ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

L-Series and Arithmetic

a thesis
presented to the Department of Mathematics
in partial fulfillment
of the requirements for the degree
of Master of Science

by
David Ter-Borch Gram Schjoldager Lilienfeldt
(david.lilienfeldt@epfl.ch)

under the supervision of:

Prof. Eva Bayer-Fluckiger
Swiss Federal Institute of Technology, Lausanne

Prof. Benedict Gross
Harvard University, Cambridge

EPFL, Lausanne
Fall Semester 2015-2016

Contents

Acknowledgment

I would like to thank Prof. Eva Bayer-Fluckiger for the opportunity of doing my master's thesis under her supervision. I would also like to thank her for introducing me to number theory and arithmetic geometry through the courses she has taught, the previous semester projects under her supervision and the teaching assistant positions offered to me in her courses. Without her I would not be doing what I do today and I am very grateful for that.

I would like to thank Prof. Benedict Gross for accepting to be my adviser at Harvard University. I thank him for the many hours spent with me, for sharing his knowledge and experience with me and for advising me both mathematically and personally. His guidance was great through every stage of the process, from the choice of the subject to the final reading of the paper. He has truly made this a unique experience that I will never forget.

I would like to thank Chi-Yun Hsu and Zijian Yao of the Department of Mathematics for making me feel at home in the department and for the many hours spent together this semester working on the paper [Gr1] of Benedict Gross. It has been a great teamwork experience and I have greatly profited from their knowledge.

I would like to thank the Department of Mathematics of Harvard University for welcoming me and providing me with an office. I have had the opportunity to attend many interesting seminars and courses during my stay.

Introduction

There are two classes of L-series. One is comprised of L-functions associated to ray-class and Grössen-characters and L-functions associated to Hecke operators. These are defined in the region $\Re s > 1$ as infinite sums, have an expression as an Euler product in the region $\Re s > 1$, can be analytically continued to the whole complex plane as meromorphic funtions and satisfy a functional equation centered at $s = 1/2$. These we will call Hecke type L-functions. The other class contains Artin L-functions and L-functions associated to algebraic varieties over number fields. One first defines local L-factors at all finite places and then takes their product to form an Euler product in some right half-plane. These L-functions encode arithmetic data of number fields and data concerning rational points on algebraic varieties. These we will call Artin type L-functions.

It is often difficult to prove analytic properties from the definition of an L-function of Artin type and thus it becomes an important problem to show that these are of Hecke type. This is the purpose and importance of reciprocity laws. For instance, the quadratic reciprocity law relates the Dedekind zeta-function of a quadratic number field to the Dirichlet L-function of the Legendre symbol. Via a more general reciprocity law, the Dedekind zeta-function of a cyclotomic field is connected to general Dirichlet L-functions. Artin reciprocity in class field theory connects the Artin L-function of a 1-dimensional character to the L-function of a ray-class character, known as a Weber L-function. Finally, modularity relates the L-function of an eliptic curve defined over $\mathbb{Q}$ to the L-function of a Hecke form. Thus every time one equates L-functions, an important reciprocity theorem is involved. These reciprocity laws constitute the bridge between the complex analytic world of Hecke type L-functions with the arithmetic world of Artin type L-functions. The introduction of L-functions in number theory has proven to bring great insight in the arithmetic of numbers.

The first examples of L-series bear the name of Dirichlet L-series and were introduced in 1837 by Pierre Gustave Lejeune Dirichlet in his paper [Dir]. These are functions in the complex variable s defined for $\Re s > 1$ by

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

where χ is a so-called Dirichlet character. In his paper, Dirichlet used these newly introduced functions to prove a purely arithmetic result, the theorem on primes in arithmetic progressions, which says that if a and q are two positive coprime integers, then there are infinitely many primes in the progression $a + \mathbb{Z}q$. Dirichlet proved that his L-functions have an Euler product in the region $\Re s > 1$, that they can be extended to the whole complex plane via analytic continuation and that they admit a functional equation centered at the point $s = 1/2$.

Perhaps more important is the work of Dirichlet and Richard Dedekind on the Dedekind zeta-function of a number field k. This type of function was introduced by Dedekind and is defined for $\Re s > 1$ by

$$\zeta_k(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

where the sum is over all non-zero integral ideals of k. A major theorem in algebraic number theory says that this function has a simple pole at the point $s = 1$ with residue given by the formula

$$\mathrm{Res}_{s=1}(\zeta_k(s)) = \frac{2^{r_1}(2\pi)^{r_2} R_k}{\omega_k |d_k|^{\frac{1}{2}}} h_k$$

where r_1, r_2, ω_k, R_k and h_k are respectively the number of real embeddings of k, the number of pairs of complex embeddings of k, the number of roots of unity in k, the regulator of k and the ideal class number of k. This formula is known as the analytic class number formula. It was proved in the case of a quadratic field by Dirichlet and later extended to arbitrary number fields by Dedekind. It relates important arithmetic invariants of the number field k with a special value of an Artin type L-function. The Dedekind zeta-function was shown by Erich Hecke to admit analytic continuation to the complex plane as a meromorphic function via a functional equation centered at the point $s = 1/2$. The analytic class number formula was then transferred to the point $s = 0$ and gave the neater formula

$$\zeta_k(s) \sim -\frac{h_k R_k}{\omega_k} s^{r_1+r_2-1}, \text{ as } s \to 0.$$

We remark that the order of the Dedekind zeta-function at $s = 0$ is the rank of the unit group of k by Dirichlet's Unit Theorem and that the leading coefficient of the Taylor expansion of ζ_k around $s = 0$ is the product of an algebraic number with the determinant of a square matrix of size $r_1 + r_2 - 1$ whose entries are logarithms of the absolute values of a system of fundamental units of k.

Emil Artin introduced Artin L-functions in his 1923 paper [Ar1]. If K/k is a finite Galois extension of number fields with Galois group G, then to a character χ of G, Artin associated the L-function denoted by

$$L(s, \chi, K/k).$$

This new class of functions encompasses Dirichlet L-functions and Dedekind zeta-functions. Artin proved his Artin Reciprocity Theorem and hereby completed class field theory. This enabled him to show that Artin L-functions of 1-dimensional characters are Weber L-functions which are of Hecke type. Based on this observation and on a result he proved in representaton theory called Artin's Induction Theorem, he was led to conjecture that his L-functions admitted an analytic continuation to the whole complex plane as meromorphic functions and holomorphic functions in the case of a non-trivial character. This is today known as Artin's Conjecture and remains unproven. However, in

1947 Richard Brauer proved a stronger version of Artin's theorem, now called Brauer's Induction Theorem, which made it possible to show that Artin L-functions admit an analytic continuation to the complex plane as meromorphic functions via a functional equation centered at the point $s = 1/2$. Artin proved the following formula

$$\zeta_K(s) = \prod_{\chi} L(s, \chi, K/k)^{\chi(1)}$$

where the product is over all irreducible character of the Galois group G.

In the beginning of the 1970's it occurred to Harold Stark in view of the above decomposition that there might exist and analogue of the analytic class number formula for Artin L-functions. More precisely, one should be able to obtain a formula for the leading coefficient of the Taylor expansion of Artin L-functions around $s = 0$ in the form of an algebraic number times the determinant of a square matrix of size the rank of the Artin L-function at $s = 0$. Having computed this rank and defined an analogue of the regulator of a number field called the Stark regulator, he verified his ideas in a large number of specific cases which let him to conjecture in his series of papers [StI], [StII], [StIII] and [StIV] what became known as Stark's Conjecture. John Tate expanded the ideas of Stark and gave the conjecture its modern formulation in his book [Ta1]. In the rank one abelian case, Stark was led to further refine his conjecture. This refined conjecture, known as the abelian Stark conjecture, relates the values of the derivative of Artin L-function of 1-dimensional characters at $s = 0$ to the logarithm of the absolute value of a special type of unit, known as a Stark unit. Since by Artin Reciprocity these specific Artin L-functions are actually ray-class character L-functions, this refined conjecture has a connection to Hilbert's Twelfth Problem. The conjecture has only been proved in the cases where the class field theory of k is known and this might suggest that a solution to Hilbert's problem is needed in order to prove Stark's conjecture. The original Stark's Conjecture is still largely unproven except for specific cases but there is a large amount of computational evidence suggesting its truth. There is however no clear strategy of proof today.

In the theory of arithmetic geometry, Louis Mordell proved in his 1922 paper [Mor] what is known as Mordell's Theorem. It says that the group of rational points over $\mathbb{Q}$ of an elliptic curve $E/\mathbb{Q}$ is finitely generated. André Weil extended this result to the case of an arbitrary number field k in [We2] and this is known as the Mordell-Weil Theorem.

A rather naive idea was that one might expect a larger number of rational points to yield a larger number of points on reductions modulo finite places. In this case, if $L(E/k, s)$ denotes the Hasse-Weil L-function of the elliptic curve E/k and S is the set of infinite places and finite places of bad reduction, then the partial product

$$L_S(E/k, 1)" = " \prod_{v \notin S} \frac{\#\mathbb{F}_v}{\#\tilde{E}_v(\mathbb{F}_v)}$$

would tend to be relatively small. Supported by numerical evidence assembled by Peter Swinnerton-Dyer in the early 1960's, Bryan Birch and Swinnerton-Dyer formulated in their 1965 paper [BSD] what became known as the Birch and Swinnerton-Dyer Conjecture. It says the following: if E/k is an elliptic curve defined over a number field and n denotes the rank of the Mordell-Weil group $E(k)$, then the Hasse-Weil L-function $L(E/k, s)$ has a meromorphic continuation to a neighborhood of the point $s = 1$ and

$$L(E/k, s) \sim P(E/k)R(E/k)|Ш(k, E)|s^n, \text{ as } s \to 1$$

where $P(E/k), R(E/k)$ and $Ш(k, E)$ are respectively the global period, the regulator and the Tate-Shafarevitch group of E/k. This formula is analogous to Dirichlet's class number formula for number fields and again relates important arithmetic invariants of the elliptic curve to the special value of an L-function of Artin type. Note that due to the Modularity Theorem, it is known that L-functions of elliptic curves defined over $\mathbb{Q}$ admit an analytic continuation to the whole complex plane and satisfy a functional equation centered at $s = 1$.

The conjecture of Birch and Swinnerton-Dyer is one of the Millenium Prize Problems and is still largely unsolved. Using ideas analogous to the ones of Stark, Benedict Gross was led in [Gr1] to propose a refinement of the conjecture of Birch and Swinnerton Dyer using Heegner points on the modular curve $X_0(N)$. Extending these methods together with Don Zagier, they proved in 1986 the Gross-Zagier Formula in [GZ] which implies that if a modular elliptic curve defined over $\mathbb{Q}$ has a first order zero at $s = 1$, then it has a rational point of infinite order. Note that the modularity assumption (necessary to assume at the times) is needed in order to connect the worlds of Heegner points $X_0(N)$ and the elliptic curve. Further progress has been made in the rank 0 and rank 1 case but virtually nothing is known about the higher rank cases.

In chapter 1 we prove Dirichlet's analytic class number formula. It will involve defining all the necessary ingredients in the formula and we will prove the finiteness of the ideal class number as well as Dirichlet's unit theorem. We mostly follow the exposition of Pierre Samuel in [Sam]. For the proof of the analytic class number formula we follow the book of Serge Lang [Lan].

The aim of the next three chapters is to go through the background needed to define Artin L-functions. Chapter 2 is devoted to a rapid exposition of the main results of global class field theory without the proofs. Our reference here is the book of David Cox [Cox]. In chapter 3 we present the theory of finite-dimensional complex representations of finite groups following the book of Jean-Pierre Serre [Se1] on the subject. Chapter 4 is concerned with finite-dimensional representations of finite groups over non-algebraically closed fields. We also follow [Se1] and use the book of Joseph Rotman [Ro1] as a reference for the theory of non-commutative algebra.

In chapter 5 we introduce L-functions and in particular Artin L-functions and study the properties of these. We follow [Lan] for most of the proofs. We also profited from [Cog].

In chapter 6 we introduce Stark's Conjecture. After explaining the motivation behind the conjecture and defining the necessary objects, we state the main conjecture and show how it is independent of the various choices made in the statement. We then analyze special cases of the conjecture. We prove it in the case of rank 0 and analyze in depth the case of rank one. Here we introduce Stark units and study the abelian rank one Stark conjecture. We end this chapter with an example with cyclotomic units. Our main reference here is the book of Tate [Ta1]. We have also profited from the expositions [Das] and [Mos].

In chapter 7 we state the Birch and Swinnerton-Dyer Conjecture. We give an introduction to elliptic curves and sketch the proof of the Mordell-Weil Theorem, defining the regulator of an elliptic curve as well as the Tate-Shafarevitch group as we go along. We then introduce the L-function associated to an elliptic curve and show how its construction relates to the one of Artin L-functions. Finally, we define the global period of an elliptic curve and state the conjecture. We follow the paper of Gross [Gr2] and supplement it with results concerning the theory of elliptic curves using the book of Joseph Silverman [Sil].

We have attempted to keep this thesis as self-contained as possible. All theorems that we do not prove are given clear references. The only needed prerequisites for reading this paper is a course in basic algebraic number theory. The bibliography lists all references cited in the text and also references that the author has been reading throughout the course of the project.

Basic Notations

Let k be a number field, that is, a finite extension of $\mathbb{Q}$. We shall write d_k for the absolute discriminant of k. Let $\mathcal{O}_k$ be the ring of integers of k which is a Dedekind domain. We will denote by U_k the multiplicative group of invertible elements $\mathcal{O}_k^*$. Let M_k be the set of absolute values on k modulo equivalence. Elements of M_k will be denoted by v and referred to as places of k.

Let M_k^∞ denote the set of infinite places, that is, the places corresponding to archimedean absolute values. Let r_1 be the number of real infinite places and let r_2 be the number of pairs of conjugate complex infinite places. Then $|M_k^\infty| = r_1 + r_2$ and $[k : \mathbb{Q}] = r_1 + 2r_2$. We define $k_\mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Let M_k^0 be the set of finite places, that is, the places corresponding to the non-archimedean absolute values. This set is in bijection with the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$. We will indifferently use the notation v or $\mathfrak{p}$ to designate a finite place of k. For a finite place v, let k_v denote the completion of k with respect to the metric defined by v. One can check that this is a topological field. Let $\mathcal{O}_v$ be the closed unit ball $\{x \in k \mid v(x) \geq 0\}$ in k_v with respect to this metric, also called the ring of v-integers. This is a discrete valuation ring with maximal ideal the open unit ball $\mathfrak{m}_v$. We will use π_v to denote a uniformizer for v. It is unique up to multiplication by a unit of $\mathcal{O}_v$. With this notation we have $\mathfrak{m}_v = \pi_v \mathcal{O}_v$. We denote by $\mathbb{F}_v$ the residue field $k_v/\mathfrak{m}_v = \mathcal{O}_k/\mathfrak{p}$ which is a finite field of order $N(\mathfrak{p})$ where N denotes the ideal norm of k. We will often write $q_v = |\mathbb{F}_v|$.

