O}_K$. Like the L-functions, the Dedekind zeta function converges absolutely for all complex numbers s with real part $\mathrm{Re}(s) > 1$. In a manner similar to the proof that L-functions have an Euler product, as we shall see in 2.2, one can prove that the Dedekind zeta function has one, given by the following

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \mathrm{Max}(O_K)} \left(1 - \|\mathfrak{p}\|^{-s}\right)^{-1}.$$

Also, the Dedekind zeta function satisfies the functional equation

$$A^s \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s) = A^{1-s} \Gamma\left(\frac{1-s}{2}\right)^{r_1} \Gamma(1-s)^{r_2} \zeta_K(1-s),$$

where $A = 2^{-r_2} \pi^{-N/2} \sqrt{|d_K|}$, $N = [K : \mathbb{Q}]$, r_1 is the number of real embeddings and r_2 is the number of pairs of complex embeddings.

Now, we present one of the most important results in number theory, which connects analytical aspects of the zeta function with some of the key invariants of the number field K.

Theorem 4.2 (Class Number Formula)**.** *Let $\zeta_K(s)$ be the Dedekind zeta function for the number field K, then*

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}(K)h_K}{W(K)\sqrt{|d_K|}}.$$

Theorem 4.3 (Class Number Formula II)**.** *The function $\zeta_K(s)$ has a zero of order $r = r_1 + r_2 - 1$ at $s = 0$ and*

$$\lim_{s\to 0} s^{-r}\zeta_K(s) = -\frac{\mathrm{Reg}(K)h_K}{W(K)}.$$

2 Dirichlet L-series

2.1 Dirichlet Characters and Gauss sums

A Dirichlet character is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Note that if $n|m$ then χ induces a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ by composition with the natural map $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. Thus, we can regard χ as being defined mod m or mod n. It is convenient to choose the minimal n for which χ can be defined and call it the conductor of χ, denoted f_χ. If the modulus and conductor are equal the character is *primitive*, otherwise *imprimitive*. The simplest possible character, $\chi_0 = 1$, called the *trivial character*, exists for all modulus n. Since this behavior is independent of the modulus n, the trivial character can be regarded as defined with conductor 1.

We shall always regard χ as being a primitive character unless otherwise stated. Additionally, we regard χ as a map $\mathbb{Z} \to \mathbb{C}$ by defining

$$\chi(a) = \begin{cases} 0 & \text{if } (a, f_\chi) \neq 1 \\ \chi(a \bmod f_\chi) & \text{if } (a, f_\chi) = 1. \end{cases}$$

Therefore, $\chi : \mathbb{Z} \to \mathbb{C}$ is periodic of period f_χ. Let χ and ψ be Dirichlet characters of conductors f_χ and f_ψ. We define the multiplication $\chi\psi$ as follows. Consider the homomorphism

$$\begin{aligned} \gamma : (\mathbb{Z}/lcm(f_\chi, f_\psi)\mathbb{Z})^\times &\to \mathbb{C}^\times \\ a &\to \chi(a)\psi(a). \end{aligned}$$

Then $\chi\psi$ is defined as the primitive character associated to γ. Let χ be any character and let $\psi = \bar{\chi}$ (complex conjugate). It is to see that if $(a, f_\chi) = 1$ then $\chi(a)$ is a $\phi(f_\chi)-$th root of unity. Therefore, $\psi(a) = \chi(a)^{-1}$ if $(a, f_\chi) = 1$. It follows that $\chi\overline{\chi}$ is the trivial character. Then it makes sense to consider groups of Dirichlet characters with a fixed modulus.
It is convenient to classify characters into two types: if $\chi(-1) = 1$ then χ is called even; if $\chi(-1) = -1$ then χ is called odd. We have the following properties of Dirichlet characters.

- If $(f_\chi, f_\psi) = 1$ then $f_{\chi\psi} = f_\chi f_\psi$.
- If χ is a nontrivial character, then
$$\sum_{a=1}^{f_\chi} \chi(a) = 0.$$

Since $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, it is natural to ask whether a Dirichlet character provides arithmetic information about subfields of $\mathbb{Q}(\zeta_n)$. Let us explore some results regarding the relationship between Dirichlet characters and the arithmetic of number fields. For the proof of these results, see Chapter 3, [18].

Let χ be a character mod n. Let K be the fixed field of the kernel of χ. Then $K \subseteq \mathbb{Q}(\zeta_n)$, and if n is minimal then $n = f_\chi$. The field K depends only on χ and is called the field belonging to χ. More generally, let X be a finite group of Dirichlet characters. Let n be the least common multiple of the conductors of the characters in X, so X is a subgroup of the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let H be the intersection of the kernels of these characters and let K be the fixed field of H. Then X is precisely the set of homomorphisms $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$. The field K is called the field belonging to X, and we have $[K : \mathbb{Q}] = |X|$; in fact, $X \cong \mathrm{Gal}(K/\mathbb{Q})$. If X is cyclic, generated by χ, then K is precisely the same as the field belonging to χ mentioned above.

We have the following statements: Let X_i correspond to K_i. Then

1. $X_1 \subseteq X_2 \iff K_1 \subseteq K_2$.
2. The group generated by X_1 and X_2 corresponds to the compositum K_1K_2.

Let $n = \prod p^a$. Corresponding to the decomposition

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod (\mathbb{Z}/p^a\mathbb{Z})^\times$$

we may write any character χ defined mod n as

$$\chi = \prod \chi_p$$

where χ_p is a character defined mod p^a. If X is a group of Dirichlet characters, then we let

$$X_p = \{\chi_p \mid \chi \in X\}.$$

Theorem 4.4. *Let X be a group of Dirichlet characters and K the associated field. Let p be a prime number with ramification index e in K. Then $e = \#(X_p)$.*

Corollary 4.4.1. *Let χ be a Dirichlet character and K the associated field. Then p ramifies in $K \iff \chi(p) = 0$ (equivalently $p \mid f_\chi$).*
More generally, let L be the field associated with a group X of Dirichlet characters. Then p is unramified in $L/\mathbb{Q} \iff \chi(p) \neq 0$ for all $\chi \in X$.

Theorem 4.5. *Let X be a group of Dirichlet characters, K the associated field. Let*

$$Y = \{\chi \in X \mid \chi(p) \neq 0\}, \quad Z = \{\chi \in X \mid \chi(p) = 1\}.$$

Then

$$e = [X : Y], \quad f = [Y : Z], \quad \text{and} \quad g = [Z : \{1\}]$$

are the ramification index for p in K, the residue class degree, and the number of primes lying above p, respectively. In fact,

$$X/Y \cong \text{the inertia group}, \quad X/Z \cong \text{the decomposition group}, \quad Y/Z \text{ is cyclic of order } f.$$

Proposition 4.1. *Let G be any finite abelian group. Then there exist fields L and K such that*

(a) $\mathrm{Gal}(L/K) \cong G$, *and*

(b) L/K *is unramified at all primes (including the Archimedean primes).*

We may also make $L/\mathbb{Q}$ *abelian and* $K/\mathbb{Q}$ *cyclic.*

The following corollary uses the existence of the Hilbert class field.

Corollary 4.5.1. *Given any finite abelian group* G*, there exists a cyclic extension* K *of* $\mathbb{Q}$ *such that the ideal class group of* K *contains a subgroup isomorphic to* G*.*

Let us recall that if K is a number field with r_2 pairs of complex embeddings, then $d_K =$ discriminant of K has sign $(-1)^{r_2}$.

Theorem 4.6 (Conductor–Discriminant Formula)**.** *Let* K *be the number field associated with the group* X *of Dirichlet characters. Then the discriminant of* K *is given by*

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

Now, we define the Gauss sum of a Dirichlet character χ as

$$\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a) e^{2\pi i a/f_\chi}.$$

Gauss sums are crucial in understanding character sums and for proving the quadratic reciprocity law. The following are key properties of Gauss sums

- For every integer b,
$$\sum_{a=1}^{f_\chi} \overline{\chi}(a) e^{2\pi i a b/f_\chi} = \chi(b)\tau(\overline{\chi}).$$
In particular,
$$\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi}).$$
- $|\tau(\chi)| = \sqrt{f_\chi}$.

2.2 Dirichlet $L-$Series

Let χ be a Dirichlet character of conductor f_χ. The $L-$series attached to χ is defined by

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

For $\chi = 1$, this is the usual Riemann zeta function. We shall prove that this function is analytic for $\mathrm{Re}(s) > 1$. Let $c > 1$. Note that when $\mathrm{Re}(s) \geq c$

$$\left|\frac{\chi(n)}{n^s}\right| = \frac{\left|\chi(n)\right|}{\left|n^s\right|} \leq \frac{1}{n^c},$$

since the series $\sum_{n=1}^{\infty} \frac{1}{n^c}$ converges, so $L(s,\chi)$ converges uniformly and absolutely in the domain $\mathrm{Re}(s) \geq c$. Recall that a uniform limit of analytic functions is analytic, and therefore $L(s,\chi)$ defines an analytic function for $\mathrm{Re}(s) > c$. This is true for every $c > 1$, hence $L(s,\chi)$ is analytic for $\mathrm{Re}(s) > 1$.

Let $\Gamma(s)$ be the gamma function, $W_\chi = \frac{\tau(\chi)}{\sqrt{f} i^\delta}$, and $\delta = 0$ if $\chi(-1) = 1$, $\delta = 1$ if $\chi(-1) = -1$. Dirichlet $L-$series satisfies the following functional equation

$$\left(\frac{f_\chi}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s,\chi) = W_\chi \left(\frac{f_\chi}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s,\bar{\chi}).$$

The functional equation may be rewritten as

$$\Gamma(s)\cos\left(\frac{\pi(s-\delta)}{2}\right) L(s,\chi) = \frac{\tau(\chi)}{2i^\delta}\left(\frac{2\pi}{f_\chi}\right)^s L(1-s,\overline{\chi}).$$

Therefore, Dirichlet $L-$series admits an analytic continuation to the whole complex plane, except for a simple pole at $s = 1$ when $\chi = 1$.

Like the Riemann zeta function, Dirichlet $L-$series has an Euler's product.

Proposition 4.2. *For* $\mathrm{Re}(s) > 1$ *one has a product representation*

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}},$$

where p runs through the prime numbers.

Proof. In order to prove the above identity, we remind ourselves that an infinite product $\prod_{k=1}^\infty z_k$ of complex numbers z_k is said to converge if the sequence of partial products $P_k = z_1 \cdots z_k$ has a nonzero limit. This is the case if and only if the series $\sum_{k=1}^\infty \log(z_k)$ converges, where log denotes the principal branch of the logarithm. The product is called absolutely convergent if the series converges absolutely. In this case, the product converges to the same limit even after a reordering of its terms z_k.

Let

$$E(s) = \prod_p \frac{1}{1-\chi(p)p^{-s}}.$$

If we formally take the logarithm, we obtain the series

$$\log E(s) = \sum_p \log\left(\frac{1}{1-\chi(p)p^{-s}}\right)$$

since

$$\log\left(\frac{1}{1-z}\right) = \sum_{k=1}^\infty \frac{z^k}{k},$$

hence

$$\log E(s) = \sum_p \sum_{k=1}^\infty \frac{(\chi(p))^k}{kp^{sk}}.$$

Let $c > 1$. If $\mathrm{Re}(s) \geq c$ then

$$\left|\frac{(\chi(p))^k}{kp^{sk}}\right| \leq \frac{1}{p^{ck}} = \left(\frac{1}{p^c}\right)^k$$

therefore

$$\sum_p \sum_{k=1}^\infty \left|\frac{(\chi(p))^k}{kp^{sk}}\right| \leq \sum_p \sum_{k=1}^\infty \left(\frac{1}{p^c}\right)^k \leq \sum_p \frac{1}{p^c - 1} \leq 2\sum_p \frac{1}{p^c}.$$

This implies the absolute convergence of the product

$$E(s) = \exp\left(\sum_p \sum_{k=1}^{\infty} \frac{(\chi(p))^k}{kp^{sk}}\right).$$

In this product, we now expand the product of the factors

$$\frac{1}{1-\chi(p)p^{-s}} = 1 + \frac{\chi(p)}{p^s} + \frac{(\chi(p))^2}{p^{2s}} + \frac{(\chi(p))^3}{p^{3s}} + \cdots$$

Let $N \geq 0$ be a natural number, for all prime numbers $p_1, p_2, ..., p_r \leq N$, since χ is completely multiplicative we have

$$\prod_{p\leq N} \frac{1}{1-\chi(p)p^{-s}} = \sum_{\nu_1,\ldots,\nu_r=0}^{\infty} \frac{\chi(p_1^{\nu_1}\cdots p_r^{\nu_r})}{(p_1^{\nu_1}\cdots p_r^{\nu_r})^s} = \sum_{n:\,\text{If}\,p|n\Rightarrow p\leq N} \frac{\chi(n)}{n^s}$$

where the right-hand side is a sum over all natural numbers which are divisible only by primes numbers $p \leq N$. For all natural number n such that $p|n$ and $p > N$ we have that $n > N$, therefore

$$\left|L(s,\chi) - \prod_{p\leq N} \frac{1}{1-\chi(p)p^{-s}}\right| \leq \left|\sum_{\substack{n>N\\ p_i\nmid n}} \frac{\chi(n)}{n^s}\right| \leq \sum_{\substack{n>N\\ p_i\nmid n}} \left|\frac{\chi(n)}{n^s}\right| \leq \sum_{n>N} \frac{1}{n^c}$$

where the right-hand side goes to zero as $N \to \infty$ because it is the remainder of a convergent series. This proves the proposition.

□

In view of the proposition proved above, it follows that $L(s,\chi) \neq 0$ for $\text{Re}(s) > 1$. It is also true that $L(1,\chi) \neq 0$, but this is a deeper fact which will be proved later.

