ARITHMETIC EQUIVALENCE THROUGH GALOIS REPRESENTATIONS

by

Jerson Leonardo Caro Reyes

Thesis advisor

Ph.D Guillermo Mantilla-Soler

A thesis presented for the degree of
Master of Science in Mathematics

Departamento de Matemáticas
Facultad de Ciencias
Universidad de los Andes
Colombia
2016

Acknowledgements

I would like to thank my advisor Guillermo Mantilla-Soler. First of all, because his office was always open whenever I needed advice and guidance in solving all the problems that arose while writting this thesis. Second for the trust that he gave me, consistently he allowed this thesis to be my own work, but pointed me in the right the direction whenever he thought I needed it.

I would also like to thank my friends and classmates: Daniel Ávila, Santiago Pinzón, Hernan García, Julian Forero, Andres Galindo, Nicolas Walteros, Gustavo Chaparro, Edison Lopez, Nicolas Escobar, Jorge Muñoz, Cesar Venegas, Carolina Herrera and Yeini Montes, who gave me a support in many opportunities when I wanted to put aside mathematics for personal problems.

Finally, I must express my very profound gratitude to my mother and my brother for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of creation of this thesis. This accomplishment would not have been possible without them.

Thank you.

Abstract

An important objective in Algebraic number theory is the study of number fields and their ring of algebraic integers. One of the crucial arithmetic invariants associated with a number field K is its Dedekind zeta function $\zeta_K(s) = \prod \frac{1}{1-\|\mathfrak{P}\|^{-s}}$, where the product runs over all prime ideals $\mathfrak{P} \neq 0$ in the ring of algebraic integers O_K, and $\|\mathfrak{P}\| := |O_K/\mathfrak{P}|$. This function is the natural generalization of the Riemann zeta function and gives us arithmetic information about the number field. For example, if we compute its residue at the isolated singularity 1, we get a formula for the order of the class group, in the case of non real quadratic fields.

Then a natural question is: What are some necessary and sufficient conditions over two number fields so that these fields have the same Dedekind zeta function? In this sense, Robert Perlis [Per77] proved that two number fields K and K' are *arithmetically equivalent* (i.e., they have the same Dedekind zeta function) if and only if the subgroups $H := \mathrm{Gal}(N/K)$ and $H' := \mathrm{Gal}(N/K')$ of $G := \mathrm{Gal}(N/\mathbb{Q})$ are *Gassmann equivalents*, that is, $\left|c^G \cap H\right| = \left|c^G \cap H'\right|$, for all $c \in G$ and $c^G = \{gcg^{-1} : g \in G\}$ and N the normal closure of KK'. To show this, he uses an ad hoc process that uses complex analysis. Motivated by this, it arose the idea of addressing the problem via Artin's L-functions of specific Galois representations.

Introduction

A good example of the power of Algebraic Number Theory can be seen when it is used to find solutions to the Diophantine equation $x^2 + y^2 = z^2$, with $xyz \neq 0$ and pairwise coprimes. For this purpose, we express this equation in $\mathbb{Z}[i]$ as $(x + yi)(x - yi) = z^2$. Assuming that this ring is a Unique Factorization Domain and since $(x + yi, x - yi) = 1$, we get that $x + yi$ is a square in $\mathbb{Z}[i]$, that is, $x + iy = (p + iq)^2$, and we obtain

$$x = p^2 - q^2, \qquad y = 2pq, \qquad z = p^2 + q^2.$$

In this sense, and with a similar process, Gabriel Lamé in March of 1847 gave a "proof" of Fermat's last theorem using the factorization in $\mathbb{Z}[\zeta]$, where ζ is a n-primitive root of the unity,

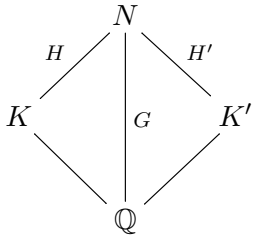
$$x^n + y^n = (x + y)(x + \zeta y)(x + \zeta^2 y) \cdots (x + \zeta^{n-1} y).$$

However, he assumed that this ring was a UFD. A few years before this, Kummer had already discovered that such unique factorization properties did not necessarily hold in these rings. He introduced the notion of ideals in an attempt to salvage the lack of unique factorization. Furthermore, he introduced the class number, which is the order of the quotient of all fractional ideals by the principal ideals, and an analytic formula describing it from the Dedekind zeta function $\zeta_K(s)$ in cases like $\mathbb{Q}(i)$.

On the other hand, the Dirichlet theorem on arithmetic progressions is also obtained by studying $\zeta_K(s)$ (see Chapter 2 and Chapter 3) and more generally the Tchebotarev density theorem, since Dirichlet density is defined using the fact that this zeta function has a singularity at 1.

Then a natural question is: What are some necessary and sufficient conditions over two number fields so that these fields have the same Dedekind zeta function? In 1977, Robert Perlis showed a characterization of the number fields via the Dedekind zeta function which he calls arithmetic equivalent [Per77]. The proof uses some results in complex analysis and group theory. It begins with two number fields K and K' and a Galois extension $N/\mathbb{Q}$ with $K, K' \subset N$, thus, he considers the subgroups $H := \mathrm{Gal}(N/K)$ and $H' := \mathrm{Gal}(N/K')$ of $G := \mathrm{Gal}(N/\mathbb{Q})$. This situation can be

visualized in the following diagram:



He proves that this fields are arithmetic equivalents if and only if the groups H and H' have a special property as subgroups of G, called Gassmann equivalence i.e., $\left|c^G \cap H\right| = \left|c^G \cap H'\right|$, for all $c \in G$ and $c^G = \{gcg^{-1} : g \in G\}$. In order to show that, he uses a intermediate step using the ramification of the primes in $\mathbb{Q}$.

In 2016 Mantilla-Soler [MS16] improves Perlis' result using Artin L-series of Galois Representations. In order to achieve this, he weakens the hypothesis in the intermediate step of Perlis' proof. The objectives of this thesis are the following: First, we show an alternative proof of [MS16], so that it can be understood by people with less expertise in Galois Representations. Second, we give a proof of another characterization of arithmetic equivalence, using the tools stated above.

In this thesis we assume that the reader has a basic knowledge of topics usually covered in a first course in Algebraic Number Theory, but we will recall basic concepts for the reader's convenience.

The first chapter gives a brief motivation for studying of Dedekind zeta functions. Furthermore, we define some important invariants in basic algebraic number theory and general topics such as Dirichlet series, Artin L-functions, Galois representations, among others.

In the second chapter, it is proved the Class number formula, that is, the formula for the residue at 1 of the Dedekind zeta function. For this purpose, we will use lattices to compute the residue of a partial Dedekind zeta function i.e., the sum restricted to all integral ideals in a fixed class in the Class group; this will be useful since such residue does not depend on the class, so, we obtain the class number formula multiplying this residue for the class number h_k. Also, we give some applications of this formula to compute the Class number of a complex quadratic field. Thanks to this result, we can define the Dirichlet density, which is a measure for the prime numbers.

The third chapter uses the Dirichlet density to "count" in a Galois extension L/K how many primes in K have their Frobenius automorphism in a fixed conjugacy class of $\mathrm{Gal}(L/K)$. This is the Tchebotarev density theorem. We begin by reducing the general case of the theorem to the cyclic case while simultaneously proving it for Cyclotomic extensions. Finally we will prove the theorem for cyclic extension using a weak form of the Dirichlet density theorem.

In the last chapter we sketch the proof of Perlis' theorem and we give another one using the tools stated above. In the same way we prove a theorem which gives other characterization of arithmetic equivalence, based in the number of primes over a rational prime. This theorem was shown by Stuart, Donna and Perlis, Robert in 1995 [SP95].

Contents

Chapter 1

Preliminaries

1.1 Basic Algebraic Number Theory

We summarize here the most important notions and results used in this thesis. For basic notation and definitions, the reader can see [Neu13] Chapter I. We begin with a number field K, and its ring of integers O_K, which is the set of all $\alpha \in K$, such that its minimal monic polynomial belongs to $\mathbb{Z}[x]$. Since O_K is a Dedekind Domain, i.e. is an integrally closed Noetherian domain with Krull dimension one (every nonzero prime ideal is maximal), this ring has the unique factorization property for prime ideals. We denote by $\|\mathfrak{A}\| := |O_K/\mathfrak{P}|$, for any integral ideal of K. So, if $p \in \mathbb{Z}$ is a prime, then

$$pO_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

has a prime decomposition in O_K with ramification indices $e(\mathfrak{P}_i/p) := e_i$ and residue degrees $f(\mathfrak{P}_i/p) = [\mathbb{F}_{\mathfrak{P}_i} : \mathbb{F}_p]$, where $\mathbb{F}_{\mathfrak{P}_i} = O_K/\mathfrak{P}_i$. Then the following *fundamental equality* holds:

$$\sum_{i=1}^{g} e(\mathfrak{P}_i/p) f(\mathfrak{P}_i/p) = [K : \mathbb{Q}].$$

Observation 1. We classify some rational primes (i.e. the primes in $\mathbb{Z}$) from their decomposition in primes of O_K.

- We say that p is totally split or splits completely if g, the number of primes in O_K over it, is equal to $[K : \mathbb{Q}]$.
- The prime p is called inert if pO_K is a prime ideal of O_K.
- The prime p is called ramified if some of these $e(\mathfrak{P}/p)$ is greater than 1, and it is called unramified in any other case.

Ramified primes are characterized by the following fact: Let $x_1, \ldots, x_n \in O_K$ be an integral basis for K over $\mathbb{Q}$. We define the **discriminant** as follows: $\text{disc}(O_K) = \det(\text{Tr}(x_i x_j))$, where $\text{Tr}(x)$ is the trace of the linear operator multiplication by x. Since $\text{Tr}(O_K) \subset \mathbb{Z}$, then $\text{Tr}(x_i x_j) \in \mathbb{Z}$, so

that $\text{disc}(O_K) \in \mathbb{Z}$. For more details and the proof that $\text{disc}(O_K)$ is independent of the integral base, see [Neu13] chapter I, section 2. The prime ideals which ramify are exactly the primes that divide the discriminant. Hence there exist only a finite number of primes that ramify. For quadratic fields, we know the explicit value for the discriminant. Let $K = Q(\sqrt{d})$, with $d \neq 1$ an square free integer, then:

$$\text{disc}(O_K) = \begin{cases} d & \text{if} \quad d \equiv_4 1 \\ \\ 4d & \text{if} \quad d \equiv_4 3, 2 \end{cases}$$

Also the following theorem helps to find the decomposition of a rational prime in a number field.

Theorem 1 (Dedekind Criterion). Let $K = \mathbb{Q}(\alpha)$ be a number field, $f(x)$ the minimal monic polynomial in $\mathbb{Z}[x]$ of α, and take a prime $p \in \mathbb{Z}$ such that $p \nmid [O_K : \mathbb{Z}[\alpha]]$. Let $\prod_{i=1}^{g} \overline{h_i}^{e_i}(x)$ denote the monic irreducible factorization of $\overline{f(x)}$ in $\mathbb{F}_p[x]$. Then the prime factorization of pO_K has the form

$$pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where $\mathfrak{p}_i = \langle p, h_i(\alpha) \rangle$ for any $h_i \in \mathbb{Z}[x]$ lifting $\overline{h_i} \in \mathbb{F}_p[x]$. Moreover, there is an isomorphism of residue fields $\mathbb{F}_p[x]/\overline{h_i} \to O_K/\mathfrak{p}_i$ via $x \to \alpha \, \text{mod} \mathfrak{p}_i$, so the residue field degree $f_i(\mathfrak{p}_i/p)$ is equal to $\deg(\overline{h_i})$.

For a proof of this theorem the reader can see [Jan96] Theorem 7.4, page 37.

If the extension is Galois, we have some important results with respect to this decomposition. For example if $G := \text{Gal}(K/\mathbb{Q})$ is its Galois group, then G acts transitively in the prime ideals of O_K over each rational prime p, hence by unique factorization for each rational prime its ramification indices coincide, and the same occurs for the residue degrees.

Given a Galois extension of number fields L/K and $\mathfrak{p}$ prime in L, we can define $D_{\mathfrak{p}}(L/K)$ and $I_{\mathfrak{p}}(L/K)$ the decomposition and inertia subgroups of G, respectively,

$$D_{\mathfrak{p}}(L/K) := \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\},$$

and

$$I_{\mathfrak{p}}(L/K) := \{\sigma \in G : \sigma(x) \equiv x (\text{mod } \mathfrak{p}) \text{ for all } x \in O_L\}.$$

Clearly $I_{\mathfrak{p}}(L/K) \leq D_{\mathfrak{p}}(L/K)$. Whenever there is no possible ambiguity we denote these, with $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$, respectively, and $e = |I_{\mathfrak{p}}|$, where e is the common ramification index.

Now, we can define the homomorphism $\pi_{\mathfrak{p}}$ from $D_{\mathfrak{p}}$ onto $\text{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ defined by the restriction of $\sigma \in D_{\mathfrak{p}}$ to O_K. It can be shown that this homomorphism is surjective and its kernel is $I_{\mathfrak{p}}$ [see [Jan96] Chapter III, section 1]. Hence $I_{\mathfrak{p}} \trianglelefteq D_{\mathfrak{p}}$ and $D_{\mathfrak{p}}/I_{\mathfrak{p}}$ is isomorphic to $\text{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ which is cyclic. So, when p is unramified $D_{\mathfrak{p}}$ is cyclic; then we can define the Frobenius automorphism $\text{Frob}_{\mathfrak{p}}(L/K)$, which is a generator of $D_{\mathfrak{p}}$, and is the unique that satisfies the following equation

$$\text{Frob}_{\mathfrak{p}}(L/K)(x) \equiv x^{\|\mathfrak{p}\|} \, (\text{mod } \mathfrak{p}), \qquad x \in O_K.$$

Whenever there is no possible ambiguity we denote the Froenius element by $\text{Frob}_{\mathfrak{p}}$.

Example 1. Let $K = \mathbb{Q}(\zeta_3)$. We can classify the prime ideals from its decomposition in three different sets (by the fundamental equivalence) the ones that ramify, the ones that are inert and the ones that split completely, as follow:

(a) Since $\text{disc}(O_K) = -3$ then the only rational prime that ramifies is 3, hence over $3O_K$ there is only one prime $\mathfrak{P}$, and from the fundamental equality, we have $3O_K = \mathfrak{P}^2$. Because the norm is multiplicative, we have $\|\mathfrak{P}\| = 3$.

(b) Notice that a prime split completely if and only if its decomposition subgroup is the trivial group. Since the Frobenius automorphism generates this subgroup, we have that p splits completely if and only if

$$\text{Frob}_p\,(L/K)\,\zeta_3 \equiv \zeta_3^p (\text{mod } \mathfrak{P}),$$

and that happens, if and only if $p \equiv 1 \mod 3$. Finally, from the fundamental equality, we have $pO_K = \mathfrak{P}_1\mathfrak{P}_2$, with $\|\mathfrak{P}_\text{i}\| = p$ for $(i = 1, 2)$.

(c) Finally a prime is inert if and only if $p \equiv 2 \mod 3$, and we have $\|pO_K\| = p^2$.

On the other hand we can characterize the units in O_K, denoted by $(O_K)^*$ from the following theorem.

Theorem 2 (Dirichlet's Unit Theorem). The group of units $(O_K)^*$ is the direct product of the torsion subgroup $\mu(K)$ (the finite cyclic subgroup of all roots of unity in K) and a free abelian group of rank $r + s - 1$.

In other words: there exist units $\xi_1, \ldots, \xi_{r+s-1}$, called fundamental units, such that any other unit ξ can be written uniquely as a product

$$\xi = \zeta \xi_1^{e_1} \cdots \xi_{r+s-1}^{e_{r+s-1}}$$

with ζ a root of unity and integers e_i.

For details of the proof the reader can see [Neu13], page 42, Theorem 7.4.

Finally, and also from the fact that O_K is a Dedekind Domain, we can consider I_K the group of all fractional ideals of K, and P_K the subgroup of all fractional principal ideals. Set $Cl(K) = I_K/P_K$ the quotient group called *the ideal class group*. $Cl(K)$ is finite from lattice theory [see [Neu13] chapter I, section 5], so, we denote by h_K its order.

A Brief Motivation

One of first results in arithmetic is the infinitude of the primes. It is well known that Euclides gave a proof obtaining a new prime from a finite list of these. But Euler also gave a proof using the Riemann zeta function presented as a product, as follows: suppose that there are only a finitely many primes, then

$$\zeta(s) = \sum_{n \geq 0} \frac{1}{n^s} = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}, \qquad \text{for Re}(s) > 1$$

the product on the right is finite and converge for any $s \neq 0$ and in the case of $s = 1$ the sum is the harmonic series, in which case does not converge.

The last proof shows an application of the zeta function. The following definition is a natural generalization of this function.

Definition 1. A Dirichlet series is a function of the form

$$f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s},$$

where the $a(n)$ are complex numbers and $s = \sigma + it$ is a complex variable.

Example 2. (a) The Riemann zeta function is a Dirichlet serie taking $a(n) = 1$ for all n.

(b) The function

$$\zeta_K(s) = \sum_{\substack{\mathfrak{A} \text{ integral} \\ \mathfrak{A} \neq 0}} \frac{1}{\|\mathfrak{A}\|^s},$$

is a Dirichlet series taking $a(n)$ the number of integral ideals of norm n. In the Corollary 1 we will prove that this function is exactly the Dedekind zeta function.

The idea in the following section is to find the convergence range of a Dirichlet series and compute explicitly the residue at the isolated singularity 1 of the Riemann zeta function.

1.2 Invariants of the Dirichlet series

Before starting, we prove the following Lemma from [Jan96], which in particular states that for Dirichlet series such that $\sum_{n \leq x} a(n)$ is bounded by a linear function for x large enough, this series is analytic for $s > 1$. This is the case of Dedekind zeta functions.

Lemma 1. Let $f(s)$ be a Dirichlet series and let

$$S(x) = \sum_{n \leq x} a(n).$$

Suppose there exist positive constants a and b such that $|S(x)| \leq ax^b$ for all $x \geq r$ for some positive r. Then the series $f(s)$ is uniformly convergent in

$$D(b, \delta, \varepsilon) := \{s : Re(s) \geq b + \delta, |\arg(s - b)| \leq \pi/2 - \varepsilon\},$$

for any positive δ, ε.

Proof. Observe that $a(n) = S(n) - S(n-1)$, so for $v \geq u + 1$ we have

$$\begin{aligned}
\left| \sum_{n=u}^{v} \frac{a(n)}{n^s} \right| &= \left| \sum_{n=u}^{v} \frac{S(n)}{n^s} - \sum_{n=u-1}^{v-1} \frac{S(n)}{(n+1)^s} \right| \\
&= \left| \frac{S(v)}{v^s} - \frac{S(u-1)}{u^s} + \sum_{n=u}^{v-1} S(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| \\
&\leq \left| \frac{S(v)}{v^s} \right| + \left| \frac{S(u-1)}{u^s} \right| + \sum_{n=u}^{v-1} |S(n)| \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right|.
\end{aligned}$$

Now notice that

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = s\int_n^{n+1} \frac{dt}{t^{s+1}}.$$

Since $|n^s| = n^\sigma$ if $s = \sigma + it$, $n > 0$ and $|S(x)| \leq ax^b$ (by hypothesis), we have

$$\left|\sum_{n=u}^{v} \frac{a(n)}{n^s}\right| \leq \frac{a}{v^{\sigma-b}} + \frac{a}{u^{\sigma-b}} + \sum_{n=u}^{v-1} |s|\,(an^b)\left|\int_n^{n+1} \frac{df}{t^{s+1}}\right|,$$

and note that

$$\sum_{n=u}^{v-1} |s|\,(an^b)\left|\int_n^{n+1} \frac{df}{t^{s+1}}\right| \leq a\,|s|\left|\int_n^{\infty} \frac{df}{t^{s+1-b}}\right| = \frac{a\,|s|}{(\sigma-b)u^{\sigma-b}}.$$

From the fact that $v > u > 0$, and $\sigma - b > 0$, we set $\frac{a}{v^{\sigma-b}} \leq \frac{a}{u^{\sigma-b}}$, then

$$\left|\sum_{n=u}^{v} \frac{a(n)}{n^s}\right| \leq \frac{2a}{u^{\sigma-b}} + \frac{a\,|s|}{(\sigma-b)u^{\sigma-b}},$$

now, let θ the argument of $s - b$, then $\cos(\theta) = \frac{\sigma-b}{|s-b|}$, and since $\sigma - b = Re(s) - b \geq \delta$ by hypothesis, we get

$$\frac{|s|}{\sigma-b} \leq \frac{|s-b|+b}{\sigma-b} \leq \frac{1}{\cos(\theta)} + \frac{b}{\delta},$$

since $s \in D(b, \delta, \varepsilon)$, we have $|\arg(s-b)| = |\theta| \leq \pi/2 - \varepsilon$, hence there exist a constant $M \geq \frac{1}{\cos(\theta)}$. Finally for any ε_0, you can find n large enough such that

$$\frac{2a}{u^{\sigma-b}} + \frac{a\,|s|}{(\sigma-b)u^{\sigma-b}} \leq \frac{2a + M + b/\delta}{u^{\sigma-b}} \leq \varepsilon_0.$$

□

Below we show that the Riemman Zeta function has residue 1 at its singularity 1.