When referring to a place v of k, we are referring to an equivalence class of absolute values. We will always have in mind a preferred absolute values and we make the following normalization:

- If v is a real archimedean place, corresponding to an embedding $\sigma : k \hookrightarrow \mathbb{R}$, then we set $|x|_v = |\sigma(x)|$ where the latter is the standard absolute value on $\mathbb{R}$.
- If v is a complex archimedean place, corresponding to an embedding $\sigma : k \hookrightarrow \mathbb{C}$, then we set $|x|_v = \sigma(x)\bar{\sigma}(x)$.
- If v is a finite place, then we set $|\pi_v|_v = q_v^{-1}$.

With these normalizations, we have the product formula

$$\prod_v |\alpha|_v = 1, \qquad \text{for all } \alpha \in k^*. \tag{0.0.0.1}$$

See ([Lil], App. C) for a proof of this result.

Let v be a finite place of k. Then k_v is complete with finite residue field, hence locally compact and the ring of v-integers $\mathcal{O}_v$ is compact. Moreover, k_v

is also Hausdorff and second countable. There exists therefore a unique (up to normalization) Haar measure μ_v on k_v^+. The measure μ_v is uniquely defined by the condition $\mu_v(\mathcal{O}_v) = 1$. If $x \in k_v$, then we denote by m_x the multiplication-by-x automorphism of k_v. Then the pull-back $m_x^*(\mu_v) = \mu_v \circ m_x$ is again a Haar measure on k_v^+. It differs by uniqueness from μ_v by a constant and one can show that with the above normalizations we have $m_x^*(\mu_v)/\mu_v = |x|_v$. It follows that $\mu_v(\mathfrak{m}_v^m) = \mu_v(\pi_v^m \mathcal{O}_v) = q_v^{-m}$.

Let S be a finite subset of M_k containing M_k^∞. We let $\mathcal{O}_{k,S}$ denote the ring of S-integers of k, that is,

$$\mathcal{O}_{k,S} = \{x \in k \mid v(x) \geq 0, \text{ for all } v \notin S\} = \bigcap_{v \notin S} \mathcal{O}_v.$$

This is a Dedekind domain whose prime ideals are in bijection with the prime ideals of $\mathcal{O}_k$ that do not belong to S. This type of ring generalizes the ring of integers in the sense that $\mathcal{O}_k = \mathcal{O}_{k,M_k^\infty}$. We shall use $U_{k,S}$ to denote the multiplicative group $\mathcal{O}_{k,S}^*$.

Let $I_{k,S}$ denote the group of fractional ideals associated to $\mathcal{O}_{k,S}$, that is, the group of finitely generated sub-$\mathcal{O}_{k,S}$-modules of k. It is isomorphic to the free abelian group on the prime ideals of $\mathcal{O}_{k,S}$. Let $P_{k,S}$ denote the subgroup of principal fractional ideals. The quotient group $\mathrm{Cl}(\mathcal{O}_{k,S}) = I_{k,S}/P_{k,S}$ is called the S-ideal class group of k. As we shall see, this groups is finite of cardinality $h_{k,S}$ called the S-ideal class number.

Let M be a $\mathbb{Z}$-module and let E be a field of characteristic zero. We shall write EM for the tensor product $E \otimes_{\mathbb{Z}} M$. If $f : M \longrightarrow N$ is a homomorphism, then we shall again denote by f the homomorphism of vector spaces $1 \otimes f : EM \longrightarrow EN$. When tensoring over a ring R other than $\mathbb{Z}$, we will indicate this with the notation $\otimes_R$.

Chapter 1

The Analytic Class Number Formula

We present and prove three classical results of algebraic number theory, namely the finiteness of the ideal class group, Dirichlet's unit theorem and the analytic class number formula. We will employ only elementary methods using euclidean lattice theory. Our main references in this chapter are [Sam] and [Lan].

1.1 Euclidean Lattices

Let $n \geq 1$ be an integer. We review some results concerning lattices in the euclidean space $\mathbb{R}^n$ with the standard euclidean topology. A discrete subset X of $\mathbb{R}^n$ is a subset for which the induced subset topology is the discrete topology. That is, for every $x \in X$, there exists an open subset U of $\mathbb{R}^n$ such that $X \cap U = \{x\}$. Alternatively, one could define X to be discrete if and only if for any compact subset $K \subset \mathbb{R}^n$ the intersection $X \cap K$ is finite. In fact, if X is discrete and K is compact, then $X \cap K$ is both discrete and compact. Consider the open covering $X \cap K = \bigcup_{x \in X \cap K} \{x\}$. By compactness it must have a finite open subcover, whence $X \cap K$ is finite. Conversely, suppose that $X \cap K$ is finite whenever K is compact. For every integer $m \geq 1$, let B_m denote the closed ball centered at 0 with radius m. We have $X = \bigcup_{m \geq 1} X \cap B_m$ and each $X \cap B_m$ is finite. Thus X is at most countable infinite and thus necessarily discrete.

The following result concerns discrete subgroups of $\mathbb{R}^n$.

Proposition 1. *If G is a discrete subgroup of $\mathbb{R}^n$, then G is a free $\mathbb{Z}$-module generated by $r \leq n$ elements that are linearly independent over $\mathbb{R}$.*

Proof. Let $e_1, \ldots, e_r$ be elements in G that are linearly independent over $\mathbb{R}$ and suppose that r is maximal with this property. Evidently we have $r \leq n$. Consider now the compact subset of $\mathbb{R}^n$ defined by $P = \{\sum_{i=1}^r \alpha_i e_i \,|\, \alpha_i \in [0, 1]\}$. Let x be an element of G. By maximality of r, there exist real constants λ_i for $i = 1, \ldots, r$ such that $x = \sum_{i=1}^r \lambda_i e_i$. For every integer $m \geq 1$, consider $x_m = mx - \sum_{i=1}^r [m\lambda_i] e_i = \sum_{i=1}^r \{m\lambda_i\} e_i$ where the brackets denote the integer part and the braces denote the fractional part. We have $x_m \in P \cap G$ for all m. Since $x = x_1 + \sum_{i=1}^r [\lambda_i] e_i$ and x is an arbitrary element of G, we see that G is generated as a group by the intersection $P \cap G$. This intersection is finite by discreteness of G and compactness of P so we have shown that G is finitely generated as a group.

On one hand the intersection $P \cap G$ is finite and on the other hand we have $x_m \in P \cap G$ for all $m \geq 1$. Therefore, there exist at least two integers j and k such that $x_j = x_k$. This implies that $\sum_{i=1}^{r}(\{j\lambda_i\} - \{k\lambda_i\})e_i = 0$ and by linear independence of the e_i we obtain $\{j\lambda_i\} = \{k\lambda_i\}$ for all i. In other terms, we have $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$ and this proves that λ_i is rational for all i. Consequently, every x_m is a rational combination of the e_i. We conclude that G is generated by finitely many elements which are all rational combinations of the e_i. Let d be the product of all the denominators of the all the rational coefficients of all the finitely many generators of G. Then dG is a sub-$\mathbb{Z}$-module of the free module $\bigoplus_{i=1}^{r} \mathbb{Z}e_i$. It follows that dG is free of rank $q \leq r$ (see [Sam], § 1.5 Theorem 1). But dG is isomorphic as a group to G and the latter contains $\bigoplus_{i=1}^{r} \mathbb{Z}e_i$ so that $s = r$. There exist non-zero integers a_i such that the $a_i e_i$ form a basis of dG (see [Sam], § 1.5 Theorem 1). Then $a_i e_i/d$ is a basis of G of size r which is linearly independent over $\mathbb{R}$ by linear independence of the e_i. □

Definition 1. A euclidean lattice Λ is a discrete subgroup of $\mathbb{R}^n$ of rank n which has a basis that is linearly independent over $\mathbb{R}$. In other words, it is a free $\mathbb{Z}$-module such that $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^n$.

Alternatively, one could define a lattice Λ to be a subgroup which is both discrete and cocompact, meaning that $\mathbb{R}^n/\Lambda$ is compact in the quotient topology. In fact, suppose that Λ is a lattice and let $e = (e_1, \ldots, e_n)$ be a basis of $\mathbb{R}^n$ such that $\Lambda = \bigoplus_{i=1}^{n} \mathbb{Z}e_i$. Define

$$P_e = \left\{ \sum_{i=1}^{n} \alpha_i e_i \mid \alpha_i \in [0, 1[\right\}.$$

This is called the fundamental domain of Λ with respect to the basis e. It has the property that the quotient map $P_e \longrightarrow \mathbb{R}^n/\Lambda$ is surjective. Indeed, if $x \in \mathbb{R}^n$, then we may write $x = \sum_{i=1}^{n} \lambda_i e_i$ uniquely with $\lambda_i \in \mathbb{R}$. Let $\lambda = \sum_{i=1}^{n}[\lambda_i]e_i \in \Lambda$. Then $x - \lambda = \sum_{i=1}^{n}\{\lambda_i\}e_i \in P_e$ so that x and λ are equal in the quotient $\mathbb{R}^n/\Lambda$. In particular, if $\bar{P}_e$ denotes the closure of P_e which is compact, then $\mathbb{R}^n/\Lambda$ is the image of $\bar{P}_e$ under a continuous map so that $\mathbb{R}^n/\Lambda$ is also compact.

Conversely, suppose that $\mathbb{R}^n/\Lambda$ is compact. Since Λ is a discrete subgroup of $\mathbb{R}^n$, by Proposition 1 we know that Λ is a free $\mathbb{Z}$ module of rank $r \leq n$ and that $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^r$. The compactness of $\mathbb{R}^n/\Lambda$ implies that $r = n$ so that Λ is indeed a lattice.

We have seen that the map $P_e \longrightarrow \mathbb{R}^n/\Lambda$ is surjective. We now show that it is also injective. Suppose that $x, y \in P_e$ and that $x - y \in \Lambda$. We may write $x = \sum_{i=1}^{n} \alpha_i e_i$ and $y = \sum_{i=1}^{n} \beta_i e_i$ with $\alpha_i, \beta_i \in [0, 1[$. There exist integers n_i such that $x = y + \sum_{i=1}^{n} n_i e_i$. By linear independence of the e_i, this implies that $\alpha_i = \beta_i + n_i$ which is only possible if $n_i = 0$ for all i. This proves injectivity. We conclude that we have a homeomorphism $P_e \xrightarrow{\sim} \mathbb{R}^n/\Lambda$.

Let μ denote the Lebesgue measure on $\mathbb{R}^n$ normalized so that the unit n-cube spanned by the standard orthonormal basis of $\mathbb{R}^n$ for the euclidean inner product $\langle\cdot,\cdot\rangle$ has measure (or volume) equal to 1. The fundamental domain P_e is the unit n-cube spanned by the basis e and its volume is given by

$$\mu(P_e) = |\det(\langle e_i, e_j\rangle)|^{1/2} = |\det E|$$

where E is the base change matrix from e to the standard orthonormal basis.

Suppose that e' is another basis of Λ and denote by E' the base change matrix from e' to the standard orthonormal basis. The base-change matrix M of Λ from e' to e is given by $M = E^{-1}E'$. It is an invertible matrix of size n with coefficients in $\mathbb{Z}$ since both e and e' are integral bases. Thus the determinant of M is ± 1. We have $\det E' = \det E \det M$ so that $\mu(P_e) = \mu(P_{e'})$. This proves that $\mu(P_e)$ is independent of the choice of basis. We may therefore make the following definition:

Definition 2. Let Λ be a lattice in $\mathbb{R}^n$. We define the covolume of Λ to be the real number

$$v(\Lambda) = \mu(P_e) = |\det(\langle e_i, e_j\rangle)|^{1/2}$$

where e denotes any choice of basis of Λ that is also a basis for $\mathbb{R}^n$.

The bijection $P_e \xrightarrow{\sim} \mathbb{R}^n/\Lambda$ tells us that $\mathbb{R}^n = \bigcup_{x\in\Lambda}(x+P_e)$ where the union is disjoint. The next result shows that P_e is the "largest" subset of $\mathbb{R}^n$ with this property of mutual disjointness.

Proposition 2. *Let Λ be a lattice in $\mathbb{R}^n$ and let M be a Lebesgue-measurable subset of $\mathbb{R}^n$ with the property that the sets $x + M$ are mutually disjoint as x ranges over Λ. Then $\mu(M) \leq v(\Lambda)$.*

Proof. Let P_e be the fundamental domain associated to a basis e of Λ which is also a basis for $\mathbb{R}^n$. Since the sets $x + P_e$ with $x \in \Lambda$ cover $\mathbb{R}^n$, we have

$$\mu(M) = \mu\left(\bigcup_{x\in\Lambda} M \cap (x + P_e)\right).$$

Since all these sets are mutually disjoint we obtain

$$\mu(M) = \sum_{x\in\Lambda}\mu(M\cap(x+P_e)) = \sum_{x\in\Lambda}\mu((M-x)\cap P_e) = \sum_{x\in\Lambda}\mu((M+x)\cap P_e).$$

All these set are mutually disjoint by assumption so that the latter is equal to $\mu(\cup_{x\in P_e}(M+x)\cap P_e)$ which in turn is less than $\mu(P_e) = v(L)$. □

The negation of this proposition will be useful to us and we therefore record it as a corollary:

Corollary 1. *Let Λ be a lattice in $\mathbb{R}^n$ and let M be a Lebesgue-measurable subset of $\mathbb{R}^n$ such that $\mu(M) > v(\Lambda)$. Then there exist two distinct elements $x, y \in \Lambda$ such that $(x + M) \cap (y + M) \neq \emptyset$. In particular, there exist distinct elements m and m' of M such that $m - m' \in \Lambda$.*

Proof. Since $(x + M) \cap (y + M) \neq \emptyset$ there exist $m, m' \in M$ such that $x + m = y + m'$. This implies that $m' - m = x - y \in \Lambda \setminus \{0\}$. □

This allows us to prove the following:

Proposition 3. *Let Λ be a lattice in $\mathbb{R}^n$ and let M be a Lebesgue-measurable subset of $\mathbb{R}^n$. Suppose that M is convex and symmetric around the origin. If one of the following conditions hold:*

(i) $\mu(M) > 2^n v(\Lambda)$

(ii) $\mu(M) \geq 2^n v(\Lambda)$ *and M is compact,*

then $M \cap (\Lambda \setminus \{0\})$ is non-empty.

Proof. Proof of (i): set $M' = \frac{1}{2}M$. This is a Lebesgue-measurable set and $\mu(M') = 2^{-n}\mu(M) > v(\Lambda)$ by assumption. By Corollary 1, there exist $m, m' \in M'$ distinct elements such that $m - m' \in \Lambda$. We may write this difference as $m - m' = ((2m) + (-2m'))/2$. By symmetry of M, $-2m' \in M$ and by convexity $m - m' \in M$. We conclude that $m - m' \in M \cap (\Lambda \setminus \{0\})$.