It is in our interest to give the number $L(1-n,\chi)$ explicitly. For this, we need the generalized Bernoulli numbers. The ordinary Bernoulli numbers B_n are defined by

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

The generalized Bernoulli numbers $B_{n,\chi}$ are defined by

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

Note that when $\chi = 1$ we have

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

so $B_{n,1} = B_n$ except for $n = 1$, when we have $B_{1,1} = \frac{1}{2}$, $B_1 = -\frac{1}{2}$. Since the power series expansion of $\frac{te^{at}}{e^{f_\chi t}-1}$ has constant term equal to 1, then

$$B_{0,\chi} = \sum_{a=1}^{f_\chi} \chi(a).$$

Observe that if $\chi \neq 1$ then $B_{0,\chi} = 0$.

We define Bernoulli polynomials $B_n(X)$ by

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

Since

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

we obtain that $B_n(1-X) = (-1)^n B_n(X)$.

Since $\frac{t}{e^t-1} = \sum B_n \frac{t^n}{n!}$ and $e^{Xt} = \sum X^n \frac{t^n}{n!}$, we have

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}.$$

Proposition 4.3. *Let F be any multiple of f_χ. Then*

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

Proof. To begin, we observe that

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

Let $g = F/f_\chi$ and $a = b + cf_\chi$. Then we have

$$\sum_{b=1}^{f_\chi}\sum_{c=0}^{g-1}\chi(b)\frac{te^{(b+cf_\chi)t}}{e^{f_\chi gt}-1} = \sum_{b=1}^{f_\chi}\chi(b)\frac{te^{bt}}{e^{f_\chi t}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}.$$

This proves the proposition. □

In particular, if $n = 1$ and $F = f_\chi$; $B_1(X) = X - \frac{1}{2}$ and therefore

$$B_{1,\chi} = \sum_{a=1}^{f_\chi}\chi(a)\frac{a}{f_\chi} - \frac{1}{2}\underbrace{\sum_{a=1}^{f_\chi}\chi(a)}_{0} = \frac{1}{f_\chi}\sum_{a=1}^{f_\chi}\chi(a)a, \quad \chi \neq 1.$$

It is easy to see that the defining relation for the $B_{n,\chi}$ is an even function of t when χ is even and odd when χ is odd. Therefore

$$B_{n,\chi} = 0 \quad \text{if} \quad n \not\equiv \delta \pmod 2,$$

with the usual exception $B_{1,1} = \frac{1}{2}$ (or $B_1 = -\frac{1}{2}$). We define the Hurwitz zeta function

$$\zeta(s,b) = \sum_{m=0}^{\infty}\frac{1}{(b+m)^s}, \quad \mathrm{Re}(s) > 1, \quad 0 < b \leq 1.$$

note that

$$L(s,\chi)=\sum_{a=1}^{f_\chi}\sum_{m=0}^{\infty}\frac{\chi(a+f_\chi m)}{(a+f_\chi m)^s}=\sum_{a=1}^{f_\chi}\sum_{m=0}^{\infty}\frac{\chi(a)}{(f_\chi)^s\left(\frac{a}{f_\chi}+m\right)^s}=\sum_{a=1}^{f_\chi}\chi(a)f_\chi^{-s}\zeta\left(s,\frac{a}{f_\chi}\right).$$

We are now able to prove the following result.

Theorem 4.7. *$L(1-n,\chi)=-B_{n,\chi}/n$, $n\geq 1$. More generally, $\zeta(1-n,b)=-B_n(b)/n$, $0<b\leq 1$.*

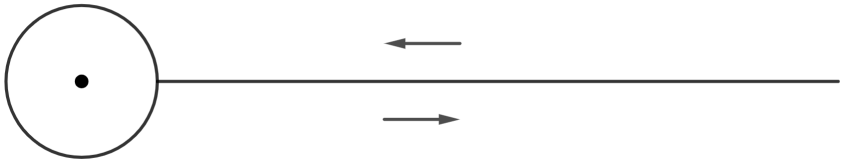
Proof. Let

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

Define

$$H(s)=\int_{\gamma_\varepsilon}F(z)z^{s-2}\,dz,$$

where $\gamma_\varepsilon=(\infty,\varepsilon]+C_\varepsilon+[\varepsilon,\infty)$ and $C_\varepsilon=\{z:|z|=\varepsilon\}$ is oriented in the positive direction:



Here, the integrals over $(\infty,\varepsilon]$ and $[\varepsilon,\infty)$ do not cancel each other because we must regard $z^s=\exp(s\log(z))$ as a multivalued function. The integration takes place on the universal covering of $\mathbb{C}^*$,

$$X=\{(z,\theta)\in\mathbb{C}^*\times\mathbb{R}:\arg(z)\equiv\ \theta \bmod 2\pi\}.$$

Then we can take log as $\ln|z|$ on $(\infty,\varepsilon]$ and $\ln|z|+2\pi i$ on $[\varepsilon,\infty)$. $H(s)$ is defined and analytic for all s. We may write

$$H(s)=(e^{2\pi is}-1)\int_\varepsilon^\infty F(t)t^{s-2}\,dt+\int_{C_\varepsilon}F(z)z^{s-2}\,dz.$$

We want to find a functional equation for $H(s)$, so we first assume that $\mathrm{Re}(s)>1$. Then, if $\mathrm{Re}(s)>1$, it is easy to see that

$$\int_{C_\varepsilon}F(z)z^{s-2}\,dz\to 0\ \text{ as }\ \varepsilon\to 0,$$

since $H(s)$ is holomorphic on X, it is independent of ε, and therefore

$$\begin{aligned}H(s)&=(e^{2\pi is}-1)\int_0^\infty F(t)t^{s-2}\,dt\\&=(e^{2\pi is}-1)\int_0^\infty t^{s-1}\sum_{m=0}^{\infty}e^{-(b+m)t}\,dt\\&=(e^{2\pi is}-1)\sum_{m=0}^{\infty}\int_0^\infty t^{s-1}e^{-(b+m)t}\,dt\\&=(e^{2\pi is}-1)\sum_{m=0}^{\infty}\frac{1}{(m+b)^s}\Gamma(s)\\&=(e^{2\pi is}-1)\Gamma(s)\zeta(s,b).\end{aligned}$$

By the Fubini–Tonelli theorem, the interchange of summation and integration is justified because

$$\sum_{m=0}^{\infty} \int_0^{\infty} |t^{s-1} e^{-(b+m)t}| \, dt < \infty$$

Therefore

$$\frac{H(s)}{(e^{2\pi i s} - 1)\Gamma(s)} = \zeta(s, b)$$

which by analytic continuation holds for all $s \neq 1$. Incidentally, this gives the analytic continuation of $\zeta(s, b)$. Therefore, if $s = 1 - n$, where $n \geq 1$, then $e^{2\pi i s} = 1$, so

$$H(1-n) = \int_{C_\varepsilon} F(z) z^{-n-1} dz = (2\pi i) \frac{B_n(1-b)}{n!}.$$

Also, note that

$$\lim_{s \to 1-n} \left(e^{2\pi i s} - 1\right) \Gamma(s) = \frac{(2\pi i)(-1)^{n-1}}{(n-1)!}.$$

Thus,

$$\zeta(1-n, b) = (-1)^{n-1} \frac{B_n(1-b)}{n} = -\frac{B_n(b)}{n}.$$

Consequently

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

This completes the proof.

□

Below, we illustrate a connection between the L-functions and the Dedekind zeta function.

Theorem 4.8. *Let X be a group of Dirichlet characters, K the associated field, and $\zeta_K(s)$ the Dedekind zeta function of K. Then*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

Proof. It suffices to consider the Euler factors corresponding to each prime p. Suppose

$$(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$$

is the prime factorization of p in K, and each $\mathfrak{P}$ has residue class degree f, $\|\mathfrak{P}\| = p^f$. Then $\zeta_K(s)$ contains the factor

$$\prod_{\mathfrak{P}|p} \left(1 - \|\mathfrak{P}\|^{-s}\right)^{-1} = (1 - p^{-fs})^{-g}.$$

The L-series gives us $\prod_{\chi \in X} (1 - \chi(p) p^{-s})^{-1}$. Those χ with $\chi(p) = 0$ do not contribute, so we ignore them. Since Y/Z is cyclic of order f, where Y is the group of those $\chi \in X$ with $\chi(p) \neq 0$, and Z consists of those with $\chi(p) = 1$. As χ runs through a set of coset representatives for Y/Z, $\chi(p)$ runs through all fth roots of unity. Each coset has g elements. Since

$$\prod_{a=0}^{f-1} \left(1 - \zeta_f^a p^{-s}\right) = (1 - p^{-fs}),$$

the result follows. □

Corollary 4.4. $L(1, \chi) \neq 0$.

Proof. Let K be the field belonging to χ. It is well known that the zeta function of K has a (simple) pole at $s = 1$. Let b be the order of χ. Then

$$\zeta_K(s) = \prod_{a=0}^{b-1} L(s, \chi^a) = \zeta(s) \cdot \prod_{a=1}^{b-1} L(s, \chi^a).$$

Since $\zeta(s)$ has only a simple pole at $s = 1$, none of the factors $L(s, \chi^a)$ can vanish at $s = 1$. This completes the proof. □

3 Hecke L-series

Let K be a number field and let $\mathfrak{m}$ be a modulus of K, which is a formal product of prime ideals of $\mathcal{O}_K$ and infinite real prime of K. Let $I_{\mathfrak{m}}(K)$ denote the group of fractional ideals of K that are coprime to $\mathfrak{m}$. Let $P^+_{\mathfrak{m}}(K)$ denote the group of principal ideals generated by elements of $K^\times$ that are:

- Congruent to 1 mod $\mathfrak{m}$ at the prime ideals dividing $\mathfrak{m}$,
- Positive at all infinite real primes of K.

The *narrow ray class group* modulo $\mathfrak{m}$ is the quotient:

$$\mathrm{Cl}^+_{\mathfrak{m}}(K) = \frac{I_{\mathfrak{m}}(K)}{P^+_{\mathfrak{m}}(K)}.$$

A *Hecke Character* χ modulo $\mathfrak{m}$ (also called a *Grössencharakter*) of the narrow ray class group is a homomorphism:

$$\chi : I_{\mathfrak{m}}(K) \to \mathbb{C}^\times$$

satisfying the following conditions:

1. Multiplicativity: For any two fractional ideals $\mathfrak{a}, \mathfrak{b} \in I_{\mathfrak{m}}(K)$,

   $$\chi(\mathfrak{a} \cdot \mathfrak{b}) = \chi(\mathfrak{a}) \cdot \chi(\mathfrak{b}).$$

2. Compatibility with Principal Ideals: If $\alpha \in K^\times$ generates a principal ideal (α), and $\alpha \equiv 1 \mod \mathfrak{m}$ and α is positive at all real places of K, then

   $$\chi((\alpha)) = 1.$$

   This ensures that the Hecke character factors through the narrow ray class group $\mathrm{Cl}^+_{\mathfrak{m}}(K)$.

A Hecke character can also be extended to an infinite part to deal with the real and complex infinite primes of K. For an element $\alpha \in K^\times$, this archimedean component often takes the form:

$$\chi((\alpha)) = \prod_{\sigma} \sigma(\alpha)^{s_\sigma},$$

where σ runs over the real embeddings and complex embeddings of K, and s_σ is a complex parameter associated with each embedding. This part captures the behavior of α at the real and complex infinite primes.

A Hecke character can typically be factored into two components:

- A *finite part*, which is defined in terms of the narrow ray class group and only depends on the prime ideals of $\mathcal{O}_K$,
- An *infinite part*, which deals with the behavior at real and complex infinte primes of K as described above.

Let χ be a Hecke character of the narrow ray class group $\mathrm{Cl}^+_{\mathfrak{m}}(K)$ for some modulus $\mathfrak{m}$ of K. The complex *Hecke L-function* attached to χ is given by

$$L_K(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\|\mathfrak{a}\|^s}, \qquad \mathrm{Re}(s) > 1.$$

where $\mathfrak{a}$ varies over the integral ideals of K and we put $\chi(\mathfrak{a}) = 0$ whenever $(\mathfrak{a}, \mathfrak{m}) \neq 1$.

Proposition 4.4. *The L-series $L_K(s,\chi)$ converges absolutely and uniformly in the domain* $\mathrm{Re}(s) > 1$*, and one has*

$$L_K(s,\chi) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\|\mathfrak{p}\|^{-s}},$$

where $\mathfrak{p}$ varies over the prime ideals of K.

The Hecke L-function satisfies a functional equation that relates the values of $L_K(s,\chi)$ at s and $1-s$, much like the classical functional equation for the Riemann zeta function or Dirichlet L-functions. For our purposes, it is not necessary to present it here.

4 Artin L-Series

Given a Galois extension of number fields L/K with Galois group $G = \mathrm{Gal}(L/K)$, and a finite-dimensional complex representation $\rho : G \to \mathrm{GL}(V)$ of G on a vector space V, the *Artin L-series* $L(s,\rho)$ associated with the representation ρ is defined as an Euler product:

$$L(s,\rho) = \prod_{\mathfrak{p}} \det\left(1 - \rho(\mathrm{Frob}_{\mathfrak{p}})\|\mathfrak{p}\|^{-s} \mid V^{I_{\mathfrak{p}}}\right)^{-1},$$

where the product runs over all prime ideals $\mathfrak{p}$ of K, and:

- $\mathrm{Frob}_{\mathfrak{p}}$ is a Frobenius element associated with $\mathfrak{p}$ in G, defined up to conjugacy (recall that it exists if $\mathfrak{p}$ is unramified in L).
- $I_{\mathfrak{p}}$ is the inertia group of $\mathfrak{p}$, and $V^{I_{\mathfrak{p}}}$ is the subspace of V fixed by the inertia group $I_{\mathfrak{p}}$.