Proposition 1. Let $\zeta(s)$ be the Riemman zeta function, then the residue at the isolated singularity 1, is equal to 1, i.e.

$$\lim_{s\to 1^+} (s-1)\zeta(s) = 1.$$

Proof. Consider the series

$$\begin{aligned}
\zeta(s)\left(1 - 2^{1-s}\right) &= \zeta(s) - 2^{1-s}\zeta(s) \qquad \text{[by lemma 1]} \\
&= \sum_{n=1}^{\infty} \frac{1}{n^s} - 2^{1-s}\sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{\infty} \frac{2}{2n^s} \\
&= \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}.
\end{aligned}$$

Now we have

$$\lim_{s\to 1^+}(s-1)\zeta(s) = \lim_{s\to 1^+}\frac{s-1}{1-2^{1-s}}\cdot(1-2^{1-s})\zeta(s) = \lim_{s\to 1^+}\frac{s-1}{1-2^{1-s}}\cdot\lim_{s\to 1^+}(1-2^{1-s})\zeta(s)$$
$$= \lim_{s\to 1^+}\frac{s-1}{1-2^{1-s}}\cdot\lim_{s\to 1^+}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s}.$$

Applying l'Hopital's rule for the first limit (because $s-1$ and $1-2^{1-s}$ are analytic), we obtain

$$\lim_{s\to 1^+}\frac{s-1}{1-2^{1-s}} = \lim_{s\to 1^+}\frac{1}{2^{1-s}\ln(2)} = \frac{1}{\ln(2)}.$$

Now Lemma 1 states that the Dirichlet series in the second limit is uniformly convergent in $D(0,\delta,\varepsilon)$, because the sum of the first n coefficients is 0 or 1. In particular it is analytic in the disk $|s-1|<\frac{1}{2}$, i.e.

$$\lim_{s\to 1^+}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s} = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n} = \ln(2).$$

□

Now, we can characterize the Dirichlet series which converge and agree for s sufficiently large.

Lemma 2. Let

$$f(s) = \sum_{n=1}^{\infty}\frac{a(n)}{n^s} \text{ and } g(s) = \sum_{n=1}^{\infty}\frac{b(n)}{n^s},$$

be two Dirichlet series, such that are uniformly convergent and $f(s)=g(s)$ for $\mathrm{Re}(s)>b$ for some $b\in\mathbb{R}$. Then $a(n)=b(n)$ for all $n\in\mathbb{Z}^+$.

Proof. Notice that

$$\lim_{s\to\infty}f(s) = a(1) \text{ and } \lim_{s\to\infty}g(s) = b(1),$$

then $a(1)=b(1)$, hence

$$\sum_{n\geq 2}\frac{a(n)}{n^s} = \sum_{n\geq 2}\frac{b(n)}{n^s},$$

Multiplying by 2^s, and letting $s\to\infty$ we obtain that $a(2)=b(2)$. Inductively we get that $a(m)=b(m)$, for all $m\in\mathbb{Z}^+$. □

Now, following the ideas in [FT93] we will show that the Dedekind zeta function converges for $s>1$. Before we need the following lemma.

Definition 2. Let $\{b_n\}$ a sequence of complex numbers with $b_n\neq 1$, for each n, and consider the product $\prod_{n=1}^{\infty}(1+b_n)$, it is said to *converge* if the partial products $\prod_{n=1}^{m}(1+b_n)$ converge to a non-zero value. We call that this product converges absolutely, if $\prod_{n=1}^{\infty}(1+|b_n|)$ converges. It is well known that if $\prod_{n=1}^{\infty}(1+b_n)$ converges absolutely, then it converges.

Lemma 3. Let $\{b_n\}$ be a sequence of complex numbers. The product $\prod_{n=1}^{\infty}(1+|b_n|)$ converges absolutely if and only if the series $\sum_{n=1}^{\infty} b_n$ converges absolutely.

Proof. We can assume that $b_n \leq 0$. Set $P_m = \prod_{n=1}^{m}(1+b_n)$ and $S_n = \sum_{n=1}^{m} b_n$ and notice that $\{P_n\}$ and $\{S_n\}$ are monotonic increasing sequences. Since $P_n \geq 1 + S_n$, we have that $\sum_{n=1}^{\infty} b_n$ converges if $\prod_{n=1}^{\infty}(1+|b_n|)$ does.

The Taylor expansion of the exponential function says that for $b \geq 0$, e^b and so $e^{S_n} \geq P_n$, so, if $\sum_{n=1}^{\infty} b_n$ converges, then $\prod_{n=1}^{\infty}(1+|b_n|)$ is upper bounded. □

Lemma 4. The Dedekind zeta function

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \|\mathfrak{p}\|^{-s}\right)^{-1},$$

converges for $s > 1$.

Proof. Notice that

$$\begin{aligned} 1 + \|\mathfrak{p}\|^{-s} <& 1 + (\|\mathfrak{p}\|^{s} - 1)^{-1} \\ =& (1 - \|\mathfrak{p}\|^{-s})^{-1} \leq 1 + 2\|\mathfrak{p}\|^{-s}, \end{aligned}$$

where the last inequality is obtained from $\|\mathfrak{p}\|^{-s} \geq 2$. Set $(1 - \|\mathfrak{p}\|^{-s})^{-1} = 1 + b_{\mathfrak{p}}$. By the fundamental equality we have that

$$\begin{aligned} \sum_{\mathfrak{p}|p} b_{\mathfrak{p}} =& \sum_{\mathfrak{p}|p} (1 - \|\mathfrak{p}\|^{-s})^{-1} - 1 \\ \leq& \sum_{\mathfrak{p}|p} 2\|\mathfrak{p}\|^{-s} \leq 2[K:\mathbb{Q}]p^{-s}, \end{aligned}$$

since $\|\mathfrak{p}\|^{-s} \geq p$ and the number the primes of O_K above p are at most $[K:\mathbb{Q}]$, hence

$$\sum_{\mathfrak{p}} b_{\mathfrak{p}} \leq 2[K:\mathbb{Q}] \sum_{p} p^{-s} \leq 2[K:\mathbb{Q}]\zeta(s),$$

then $\sum_{\mathfrak{p}} b_{\mathfrak{p}}$ converges, and for this reason $\prod_{\mathfrak{p}}(1 - \|\mathfrak{p}\|^{-s})^{-1})$ converges because of the Lemma 3. □

1.3 Artin's L-functions

The idea in this section is to define the Artin's L- functions. This will allow us to write some Dirichlet series like an Euler product. The Dedekind zeta functions are particular cases of Artin's L-functions.

Definition 3. A modulus for K is a formal product as follows

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})},$$

where the product runs over all finite primes (the integral prime ideals), infinite real primes (the real embeddings $K \hookrightarrow \mathbb{R}$) and infinite complex primes (one of each pair of conjugate complex embeddings $K \hookrightarrow \mathbb{C}$). Each exponent $n(\mathfrak{p})$ is a nonnegative integer, and $n(\mathfrak{p}) \neq 0$ for only a finite number of $\mathfrak{p}$. In the case that $\mathfrak{p}$ is a real infinite prime then $n(\mathfrak{p}) = 0$ or 1, and $n(\mathfrak{p}) = 0$ in the case that $\mathfrak{p}$ is a complex infinite prime.

Also, we can consider $\mathfrak{m}$ as a product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where

$$\mathfrak{m}_0 = \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{n(\mathfrak{p})}, \qquad \mathfrak{m}_\infty = \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}^{n(\mathfrak{p})}.$$

For a modulus $\mathfrak{m}$ of K, let $I_\mathfrak{m}$ be the multiplicative subgroup of fractional ideals of K relatively prime to $\mathfrak{m}_0$, i.e., $\mathfrak{a} \in I_\mathfrak{m}$ if and only if there is not $\mathfrak{p}|\mathfrak{a}$, with $n(\mathfrak{p}) > 0$. Also we define $U^\mathfrak{m}$ be the multiplicative subgroup of principal fractional ideals $\langle\alpha\rangle$, with $\alpha \in K^*$ satisfying the conditions $\alpha \equiv 1 \mod \mathfrak{p}^{n(\mathfrak{p})}$, and for σ a real embedding of K dividing $\mathfrak{m}$, $\sigma(\alpha) > 0$. Then, we can consider $I_\mathfrak{m}/U^\mathfrak{m}$, which has finite order, in the same way that the Class Group (for details, see Chapter IV, section 2, Lemma (2.3) [Jan96]).

Example 3. (a) If $n(\mathfrak{p}) = 0$ for all $\mathfrak{p}$, then $I_\mathfrak{m}$ is exactly I_K, and $U^\mathfrak{m}$ are the principal ideals P_K. Obviously $I_\mathfrak{m}/U^\mathfrak{m}$ is the class group.

(b) Let m be an integer that is either odd or divisible by 4, and let $\mathfrak{m} = (m\mathbb{Z})\cdot\infty$ where ∞ denotes the real prime of $\mathbb{Q}$. Then $I_\mathfrak{m}$ is the set of all ideals $(a) = \prod(p)^{r(p)}$ where $(m, p) = 1$. And $U^\mathfrak{m}$ are the principal ideals generated by $\ell = a/b$, with $(a, m) = (b, m) = 1$, $\ell > 0$ and $\nu_p(a - 1) \leq r$ if $p^r|m, r > 0$. Therefore there is a well-defined map $(b/c) \to \overline{b}^m \cdot (\overline{c}^m)^{-1} : I_\mathfrak{m} \to (\mathbb{Z}/m\mathbb{Z})^*$, which one can show induces an isomorphism $I_\mathfrak{m}/U^\mathfrak{m} \to (\mathbb{Z}/m\mathbb{Z})^*$.

1.3.1 Zeta and L-functions for number fields

We begin, with a brief motivation of L-functions for $\mathbb{Q}$, the rational numbers.

Example 4. Consider the following series

$$\sum_{n\geq 0} \frac{1}{9n^2 + 9n + 2} = \sum_{n\geq 0} \left(\frac{1}{3n + 1} - \frac{1}{3n + 2} \right).$$

This is a Dirichlet series; if we consider the nontrivial homomorphism $\chi : (\mathbb{Z}/3\mathbb{Z})^* \to \{\pm 1\}$, then

$$\sum_{n\geq 0} \frac{1}{9n^2 + 9n + 2} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where by abuse of notation we denote the extension of χ to $\mathbb{Z}$ by χ. Such extension is: $\chi(n) = \chi(n \bmod 3)$, where $\chi(3k) = 0$.

Definition 4. If k is a integer bigger than 1, then a function $\chi(n)$ is called a Dirichlet character (mod k) if it is completely multiplicative, periodic with period k, and vanishes when $(n,k) > 1$.

An example is the principal character (mod k):

$$\chi(n) = \begin{cases} 1 & \text{if} \quad (n,k) = 1 \\ \\ 0 & \text{otherwise} \end{cases}$$

A Dirichlet character χ (mod k) is called primitive if for every proper divisor d of k there exists an integer $a \equiv_d 1$, with $(a,k) = 1$ and $\chi(a) \leq 1$.

Definition 5. Let χ be a nontrivial character of $(\mathbb{Z}/m\mathbb{Z})^*$. We can extend χ to $\mathbb{Z}^+$, and by abuse of notation we denote that extension with χ, as follows: $\chi(n) = \chi(\overline{n}^m)$ if $(n,m) = 1$ and $\chi(n) = 0$, otherwise. The Dirichlet series associated to χ is defined as follows:

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

It follows from the Lemma 1 that $L(s,\chi)$ is analytic for Re$(s) > 0$.

In general, let K be a number field, $\mathfrak{m}$ a modulus for K and χ a character of the groups $I^{\mathfrak{m}}/U^{\mathfrak{m}}$. Notice that we can see χ like a multiplicative homomorphism of $I^{\mathfrak{m}}$ with $U^{\mathfrak{m}}$ in its kernel, and we define $\chi(\mathfrak{A})$ as a value of χ at the coset $\mathfrak{A}U^{\mathfrak{m}}$. The L-serie associated to χ and $\mathfrak{m}$ is

$$L(s,\chi,\mathfrak{m}) = \sum_{\substack{\mathfrak{A} \in I^{\mathfrak{m}} \\ \mathfrak{A} \text{ integral} \\ \mathfrak{A} \neq 0}} \frac{\chi(\mathfrak{A})}{\|\mathfrak{A}\|^s},$$

where the sum runs over all integral ideals prime to $\mathfrak{m}$.

Theorem 3. For all s with $Re(s) > 1$ the function $L(s,\chi,\mathfrak{m})$ can be expressed as a uniformly convergent product

$$L(s,\chi,\mathfrak{m}) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \left(1 - \frac{\chi(\mathfrak{p})}{\|\mathfrak{p}\|^s}\right)^{-1},$$

where the product runs over all prime ideals not dividing $\mathfrak{m}$.

Proof. Notice that for $\mathfrak{p}$ a prime ideal we have

$$\left(1 - \frac{\chi(\mathfrak{p})}{\|\mathfrak{p}\|^s}\right)^{-1} = 1 + \frac{\chi(\mathfrak{p})}{\|\mathfrak{p}\|^s} + \frac{\chi(\mathfrak{p}^2)}{\|\mathfrak{p}^2\|^s} + \ldots,$$

since the character and the norm are multiplicative and the uniqueness of prime decomposition. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ all the prime ideals of norm less than or equal to n and $\mathfrak{p}_i | \mathfrak{m}$ for all $i = 1, \ldots, g$.

Now consider

$$\begin{aligned} \prod_i \left(1 - \frac{\chi(\mathfrak{p}_i)}{\|\mathfrak{p}_i\|^s}\right)^{-1} &= \sum_{e_j \geq 0} \frac{\chi(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g})}{\left\|\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}\right\|^s} \\ &= \sum_{\mathfrak{A}} \frac{\chi(\mathfrak{A})}{\|\mathfrak{A}\|^s}, \end{aligned}$$

where the sum runs over all integral ideals divisible exactly for some $\mathfrak{p}_i$'s. Then

$$\left| L(s,\chi,\mathfrak{m}) - \prod_{\|\mathfrak{p}\|\leq n} \left(1 - \frac{\chi(\mathfrak{p})}{\|\mathfrak{p}\|^s}\right)^{-1} \right| \leq \sum_{\|\mathfrak{A}\|>n} \left| \frac{\chi(\mathfrak{A})}{\|\mathfrak{A}\|^s} \right|.$$

Since $|\chi(\mathfrak{A})| = 1$ (because it is a root of the unity) and by Lemma 1 is uniformly convergent, so is 0 when $n \to \infty$. □

Corollary 1. In the case that χ is the trivial character, $K = \mathbb{Q}$ and $\mathfrak{m} = \emptyset$, $L(s,\chi,\mathfrak{m})$ is the Euler product of the Riemann zeta function. In particular

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \|\mathfrak{p}\|^{-s}\right)^{-1} = \sum_{\mathfrak{A}} \|\mathfrak{A}\|^{-s}.$$

1.3.2 Artin's L-functions

In the last section we defined the L-series depending on a modulus and a character of the group $I_{\mathfrak{m}}/U^{\mathfrak{m}}$. This is important when we want to neglect the ramified primes. In this section, we will define the Artin's L-functions. It is defined locally (at each prime) and the ramified primes are also included. An important result about Artin's L-functions is that whenever N/K is a Galois extension of number fields, then $\zeta_N(s) = a \cdot \zeta_K(s)$, where a depends only on the nontrivial characters of $\mathrm{Gal}(N/K)$.

We begin with a Galois extension N/K and ψ a character of $G = \mathrm{Gal}(N/K)$, then we can define the Artin's L-function, which is an Euler product:

$$L(s,\psi,N/K) = \prod_{\mathfrak{p}\in\mathcal{P}_K} L_{\mathfrak{p}}(s,\psi,N/K),$$

where $L_{\mathfrak{p}}$ (local Euler factor) is defined in the following sense: Let $\Psi : G \to Gl(V)$ be a finite dimension complex representation of G with character ψ. Then if $\mathfrak{p}$ is unramified, we define the local factor, as:

$$L_{\mathfrak{p}}(s,\psi,N/K) := \frac{1}{\det(\mathrm{Id} - \Psi(\mathrm{Frob}_{\mathfrak{P}}))\,\|\mathfrak{p}\|^{-s})}.$$

In the case that $\mathfrak{p}$ is ramified, we take $\mathfrak{P} \in \mathcal{P}_N$ be any prime over $\mathfrak{p}$. Let $\sigma(\mathfrak{P}/\mathfrak{p})$ be any Frobenius automorphism, i.e. $\overline{\sigma(\mathfrak{P}/\mathfrak{p})}$ generates $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$, and define the Euler factor as follows:

$$L_{\mathfrak{p}}(s,\psi,N/K) := \frac{1}{\det[(\mathrm{Id} - \Psi(\sigma(\mathfrak{P}/\mathfrak{p}))\,\|\mathfrak{p}\|^{-s})|_{V^{I_{\mathfrak{P}}}}]}.$$

where $V^{I_{\mathfrak{P}}}$ denotes the vector subspace of V, fixed by the inertia group $I_{\mathfrak{P}}$ under the action of $\Psi : G \to Gl(V)$. In the case that $V^{I_{\mathfrak{P}}} = 0$, we define $\det[(\mathrm{Id} - \Psi(\sigma(\mathfrak{P}/\mathfrak{p}))\,\|\mathfrak{p}\|^{-s})|_{V^{I_{\mathfrak{P}}}}] = 1$.

Example 5. (a) Let N/K be a Galois extension of number fields, and $G := \mathrm{Gal}(N/K)$. Consider the trivial character of G, then

$$L(s,\psi,N/K) = \prod_{\mathfrak{p}\in\mathcal{P}_K} \frac{1}{1 - \|\mathfrak{p}\|^{-s}} = \zeta_K(s).$$

(b) Let $K = \mathbb{Q}(i)$, $G := \mathrm{Gal}(N/K)$, and consider the ψ nontrivial character of G i.e., $\psi(Id) = 1$ and $\psi(\sigma) = -1$, where σ is the complex conjugacy. Then in the case that p is unramified, we have

$$L_p(s, \psi, K/\mathbb{Q}) = \frac{1}{\det[(\mathrm{Id} - \Psi(\mathrm{Frob}_p)p^{-s})]} = \frac{1}{1 - \psi(\mathrm{Frob}_p)p^{-s}},$$

Notice that $\mathrm{Frob}_p = Id$ if p is completely split ($p \equiv_4 1$) and $\mathrm{Frob}_p = \sigma$ if p is inert ($p \equiv_4 3$). On the other hand, 2 is the only prime that ramifies in K, because $\mathrm{disc}(O_K) = 4$, but $V^{I_2} = 0$, then $L_2(s, \psi, K/\mathbb{Q}) = 1$, so:

$$L(s, \psi, K/\mathbb{Q}) = \sum_{n \geq 0} \frac{(-1)^n}{(2n+1)^s}.$$

(c) Consider $K = \mathbb{Q}(\zeta_3)$. By the example 1. If we consider the nontrivial character of $\mathrm{Gal}(K/\mathbb{Q})$, like in the previous example, we have

$$\sum_{n \geq 0} \frac{1}{9n^2 + 9n + 2} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

where χ is the character like in Example 4.