Proof of (ii): let $\epsilon > 0$ be an arbitrary real number and set $M_\epsilon = (1+\epsilon)M$. This is a Lebesgue-measurable set. It is convex, symmetric around the origin and even compact since this is true for M. Moreover, we have $\mu(M_\epsilon) = (1+\epsilon)^n\mu(M) > \mu(M) \geq 2^n v(\Lambda)$. By (i), we see that $M_\epsilon \cap (\Lambda \setminus \{0\})$ is non-empty. This holds true for all $\epsilon > 0$. In particular, we have a nested sequence

$$(1+1)M \cap \Lambda \setminus \{0\} \supset \left(1+\frac{1}{2}\right) M \cap \Lambda \setminus \{0\} \ldots \supset \left(1+\frac{1}{m}\right) M \cap \Lambda \setminus \{0\} \supset \ldots$$

of non-empty compact (actually finite since discrete and compact) sets. By Cantor's Intersection Theorem (cf. Theorem 1.1.1 below), we have

$$\bigcap_{m\geq 1} \left(1+\frac{1}{m}\right) M \cap \Lambda \setminus \{0\} \neq \emptyset.$$

Thus there exists x such that $x \in \left(1+\frac{1}{m}\right) M \cap \Lambda \setminus \{0\}$ for all $m \geq 0$. In other words, for every m there exists $x_m \in M$ such that $x = (1+1/m)x_m$. By compactness of M, the sequence x_m admits a subsequence that converges to a limit in M. Obviously, x is that limit so that $x \in M$. In conclusion, we have $x \in M \cap \Lambda \setminus \{0\}$. □

Remark 1. We now give a proof of the result on nested sets referred to earlier.

Theorem 1.1.1 (Cantor's Intersection Theorem)**.** *Let X be a compact subset of $\mathbb{R}^n$ and let $(C_m)_{m=1}^\infty$ be a nested sequence*

$$C_1 \supset C_2 \supset \ldots \supset C_m \supset \ldots$$

of non-empty compact subsets of X. Then the intersection $\bigcap_{m\geq 1} C_m$ is non-empty.

Proof. Suppose that $\bigcap_{m\geq 1} C_m = \emptyset$ by contradiction. Let $U_m = X \setminus C_m$ for every m. The U_m are open subsets of X and we have

$$\bigcup_{m\geq 1} U_m = X \setminus \bigcap_{m\geq 1} C_m = X.$$

By compactness of X we can extract a finite subcover $(U_m)_{m=1}^k$. Since the sequence C_m is nested we have $U_m \subset U_{m+1}$ for all m. Thus $X = U_k$ and $C_k = \emptyset$ which is a contradiction. □

1.2 Application to Number Fields

Having introduced euclidean lattices and studied some of their basic properties, we now turn to their application to algebraic number theory. Let thus k be a number field of degree n. Consider the tensor product $\mathbb{R} \otimes_{\mathbb{Q}} k$. This is an $\mathbb{R}$-algebra of dimension n and we have a natural embedding $k \hookrightarrow \mathbb{R} \otimes_{\mathbb{Q}} k$.

Let M be a free sub-$\mathbb{Z}$-module of k. A basis of M is also a $\mathbb{Q}$-basis of k and therefore M naturally sits as a lattice in $\mathbb{R} \otimes_{\mathbb{Q}} k$. In particular, the ring of integers $\mathcal{O}_k$ is a free $\mathbb{Z}$-module of rank n (cf. [Sam] § 2.7, Theorem 1) and therefore $\mathcal{O}_k$ is a lattice in $\mathbb{R} \otimes_{\mathbb{Q}} k$.

Moreover, let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_k$. In other words, $\mathfrak{a}$ is a sub-$\mathbb{Z}$-module of the free $\mathbb{Z}$-module $\mathcal{O}_k$. It is therefore free of rank $q \leq n$ (cf. [Sam] § 1.5, Theorem 1 (a)). Let $x \in \mathfrak{a}$ be a non-zero element. Then $\mathfrak{a}$ contains the ideal $x\mathcal{O}_k$ which is isomorphic as a $\mathbb{Z}$-module to $\mathcal{O}_k$. This implies that the rank of $\mathfrak{a}$ is greater or equal to n. We conclude that $\mathfrak{a}$ is free of rank n and therefore is a lattice in $\mathbb{R} \otimes_{\mathbb{Q}} k$.

Finally, let $\mathfrak{a}$ be a non-zero fractional ideal of k. By definition, there exists an element $\alpha \in \mathcal{O}_k$ such that $\alpha\mathfrak{a}$ is an ideal of $\mathcal{O}_k$. By the above, $\alpha\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n. Since $\mathfrak{a}$ and $\alpha\mathfrak{a}$ are isomorphic as $\mathbb{Z}$-modules this implies that $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n and in particular it is a lattice in $\mathbb{R} \otimes_{\mathbb{Q}} k$.

We have just seen that all non-zero fractional ideals of k are lattices in $\mathbb{R} \otimes_{\mathbb{Q}} k$, meaning that they are free of rank n as $\mathbb{Z}$-modules and contain a basis of $\mathbb{R} \otimes_{\mathbb{Q}} k$. We are interested in computing the covolumes of these lattices and in order to do so we need some euclidean structure on $\mathbb{R} \otimes_{\mathbb{Q}} k$. We choose real and complex embeddings of k to make an isomorphism of $\mathbb{R} \otimes_{\mathbb{Q}} k$ with products of $\mathbb{R}$ and $\mathbb{C}$. More precisely, let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings $k \hookrightarrow \mathbb{R}$ corresponding to the real archimedean places of k and fix a choice of complex embedding $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ of k corresponding to the complex archimedean places of k. We have $n = r_1 + 2r_2$ and $|M_k^\infty| = r_1 + r_2$. Additionally, if τ denotes complex conjugation then we set $\tau \circ \sigma_{r_1+i} = \sigma_{r_1+r_2+i}$ for $i = 1, \ldots r_2$. Then $\sigma_1, \ldots, \sigma_n$ are all the distinct $\mathbb{Q}$-homomorphisms of k into an algebraically closed field containing k. Consider the $\mathbb{R}$-algebra $k_{\mathbb{R}} := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of dimension n. This is sometimes referred to as the Minkowski space of k. Define the diagonal embedding

$$\sigma : k \longrightarrow k_{\mathbb{R}}, \qquad x \longmapsto (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)).$$

We extend σ to $\mathbb{R} \otimes_{\mathbb{Q}} k$ by tensoring and denote the resulting map by σ again. This gives an injective homomorphism of $\mathbb{R}$-algebras from $\mathbb{R} \otimes_{\mathbb{Q}} k$ to $k_{\mathbb{R}}$. Since these algebras have the same dimension over $\mathbb{R}$, this map must be an isomorphism. Explicitly, if $x_1, \ldots, x_n$ is a basis of k over $\mathbb{Q}$ then $1 \otimes x_1, \ldots, 1 \otimes x_n$ is a basis for $\mathbb{R} \otimes_{\mathbb{Q}} k$ over $\mathbb{R}$ and for $\lambda_i \in \mathbb{R}$ we have

$$\sigma\left(\sum_{i=1}^{n} \lambda_i (1 \otimes x_i)\right) = \sum_{i=1}^{n} \lambda_i \sigma(x_i) = \left(\sum_{i=1}^{n} \lambda_i \sigma_1(x_i), \ldots, \sum_{i=1}^{n} \lambda_i \sigma_{r_1+r_2}(x_i)\right) \in k_{\mathbb{R}}.$$

In $k_{\mathbb{R}}$ we have a euclidean structure given by an inner product and an orthonormal basis for this structure is given by choosing as basis for $\mathbb{C}$ over $\mathbb{R}$ the basis $\{(1,0),(0,i)\}$. We sum this up in the following diagram:

$$k \hookrightarrow \mathbb{R} \otimes_{\mathbb{Q}} k \overset{\sigma}{\cong} k_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times (\mathbb{R} \oplus i\mathbb{R})^{r_2} \qquad (1.2.0.1)$$

where all isomorphisms are ones of $\mathbb{R}$-algebras. Thus σ provides a basis for $\mathbb{R} \otimes_{\mathbb{Q}} k$ and an inner product with respect to which this basis is orthonormal. The lattice computations in $\mathbb{R} \otimes_{\mathbb{Q}} k$ will be performed in this basis.

A typical element of $k_{\mathbb{R}}$ will be denoted $x = (x_1, \dots, x_{r_1}; x_{r_1+1}, \dots, x_{r_1+r_2})$ where x_j for $j = 1, \dots, r_1$ is real and x_j for $j = r_1 + 1, \dots, r_1 + r_2$ is complex. In the latter case we write $x_j = y_j + iz_j$. When writing an element in the above orthonormal basis we shall use vector notation so that

$$x = (x_1, \dots, x_{r_1}; y_{r_1+1}, z_{r_1+1}, \dots, y_{r_1+r_2}, z_{r_1+r_2}).$$

An element x of k is expressed in the orthonormal basis for $\mathbb{R} \otimes_{\mathbb{Q}} k$ as follows:

$$x = (\sigma_1(x), \dots, \sigma_{r_1}(x); \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \dots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)).$$

Remark 2. The map σ is not conceptually important. It is merely there to allow for a nice choice of basis for $\mathbb{R} \otimes_{\mathbb{Q}} k$. We equip $\mathbb{R} \otimes_{\mathbb{Q}} k$ with this basis and make no further reference to $k_{\mathbb{R}}$ or σ. When we write

$$x = (x_1, \dots, x_{r_1}; x_{r_1+1}, \dots, x_{r_1+r_2}) \in \mathbb{R} \otimes_{\mathbb{Q}} k$$

this is simply the expression of x in $k_{\mathbb{R}}$ via σ. We identify $\mathbb{R} \otimes_{\mathbb{Q}} k$ with $k_{\mathbb{R}}$ and we identify k with its image in $\mathbb{R} \otimes_{\mathbb{Q}} k$ which is now also $\sigma(k)$ in $k_{\mathbb{R}}$.

We extend the map $N_{k/\mathbb{Q}} : k \longrightarrow \mathbb{Q}$ to a map $N : \mathbb{R} \otimes_{\mathbb{Q}} k \longrightarrow \mathbb{R}$ by defining $N(x) = \det m_x$ where $m_x : \mathbb{R} \otimes_{\mathbb{Q}} k \longrightarrow \mathbb{R} \otimes_{\mathbb{Q}} k$ is multiplication by the element x. In the orthonormal basis m_x is given in matrix form by

$$\begin{pmatrix}
x_1 & & & & & & & \\
& \ddots & & & & & & \\
& & x_{r_1} & & & & & \\
& & & y_{r_1+1} & -z_{r_1+1} & & & \\
& & & z_{r_1+1} & y_{r_1+1} & & & \\
& & & & & \ddots & & \\
& & & & & & y_{r_1+r_2} & -z_{r_1+r_2} \\
& & & & & & z_{r_1+r_2} & y_{r_1+r_2}
\end{pmatrix}$$

so that

$$\begin{aligned}
N(x) &= x_1 \dots x_{r_1} (y_{r_1+1}^2 + z_{r_1+1}^2) \dots (y_{r_1+r_2}^2 + z_{r_1+r_2}^2) \\
&= x_1 \dots x_{r_1} |x_{r_1+1}|^2 \dots |x_{r_1+r_2}|^2.
\end{aligned}$$

Remark that if $x \in k$, then $N(x) = N_{k/\mathbb{Q}}(x)$ and therefore N does extend $N_{k/\mathbb{Q}}$ as claimed.

Proposition 4. *Let M be a free sub-$\mathbb{Z}$-module of k of rank n and let $x_1, \dots, x_n$ be a basis of M. The covolume of M as a lattice in $\mathbb{R} \otimes_{\mathbb{Q}} k$ is given by*

$$v(M) = 2^{-r_2} \left| \det_{1 \leq i,j \leq n} (\sigma_i(x_j)) \right|.$$

Proof. The covolume of M in $\mathbb{R} \otimes_{\mathbb{Q}} k$ is the absolute value of the determinant of the matrix, say D, whose columns are given by the vectors

$$(\sigma_1(x_i), \dots, \sigma_{r_1}(x_i); \Re\sigma_{r_1+1}(x_i), \Im\sigma_{r_1+1}(x_i), \dots, \Re\sigma_{r_1+r_2}(x_i), \Im\sigma_{r_1+r_2}(x_i)).$$

Using the formulas

$$\Re\sigma_{r_1+j}(x_i) = \frac{1}{2}(\sigma_{r_1+j}(x_i) + \sigma_{r_1+r_2+j}(x_i))$$
$$\Im\sigma_{r_1+j}(x_i) = \frac{1}{2i}(\sigma_{r_1+j}(x_i) - \sigma_{r_1+r_2+j}(x_i)),$$

we see that the determinant of D equals $(2i)^{-r_2}\det(D')$ where D' is the same matrix as D but every r_1+2j^{th} line, for $j = 1,\dots,r_2$, multiplied by $2i$. By adding every r_1+2j^{th} line to the r_1+2j-1^{th} line and then subtracting the r_1+2j-1^{th} line from the r_1+2j^{th} line we get $|\det(D')| = |\det(\sigma_i(x_j))|$. We have thus found that $|\det(D)| = 2^{-r_2}|\det(\sigma_i(x_j))|$. □

Corollary 2. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_k$. Then the covolumes of $\mathcal{O}_k$ and $\mathfrak{a}$ in $\mathbb{R}\otimes_{\mathbb{Q}} k$ are given by*

$$v(\mathcal{O}_k) = 2^{-r_2}|d_k|^{\frac{1}{2}}, \quad v(\mathfrak{a}) = 2^{-r_2}|d_k|^{\frac{1}{2}}N(\mathfrak{a}).$$

Proof. Let $x_1,\dots,x_n$ be a basis of $\mathcal{O}_k$. Applying Proposition 4 with $M = \mathcal{O}_k$ and using the fact that $d_k = \det(\sigma_i(x_j))^2$ (cf. [Sam] § 2.7, Proposition 3) we obtain the first assertion.

For the second assertion, use the fact that there exists a basis $x_1,\dots,x_n$ of $\mathcal{O}_k$ and non-zero integers $c_1,\dots,c_n$ such that $c_1x_1,\dots,c_nx_n$ is a basis of $\mathfrak{a}$ (cf. [Sam] § 1.5, Theorem 1 (b)). Applying Proposition 4 to $\mathfrak{a}$ we see that

$$v(\mathfrak{a}) = 2^{-r_2}|\det(c_j\sigma_i(x_j))| = 2^{-r_2}|\det(\mathrm{Diag}(c_1,\dots,c_n)\cdot(\sigma_i(x_j)))|.$$

But the determinant of $\mathrm{Diag}(c_1,\dots,c_n)$ is $c_1\dots c_n$. On the other hand, the quotient $\mathcal{O}_k/\mathfrak{a}$ is isomorphic as a $\mathbb{Z}$-module to $\bigoplus_{i=1}^n \mathbb{Z}/c_i\mathbb{Z}$. Thus the product of the c_i is $|\mathcal{O}_k/\mathfrak{a}|$ which by definition is $N(\mathfrak{a})$. Hence $v(\mathfrak{a}) = 2^{-r_2}|d_k|^{\frac{1}{2}}N(\mathfrak{a})$ as desired. □

1.3 Finiteness of the Ideal Class Group

If k is a number field, we denote by I_k its group of fractional ideals and P_k the subgroup of principal fractional ideals. The quotient group $\mathrm{Cl}(\mathcal{O}_k) := I_k/P_k$ is called the ideal class group of k. In this section we prove that this quotient group is finite. Its cardinality, denoted by h_k, is called the ideal class number, hence the name of this section. This finiteness of the ideal class number is due to Dirichlet. We will end this section by showing a similar finiteness result in the case of the ring of S-integers. Everything relies on the following bound due to Minkowski.