The link between Artin and Hecke L-series is provided by class field theory. Let L/K be an abelian extension, and let $\mathfrak{f}$ be the *conductor* of L/K, i.e., the smallest modulus

$$\mathfrak{f} = \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{n_{\mathfrak{p}}}$$

The *Artin symbol* $\left(\frac{L/K}{\mathfrak{a}}\right)$ then gives us a surjective homomorphism

$$J^{\mathfrak{f}}/P^{\mathfrak{f}} \longrightarrow G(L/K), \quad \mathfrak{a} \mod P^{\mathfrak{f}} \longmapsto \left(\frac{L/K}{\mathfrak{a}}\right),$$

from the *ray class group* $J^{\mathfrak{f}}/P^{\mathfrak{f}}$. Here $J^{\mathfrak{f}}$ is the group of fractional ideals prime to $\mathfrak{f}$, and $P^{\mathfrak{f}}$ is the group of principal ideals $(\mathfrak{a})$ such that $\mathfrak{a} \equiv 1 \mod \mathfrak{f}$ and $\mathfrak{a}$ is positive in $K_{\mathfrak{p}} = \mathbb{R}$ if $\mathfrak{p}$ is real.

Now let χ be an irreducible character of the abelian group $G(L/K)$, i.e., a homomorphism

$$\chi : G(L/K) \to \mathbb{C}^*.$$

Composing with the Artin symbol $\left(\frac{L/K}{\mathfrak{a}}\right)$, this gives a character of the ray class group $J^{\mathfrak{f}}/P^{\mathfrak{f}}$. It induces a character on $J^{\mathfrak{f}}$, which we denote by

$$\tilde{\chi} : J^{\mathfrak{f}} \to \mathbb{C}^*.$$

this character on ideals is a Grössencharakter mod $\mathfrak{f}$, and we have the

Theorem 4.9. *Let L/K be an abelian extension, let $\mathfrak{f}$ be the conductor of L/K, let $\chi \neq 1$ be an irreducible character of $G(L/K)$, and $\tilde{\chi}$ the associated Grössencharakter mod $\mathfrak{f}$. Then, the Artin L-series for the character χ and the Hecke L-series for the Grössencharakter $\tilde{\chi}$ satisfy the identity*

$$\mathcal{L}(L/K, \chi, s) = \prod_{\mathfrak{p} \in S} \frac{1}{1 - \chi(\mathrm{Frob}_{\mathfrak{P}}) \|\mathfrak{p}\|^{-s}} L(\tilde{\chi}, s),$$

where $S = \{\mathfrak{p} \mid \mathfrak{f} : \chi(I_{\mathfrak{P}}) = 1\}$.

Chapter 5

Arithmetic Equivalence

In the previous chapter, we saw that $\zeta_K(s)$ governs the arithmetic of an algebraic number field K. We now study when two number fields K and K' have identical zeta functions

$$\zeta_K(s) = \zeta_{K'}(s). \tag{1}$$

In 1925, Fritz Gassmann proved the existence of two number fields K and K' such that $\zeta_K(s) = \zeta_{K'}(s)$ but $K \ncong K'$. Also, it is known that if N is a Galois extension over $\mathbb{Q}$, then N is isomorphic to any field L that has the same zeta function. The purpose of the present chapter is to study equivalent conditions for the Equation (1) and some of its consequences.

1 Perlis' Theorem

The exposition given in this section is mainly based on the paper by Robert Perlis [14].

Throughout this section, $L/\mathbb{Q}$ will denote a finite normal extension containing K and K'. Let $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ be the prime decomposition of a rational prime p and let $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ be the inertia degree of $\mathfrak{p}_i$, numbered so that $f_i \leq f_{i+1}$. Then the tuple $A = (f_1, ..., f_g)$ is called the *splitting type* of p in K. Every tuple is associated with the set

$$P_K(A) = \{p \in \mathbb{Z} : p \text{ has splitting type } A \text{ in } K\}$$

Since $f_1 + \cdots + f_g \leq [K : \mathbb{Q}]$, $P_K(A)$ is empty except for finitely many A. The notation

$$P_K(A) \doteq P_{K'}(A)$$

will be used to indicate that these two sets differ by, at most, a finite number of elements. This is convenient for excluding the ramified primes from consideration. Remember that K is not necessarily a Galois extension over $\mathbb{Q}$. Therefore, the decomposition group is not necessarily defined. The key to solving this is to consider the subgroup $H = \mathrm{Gal}(L/K)$ of $G = \mathrm{Gal}(L/\mathbb{Q})$. Let $p \in \mathbb{Z}$ be a prime number unramified in L. Let $\mathfrak{p}$ be a prime of K lying above p, and let $\mathfrak{P}$ be a prime of L lying above $\mathfrak{p}$. We know that $G \cdot \mathfrak{P} = \{\sigma(\mathfrak{P}) : \sigma \in G\}$ is set of primes of L lying above p, so if $\sigma(\mathfrak{P})$ is a prime lying above $\mathfrak{p}$ then the set of primes of L lying above $\mathfrak{p}$ is $\{h(\sigma(\mathfrak{P})) : h \in H\}$. Therefore, if $\tau \in G$ is such that $\tau(\mathfrak{P})$ is a prime lying above $\mathfrak{p}$ then $\tau(\mathfrak{P}) = h(\sigma(\mathfrak{P}))$ for some $h \in H$, that is, $\tau^{-1} \cdot h \cdot \sigma \in C = D(\mathfrak{P} \mid p)$, namely, $\tau = h \cdot \sigma \cdot c$ for some $c \in C$. Thus, the prime $\mathfrak{p}$ is uniquely represented by the set $H\sigma C$, which is the equivalence class of σ under the following equivalence relation in G

$$\sigma \sim \tau \text{ if and only if } \tau = h \cdot \sigma \cdot c \text{ for some } h \in H; \text{ for some } c \in C.$$

The above equivalence relation is known in group theory as *double coset*, where the (H, C)-double coset of σ is the set $H\sigma C$, and the set of all (H, C)-double cosets is denoted by $H\backslash G/C$. Note that if $(f_1, ..., f_g)$ is the splitting type of p in K, then $|H\backslash G/C| = g$. Moreover, we can consider the double coset $H\sigma C$ as the right action of C on $H\sigma$. Suppose that $\mathfrak{p}_i$ is represented by the double coset $H\sigma_i C$, for $1 \leq i \leq g$. Note that

$$\begin{aligned}\mathrm{Stab}(H\sigma_i) &= \{c \in C : H\sigma_i \cdot c = H\sigma_i\} = \{c \in C : H\sigma_i \cdot c \cdot \sigma_i^{-1} \ = H\} = \{c \in C : \sigma_i \cdot c \cdot \sigma_i^{-1} \in H\} \\ &= \{c \in C : c \in \sigma_i^{-1} H\sigma_i\} = C \cap \sigma_i^{-1} H\sigma_i.\end{aligned}$$

In view of the following one-to-one correspondence

$$\begin{aligned} D(\sigma(\mathfrak{P}) \mid \mathfrak{p}) &\to C \cap \sigma_i^{-1} H\sigma_i \\ h \quad &\to \ \sigma_i^{-1} \cdot h \cdot \sigma_i \end{aligned}$$

we obtain $|C \cap \sigma_i^{-1} H\sigma_i| = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}_i]$. Therefore

$$|H\sigma_i C| = \sum_{\substack{c \text{ representative} \\ \text{of } C/C\cap\sigma_i^{-1}H\sigma_i}} |H\sigma_i \cdot c| = \sum_{\substack{c \text{ representative} \\ \text{of } C/C\cap\sigma_i^{-1}H\sigma_i}} |H| = |H| \cdot \frac{|C|}{|C \cap \sigma_i^{-1} H\sigma_i|} = |H| \cdot [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}] = |H| \cdot f_i.$$

Therefore, if C is the decomposition group of p in G and $H = \mathrm{Gal}(L/K)$, then the splitting type $(f_1, ..., f_g)$ is simultaneously the *coset type* of G modulo (H, C) : If $G = \bigcup_{i=1}^{n} H\sigma_i C$ is disjoint, then $n = g$ and $|H\sigma_i C| = |H| \cdot f_i$, the cosets having been numbered in increasing order. Thus, p has the same splitting type in both K and K' if and only if

$$\text{coset type } [G \bmod (H, C)] \ = \text{coset type } [G \bmod (H', C)] \tag{2}$$

where $H' = \mathrm{Gal}(L/K')$.

Since p is unramified then C is a cyclic group; by the Frobenius density theorem, every cyclic subgroup of G is a decomposition group for infinitely many primes numbers $p \in \mathbb{Z}$. Thus $P_K(A) \doteq P_{K'}(A)$ for all tuple A is equivalent to (2) for all cyclic subgroup C of G.

Now, let us see an equivalent condition to criterion (2). Two subgroups H and H' of a finite group G are said to be *Gassman Equivalent* in G when

$$|c^G \cap H| = |c^G \cap H'|$$

for every conjugacy class $c^G = \{g \cdot c \cdot g^{-1}\}$ in G.

Lemma 5.1 (Gassman)**.** *Two subgroups H and H' of a finite group G are Gassmann equivalent if and only if the coset types of G mod (H, C) and G mod (H', C) coincide for every cyclic subgroup C of G.*

Proof. First, let us see that either condition implies that $|H| = |H'|$.
(*Gassman equivalent* $\Rightarrow |H| = |H'|$). If two conjugacy classes, say c^G and d^G, overlap, then there are $\sigma, \tau \in G$ such that $\sigma c \sigma^{-1} = \tau d \tau^{-1}$, so $c = \sigma^{-1}\tau d(\sigma^{-1}\tau)^{-1}$, giving $c^G \subseteq d^G$, hence these conjugacy classes are equal. For an arbitrary $h \in H$, we have $h\mathrm{Id} = h$, so the conjugacy classes cover H. Hence

$$H = \bigsqcup_{c \in G, \text{ repr.}} (c^G \cap H),$$

i.e., H is a disjoint union of representatives of conjugacy classes intersected with the subgroup H. Thus, we have

$$|H| = \sum_{c \in G,\ \text{repr.}} |c^G \cap H| = \sum_{c \in G,\ \text{repr.}} |c^G \cap H'| = |H'|.$$

(*Equal coset types* $\Rightarrow |H| = |H'|$). We have $f_i = f_i'$ for all $i \in \{1, \dots, h\}$ where the f_i and f_i' are given by

$$|HT_iC| = |H| \cdot f_i \quad \text{and} \quad |H'\tau_i'C| = |H'| \cdot f_i'.$$

Because $G = \bigcup_{i=1}^h HT_iC = \bigcup_{i=1}^h H'\tau_i'C$ we can deduce

$$|G| = |H| \cdot \sum_{i=1}^h f_i = |H'| \cdot \sum_{i=1}^h f_i',$$

hence $|H| = |H'|$.
By defining numbers l_i, which depend on the coset type, we can make numbers k_i, which depend on the Gassmann equivalence class. Let C be an arbitrary cyclic subgroup of G, and let c be its generator. Define the number l_i:

$$\begin{aligned} l_i &= \#\{g \in G : |HgC| = |H| \cdot i\} \\ &= \#\{\text{cosets of } HgC : \text{order is } |H| \cdot i\} \cdot |H| \cdot i \end{aligned}$$

The last equation holds because each coset of order $|H| \cdot i$ has exactly $|H| \cdot i$ elements. Define the number k_i

$$\begin{aligned} k_i &= \#\sum_{d|i} l_d \\ &= \#\{g \in G : |HgC| \text{ divides } |H| \cdot i\} \\ &= \#\left\{g \in G : \frac{|C^g|}{|H \cap C^g|} \text{ divides } i\right\} \\ &= \#\left\{g \in G : H \cap \langle c^g \rangle \supseteq \langle c^i g \rangle\right\} \\ &= \#\left\{g \in G : gc^i g^{-1} \in H\right\} \\ &= |\langle c^i \rangle^G \cap H| \cdot \text{stabilizer of } c^i. \end{aligned}$$

(1) Because $|HgC| = |HgCg^{-1}| = |HCg^{-1}| = |H| \cdot |C^g| / |H \cap C^g|$.

(2) The order divides i, so for an arbitrary $a \in C^g$ we have $a^i \sim 1$ in $C^g/(H \cap C^g)$, and thus $a^i \in (H \cap C^g)$. Actually, we have $\langle c^i \rangle^g \subseteq H \cap \langle c^g \rangle$.

(3) Since $g\langle c^i \rangle g^{-1} \subseteq \langle c^g \rangle$, we can simplify $\langle c^i \rangle^g \subseteq (H \cap \langle c^g \rangle)$ to $g\langle c^i \rangle g^{-1} \subseteq H$. Because H is a group, it is enough to only require this for the generator.

Now Möbius inversion gives us $l_i = \sum_{d|i} k_d \mu(i/d)$, where μ is the classical Möbius function. Analogously, we get l_i' and k_i' for the group H'. We have defined l_i and l_i' in such a way that we have that if for all cyclic groups C the coset types are equal if and only if $l_i = l_i'$ for all i (by $|H| = |H'|$). By the last part of the proof, we have $l_i = l_i'$ for all i if and only if $k_i = k_i'$ for all i. The number k_i respectively k_i' is equal to the number of elements of the conjugates of c^i which are in H respectively H' times the number of elements which stabilize c^i. Because the last part of this definition is equal for k_i and k_i', we get that we have $k_i = k_i'$ for all i if and only if $\langle c^i \rangle^G \cap H = \langle c^i \rangle^G \cap H'$ for all i, and this defines Gassmann equivalence for H and H'.

□

Lemma 5.2. *Let $\tau_1(s) = \prod_{j=1}^{n}(1 - c_j^{-s})$ and $\tau_2(s) = \prod_{j=1}^{m}(1 - d_j^{-s})$ with real $c_j, d_j > 1$. Let $f(s)$ be a meromorphic function whose zeroes and poles do not lie among the zeros of either $\tau_1(s)$ and $\tau_2(s)$. If $\tau(s) = \tau_1(s)/\tau_2(s)$ satisfies*

$$\tau(s) = f(s) \cdot \tau(1 - s)$$

then $\tau_1(s) = \tau_2(s)$ and $f(s) = 1$.