Artin's Formalism

In this section, we will define the Artin's L-functions from the algebra of the representations, that is, the addition, restriction and induction.

Theorem 4. Let N/K be a Galois extension of number fields with group G and $\mathfrak{p} \in \mathcal{P}_K$,

(a) For characters ψ_1, ψ_2 of G we have:

$$L_{\mathfrak{p}}(s, \psi_1 + \psi_2, N/K) = L_{\mathfrak{p}}(s, \psi_1, N/K) \cdot L_{\mathfrak{p}}(s, \psi_2, N/K).$$

(b) Let $N/L/K$ be a tower of fields with L/K Galois and $\pi : \mathrm{Gal}(N/K) \to \mathrm{Gal}(L/K)$ the natural projection. Then for any character ψ of $\mathrm{Gal}(L/K)$ and its lifting $\psi' = \psi \circ \pi$ to G we have:

$$L_{\mathfrak{p}}(s, \psi, L/K) = L_{\mathfrak{p}}(s, \psi', N/K).$$

(c) Let $N/L/K$ be a tower of fields, ψ a character of $\mathrm{Gal}(N/L)$ and ψ^G the induced character of G. Then we have:

$$\prod_{\substack{\mathfrak{P} \in \mathcal{P}_L \\ \mathfrak{P}|\mathfrak{p}}} L_{\mathfrak{P}}(s, \psi, N/L) = L_{\mathfrak{p}}(s, \psi^G, N/K).$$

Proof. For (a) take $\Psi_1 : G \to Gl(V_1)$ and $\Psi_2 : G \to Gl(V_2)$ representations of G with characters ψ_1 and ψ_2, respectively. Then

$$L_{\mathfrak{p}}(s, \psi_1 + \psi_2, N/K) = \frac{1}{\det(\mathrm{Id} - \Psi_1 \oplus \Psi_2(F(\mathfrak{P}/\mathfrak{p}))\, \|\mathfrak{p}\|^{-s})}.$$

Now, we will compute the determinant

$$\det(\mathrm{Id} - \Psi_1 \oplus \Psi_2(F(\mathfrak{P}/\mathfrak{p}))\, \|\mathfrak{p}\|^{-s}) = \left| \mathrm{Id}_{V_1 \oplus V_2} - \begin{bmatrix} \Psi_1(F(\mathfrak{P}/\mathfrak{p})) & 0 \\ 0 & \Psi_2(F(\mathfrak{P}/\mathfrak{p}))) \end{bmatrix} \right|$$

$$= \begin{vmatrix} \mathrm{Id}_{V_1} - \Psi_1(F(\mathfrak{P}/\mathfrak{p})) & 0 \\ 0 & \mathrm{Id}_{V_2} - \Psi_2(F(\mathfrak{P}/\mathfrak{p}))) \end{vmatrix},$$

and we get the result.

The proof of (b) is obtained as follows: first, let $\mathfrak{P}/\mathfrak{p}/p$ the tower of primes, then if p in is nonramified in N is clear that $F(\mathfrak{P}/p)|_L = F(\mathfrak{P}/\mathfrak{p})$. In the case of p ramify in N, also we get this equality, because of the following exact sequence:

$$I_{\mathfrak{P}/\mathfrak{p}} \hookrightarrow I_{\mathfrak{P}/p} \twoheadrightarrow I_{\mathfrak{p}/p}.$$

For a proof of item (c), see [Kli98]. □

Theorem 5. Let N/K be a Galois extension of number fields and $G := \mathrm{Gal}(N/K)$. Then we have:

$$\zeta_N(s) = \prod_{\psi \in \widehat{G}} L(s, \psi, N/K)^{\dim \psi} = \zeta_K(s) \cdot \prod_{\psi \neq 1_G} L(s, \psi, N/K)^{\dim \psi}.$$

Proof. Notice that

$$1^G_{\{1\}}(g) = \sum_{x \in G} \dot{1}_{\{1\}}(x^{-1} g x) = \begin{cases} |G| & \text{if} \quad x = 1 \\ \\ 0 & \text{otherwise} \end{cases}$$

Now by the orthogonality relation among the characters, we have for all $a, b \in G$

$$\sum_{\psi \in \widehat{G}} \psi(a)\psi(b) = \begin{cases} |G| & \text{if} \quad a = b^{-1} \\ \\ 0 & \text{otherwise} \end{cases}$$

So,

$$1^G_{\{1\}}(x) = \sum_{\psi \in \widehat{G}} \psi(1)\psi(x) = \sum_{\psi \in \widehat{G}} \dim(\psi)\psi(x).$$

Then

$$\begin{aligned}\zeta_N(s) &=_{(c)} L(s, 1_{\{1\}}, N/N) = L(s, 1^G_{\{1\}}, N/K) \\ &= L(s, \sum_{\psi\in\widehat{G}} \dim(\psi)\psi(x), N/K) =_{(a)} \prod_{\psi} L(s, \psi, N/K)^{\dim\psi} \\ &= \zeta_K(s) \cdot \prod_{\psi\neq 1_G} L(s, \psi, N/K)^{\dim\psi}\end{aligned}$$

□

Thanks to the above theorem we can describe the Dedekind zeta function in terms of the Riemann zeta function.

Example 6. Consider $K = \mathbb{Q}(\zeta_3)$ and y Example 5 (c) and Theorem 5, we have the Dedekind zeta function for $K = \mathbb{Q}(\zeta_3)$:

$$\zeta_K(s) = \zeta(s) \prod_{p \text{ prime}} (1 - \chi(p)p^{-s})^{-1}$$

Where χ is like in example 4, and by the same example, we have

$$\zeta_K(s) = \zeta(s) \sum_{n\geq 0} \left(\frac{1}{(3n+1)^s} - \frac{1}{(3n+2)^s} \right).$$

1.3.3 The conductor

In this section we will define the conductor from a representation of the group of a Galois extension, which is a generalization of the discriminant. This invariant is important because it can say when two extensions have the same discriminant. The definitions and facts given here may be consulted in [CF67] and [Ser13].

Definition 6 (Ramification groups). Let L/K be a Galois extension of local fields with group $G := \mathrm{Gal}(L/K)$. We define the function $i_G : G \to \{\mathbb{Z} \cup \infty\}$ as follows. For $g \in G$, let x be a generator of O_L as an O_K-module. Set $i_G(g) = \nu_L(g(x) - x)$.

Now define G_i for all positive integer numbers i by: $g \in G_i$ if and only if $i_G(g) \leq i + 1$. The groups G_i are called the ramification groups of G.

Now, with the above conditions and χ be a character of G, then we can consider the following number called the Artin conductor:

$$f(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \left(\chi(1) - \chi(G_i)\right),$$

where $g_i = |G_i|$ and $\chi(G_i) = \frac{1}{g_i} \sum_{s\in G_i} \chi(s)$.

Definition 7 (Global Conductor). Let $L/\mathbb{Q}$ be a finite Galois extension of number fields and let $G = \mathrm{Gal}(L/\mathbb{Q})$ be the Galois group. If χ is a character of G, then we define the number $\mathfrak{f}(\chi)$, the

global conductor of χ as follows. Let $p \in \mathbb{Z}$ be a prime and choose a prime ideal $\mathfrak{p}$ in L which divides p. Let $G_p = \mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_p)$ be the corresponding decomposition subgroup. Let $f(\chi, p)$ be the Artin conductor of the restriction of χ to G_p as defined above. Then

$$\mathfrak{f}(\chi) = \prod_p p^{f(\chi,p)}.$$

The following lemma is a Corollary in [CF67] in page 159.

Lemma 5. Let $K/\mathbb{Q}$ be a finite extension and let $N/\mathbb{Q}$ the normal closure of K. Set $H := \mathrm{Gal}(/K)$ and $G := \mathrm{Gal}(N/\mathbb{Q})$, then:

$$\mathfrak{f}\left(\psi_{\mathrm{Ind}_H^G\{1_H\}}\right) = \mathrm{disc}(O_K).$$

In the subsequent section we talk about Galois representation, because we will use the Artin's L-functions with these representations, which holds the same properties that the representations of finite groups, such as the eigenvalues of each matrix in the image are roots of the unity, all the matrix in the image is diagonalizable, because has a finite image.

Observation 2. Let K and K' be two number fields, with the same normal closure N. Set $G := \mathrm{Gal}(N/\mathbb{Q})$, $H := \mathrm{Gal}(N/K)$ and $H' := \mathrm{Gal}(N/K')$. Suppose that $\mathrm{Ind}_H^G\{1_H\} \cong \mathrm{Ind}_{H'}^G\{1_{H'}\}$, then by Lemma 5, $\mathrm{disc}(O_K) = \mathrm{disc}(O_{K'})$.

Kronecker-Weber Theorem

Furthermore, Artin's L-series allow us to consider problems with Galois extensions using the characters of its group. For example, the Kronecker-Weber theorem. This is one of the most important theorems in number theory of at the end of the 19th century and early 20th century, because it characterizes all abelian extensions.

Theorem 6 (Kronecker-Weber Theorem). A number field L is an abelian extension of $\mathbb{Q}$ if and only if $L \subset \mathbb{Q}(\zeta_m)$ for ζ_m some m-th root of unity.

Notice that Theorem 6 is equivalent to prove that $\mathbb{Q}^{ab}$, is the extension of $\mathbb{Q}$ generates for all the n-roots of the unity for $n \geq 1$ where $\mathbb{Q}^{ab}$ is the maximal abelian extension, i.e. the field that contain all abelian extensions of $\mathbb{Q}$.

From Artin's L- series we can consider this theorem as follows:

Theorem 7. Let $K/\mathbb{Q}$ be an abelian extension with Galois group G, let $\rho : G \to \mathbb{C}^*$ be a character and $L(\rho, s)$ its L-functionas as above. There exists a unique Dirichlet character χ modulo q for some $q \geq 1$ such that

$$L(\rho, s, K/\mathbb{Q}) = L(\chi, s, K/\mathbb{Q}).$$

Sketching the proof, we consider $\zeta_K(s)$, like the product in Theorem 5. Then, we set m the l.c.m. of the conductors of the characters in such product. So, using the fact that p is totally split in K, if is totally split in $\mathbb{Q}(\zeta_m)$, and using Corollary 3, we get $K \subset \mathbb{Q}(\zeta_m)$. Kronecker-Weber Theorem will be important when we give a proof of the Tchebotarev density theorem.

1.4 Absolute Galois group and Galois representation

Let $K/\mathbb{Q}$ be an algebraic infinite extension. We can define its Galois group as an inverse limit, as follows

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(F/\mathbb{Q}),$$

where F runs over all the sub extensions of $K/\mathbb{Q}$ with $F/\mathbb{Q}$ Galois and finite. The isomorphism is obtained identifying the automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with the element $(\sigma|_F)_F$. For a definition of inverse limit see [DDSMS03]. Now, we define a prime $(\mathfrak{p}_F)_F$ of K over $p \in \mathbb{Q}$, as a sequence of primes, one for each finite sub extension of K such that if $F' \subset F$ then $\mathfrak{p}_F$ is over $\mathfrak{p}_{F'}$. In this sense, we can define the decomposition and inertia subgroups of a prime $\mathfrak{p}$ of K, as follows

$$D_{\mathfrak{p}} = \varprojlim D_{\mathfrak{p}_F}, \qquad I_{\mathfrak{p}} = \varprojlim I_{\mathfrak{p}_F}.$$

When $K = \overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ we call $\mathrm{Gal}(K/\mathbb{Q})$ the absolute Galois group. Now, we define profinte groups because it facilitates the topology of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Definition 8. A profinite group is a compact Hausdorff topological group whose open subgroups form a base for the neighborhoods of the identity, that is, every open set containing the identity contains an open subgroup.

The following Proposition gives us a characterization of the inverse limit from profinite groups. For a proof the reader can see [DDSMS03] proposition 1.3, page 17.

Proposition 2. If G is a profinite group, then G is (topologically) isomorphic to

$$\varprojlim (G/N)_N,$$

where the limit runs over all normal subgroups with finite index on G. Conversely, the inverse limit of any inverse system of finite groups is a profinite group.

Galois representation

Definition 9. A Galois representation is a continuous homomorphism:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(k),$$

where k is an algebraically closed field ($\mathbb{C}$, $\overline{\mathbb{Q}_p}$, $\overline{\mathbb{F}_p}$). In the case that $k = \mathbb{C}$ we call it an Artin's representation, if $k = \overline{\mathbb{F}_p}$ it is called discrete, and if $k = \overline{\mathbb{Q}_p}$ is called p-adic.

Now, we will prove that any Artin's representation has finite image.

Lemma 6. Let G be a Lie group (for a definition see [DK12]), then there exists a neighborhood U of the identity in G such that U does not contain any non trivial subgroup of G.

Proof. let $\mathfrak{g}$ be the Lie algebra of G. We know that $T_0(\exp)(X) = X$ for $X \in \mathfrak{g}$, that is, $T_0(\exp)$ is equal to the identity $\mathfrak{g} \to \mathfrak{g}$. By the inverse mapping theorem, we know that: There is an open neighborhood U' (we may choose it with finite diameter) of 0 in $\mathfrak{g}$ and V' of e in G, such that the

exponential map is a C^1 diffeomorphism from U' to V'. Set $V = \exp(U'/2)$. We claim that V is the desired neighborhood. Otherwise if $x \in V$ is not the identity, we have that $x = \exp\left(\frac{1}{2}u\right)$ for some $u \in U'$. Then,

$$x^n = \exp\left(\frac{1}{2}u\right) \cdots \exp\left(\frac{1}{2}u\right) \qquad (n \text{ times}),$$

for any positive integer n. Now, given v, we can find N such that $\frac{N}{2}u \in U' \setminus \frac{1}{2}U'$. Then, $x^N \in \exp(V') \setminus \exp(\frac{1}{2}U') = V \setminus V'$. □

Observation 3. Notice that Lemma 6 states that any profinite group G that is also Lie group is finite; indeed by definition, any neighborhood of the identity must contain an open subgroup of G, so $\{e\}$ is open. Since G is a topological group, $\{x\}$ is open for any $x \in G$, hence G has the discrete topology. And since G is compact, then G is finite.

Theorem 8. Let G be a profinite group and let $\rho : G \to GL_n(\mathbb{C})$ be a continuous homomorphism then ρ has a finite image.

Proof. Since $\rho : G \to GL_n(\mathbb{C})$ is continuous and the kernel of ρ is the pre-image of $\{e\}$ (a closed subset because $GL_n(\mathbb{C})$ is Hausdorff), $\ker(\rho)$ is closed, so, the quotient is also a profinite group, and we may assume ρ is injective. Now $\rho : G \to \rho(G)$ is a bijection. Since G is compact and $\rho(G)$ is Hausdorff with the subspace topology, then $\rho : G \to \rho(G)$ is an homeomorphism. Also, we know that $\rho(G)$ is compact in the topology of $GL_n(\mathbb{C})$ (because it is compact with the subspace topology), hence is closed, since $GL_n(\mathbb{C})$ is Hausdorff. Then $\rho(G)$ is a Lie subgroup with the subspace topology. Thus, G has the same topology of $\rho(G)$, hence it is a profinite group, and by Observation 1 we conclude that is finite. □

Chapter 2

The Class Number Formula

An important result in Algebraic number theory is the class number formula. It computes the residue at the isolated singularity 1 of a Dedekind zeta function. This residue is important because it gives a relation between the Dedekind zeta function of K and some invariants of this field such as the order of the Class group of O_K, the determinant and other invariants. The proof that we will present in this section was taken from [Jan96] and [Jar14].

We begin with the definition of a lattice, and its volume [Neu13], which measures in some sense the number of points in the lattice. Furthermore, we define the regulator, which is the volume of the units in O_K.

Definition 10. Let V be an n-dimensional $\mathbb{R}$-vector space. A *lattice* in V is an additive subgroup of the form:

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

with $v_1, \ldots, v_m$ linearly independents in V. The set $\{v_1, \ldots, v_m\}$ is called a *basis* and the set

$$\Psi = \{x_1v_1 + \cdots + x_mv_m : x_i \in \mathbb{R},\ 0 \leq x_i < 1\}$$

the *fundamental mesh* of the lattice. The lattice is called *complete*, if $m = n$, in whose case we can associate a volume to Γ, as follow:

$$\text{vol}(\Gamma) = \text{vol}(\Psi) = |\det A|$$

where A is the matrix of the basis change from $e_1, \ldots, e_n$ to $v_1, \ldots, v_n$.

Definition 11 (The regulator of K). By Theorem 2, we know that $(O_K)^* \simeq \mathbb{Z}^{r+s-1} \times \mu(K)$. Set $|\mu(K)| = \omega_K$. Then we can consider $(O_K)^*$ like a complete lattice inside $\mathbb{R}^{r+s-1}$, as follows: let $\xi_1, \ldots, \xi_{r+s-1}$ be the fundamental units. Remember that the norm of a real embedding is given by $\|\alpha\|_i = |\sigma_i(\alpha)|$ for $1 \leq i \leq r$, and the norm of a complex embedding is given by $\|\alpha\|_{r+j} = |\tau_j(\alpha)|^2$ for $1 \leq j \leq s$. Consider the following matrix

$$A = \begin{bmatrix} \log \|\xi_1\|_1 & \log \|\xi_2\|_1 & \cdots & \log \|\xi_{r+s-1}\|_1 \\ \log \|\xi_1\|_2 & \log \|\xi_2\|_2 & \cdots & \log \|\xi_{r+s-1}\|_2 \\ \vdots & \vdots & \ddots & \vdots \\ \log \|\xi_1\|_{r+s} & \log \|\xi_2\|_{r+s} & \cdots & \log \|\xi_{r+s-1}\|_{r+s} \end{bmatrix},$$

of order $(r+s)\times(r+s-1)$. We define A_i to be the $(r+s-1)\times(r+s-1)$ minors obtained by subtracting the i-th row of A. Then the regulator of K, denoted reg(K), is given by $|\det A_i|$, which is independent of i. For details, see [Neu13], page 43, Proposition 7.5.

In other words, we consider $\Gamma\subset\mathbb{R}^{r+s}$ a lattice associated to $(O_K)^*$ with base

$$v_i=(\log\|\xi_1\|_1,\log\|\xi_2\|_1,\ldots,\log\|\xi_{r+s-1}\|_1)\qquad[i=1,\ldots,r+s-1]$$

then if we take the image of Γ via the i-th natural projection of $\mathbb{R}^{r+s}$ to $\mathbb{R}^{r+s-1}$ then we have a complete lattice in $\mathbb{R}^{r+s-1}$, and its volume is reg(K).

In the case that $r+s-1=0$, i.e. $K=\mathbb{Q}(\sqrt{d})$, with $d<0$ and squarefree or $K=\mathbb{Q}$, we have that reg$(K)=1$.

2.1 Class number Formula

Let K be an algebraic number field, with r real embedding $\sigma_1,\ldots,\sigma_r$ and s pairs of complex embeddings $\tau_1,\overline{\tau_1},\ldots,\tau_s,\overline{\tau_s}$. For each nonzero integral ideal $\mathfrak{A}$ (ideal of O_K) we have defined $\|\mathfrak{A}\|=|O_K/\mathfrak{A}|$. The unique factorization of ideals and the fundamental equality, imply that there is only a finite number $a_K(n)$ of integral ideals with norm n. Then, by Lemma 1 the Dedekind zeta function converges for $s>1$ we can also write this as follows

$$\zeta_K(s)=\prod\frac{1}{1-\|\mathfrak{P}\|^{-s}}=\sum_{n\geq1}\frac{a_K(n)}{n^s}.$$

We begin by defining the ζ-function of a coset $\mathbf{k}$ of the class group $Cl(K)$

$$\zeta_K(s,\mathbf{k})=\sum_{\substack{\mathfrak{A}\in\mathbf{k}\\ \mathfrak{A}\text{ integral}}}\frac{1}{\|\mathfrak{A}\|^s}=\sum_{n\geq1}\frac{a(n,\mathbf{k})}{n^s},$$

where $a(n,\mathbf{k})$ is the number of integral ideals in $\mathbf{k}$ having norm exactly n. Notice that

$$\zeta_K(s)=\sum_{\mathbf{k}\in Cl(K)}\left(\sum_{\substack{\mathfrak{A}\in\mathbf{k}\\ \mathfrak{A}\text{ integral}}}\frac{1}{\|\mathfrak{A}\|^s}\right)=\sum_{\mathbf{k}\in Cl(K)}\zeta_K(s,\mathbf{k}),$$

and choose $\mathfrak{a}\in\mathbf{k}^{-1}$ such that $\mathfrak{a}\subset O_K$ (it is well known that each class of $Cl(K)$ has an integral ideal [Jan96] page 146, Lemma 2.3), so that $\mathfrak{a}\mathfrak{A}$ is principal, for all $\mathfrak{A}\in\mathbf{k}$. Then multiplication by $\mathfrak{a}$ gives a bijection between integral ideals in $\mathbf{k}$ and principal ideals divisible by $\mathfrak{a}$. Thus

$$\zeta_K(s,\mathbf{k})=\|\mathfrak{a}\|^s\sum_{\substack{\alpha\in K^*\\ \mathfrak{a}\,|\langle\alpha\rangle}}\frac{1}{\|\langle\alpha\rangle\|^s}.\tag{2.1}$$

In order to evaluate this sum, we may use lattice points in n-dimensional solids.