Proposition 5. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_k$. Then $\mathfrak{a}$ contains a non-zero element x for which*

$$|N_{k/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d_k|^{\frac{1}{2}}N(\mathfrak{a}).$$

Proof. For any element x of k we have

$$|N_{k/\mathbb{Q}}(x)| = \prod_{v\in M_k^\infty}|x|_v = \prod_{i=1}^{r_1}|\sigma_i(x)|\prod_{j=r_1+1}^{r_2}|\sigma_j(x)|^2.$$

Using the geometrical-arithmetic inequality (apply Jensen's inequality to the convex function $-\log$) yields the inequality

$$|N_{k/\mathbb{Q}}(x)| \leq \frac{1}{n^n}\left(\sum_{i=1}^{r_1}|\sigma_i(x)| + 2\sum_{j=r_1+1}^{r_2}|\sigma_j(x)|\right)^n. \tag{1.3.0.1}$$

In order to bound $|N_{k/\mathbb{Q}}(x)|$, it is natural to look to bound the quantity

$$\sum_{i=1}^{r_1}|\sigma_i(x)| + 2\sum_{j=r_1+1}^{r_2}|\sigma_j(x)|.$$

Define

$$B_t = \left\{(x_1,\dots,x_{r_1};x_{r_1+1},\dots,x_{r_1+r_2}) \in \mathbb{R}\otimes_{\mathbb{Q}} k \ : \ \sum_{i=1}^{r_1}|x_i| + 2\sum_{j=r_1+1}^{r_2}|x_j| \leq t\right\}$$

where t is a positive real number. Proving the proposition amounts to proving that the intersection $B_t \cap (\mathfrak{a}\setminus\{0\})$ is non-empty for a suitable t.

From the definition of B_t, it is obvious that it is measurable, convex, symmetric around the origin in $\mathbb{R}\otimes_{\mathbb{Q}} k$ and compact. Its volume is given by

$$\mu(B_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}$$

(cf. [Sam], Chapter IV, Appendix).

Choose t_0 such that $\mu(B_{t_0}) = 2^n v(\mathfrak{a})$, that is, take t_0 so that

$$t_0^n = 2^{r_2}\left(\frac{2}{\pi}\right)^{r_2} n!|d_k|^{\frac{1}{2}}N(\mathfrak{a}).$$

We apply Proposition 3, which says that $B_{t_0}\cap(\mathfrak{a}\setminus\{0\})$ is non-empty. Let x be an point in this intersection. By (1.3.0.2), we get that

$$|N_{k/\mathbb{Q}}(x)| \leq \frac{t_0^n}{n^n} = \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d_k|^{\frac{1}{2}}N(\mathfrak{a}).$$

□

Corollary 3. *Every ideal class of k contains an integral ideal $\mathfrak{b}$ such that*

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d_k|^{\frac{1}{2}}.$$

Proof. Let $C \in \mathrm{Cl}(\mathcal{O}_k)$ and let $\mathfrak{a}$ be a non-zero fractional ideal in C. Let $\mathfrak{a}'$ be the inverse of $\mathfrak{a}$. Without loss of generality, we may suppose that $\mathfrak{a}'$ is an integral ideal. It is of course non-zero. By Proposition 5 there exists a non-zero element x of $\mathfrak{a}'$ such that $|N_{k/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d_k|^{\frac{1}{2}}N(\mathfrak{a}')$. Define $\mathfrak{b}' = x\mathfrak{a}$. This is an integral ideal of k since $\mathfrak{a}'\mathfrak{a} = \mathcal{O}_k$ and thus $x\mathfrak{a} \subset \mathcal{O}_k$. Moreover $\mathfrak{b}$ belongs to C and by multiplicativity of the norm, we get

$$N(\mathfrak{b})N(\mathfrak{a}') = N(\mathfrak{b}\mathfrak{a}') = N(x\mathcal{O}_k) = |N_{k/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d_k|^{\frac{1}{2}}N(\mathfrak{a}').$$

Dividing on both sides by $N(\mathfrak{a}')$, which is non-zero, we obtain the desired result.

□

Corollary 4 (Dirichlet)**.** *Let k be a number field. Then the ideal class number h_k is finite.*

Proof. We prove that there are only finitely many ideals of $\mathcal{O}_k$ with a given norm. Let $\mathfrak{a}$ be an ideal with norm equal to the natural number m. By definition, this means that the quotient $\mathcal{O}_k/\mathfrak{a}$ is of order m. The order of an element of a group divides the order of the group. Thus, if x is an element of $\mathcal{O}_k$ then mx must belong to $\mathfrak{a}$. In particular, if we take x to be 1 we get that m belongs to $\mathfrak{a}$. Thus $\mathfrak{a}$ contains the ideal $m\mathcal{O}_k$ or in other words $\mathfrak{a}$ divides $m\mathcal{O}_k$ which has only finitely many divisors. There are therefore only finitely many possibilities for $\mathfrak{a}$. As a consequence, $\mathcal{O}_k$ contains only finitely many ideals whose norm is bounded. In particular, there are only finitely many ideals that satisfy the bound in Corollary 3 and therefore there can only be finitely many ideal classes. □

As announced in the introduction of this section we will now generalize this result. More precisely, let S be a finite subset of M_k containing M_k^∞, let $I_{k,S}$ denote the group of fractional ideals associated to $\mathcal{O}_{k,S}$ and let $P_{k,S}$ denote the subgroup of principal fractional ideals. We will prove that the S-ideal class group $\mathrm{Cl}(\mathcal{O}_{k,S}) = I_{k,S}/P_{k,S}$ is finite. This will be an easy consequence of Corollary 4 once we have the following:

Lemma 1. *Let S be a finite subset of M_k containing M_k^∞. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$ that does not belong to S and define $S' = S \cup \{\mathfrak{p}\}$. If $[\mathfrak{p}]$ denotes the class of $\mathfrak{p}$ in $\mathrm{Cl}(\mathcal{O}_{k,S})$, then we have a short exact sequence of groups*

$$1 \longrightarrow \langle[\mathfrak{p}]\rangle \longrightarrow \mathrm{Cl}(\mathcal{O}_{k,S}) \longrightarrow \mathrm{Cl}(\mathcal{O}_{k,S'}) \longrightarrow 1.$$

Proof. We have a homomorphism from $I_{k,S}$ to $I_{k,S'}$ given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{k,S'}$. We claim that this is a surjective homomorphism. Indeed, if $\mathfrak{a}' \in I_{k,S'}$ then it decomposes uniquely as $\mathfrak{a}' = \prod_{\mathfrak{q}\notin S'} \mathfrak{q}^{v_\mathfrak{q}(\mathfrak{a}')}\mathcal{O}_{k,S'}$ where $v_\mathfrak{q}(\mathfrak{a}')$ is an integer since $\mathcal{O}_{k,S'}$ is a Dedekind domain and its primes ideals are exactly the ones of $\mathcal{O}_k$ that do not belong to S'. Then for any non-negative integer e, $\mathfrak{a}_e := \mathfrak{p}^e\mathcal{O}_{k,S}\prod_{\mathfrak{q}\notin S'} \mathfrak{q}^{v_\mathfrak{q}(\mathfrak{a}')}\mathcal{O}_{k,S}$ is an element of $I_{k,S}$ whose image is $\mathfrak{a}'$. This proves our claim.

Notice that $P_{k,S} \subset \ker(I_{k,S} \twoheadrightarrow I_{k,S'} \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_{k,S'}))$ and thus from the universal property of the quotient we get a surjective homomorphism of groups $\phi : \mathrm{Cl}(\mathcal{O}_{k,S}) \longrightarrow \mathrm{Cl}(\mathcal{O}_{k,S'})$.

It is clear that $\langle[\mathfrak{p}]\rangle$ is contained in the kernel of ϕ. Conversely, let $[\mathfrak{a}]$ be an element of $\ker(\phi)$. Then $\mathfrak{a}\mathcal{O}_{k,S'}$ belongs to $P_{k,S'}$. As a consequence, there exists an element $\beta \in k^*$ such that $\mathfrak{a}\mathcal{O}_{k,S'} = \beta\mathcal{O}_{k,S'}$. It follows that for all $\mathfrak{q} \notin S'$, we have $v_\mathfrak{q}(\mathfrak{a}) = v_\mathfrak{q}(\beta\mathcal{O}_{k,S'}) = v_\mathfrak{q}(\beta\mathcal{O}_{k,S})$. Let $e = v_\mathfrak{p}(\mathfrak{a}) - v_\mathfrak{p}(\beta\mathcal{O}_{k,S})$. Then $\mathfrak{a} = \mathfrak{p}^e\beta\mathcal{O}_{k,S}$ and $[\mathfrak{a}] = [\mathfrak{p}]^e$. This proves that $\ker(\phi) = \langle[\mathfrak{p}]\rangle$. □

Corollary 5. *Let S be a finite subset of M_k containing M_k^∞. Then $h_{k,S} := |\mathrm{Cl}(\mathcal{O}_{k,S})|$ is finite.*

Proof. We prove this by induction on $n = |S\backslash M_k^\infty|$. The case $n = 0$ is Corollary 4. Suppose the result true for all sets S' with $|S' \setminus M_K^\infty| = n - 1$. Let $\mathfrak{p}$ be a finite place in S and define $S' = S \setminus \{\mathfrak{p}\}$. Then $h_{k,S'}$ is finite by induction hypothesis and by Lemma 1, if m denotes the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(\mathcal{O}_{k,S'})$, then $h_{k,S} = h_{k,S'}/m$ and is therefore finite. □

1.4 The Unit Theorem

We give a full proof of Dirichlet's famous unit theorem originally proved in 1846 as well as a proof of its generalization due to Chevalley and Hasse in 1940 and 1980 respectively, namely the S-unit theorem. We end this section by defining the S-regulator of a number field. We begin with some notations.

Let S be a finite subset of M_k containing M_k^∞. Let $Y_{k,S}$ be the free abelian group on S, that is, $Y_{k,S} = \bigoplus_{v\in S} \mathbb{Z}v$. Consider the surjective homomorphism of group

$$\mathrm{aug} : Y_{k,S} \longrightarrow \mathbb{Z}, \qquad \sum_{v\in S} n_v v \longmapsto \sum_{v\in S} n_v$$

called the augmentation map. Define the subgroup

$$X_{k,S} = \left\{ \sum_{v\in S} n_v v \in Y_{k,S} \mid \sum_{v\in S} n_v = 0 \right\}$$

so that we have an exact sequence

$$0 \longrightarrow X_{k,S} \longrightarrow Y_{k,S} \xrightarrow{\mathrm{aug}} \mathbb{Z} \longrightarrow 0.$$

It is not difficult to verify that for any choice of $v_0 \in S$, we have

$$X_{k,S} = \bigoplus_{v\neq v_0} \mathbb{Z}(v - v_0)$$

and thus $X_{k,S}$ is a free abelian group of rank $|S| - 1$. Denote by $\mathbb{R}Y_{k,S}$ and $\mathbb{R}X_{k,S}$ the respective tensor products $\mathbb{R} \otimes_{\mathbb{Z}} Y_{k,S}$ and $\mathbb{R} \otimes_{\mathbb{Z}} X_{k,S}$. We consider the map

$$\lambda_{k,S} : k^* \longrightarrow \mathbb{R}Y_{k,S}, \qquad x \longmapsto \sum_{v\in S} \log |x|_v v.$$

This is a homomorphism of groups. We will be interested in the restriction of this map to the multiplicative group of S-units $\mathcal{O}_{k,S}^*$ that we shall denote by $U_{k,S}$. We claim that the image $\lambda_{k,S}(U_{k,S})$ lies in $\mathbb{R}X_{k,S}$. Indeed, if $u \in U_{k,S}$ then $|u|_v = 1$ for all $v \notin S$ and by the product formula (0.0.0.1) we have

$$1 = \prod_{v\in M_k} |u|_v = \prod_{v\in S} |u|_v.$$

Taking the logarithm, we get $\sum_{v\in S} \log |u|_v = 0$ which proves that $\lambda_{k,S}(U_{k,S}) \subset \mathbb{R}X_{k,S}$. Let $G_{k,S}$ denote the kernel of this map so that we have an exact sequence

$$1 \longrightarrow G_{k,S} \longrightarrow U_{k,S} \longrightarrow \lambda_{k,S}(U_{k,S}) \longrightarrow 0.$$

The S-unit theorem consists of proving on one hand that $G_{k,S} = \mu_k$, that is, the finite cyclic subgroup of $U_{k,S}$ consisting of the roots of unity contained in k and on the other hand that $\lambda_{k,S}(U_{k,S})$ sits as a lattice in the $(|S| - 1)$-dimensional real vector space $\mathbb{R}X_{k,S}$. In particular, $\lambda_{k,S}(U_{k,S})$ is a free group and the above sequence splits and we obtain:

Theorem 1.4.1 (S-unit theorem)**.** *Let k be a number field and let S be a finite subset of M_k containing M_k^∞. Then $U_{k,S} \cong \mu_k \times \mathbb{Z}^{|S|-1}$.*

As with the proof of the finiteness of the S-ideal class group (Corollary 5), we will start by treating the simplest case $S = M_k^\infty$ and then we generalize the result using a suitable lemma.