Proof. Suppose that after all common factors have been canceled from $\tau_1(s)$ and $\tau_2(s)$ we obtain that $\tau_1(s) \neq \tau_2(s)$. Note that

$$1 - c_j^{-s} = 0 \iff c_j^s = 1 \iff e^{\log(c_j)\cdot s} = 1 \iff \log(c_j) \cdot s = 2\pi i k \text{ for some } k \in \mathbb{Z},$$

therefore, the set of zeros of $\tau_1(s)$ is

$$\{2\pi i k/\log(c_j)\}_{(k,j)\in\mathbb{Z}\times[1..n]}$$

analogously, the set of zeros of $\tau_2(s)$ is

$$\{2\pi i k/\log(d_j)\}_{(k,j)\in\mathbb{Z}\times[1..m]}.$$

Let $\alpha_1 = 2\pi i/\log(c_1)$, then

- $\tau_1(\alpha_1) = 0$
- $\tau_1(1 - \alpha_1) \neq 0$ (because the zeros of τ_1 are purely imaginary)
- $f(\alpha_1) \neq 0$ (by hypothesis)

so $\tau_2(\alpha_1) = 0$. Thus $2\pi i/\log(c_1) = 2\pi i \cdot r_1/\log(d_{j_1})$ for some $r_1 \in \mathbb{Z}$ and some d_{j_1}. By setting $c_{j_1} = c_1$ we have that

$$d_{j_1} = c_{j_1}^{r_1}$$

Since c_{j_1} and d_{j_1} are greater than 1, the integer r_1 must be positive. Similarly, selecting $\alpha_2 = 2\pi i/\log(d_{j_1})$ produces the relation

$$c_{j_2} = d_{j_1}^{l_1}, \;\; l_1 > 0.$$

Thus $c_{j_2} = c_{j_1}^{r_1 l_1}$. Since there are at most n distinct c_j's, repeating this procedure n times yields a relation

$$c_{j_k} = c_{j_k}^{r_k l_k \cdots r_{k+n} l_{k+n}}$$

from which it follows that $r_k = l_k = \cdots = 1$. But then $d_{j_k} = c_{j_k}^{r_k} = c_{j_k}$ so $\tau_1(s)$ and $\tau_2(s)$ have a common factor, which is a contradiction. □

Let $r_1(K)$ and $r_1(K')$ denote the number of real embeddings of the number fields K and K', respectively. Let $r_2(K)$ and $r_2(K')$ denote the number of complex embeddings of K and K', respectively.

Theorem 5.1 (Perlis' theorem)**.** *Let K and K' be two number fields and L be a Galois extension of $\mathbb{Q}$ containing K and K'. The following are equivalent:*

(a) $\zeta_K(s) = \zeta_{K'}(s)$

(b) $P_K(A) = P_{K'}(A)$ *for every tuple A.*

(c) $P_K(A) \doteq P_{K'}(A)$ *for every tuple A.*

(d) $H = \mathrm{Gal}(L/K)$ *and* $H' = \mathrm{Gal}(L/K')$ *are Gassmann equivalent in* $G = \mathrm{Gal}(L/\mathbb{Q})$.

If one of these statements is true then we say that K *and* K' *are arithmetically equivalent, and all of the following hold:*

(1) $[K : \mathbb{Q}] = [K' : \mathbb{Q}]$.

(2) The discriminants of K *and* K' *are equal.*

(3) $r_1(K) = r_1(K')$ *and* $r_2(K) = r_2(K')$.

(4) K *and* K' *have the same normal closure.*

(5) K *and* K' *have the same normal core.*

(6) The unit groups U_K *and* $U_{K'}$ *are isomorphic.*

Proof. "(a) ⇒ (b)": Define

$$A(n) = \{I \subset \mathcal{O}_K : \|I\| = n\}$$
$$A'(n) = \{I \subset \mathcal{O}_{K'} : \|I\| = n\}.$$

Now $\zeta_K(s) = \sum_{n\in\mathbb{N}} \frac{A(n)}{n^s}$ and $\zeta_{K'}(s) = \sum_{n\in\mathbb{N}} \frac{A'(n)}{n^s}$ for $\mathrm{Re}(s) > 1$. Thus

$$A(1) = \lim_{s\to\infty} \zeta_K(s) = \lim_{s\to\infty} \zeta_{K'}(s) = A'(1).$$

Let us suppose $A(i) = A'(i)$ for all $i = 1, \ldots, l-1$. Now cancel the terms $A(i)$ respectively $A'(i)$ in the zeta functions and multiply this with l^s. The limit for s going to infinity gives the following equality

$$A(l) = \lim_{s\to\infty} \sum_{n\geq l} \frac{A(n)}{n^s} \cdot l^s = \lim_{s\to\infty} \sum_{n\geq l} \frac{A'(n)}{n^s} \cdot l^s = A'(l) \quad \forall l \in \mathbb{N},$$

so this is true for all $l \in \mathbb{N}$. In $\mathcal{O}_K$ and $\mathcal{O}_{K'}$ every nonzero prime ideal is maximal. To consider only the prime ideals, we have to subtract all the non-maximal ideals. Let $B(p^f)$ be the number of prime ideals of norm p^f, hence

$$B(p^f) = A(p^f) - \sum_{\substack{a_1+\cdots+a_t=f \\ a_i\in\mathbb{N}, t\geq 2}} A(p^{a_1}) \ldots A(p^{a_t}).$$

Now $B(p^f)$ determines the splitting type of p in K. We can define $B'(p^f)$ analogously and $B(p^f) = B'(p^f)$. It follows that $P_K(A) = P_{K'}(A)$.

"(b) ⇒ (c)": This is trivial.

"(c) ⇔ (d)": By Lemma 5.1, we have for every tuple A that $P_K(A) \doteq P_{K'}(A)$ if and only if the coset types of (G, H, C) is equal to the coset type of (G, H', C) for all cyclic subgroups C of G. Secondly, let us recall that we have equal coset types if and only if H and H' are Gassmann equivalent.

"(d) ⇒ (a)": In this case, C is the decomposition group of the real infinite divisor of $\mathbb{Q}$, i.e., either C consists only of the identity or C also has complex conjugation, so this group C is cyclic. Now

$$r_1(K) = \{Ht_iC : |Ht_iC| = |H|\} = r_1(K'),$$

because by (d) and the fact that $|H| = |H'|$. Similarly, we have

$$r_2(K) = \{Ht_iC : |Ht_iC| = 2|H|\} = r_2(K').$$

Define

$$G_1(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right), \quad G_2(s) := (2\pi)^{1-s}\Gamma(s)$$

$$Z_K(s) = G_1(s)^{r_1(K)}G_2(s)^{r_2(K)}\zeta_K(s).$$

The completed zeta function Z_K is analytic outside 0 and 1 and $Z_K(s) = |d_K|^{(1/2)-s}Z_K(1-s)$, where d_K and $d_{K'}$ are the corresponding discriminants.
Since the real and complex valuations are equal for K and K', it follows that:

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = \frac{Z_K(s)}{Z_{K'}(s)} = \left|\frac{d_K}{d_{K'}}\right|^{(1/2)-s} \cdot \frac{\zeta_K(1-s)}{\zeta_{K'}(1-s)}.$$

Let us recall that the zeta function has an Euler product. Since we have (c) if and only if we have (d), we know that there are only finitely many primes which have a different splitting type. Hence the quotient of the zeta functions of K and K' is a finite product:

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = \frac{\prod_{j=1}^{m}(1-d_j^{-s})^{-1}}{\prod_{j=1}^{n}(1-c_j^{-s})^{-1}}.$$

By the analytic continuation, this is true for all complex s. We get by Lemma 5.2, $\zeta_K(s) = \zeta_{K'}(s)$.

Let us now prove the properties of arithmetically equivalent number fields K and K'.

"(1)": This is obvious as $|H| = |H'|$ and

$$|H| \cdot [K:\mathbb{Q}] = [N:K][K:\mathbb{Q}] = [N:K'][K':\mathbb{Q}] = |H'| \cdot [K':\mathbb{Q}],$$

hence $[K:\mathbb{Q}] = [K':\mathbb{Q}]$.

"(2)": Since $\left|\frac{d_K}{d_{K'}}\right| = 1$ and hence $d_K = (-1)^{r_2(K)}|d_K|$. Because of the complex embbedings of K and K' are equal, the discriminants are also equal.

"(3)": This follows from the proof of (d) implies (a).

"(4)": The normal closure of $K/\mathbb{Q}$ is equal to the fixed field of

$$\bigcap_{\sigma\in G} H^\sigma = \{g \in G \mid \forall \sigma \in G : \sigma^{-1}g\sigma \in H\},$$

which indeed contains K. Take $h \in \bigcap_{\sigma\in G} H^\sigma$. For all $\sigma \in G$, $\sigma h\sigma^{-1} \in H$, so by (d) $|h^G| = |h^G \cap H| = |h^G \cap H'|$. Thus $h \in \bigcap_{\sigma\in G} H^{\sigma'}$. Likewise $\bigcap_{\sigma\in G} H^{\sigma'} \subseteq \bigcap_{\sigma\in G} H^\sigma$, so $\bigcap_{\sigma\in G} H^\sigma = \bigcap_{\sigma\in G} H'^\sigma$.

"(5)": The normal core of K is the fixed field of $\langle H^\sigma \mid \sigma \in G\rangle$. For all $h \in H$, $h^{\mathrm{Id}} \in H$, so $|h^G \cap H'| = |h^G \cap H| \neq 0$. It follows that there exists a $\sigma \in G$ such that $h^\sigma \in H'$. This is true for each h, and the analogue is true for all $h' \in H'$. Thus we have an inclusion of the generators. Hence $\langle H^\sigma \mid \sigma \in G\rangle = \langle H'^\sigma \mid \sigma \in G\rangle$.

"(6)": By Dirichlet's unit theorem the unit group is a direct product of a free group and a finite cyclic group generated by the largest root of unity of K resp. K'. This free group has rank $r_1(K) + r_2(K) - 1$ resp. $r_1(K') + r_2(K') - 1$, which are equal because the valuations are equal. Adjoining a generating root of unity ζ of K to $\mathbb{Q}(\zeta)$ is a normal extension which lies in K' by (5). Likewise, the roots of unity of K' lie in K, so K and K' have the same roots of unity. Hence, the unit groups are isomorphic.

□

Chapter 6

p-adic L-functions

In the present chapter, we describe two different methods of constructing $p-$adic $L-$functions, one given by Kubota-Leopoldt and another given by Iwasawa. Finally, we discuss a deep relationship between $p-$adic $L-$functions and $\Lambda-$modules. The exposition given in this chapter is mainly based on the book by Lawrence C. Washington [18].

1 Kubota-Leopoldt's construction

In this section, we shall construct $p-$adic analogues of Dirichlet $L-$functions. First, we need some basic results on $p-$adic analysis. For the proof of these results, see section 5.1, [18].

Let $\overline{\mathbb{Q}_p}$ be the algebraic closure of $\mathbb{Q}_p$. The absolute value on $\mathbb{Q}_p$ extends uniquely to $\overline{\mathbb{Q}_p}$; we let ord_p denote the usual valuation on $\overline{\mathbb{Q}_p}$, normalized by $ord_p(p) = 1$, and let $|x|_p = p^{-ord_p(x)}$.

Proposition 6.1. $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ *is not complete.*

It is more convenient to do analysis in a complete field, therefore, we let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}_p}$. The $p-$adic absolute value naturally extends to $\mathbb{C}_p$ and $\overline{\mathbb{Q}_p}$ is dense in $\mathbb{C}_p$.

Proposition 6.2. $\mathbb{C}_p$ *is algebraically closed.*

$\mathbb{C}_p$ may be regarded as the $p-$adic analogue of the complex numbers. In fact, $\mathbb{C}_p$ and $\mathbb{C}$ are algebraically, but not topologically, isomorphic. Sometimes, for technical reasons, it is convenient to embed $\mathbb{C}_p$ in $\mathbb{C}$, or vice versa.

From now on, unless otherwise stated, we shall be working in $\mathbb{C}_p$.

Definition 6.1. ($p-$adic exponential function). The $p-$adic exponential is defined by

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Proposition 6.3. *The $p-$adic exponential* $\exp(X)$ *has a radius of convergence* $p^{-\frac{1}{p-1}}$.

We now define the $p-$adic logarithmic function:

$$\log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} X^n}{n}.$$

Let W denote the group of all roots of unity of order prime to p in $\mathbb{C}_p^\times$. Then

$$\mathbb{C}_p^\times = p^{\mathbb{Q}} \times W \times U_1$$

where

$$U_1 = \{x \in \mathbb{C}_p \mid |x-1| < 1\}.$$

Proposition 6.4. *There exists a unique extension of* $\log_p$ *to all of* $\mathbb{C}_p^\times$ *such that*

$$\log_p(p) = 0 \quad \textit{and} \quad \log_p(xy) = \log_p x + \log_p y \quad \textit{for all } x, y \in \mathbb{C}_p^\times.$$

Lemma 6.1. *If* $|x|_p < p^{-1/(p-1)}$ *then* $|\log_p(1+x)|_p = |x|_p$ *and if* $|x|_p \le p^{-1/(p-1)}$ *then* $|\log_p(1+x)|_p \le |x|_p$.

The following result provides a way to lift a root of a polynomial modulo p to a root in $\mathbb{Z}_p$, under suitable conditions. It is a key tool in p-adic number theory.

Theorem 6.1 (Hensel's Lemma)**.** *Let* $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ *be a polynomial in* $\mathbb{Z}_p[X]$ *with formal derivative* $f'(X) = nX^{n-1} + \cdots + a_1$. *Let* c_0 *be a* $p-$*adic integer such that* $f(c_0) \equiv 0 \pmod p$ *and* $f'(c_0) \not\equiv 0 \pmod p$. *Then there exists a unique* $p-$*adic integer such that* $f(c) = 0$ *and* $c_0 \equiv c \pmod p$.

We note an important consequence of Hensel's lemma. Letting $f(X) = X^p - X$, we have $f'(X) \equiv -1 \pmod p$ and $f(a) \equiv 0 \pmod p$, $a = 0, 1, ..., p-1$; we find that $\mathbb{Z}_p$ contains the $(p-1)$th roots of unity.