First, we define the space $\mathcal{L}^{r,s}$ to be the set of points $(x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+s})$ where the first r coordinates are real and the remaining s are complex, which has dimension $r + 2s = n$. Notice that $\mathcal{L}^{r,s}$ is a vector subspace of $\mathbb{R}^n$. With scalar multiplication as well as component wise addition and multiplication of points, this forms a commutative ring and a linear space.

Finally, we define a norm on $\mathcal{L}^{r,s}$ as follow $\mathcal{N}(x) = |x_1 \cdots x_r| \, |x_{r+1}|^2 \cdots |x_{r+s}|^2$. And we can consider the injection $\phi : K \to \mathcal{L}^{r,s}$ defined by

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha); \tau_1(\alpha), \ldots, \tau_s(\alpha));$$

Clearly ϕ is a homomorphism of commutative rings, and $\mathcal{N}(\phi(\alpha)) = \|\langle\alpha\rangle\|$.

Now, we need to rewrite the sum (2.1) in terms of $\mathcal{L}^{r,s}$, as follows: Let $\mathcal{A}$ be the set of the α such that $\mathfrak{a} \,|\, \langle\alpha\rangle$, where from each possible set of associate values (i.e. all α that generates the same principal ideal) we select one. Define $\Gamma = \phi(\mathfrak{a}) = \{x \in \mathcal{L}^{r,s} : x = \phi(b) \text{ for some } b \in \mathfrak{a}\}$, and $\Theta = \{x \in \mathcal{L}^{r,s} : x = \phi(b) \text{ for some } b \in \mathcal{A}\}$. Then

$$\zeta_K(s, \mathbf{k}) = \|\mathfrak{a}\|^s \sum_{\alpha \in \Theta} \frac{1}{\mathcal{N}(\alpha)^s}. \tag{2.2}$$

So, the idea to compute the residue at the isolated singularity 1 of a Dedekind zeta function is to reform (2.2) in terms of Γ. Then using Lemma 8 we will be able to compute such residue.

In order to achieve this, we denote $l_k(x) = \log |x_k|$ for $1 \leq k \leq r$ and $l_{r+k}(x) = \log |x_{r+k}|^2$ for $1 \leq k \leq s$; we may then define for $x \in \mathcal{L}^{r,s}$ the vector $l(x) = (l_1(x), \ldots, l_{r+s}(x))$. The set of all points of $\mathcal{L}^{r,s}$ with nonzero components, form a group under componentwise multiplication, and this mapping is a homomorphism onto the additive group $\mathcal{L}^{r,s}$.

If $\alpha \in K$, then write $l(\alpha) = l(\phi(\alpha))$. This geometric representation $l(\alpha)$ is called the logarithmic representation of α, and the sum of its components is equal to $\log |\|\alpha\||$.

Let $\xi_1, \ldots, \xi_{r+s-1}$ be the fundamental units. Define $\lambda = (1, \ldots, 1; 2, \ldots, 2)$. Then $\{\lambda, l(\xi_1), \ldots, l(\xi_{r+s-1})\}$ is a basis for $\mathbb{R}^{r+s}$, for more details the reader can see [Jan96], page 148. For $x \in \mathcal{L}^{r+s}$, we can write $l(x)$ as follows:

$$l(x) = c\lambda + c_1 l(\xi_1) + \cdots + c_{r+s-1} l(\xi_{r+s-1}),$$

where $c = \frac{1}{n} \log(\mathcal{N}(x))$, since the sum of the components in $l(x)$ is $\log(\mathcal{N}(x))$, and the sum of the components in $l(\xi_j)$ is $\log \|\xi_j\| = 0$.

Now we need to give the definition of a cone:

Definition 12. Let V be an n-dimensional $\mathbb{R}$-vector space. A set $X \subset V$ is called a cone if for $x \in X$ and $\alpha > 0$ implies $\alpha x \in X$.

Define X to be the cone consisting of all $x \in \mathcal{L}^{r,s}$ such that:

(a) $\mathcal{N}(x) \neq 0$.

(b) $0 \leq c_i < 1$ for $i = 1, \ldots, r + s - 1$.

(c) $0 \leq \arg(x_1) < \frac{2\pi}{\omega_K}$, where x_1 is the first component of x.

This is a cone because for $\alpha > 0$, we have $l(\alpha x) = (\log \alpha)\lambda + l(x)$, hence the coefficient of $l(\xi_i)$ belongs to $[0, 1)$, and $\arg(\alpha x_1) = \arg(x_1)$.

Then the following Lemma states that $\Theta = \Gamma \cap X$.

Lemma 7. Let $[\alpha] \subset O_K$ be the set of all elements in O_K which generate $\langle\alpha\rangle$. Then exactly one member of $[\alpha]$ has image in X.

Proof. Since for all $\beta \in [\alpha]$ there exists $\xi \in O_k^*$, such that $\beta = \xi\alpha$, then to prove this, is enough to show that given $y \in \mathbb{R}^n$ with nonzero norm, y can be written uniquely as $x \cdot \phi(\xi)$, where $x \in X$ (multiplication is componentwise) and ξ is a unit. Like above, we can put $l(y)$ as the following sum $c\lambda + c_1 l(\xi_1) + ... + c_{r+s-1} l(\xi_{r+s-1})$. For each i, we can write c_i equal to $m_i + \mu_i$, where $m_i \in \mathbb{Z}$ and $0 \leq \mu_i < 1$, and write $u = \xi_1^{m_1} \cdots \xi_{r+s-1}^{m_{r+s-1}}$. Then define $z = y \cdot \phi(u^{-1})$, and notice that the coefficients of z for each $l(\xi_i)$ are in the correct range. Now we can correct $\arg(z_1)$; let r be the unique integer such that $0 \leq \arg(z_1) - \frac{2\pi r}{\omega_K} < \frac{2\pi}{\omega_K}$, and choose a root of unity ω such that $\rho_1(\omega) = e^{\frac{2\pi i}{\omega_K}}$, where ρ_1 gives the first component of the map ϕ. Then $z \cdot \phi(\omega^{-r}) = y \cdot \phi(u^{-1})\phi(\omega^{-r}) =: x \in X$, then $y = x \cdot \phi(u\omega^r)$ as desired. The uniqueness follows from the construction. □

We now use the result of Lemma 7 to rewrite:

$$\zeta_K(s, \mathbf{k}) = \|\mathfrak{a}\|^s \sum_{x \in \Gamma \cap X} \frac{1}{\mathcal{N}(x)^s},$$

which we may evaluate from the following Lemma.

Lemma 8. Let X be a cone in $\mathbb{R}^n$ and $F : X \to \mathbb{R}_{>0}$ be a function such that $F(\xi x) = \xi^n F(x)$ for $x \in X$ and $\xi \in \mathbb{R}_{>0}$, and $\mathcal{F} = \{x \in X : F(x) \leq 1\}$ is bounded with $\mathrm{vol}(\mathcal{F}) > 0$. Let $\Gamma \subset \mathbb{R}^n$ be a complete lattice with volume $\mathrm{vol}(\Gamma)$. Suppose that

$$\zeta_\Gamma(s) = \sum_{x \in \Gamma \cap X} \frac{1}{F(x)^s},$$

converges on $\mathrm{Re}(s) > 1$, then $\lim_{s \to 1}(s-1)\zeta_\Gamma(s) = \frac{\mathrm{vol}(\mathcal{F})}{\mathrm{vol}(\Gamma)}$.

Proof. Let r be a positive real number, we know $\mathrm{vol}(\frac{1}{r}\Gamma) = \frac{1}{r^n}\mathrm{vol}(\Gamma)$.

The volume of $\mathcal{F}$ may be computed in the following way. For a real number $r > 0$ consider the points of $\left(\frac{1}{r}\Gamma\right) \cap \mathcal{F}$. Using each such point as center, place a n-dimensional parallelepiped equal to a translate of a fixed fundamental mesh of $\frac{1}{r}\Gamma$. Let $T_1(r)$ be the number of these parallelepipeds contained in $\mathcal{F}$. Their union is a polyhedron of volume $\frac{1}{r^n}\mathrm{vol}(\Gamma)T_1(r)$ which serves to approximate $\mathcal{F}$ from the inside. Thus, the volume of $\mathcal{F}$ is the limit of $\frac{1}{r^n}\mathrm{vol}(\Gamma)T_1(r)$ as $r \to \infty$.

Now we want to approximate $\mathcal{F}$ from the outside. Let $T_2(r)$ be the number of parallelepipeds with center at some point of $\frac{1}{r}\Gamma$ and having nonempty intersection with $\mathcal{F}$. The polyhedron consisting of these parallelepipeds containing $\mathcal{F}$ and the volume of $\mathcal{F}$ is the limit of $\frac{1}{r^n}\mathrm{vol}(\Gamma)T_1(r)$ as $r \to \infty$.

Finally let $T(r)$ be the number of points of $\frac{1}{r}\Gamma \cap \mathcal{F}$. Then $T_1(r) < T(r) < T_2(r)$ and it follows that:

$$\text{vol}(\mathcal{F}) = \text{vol}(\Gamma) \lim_{r\to\infty} \frac{\left|\left(\frac{1}{r}\Gamma\right) \cap \mathcal{F}\right|}{r^n},$$

then

$$\frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)} = \lim_{r\to\infty} \frac{\left|\left(\frac{1}{r}\Gamma\right) \cap \mathcal{F}\right|}{r^n}.$$

But by definition of $\mathcal{F}$,

$$\left|\left(\frac{1}{r}\Gamma\right) \cap \mathcal{F}\right| = \left|\{x \in \Gamma \cap X : F(x) \leq r^n\}\right|.$$

Since $\mathcal{F}$ is bounded, for a fix r the set $\left(\frac{1}{r}\Gamma\right) \cap \mathcal{F}$ is finite. Therefore, we can list the points of $\Gamma \cap X$ such that $0 < F(x_1) \leq F(x_2) \leq \ldots$ and define $r_k = F(x_k)^{1/n}$. If we define $\gamma(r) = \left|\left(\frac{1}{r}\Gamma\right) \cap \mathcal{F}\right|$, then we have that for $\varepsilon > 0$, $\gamma(r_k - \varepsilon) < k \leq \gamma(r_k) := |\{i \in \mathbb{Z}^+ : F(x_i) \leq F(x_k)\}|$. Dividing by r_k^n gives

$$\frac{\gamma(r_k - \varepsilon)}{(r_k - \varepsilon)^n} \left(\frac{r_k - \varepsilon}{r_k}\right)^n < \frac{k}{r_k^n} \leq \frac{\gamma(r_k)}{r_k^n}.$$

Since $r_k^n = F(x_k)$, we have $\lim_{k\to\infty} \frac{k}{r_k^n} = \frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)}$.

Now given $\varepsilon > 0$, by the above inequality there exists k_0 such that $k \leq k_0$ implies

$$\left(\frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)} - \varepsilon\right)^s \frac{1}{k^s} < \frac{1}{F(x_k)^s} < \left(\frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)} + \varepsilon\right)^s \frac{1}{k^s}.$$

If $s \to 1^+$, in the sum over all $k \geq k_0$ multiply by $(s-1)$, and since $\lim_{s\to1}(s-1)\zeta(s) = 1$ we get

$$\lim_{s\to1} \left(\frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)} - \varepsilon\right)^s \leq \lim_{s\to1}(s-1)\zeta_\Gamma(s) \leq \lim_{s\to1} \left(\frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)} + \varepsilon\right)^s,$$

and since ε is arbitrary, we have

$$\lim_{s\to1}(s-1)\zeta_\Gamma(s) = \frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)}.$$

□

We thus need compute $\text{vol}(\mathcal{F}) = \text{vol}(\{x \in X : \|x\| \leq 1\})$ and $\text{vol}(\Gamma) = \text{vol}(\phi(\mathfrak{a})) = \text{vol}(\{x \in \mathcal{L}^{r,s} : x = \phi(b) \text{ for some } b \in \mathfrak{a}\})$, because Lemma 8 states that

$$\lim_{s\to1}(s-1)\zeta_K(s, \mathbf{k}) = \|\mathfrak{a}\| \cdot \frac{\text{vol}(\mathcal{F})}{\text{vol}(\Gamma)}.$$

Now we will compute separately $\text{vol}(\mathcal{F})$ and $\text{vol}(\Gamma)$.

(a) $\text{vol}(\Gamma) = \|\mathfrak{a}\| \, |\text{disc}(O_K)|^{1/2}$.

Proof. Since $\mathfrak{a}$ has rank n, then is generated by $\alpha_1, \ldots, \alpha_n$, so that Γ is generated by $\phi(\alpha_1)$, $\cdots, \phi(\alpha_n)$. Let B be the matrix with entries $(\sigma_i \alpha_j)$, where σ_i varies over all embeddings (real and complex) of K. Then $\text{disc}(\mathfrak{a}) = \det(B)^2 = \|\mathfrak{a}\|^2 \text{disc}(O_K)$. Also, let C be the matrix consisting of n inner products $(\langle \phi(\alpha_i), \phi(\alpha_j) \rangle) = (\sum_{k=1}^{n} \sigma_k(\alpha_i)\overline{\sigma_k(\alpha_j)} = B^T B$. Thus $|\det C|^{1/2} = |\det B|$, and since $\text{vol}(\Gamma) = |\det C|^{1/2} = \text{disc}(\mathfrak{a})$, we have $\text{vol}(\Gamma) = \|\mathfrak{a}\| \, |\text{disc}(O_K)|^{1/2}$. □

(b) $\text{vol}(\mathcal{F}) = \frac{2^{r+s}\pi^s \text{reg}(K)}{\omega_k}$.

Proof. Define $\mathcal{F}_k$ for $0 \leq k < \omega_K$ by applying the map $x \mapsto e^{\frac{2k\pi i}{\omega_K}} x$ to $\mathcal{F}$; since multiplication by a n-th root of unity preserve volume, we have $\text{vol}(\mathcal{F}) = \text{vol}(\mathcal{F}_k)$. Let $\widetilde{\mathcal{F}} = \left(\bigcup_{k=0}^{\omega_K} \mathcal{F}_K\right) \cap \{(x_1, \ldots, x_r; x_{r+1}, \ldots, x_{r+s}) : x_1, \ldots, x_r > 0\}$. Multiplying any point in $\widetilde{\mathcal{F}}$ by $(\pm 1, \ldots, \pm 1; 1, \ldots, 1)$ shows that $\text{vol}(\mathcal{F}) = \frac{2^r}{\omega_K} \text{vol}(\widetilde{\mathcal{F}})$, and so we will compute $\text{vol}(\mathcal{F})$ through multiple changes of variable.

First, we change from the $(r+s)$-dimensional complex space $\mathcal{L}^{r,s}$ to $\mathbb{R}^n$ via the transformation which maps a point $(x_1, \ldots, x_r; x_{r+1}, \ldots, x_{r+s}) \in \mathcal{F}$ to the real valued point $(\rho_1, \ldots, \rho_r, \rho_{r+1}, \varphi_{r+1}, \ldots, \rho_{r+s}, \varphi_{r+s})$, where $\rho_j = |x_j|$ and $\varphi_j = \arg x_j$ for all j (we say $x_j = y_j + i z_j = \rho_j e^{i\varphi_j}$). Now we compute the Jacobian of the transformation $\rho_{s+1} \cdots \rho_{r+s}$. Then $\widetilde{\mathcal{F}}$ is given by the conditions $\rho_1, \ldots, \rho_{r+s} > 0$; $\prod_{j=1}^{r+s} \rho_j^{e_j} \leq 1$, where e_j is the j-th coordinate of $\lambda = (1, \ldots, 1; 2, \ldots, 2)$; and $0 \leq \gamma_k < 1$ in the formula for each j-th coordinate of $l(x)$:

$$\log \rho_j^{e_j} = \frac{e_j}{n} \log \left(\prod_{k=1}^{r+s} \rho_k^{e_k} \right) + \sum_{k=1}^{r+s-1} \gamma_k l_j(\xi_k).$$

These conditions do not restrict φ_j for any value $r+1 \leq j \leq r+s$, so they take on all values in $[0, 2\pi)$. We now change variables again, replacing $\rho_1, \ldots, \rho_{r+s}$ with $\gamma, \gamma_1, \ldots, \gamma_{r+s-1}$ according to

$$\log \rho_j^{e_j} = \frac{e_j}{n} \log \gamma + \sum_{k=1}^{r+s-1} \gamma_k l_j(\xi_k).$$

Since the sum of the e_j is n, and $\sum_{j=1}^{r+s} l_j(\xi_k) = 0$, we sum all the above equation and find $\gamma = \prod_{j=1}^{r+s} \rho_j^{e_j}$. Thus $\widetilde{\mathcal{F}}$ is now defined by the conditions $0 < \gamma \leq 1$ and $0 \leq \gamma_k < 1$ for $1 \leq k \leq r+s$; clearly this set has positive volume now. This transformation has Jacobian

$$J = \begin{vmatrix} \frac{\rho_1}{n\gamma} & \frac{\rho_1}{e_1} l_1(\xi_1) & \cdots & \frac{\rho_1}{e_1} l_1(\xi_{r+s-1})) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{r+s}}{n\gamma} & \frac{\rho_{r+s}}{e_{r+s}} l_{r+s}(\xi_1) & \cdots & \frac{\rho_{r+s}}{e_{r+s}} l_{r+s}(\xi_{r+s-1})) \end{vmatrix}$$

$$= \frac{\rho_1 \cdots \rho_{r+s}}{n\gamma 2^s} \begin{vmatrix} e_1 & l_1(\xi_1) & \cdots & l_1(\xi_{r+s-1})) \\ \vdots & \vdots & \ddots & \vdots \\ e_{r+s} & l_{r+s}(\xi_1) & \cdots & l_{r+s}(\xi_{r+s-1})) \end{vmatrix}$$

$$= \frac{\rho_1 \cdots \rho_{r+s}}{n\gamma 2^s} \begin{vmatrix} n & 0 & \cdots & 0 \\ e_2 & l_2(\xi_1) & \cdots & l_2(\xi_{r+s-1})) \\ \vdots & \vdots & \ddots & \vdots \\ e_{r+s} & l_{r+s}(\xi_1) & \cdots & l_{r+s}(\xi_{r+s-1})) \end{vmatrix}.$$

This determinant is now exactly $n \cdot \text{reg}(K)$, so

$$J = \frac{\rho_1 \cdots \rho_{r+s}}{n(\rho_1 \cdots \rho_s \rho_{s+1}^2 \cdots \rho_{r+s}^2)2^s} n \cdot \text{reg}(K) = \frac{\text{reg}(K)}{(\rho_{s+1} \cdots \rho_{r+s})2^s}.$$

Now, we can compute the volume of $\widetilde{\mathcal{F}}$:

$$\begin{aligned} \text{vol}(\widetilde{\mathcal{F}}) &= 2^s \int \cdots \int_{\widetilde{\mathcal{F}}} dx_1 \cdots dx_r dy_{r+1} dz_{r+1} \cdots dy_{r+s} dz_{r+s} \\ &= 2^s \int \cdots \int_{\widetilde{\mathcal{F}}} \rho_{r+1} \cdots \rho_{r+s} \cdot d\rho_1 \cdots d\rho_r d\rho_{r+1} d\varphi_{r+1} \cdots d\rho_{r+s} d\varphi_{r+s} \\ &= 2^s (2\pi)^s \int_0^1 \cdots \int_0^1 \rho_{r+1} \cdots \rho_{r+s} \cdot |J| \, d\gamma d\gamma_1 \cdots d\gamma_{r+s-1} \\ &= 2^s (2\pi)^s \frac{\text{reg}(K)}{2^s} = (2\pi)^s \text{reg}(K), \end{aligned}$$

Thus $\text{vol}(\mathcal{F}) = \frac{2^r}{\omega_K} \text{vol}(\widetilde{\mathcal{F}}) = \frac{2^{r+s}\pi^s \text{reg}(K)}{\omega_k}$ as desired. □

Using (a) and (b), we obtain the next result:

Theorem 9 (The class number formula). Let $\zeta_K(s)$ the Dedekind zeta function for the number field K, then

$$\lim_{s \to 1^+} (s-1)\zeta_K(s) = \frac{2^{r+s}\pi^s \text{reg}(K)}{\omega_K(|\text{disc}(O_K)|)^{1/2}} h_K,$$

where r and s are the numbers of real and complex primes of K respectively, $\text{reg}(K)$ is the regulator of K (i.e. the volume of the $(r+s-1)$-dimensional lattice of units), ω_K is the number of roots of 1 in K, $\text{disc}(O_K)$is the discriminant of $K/\mathbb{Q}$, and h_k is the class number.