Set $S = M_k^\infty$. In this case, we drop the subscript S in all of the above defined notations and we have the exact sequence

$$1 \longrightarrow G_k \longrightarrow U_k \longrightarrow \lambda_k(U_k) \longrightarrow 0.$$

Let r_1 and r_2 be the usual numbers attached to k and order the elements of M_k^∞ so that the r_1 first ones correspond to the real places and the r_2 remaining ones correspond to the complex places. This case of the unit theorem is due to Dirichlet:

Theorem 1.4.2 (Dirichlet)**.** *Let k be a number field and let $r = r_1 + r_2 - 1$. Then $U_k \cong \mu_k \times \mathbb{Z}^r$.*

Proof. Identify $\mathbb{R}X_k$ with $\mathbb{R}^r$ by choosing a basis and give it the standard euclidean topology. Let B be a compact subset of $\mathbb{R}X_k$ and consider the set $\lambda_k^{-1}(B) \subset U_k$. Let $u \in \lambda_k^{-1}(B)$. Since B is bounded in $\mathbb{R}^r$, we see that $\log|\sigma_i(u)|$ is bounded for all $i = 1, \ldots, r_1 + r_2$ and thus $|\sigma_i(u)|$ is bounded from above and below. In particular, all elementary symmetric functions in the $\sigma_i(u)$ are bounded in absolute values. In particular, the coefficients of the minimal polynomial of u over $\mathbb{Q}$ are bounded. But u is an algebraic integer, so these coefficients lie in $\mathbb{Z}$. Consequently, there are only finitely many possibilities for the minimal polynomial of u over $\mathbb{Q}$ and thus finitely many possibilities for the value of u. This proves that $\lambda_k^{-1}(B)$ is finite. There are two important consequences to this:

- The group $G_k = \lambda_k^{-1}(\{0\})$ is finite. It is therefore a product of finite cyclic groups $C_{d_1} \times \ldots \times C_{d_m}$ and we may suppose that $d_i | d_{i+1}$ for $i = 1, \ldots, m-1$. As a consequence, we have $y^{d_m} = 1$ for all $y \in G_k$. But there are at most d_m elements in k satisfying this equation. Thus $d_m \geq |G_k| = d_1 \ldots d_m$. This implies that $m = 1$ and thus G_k is cyclic comprised of roots of unity. If ζ denotes a root of unity in k, then $|\sigma_i(\zeta)| = 1$ for all $i = 1, \ldots, r_1 + r_2$ and therefore $\zeta \in G_k$. We have therefore proved that $G_k = \mu_k$ as desired.

- The image $\lambda_k(U_k)$ is a discrete subgroup of $\mathbb{R}X_{k,S}$. In fact, if $B \subset \mathbb{R}X_k$ is compact, then $\lambda_k(U_k) \cap B = \lambda_k(\lambda_k^{-1}(B))$ is finite. By Proposition 1, $\lambda_k(U_k)$ is a free $\mathbb{Z}$-module of rank $s \leq r$.

It remains to be proved that $\lambda_k(U_k)$ contains r linearly independent vectors over $\mathbb{R}$. We will prove that for any non-zero linear form $f : \mathbb{R}X_k \longrightarrow \mathbb{R}$ we have $f(\lambda_k(U_k)) \neq 0$. We claim that this will end the proof. Indeed, pick f_1 to be a non-zero linear form on $\mathbb{R}X_k$. Choose $u_1 \in U_k$ such that $f_1(\lambda_k(u_1)) \neq 0$. Rescaling f_1 if necessary, we may suppose that $f_1(\lambda_k(u_1)) = 1$. Let f_2 be a non-zero linear form such that $f_2(\lambda_k(u_1)) = 0$. This is obviously possible. Choose $u_2 \in U_k$ such that $f_2(\lambda_k(u_2)) \neq 0$ and rescale f_2 so that $f_2(\lambda_k(u_2)) = 1$. At the m-th stage, for $1 \leq m \leq r-1$, we have linear forms f_i and elements $u_i \in U_k$ for every $i \leq m$ such that $f_i(\lambda_k(u_i)) = 1$ and $f_i(\lambda_k(u_j)) = 0$ for all $j < i$. We pick a non-zero linear form f_{m+1} such that $f_{m+1}(\lambda_k(u_i)) = 0$ for all $i \leq m$. This is possible since we impose $m \leq r$ conditions on r variables. Choose $u_{m+1} \in U_k$ such that $f_{m+1}(\lambda_k(u_{m+1})) \neq 0$ and rescale so that $f_{m+1}(\lambda_k(u_{m+1})) = 1$. At the r-th stage of this procedure, we have produces linear forms f_i and elements $u_i \in U_k$ for $i = 1, \ldots, r$ such that

$$f_i(\lambda_k(u_i)) = 1 \qquad f_i(\lambda_k(u_j)) = 0 \text{ for j<i .}$$

Let α_i be real numbers for $i = 1, \ldots, r$ and suppose that $\sum_{i=1}^r \alpha_i \lambda_k(u_i) = 0$. Applying f_r to this relation, we obtain $\alpha_r = 0$ and the remaining equation is $\sum_{i=1}^{r-1} \alpha_i \lambda_k(u_i) = 0$. Applying f_{r-1} to this equation yields $\alpha_{r-1} = 0$. Proceeding like this r times gives $\alpha_i = 0$ for all i. This proves that $\lambda_k(u_1), \ldots, \lambda_k(u_r)$ are linearly independent over $\mathbb{R}$.

It thus remains to prove our claim. Let $f : \mathbb{R}X_k \longrightarrow \mathbb{R}$ be a non-zero linear form. Let v_0 be a complex archimedean place of k. Then a basis for $\mathbb{R}X_k$ as a real vector space is given by $(v - v_0)$ for $v \in S \setminus \{v_0\}$. We order this basis by letting the r_1 first elements correspond to the real places of k and the remaining $r_2 - 1$ elements correspond to the complex places except v_0. We shall write $(x_1, \ldots, x_r)$ for the element $\sum_{v \neq v_0} x_v(v - v_0)$ and we thus explicitly identify $\mathbb{R}X_k$ with $\mathbb{R}^r$. We may write f in the form

$$f(x_1, \ldots, x_r) = c_1 x_1 + \ldots + c_r x_r, \text{ with } c_i \in \mathbb{R}.$$

Let $\gamma = (\gamma_1, \ldots, \gamma_r)$ be an element of $\mathbb{R}^r_{>0}$ and choose $\gamma_{r+1} \in \mathbb{R}_{>0}$ such that

$$\prod_{i=1}^{r_1} \gamma_i \prod_{j=r_1+1}^{r_1+r_2} \gamma_j^2 = \left(\frac{2}{\pi}\right)^{r_2} |d_k|^{\frac{1}{2}} := C.$$

Consider the subset of $\mathbb{R} \otimes_{\mathbb{Q}} k$ defined by

$$B_\gamma = \{(x_1, \ldots, x_{r_1}; x_{r_1+1}, \ldots, x_{r_1+r_2}) \in \mathbb{R} \otimes_{\mathbb{Q}} k \ : \ |x_i| \leq \gamma_i, |x_j| \leq \gamma_{r_1+j}\}.$$

This is a Lebesgue-measurable compact subset which is convex and symmetric around the origin of $\mathbb{R} \otimes_{\mathbb{Q}} k$. Moreover, we have

$$\mu(B_\gamma) = \prod_{i=1}^{r_1} 2\gamma_i \prod_{j=r_1+1}^{r_1+r_2} \pi \gamma_j^2 = 2^{r_1} \pi^{r_2} \left(\frac{2}{\pi}\right)^{r_2} |d_k|^{\frac{1}{2}} = 2^n v(\mathcal{O}_k)$$

where in the last equality we made use of Corollary 2. By Proposition 3 the intersection $B_\gamma \cap (\mathcal{O}_k \setminus \{0\})$ is non-empty. Let a_γ be an element in this intersection. Since a_γ is a non-zero algebraic integer, its norm is a non-zero integer. Consequently, we have

$$1 \leq |N_{k/\mathbb{Q}}(a_\gamma)| = \prod_{v \in M_k^\infty} |a_\gamma|_v \leq \prod_{i=1}^{r_1} \gamma_i \prod_{j=r_1+1}^{r_1+r_2} \gamma_j^2 = C. \qquad (1.4.2.1)$$

For $i = 1, \ldots, r_1 + r_2$ if we let v_i denote the corresponding place of k we have

$$\gamma_i^{\epsilon_i} \geq |a_\gamma|_{v_i} = |N_{k/\mathbb{Q}}(a_\gamma)| \left(\prod_{v \neq v_i} |a_\gamma|_v \right)^{-1} \geq \gamma_i^{\epsilon_i} C^{-1},$$

where ϵ_i is 1 if v_i is real and 2 if v_i is complex. This implies that

$$0 \leq \log \gamma_i^{\epsilon_i} - \log |a_\gamma|_{v_i} \leq \log C.$$

It follows that

$$\left|\sum_{i=1}^{r} c_i \log |a_\gamma|_{v_i} - \sum_{i=1}^{r} c_i \log \gamma_i^{\epsilon_i}\right| \leq \log C \sum_{i=1}^{r} |c_i|.$$

Let $\beta > 0$ be a constant that is larger than the right hand side. For every $m \geq 1$, choose an r-tuple $\gamma(m) = (\gamma_1(m), \ldots, \gamma_r(m))$ of positive real numbers such that $\sum_{i=1}^{r} c_i \log \gamma_i(m)^{\epsilon_i} = 2\beta m$. Let $a_{\gamma(m)}$ be a non-zero element of $B_{\gamma(m)} \cap \mathcal{O}_k$. Then for all $m \geq 1$ we have

$$\left|\sum_{i=1}^{r} c_i \log |a_{\gamma(m)}|_{v_i} - 2\beta m\right| < \beta.$$

As a consequence, we have

$$(2k-1)\beta < \left|\sum_{i=1}^{r} c_i \log |a_{\gamma(m)}|_{v_i}\right| < (2k+1)\beta.$$

We conclude that all the real numbers $\sum_{i=1}^{r} c_i \log |a_{\gamma(m)}|_{v_i}$ are distinct. By (1.4.2.1), we see that $N(a_{\gamma(m)}\mathcal{O}_k) = |N_{k/\mathbb{Q}}(a_{\gamma(m)})|$ is bounded. In the course of proving Corollary 1.4.2, we showed that the number of ideals of $\mathcal{O}_k$ with norm bounded by a given constant is finite. We conclude that there exist at least two distinct integers l and j such that $a_{\gamma(l)}\mathcal{O}_k = a_{\gamma(j)}\mathcal{O}_k$. Hence, there exists a unit $u \in U_k$ such that $a_{\gamma(l)} = u a_{\gamma(j)}$. But then we have

$$f(\lambda_k(u)) = \sum_{i=1}^{r} c_i \log |a_{\gamma(l)}|_{v_i} - \sum_{i=1}^{r} c_i \log |a_{\gamma(j)}|_{v_i} \neq 0.$$

This completes the proof by our above discussion. □

Our goal is now to prove Theorem 1.4.1. This is an easy consequence of Theorem 1.4.2 once we have the following:

Lemma 2. *Let S be finite subset of M_k containing M_K^∞. Let $\mathfrak{p}$ be a prime ideal that does not belong to S. Define $S' = S \cup \{\mathfrak{p}\}$. Then $U_{k,S'} \cong U_{k,S} \times \mathbb{Z}$.*

Proof. Let m be the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(\mathcal{O}_{k,S})$. By definition of m, the ideal $\mathfrak{p}^m\mathcal{O}_{k,S}$ is a principal fractional ideal of the ring of S-integers so there exists an element α of k^* such that $\mathfrak{p}^m\mathcal{O}_{k,S} = \alpha\mathcal{O}_{k,S}$. We will show that α is a unit in $\mathcal{O}_{k,S'}$ and that it generates $U_{k,S'}/U_{k,S}$.

Let u be an S'-unit. We have $v_\mathfrak{p}(\alpha) = m$ and therefore $0 \leq v_\mathfrak{p}(u\alpha^j) \leq m-1$ for a suitable choice of an integer j. Since $v_\mathfrak{q}(u\alpha^j) = 0$ for all $\mathfrak{q} \notin S'$, we have $u\alpha^j\mathcal{O}_{k,S} = \mathfrak{p}^{v_\mathfrak{p}(u\alpha^j)}\mathcal{O}_{k,S}$ so that $[\mathfrak{p}]^{v_\mathfrak{p}(u\alpha^j)} = [1]$ in $\mathrm{Cl}(\mathcal{O}_{k,S})$. This implies that $v_\mathfrak{p}(u\alpha^j)$ is a multiple of m by definition of the order and consequently that $v_\mathfrak{p}(u\alpha^k) = 0$ so that $u\alpha^j$ is an S-unit. Thus $[u] = [\alpha^{-j}]$ in $U_{k,S'}/U_{k,S}$ and the claim is proved. Since $v_\mathfrak{p}(\alpha^j) = jm$ for all integers j it is clear that α^j is an S-unit if and only if $j = 0$. Thus α has infinite order in $U_{k,S'}/U_{k,S}$ and $U_{k,S'}/U_{k,S} \cong \mathbb{Z}$. We have an exact sequence

$$1 \longrightarrow U_{k,S} \longrightarrow U_{k,S'} \longrightarrow \mathbb{Z} \longrightarrow 1.$$

It splits since $\mathbb{Z}$ is free, so that $U_{k,S'} \cong U_{k,S} \times \mathbb{Z}$. □

Proof of Theorem 1.4.1. We will perform a proof by induction on $s = |S \setminus M_k^\infty|$. The case $s = 0$ is Theorem 1.4.2. Suppose the result true for sets S' with $|S' \setminus M_k^\infty| = s - 1$. Let $\mathfrak{p}$ be a finite place of S and define $S' = S \setminus \{\mathfrak{p}\}$. By induction hypothesis we know that $U_{k,S'} \cong \mu_k \times \mathbb{Z}^{|S|-2}$. By Lemma 2, we have

$$U_{k,S} \cong U_{k,S'} \times \mathbb{Z} \cong \mu_k \times \mathbb{Z}^{|S|-1}.$$

□

We know now that $\lambda_{k,S}(U_{k,S})$ sits as a lattice in $\mathbb{R}X_{k,S} \cong \mathbb{R}^{|S|-1}$. The covolume of this lattice is an important invariant of the number field k. We make the following definition:

Definition 3. Let k be a number field and let S be a finite subset of M_k containing M_k^∞. We define the regulator of k associated to S to be

$$R_{k,S} = |S|^{-\frac{1}{2}} v(\lambda_{k,S}(U_{k,S})).$$

Up to a constant, the regulator is the volume of a fundamental domain for the lattice $\lambda_{k,S}(U_{k,S})$ in the vector space $\mathbb{R}X_{k,S}$. One can give the following more explicit and less geometric formula for the regulator:

Proposition 6. *Let k be a number field and let S be finite subset of M_k containing M_k^∞. Let $u_1, \dots, u_{|S|-1}$ be a system of fundamental units of $U_{k,S}$, that is, a basis for the free $\mathbb{Z}$-module $U_{k,S}/\mu_k$. We have the formula*

$$R_{k,S} = \left| \det_{\substack{v \in S \setminus \{v_0\} \\ 1 \le i \le |S|-1}} (\log |u_i|_v) \right|$$

where v_0 is any valuation in S.