Definition 6.2 (Teichmüller Character)**.** *The Teichmüller character is a homomorphism of multiplicative groups* :

$$\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$$

such that $\omega(a)$ *is the unique* $(p-1)$*th root of unity in* $\mathbb{Z}_p$ *such that* $\omega(a) \equiv a \pmod p$. Also, $\omega(a)$ *is called the Teichmüller lift of* a.

Let $\langle a \rangle$ denote $\omega(a)^{-1}a$, so $\langle a \rangle \equiv 1 \pmod p$. Since $|\langle a \rangle - 1|_p < 1$ then by lemma 6.1 $\log_p(a) = \log_p(\langle a \rangle)$.

Proposition 6.5. *If* $|x| < p^{-1/(p-1)}$ *then*

$$\log_p \exp(x) = x$$

and

$$\exp \log_p(1+x) = 1 + x.$$

Finally, let $a \in \mathbb{Z}_p$, $p \nmid a$. We may define

$$\langle a \rangle^x = \exp(x \log_p \langle a \rangle) = \exp(x \log_p a).$$

Since $|\log_p \langle a \rangle| \le |q| = 1/q$, this converges if $|x| < qp^{-1/(p-1)} > 1$. If $x = 1$ then $\langle a \rangle^1 = \langle a \rangle$ by Proposition 6.5. Similarly, if $n \in \mathbb{Z}$ then $\langle a \rangle^n$ agrees with the usual definition. In particular, if $n \equiv 0 \pmod{p-1}$, or $0 \pmod 2$ if $p = 2$, then $\langle a \rangle^n = a^n$.

Let

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

Then $\binom{X}{n}$ is a polynomial of degree n in X and if X is an integer we obtain a binomial coefficient. If $X \in \mathbb{Z}_p$ then X is close to a rational integer, so $\binom{X}{n}$ is close to an integer. It follows that $\binom{X}{n} \in \mathbb{Z}_p$ if $X \in \mathbb{Z}_p$.

We are now ready to present p-adic L-functions. Let χ be a Dirichlet character. If we fix, once and for all, an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$, we may regard the values of χ as lying in $\mathbb{C}_p$. Also, observe that $\omega(a)$ is a p-adic Dirichlet character of conductor p and order $\varphi(q) = p-1$. It may be regarded as coming from a complex character if desired, but the choice is noncanonical and depends on an embedding of $\mathbb{Q}(\zeta_{p-1})$ into $\mathbb{Q}_p$. It is better to regard ω as a p-adic object. Note that it generates the group of Dirichlet characters defined mod p.

Theorem 6.2. *Let χ be a Dirichlet character of conductor f and let F be any multiple of p and f. Then there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function $L_p(s,\chi)$ on $\{s \in \mathbb{C}_p \mid |s| < p \cdot p^{-1/(p-1)}\}$ such that*

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

If $\chi = 1$, then $L_p(s,1)$ is analytic except for a pole at $s=1$ with residue $(1-1/p)$. In fact, we have the formula

$$L_p(s,\chi) = \frac{1}{F}\frac{1}{s-1}\sum_{a=1}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)\binom{F}{a}^j.$$

2 Iwasawa's construction

In this section, we give an alternative method to construct the $p-$adic $L-$functions. This construction was given by Iwasawa in 1969.

Let p be an odd prime number. Remember that $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q} \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. Let us see that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Let $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p^\times$, note that

$$\sigma_a(\zeta_{p^n}) = \prod_{i=0}^{\infty}(\zeta_{p^n})^{a_i p^i},$$

which is a finite product since $(\zeta_{p^n})^{p^i} = 1$ for $i \geq n$. Clearly $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, we know what happens at each finite level,

$$\sigma(\zeta_{p^n}) = (\zeta_{p^n})^{S_{n-1}},$$

for some $S_{n-1} = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Therefore, if

$$a = a_0 + a_1 p + a_2 p^2 + \cdots,$$

then $\sigma = \sigma_a$.

It is well known that the functions $\exp : p\mathbb{Z}_p \to 1 + p\mathbb{Z}_p$ and $\log_p : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$ are inverses, so $\log_p$ is an isomorphism from the multiplicative group $1 + p\mathbb{Z}_p$ to the addictive group $p\mathbb{Z}_p$. Note that

$$\log_p(1+p) = \sum_{k=1}^{\infty} = (-1)^{k+1}\frac{p^k}{k} = p \cdot (\text{unit}).$$

Now,

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

where the isomorphism is given by

$$a \longmapsto (\omega(a) \bmod p, \langle a \rangle) \longmapsto \left(\omega(a) \bmod p, \frac{\log_p(\langle a \rangle)}{\log_p(1+p)}\right)$$

Also, using properties of $\exp_p$ and $\log_p$ we see that $1+p$ is a topological generator for $1+p\mathbb{Z}_p$; i.e., $(1+p)^{\mathbb{Z}_p} = 1+p\mathbb{Z}_p$.

Let m be an integer such that $(m,p)=1$. Now, a Dirichlet character χ is called a character of the first kind if its conductor $f_\chi = m$ or $f_\chi = mp$ and it is called a character of the second kind if $f_\chi = 1$ or $f_\chi = p^n$, $n \geq 1$. Consider the natural isomorphism

$$\pi : (\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times.$$

Note that $\mathrm{Ker}(\pi) = \{1+pk : 0 \leq k < p^{n-1}\}$. Since if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ then $a \cdot \mathbb{Z}/p^{n-1}\mathbb{Z} = \mathbb{Z}/p^{n-1}\mathbb{Z}$, therefore $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathrm{Ker}(\pi)$. Since $|\mathrm{Ker}(\pi)| \leq |(\mathbb{Z}/p^n\mathbb{Z})^\times|$ then $\mathrm{Ker}(\pi)$ is a cyclic group, so $\mathrm{Ker}(\pi) \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$, therefore

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p^{n-1}\mathbb{Z}).$$

On the other hand, we have

$$(\mathbb{Z}/dp^n\mathbb{Z})^\times \cong (\mathbb{Z}/d\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times, \qquad (d,p)=1.$$

We see that any Dirichlet character χ can be uniquely decomposed into a product of a character of the first kind, say, θ, and a character of the second kind, say, ψ :

$$\chi = \theta\psi.$$

Let d be a positive integer with $(p,d)=1$. We assume $d \not\equiv 2 \pmod 4$. Let $q_n = p^{n+1}d$, $n \geq 0$; $K_n = \mathbb{Q}(\zeta_{q_n})$, and $K_\infty = \bigcup_{n\geq 0}\mathbb{Q}(\zeta_{q_n})$. Then $K_n = K_0(\zeta_{p^{n+1}})$ and $K_\infty = K_0(\zeta_{p^\infty})$. Let $\sigma \in \mathrm{Gal}(K_\infty/\mathbb{Q})$. Then $\sigma|_{K_0} = \delta_{a_\sigma} \in \Delta = \mathrm{Gal}(K_0/\mathbb{Q})$ such that $\delta_{a_\sigma}(\zeta_{pd}) = (\zeta_{pd})^{a_\sigma}$ for some $a_\sigma \in (\mathbb{Z}/pd\mathbb{Z})^\times$. Define $\delta^*_{a_\sigma} \in \mathrm{Gal}(K_\infty/\mathbb{Q})$ such that $\delta^*_{a_\sigma}(\zeta_{q_n}) = (\zeta_{q_n})^{a_\sigma}$ for any $n \geq 0$. Clearly $(\delta^*_{a_\sigma})^{-1} \circ \sigma \in \Gamma = \mathrm{Gal}(K_\infty/K_0)$, therefore, it follows easily that

$$\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \Delta \times \Gamma.$$

More explicitly, $\Gamma = 1+q_0\mathbb{Z}_p = (1+q_0)^{\mathbb{Z}_p}$, where $(1+q_0)^{\mathbb{Z}_p} = \{(1+q_0)^x : x \in \mathbb{Z}_p\}$. Then $1+q_0$ gives a topological generator. The elements of Γ which fix K_n are

$$1+q_n\mathbb{Z}_p = (1+q_0)^{p^n\mathbb{Z}_p} = \Gamma^{p^n}.$$

Since $d\mathbb{Z}_p = \mathbb{Z}_p$ then

$$\Gamma_n = \mathrm{Gal}(K_n/K_0) = \Gamma/\Gamma^{p^n} = (1+p\mathbb{Z}_p)/(1+p^{n+1}\mathbb{Z}_p) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

Therefore

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong \Delta \times \Gamma_n$$

Corresponding to this decomposition, we write

$$\sigma_a = \delta(a)\gamma_n(a), \quad \text{with } \delta(a) \in \Delta, \gamma_n(a) \in \Gamma_n.$$

Let χ be a character of $\mathrm{Gal}(K_n/\mathbb{Q})$ whose conductor is of the form dp^j for some $j \geq 0$. We see that χ can be uniquely decomposed as $\chi = \theta\psi$, where θ has conductor d or dp, so θ is of the first kind, while ψ

is a character of Γ_n, so ψ is a character of the second kind. Suppose that θ is an even character, and let $\theta^* = \omega\theta^{-1}$, so θ is odd. Let $K_\theta = \mathbb{Q}_p(\theta(1), \theta(2), ...)$, so $\mathcal{O}_\theta = \mathbb{Z}[\theta(1), \theta(2), ...]$. Let $\{x\}$ denote the fractional part of the real number x; so $x - \{x\} \in \mathbb{Z}$ and $0 \leq \{x\} < 1$. We define the *Stickelberger element*

$$\xi_n = -\sum_{\substack{0<a<q_n \\ (a,q_0)=1}} \left\{\frac{a}{q_n}\right\} \delta(a)^{-1}\gamma_n(a)^{-1}$$

since $\sigma_{a(1+q_0)} = \delta(a(1+q_0))\gamma_n(a(1+q_0)) = \delta(a)\gamma_n(a)\gamma_n(1+q_0)$ then

$$\xi_n = -\sum_{\substack{0<a<q_n \\ (a,q_0)=1}} \left\{\frac{a(1+q_0)}{q_n}\right\} \delta(a)^{-1}\gamma_n(a)^{-1}\gamma_n(1+q_0)^{-1}.$$

Let

$$\begin{aligned}\eta_n &= (1-(1+q_0)\gamma_n(1+q_0)^{-1})\xi_n \\ &= -\sum_{\substack{0<a<q_n \\ (a,q_0)=1}} \left(\left\{\frac{a(1+q_0)}{q_n}\right\} - (1+q_0)\frac{a}{q_n}\right) \delta(a)^{-1}\gamma_n(a)^{-1}\gamma_n(1+q_0)^{-1}\end{aligned}$$

note that $\eta_n \in \mathbb{Z}_p[\Delta \times \Gamma_n]$. Let

$$\varepsilon_{\theta^*} = \frac{1}{|\Delta|}\sum_{\delta\in\Delta} = \theta^*(\delta)\delta^{-1}$$

be the idempotent for θ^*. Then $\varepsilon_{\theta^*}\xi_n = \xi_n(\theta)\varepsilon_{\theta^*}$ and $\varepsilon_{\theta^*}\eta_n = \eta_n(\theta)\varepsilon_{\theta^*}$, where

$$\xi_n(\theta) = -\frac{1}{q_n}\sum_a a\theta\omega^{-1}(a)\gamma_n(a)^{-1} \in K_\theta[\Gamma_n],$$

and

$$\begin{aligned}\eta_n(\theta) &= (1-(1+q_0)\gamma_n(1+q_0)^{-1})\xi_n(\theta) \\ &= \sum_a \left((1+q_0)\left(\frac{a}{q_n}\right) - \left(\frac{a(1+q_0)}{q_n}\right)\right) \times \theta\omega^{-1}(a)\gamma_n(a)\gamma_n(1+q_0)^{-1} \in \mathcal{O}_\theta[\Gamma_n].\end{aligned}$$

The elements $\eta_n(\theta)$ and $\xi_n(\theta)$, as defined above, satisfy the following properties:

Proposition 6.6. *(a) $\frac{1}{2}\eta_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$;*
(b) if $\theta \neq 1$, then $\frac{1}{2}\xi_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$;
(c) if $m \geq n \geq 0$, then $\eta_m(\theta) \mapsto \eta_n(\theta)$ and $\xi_m(\theta) \mapsto \xi_n(\theta)$ under the natural map from $K_\theta[\Gamma_m]$ to $K_\theta[\Gamma_n]$.

Since $\mathcal{O}_\theta[[\Gamma]] \cong \mathcal{O}_\theta[[T]]$ and the above proposition, we find that there are power series $f, g, h \in \mathcal{O}_\theta[[T]]$ such that

$$\begin{gathered}\lim \xi_n(\theta) \leftrightarrow f(T,\theta) \quad (\text{if } \theta \neq 1) \\ \lim \eta_n(\theta) \leftrightarrow g(T,\theta) \\ \lim 1-(1+q_0)\gamma_n(1+q_0)^{-1} \leftrightarrow h(T,\theta).\end{gathered}$$

It is easy to see that

$$h(T,\theta) = 1 - \frac{1+q_0}{1+T}.$$

Also,

$$f(T,\theta) = \frac{g(T,\theta)}{h(T,\theta)}.$$

If $\theta = 1$, we take this as the definition of $f(T,\theta)$.

Theorem 6.3. *Let $\chi = \theta\psi$ be an even Dirichlet character (θ = first kind, ψ = second kind), and let $\zeta_\psi = \psi(1+q_0)^{-1} = \chi(1+q_0)^{-1}$ (a root of unity of p-power order). Then*

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

3 The Main Conjecture

As before, let $\mathbb{Q}_\infty/\mathbb{Q}$ be the unique cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let L_n be the maximal unramified abelian p-extension of $\mathbb{Q}_n$ and A_n be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}_n$. Set $X_n = \mathrm{Gal}(L_n/\mathbb{Q}_n) \cong A_n$, $L = \bigcup_{n\geq 0} L_n$ and $X = \mathrm{Gal}(L/\mathbb{Q}_\infty)$. $\Gamma_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ 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. Using $\Lambda \cong \mathbb{Z}_p[[\Gamma]]$, A becomes a Λ-module by defining the action componentwise. We also have $X \cong \varprojlim X_n \cong \varprojlim A_n$.