More generally, but in the same sense, the residue of

$$\zeta_K(s, \mathbf{k}) = \sum_{\substack{\mathfrak{A} \in \mathbf{k} \\ \mathfrak{A} \text{ integral}}} \frac{1}{\|\mathfrak{A}\|^s},$$

where $\mathbf{k}$ is a coset of $U^{\mathfrak{m}}$ over $I_{\mathfrak{m}}$ with $\mathfrak{m}$ a modulus for K. Is given for:

$$g_{\mathfrak{m}} = \frac{2^{r+s}\pi^s \text{reg}(\mathfrak{m})}{\omega_{\mathfrak{m}} \|\mathfrak{m}_0\| \, |\text{disc}(O_K)|},$$

where

$$\begin{aligned} \text{reg}(\mathfrak{m}) &= \text{vol}((O_K)^* \cap K_{\mathfrak{m},1}) \\ \omega_{\mathfrak{m}} &= \text{ number of unity in } (O_K)^* \cap K_{\mathfrak{m},1}, \end{aligned}$$

with $\alpha \in K_{\mathfrak{m},1}$ if and only if satisfies the conditions $\alpha \equiv 1 \mod \mathfrak{p}^{n(\mathfrak{p})}$, and for σ a real embedding of K dividing $\mathfrak{m}$, $\sigma(\alpha) > 0$.

Proposition 3. Let χ be a character of the class group $I_{\mathfrak{m}}/U^{\mathfrak{m}}$, then

$$\lim_{s\to 1}(s-1)L(s,\chi) = \begin{cases} h_{\mathfrak{m}} g_{\mathfrak{m}} & \text{if} \quad \chi = \chi_0 \\ \\ 0 & \text{otherwise} \end{cases}$$

where $h_{\mathfrak{m}}$ is the order of the class group $I_{\mathfrak{m}}/U^{\mathfrak{m}}$.

Proof. Since

$$L(s,\chi) = \sum_{\mathbf{k}} \chi(\mathbf{k}) \sum_{\substack{\mathfrak{A}\in\mathbf{k} \\ \mathfrak{A} \text{ integral}}} \|\mathfrak{A}\|^{-s} = \sum_{\mathbf{k}} \chi(\mathbf{k})\zeta(s,\mathbf{k}),$$

hence

$$\lim_{s\to 1}(s-1)L(s,\chi) = \sum_{\mathbf{k}} \chi(\mathbf{k}) g_{\mathfrak{m}},$$

and the result is obtained from the orthogonality relation of the characters. □

2.2 Applications to Quadratic Number Fields

In this section we use the class number formula to compute the class number for quadratic extension. For instance, we know now that the only imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$, d squarefree and $d < 0$, which have class number 1 are those with

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Example 7. Consider $K = \mathbb{Q}(\zeta_3)$. In this case $\text{reg}(K) = 1$, the class number formula states

$$\begin{aligned} \lim_{s\to 1^+}(s-1)\zeta_K(s) &= \frac{2^{r+s}\pi^s \text{reg}(K)}{\omega_K(|\text{disc}(O_K)|)^{1/2}} h_K \\ &= \frac{2\pi}{6(3)^{1/2}} h_K = \frac{\pi}{3\sqrt{3}} h_K. \end{aligned} \tag{2.3}$$

By Example 6 we have

$$\zeta_K(s) = \zeta(s) \sum_{n\geq 0} \left(\frac{1}{(3n+1)^s} - \frac{1}{(3n+2)^s} \right). \tag{2.4}$$

By (2.3) and (2.4), we obtain

$$\begin{aligned} \frac{\pi}{3\sqrt{3}} h_K &= \lim_{s\to 1^+} (s-1)\zeta_K(s) \\ &= \lim_{s\to 1^+} (s-1)\zeta(s) \sum_{n\geq 0} \left(\frac{1}{(3n+1)^s} - \frac{1}{(3n+2)^s} \right). \end{aligned}$$

Because this sum is a Dirichlet series and the sum of the first n-th partial sum is 0 or 1, by part (a) of Lemma 1, it is uniformly convergent in $D(0;\delta,\varepsilon)$. In particular, it is analytic in the disk $|s-1| < \frac{1}{2}$. Then

$$\begin{aligned} \frac{\pi}{3\sqrt{3}} h_K &= \lim_{s\to 1^+} (s-1)\zeta(s) \sum_{n\geq 0} \left(\frac{1}{(3n+1)^s} - \frac{1}{(3n+2)^s} \right) \\ &= \lim_{s\to 1^+} (s-1)\zeta(s) \lim_{s\to 1^+} \sum_{n\geq 0} \left(\frac{1}{(3n+1)^s} - \frac{1}{(3n+2)^s} \right) \\ &= \sum_{n\geq 0} \left(\frac{1}{3n+1} - \frac{1}{3n+2} \right). \end{aligned}$$

Consider

$$\frac{1}{x^2+x+1} = \frac{1-x}{1-x^3} = (1-x) \sum_{n\geq 0} x^{3n} = \sum_{n\geq 0} \left(x^{3n} - x^{3n+1} \right),$$

then

$$\begin{aligned} \frac{2}{\sqrt{3}} \tan^{-1}\left(\frac{2x+1}{\sqrt{3}} \right) = \int \frac{dx}{x^2+x+1} &= \int \sum_{n\geq 0} \left(x^{3n} - x^{3n+1} \right) dx \\ &= \sum_{n\geq 0} \left(\frac{x^{3n+1}}{3n+1} - \frac{x^{3n+2}}{3n+2} \right). \end{aligned}$$

Now if we take $x \to 1$, we have that

$$\sum_{n\geq 0} \left(\frac{1}{3n+1} - \frac{1}{3n+2} \right) = \frac{2}{\sqrt{3}} \tan\left(\frac{3}{\sqrt{3}} \right) = \frac{\pi}{3\sqrt{3}},$$

then $h_K = 1$, so, O_K is a PID.

Example 8. Consider $K = \mathbb{Q}(i)$. In this case $\text{reg}(K) = 1$, the class number formula tells us

$$\begin{aligned} \lim_{s\to 1^+} (s-1)\zeta_K(s) &= \frac{2^{r+s}\pi^s \text{reg}(K)}{\omega_K(|\text{disc}(O_K)|)^{1/2}} h_K \\ &= \frac{2\pi}{4(4)^{1/2}} h_K = \frac{\pi}{4} h_K. \end{aligned} \tag{2.5}$$

By Example 5 (b) and Theorem 5, we have the Dedekind zeta function for $K = \mathbb{Q}(i)$:

$$\zeta_K(s) = \zeta(s) \sum_{n \geq 0} \frac{(-1)^n}{(2n+1)^s}. \tag{2.6}$$

By (2.5) and (2.6), we obtain

$$\frac{\pi}{4} h_K = \sum_{n \geq 0} \frac{(-1)^n}{(2n+1)^s}.$$

And is well known that

$$\sum_{n \geq 0} \frac{(-1)^n}{(2n+1)^s} = \frac{\pi}{4},$$

then $h_K = 1$, so O_K is a PID.

In the same way, we can generalize this process to quadratic extensions (different to the above examples), as follow

$$h_K = -\frac{1}{|\text{disc}(O_K)|} \sum_{n=1}^{|\text{disc}(O_K)|-1} \left(\frac{\text{disc}(O_K)}{n} \right) \cdot n,$$

where $\left(\frac{\text{disc}(O_K)}{n} \right)$ is the extended Jacobi symbol. For example, if $K = \mathbb{Q}(\sqrt{-163})$, since $\text{disc}(O_K) = -163$ we have

$$h_K = -\frac{1}{163} \sum_{n=1}^{162} \left(\frac{-163}{n} \right) \cdot n,$$

and implementing the following code in MAGMA, to compute the sum:

```
sum:=0;
for i in [1..162] do
    sum:=sum+KroneckerSymbol(i, -163)*i;
    sum;
end for;
```

we obtain that this sum is equal to -163, so, $h_K = 1$. In the case that $d \equiv_4 3, 2$ we use the code:

```
sum:=0;
for i in [1..|d|-1] do
    sum:=sum+KroneckerSymbol(i, 4d-i)*i;
    sum;
end for;
```

Using this code, we can find h_K, for the d's mentioned at the beginning of the section.

d	disc(O_K)	sum
-2	-8	-8
-7	-7	-7
-11	-11	-11
-19	-19	-19
-43	-43	-43
-67	-67	-67

Table 2.1: Quadratic number fields with $h_K = 1$

2.3 Natural and Dirichlet Density

In this section the idea is to define a measure for the prime ideals of a number field K. We begin with the definition of Natural density and the Dirichlet density, which coincide when the natural density exists. So, we use the word "density", for referring to Dirichlet density.

This concept is important because the Tchebotarev Density Theorem, which computes the density of primes in a number field K, whose Frobenius automorphism are in a fixed conjugacy class in $\mathrm{Gal}(L/K)$, where L/K is a Galois extension of number fields.

Definition 13 (Natural density). Let K be any number field and $\mathcal{A}$ any set of prime ideals $\mathfrak{P} \neq \{0\}$ in O_K. Then its Natural density $\delta_{Nat}(\mathcal{A})$ is defined as the following limit (if it exists)

$$\delta_{Nat}(\mathcal{A}) = \lim_{x\to\infty} \frac{|\{\mathfrak{P} \in \mathcal{A} : \|\mathfrak{P}\| \leq x\}|}{|\{\mathfrak{P} \in \mathcal{P}_K : \|\mathfrak{P}\| \leq x\}|}.$$

Example 9. A nice example is an infinite subset of prime numbers with natural density 0.

Set p_n the n-th prime number, and consider the set $S = \{p_i | i = n^2, n \in \mathbb{Z}^+\}$. By definition

$$\delta_{Nat}(S) = \lim_{n\to\infty} \frac{|S_n|}{|P_n|},$$

where P_n are the primes less or equal than n, and S_n are the primes in S with the same condition. So

$$\lim_{n\to\infty} \frac{|S_n|}{|P_n|} = \lim_{n\to\infty} \frac{\sqrt{|P_n|}}{|P_n|} = 0.$$

Now, we define an important mathematical object which gives us information about the proportion of a subset of the prime numbers.

Notice that

$$\ln(\zeta_K(s)) = \ln\left(\prod_{\mathfrak{P}\in\mathcal{P}_K} (1 - \|\mathfrak{P}\|^{-s})^{-1}\right) = -\sum_{\mathfrak{P}} \ln(1 - \|\mathfrak{P}\|^{-s}) = \sum_{\mathfrak{P}} \sum_{m\geq 1} \frac{1}{m \|\mathfrak{P}\|^{sm}}.$$

And the last summation when $m > 1$ converges for $s = 1$, hence

$$\ln(\zeta_K(s)) \sim \sum_{\mathfrak{P}} \|\mathfrak{P}\|^{-s},$$

for the same reason we can neglect those prime ideals $\mathfrak{P}$ with $\|\mathfrak{P}\| = p^f \geq p^2$ and get

$$\ln(\zeta_K(s)) \sim \sum_{\substack{\mathfrak{P}\in\mathcal{P}_K \\ f(\mathfrak{P}/p)=1}} \|\mathfrak{P}\|^{-s},$$

and since from the class number formula we have

$$\zeta_K(s) \sim \frac{2^{r+s}\pi^s \text{reg}(K)}{\omega_K(|\text{disc}(O_K)|)^{1/2}} h_K \cdot \frac{1}{s-1},$$

then

$$\sum_{\substack{\mathfrak{P}\in\mathcal{P}_K \\ f(\mathfrak{P}/p)=1}} \|\mathfrak{P}\|^{-s} \sim \ln(\zeta_K(s)) \sim \ln\left(\frac{1}{s-1}\right).$$

This allow us to define the Dirichlet density.

Definition 14 (Dirichlet density). Let K be any number field and $\mathcal{A}$ any set of prime ideals $\mathfrak{P} \neq \{0\}$ in O_K. Then its Dirichlet density $\delta(\mathcal{A})$ is defined as the number that grants the following asymptotic equivalence (if it exists)

$$\delta(\mathcal{A}) \sum_{\substack{\mathfrak{P}\in\mathcal{A} \\ f(\mathfrak{P}/p)=1}} \|\mathfrak{P}\|^{-s} \sim \delta(\mathcal{A}) \sum_{\mathfrak{P}\in\mathcal{A}} \|\mathfrak{P}\|^{-s} \sim \sum_{\mathfrak{P}\in\mathcal{P}_K} \|\mathfrak{P}\|^{-s} \sim \log\left(\frac{1}{s-1}\right).$$

It is well known that the existence of $\delta_{Nat}(M)$ implies the existence of $\delta(M)$, and that one has $\delta_{Nat}(M) = \delta(M)$, see [Neu13], page 543. So that when we will mention the density of a set of prime ideals, we assume that it is the Dirichlet density.

Lemma 9. Let L/K be a Galois extension of number fields. Then the density of the primes in K that split completely in L is $1/[L:K]$.

Proof. Consider $Spl(L/K)$ the set of all prime ideals in $\mathcal{P}_K$ such that split completely in L and notice that over each $\mathfrak{p} \in Spl(L/K)$ there are exactly $[L:K]$ primes. Let $\mathcal{A}$ be the set of all primes of $\mathcal{P}_L$, above some prime in $Spl_S(L/K)$. Then:

$$\ln\left(\frac{1}{s-1}\right) \sim \sum_{\substack{\mathfrak{P}\in\mathcal{P}_K \\ f(\mathfrak{P}/\mathfrak{p})=1}} \|\mathfrak{P}\|^{-s} = [L:K] \sum_{\mathfrak{p}\in\mathcal{A}} \|\mathfrak{p}\|^{-s}.$$

Then $\delta(Spl(L/K)) = 1/[L:K]$. □

Corollary 2. Given $m \in \mathbb{Z}^+$ There exist infinitely many prime numbers p such that $p \equiv 1 \pmod{m}$.

Proof. Take $K = \mathbb{Q}(\zeta_m)$, then p is totaly split in K if and only if Frob_p is the identity. Since the Frobenius automorphism is characterized by the equation $x^p \equiv \text{Frob}_p(x) \pmod{\mathfrak{p}}$, with $\mathfrak{p}|p$ and $x \in O_K$, then p is totaly split if and only if $p \equiv 1 \pmod{m}$. So, the set of all primes satisfying that condition, has positive density, as desired. □

Corollary 3. Suppose that L_1 and L_2 are Galois extensions of K, and S is a finite subset of primes in K. Then $L_1 = L_2$ if and only if $Spl_S(L_1/K) = Spl_S(L_2/K)$, where $Spl_S(L_i/K) = \{p \in \mathcal{P}_K : p \text{ is completely decomposed in } L_i \text{ and } p \notin S\}$.

Proof. Is clear that if $L_1 = L_2$ then $Spl_S(L_1/K) = Spl_S(L_2/K)$. On the other hand, consider the Galois extension $L = L_1L_2$, and the injective homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$, sending $\sigma \in \mathrm{Gal}(L/K)$ to $(\mathrm{res}_{L_1}(\sigma), \mathrm{res}_{L_2}(\sigma)) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Now, let $\mathfrak{P}$ a prime in L_1L_2 unramified in K, and let $\mathfrak{P}_i = \mathfrak{P} \cap L_i$ with $i = 1, 2$ and notice that the above homomorphism sends $\mathrm{Frob}_{\mathfrak{P}}(L/K)$ to $\mathrm{Frob}_{\mathfrak{P}_1}(L_1/K) \times \mathrm{Frob}_{\mathfrak{P}_2}(L_2/K)$. Suppose that $\mathfrak{P}$ split completely, then the decomposition subgroup $D_{\mathfrak{P}}$ is trivial, so we have

$$Spl_S(L/K) = Spl_S(L_1/K) \cap Spl_S(L_2/K) = Spl_S(L_1/K) = Spl_S(L_2/K).$$

By Lemma 9, we have that $\delta(Spl_S(L/K)) = 1/[L : K]$, then

$$\frac{1}{[L : K]} = \frac{1}{[L_1 : K]} = \frac{1}{[L_2 : K]} \Rightarrow [L : K] = [L_1 : K] = [L_2 : K],$$

hence $L_1 = L_2$. □

An important result in basic algebraic number theory is:

Theorem 10. Let L/K be a finite (not necessarily Galois) extension of number fields and N/K the normal closure of L/K. Then the prime ideal $\mathfrak{p}$ is totally split in K if and only if is totally split in N.

For a proof of this theorem the reader can see [Neu13], page 58. Now, we can prove the following corollary.

Corollary 4. Suppose that L_1 and L_2 are finite extensions of K, and S is a finite subset of primes in K. Then L_1 and L_2 have the same normal closure if and only if $Spl_S(L_1/K) = Spl_S(L_2/K)$.

Proof. If L_1 and L_2 have the same normal closure N, then for a prime ideal $\mathfrak{p}$ of O_K is totally split in L_1 if and only if it is so in N by 10, and this happens if and only if $\mathfrak{p}$ is totally split in L_2. On the other hand, let N_1 and N_2 be the normal closures of L_1 and L_2, respectively. Then by Theorem 10 $Spl_S(N_1/K) = Spl_S(N_2/K)$, and by Corollary 3 we have that $N_1 = N_2$. □

Chapter 3

Tchebotarev Density Theorem

Theorem 11 (Tchebotarev Density Theorem). Let E/K be a Galois extension of number fields with Galois group G and let $\mathcal{C}$ be a conjugacy class in G. Then the set

$$\begin{aligned} S &:= \{p \in \mathcal{P}_K : \mathrm{Frob}_{\mathfrak{P}}(E/K) \in \mathcal{C} \text{ for some } \mathfrak{P} \mid \mathfrak{p}\} \\ &= \{p \in \mathcal{P}_K : p \text{ is not ramified in } E,\ \mathrm{Frob}_p(E/K) = \mathcal{C}\}, \end{aligned}$$

has density $c/|G|$, where $|\mathcal{C}| = c$ and $\mathrm{Frob}_p(E/K) = \{\mathrm{Frob}_{\mathfrak{P}}(E/K) : \mathfrak{P} \mid p\}$.

3.1 Reduction To The Cyclic Case

The idea of the proof is to reduced to the case of cyclic extensions, next we prove the theorem for cyclotomic extension, and finally using the last case we prove it in the cyclic case.

Proof. (*of Theorem 11).* Suppose the theorem holds for cyclic extensions. Let $\sigma \in G$ and L be the field fixed by $\langle\sigma\rangle$. Hence E/L is a cyclic extension of degree $|\sigma|$. By assumption the set

$$S_\sigma := \{\mathfrak{p} \in \mathcal{P}_L : \mathrm{Frob}_{\mathfrak{P}}(E/L) = \sigma \text{ for some } \mathfrak{P} \mid \mathfrak{p}\},$$

has density $1/|\sigma|$. Now, notice that the set $S' := \{\mathfrak{p} \in S_\sigma : f(\mathfrak{p}/\mathfrak{p} \cap K) = 1\}$ also has density $1/|\sigma|$. We may define S from S' as follows:

$$S = \left\{p \in \mathcal{P}_K : \mathfrak{p} \in S' \text{ for some } \mathfrak{p} \in \mathcal{P}_L \text{ such that } \mathfrak{p} \mid p \text{ nonramified } \right\}, \tag{3.1}$$

First, we show that for $\mathfrak{P} \in \mathcal{P}_E$ it holds that $\mathrm{Frob}_{\mathfrak{P}}(E/K) = \sigma$ if and only if $\mathrm{Frob}_{\mathfrak{P}}(E/L) = \sigma$ and $f(\mathfrak{P} \cap L/p) = 1$.