Proof. The family $\lambda_{k,S}(u_1), \dots, \lambda_{k,S}(u_{|S|-1})$ is a basis for the lattice $\lambda_{k,S}(U_{k,S})$ and we denote by P the fundamental domain associated to this basis. We know that the volume is independent of the choice of basis. Define

$$u^* = |S|^{-\frac{1}{2}}(1, \dots, 1) = |S|^{-\frac{1}{2}} \sum_{v \in S} v \in \mathbb{R}Y_{k,S}.$$

This vector is orthogonal to $\mathbb{R}X_{k,S} \cong \mathbb{R}^{|S|-1}$ and has length equal to 1. Thus $u^*, \lambda_{k,S}(u_1), \dots, \lambda_{k,S}(u_{|S|-1})$ forms a basis of $\mathbb{R}Y_{k,S} \cong \mathbb{R}^{|S|}$ and the $(|S|-1)$-dimensional volume of P equals the $|S|$-dimensional volume of the fundamental paralleliped in $\mathbb{R}^{|S|}$ constructed on this basis. This volume is equal to the absolute value of the determinant of the $|S| \times |S|$ matrix whose columns consist of the basis vectors. This is equal to $|S|^{-\frac{1}{2}}$ times the absolute value of the determinant of the same matrix but where we have multiplied the first column by $|S|^{\frac{1}{2}}$. Now we add all the rows to the row corresponding to some $v_0 \in S$ which becomes

$$(|S|, \operatorname{aug}(\lambda_{k,S}(u_1)), \dots, \operatorname{aug}(\lambda_{k,S}(u_{|S|-1})) = (|S|, 0, \dots, 0)$$

by definition of $X_{k,S}$. Expanding the determinant with respect to this row we obtain

$$R_{k,S} = \left| \det_{\substack{v \in S \setminus \{v_0\} \\ 1 \le i \le |S|-1}} (\log |u_i|_v) \right|.$$

□

Remark 3. We have the following exact sequence

$$1 \longrightarrow \mu_k \longrightarrow U_{k,S} \longrightarrow \lambda_{k,S}(U_{k,S}) \longrightarrow 0.$$

Tensoring with $\mathbb{C}$ over $\mathbb{Z}$ we get an isomorphism of $\mathbb{C}$-vector spaces

$$\lambda_{k,S} : \mathbb{C}U_{k,S} \xrightarrow{\sim} \mathbb{C}X_{k,S}$$

since μ_k is finite. Actually, this map is $1 \otimes \lambda_{k,S}$ but we shall keep the notation $\lambda_{k,S}$. Let $u_1, \ldots, u_{|S|-1}$ be a choice of basis for $\mathbb{C}U_{k,S}$. For a choice $v_0 \in S$, $(v - v_0)_{v \in S}$ is a basis for $\mathbb{C}X_{k,S}$. By Proposition 6, the regulator $R_{k,S}$ is the absolute value of the determinant of the map $\lambda_{k,S}$ corresponding to these choices of bases. Moreover, this determinant is independent of the choice of v_0.

The following result relates the regulator $R_{k,S}$ with $R_{k,S'}$ for sets S and S' that differ only by one element. It will prove to be useful later on.

Proposition 7. *Let k be a number field and let S be a finite subset of M_k containing M_k^∞. Let $\mathfrak{p}$ be a prime ideal that does not belong to S and define $S' = S \cup \{\mathfrak{p}\}$ and let m be the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(\mathcal{O}_{k,S})$. Then*

$$R_{k,S'} = m \log N(\mathfrak{p}) R_{k,S}.$$

Proof. By definition of m, the ideal $\mathfrak{p}^m\mathcal{O}_{k,S}$ is a principal fractional ideal of the ring of S-integers so there exists an element α of k^* such that $\mathfrak{p}^m\mathcal{O}_{k,S} = \alpha\mathcal{O}_{k,S}$. Let $u_1, \ldots, u_{|S|-1}$ be a system of fundamental units of $U_{k,S}$. In the course of proving Lemma 2, we saw that $u_1, \ldots, u_{|S|-1}, u_{|S|} := \alpha$ is a system of fundamental units of $\mathcal{O}_{k,S'}$. Let $v_0 \in S \cap S'$ and define

$$M_S = (\log |u_i|_v)_{\substack{v \in S \setminus \{v_0\},\\ 1 \le i \le |S|-1}} \qquad M_{S'} = (\log |u_i|_v)_{\substack{v \in S' \setminus \{v_0\}.\\ 1 \le i \le |S|}}$$

Then by Proposition 6 we have $R_{k,S} = |\det M_S|$ and $R_{k,S'} = |\det M_{S'}|$. Since $v_\mathfrak{q}(u_{|S|}) = 0$ for all $\mathfrak{q}$ in S we see that

$$M(S') = \begin{pmatrix} M_S & 0 \\ * & \log |u_{|S|}|_\mathfrak{p} \end{pmatrix}$$

so taking the absolute value of the determinant yields the desired result since $|u_{|S|}|_\mathfrak{p} = N(\mathfrak{p})^{-m}$. □

1.5 The Analytic Class Number Formula

The analytic class number formula is an important formula in the theory of basic algebraic number theory: it constitutes a bridge between the arithmetic of a number field and the analytic theory of a number field. All arithmetic invariants associated to a number field that we have defined so far such as the class number, the regulator and the discriminant are related in this formula to the leading coefficient of the Taylor series at $s = 1$ of a function of one complex variable attached to k called the Dedekind zeta-function of k. This formula means that one can compute for example the class number of k by using the other arithmetic invariants of k and by knowing the zeta-function of k. One can understand the arithmetic of a number field via analytic methods and vice-versa. Our main reference for this section is [BS], Chapter 5, § 1.

1.5.1 Statement of the Theorem

We define the Dedekind zeta-function of k and state the class number formula. We then present the main tool in the proof of the formula. We believe that this motivates the study of the fundamental domain in the next section and clarifies the strategy of the proof.

Definition 4. Let k be a number field. The associated Dedekind zeta-function is the function of one complex variable s which is defined for $\Re s > 1$ by the Dirichlet series

$$\zeta_k(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$$

where the sum runs over all non-zero ideals of $\mathcal{O}_k$. If S is a finite subset of M_k containing M_k^∞, then we define the S-modified Dedekind zeta-function for $\Re s > 1$ by the formula

$$\zeta_{k,S}(s) = \sum_{(\mathfrak{a},S)=1} N(\mathfrak{a})^{-s}$$

where the sum runs over all non-zero ideals of $\mathcal{O}_k$ that are coprime to S.

Remark 4. The infinite sum above is to be understood as follows:

$$\sum_{\mathfrak{a}} := \lim_{m\to\infty} \sum_{\mathfrak{a}:N(\mathfrak{a})\leq m}$$

where for all $m \geq 1$ the sum on the right hand is finite (cf. proof of Corollary 4). Let $N_m := |\{\mathfrak{a} : N(\mathfrak{a}) = m\}|$. Then for $\Re s > 1$ we have

$$\zeta_k(s) = \lim_{m\to\infty} \sum_{\mathfrak{a}:N(\mathfrak{a})\leq m} N(\mathfrak{a})^{-s} = \sum_{i=1}^{\infty} \frac{N_i}{i^s}.$$

Remark 5. Once we prove that $\zeta_k(s)$ converges absolutely for $\Re s > 1$, it will follow that it has an Euler product expression in this region given by

$$\zeta_k(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

where the product runs over all prime ideals of $\mathcal{O}_k$. This is a consequence of the fact that the norm function is completely multiplicative and follows from general theory of Dirichlet series.

We can now formulate the analytic class number formula:

Theorem 1.5.1 (Analytic class number formula)**.** *Let k be a number field of degree n. Denote by ω_k the order of the finite group μ_k. The Dedekind zeta-function $\zeta_k(s)$ converges in the region $\Re s > 1$ and has a simple pole at $s = 1$ with residue given by the formula*

$$\mathrm{Res}_{s=1}(\zeta_k(s)) = \frac{2^{r_1}(2\pi)^{r_2} R_k}{\omega_k |d_k|^{\frac{1}{2}}} h_k.$$

The proof of this theorem relies on the next result. By a cone in $\mathbb{R}^n$ we refer to a subset $X \subset \mathbb{R}^n$ with the property that if $x \in X$ then $\xi x \in X$ for all $\xi > 0$.

Theorem 1.5.2. *Let X be a cone in $\mathbb{R}^n$ and let $F : X \longrightarrow \mathbb{R}_{>0}$ be a function subject to the conditions:*

(i) $F(\xi x) = \xi^n F(x)$ for all $x \in X$ and all $\xi > 0$.

(ii) The set $T = \{x \in X \ : \ F(x) \leq 1\}$ is bounded and Lebesgue-measurable with non-zero measure.

Let Λ be a euclidean lattice in $\mathbb{R}^n$ and consider the function

$$\bar{\zeta}(s) = \sum_{x \in \Lambda \cap X} F(x)^{-s}$$

in the complex variable s. The function $\bar{\zeta}(s)$ converges for $\Re s > 1$ and has a simple pole at $s = 1$ with residue given by

$$\mathrm{Res}_{s=1}(\bar{\zeta}(s)) = \frac{\mu(T)}{v(\Lambda)}.$$

Remark 6. The sum above is to be understood as the limit

$$\sum_{x \in \Lambda \cap X} F(x)^{-s} = \lim_{i \to \infty} \sum_{\substack{x \in \Lambda \cap X \\ F(x) \leq i}} F(x)^{-s}.$$

The set $\{x \in \Lambda \cap X \mid F(x) \leq i\}$ is bounded by (ii) and discrete so it is finite and therefore the sums in the limit are finite.

Proof. For any positive real number r we define $\Lambda_r = r^{-1}\Lambda$. We have $v(\Lambda_r) = r^{-n}v(\Lambda)$. Since T is bounded by (ii) and Λ is discrete, the intersection $T \cap \Lambda_r$ is finite for all $r > 0$. We define $n(r) := |T \cap \Lambda_r|$. By (ii), T is Lebesgue-measurable and by definition of the Lebesgue measure its volume is given by the limit

$$\mu(T) = \lim_{r \to \infty} n(r)v(\Lambda_r) = v(\Lambda) \lim_{r \to \infty} \frac{n(r)}{r^n}.$$

Meanwhile, we also have $n(r) = |rT \cap L|$. We have $y \in rT \cap \Lambda$ if and only if $y = rx \in \Lambda$ for some x in T. By (i), we then have $F(y) = F(rx) = r^n F(x) \leq r^n$. We conclude that

$$rT \cap \Lambda = \{y \in \Lambda \cap X \mid F(y) \leq r^n\}.$$

Since a euclidean lattice is countably infinite, we have in particular that $L \cap X$ is countable. We choose a ordering $L \cap X = \{x_1, x_2, \ldots\}$ such that $F(x_i) \leq F(x_j)$ whenever $i \leq j$. For every integer $i \geq 1$ we set r_i to be the real positive number $r_i = \sqrt[n]{F(x_i)}$. If $i \leq j$, then $F(x_i) = r_i^n \leq F(x_j) = r_j^n$. Thus for all i, the set $r_i T \cap L$ contains the points $x_1, \ldots, x_i$ and thus $n(r_i) \geq i$. On the other hand, for any $\epsilon > 0$, x_i does not belong to $(r_i - \epsilon)T$. As a consequence, $n(r_i - \epsilon) < i$. Thus

$$\frac{n(r_i - \epsilon)}{r_i^n} = \frac{n(r_i - \epsilon)}{(r_i - \epsilon)^n} \left(\frac{r_i - \epsilon}{r_i} \right)^n \leq \frac{i}{r_i^n} \leq \frac{n(r_i)}{r_i^n}.$$

We conclude that $\lim_{i \to \infty} n(r_i)/r_i^n = \lim_{i \to \infty} i/r_i^n$ and therefore

$$\mu(T) = v(\Lambda) \lim_{i \to \infty} \frac{i}{r_i^n} = v(\Lambda) \lim_{i \to \infty} \frac{i}{F(x_i)}.$$

We have

$$\bar{\zeta}(s) = \sum_{i\geq 1} \frac{1}{F(x_i)^s} = \sum_{i\geq 1} \frac{(i/F(x_i)^s)}{i^s}.$$

Since $\lim_{i\to\infty}(i/F(x_i)) = \mu(T)/v(\Lambda)$, the sequence $(i/F(x_i))$ is bounded and by comparing $\bar{\zeta}$ with the Riemann zeta-function ζ we see that $\bar{\zeta}(s)$ converges for $\mathcal{R}(s) > 1$. Also from the existence of this limit, for all $\epsilon > 0$ there exists a rank i_0 such that

$$(\mu(T)/v(\Lambda))^s - \epsilon < (i/F(x_i))^s < (\mu(T)/v(\Lambda))^s + \epsilon$$

for all $i \geq i_0$. Thus, for $\mathcal{R}(s) > 1$, we have

$$((v(T)/\Delta)^s - \epsilon)\sum_{i\geq i_0}\frac{1}{i^s} < \sum_{i\geq i_0}\frac{1}{F(x_i)^s} < ((v(T)/\Delta)^s + \epsilon)\sum_{i\geq i_0}\frac{1}{i^s}.$$

Multiplying by $(s-1)$, taking the limit as $s \to 1^+$ and using the fact that the Riemann zeta-function has a simple pole at $s = 1$ with residue equal to 1, we see that

$$\lim_{s\to 1^+}(s-1)\bar{\zeta}(s) = \frac{\mu(T)}{v(\Lambda)}$$

which is non-zero by (ii) and the proof is complete. □

1.5.2 Fundamental Domain of a Number Field

Henceforth, our goal is to apply Theorem 1.5.2 to the Dedekind zeta-function ζ_k. It is not obvious how this can be done and first we need to write ζ_k in the appropriate form. This implies finding a suitable cone and a suitable lattice. This section is concerned with the cone.

By Corollary 1.4.2 there exists a system of fundamental units $u_1, \ldots, u_r$ of k, that is, a basis for U_k/μ_k. Then $\lambda_k(u_1), \ldots, \lambda_k(u_r)$ are linearly independent over $\mathbb{R}$ and form a basis for the lattice $\lambda_k(U_k)$ in $\mathbb{R}X_k$. Let $u^* = (1, \ldots, 1, 2, \ldots, 2) = \sum_{v\in M_k^\infty} \epsilon_v v \in \mathbb{R}Y_k \cong \mathbb{R}^{r+1}$ where $e_v = 1$ if v is real and $e_v = 2$ if v is complex. The family $(u^*, \lambda_k(u_1), \ldots, \lambda_k(u_r))$ forms a basis of $\mathbb{R}Y_k$.

We extend the map $\lambda_k : k^* \longrightarrow \mathbb{R}Y_k$ a map on $(\mathbb{R}\otimes_{\mathbb{Q}} k)^*$ by defining the map $\lambda : (\mathbb{R}\otimes_{\mathbb{Q}} k)^* \longrightarrow \mathbb{R}Y_k$ by letting $x = (x_1, \ldots, x_{r_1}; x_{r_1+1}, \ldots, x_{r_1+r_2})$ map to

$$(\log|x_1|, \ldots, \log|x_{r_1}|, \log|x_{r_1+1}|^2, \ldots, \log|x_{r_1+r_2}|^2).$$

It is an extension since if $x \in k$, then $\lambda(x) = \lambda_k(x)$.

For any $x \in \mathbb{R}\otimes_{\mathbb{Q}} k$, there exist unique real coefficients $\xi, \xi_1, \ldots, \xi_r$ such that

$$\lambda(x) = \xi u^* + \sum_{i=1}^{r} \xi_i \lambda_k(u_i). \tag{1.5.2.1}$$

Definition 5. With the notations above, we define the fundamental domain of k with respect to the given system of fundamental units to be the subset X of $\mathbb{R}\otimes_{\mathbb{Q}} k$ consisting of elements $x = (x_1, \ldots, x_{r_1}; x_{r_1+1}, \ldots, x_{r_1+r_2})$ such that

- $N(x) \neq 0$;

- The coefficients in (1.5.2.1) satisfy $0 \leq \xi_i < 1$;
- If $r_1 \geq 1$, then $x_1 > 0$ and if $r_1 = 0$, then $0 \leq \arg x_1 < 2\pi/\omega_k$.