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

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

where $\mathbb{Q}$ 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. $\sum_{\chi\in\hat{G}}\varepsilon_\chi = 1$, and
4. $\varepsilon_\chi\sigma = \chi(\sigma)\varepsilon_\chi$.

The ε_χ's are called the orthogonal idempotents of the group ring $\mathbb{Q}[G]$. Let M be a module over $\mathbb{Q}[G]$ and $M_\chi = \varepsilon_\chi M$. For $m \in M$, property 3 implies $\sum_{\chi\in\hat{G}}\varepsilon_\chi m = m$ and $\sum_{\chi\in\hat{G}}\varepsilon_\chi\varepsilon_\psi = 0 \Longrightarrow \varepsilon_\chi\varepsilon_\psi = 0$ 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 $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Then $\hat{G} = \{\omega^i | 0 \leq i \leq p-2\}$ where ω is the p-adic Dirichlet character. The idempotent elements 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 $A_n \cong X_n$ was defined, G acts on A_n and thus A_n can be considered as a $\mathbb{Z}_p[G]$-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 $\varprojlim \varepsilon_i A_n \cong \varepsilon_i X$ is a Λ-module. The following amazing result relates these Λ-modules (algebraic objects) to p-adic L-functions (analytic objects):

Theorem 6.4. *Assume $p \nmid h(\mathbb{Q}(\zeta_p^+))$. Let $P_n(T) = (1+T)^{p^n} - 1$. Then for $i = 3, 5, \ldots, p-2$,*

$$\varepsilon_i X \cong \Lambda/(P_n(T), f(T, \omega^{1-i}))$$

and

$$\varepsilon_i X \cong \Lambda/(f(T, \omega^{1-i})),$$

where $f(T, 1-i)$ is the power series satisfying $f(1+T)^{p^n} - 1 = L_p(s, \omega^{1-i})$.

We factor $f(T,\omega^{1-i}) = p^{\mu_i} g_i(T) U_i(T)$ with g_i distinguished and $U_i \in \Lambda^\times$. Therefore, $\varepsilon_i X = \Lambda/(p^{\mu_i} g_i(T)) \cong \Lambda/(p^{\mu_i}) \oplus \Lambda/(g_i)$ which is of the form of decomposition of $\varepsilon_i X$ as a Λ-module. It is known that $\mu_i = 0$ for cyclotomic $\mathbb{Z}_p$-extensions. Therefore

$$\varepsilon_i X \cong \Lambda/(f(T,\omega^{1-i})) \cong \Lambda/(g_i(T)).$$

So in this case the distinguished polynomial in the decomposition of $\varepsilon_i X$ is essentially the p-adic L-function. Iwasawa conjectured that this is true in more general situations.

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

$$\varepsilon_\chi X \hookrightarrow \bigoplus_i \Lambda/(p^{k_i^\chi}) \oplus \bigoplus_j \Lambda/(g_j^\chi(T))$$

with finite cokernel. Let $\mu_\chi = \sum k_i^\chi$ and let $g_\chi(T) = p^{\mu_\chi} \prod_j g_j^\chi(T)$ (where g_χ is called the characteristic polynomial associated with $\varepsilon_\chi X$). Let γ_0 be the generator of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ corresponding to $1+T$. Define $\kappa_0 \in 1 + p\mathbb{Z}_p$ by $\gamma_0 \zeta_p = \zeta_p^{\kappa_0}$ 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 6.5 (The Main Conjecture)**.** *$f_\chi(x) = g_\chi(T) U_\chi(T)$ with $U_\chi(T) \in \Lambda^\times$.*

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 to 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

$$Y \cong \bigoplus_i \Lambda/(p^{k_i}) \oplus \bigoplus_j \Lambda/(g_j(T)),$$

we have

$$V \cong \bigoplus_i \mathbb{C}_p/(p^{k_i}) \oplus \bigoplus_j \mathbb{C}_p/(g_j(T)),$$

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 $T+1 = \gamma_0$ acts on V by multiplication. Thus, Γ acts on V. Let $g(T) = \prod g_j(T)$ be the characteristic polynomial of $\gamma_0 - 1$ acting on V. The vector space V is clearly a $\mathbb{Q}_p[\Delta]$-module, so we can decompose

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

Then

$$g(T) = \prod_\chi g_\chi(T)$$

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

Theorem 6.6 (The Main Conjecture (second form))**.** $\tilde{f}_\chi(T) = g_\chi(T)$.

Chapter 7

On Zeta Functions And Iwasawa Modules

The exposition in this chapter is based on the works of Jangheon Oh [13] and Keiichi Komatsu [7].

1 In The Totally Real Number Field Case

1.1 The Main Conjecture for totally real fields.

In this subsection, we present the Main Conjecture for totally real number fields in the context of more general L-functions, specifically Hecke L-functions, as we will make significant use of this fact in the next subsection.

Let K be a totally real number field. Fix a rational odd prime p, let $\Delta = \mathrm{Gal}(K(\zeta_p)/K)$. Note that

$$|\Delta| = [K(\zeta_p) : K(\zeta_p + \zeta_p^{-1})][K(\zeta_p + \zeta_p^{-1}) : K].$$

Recall that ζ_p is a root of $X^2 - (\zeta_p + \zeta_p^{-1})X + 1$, since K is a totally real number field then

$$[K(\zeta_p) : K(\zeta_p + \zeta_p^{-1})] = 2,$$

therefore $|\Delta|$ is an even integer.

For every integer $n \geq 0$, let $K_n = K(\zeta_{p^{n+1}})$, so $K_\infty = \bigcup K_n$ is the cyclotomic $\mathbb{Z}_p-$extension of K, then $\Gamma = \mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_p$ and $\mathrm{Gal}(K_\infty/K) = \Delta \times \Gamma$. Let $X_{K(\zeta_p)}$ denote the Iwasawa module. Write θ for the character with values in $\mathbb{Z}_p^\times$, giving the action of Δ on ζ_p. Let κ be the character giving the action of Γ on the group of $p-$powers roots of unity and let $u = \kappa(\gamma_0)$.

Recall that, from Chapter 4, we may regard θ as a Hecke character. By the work of Deligne–Ribet [6], Cassou-Noguès [4], and Barsky [2], there exists a continuous p-adic L-function $L_{K,p}(s, \chi)$, defined on $\mathbb{Z}_p \setminus \{1\}$ and taking values in $\mathbb{C}_p$.

For all integers $s \leq 0$ with $s \equiv 1 \pmod{|\Delta|}$, we have

$$L_{K,p}(s, \theta^i) = L_K(s, \theta^i) \prod_{\mathfrak{p}|p} \left(1 - \theta^i(\mathfrak{p})\|\mathfrak{p}\|^{-s}\right),$$

where $L_K(s, \theta^i)$ is the Hecke L-series of θ^i. Moreover, for all integers i and $n > 1$, the value $L_K(1-n, \theta^i)$ is nonzero if and only if i and n have the same parity.

For any integer $i = 0, 1, ..., |\Delta| - 1$, define θ^i-idempotent

$$e_i = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \theta^i(\delta)\delta$$

We define the minus part of $X_{K(\zeta_p)}$ by

$$X^-_{K(\zeta_p)} = \sum_{i=1 \text{ odd}}^{|\Delta|} e_i X_{K(\zeta_p)}$$

There is a fraction of power series $G(T, \theta^i)$ in the field of fractions of Λ satisfying

$$G(u^s - 1, \theta^i) = L_{K,p}(s, \theta^{1-i})$$

where $L_{K,p}(s, \theta^{1-i})$ is the $p-$adic $L-$function of θ^{1-i}.

1.2 The $X^-_{K(\zeta_p)}$ module and zeta function

The purpose of this section is to prove the following theorem.

Theorem 7.1 (Jangheon Oh, 1998)**.** *Let S be a finite set of primes. Let K be a totally real number field. Suppose we know $X^-_{K(\zeta_p)}$ as a $\Lambda[\Delta]-$module up to pseudo-isomorphism for all $p \notin S$; then we can determine the zeta function ζ_K of K.*

Proposition 7.1. *The Iwasawa modules $X^-_{K(\zeta_p)}$, for all primes not in S, determine the absolute value of ζ_K at negative integers, up to primes in S.*

Proof. If n is an negative even integer, then $\zeta_K(n) = 0$. Fix a negative odd integer n. Let p be a prime number not in S. Then $n \equiv i_n \pmod{|\Delta|}$, for some odd integer i_n, $0 \leq i_n \leq |\Delta| - 1$. Since $|\Delta|$ divides $n - i_n$, we know the value

$$\begin{aligned} ord_p(G(u^n - 1, \theta^{i_n})) &= ord_p\left(L_K(n, \theta^{-i_n+n}) \prod_{\mathfrak{p}|p}(1 - \theta^{-i_n+n}(\mathfrak{p})\|\mathfrak{p}\|^{-n})\right) \\ &= ord_p(L_K(n, 1)) + ord_p\left(\prod_{\mathfrak{p}|p}(1 - \|\mathfrak{p}\|^{-n})\right) \\ &= ord_p(\zeta_K(n)) + 0 \end{aligned}$$

Therefore the absolute value of $\zeta_K(n)$ is determined up to primes is S.

□

Lemma 7.1. *Let $\{x_n\}$ be a sequence in $\mathbb{C}_p$, which converges to $x \neq 0$. Then $ord_p(x_n) = ord(x)$ for n sufficiently large.*

Proof. Since x_n approaches x, $|x_n - x|_p$ is strictly less than $|x|_p$ for n sufficiently large. Therefore $|x_n|_p = max\{|x_n - x|_p, |x|_p\} = |x|_p$ for n sufficiently large. □

Proposition 7.2. *Let $S = \{p_1, ..., p_r\}$ be any finite set of primes. Then there is a sequence $\{a_n\}$ of odd integers such that $ord_p(\zeta_K(a_n))$ is constant for n sufficiently large for all primes p in S.*

Proof. Let $\delta_i = |\mathrm{Gal}(K(\zeta_{p_i})/K)|$ and $\sigma_i = p_i - 1$ for an odd prime p_i, and $\sigma_i = 2$ if $p_i = 2$. Then δ_i divides σ_i. We define

$$a_n = 1 - 2\sigma_1 \cdots \sigma_r - 2\sigma_1 \cdots \sigma_r p_1^n \cdots p_r^n,$$

then

$$L_{p_i}(a_n, 1) = \left(\prod_{\mathfrak{p}|p_i} (1 - \|\mathfrak{p}\|^{-a_n}) \right) \zeta_K(a_n)$$

so

$$|L_{p_i}(1 - 2\sigma_1 \cdots \sigma_r, 1) - \zeta_K(a_n)|_p \leq |L_{p_i}(1 - 2\sigma_1 \cdots \sigma_r, 1) - L_{p_i}(a_n, 1)|_p + \left| \prod_{\mathfrak{p}|p_i} (1 - \|\mathfrak{p}\|^{-a_n}) - 1 \right|_p |\zeta_K(a_n)|_p,$$

therefore $\zeta_K(a_n)$ approaches $L_{p_i}(1 - 2\sigma_1 \cdots \sigma_r, 1)$ p_i-adically with n. Since $L_{p_i}(1 - 2\sigma_1 \cdots \sigma_r, 1) \neq 0$, therefore there exists a positive integer N such that $ord_{p_i}(\zeta_K(a_n)) = ord_{p_i}(\zeta_K(1 - 2\sigma_1 \cdots \sigma_r))$ for every integer $n > N$ and $i = 1, ..., r$. This completes the proof. □

Since K is a totally real number field, we have the following functional equation.

$$A^s \Gamma(s/2)^N \zeta_K(s) = A^{1-s} \Gamma((1-s)/2)^N \zeta_K(1-s),$$

where $A = d_K^{\frac{1}{2}} \pi^{-\frac{N}{2}}$, $N = [K : \mathbb{Q}]$. Hence we have

$$\begin{aligned} \zeta_K(1-s) &= A^{2s-1} \Gamma(s/2)^N \Gamma((1-s)/2)^{-N} \zeta_K(s) \\ &= A^{2s-1} (\Gamma(s/2)/\Gamma((1-s)/2))^N \zeta_K(s) \\ &= A^{2s-1} (\Gamma(s) 2^{1-s} \pi^{-\frac{1}{2}} \cos((s\pi/2)))^N \zeta_K(s) \end{aligned} \tag{1}$$

thus, if ℓ is any positive even integer, we have

$$|\zeta_K(1-\ell)| = A^{2\ell-1} \Gamma(\ell)^N (2^{1-\ell})^N \pi^{-\frac{N}{2}} |\zeta_K(\ell)|. \tag{2}$$

Let us see that we can determine N. Let $x > 0$ be a real number. Then from the equation (2), we have the following equation;

$$|\zeta_K(1-\ell)|/\Gamma(\ell)^x = (A^2 2^{-N})^\ell \Gamma(\ell)^{N-x} 2^N \pi^{-\frac{N}{2}} A^{-1} |\zeta_K(\ell)| \tag{3}$$

By Stirling's formula,

$$C^s/\Gamma(s) \to 0 \text{ as } s \to \infty$$

for any real $C > 0$. Since $\zeta_K(\ell) \to 1$ as $\ell \to \infty$, therefore if $N > x$ the right-hand side of the equation (3) goes to ∞ if $\ell \to \infty$. If $N < x$ then the right-hand side of the Equation (3) approaches 0 as $\ell \to \infty$. Choose a sequence $\{a_n\}$ as in Proposition 7.2, and let $a_n = 1 - \ell_n$. By Propositions 7.1 and 7.2, we know the value of $|\zeta_K(1 - \ell_n)|$ up to an (unknown) constant independent of n, as long as n is sufficiently large. Therefore we can find out N using

$$|\zeta_K(1 - \ell_n)|/\Gamma(\ell_n)^x$$

by testing values of x and taking the limit as n goes to ∞.