The left implications is clear because

$$\mathrm{Frob}_{\mathfrak{P}}(E/K)^{f(\mathfrak{P}\cap L/p)} = \mathrm{Frob}_{\mathfrak{P}}(E/L). \tag{3.2}$$

On the other hand, $\overline{\sigma}$ generates $\mathrm{Gal}\,(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$. And since $\sigma \in \mathrm{Gal}(E/L)$, this is possible if and only if $\mathbb{F}_p = \mathbb{F}_{\mathfrak{p}}$, because $\overline{\sigma}$ also generates $\mathrm{Gal}\,(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$, hence $f\,(\mathfrak{P} \cap L/p) = [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p]$. And again using (3.2) we obtain the result. Now, notice that

$$\begin{aligned} p \in S &\iff p \text{ has a prime factor } \mathfrak{P} \text{ in } E \text{ with } \mathrm{Frob}_{\mathfrak{P}}(E/K) = \sigma \\ &\iff \mathrm{Frob}_{\mathfrak{P}}(E/L) = \sigma \text{ and } f\,(\mathfrak{P} \cap L/p) = 1 \text{ with } \mathfrak{P} \in \mathcal{P}_E,\ \mathfrak{P} \mid p \\ &\iff p \text{ has a prime factor } \mathfrak{p} \in L, \text{ with } \mathfrak{p} \in S', \end{aligned}$$

hence, we have (3.1).

Now, define $r_p = |\{\mathfrak{p} \in S' : \mathfrak{p} \mid p\}|$ and notice that

$$\delta(S') = \sum_{\mathfrak{p} \in S'} \|\mathfrak{p}\|^{-s} = \sum_{p \in S} \sum_{\mathfrak{p} \in S'} \|\mathfrak{p}\|^{-s} = \sum_{p \in S} r_p \cdot p^{-s}. \tag{3.3}$$

Now we prove that $r_p = \frac{|G|}{c \cdot |\sigma|}$ for all $p \in S$.

Notice that $r_p = |\{\mathfrak{P} \in \mathcal{P}_E : \mathcal{P} \mid p,\ \mathrm{Frob}_{\mathfrak{P}}(E/K) = \sigma\}|$, because for any $\mathfrak{p} \in S'$ and for some prime divisor $\mathfrak{P} \mid \mathfrak{p}$, we have that $\mathrm{Frob}_{\mathfrak{P}}(E/L) = \sigma$, hence $f\,(\mathfrak{P}/\mathfrak{p}) = |\sigma| = [E : L]$, because σ generates $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. Thus $\mathfrak{P}$ is the only prime of E over $\mathfrak{p}$.

By the new definition of S, $r_p \leq 0$ for all $p \in S$, then we can choose $\mathfrak{P}$ in E over p, such that $\mathrm{Frob}_{\mathfrak{P}}(E/K) = \sigma$. Then we can define r_p as follows:

$$\begin{aligned} r_p &= \{\tau\mathfrak{P} : \tau \in G,\ \mathrm{Frob}_{\tau\mathfrak{P}}(E/K)\} \\ &= \left\{\tau\mathfrak{P} : \tau \in G,\ \tau\sigma\tau^{-1} = \sigma\right\}. \end{aligned}$$

Because any element in O_E is of the form $\tau^{-1}(x)$, with $x \in O_E$, then

$$\mathrm{Frob}_{\mathfrak{P}}(E/K)\tau^{-1}(x) \equiv \tau^{-1}(x)^q (mod\, \mathfrak{P}),$$

composing with τ

$$\tau\,\mathrm{Frob}_{\mathfrak{P}}(E/K)\tau^{-1}(x) \equiv x^q (mod\, \tau(\mathfrak{P})),$$

hence $r_p = |\{\tau\mathfrak{P} : \tau \in C_G(\sigma)\}| = [C_G(\sigma) : C_G(\sigma) \cap D_{\mathfrak{P}}]$ where $C_G(\sigma)$ is a centralizer of σ. Since $\mathrm{Frob}_{\mathfrak{P}}(E/K) = \sigma$, we have $D_{\mathfrak{P}} = \langle\sigma\rangle \subset C_G(\sigma)$, then

$$r_p = \frac{|C_G(\sigma)|}{|\sigma|} = \frac{|G|}{|\sigma| \cdot c}. \tag{3.4}$$

Then by (3.3) and (3.4), we have

$$\frac{1}{|\sigma|} = \delta(S') = r_p \delta(S) = \frac{|G|}{|\sigma| \cdot c} \delta(S),$$

hence

$$\delta(S) = \frac{c}{|G|}.$$

□

3.2 Cyclotomic Extension Case

Before proving this theorem we need to define some invariants, for more details the reader can see [Mil97].

Definition 15 (The Artin map). Let L/K be an abelian extension of number fields with Galois group G. Let $\mathrm{Frob}_{\mathfrak{p}}$ the Frobenius automorphism associated to $\mathfrak{p}$ a prime ideal in K. For any finite set S of primes of K containing all primes that ramify in L, we define I^S the group of all fractional ideals of K relatively prime to the primes in S, and

$$\varphi_{L/K} : I^S \longrightarrow \mathrm{Gal}(L/K), \qquad \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t} \to \prod_{i=1}^{t} \mathrm{Frob}_{\mathfrak{p}_i}^{n_i},$$

called the global Artin map.

Milne in [Mil97] (chapter V, page 122) gives two examples of the Artin map.

Example 10. Let $K = \mathbb{Q}(\sqrt{m})$ where m is a squarefree integer. Let S be the set of finite primes ramifying in K. Since $\mathrm{disc}(O_K) = m$ if $m \equiv 1(\bmod 4)$ and is equal to $4m$ otherwise. Identify $\mathrm{Gal}(K/\mathbb{Q})$ with $\{\pm 1\}$. The Artin map is the homomorphism determined by

$$p \mapsto \left(\frac{\mathrm{disc}(O_K)}{p}\right) : I^S \to \mathrm{Gal}(K/\mathbb{Q}),$$

where $\left(\frac{\mathrm{disc}(O_K)}{p}\right)$ is the Legendre symbol.

Example 11. Let $K = Q(\zeta_m)$ where m is a primitive n-th root of 1. Assume that m is odd or divisible by 4 (so that the primes ramifying in K are precisely the primes dividing m). The map sending an integer m prime to n to the automorphism $\sigma_n : \zeta_m \mapsto \zeta_m^n$ of K is an isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/m\mathbb{Z})^*$. For p not dividing m $\mathrm{Frob}_p(K/\mathbb{Q}) = \sigma_p$ Then, the Artin map is the composite of

$$I^S \xrightarrow{(r/s)\mapsto \overline{r}\cdot\overline{s}^{-1}} (\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\overline{n}\mapsto(\zeta_m\mapsto\zeta_m^n)} \mathrm{Gal}(K/\mathbb{Q}).$$

And if we denote U^S the set of all principal ideals $\langle x\rangle$ such that $x \equiv 1$ (mod m) and $x > 0$, clearly $U^S \subset \ker(\varphi_{K/\mathbb{Q}})$. So we have the map of I^S/U^S to $\mathrm{Gal}(K/\mathbb{Q})$.

Theorem 12. Let $L/K'/K$ be a tower of fields, with L/K an abelian extension. Then the following diagram commutes

$$\begin{array}{ccc} I_{K'}^S & \xrightarrow{\varphi_{L/K'}} & \mathrm{Gal}(L/K') \\ {\scriptstyle \|\cdot\|_{L/K'}}\downarrow & & \downarrow{\scriptstyle i} \\ I_K^S & \xrightarrow{\varphi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

where S is any finite set of prime ideals of K containing all those that ramify in L and prime ideals of K' over a prime in S.

Proof. Let $\mathfrak{p}' \in \mathcal{P}_{K'}$ such that $\mathfrak{p} = \mathfrak{p}' \cap K \notin S$. Then $\|\mathfrak{p}'\|_{L/K'} = \mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}$. But since $\mathrm{Frob}_{\mathfrak{P}}(L/K) = \mathrm{Frob}_{\mathfrak{P}}(L/K')^{f(\mathfrak{p}'/\mathfrak{p})}$ for any prime ideal $\mathfrak{P}$ of L lying over $\mathfrak{p}$, then $\varphi_{L/K'}(\mathfrak{p}') = \varphi_{L/K}\left(\mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}\right)$. □

Corollary 5. For any abelian extension L of K

$$\left\|I_L^S\right\|_{L/K} \subset \ker\left(\varphi_{L/K} : I^S \to \mathrm{Gal}(L/K)\right).$$

Proof. Take $K' = L$ in the above diagram. □

Lemma 10. Let $L = K(\zeta_m)$, $G := \mathrm{Gal}(L/K)$ and $n = |G/H|$ where H is the image of $I_K^{\mathfrak{m}}/U_K^{\mathfrak{m}}$ over $\varphi_{L/K}$ with $\mathfrak{m} = mO_L$. Then

$$\prod_{\mathfrak{p}\nmid\mathfrak{m}} \left(1 - \|\mathfrak{p}\|^{-s}\right)^{-1} =: \zeta_L(s, \mathfrak{m}) = \prod_{\chi\in\widehat{H}} L(s, \mathfrak{m}, \chi \circ \varphi_{L/\mathbb{Q}})^n.$$

Proof. Let p be a rational number with $p \nmid m$. Suppose that $pO_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ with $f(\mathfrak{P}_i/p) = f$. Because p is nonramified in L, we have that $fg = [L : K] = n|H| = \varphi(m)$. In this way $g = \frac{n|H|}{f}$ and $\mathrm{Ord}(\varphi_{L/K}(p)) =$ order of $D_{\mathfrak{P}_i/p} = f$.

Then

$$\begin{aligned}\prod_{\chi\in\widehat{H}} L(s, \mathfrak{m}, \chi \circ \varphi_{L/K})^n &= \prod_{\chi\in\widehat{H}} \left(\prod_{p\nmid m} \left(1 - \frac{\chi(\varphi_{L/K}(p))}{p^s}\right)^{-n}\right) \\ &= \prod_{p\nmid m} \left(\prod_{\chi\in\widehat{H}} \left(1 - \frac{\chi(\varphi_{L/K}(p))}{p^s}\right)^{-n}\right).\end{aligned}$$

Now, we compute the product inside the first brackets.

$$\begin{aligned}\prod_{\chi\in\widehat{H}} \left(1 - \frac{\chi(\varphi_{L/K}(p))}{p^s}\right)^{-n} &= \prod_{i=0}^{f-1} \left(1 - \frac{\zeta_f^i}{p^s}\right)^{-\frac{n|H|}{f}} = \left(1 - \frac{1}{p^{sf}}\right)^{-\frac{n|H|}{f}} \\ &= \prod_{i=1}^{g} \left(1 - \frac{1}{\|\mathfrak{P}_i\|^s}\right),\end{aligned}$$

where ζ_f is a primitive f-root of the unity. □

Lemma 11. Let $L = K(\zeta_m)$ be a Galois extension and $G = \mathrm{Gal}(L/K)$ its Galois group, then we have that

$$\sum_{\chi\in\widehat{G}} \chi(g^{-1}) \log(L(s, \mathfrak{m}, \chi \circ \varphi_{K/K})) \sim \log\left(\frac{1}{s-1}\right).$$

Proof. With the notation as above, if χ is non trivial character of H, then $\chi\circ\varphi_{L/K}$ over $I_L^{\mathfrak{m}}/U_K^{\mathfrak{m}}$. By Proposition 3, $L(s,\mathfrak{m},\chi\circ\varphi_{L/K})$ has a simple pole at $s=1$, for $\chi=1$ and is analityc around $s=1$, for all non trivial characters. Suppose that for some non trivial character $L(s,\mathfrak{m},\chi\circ\varphi_{L/K})=0$, then $\prod_{\chi\in\widehat{H}} L(s,\mathfrak{m},\chi\circ\varphi_{L/K})^n$ would be analytic at $s=1$; which is a contradiction, because $\zeta_L(s,\mathfrak{m})$ has a simple pole at $s=1$, by the same proposition. □

Theorem 13. Let L/K be a Galois extension with $L=K(\zeta_m)$, $g\in\mathrm{Gal}(E/K)$ and

$$S:=\{p\in\mathbb{Z}:\mathrm{Frob}_p(E/K)=g, p \text{ nonramified in } E\}.$$

Then $\delta(S)=1/[L:K]$.

Proof. Let $\mathfrak{m}=mO_K$ be the modulus for L. Consider the function

$$h(s)=\sum_{\chi\in\widehat{G}}\chi(g^{-1})\log(L(s,\mathfrak{m},\chi\circ\varphi_{L/K})).$$

From Lemma 11, we have that

$$h(s)\sim\log\left(\frac{1}{s-1}\right), \tag{3.5}$$

but also

$$\begin{aligned} h(s)&\sim\sum_{p|\mathfrak{m}_0}\left(\sum_{\chi\in\widehat{G}}\chi(g^{-1})\chi(\varphi_{L/K}(p))p^{-s}\right)\sim[L:K]\sum_{\substack{p|\mathfrak{m}_0\\ \varphi_{L/K}(p)=g}}p^{-s}\\ &\sim[L:K]\sum_{\substack{p\\ \varphi_{L/K}(p)=g}}p^{-s}\sim[L:K]\sum_{p\in S}p^{-s}. \end{aligned}\tag{3.6}$$

Since (3.5) and (3.6), we have that

$$\sum_{p\in S}p^{-s}\sim\frac{1}{[L:K]}\log\left(\frac{1}{s-1}\right),$$

hence $\delta(S)=1/[L:K]$. □

3.3 Cyclic Case

We begin proving that if L/K is a cyclotomic extension, then for all intermediate extension the theorem holds.

Theorem 14. Let E/K be a Galois extension such that $E\subset L=K(\zeta_m)$, $g\in\mathrm{Gal}(E/K)$ and

$$S:=\{p\in\mathcal{P}_K:\mathrm{Frob}_p(E/K)=g, p \text{ nonramified in } E\}.$$

Then $\delta(S)=1/[E:K]$.

Proof. Let $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ denote the restriction map. We know that $\mathrm{res}\left(\mathrm{Frob}_p(L/K)\right) = \mathrm{Frob}_p(E/K)$, where p is a prime in O_K is nonramified in L.

Now, for each g in $\mathrm{Gal}(E/K)$ define

$$S' := \left\{p \in \mathcal{P}_K : \mathrm{Frob}_p(L/K) \in \mathrm{res}^{-1}(g), p \text{ nonramified in } L\right\}.$$

Notice that S' is contained in S, and $S \setminus S'$ is finite, i.e. $\delta(S) = \delta(S')$. By the Tchebotarev density theorem for cyclotomic extensions, we obtain that:

$$\delta(S') = \frac{\left|\mathrm{res}^{-1}(g)\right|}{[L:K]}.$$

Since $\left|\mathrm{res}^{-1}(g)\right| = [L:E]$, we have:

$$\delta(S) = \frac{[L:E]}{[L:K]} = \frac{1}{[E:K]}.$$

□

Before that prove the Tchebotarev theorem in the cyclic case, we need the following Lemma.

Lemma 12. Let L be a finite extension of a number field K and m a natural number, then there exists a cyclic extension M of K, contained in a cyclotomic extension of K, such that $[M:K] = m$ and $L \cap M = K$.

Proof. It is enough to find $M \subset \mathbb{Q}(\zeta)$ for some root of the unity ζ, sucha that $L \cap M = \mathbb{Q}$ and $[M:\mathbb{Q}]m$. If we have that , then $KM \subset K(\zeta)$, $L \cap KM = K$ and $[MK:K] = m$.

Let ω_L the number of roots of the unity in L, then $\mathbb{Q}(\zeta_{\omega_L}) \subset L$, so that by Corollary 2 we cand find p be a odd prime, such that $p = 1 + \omega_L m$. Then $\mathbb{Q}(\zeta_p)/\mathbb{Q}$is a cyclic extension and $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ and this group has a subgroup of order ω_L. We denote this group by H and the fixed field by H is the desired field, because $L \cap M \subset \mathbb{Q}(\zeta_{\omega_L}) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ since $(\omega_L, p) = 1$ and $[M:\mathbb{Q}] = [\mathbb{Q}(\zeta_p):\mathbb{Q}]/|H| = \omega_L m/\omega_L = m$. □

Theorem 15. Let L/K be a cyclic extension, and take $g \in \mathrm{Gal}(L/K)$ and

$$S_g := \{p \in \mathbb{Z} : \mathrm{Frob}_p(E/K) = g, p \text{ nonramified in } E\}.$$

Then $\delta(S_g) = 1/[L:K]$.

Proof. Let M be a cyclic extension of K, contained in $K(\zeta)$, for some ζ a root of the unity, $M \cap L = K$ and $|G|$ dividing $[M:K]$. Such extension exists by Lemma 12. Let τ be an element in $\mathrm{Gal}(M/K)$ such that Ord$(g) \mid$ Ord(τ).

Now, we can consider a Galois extension LM of K, and we know that $\mathrm{Gal}(LM/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$. Denote by ρ the image via this isomorphism of (g, τ), and let E be the fixed field by $\langle\rho\rangle$.

First, we prove that $EM = LM$. Let $\sigma \in \mathrm{Gal}(LM/K)$ such that $\sigma(EM) = EM$. In particular, $\sigma \in \mathrm{Gal}(LM/E) = \langle \rho \rangle$, so, $\sigma = (g^i, \tau^i)$. And because τ^i is the identity in $\mathrm{Gal}(M/K)$, then g^i is also the identity in $\mathrm{Gal}(L/K)$, since Ord$(g) \mid$ Ord(τ). Then σ is the identity in $\mathrm{Gal}(LM/K)$. Notice that EM is contained in a cyclotomic extension of E, so the Tchebotarev theorem holds for $\mathrm{Gal}(EM/E)$. Then we know the density of the following set:

$$\mathcal{A}_\tau = \{\mathfrak{p} \in \mathcal{P}_E : \mathrm{Frob}_\mathfrak{p}(EM/E) = \rho\},$$

which is $\delta(\mathcal{A}_\tau) = 1/[EM : E]$, and we know that this set has the same density that:

$$\mathcal{B}_\tau = \{\mathfrak{p} \in \mathcal{P}_E : \mathrm{Frob}_\mathfrak{p}(EM/E) = \rho \text{ and } \|\mathfrak{p} \cap K\| = \|\mathfrak{p}\|\}.$$

Consider $p \in \mathcal{P}_K$ such that $\mathfrak{p}|p$ such that $\mathfrak{p}|p$ for some $\mathfrak{p} \in \mathcal{P}_K$, then

$$\mathrm{Frob}_p(LM/K) = \mathrm{Frob}_\mathfrak{p}(LM/E) = \rho.$$

This implies that $p \in \mathcal{C}_\tau := \{p \in \mathcal{P}_K : \mathrm{Frob}_p(LM/K) = \rho\}$.