We first claim that X is a cone in $\mathbb{R} \otimes_{\mathbb{Q}} k$. Indeed, let α be a positive real number and let $x \in X$. We have

$$N(\alpha x) = \alpha x_1 \dots \alpha x_{r_1} |\alpha x_{r_1+1}|^2 \dots |\alpha x_{r_1+r_2}|^2 = \alpha^n N(x) \neq 0.$$

Moreover, we have

$$\lambda(\alpha x) = \log \alpha u^* + \lambda(x) = (\log \alpha + \xi) u^* + \sum_{i=1}^{r} \xi_i \lambda_k(u_i).$$

Finally if $r_1 \geq 1$, then $\alpha x_1 > 0$ and if $r_1 = 0$, then $\arg(\alpha x_1) = \arg x_1$. This proves that $\alpha x \in X$ and thus that X is a cone as claimed.

Proposition 8. *Every class of the quotient group $(\mathbb{R} \otimes_{\mathbb{Q}} k)^*/U_k$ has a unique representative that lies in X.*

Proof. Let $y \in (\mathbb{R} \otimes_{\mathbb{Q}} k)^*$ and write

$$\lambda(y) = \gamma u^* + \sum_{i=1}^{r} \gamma_i \lambda_k(u_i), \qquad \gamma, \gamma_i \in \mathbb{R}.$$

Let $\eta = u_1^{[\gamma_1]} \dots u_r^{[\gamma_r]} \in U_k$ and set $z = y\eta^{-1}$. Then

$$\lambda(z) = \lambda(y) - \lambda_k(\eta) = \gamma u^* + \sum_{i=1}^{r} \{\gamma_i\} \lambda_k(u_i)$$

where the brackets as usual denote the fractional part. If $r_1 \geq 1$, then z or $-z$ belongs to X and we have $y = z\eta$ and we have proved existence. If $r_1 = 0$, then let m be the integer in $\{0, \dots, \omega_k - 1\}$ such that $2\pi m/\omega_k \leq \arg z_1 < 2\pi(m+1)/\omega_k$. Pick $t \in \mu_k \cap \mathbb{R} \otimes_{\mathbb{Q}} k$ with $t_1 = e^{2\pi m/\omega_k}$ and set $x = zt^{-1}$. Then $0 \leq \arg x_1 < 2\pi/\omega_k$ and

$$\lambda(x) = \lambda(z) - \lambda_k(t) = \lambda(z)$$

since $\mu_k = \ker \lambda_k$. It follows that $x \in X$ and $y = x(t\eta)$ and we have proved existence in the case $r_1 = 0$.

We now prove uniqueness. Suppose that $y = x\epsilon = x'\epsilon'$ with $x, x' \in X$ and $\epsilon, \epsilon' \in U_k$. Write $\epsilon = tu_1^{n_1} \dots u_r^{n_r}$ and $\epsilon' = t'u_1^{n_1'} \dots u_r^{n_r'}$ with $t, t' \in \mu_k$ and $n_i, n_i' \in \mathbb{Z}$. We have $\lambda(x) - \lambda(x') = \lambda_k(\epsilon') - \lambda_k(\epsilon)$ so that

$$(\xi - \xi')u^* + \sum_{i=1}^{r} (\xi_i - \xi_i')\lambda_k(u_i) = \sum_{i=1}^{r} (n_i' - n_i)\lambda_k(u_i).$$

By linear independence we obtain $\xi = \xi'$ and $\xi_i - \xi_i' = n_i' - n_i$ for all $i = 1, \dots, r$. But $\xi_i - \xi' \in]-1, 1[$ so that $n_i = n_i'$ and therefore $\xi_i = \xi_i'$. We have $\epsilon' = \zeta_0 \epsilon$ for some $\zeta_0 \in \mu_k$ so that $x = x'\zeta_0$. If $r_1 \geq 1$ we must have $\zeta_0 = \pm 1$ but the condition $x_1, x_1' > 0$ forces $\zeta_0 = 1$. If $r_1 = 0$, then $\arg x_1 = \arg x_1' + \arg \zeta_0$ and the condition on $\arg x_1$ and $\arg x_1'$ imply that $\arg \zeta_0 = 0$ so that $\zeta_0 = 1$. □

Corollary 6. *Let $\alpha \in k^*$. Then there is a unique $\beta \in k \cap X$ such that $\alpha\mathcal{O}_k = \beta\mathcal{O}_k$.*

Proof. We have $\alpha \in (\mathbb{R} \otimes_{\mathbb{Q}} k)^*$ so by Proposition 8 there exist a unique β in X and a unique $\epsilon \in U_k$ such that $\alpha = \beta\epsilon$. We have $\beta = \alpha\epsilon^{-1} \in k$ and $\alpha\mathcal{O}_k = \beta\mathcal{O}_k$. □

Theorem 1.5.3. *With notations as above, the set $T = \{x \in X \,:\, |N(x)| \leq 1\}$ is bounded, Lebesgue-measurable and its volume is given by*

$$\mu(T) = \frac{2^{r_1}\pi^{r_2}R_k}{\omega_k}$$

In particular this volume is non-zero and independent of the choice of fundamental units.

Proof. We start by proving that T is bounded. Let $S = \{x \in X \,:\, |N(x)| = 1\}$. Since $|N(\alpha x)| = \alpha^n|N(x)|$ for all $\alpha > 0$, it is easy to see that

$$T = \{\alpha x \,:\, x \in S, \alpha \in]0,1]\}.$$

Therefore, if S is bounded then T too is bounded.

In order to ease the notation we define $e_i = 1$ for $i = 1, \ldots, r_1$ and $e_j = 2$ for $j = r_1 + 1, \ldots, r + 1$. For $x \in \mathbb{R} \otimes_{\mathbb{Q}} k$ we have the expression

$$\lambda(x) = \xi u^* + \sum_{i=1}^{r} \xi_i \lambda_k(u_i).$$

We sum the $r + 1$ coefficients of the left hand side vector and obtain

$$\sum_{i=1}^{r_1} \log|x_i| + \sum_{j=1}^{r_2} \log|x_j|^2 = \log|N(x)|.$$

We do the same on the right hand side and obtain

$$\xi n + \sum_{l=1}^{r} \xi_i \mathrm{aug}(\lambda_k(u_i)) = \xi n.$$

We conclude that $\xi = \log|N(x)|/n$. In particular, if x belongs to S then $\xi = 0$. In this case, for all $1 \leq j \leq r + 1$, we get

$$\lambda(x)_j = \sum_{i=1}^{r} \xi_i \lambda_k(u_i)_j < \sum_{i=1}^{r} \lambda_k(u_i)_j := C.$$

Consequently, we have the inclusion $S \subset \{x \in \mathbb{R} \otimes_{\mathbb{Q}} k \,:\, |x_i| \leq e^C, |x_j|^2 \leq e^C\}$ which proves that S is bounded.

We now turn to the computation of the volume of T. It will become clear that T is measurable during the process. Let $\zeta \in \mu_k \cap \mathbb{R} \otimes_{\mathbb{Q}} k$ such that $\zeta_1 = e^{\frac{2\pi i}{\omega_k}}$. Note that if $r_1 \geq 1$ we have $\omega_k = 2$ and $\zeta = -1$. Consider for $k = 0, 1, \ldots, \omega_K - 1$ the multiplication-by-ζ^k map on $\mathbb{R} \otimes_{\mathbb{Q}} k$ which we denote by L_k. The determinant of this map is $N_{k/\mathbb{Q}}(\zeta) = \pm 1$ so that these transformations are volume preserving.

Define $V_T = \bigcup_{i=0}^{\omega_k-1} L_i(T)$. This is the subset of $\mathbb{R}\otimes_{\mathbb{Q}} k$ consisting of elements x such that $0 < |N(x)| \leq 1$ and $\lambda(x) = \xi u^* + \sum_{i=1}^{r} \xi_i \lambda_k(u_i)$ with $0 \leq \xi_i < 1$. We have eliminated the original constraint on the first coordinate x_1. Since the above transformations are volume-preserving, we have $\mu(T) = \mu(V_T)/\omega_k$. Consider the subset

$$V_T' = \{x \in V_T \mid x_i > 0, 1 \leq i \leq r_1\}.$$

Let Δ be the set of elements of $\mathbb{R}\otimes_{\mathbb{Q}} k$ with first r_1 coordinates equal to ± 1 and the last r_2 equal to 1. This is a set of cardinality 2^{r_1}. For any $\delta \in \Delta$, denote by L_δ the multiplication-by-δ map which is volume preserving. We have the equality of sets $V_T = \bigcup_\delta V_T'$ so that

$$\mu(T) = \frac{2^{r_1}\mu(V_T')}{\omega_k}.$$

So it remain to prove that $\mu(V_T') = \pi^{r_2} R_k$. We recall that V_T' consists of elements x that satisfy:

- $0 < |N(x)| \leq 1$;
- For all j, $\lambda(x)_j = \frac{e_j}{n} \log |N(x)| + \sum_{i=1}^{r} \xi_i \lambda_k(u_i)_j$ with $0 \leq \xi_i < 1$;
- $x_1, \ldots, x_{r_1} > 0$.

We transit to polar coordinates by setting

$$\begin{aligned} x_i &= \rho_i, & i &= 1, \ldots, r_1 \\ z_j &= \rho_{r_1+j} e^{i\theta_j}, & j &= 1, \ldots, r_2. \end{aligned}$$

The Jacobian of this change of variables is equal to $\rho_{r_1+1} \ldots \rho_{r_1+r_2}$ and the new variables are subject the following conditions:

- $\rho_1, \ldots, \rho_{r_1+r_2} > 0$, $\prod_{j=1}^{r_1+r_2} \rho_j^{e_j} \leq 1$
- $\log \rho_j^{e_j} = \frac{e_j}{n} \log \prod_{j=1}^{r_1+r_2} \rho_j^{e_j} + \sum_{i=1}^{r} \xi_i \lambda_k(u_i)_j$ with $0 \leq \xi_i < 1$.

We perform a new change of variable $(\rho_1, \rho_2, \ldots, \rho_{r_1+r_2}) \leftrightarrow (\xi, \xi_1, \ldots, \xi_r)$ given by

$$\rho_j = \xi^{\frac{1}{n}} \prod_{i=1}^{r} e^{\frac{\xi_i}{e_j} l_j(\epsilon_i)}.$$

Note that $\xi = \prod_{j=1}^{r_1+r_2} \rho_j^{e_j}$. The set V_T' becomes the set of elements x with

$$\begin{aligned} x_i &= \xi^{\frac{1}{n}} \textstyle\prod_{l=1}^{r} e^{\xi_l \lambda_k(u_l)_i}, i = 1, \ldots, r_1 \\ x_j &= \xi^{\frac{1}{n}} e^{i\theta_1} \textstyle\prod_{l=1}^{r} e^{\frac{\xi_l}{2} \lambda_k(u_l)_j}, j = r_1+1, \ldots, r_1+r_2 \end{aligned}$$

subject to the conditions $0 < \xi \leq 1$ and $0 \leq \xi_i < 1$ for $i = 1, \ldots, r$. There are no conditions on the θ_j's. The Jacobian $|J|$ of this change of variables is given by

$$\begin{vmatrix} \frac{\rho_1}{n\xi} & \rho_1 l_1(\epsilon_1) & \ldots & \rho_1 l_1(\epsilon_r) \\ \vdots & \vdots & & \vdots \\ \frac{\rho_{r_1+r_2}}{n\xi} & \frac{\rho_{r_1+r_2}}{2} l_{r_1+r_2}(\epsilon_1) & \ldots & \frac{\rho_{r_1+r_2}}{2} l_{r_1+r_2}(\epsilon_r) \end{vmatrix}.$$

This determinant is in turn equal to

$$\frac{\rho_1 \dots \rho_{r_1+r_2}}{n\xi 2^{r_2}} \begin{vmatrix} e_1 & l_1(\epsilon_1) & \dots & l_1(\epsilon_r) \\ \vdots & \vdots & & \vdots \\ e_{r_1+r_2} & l_{r_1+r_2}(\epsilon_1) & \dots & l_{r_1+r_2}(\epsilon_r) \end{vmatrix}.$$

Summing all the rows with the first row we obtain the same matrix but with first row given by $(n, 0, \dots, 0)$ and expanding the determinant with respect to this row yields

$$|J| = \frac{\rho_1 \dots \rho_{r_1+r_2} R_k}{\xi 2^{r_2}}.$$

We may now compute the volume of V'_T:

$$\begin{aligned} \mu(V'_T) &= \int_{V'_T} dx_1 \dots dx_{r_1} dz_1 \dots dz_{r_2} \\ &= \int_{V'_T} \rho_{r_1+1} \dots \rho_{r_1+r_2} d\rho_1 \dots d\rho_{r_1+r_2} d\theta_1 \dots d\theta_{r_2} \\ &= \int_0^{2\pi} \dots \int_0^{2\pi} \int_0^1 \dots \int_0^1 \frac{\prod_{j=1}^{r_1+r_2} \rho_j^{e_j} R_k}{\xi 2^{r_2}} d\theta_1 \dots d\theta_{r_2} d\xi d\xi_1 \dots d\xi_r \\ &= \pi^{r_2} R_k, \end{aligned}$$

since $\xi = \prod_{j=1}^{r_1+r_2} \rho_j^{e_j}$. □

1.5.3 Proof of the Class Number Formula

Proof of Theorem 1.5.1. Let $s > 1$ be real. Since all terms in the Dirichlet series defining the Dedekind zeta function are positive, we rearrange the terms as follows:

$$\zeta_k(s) = \sum_{C \in \mathrm{Cl}(\mathcal{O}_k)} \zeta_{k,C}(s), \qquad \zeta_{k,C}(s) = \sum_{\mathfrak{a} \in C} N(\mathfrak{a})^{-s}.$$

Fix an ideal class $C \in \mathrm{Cl}(\mathcal{O}_k)$ and an integral ideal $\mathfrak{b}$ in C^{-1}. If $\mathfrak{a}$ is an integral ideal in C, then $\mathfrak{ab} = \alpha\mathcal{O}_k$ for some $\alpha \in \mathcal{O}_k$. This gives a bijective correspondence between integral ideals $\mathfrak{a}$ in C and associate elements α in $\mathcal{O}_k$ such that $\mathfrak{b}$ divides $\alpha\mathcal{O}_k$. Two elements α and β in $\mathcal{O}_k$ are said to be associate if they determine the same principal ideal or equivalently if they differ by an element of U_k. Using the multiplicativity of the norm, we may rewrite $\zeta_{k,C}$ as follows:

$$\zeta_{k,C}(s) = N(\mathfrak{b})^s \sum_{\alpha\mathcal{O}_k : \alpha \in \mathfrak{b}} |N_{k/\mathbb{Q}}(\alpha)|^{-s}.$$