Now we are ready to prove theorem 7.1. Let q be a rational number, and S be a finite set of primes. We define

$$(q)_{S-part} = \prod_{p \in S} p^{ord_p(q)}, \text{ and } (q)_{non-S-part} = q/(q)_{S-part}.$$

First, let us see that we can determine A. By equation (2) with $\ell = \ell_n$, we have

$$A = \lim_{n\to\infty} \exp\left[\frac{1}{2\ell_n - 1}\ln\left(\frac{|\zeta_K(1-\ell_n)|_{S-part}|\zeta_K(1-\ell_n)|_{non-S-part}}{\Gamma(\ell_n)^N(2^{1-\ell_n})^N\pi^{-\frac{N}{2}}|\zeta_K(\ell_n)|}\right)\right],$$

by Proposition 7.2 $|\zeta_K(1-\ell_n)|_{S-part}$ is eventually constant, therefore by properties of limits

$$A = \lim_{n\to\infty} \exp\left[\frac{1}{2\ell_n - 1}\ln\left(\frac{|\zeta_K(1-\ell_n)|_{non-S-part}}{\Gamma(\ell_n)^N(2^{1-\ell_n})^N\pi^{-\frac{N}{2}}|\zeta_K(\ell_n)|}\right)\right],$$

by Proposition 7.1 we know $|\zeta_K(1-\ell_n)|_{non-S-part}$. Then we can read off A. Hence we know the discriminant d_K. Here $\ell_n = 1 - a_n$ is a multiple of 4 since σ_i is even. Since the value $\cos(4m\pi/2)$ for integer m and the values of zeta function at positive integers not equal to 1 are positive, we know, by Equation (1), that values $\zeta_K(a_n)$ are positive. By proposition 7.1, we know the non-S-part of the values of the zeta function at a_n, and by Proposition 7.2, the $S-$part is constant for n sufficiently large. Hence, with the functional equation, we can determine the $S-$part of the values of the zeta function at the sequence a_n for a large n, i.e, we have:

$$\begin{aligned}
\zeta_K(1-\ell_n)_{S-part} &= \lim_{m\to\infty} \frac{\zeta_K(1-\ell_m)}{\zeta_K(1-\ell_m)_{non-S-part}} \\
&= \lim_{m\to\infty} \frac{A^{2\ell_m-1}[\Gamma(\ell_m)2^{1-\ell_m}\pi^{-1/2}\cos((\ell_m\pi)/2)]^N\zeta_K(\ell_m)}{\zeta_K(1-\ell_m)_{non-S-part}} \\
&= \lim_{m\to\infty} \frac{A^{2\ell_m-1}[\Gamma(\ell_m)2^{1-\ell_m}\pi^{-1/2}]^N}{\zeta_K(1-\ell_m)_{non-S-part}}
\end{aligned}$$

for n sufficiently large. Therefore, by Proposition 7.1 we know the values $\zeta_K(1-\ell_n)$ for n sufficiently large.

To finish, let

$$\zeta_K(s) = \sum \frac{b_n}{n^s}.$$

Then we have

$$\sum_{m=1}^{\infty} \frac{b_m}{m^{\ell_m}} = A^{2(1-\ell_n)-1}\Gamma((1-\ell_n)/2)^N\Gamma((\ell_n)/2)^{-N}\zeta_K(1-\ell_n).$$

We know the values of the right-hand side of the above equation for n sufficiently large, which will be denoted by c_n. We know $b_1 = 1$, and

$$b_2 = \lim_{n\to\infty}(c_n - 1)2^{\ell_n}$$

Continuing the above process, we can determine all the coefficients $b'_m s$, so we can determine the zeta function $\zeta_K(s)$. This completes the proof of Theorem 7.1.

Let K, K' be totally real number fields, and let S be a finite set of primes containing all the primes which are ramified in K and K'. Then the number fields K and K' are linearly disjoint with $\mathbb{Q}(\zeta_{p^\infty})$ over $\mathbb{Q}$ for $p \notin S$. Let $K_\infty = K(\zeta_{p^\infty})$ and $K'_\infty = K'(\zeta_{p^\infty})$. Then we may identify $\mathrm{Gal}(K_\infty/K)$ and $\mathrm{Gal}(K'_\infty/K')$ since they are both naturally isomorphic to $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, so that we may compare the Iwasawa modules $X^-_{K(\zeta_p)}$ and $X^-_{K'(\zeta_p)}$ as $\Lambda[\Delta]-$modules. Then, from Theorem 7.1, we have the following corollary.

Corollary 7.1.1. *Let K and K' be totally real number fields. Let S be a finite set of primes containing all the primes which are ramified in K and K'. Assume that the Iwasawa modules $X^-_{K(\zeta_p)}$ and $X^-_{K'(\zeta_p)}$ are pseudo-isomorphic as $\Lambda[\Delta]-$modules for all $p \notin S$; then for every $s \in \mathbb{C}$*

$$\zeta_K(s) = \zeta_{K'}(s).$$

2 On Arithmetic Equivalence And Iwasawa Invariants

Throughout this section, we will assume basic knowledge of the representation theory of finite groups. Let us first briefly recall some results from Chapter 5.

Let K and K' be two number fields and L be a Galois extension of $\mathbb{Q}$ containing K and K'. The following are equivalent:

(a) $\zeta_K(s) = \zeta_{K'}(s)$

(b) $P_K(A) = P_{K'}(A)$ for every tuple A.

(c) $P_K(A) \doteq P_{K'}(A)$ for every tuple A.

(d) $H = \mathrm{Gal}(L/K)$ and $H' = \mathrm{Gal}(L/K')$ are Gassmann equivalent in $G = \mathrm{Gal}(L/\mathbb{Q})$.

We now add one more equivalence to the list.

Proposition 7.3. *Two subgroups H and H' of a finite group G are Gassmann equivalent if and only if $\mathbb{Q}[H\backslash G] \cong \mathbb{Q}[H'\backslash G]$ as $\mathbb{Q}[G]$-modules.*

Proof. "$\Rightarrow$" Let $\{\rho_1, \ldots, \rho_t\}$ be the right coset representatives of $H\backslash G$, and let $g \in G$. Then

$$(q_1 H\rho_1 + \cdots + q_t H\rho_t) \cdot g = q_1 H(\rho_1 g) + \cdots + q_t H(\rho_t g)$$

defines a G-linear action on $\mathbb{Q}[H\backslash G]$. Therefore,

$$\begin{aligned} T_g : \mathbb{Q}[H\backslash G] &\to \mathbb{Q}[H\backslash G] \\ v &\longmapsto v \cdot g \end{aligned}$$

defines a linear transformation. Thus, the map

$$\begin{aligned} D_H : G &\to \mathrm{GL}(\mathbb{Q}[H\backslash G]) \\ g &\longmapsto T_g \end{aligned}$$

is a representation of G. Let χ_H be the character of D_H. For every conjugacy class C of G, we have

$$\chi_H(C) = \frac{|C \cap H| \cdot |G|}{|H| \cdot |C|}.$$

Therefore if H and H' are Gassmann equivalent, we know that $|H| = |H'|$ and $|C \cap H| = |C \cap H'|$ for every conjugacy class C. Therefore, we have

$$\chi_H(C) = \chi_{H'}(C)$$

for every conjugacy class C, which implies $\chi_H = \chi_{H'}$. Thus, D_H and $D_{H'}$ are equivalent representations, meaning there exists a $\mathbb{Q}$-linear isomorphism $M : \mathbb{Q}[H\backslash G] \to \mathbb{Q}[H'\backslash G]$ such that $D_H(g)M = MD_{H'}(g)$ for every $g \in G$. Therefore, M induces an isomorphism of $\mathbb{Q}[G]$-modules.

"$\Leftarrow$" Reverse the previous argument. □

Let H and H' be Gassmann equivalent. Let $\{\rho_1, \cdots, \rho_t\}$ and $\{\rho'_1, \cdots, \rho'_t\}$ be right coset representatives of $H\backslash G$ and $H'\backslash G$, respectively. Let D_H, $D_{H'}$ and M be as in the above proposition. Then we may regard $D_H, D_{H'} : G \to \mathrm{GL}_t(\mathbb{Q})$ and $M \in \mathrm{GL}_t(\mathbb{Q})$ satisfying the following relation:

$$D_H(g)M = MD_{H'}(g) \tag{7.1}$$

for every $g \in G$. By clearing the denominators, we may assume that M is in $\mathrm{GL}_t(\mathbb{Z})$.

Let $M = (m_{ij})$. Since $g \in G$ permutes the bases $\mathcal{B}_H = \{H\rho_1, ..., H\rho_t\}$ and $\mathcal{B}_{H'} = \{H'\rho'_1, ..., H'\rho'_t\}$, there exist homomorphisms π, π' from G into the symmetric group S_t given by $\pi_g(i) = j$, where $H\rho_i g = H\rho_j$, and $\pi'_g(i) = j$, where $H'\rho'_i g = H'\rho'_j$. Therefore $D_H(g)$ and $D_{H'}(g)$ are permutation matrices, writing $M = D_H(g)^{-1} M D_{H'}(g)$, we obtain

$$m_{ij} = m_{\pi_g(i),\pi'_g(j)}$$

for all $g \in G$. We have the following proposition.

Proposition 7.4. *Let K and K' be arithmetically equivalent fields. Then there is an exact sequence of right $\mathbb{Z}_p[G]$-modules*

$$0 \to \mathbb{Z}_p[H\backslash G] \to \mathbb{Z}_p[H'\backslash G] \to A \to 0,$$

where A is a finite right-$\mathbb{Z}_p[G]$-module.

Proof. Let M be a matrix satisfying the condition

$$m_{ij} = m_{\pi_g(i),\pi'_g(j)}.$$

Define a map φ from $\mathbb{Z}_p[H\backslash G] \to \mathbb{Z}_p[H'\backslash G]$ by

$$\varphi(H\rho_i) = m_{i1}H'\rho'_1 + \cdots + m_{it}H'\rho'_t, \quad i = 1, \ldots, t,$$

Note that cokernel φ is a finitely generated $\mathbb{Z}_p$-module. By the Equation (7.1), φ is a right-$\mathbb{Z}_p[G]$-module homomorphism. Since M is invertible, φ is injective. Moreover, we have the following equation:

$$\det M \begin{pmatrix} H'\rho'_1 \\ \vdots \\ H'\rho'_t \end{pmatrix} = (\det M)M^{-1} \begin{pmatrix} \varphi(H\rho_1) \\ \vdots \\ \varphi(H\rho_t) \end{pmatrix} \in \mathrm{Im}(\varphi).$$

Hence, cokernel φ is killed by $\det M$, then cokernel φ is a $\mathbb{Z}_p/(\det M)\mathbb{Z}_p-$module, since $\mathbb{Z}_p$ is a principal ideal domain then $\mathbb{Z}_p/(\det M)\mathbb{Z}_p$ is finite, therefore cokernel φ is finite. This completes the proof. □

Now, the following question arises: in which cases do we have $A = 0$?. It is known that a projective module is determined by its character. Using that fact, we can partially answer this question.

Proposition 7.5. *If p does not divide $|H|$, then $\mathbb{Z}_p[H\backslash G] \cong \mathbb{Z}_p[H'\backslash G]$ as $\mathbb{Z}_p[G]$-modules.*

Proof. The proof for $\mathbb{Z}_p[H'\backslash G]$ is identical to the following proof for $\mathbb{Z}_p[H\backslash G]$. We fix the first right coset representative to be H, that is, $\rho_1 = 1$. Let $e : \mathbb{Z}_p[H\backslash G] \to Y$ and $f : W \to Y$ be $\mathbb{Z}_p[G]$-homomorphisms, with f surjective. We need to find a $\mathbb{Z}_p[G]$-homomorphism $g : \mathbb{Z}_p[H\backslash G] \to W$ such that $e = fg$.
It is easy to see that any $\mathbb{Z}_p[G]$-homomorphism from $\mathbb{Z}_p[H\backslash G]$ is determined by the image of H. Now, for every $h \in H$, we have $e(H) = e(Hh) = e(H)h$, so H stabilizes $e(H)$ in Y. Let $w \in W$ be any preimage of $e(H)$. Since $|H|$ is not divisible by p, it is invertible in $\mathbb{Z}_p$. Let

$$w^* = |H|^{-1} \sum_{h \in H} wh,$$

so that

$$f(w^*) = |H|^{-1} \sum_{h \in H} f(w)h = |H|^{-1} \sum_{h \in H} e(H) = e(H).$$

Clearly, H stabilizes w^*, so the map $H \mapsto w^*$ extends to the desired homomorphism g. Therefore, $\mathbb{Z}_p[H\backslash G]$ and $\mathbb{Z}_p[H'\backslash G]$ are projective $\mathbb{Z}_p[G]$-modules with the same character; hence, they are isomorphic. □

By Theorem (5.1), we have that arithmetically equivalent fields K and K' have the same normal closure. Let L be a normal closure of K and K'. The goal is to prove the following theorem.