On the other hand, if $\mathfrak{p} \in \mathcal{P}_E$, with $\mathfrak{p}|p$ and $p \in \mathcal{C}_\tau$, then $\mathrm{Frob}_\mathfrak{p}(LM/K)|_E = \mathrm{Frob}_p(E/K) = \rho|_E =$ identity. So that, p is totally split in E and $\|\mathfrak{p}\| = \|\mathfrak{p} \cap K\|$. Then in the same way as in (3.6), we have that

$$\delta(\mathcal{B}_\tau) = [E : K]\delta(\mathcal{C}_\tau),$$

hence

$$\delta(\mathcal{C}_\tau) = \frac{1}{[E : K][EM : E]} = \frac{1}{[L : K][M : K]}.$$

Since $S_g \supset \bigcup_{\tau \in D(M/K)} \mathcal{C}_\tau$, where $D(M/K) := \{\tau \in \mathrm{Gal}(M/K) : \text{Ord}(g) \mid \text{Ord}(\tau)\}$, then

$$\begin{aligned}\delta(S_g) \geq \delta\Big(\bigcup_{\tau \in D(M/K)} \mathcal{C}_\tau\Big) &= \sum_{\tau \in D(M/K)} \delta(\mathcal{C}_\tau) \\ &= \frac{1}{[L : K]} \frac{|D(M/K)|}{[M : K]}.\end{aligned}$$

Now, the idea is to prove that for all $0 < \varepsilon < 1$ there exists an extension F of K satisfying the conditions of M, and such that

$$1 > \frac{|D(F/K)|}{[F : K]} > 1 - \varepsilon,$$

because if we have that, then

$$\delta(S_g) > \frac{1}{[L : K]}(1 - \varepsilon). \qquad [0 < \varepsilon < 1]$$

So that

$$\delta(S_g) \geq \frac{1}{[L : K]},$$

and from the fact

$$\sum_{g \in \mathrm{Gal}(L/K)} \delta(S_g) = 1,$$

then $\delta(S_g) = 1/[L:K]$.

Let $\mathrm{Ord}(g) = p_1^{e_1} \cdots p_\ell^{e_\ell}$. By Lemma 12 we can construct a cyclic extension F of degree $p_1^{e_1'} \cdots p_\ell^{e_\ell'}$, with $e_i' > e_i$ for $i = 1, \ldots, \ell$. So that

$$|D(F/K)| = \prod_{i=1}^{\ell} \left(p^{e_i'} - p^{e_i - 1} \right) = [F:K] \prod_{i=1}^{\ell} \left(1 - \frac{1}{p^{e_i' - e_i + 1}} \right),$$

hence

$$\frac{|D(F/K)|}{[F:K]} = \prod_{i=1}^{\ell} \left(1 - \frac{1}{p^{e_i' - e_i + 1}} \right).$$

Since the above producct goes to 1 when e_i''s goes to infinity, for all $0 < \varepsilon < 1$ we can find $e_1', \ldots, e_\ell'$, such that F of degree $p_1^{e_1'} \cdots p_\ell^{e_\ell'}$, such that

$$1 > \frac{|D(F/K)|}{[F:K]} > 1 - \varepsilon.$$

□

3.4 Dirichlet density theorem

An important Corollary of Tchebotarev Density Theorem, is the Dirichlet density theorem, which states that any arithmetic progression of the form $\{a + bm\}_{b \in \mathbb{Z}}$ with $(a, m) = 1$, has infinite rational primes; even better we can compute the density of the set of this primes. Notice that this Theorem is the generalization of Corollary 2.

Theorem 16. Let a and m be relatively prime positive numbers. Then there exist infinitely many prime numbers p such that $p \equiv a \pmod{m}$.

Proof. Take $K = \mathbb{Q}(\zeta_m)$, if a is relative prime to m consider $\sigma_a \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma_a(\zeta_m) = \zeta_m^a$.

Moreover, notice that if $p \in \mathbb{Z}$ satisfies $p \equiv a \pmod{m}$ we have $\mathrm{Frob}_p = \sigma_a$ (we denote Frob_p because G is abelian, then the Frobenius is the same for all prime ideals over p). Since the Frobenius automorphism is characterized by the equation $x^p \equiv \mathrm{Frob}_p(x) \pmod{\mathfrak{p}}$, with $\mathfrak{p} | p$ and $x \in O_K$, the result is obtained from the fact that $O_K = \mathbb{Z}[\zeta_m]$.

Hence, if $\mathcal{A}_a = \{p \in \mathbb{Z} : p \equiv a \pmod{m}\}$ by the Tchebotarev density theorem $\delta(\mathcal{A}_a) \leq 1/\varphi(m)$, and using symmetry we get, $\delta(\mathcal{A}_{a_i}) \leq 1/\varphi(m)$ for $i = 1, \ldots, \varphi(m)$ where $a_1 = a$, and each a_i is a representative of a different coset in $(\mathbb{Z}/m\mathbb{Z})^*$. Finally, notice that

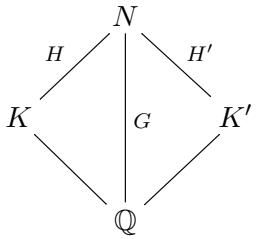
$$\sum_{i=1}^{\varphi(m)} \delta(\mathcal{A}_{a_i}) = 1.$$

So we obtain $\delta(\mathcal{A}_a) = 1/\varphi(m)$. □

Chapter 4

Arithmetic Equivalence through Galois representations

Consider the following situation: Let K and K' be two number fields, and N the normal closure of KK'. Now, we can consider the groups $H := \mathrm{Gal}(N/K)$, $H' := \mathrm{Gal}(N/K')$ and $G := \mathrm{Gal}(N/\mathbb{Q})$, which can be visualized in the following diagram



Perlis proved in [Per77] that wo number K and K' are *arithmetically equivalent* (i.e., they have the same Dedekind zeta function) if and only if the subgroups H and H' of G are *Gassmann equivalents*, that is, $|c^G \cap H| = |c^G \cap H'|$ for every conjugacy class $c^G = \{gcg^{-1} : g \in G\}$ in G, where N is the normal closure of KK'. The idea behind the proof is to try to generalize the fact that two isomorphic number fields are arithmetically equivalent, and the converse is not necessarily true. With the help of this theorem, he finds infinitely many examples of non isomorphic number fields with this property. As an intermediate step, he shows that each invariant (being arithmetically equivalent and satisfying $|c^G \cap H| = |c^G \cap H'|$) is equivalent to the following fact: "for all but a finite set of rational primes p, the decomposition of p is the same in the two number fields, that is, the number of primes in each field over p is the same and their residual degrees agree". To show this, he uses an ad hoc process that uses a fact from complex analysis. Hence, motivated by this, it arises the idea of addressing the problem with Artin's L-functions of specific Galois representations.

Additionally, [MS16] weakens in two ways the mentioned intermediate step. First, we can consider that this condition holds only for all the rational primes except for a set of density 0, and not necessarily for all but a finite number of them. Second, it is not necessary to require that for each prime all their residual degrees agree, it is enough to require this for those whose residual degree is 1.

We will give a sketch of the proof of Robert Perlis [Per77]. He began with the following definitions and lemmas. Although we will not prove them, the reader can see [Per77].

Definition 16. Let $pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, and let $f_i = [\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_p]$, numbered such that $f_i \leq f_{i+1}$. Then the tupel $A = (f_1, \ldots, f_g)$ is called the splitting type of p in K.

Every tupel A is associated with the set

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

By the fundamental equality, $P_K(A)$ is empty except for finitely many A. Further, the notation

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

means that the two sets differ by at most a finite number of primes.

Definition 17. Let p be an unramified prime of $\mathbb{Z}$, and C be a decomposition subgroup of p in G, which is cyclic since p is unramified. Consider $G = \bigcup_i^h Ht_iC$ a disjoint union of double cosets, and define the *coset type* as the f_i's obtained as follows $|Ht_iC| = |H| \cdot f_i$. We denote this invariant by *coset type*$[G \bmod (H, C)]$.

The following lemma proves that the previous two definitions are equivalent.

Lemma 13. Let p be an unramified prime of $\mathbb{Z}$, then p has the same splitting type in both K and K' if and only if

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

where C is a decomposition subgroup of p.

We have another definition, which is equivalent to the previous presented definitions.

Definition 18. Let H and H' be two subgroups of a group G, then H and H' are *Gasdsmann equivalent* if $|c^G \cap H| = |c^G \cap H'|$ for every conjugacy class $c^G = \{gcg^{-1} : g \in G\}$ in G.

Lemma 14. 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.

Next lemma is presented without a motivation, however we will show its importance in the proof of Perlis' theorem.

Lemma 15. Let $\tau_1(s) = \prod_{j=1}^n (1 - c_j^{-s})$ and $\tau_2(s) = \prod_{i=1}^m (1 - d_i^{-s})$ with real $c_j, d_i > 1$. Let $f(s)$ be a meromorphic function whose zeroes and poles do not lie among the zeroes of either $\tau_1(s)$ or $\tau_2(s)$. 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 $f(s) = 1$.

Theorem 17 (Perlis 1977). Let K and L be two number fields and $N/\mathbb{Q}$ Galois containing K and K'. Define the groups $G := \mathrm{Gal}(N/\mathbb{Q})$, $H := \mathrm{Gal}(N/K)$ and $H' := \mathrm{Gal}(N/K')$. Then 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) $|c^G \cap H| = |c^G \cap H'|$ for every conjugacy class $c^G = \{gcg^{-1} : g \in G\}$ in G

Proof. $(a) \Rightarrow (b)$ Write the Dedekind zeta function as follows

$$\zeta_K(s) = \sum_{n \geq 1} \frac{a_K(n)}{n^s}$$

where $a_K(n)$ is the number of ideals of norm n. Inductively he shows that $a_K(m) = a_{K'}(m)$, for all $m \in \mathbb{Z}^+$. And he uses the equation

$$a_K(p^f) - \sum a_K(p^{b_1})...a_K(p^{b_r})$$

where $b_1, \ldots, b_r \geq 1$, $b_1 + ... + b_r = f$ and $r \geq 2$, to show that the number of primes in K and K' with norm p^f is the same.

$(b) \Rightarrow (c)$ is clear.

$(c) \Leftrightarrow (d)$ he proves these implications using lemma 13 and lemma 14.

$(d) \Rightarrow (a)$ Using the analytic extension of $\zeta_K(s)$ for the whole complex plane except for simple poles at $s = 0, 1$

$$Z_K(s) = \left(\pi^{-s/2}\Gamma(s/2)\right)^{n_1(K)} \left((2\pi)^{1-s}\Gamma(s)\right)^{n_2(K)} \zeta_K(s),$$

where $n_1(K)$ is the number of the real embeddings of K and $n_2(K)$ is the number of complex pairs embeddings. Then, he uses the following properties of the analytic extension

$$Z_K(s) = \text{disc}(O_K)^{1/2-s} Z_K(1-s),$$

and with the quotient of $Z_K(s)$ by $Z_{K'}(s)$, he obtains:

$$\frac{\zeta_K(s)}{\zeta_{K'}(s)} = \left|\frac{\text{disc}(O_K)}{\text{disc}(O_{K'})}\right|^{(1/2)-s} \cdot \frac{\zeta_K(1-s)}{\zeta_{K'}(1-s)}.$$

By hypothesis $\zeta_K(s)/\zeta_{K'}(s)$ is a finite product, thus, using lemma 15 he obtains this implication.

Notice that $|\text{disc}(O_K)| = |\text{disc}(O_{K'})|$, and in an intermediate step in $(d) \Rightarrow (a)$ he proves that the number of complex embeddings in K and K' are the same. Then $\text{disc}(O_K) = \text{disc}(O_{K'})$, because the sign of $\text{disc}(O_K)$ is $(-1)^{n_2(K)}$. □

4.1 On the equation $\zeta_K(s) = \zeta_{K'}(s)$

We begin defining an important Galois representation for a number field such that its Artin's L-function is $\zeta_K(s)$.

Definition 19. Let $K/\mathbb{Q}$ be a finite extension with $n = [K : \mathbb{Q}]$. By the Primitive Element Theorem, we let $K = \mathbb{Q}(\alpha)$, and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Let $\Sigma_K = \{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n\}$ be the set of roots of f and let $\mathrm{Em}_K = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be all the embeddings of K into $\mathbb{C}$ such that $\sigma_i(\alpha) = \alpha_i$ for $i \in \{1, \ldots, n\}$.

Now, consider $\widetilde{K}$ the normal closure of K, and notice that for any $\sigma \in \mathrm{Em}_K$ we have that $\sigma(K) \subset \widetilde{K}$. We define $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for a fixed algebraic closure of $\mathbb{Q}$, so that $G_{\mathbb{Q}}$ acts transitively in Em_K as follows: if $\tau \in G_{\mathbb{Q}}$ and $\sigma \in \mathrm{Em}_K$, then $\tau \cdot \sigma = \tau \circ \sigma \in \mathrm{Em}_K$. Then we can define $\varphi : G_{\mathbb{Q}} \to S_n$ from the above action, where S_n is the Symmetric group. Finally, consider the following representation of S_n, $\rho : S_n \to GL_n(\mathbb{C})$, defined by permuting the columns of identity matrix. Then, we define a representation for $G_{\mathbb{Q}}$ by the composition $\rho_K := \rho \circ \varphi$. More over, we can define a representation $\widetilde{\rho_K}$ of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ by restricting to $\widetilde{K}$.

To prove the theorem of Mantilla-Soler we will need the following results. We have to show the following Lemma, which is a Corollary of Tchebotarev density theorem.

Lemma 16. Let $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{C})$ be a Galois representation which ramifies at most at finitely many primes of $\mathbb{Q}$. Then the set

$$\{\rho(\mathrm{Frob}_{\mathfrak{p}}) : \mathfrak{p} \text{ unramified}\},$$

is a dense subset of the image $\rho(G_{\mathbb{Q}})$. In other words, the Frobenius elements topologically generates the image of the Galois representation. Hence, the Galois representation is uniquely determined by the images of the Frobenius elements.

Proof. Let $A = \{\rho(\mathrm{Frob}_{\mathfrak{p}}) : \mathfrak{p} \text{ unramified}\}$. We need prove that the image of A under all natural projections $G_{\mathbb{Q}} \to G_i$ is equal to G_i, where the G_i's are finite Galois extension of $\mathbb{Q}$, then the Tchebotarev density theorem implies that the image of A in any finite quotient is all G_i. □

Definition 20. Let $p \in \mathbb{Z}$ and let $\rho : G_{\mathbb{Q}} \to GL_n(\mathbb{C})$ be a Galois representation. Then ρ is unramified in p whenever $\rho(I_{\mathfrak{P}}) = \{Id\}$ for all prime $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ over p.

Suppose that $\mathfrak{P}$ and $\mathfrak{P}'$ are primes above $\overline{\mathbb{Q}}$ over p. Notice that the subgroups $I_{\mathfrak{P}}$ and $I_{\mathfrak{P}'}$ are conjugates by any automorphism that sends $\mathfrak{P}$ to $\mathfrak{P}'$. Hence, $I_{\mathfrak{P}} \subset \ker(\rho)$ if and only if $I_{\mathfrak{P}'} \subset \ker(\rho)$, i.e. ρ is unramified in p when $\rho(I_{\mathfrak{P}}) = \{Id\}$ for some prime $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ over p.

Proposition 4. Let ρ be a Galois representation and let $K/\mathbb{Q}$ be the sub-extension of $\overline{\mathbb{Q}}$ fixed by $\ker(\rho)$. Then ρ is unramified in p if and only if p is unramified in K.

Proof. Let $\pi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ be the natural projection. Let $\mathfrak{P}|\mathfrak{p}|p$ where $\mathfrak{P}$ and $\mathfrak{p}$ are primes of $\overline{\mathbb{Q}}$ and L respectively. We know that p is unramified in K if and only if $I_{\mathfrak{p}} = \{\mathrm{Id}\}$, and since $I_{\mathfrak{p}} = \pi(I_{\mathfrak{P}})$, we obtain that $I_{\mathfrak{p}} = \{\mathrm{Id}\}$ if and only if $I_{\mathfrak{P}} \subset \ker\left(\pi|_{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}\right) = \ker(\rho)$, i.e. ρ is unramified in p. □

Lemma 17. Let $K/\mathbb{Q}$ be a finite extension of number fields and $N/\mathbb{Q}$ a Galois extension containing K with Galois group G. For any prime ideal p of $\mathbb{Q}$ which is unramified in N, define $\Omega_p^K = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p}|p, \text{ and } f(\mathfrak{p}/p) = 1\}$ and $\Gamma_{\mathfrak{P}/p}^K = \{\sigma_i \in \mathrm{Em}_K : \mathrm{Frob}_{\mathfrak{P}}(\sigma(\alpha)) = \sigma(\alpha)\}$ where $\mathrm{Frob}_{\mathfrak{P}}$ is the Frobenius automorphism of the prime $\mathfrak{P}$ of N over p. Then for any prime $\mathfrak{P}$ of N over p, $\left|\Omega_p^K\right| = \left|\Gamma_{\mathfrak{P}/p}^K\right|$.

Proof. Denote $F = \mathrm{Frob}_{\mathfrak{P}}$, then

$$F(\sigma(\alpha)) = \sigma(\alpha) \iff \sigma^{-1}F\sigma \in \mathrm{Gal}(N/K),$$

and, since by definition $\sigma^{-1}F\sigma \in D_{N/\mathbb{Q}}(\sigma(\mathfrak{P}))$ we have

$$\begin{aligned} F(\sigma(\alpha)) = \sigma(\alpha) &\iff \sigma^{-1}F\sigma \in \mathrm{Gal}(N/K) \cap D_{N/\mathbb{Q}}(\sigma(\mathfrak{P})) = D_{N/K}(\sigma(\mathfrak{P})) \\ &\iff \sigma^{-1}F\sigma \in \left\langle \mathrm{Frob}_{\sigma(\mathfrak{P})}(N/K) \right\rangle = \left\langle (\sigma^{-1}F\sigma)^{f(\sigma(\mathfrak{p})/p)} \right\rangle \\ &\iff 1 \equiv d \cdot f(\sigma(\mathfrak{p})/p) \,(\mathrm{mod}\ \mathrm{Ord}(\sigma^{-1}F\sigma)) \\ &\iff f(\sigma(\mathfrak{p})/p) = 1. \end{aligned}$$

For the last equivalence we use the fact that $f(\sigma(\mathfrak{p})/p)$ divides $f(\sigma(\mathfrak{P})/p) = \mathrm{Ord}(\sigma^{-1}F\sigma)$. □

Now, we will show the details of the proof of [MS16].

Theorem 18 (Mantilla-Soler 2016). Let K and K' be two number fields and $N/\mathbb{Q}$ Galois containing K and K'. Define the groups $G := \mathrm{Gal}(N/\mathbb{Q})$, $H := \mathrm{Gal}(N/K)$ and $H' := \mathrm{Gal}(N/K')$, and consider $\mathrm{Ind}_H^G\{1_H\}$ the induced representation of the trivial representation $1_H : H \to \mathbb{C}^*$. Then the following conditions are equivalent:

(a) $\widetilde{\rho_K} \cong \widetilde{\rho_{K'}}$

(b) $\mathrm{Ind}_H^G\{1_H\} \cong \mathrm{Ind}_{H'}^G\{1_{H'}\}$

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

(d) $\left|\Omega_p^K\right| = \left|\Omega_p^{K'}\right|$, where $\Omega_p^K = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p}|p, \text{ and } f(\mathfrak{p}/p) = 1\}$, for all $p \in \mathcal{A}$, with $\delta(\mathcal{A}) = 1$.

Proof. $(a) \Leftrightarrow (b)$. Is enough prove that $\mathrm{Ind}_H^G\{1_H\} \cong \widetilde{\rho_K}$. We know that two representation are isomorphic if and only if their characters are the same. Then it is enough to show that

$$\psi_{\mathrm{Ind}_H^G\{1_H\}} = \psi_{\widetilde{\rho_k}}.$$

Now, notice that:

$$\psi_{\mathrm{Ind}_H^G\{1_H\}}(g) = \frac{1}{|H|}\sum_{x \in G} \dot{1}_H(x^{-1}gx),$$

where

$$\dot{1}_H(x) = \begin{cases} 1 & if \quad x \in H \\ \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\begin{aligned} \psi_{\mathrm{Ind}_H^G\{1_H\}}(g) &= \frac{|\left\{x \in G \mid x^{-1}gx \in H\right\}|}{|H|} \\ &= \frac{|H \cap g^G||G|}{|H||g^G|}, \end{aligned}$$

because every conjugacy class has $|G|/|g^G|$ elements.