Theorem 7.2 (Komatsu)**.** *Let K and K' arithmetically equivalent number fields. If p does not divide $[L:K]=[L:K']$, where L is the normal closure of K over $\mathbb{Q}$, then the Iwasawa modules X_K and $X_{K'}$ are isomorphic as $\Lambda-$modules.*

For the rest of this section, let p be a fixed prime number, and let

$$L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_\infty$$

be the basic $\mathbb{Z}_p$-extension over the field $L=L_0$. Define $\Gamma=\mathrm{Gal}(L_\infty/L)\cong\mathbb{Z}_p$. Also, let

$$\Lambda_K=\mathbb{Z}_p\left[[\mathrm{Gal}(K_\infty/K)]\right] \quad \text{and} \quad \Lambda_{K'}=\mathbb{Z}_p\left[\left[\mathrm{Gal}(K'_\infty/K')\right]\right].$$

Since $K\cap\mathbb{Q}_\infty$ is a finite Galois subextension of $\mathbb{Q}_\infty$, we have $K\cap\mathbb{Q}_\infty=\mathbb{Q}_n$ for some n. Similarly, $K'\cap\mathbb{Q}_\infty=\mathbb{Q}_{n'}$ for some n'. Since K and K' have the same normal core, we obtain $\mathbb{Q}_{n'}\subseteq K$ and $\mathbb{Q}_n\subseteq K'$, which implies $K\cap\mathbb{Q}_\infty=K'\cap\mathbb{Q}_\infty$. Thus, the Galois groups of the basic $\mathbb{Z}_p$-extensions K_∞/K and K'_∞/K' can be identified. Let

$$\Lambda=\mathbb{Z}_p\left[[\mathrm{Gal}(K_\infty/K)]\right]=\mathbb{Z}_p\left[\left[\mathrm{Gal}(K'_\infty/K')\right]\right]=\mathbb{Z}_p[[T]].$$

Since $L\cap K_\infty=K_n$, for some n, and $[L:K]=[L:K_n][K_n:K]=[L:K_n]p^n$. Therefore if $p\nmid[L:K]$ then $n=0$, i.e., $L\cap K_\infty=K$. Since $L\cap K_\infty=K$, the group H can be considered as $\mathrm{Gal}(L_n/K_n)$ for any $n\geq 0$, and it commutes with Γ. Write $\mathrm{Gal}(L/K)=H$. Hence the group H acts on X_L. Regard Λ_L as a subring of Λ_K, so that Λ_L acts on X_K.

Proposition 7.6. *Suppose that $p\nmid|H|$. Then the Iwasawa modules X_L^H and X_K are pseudo-isomorphic as Λ_L-modules.*

Proof. For each n, we choose integers c_n and t_n such that $c_n|H|\equiv 1 \mod p^{t_n}$, so that p^{t_n} exceeds the order of $A_{n,L}$ and $A_{n,K}$, where $A_{n,M}$ is the p-Sylow subgroup of the ideal class group of the n-th layer of the basic $\mathbb{Z}_p$-extension over a number field M. The lifting map

$$\begin{aligned} i_n : A_{n,K} &\to A_{n,L}^H \\ [\mathfrak{a}_n] &\to \prod_{\sigma\in H}([\sigma\tilde{\mathfrak{a}}_n]) \end{aligned}$$

where $\tilde{\mathfrak{a}}_n$ is a fractional ideal of L lying above $\mathfrak{a}_n$ is clearly well-defined. Let $N_{L/K}$ be the norm map on ideal classes. Let $[\mathfrak{b}_n]$ be an element of the kernel of the map i_n, then

$$[\mathfrak{b}_n]=\left(N_{L/K}i\left([\mathfrak{b}_n]\right)\right)^{c_n}=1. \tag{7.2}$$

Let $[\mathfrak{A}_n]$ be in $A_{n,L}^H$. We have the following equation:

$$[\mathfrak{A}_n]=\left([\mathfrak{A}_n]^{|H|}\right)^{c_n}=\left(i(N_{L/K}[\mathfrak{A}_n])\right)^{c_n}=i\left(N_{L/K}[\mathfrak{A}_n]^{c_n}\right). \tag{7.3}$$

The map

$$\begin{aligned} i : \varprojlim A_{n,K} &\to \varprojlim A_{n,L}^H \\ ([\mathfrak{a}_n])_{n=1}^\infty &\mapsto (i_n([\mathfrak{a}_n]))_{n=1}^\infty, \end{aligned}$$

by construction, it is well-defined and is a Λ_L-homomorphism since H and Γ commute with each other. In view of $\varprojlim A_{n,K}\cong X_K$ and $\varprojlim A_{n,L}^H\cong X_L^H$, we obtain the result. □

Lemma 7.2. *Let G be a group. For any prime number p, for any $\mathbb{Z}_p[G]$-module A, and a subgroup $H < G$,*

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H\backslash G], A) \cong A^H,$$

where A^H is the subset of elements of A fixed under H.

Proof. Recall that any $\mathbb{Z}_p[G]$-homomorphism from $\mathbb{Z}_p[H\backslash G]$ is determined by the image of the vector $H \cdot 1$. Define

$$\begin{aligned} Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H\backslash G], A) &\to A^H \\ \phi &\longmapsto \phi(H \cdot 1) \end{aligned}$$

then ϕ is clearly well-defined and injective. To show surjectivity, for any $a \in A^H$, consider ϕ_a such that $\phi_a(H \cdot 1) = a$. □

Let K and K' be two isomorphic number fields and ϕ be an automorphism of $\mathbb{Q}$ such that $\phi(K) = K'$. Let γ be a topological generator of $\mathrm{Gal}(K_\infty/K)$. Then $\gamma' = \phi\gamma\phi^{-1}$ is a topological generator of $\mathrm{Gal}(K'_\infty/K')$. We make X_K and $X_{K'}$ into $\Lambda = \mathbb{Z}_p[[T]]$-modules in the following way.

$$\gamma x = (1+T)x \quad \text{and} \quad \gamma' x' = (1+T)x',$$

where $x \in X_K$ and $x' \in X_{K'}$.

Proposition 7.7. *Let K and K' be two isomorphic number fields. Then the Iwasawa modules X_K and $X_{K'}$ are isomorphic as Λ-modules for any prime number p.*

Proof. Let m be an integer such that $\mathbb{Q}_\infty \cap K = \mathbb{Q}_m$ and $K_n = K\mathbb{Q}_{n+m}$ be the n-th layer of the basic $\mathbb{Z}_p$-extension of K. Since $\mathbb{Q}_{n+m}$ is the normal extension of $\mathbb{Q}$, $\phi(K_n) = K'_n$. Let $x = (x_1, \ldots, x_n, \ldots) \in X_K$. Let the fractional ideal $\mathfrak{a}_n$ be a representative of x_n. Define $\phi(x_n)$ to be the class of $\mathfrak{a}_n^\phi$. Then

$$N\gamma'_n \circ \phi(x_n) = (1 + \gamma'_n + \cdots + \gamma_n'^{p^n-1})\phi(x_n) = \phi(1 + \gamma_n + \cdots + \gamma_n^{p^n-1})(x_n) = \phi \circ N\gamma_n(x_n).$$

Hence ϕ induces a map from X_K to $X_{K'}$ which is also denoted by ϕ. Moreover, it is a Λ-module homomorphism;

$$T \cdot \phi(x) = (\gamma' - 1)\phi(x) = \gamma'\phi(x)/\phi(x) = \phi(\gamma x)/\phi(x) = \phi((\gamma - 1)x) = \phi(T \cdot x).$$

The map ϕ is trivially bijective. This completes the proof. □

Lemma 7.3 (Komatsu)**.** *Let K and K' be number fields such that $\zeta_K = \zeta_{K'}$. Let M be a finite Galois extension of $\mathbb{Q}$. Then we have $\zeta_{KM}(s) = \zeta_{K'M}(s)$.*

Proof. See Lemma 1 in [17]. □

Put $\Gamma = \mathrm{Gal}(L_\infty/L)$ and $\Lambda_L = \mathbb{Z}_p[[\Gamma]]$. Now we are ready to prove the Theorem 7.2.

Proof of the Theorem 7.2. Let m be an integer such that $K \cap \mathbb{Q}_\infty = \mathbb{Q}_m = K' \cap \mathbb{Q}_\infty$, where $\mathbb{Q}_m$ is the m-th layer of the basic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. Put $K_m = K\mathbb{Q}_m$ and $K'_m = K'\mathbb{Q}_m$. By Lemma 7.3,

$$\zeta_{K_m}(s) = \zeta_{K'_m}(s). \tag{7.4}$$

Let $G = \mathrm{Gal}(L/\mathbb{Q})$, $B = \mathrm{Gal}(L/\mathbb{Q}_m)$, $H = \mathrm{Gal}(L/K_m)$, and $H' = \mathrm{Gal}(L/K'_m)$. By the above equation, two subgroups H and H' of G are Gassmann equivalent in G. By Proposition 7.5, we have

$$\mathbb{Z}_p[H\backslash G] \cong \mathbb{Z}_p[H'\backslash G]$$

Also note that B is normal in G, and that H and H' act on X_L. Since $L \cap \mathbb{Q}_\infty = \mathbb{Q}_m$, B acts on X_L so that X_L is a right $\mathbb{Z}_p[B]$-module. Consider $\mathbb{Z}_p[G]$ as a left $\mathbb{Z}_p[B]$-module. Then we can form the tensor product:

$$X' = X_L \otimes_{\mathbb{Z}_p[B]} \mathbb{Z}_p[G].$$

Then X' is a right $\mathbb{Z}_p[G]$-module via the action of $\mathbb{Z}_p[G]$ on the second factor. Note that $p^m = [G : B]$. Let $\{\rho_1, \ldots, \rho_{p^m}\}$ be right coset representatives of $B\backslash G$ with $\rho_1 = 1$. Then

$$X' \cong X_L \otimes \rho_1 + \cdots + X_L \otimes \rho_{p^m},$$

as a Λ_L-module. Note that this is a direct sum. Let $h \in H$. Since $h \in B$ and B is normal in G, $\rho_i h \rho_i^{-1} \in B$ for any $\rho_i \in G$. Let $x \in X_L$.

$$(x \otimes \rho_i)h = x \otimes \rho_i h = x \otimes \rho_i h \rho_i^{-1} \rho_i = x^{\rho_i h \rho_i^{-1}} \otimes \rho_i \in X_L \otimes \rho_i. \tag{7.5}$$

Let $x_1 \otimes \rho_1 + \cdots + x_{p^m} \otimes \rho_{p^m} \in X'$, $g \in G$ and $\gamma \in \Gamma$. Then $\rho_i g = b_i \rho_{\pi_g(i)}$ for some permutation π_g on $\{1, \ldots, p^m\}$, where $b_i \in B$. Since γ commutes with b_i, we have the following equation:

$$\left(\sum x_i \otimes \rho_i\right) g\gamma = \left(\sum x_i^{b_i} \otimes \rho_{\pi_g(i)}\right)\gamma = \left(\sum x_i^{b_i\gamma} \otimes \rho_{\pi_g(i)}\right) = \left(\sum x_i^{\gamma} \otimes \rho_i\right) g = \left(\sum x_i \otimes \rho_i\right)\gamma g.$$

Therefore Λ commutes with the action of G on X'. Therefore

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H\backslash G], X') \cong (X')^H = \sum (X_L \otimes \rho_i)^H.$$

We have a Λ-module isomorphism: $\phi : X_L \otimes \rho_i \to X_L$ by sending $x \otimes \rho_i \to x$. Then,

$$\sum (X_L \otimes \rho_i)^H \cong \sum X_L^{\rho_i H \rho_i^{-1}}.$$

Since H and $\rho_i H \rho_i^{-1}$ are conjugate in G, their fixed fields are isomorphic. By Propositions 7.6 and 7.7, we have the following equation:

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H\backslash G], X') \cong \bigoplus_{p^m\text{-copies}} X_K.$$

Analogously, we have the following equation.

$$Hom_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[H'\backslash G], X') \cong \bigoplus_{p^m\text{-copies}} X_{K'}.$$

Since $\mathbb{Z}_p[H\backslash G] \cong \mathbb{Z}_p[H'\backslash G]$ then

$$\bigoplus_{p^m\text{-copies}} X_K \cong \bigoplus_{p^m\text{-copies}} X_{K'}$$

Therefore the Theorem 7.2 follows.

Bibliography

[1] Reza Akhtar. Cyclotomic euclidean number fields. *Senior Thesis, Harvard Univ*, 20, 1995.

[2] Daniel Barsky. Zêta p-adic functions of a ray class of totally real number fields. *Ultrametric Analysis Working Group*, 5:1–23, 1977.

[3] Tristram Bogart and Guillermo Mantilla-Soler. An ℓ-p switch trick to obtain a new proof of a criterion for arithmetic equivalence. *Research in Number Theory*, 5(1):1–5, 2019.

[4] Pierrette Cassou-Nogues. Negative integer values of zêta functions and p-adic zêta functions. *Inventiones mathematicae*, 51:29–59, 1979.

[5] Bart De Smit and Robert Perlis. Zeta functions do not determine class numbers. *arXiv preprint math/9410216*, 1994.

[6] Pierre Deligne and Kenneth A Ribet. Values of abelianl-functions at negative integers over totally real fields. *Inventiones mathematicae*, 59(3):227–286, 1980.

[7] Keiichi Komatsu. On zeta-functions and cyclotomic {Z_p}-extensions of algebraic number fields. *Tohoku Mathematical Journal, Second Series*, 36(4):555–562, 1984.

[8] Álvaro Lozano-Robledo. Desde fermat, lamé y kummer hasta iwasawa: Una introducción a la teoría de iwasawa. *Gac. R. Soc. Mat. Esp*, 15:251–276, 2012.

[9] Guillermo Mantilla-Soler. Density questions on arithmetic equivalence. *arXiv preprint arXiv:2106.01166*, 2021.

[10] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[11] Hough L Montgomery and J Myron Masley. Cyclotomic fields with unique factorization. 1976.

[12] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[13] Jangheon Oh. On zeta functions and iwasawa modules. *Transactions of the American Mathematical Society*, 350(9):3639–3655, 1998.

[14] Robert Perlis. On the equation $\zeta_K(s) = \zeta_{K'}(s)$. *Journal of number theory*, 9(3):342–360, 1977.

[15] Robert Perlis. On the class numbers of arithmetically equivalent fields. *Journal of Number Theory*, 10(4):489–509, 1978.

[16] Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.

[17] Kôji Uchida. Isomorphisms of galois groups of solvably closed galois extensions. *Tohoku Mathematical Journal, Second Series*, 31(3):359–362, 1979.

[18] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.

Estudiante: Carlos Alberto Pérez López

Director: Dr. Guillermo Mantilla Soler