On the other hand we have that

$$\psi_{\widetilde{\rho_k}}(g) = tr(\rho_k(g)),$$

and $tr(\rho_k(g))$ is equal to the number of σ_i in Em_K such that σ_i is invariant under the action by g, because the i-th column has 1 in the diagonal. Then

$$\psi_{\widetilde{\rho_k}}(g) = |\{\sigma_i \in \mathrm{Em}_K \mid g \circ \sigma_i(k) = \sigma_i(k),\ \forall k \in K\}|\,.$$

It is well-known that σ_i extends to an automorphism $\widehat{\sigma_i} : \overline{K} \to \overline{K}$, where $\overline{K}$ is the normal closure. Now notice that if

$$\sigma_i \in \{\sigma_i \in \mathrm{Em}_K \mid g \circ \sigma_i(k) = \sigma_i(k),\ \forall k \in K\}\,,$$

then $\widehat{\sigma_i}^{-1} g \widehat{\sigma_i} \in H$ because it fixes all the elements in K. but notice that σ_i extends in $|H|$ different ways, so

$$\begin{aligned} |\{\sigma_i \in \mathrm{Em}_K \mid g \circ \sigma_i(k) = \sigma_i(k),\, \forall k \in K\}| &= \frac{\left|\left\{\sigma \in G \mid \sigma^{-1}g\sigma \in H\right\}\right|}{|H|} \\ &= \frac{|H \cap g^G||G|}{|H||g^G|}. \end{aligned}$$

$(b) \Rightarrow (c)$. We know that

$$\begin{aligned} L(s, \psi_{\mathrm{Ind}_H^G\{1_H\}}, N/\mathbb{Q}) &= L(s, 1, N/K) && \text{[by theorem 4(c)]} \\ &= L(s, 1, K/K) && \text{[by theorem 4(b)]} \\ &= \zeta_K(s). \end{aligned}$$

And by hypothesis $\mathrm{Ind}_H^G\{1_H\} \cong \mathrm{Ind}_{H'}^G\{1_{H'}\}$, hence

$$L(s, \psi_{\mathrm{Ind}_{H'}^G\{1_{H'}\}}, N/K') = L(s, \psi_{\mathrm{Ind}_H^G\{1_H\}}, N/K),$$

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

$(c) \Rightarrow (d)$. Write the Dedekind zeta function as follows

$$\zeta_K(s) = \sum_{n \geq 1} \frac{a_K(n)}{n^s},$$

where $a_K(n)$ is the number of ideals of norm n. So, by Lemma 2 we get that $a_K(m) = a_{K'}(m)$, for all $m \in \mathbb{Z}^+$.

In particular we obtain that the number of primes over p with residual degree 1 is the same in K and K', because $a_K(p) = a_{K'}(p)$. Hence $\left|\Omega_p^K\right| = \left|\Omega_p^{K'}\right|$.

$(d) \Rightarrow (a)$. By lemma 17 we have that

$$\left|\Gamma^K_{\mathfrak{P}/p}\right| = \left|\Gamma^{K'}_{\mathfrak{P}/p}\right|. \tag{4.1}$$

Now, we know that $\rho_K \cong \rho_{K'}$ if and only if their characters ψ_{ρ_K} and $\psi_{\rho_{K'}}$ respectively, are equals. But, by Lemma 5 is sufficient that $\psi_{\rho_K}(\mathrm{Frob}_{\mathfrak{P}}) = \psi_{\rho_{K'}}(\mathrm{Frob}_{\mathfrak{P}})$ for any prime $\mathfrak{P}$ over p that is unramified in ρ_K and $\rho_{K'}$, because the set of all primes which ramify in both representations is finite, since it is the union of the sets of primes that ramify in each one.

But notice that

$$\psi_{\rho_K}(\mathrm{Frob}_{\mathfrak{P}}) = |\{\sigma_i \in \mathrm{Em}_K : \mathrm{Frob}_{\mathfrak{P}}(\sigma(\alpha)) = \sigma(\alpha)\}| = \left|\Gamma_{\mathfrak{P}/p}\right|,$$

so, by (3) we have that

$$\psi_{\rho_K}(\mathrm{Frob}_{\mathfrak{P}}) = \psi_{\rho_{K'}}(\mathrm{Frob}_{\mathfrak{P}}).$$

□

Observation 4. Since the set of the rational primes which split completely has positive density, we can find a prime $p \in \mathbb{Z}$ such that p is totally split over K. We know that $\psi_{\mathrm{Ind}_H^G\{1_H\}}(\mathrm{Frob}_{\mathfrak{P}}) = \psi_{\mathrm{Ind}_{H'}^G\{1_{H'}\}}(\mathrm{Frob}_{\mathfrak{P}})$, where $\mathfrak{P}$ is any prime in N over p, then

$$\begin{aligned}[K : \mathbb{Q}] &= |\{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p}|p, \text{ and } f(\mathfrak{p}/p) = 1\}| = \psi_{\mathrm{Ind}_H^G\{1_H\}}(\mathrm{Frob}_{\mathfrak{P}}) \\ &= \psi_{\mathrm{Ind}_{H'}^G\{1_{H'}\}}(\mathrm{Frob}_{\mathfrak{P}}) \leq [K' : \mathbb{Q}],\end{aligned}$$

and by symmetry $[K : \mathbb{Q}] = [K' : \mathbb{Q}]$, hence $|H| = |H'|$.

Observation 5. Notice that Observation 2 and Theorem 18 say that if two number fields are arithmetically equivalents, then have the same discriminant.

Observation 6. Let r and s (r' and s') the number of real an pair of complex embeddings of K (K'), respectively. We can show that $r = r'$, and consequently $s = s'$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the complex conjugacy. Then $\sigma|_N \in \mathrm{Gal}(N/\mathbb{Q})$. So, consider

$$\psi_{\widetilde{\rho_K}}(\sigma|_N) = |\{\alpha_i \in \Sigma_K : \sigma|_N(\alpha_i) = \alpha_i\}|,$$

but α_i is in this set, if and only if $\alpha_i \in \mathbb{R}$. Then $\psi_{\widetilde{\rho_K}}(\sigma|_N) = r$. In the same way $\psi_{\widetilde{\rho_{K'}}}(\sigma|_N) = r'$.

Observation 7. Consider the subextension of K, $\mathbb{Q}(\zeta_{\omega_K})$, where ω_K is the number of roots of the unity in K. We claim that this subextension is also contained in K'.

Then, we can consider $J := \mathrm{Gal}(N/\mathbb{Q}(\zeta_{\omega_K}))$ like a subgroup of G in which case is normal because $\mathbb{Q}(\zeta_{\omega_K}))/\mathbb{Q}$ is a Galois extension. Hence, there exist $g_1, \ldots, g_\ell \in G$ such that $J = \bigcup g_i^G$ is a disjoint union of the conjugacy classes of the g_i's. So we have

$$\left|J \cap H'\right| = \sum_{i=1}^{\ell} \left|g_i^G \cap H'\right|$$

And we know that

$$\begin{aligned}\psi_{\mathrm{Ind}_H^G\{1_H\}}(\sigma) &= \frac{\left|\left\{x \in G \mid x^{-1}\sigma x \in H\right\}\right|}{|H|} \\ &= \frac{|H \cap \sigma^G||G|}{|H||\sigma^G|},\end{aligned}$$

so that

$$\begin{aligned}\left|J \cap H'\right| &= \sum_{i=1}^{\ell} \frac{\psi_{\mathrm{Ind}_{H'}^G\{1_{H'}\}}(g_i)\,|H'|\,\left|g_i^G\right|}{|G|} \\ &= \sum_{i=1}^{\ell} \frac{\psi_{\mathrm{Ind}_H^G\{1_H\}}(g_i)|H|\,\left|g_i^G\right|}{|G|} \qquad \text{[Observation 4]} \\ &= |J \cap H| = |H| = \left|H'\right|.\end{aligned}$$

Thus $H' \leq J$, hence $\mathbb{Q}(\zeta_{\omega_K}) \subset K'$ and by symmetry $\omega_K = \omega_{K'}$

Example 12. Consider $K = \mathbb{Q}(\sqrt[8]{3})$ and $K' = \mathbb{Q}(\sqrt{2} \cdot \sqrt[8]{3})$. We will prove that K and K' have the same Dedekind zeta function.

Notice that by the Dedekind Criterion is enough that $x^8 - 3$ and $x^8 - 16 \cdot 3$ have the same number of roots in $\mathbb{F}_p$, for almost all primes in $\mathbb{Z}$. To prove that statement is necessary to show the next Theorem.

Theorem 19. $f(x) = x^8 - 16$ has at least one root in $\mathbb{F}_p$ for all prime p in $\mathbb{Q}$.

Proof. $p = 2$ is clear. By quadratic reciprocity we know that for $p \equiv_8 1, 7$, there exists $\alpha \in \mathbb{F}_p$ such that $\alpha^2 \equiv_p 2$, then $f(\alpha) \equiv_p 0$. If $p = 8k + 3$ for some $k \in \mathbb{Z}$, we know that 4 is a unit in $\mathbb{F}_p$, then $4^{8k+2} \equiv_p 1$ hence $f(4^{-k}) \equiv_p 0$. In the same way, if $p = 8k + 5$ for some $k \in \mathbb{Z}$, we have $f(2^{-k}) \equiv_p 0$. □

Since, for $p \neq 2, 3$ the polynomial $x^8 - 3$ doesn't have repeated roots in $\mathbb{F}_p$, the roots in $\mathbb{F}_p$ of $x^8 - 16 \cdot 3$ are of the form $\gamma = \alpha\beta$, where α is like Theorem 19, and β is a root of $x^8 - 3$, in $\mathbb{F}_p$. Hence, $\gamma \in \mathbb{F}_p$ if and only if $\beta \in \mathbb{F}_p$.

4.2 A Galois theoretic characterization of arithmetic equivalence

Notice that from the proof above if two number fields are arithmetically equivalents all the residual degrees agree. In addition, the number of primes over p with residual degree f is given by the equation

$$a_K(p^f) - \sum a_K(p^{b_1})...a_K(p^{b_r}),$$

where $b_1, \ldots, b_r \geq 1$, $b_1 + ... + b_r = f$ and $r \geq 2$.

Hence, if two number fields K and L are arithmetically equivalents, the number of primes of O_K over p is the same that the number of primes in $O_{K'}$ over p, for all rational prime p. A nice result is that the other implication it's also true.

Definition 21. Let p be a rational prime and let K be a number field. We denote $g_K(p)$ the number of the primes of O_K over p.

Theorem 20. Let K and K' be two number fields and suppose that $g_K(p) = g_{K'}(p)$ for almost every p, then K and K' are arithmetically equivalent.

Proof. We will prove that if $g_K(p) = g_{K'}(p)$, then $\widetilde{\rho_K}(g) \cong \widetilde{\rho_{K'}}(g)$ for all $g \in G := \mathrm{Gal}(N/\mathbb{Q})$, where N is the normal closure of KK'.

First, notice that since the set of the rational primes, which split completely, has positive density, we can find a prime $p \in \mathbb{Z}$ such that p is totally split over K and $g_K(p) = g_{K'}(p)$, then

$$[K : \mathbb{Q}] = g_K(p) = g_{K'}(p) \leq [K' : \mathbb{Q}],$$

And by symmetry $[K : \mathbb{Q}] = [K' : \mathbb{Q}]$, hence $|H| = |H'|$.

Now, we will show that the multiplicity of the eigenvalue 1 in $\widetilde{\rho_K}(g)$ is equal to $g_K(p)$, where $p \in \mathbb{Z}$ is under $\mathfrak{P}$ (in O_K) and $\mathrm{Frob}_{\mathfrak{P}} = g$, and for this we have to consider $\mathrm{Frob}_{\mathfrak{P}}$ as a product of disjoint cycles from its action over the conjugates of α where $K = \mathbb{Q}(\alpha)$. The idea is to prove that the number of cycles is equal to $g_K(p)$.

We know that each prime in N over p is of the form $\sigma(\mathfrak{P})$ with $\sigma \in G$. Let $\mathfrak{p}_\sigma := \sigma(\mathfrak{P}) \cap K$.

$$\begin{aligned}
\mathfrak{p}_\sigma = \mathfrak{p}_{\sigma'} &\iff \sigma(\mathfrak{P}) \text{ is conjugate to } \sigma'(\mathfrak{P}) \text{ over } K \\
&\quad [\text{This is } \sigma(\mathfrak{P}) = \sigma'(\tau(\mathfrak{P})) \text{ for some } \tau \in \mathrm{Gal}(N/K) =: H] \\
&\iff \sigma'\tau\sigma^{-1} \in D_{\mathfrak{P}}(N/\mathbb{Q}) \text{ for some } \tau \in H \\
&\iff \sigma'\tau = (\mathrm{Frob}_{\mathfrak{P}})^m\sigma \text{ for some } m \in \mathbb{Z},\ \tau \in H \\
&\iff \sigma'(\alpha) = (\mathrm{Frob}_{\mathfrak{P}})^m(\sigma(\alpha)) \text{ for some } m \in \mathbb{Z} \\
&\quad [\Rightarrow \text{ clear } \Leftarrow \text{ because } \sigma' \in ((\mathrm{Frob}_{\mathfrak{P}})^m\sigma)H] \\
&\iff \sigma'(\alpha) \text{ is in the same orbit of } \sigma(\alpha) \text{ with the action of } \langle \mathrm{Frob}_{\mathfrak{P}} \rangle \\
&\iff \sigma'(\alpha) \text{ and } \sigma(\alpha) \text{ are in the same cycle of } \mathrm{Frob}_{\mathfrak{P}}\,.
\end{aligned}$$

Now, in $\widetilde{\rho_K}(g)$ the eigenvalue 1 has the same multiplicity of the following matrix

$$A = \left(\begin{array}{c|ccc} C_1 & & & \\ \hline & C_2 & & \\ & & \ddots & \\ & & & C_{g_K(p)} \end{array}\right),$$

where the C_i's are blocks of order f_i (such that $f_1 \leq \cdots \leq f_{g_K(p)}$) the length of the i-sm cycle, and is of the form

$$C_i = \left(\begin{array}{c|c} 0\cdots 0 & 1 \\ \hline I & \begin{array}{c} 0 \\ \vdots \\ 0 \end{array} \end{array}\right),$$

where I is the identity of order $f_i - 1$. Observe that the characteristic polynomial of C_i is $(-1)^{f_i}(\lambda^{f_i} - 1)$. Set $n = \text{Ord}(g)$. Then we get

$$\begin{aligned} \frac{1}{n}\sum_{i=1}^{n} \psi_{\widetilde{\rho_K}}(g^i) &= \frac{1}{n} tr\left(\sum_{i=1}^{n} \widetilde{\rho_K}(g^i)\right) = \frac{1}{n}\sum_{j=1}^{g_K(p)} tr\left(\sum_{i=1}^{n} C_j^i\right) \\ &= \frac{1}{n}\sum_{j=1}^{g_K(p)} \left(\sum_{i=1}^{n} tr\left(C_j^i\right)\right), \end{aligned}$$

To compute the sum inside the brackets, we use the fact that

$$tr(C_j^i) = \begin{cases} \text{Ord}(C_j) & \text{if} \quad \text{Ord}(C_j) \mid i \\ \\ 0 & \text{otherwise} \end{cases}$$

So, this sum is equal to n. Hence $\frac{1}{n}\sum_{i=1}^{n} \psi_{\widetilde{\rho_K}}(g^i) = g_K(p)$. Then we have

$$\sum_{i=1}^{n} \left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(g^i) = \sum_{i=1}^{n} \left(\psi_{\widetilde{\rho_K}}(g^i) - \psi_{\widetilde{\rho_{K'}}}(g^i)\right) = 0.$$

We claim that $\left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(g) = 0$ for all $g \in G$.

In order to prove the claim we use induction over $\text{Ord}(g)$. The first case, that is, $\langle e \rangle$, is claer since $[K : \mathbb{Q}] = [K' : \mathbb{Q}]$. Now, suppose that $\text{Ord}(g) > 1$. If $\langle x \rangle = \langle g \rangle$, $\left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(g) = \left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(x)$, owing to the fact that $x^m = g$ for some m, we have that if σ is such that $\sigma x \sigma^{-1} \in H$ then $\sigma g \sigma^{-1} = \sigma x^m \sigma^{-1} = (\sigma x \sigma^{-1})^m \in H$, and by symmetry $\sigma x \sigma^{-1} \in H \Leftrightarrow \sigma g \sigma^{-1} \in H$. So

$$\begin{aligned} \psi_{\widetilde{\rho_K}}(g) &= \frac{\left|\left\{\sigma \in G \mid \sigma^{-1} g \sigma \in H\right\}\right|}{|H|} \\ &= \frac{\left|\left\{\sigma \in G \mid \sigma^{-1} x \sigma \in H\right\}\right|}{|H|} = \psi_{\widetilde{\rho_K}}(x), \end{aligned}$$

and in the same way, we have

$$\psi_{\widetilde{\rho_{K'}}}(g) = \psi_{\widetilde{\rho_{K'}}}(x).$$

On the other hand if $\langle x\rangle \subsetneq \langle g\rangle$, using the induction hypothesis $\left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(x) = 0$. So

$$0 = \sum_{i=1}^{n} \left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(g^i) = a \cdot \left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(g),$$

where a is the number of generators of $\langle g\rangle$. Then $\left(\psi_{\widetilde{\rho_K}} - \psi_{\widetilde{\rho_{K'}}}\right)(g) = 0$. □

Bibliography

[CF67] John William Scott Cassels and Albrecht Fröhlich. *Algebraic number theory*. Academic Press, Thompson Book Co., 1967.

[DDSMS03] John D Dixon, Marcus PF Du Sautoy, Avinoam Mann, and Dan Segal. *Analytic pro-p groups*, volume 61. Cambridge University Press, 2003.

[DK12] Johannes Jisse Duistermaat and Johan AC Kolk. *Lie groups*. Springer Science & Business Media, 2012.

[DSP94] Bart De Smit and Robert Perlis. Zeta functions do not determine class numbers. *Bull. Amer. Math. Soc*, 31:213–215, 1994.

[FT93] Albrecht Fröhlich and Martin J Taylor. *Algebraic number theory*, volume 27. Cambridge University Press, 1993.

[Jan96] Gerald J Janusz. *Algebraic number fields*, volume 7. American Mathematical Soc., 1996.

[Jar14] Frazer Jarvis. *Algebraic Number Theory*. Springer Undergraduate Mathematics Series. Springer International Publishing, 1 edition, 2014.

[Kli98] Norbert Klingen. *Arithmetical similarities: Prime decomposition and finite group theory*. Oxford University Press, 1998.

[Kom78] Keiichi Komatsu. On the adele rings and zeta-functions of algebraic number fields. *Kodai Mathematical Journal*, 1(3):394–400, 1978.

[Kom84] Keiichi Komatsu. On adele rings of arithmetically equivalent fields. *Acta Arithmetica*, 43(2):93–95, 1984.

[Mar77] Jacques Martinet. Character theory and artin l-functions. *Algebraic number fields: L-functions and Galois properties*, 9:1–87, 1977.

[Mil97] James S Milne. Class field theory. *lecture notes available at http://www. math. lsa. umich. edu/jmilne*, pages 113–157, 1997.

[MS16] Guillermo Mantilla-Soler. A characterization of arithmetic equivalence via galois representations. preprint on webpage at `http://matematicas.uniandes.edu.co/~gmantilla/`, 2016.

[N$^+$86] Kiyoshi NAGATA et al. Artins l-functions and gassmann equivalence. *Tokyo Journal of Mathematics*, 9(2):357–364, 1986.

[Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[Per77] Robert Perlis. On the equation $\zeta_K(s) = \zeta_{K'}(s)$. *Journal of number theory*, 9(3):342–360, 1977.

[Per78] Robert Perlis. On the class numbers of arithmetically equivalent fields. *Journal of Number Theory*, 10(4):489–509, 1978.

[Per85] Robert Perlis. On the analytic determination of the trace form. *Canad. Math. Bull*, 28(4):422–430, 1985.

[Ser84] Jean-Pierre Serre. L'invariant de witt de la forme tr (x 2). *Commentarii Mathematici Helvetici*, 59(1):651–676, 1984.

[Ser13] Jean-Pierre Serre. *Local fields*, volume 67. Springer Science & Business Media, 2013.

[SP95] Donna Stuart and Robert Perlis. A new characterization of arithmetic equivalence. *Journal of Number Theory*, 53(2):300–308, 1995.

[Sun85] Toshikazu Sunada. Riemannian coverings and isospectral manifolds. *Annals of Mathematics*, 121(1):169–186, 1985.

[Web07] Ben Webster. Small linearly equivalent g-sets and a construction of beaulieu. *Journal of Algebra*, 317(1):306–323, 2007.