By Corollary 6, if $\alpha \in \mathcal{O}_k$ then there is a unique $x \in k \cap X$ and a unique $\epsilon \in U_k$ such that $\alpha = x\epsilon$. If α belongs to $\mathfrak{b}$, then so does x. Moreover, $N_{k/\mathbb{Q}}(\alpha) = N_{k/\mathbb{Q}}(x) = N(x)$. Therefore there is a bijection between ideals $\alpha\mathcal{O}_k$ with $\alpha \in \mathfrak{b}$ and elements of the intersection $\mathfrak{b} \cap X$. We may then write

$$\zeta_{k,C}(s) = N(\mathfrak{b})^s \sum_{x \in \mathfrak{b} \cap X} |N(x)|^{-s}.$$

By Theorem 1.5.3, the set $T = \{x \in X : |N(x)| \leq 1\}$ is bounded and Lebesgue-measurable with non-zero measure. We apply Theorem 1.5.2 with the cone

X, the lattice $\mathfrak{b}$ and the function $|N(\cdot)|$ in order to conclude that the function $\zeta_{k,C}(s)$ converges absolutely in the region $\Re s > 1$ and has a simple pole at $s = 1$ with residue given by

$$\mathrm{Res}_{s=1}(\zeta_{k,C}(s)) = N(\mathfrak{b})\mu(T)/v(\mathfrak{b}) = \frac{2^{r_1}\pi^{r_2}R_k}{\omega_k 2^{-r_2}|d_k|^{\frac{1}{2}}}$$

where in the last equality we made use of Corollary 2 and Theorem 1.5.3. We finally get that $\zeta_k(s)$ converges absolutely for $\Re s > 1$ and has a simple pole at $s = 1$ with residue given by the formula

$$\mathrm{Res}_{s=1}(\zeta_k(s)) = \frac{2^{r_1}(2\pi)^{r_2}R_k}{\omega_k|d_k|^{\frac{1}{2}}}h_k.$$

□

Chapter 2

Global Class Field Theory

We give a brief introduction to global class field theory, going through the main theorems but without proofs. The central objects of study in class field theory are finite abelian extensions of number fields and the theory establishes a correspondence between such extension and certain subgroups called generalized ideal class groups. Our main reference here is Chapter 8 of [Cox]. A presentation of this theory with ideles can be found in [CF].

2.1 Generalized Ideal Class Groups

Let k be a number field. Denote respectively by I_k and P_k the group of fractional ideals of k and its subgroup of principal fractional ideals. As we have seen (cf. Corollary 4), the ideal class group $\mathrm{Cl}(\mathcal{O}_k) = I_k/P_k$ is finite. Moreover, we have the following exact sequence

$$1 \longrightarrow U_k \longrightarrow k^* \longrightarrow P_k \longrightarrow I_k \longrightarrow \mathrm{Cl}(\mathcal{O}_k) \longrightarrow 1.$$

In what follows we will refer to elements of M_k as primes of k whether they are finite or infinite. The reason for this is that infinite places behave much like primes.

Definition 6. A formal product of primes of k

$$\mathfrak{m} = \prod_{v \in M_K} v^{m(v)}$$

is called a modulus of k if the following conditions are satisfied:

- All $m(v)$ are non-negative integers and $m(v) = 0$ for all but finitely many primes.
- If v is a complex archimedean prime, then $m(v) = 0$.
- If v is a real archimedean prime, then $m(v) \leq 1$.

We write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ in order to distinguish the finite and infinite parts of the modulus. Note that if k is totally imaginary, then a modulus of k is simply an integral ideal of k. We write $v|\mathfrak{m}$ if $m(v) > 0$ and we say that v divides the modulus.

If $\mathfrak{m}$ is a modulus of k, we denote by $I_k(\mathfrak{m})$ the subgroup of I_k that consists of fractional ideals of k coprime to $\mathfrak{m}$ (meaning coprime to $\mathfrak{m}_0$), that is, the free abelian group generated by primes ideals of $\mathcal{O}_k$ that do not divide the modulus $\mathfrak{m}$. Similarly, we define $P_k(\mathfrak{m})$ to be the subgroup of $I_k(\mathfrak{m})$ consisting of principal fractional ideals prime to $\mathfrak{m}$. We define $P_{k,1}(\mathfrak{m})$ to be the subgroup of I_k generated by principal fractional ideals $\alpha\mathcal{O}_K$ where

- $\alpha \in \bigcap_{\mathfrak{p}|\mathfrak{m}_0} \mathcal{O}_\mathfrak{p}$,
- $\alpha \equiv 1 \mod \mathfrak{m}_0$,
- $\sigma_v(\alpha) > 0$ for all $v|\mathfrak{m}_\infty$, where σ_v denotes the embedding $k \hookrightarrow \mathbb{R}$ corresponding to the real archimedean place v.

We summarize these conditions by writing simply $\alpha \equiv^* 1 \mod \mathfrak{m}$.

Proposition 9. *Let $\mathfrak{m}$ be a modulus of k. The group $P_{k,1}(\mathfrak{m})$ is a finite index subgroup of $I_k(\mathfrak{m})$. The finite quotient group $\mathrm{Cl}_k(\mathfrak{m}) := I_k(\mathfrak{m})/P_{k,1}(\mathfrak{m})$ is called the $\mathfrak{m}$-ray class group of k.*

Proof. From the definition it is obvious that $P_{k,1}(\mathfrak{m})$ is a subgroup of $I_k(\mathfrak{m})$. For the finite index assertion, we follow [Lan] p. 124-126.

We start by claiming that the map $I_k(\mathfrak{m}) \hookrightarrow I_k \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_k)$ is surjective. Indeed, let $\mathfrak{a}$ be an element of I_k. Without loss of generality we may assume that $\mathfrak{a}$ is an integral ideal. We have a decomposition $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$ where the $v_\mathfrak{p}(\mathfrak{a})$ are non-negative integers and all but finitely many are zero. For every $\mathfrak{p}$ that divides $\mathfrak{a}$, we denote by $\pi_\mathfrak{p}$ a uniformizer for $\mathfrak{p}$. By the Approximation Theorem (cf. [CF] Chapter II § 15), there exists a solution to the system

$$x \equiv \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \mod \pi_\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})+1}, \quad \mathfrak{p}|\mathfrak{m}.$$

But then $\mathfrak{a}x^{-1}\mathcal{O}_k$ belongs to $I_k(\mathfrak{m})$ and is a representative of the same class as $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O}_k)$. The kernel of the above map is $P_k \cap I_k(\mathfrak{m}) = P_k(\mathfrak{m})$ and from the inclusion $P_{k,1}(\mathfrak{m}) \subset P_k(\mathfrak{m})$ we get the exact sequence

$$1 \longrightarrow P_k(\mathfrak{m})/P_{k,1}(\mathfrak{m}) \longrightarrow \mathrm{Cl}_k(\mathfrak{m}) \longrightarrow \mathrm{Cl}(\mathcal{O}_k) \longrightarrow 1.$$

In order to prove the finiteness of $\mathrm{Cl}_k(\mathfrak{m})$ it thus suffices to prove the finiteness of $P_k(\mathfrak{m})/P_{k,1}(\mathfrak{m})$.

We denote by $k^*_{\mathfrak{m},1}$ the subgroup of k^* consisting of elements α in k^* such that $\alpha\mathcal{O}_K \in P_{k,1}(\mathfrak{m})$ and we define $U_{\mathfrak{m},1} = U_k \cap k^*_{\mathfrak{m},1}$. If $k^*_\mathfrak{m}$ denotes the elements α of k^* for which the fractional ideal $\alpha\mathcal{O}_k$ is coprime to $\mathfrak{m}$, then we have an obvious surjective homomorphism of groups $k^*_\mathfrak{m} \twoheadrightarrow P_k(\mathfrak{m}) \twoheadrightarrow P_k(\mathfrak{m})/P_{k,1}(\mathfrak{m})$ whose kernel is $U_k.k^*_{\mathfrak{m},1}$ so that we obtain an isomorphism

$$k^*_\mathfrak{m}/U_k.k^*_{\mathfrak{m},1} \cong P_k(\mathfrak{m})/P_{k,1}(\mathfrak{m}).$$

Consider the following map:

$$\psi : k^*_\mathfrak{m} \longrightarrow \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(\mathcal{O}_\mathfrak{p}/(\pi_\mathfrak{p}^{m(\mathfrak{p})})\right)^* \times \prod_{v|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}_{>0}$$

defined for each component by $\psi(\alpha)_\mathfrak{p} = \alpha \mod \pi_\mathfrak{p}^{m(\mathfrak{p})}$ and $\psi(\alpha)_v = \sigma_v(\alpha) \mod \mathbb{R}_{>0}$. Note that $\mathbb{R}^*/\mathbb{R}_{>0} \cong \{\pm 1\}$ and each $\mathcal{O}_\mathfrak{p}/(\pi_\mathfrak{p}^{m(\mathfrak{p})})$ is finite.

The map ψ is well-defined homomorphism: if α belongs to $k^*_{\mathfrak{m}}$, then $v_{\mathfrak{p}}(\alpha) = 0$ for all $\mathfrak{p}|\mathfrak{m}_0$ so that the class $[\alpha]_{\mathfrak{p}}$ of α in the quotient group $\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}^{m(\mathfrak{p})}$ is relatively prime to $\pi_{\mathfrak{p}}^{m(\mathfrak{p})}$ which implies that it is invertible in this quotient by Bézout's identity (the local ring $\mathcal{O}_{\mathfrak{p}}$ is a principal ideal domain and therefore has a well-defined notion of divisibility and gcd).

We claim that ψ is also surjective. Let $([\alpha_v]_v)_{v|\mathfrak{m}}$ be an element of the above product. Given any $\epsilon > 0$, by the Approximation Theorem (cf. [CF] Chapter II § 15), we may find $\alpha \in k$ such that

$$|\alpha - \alpha_v|_v \leq \epsilon, \text{ for all } v|\mathfrak{m}.$$

Taking $\epsilon \leq \min_{\mathfrak{p}|\mathfrak{m}_0}\{N(\mathfrak{p})^{-m(\mathfrak{p})}\}$, we see that

$$v_{\mathfrak{p}}(\alpha - \alpha_{\mathfrak{p}}) \geq m(\mathfrak{p}), \text{ for all } \mathfrak{p}|\mathfrak{m}_0$$

which implies that $\alpha - \alpha_{\mathfrak{p}} \in (\pi_{\mathfrak{p}}^{m(\mathfrak{p})})$. Moreover, for $\mathfrak{p}|\mathfrak{m}_0$, we have

$$v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\alpha - \alpha_{\mathfrak{p}} + \alpha_{\mathfrak{p}}) = v_{\mathfrak{p}}(\alpha_v) = 0$$

so that $\alpha \in k^*_{\mathfrak{m}}$. Taking ϵ even smaller if necessary, we see that for v real, $\sigma_v(\alpha)$ and $\sigma_v(\alpha_v)$ have the same sign which implies equality in the quotient $\mathbb{R}^*/\mathbb{R}_{>0}$. Thus $\psi(\alpha) = ([\alpha_v]_v)_{v|\mathfrak{m}}$ and we have proved surjectivity.

The kernel of ψ is exactly $k^*_{\mathfrak{m},1}$ and we therefore have an isomorphism

$$k^*_{\mathfrak{m}}/k^*_{\mathfrak{m},1} \cong \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(\mathcal{O}_p/(\pi_{\mathfrak{p}}^{m(\mathfrak{p})})\right)^* \times \prod_{v|\mathfrak{m}_\infty} \mathbb{R}^*/\mathbb{R}_{>0}.$$

This proves that $k^*_{\mathfrak{m}}/k^*_{\mathfrak{m},1}$ is a finite group. By the universal property of the quotient we have a surjective homomorphism

$$k^*_{\mathfrak{m}}/k^*_{\mathfrak{m},1} \longrightarrow k^*_{\mathfrak{m}}/U_k.k^*_{\mathfrak{m},1}$$

and therefore the latter is finite. □

Definition 7. Let $\mathfrak{m}$ be a modulus of k. A subgroup H of $I_k(\mathfrak{m})$ is called a congruence subgroup for $\mathfrak{m}$ is it satisfies the inclusions

$$P_{k,1}(\mathfrak{m}) \subset H \subset I_k(\mathfrak{m}).$$

In this case, the quotient group $I_k(\mathfrak{m})/H$ is called a generalized ideal class group for $\mathfrak{m}$.

Example 1. Consider the case $k = \mathbb{Q}$. This example will help better understand what the ray class groups are and why we choose to include infinite primes in the definition of a modulus. In the present case, $\mathcal{O}_k = \mathbb{Z}$ which is a principal ideal domain. Consequently, the ideal class group is trivial and every fractional ideal of $\mathbb{Q}$ is of the form $\frac{a}{b}\mathbb{Z}$ with $\gcd(a,b) = 1$. There are only two possible sorts of moduli in this case.

(1) Consider a modulus of the form $\mathfrak{m} = m\mathbb{Z}$ where m is an integer. In this case $\mathfrak{m} = \mathfrak{m}_0$. Write $m = p_1^{m_1} \dots p_r^{m_r}$. Then

$$I_{\mathbb{Q}}(\mathfrak{m}) = \{\frac{a}{b}\mathbb{Z} \, : \, p_i \nmid a, p_i \nmid b, \gcd(a,b) = 1\}.$$

The condition $\frac{a}{b} \equiv^* 1 \mod m$ translates as $a \equiv b \mod m$, that is, $ab^{-1} \equiv 1 \mod m$. This last notation makes sense since b is prime to m and thus invertible in $\mathbb{Z}/m\mathbb{Z}$. Thus $P_{\mathbb{Q},1}(\mathfrak{m})$ consists of principal fractional ideals which can be expressed as (a/b) with $ab^{-1} \equiv 1 \mod m$. We say "expressed" since there is no unique way to write a principal ideal: the other generator of this ideal is $-a/b$. Thus $P_{\mathbb{Q},1}(\mathfrak{m})$ actually consists of the principal fractional ideals (a/b) such that $ab^{-1} \equiv \pm 1 \mod m$. Consider the following map

$$I_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}, \qquad \frac{a}{b}\mathbb{Z} \longmapsto [ab^{-1}].$$

This is well-defined since $[ab^{-1}] = [-ab^{-1}]$ in the target and both a and b are invertible in $\mathbb{Z}/m\mathbb{Z}$. It is clearly a homomorphism and it is surjective since for any n coprime to m, the ideal $n\mathbb{Z}$ belongs to $I_{\mathbb{Q}}(\mathfrak{m})$ and maps to $[n]$. Finally, the kernel is exactly $P_{\mathbb{Q},1}(\mathfrak{m})$. We therefore have an isomorphism

$$\mathrm{Cl}_{\mathbb{Q}}(m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}.$$

(2) Let v_∞ denote the unique archimedean place of $\mathbb{Q}$. This is simply the standard absolute value. Consider now the modulus of the form $\mathfrak{m} = m\mathbb{Z}v_\infty$. The group $I_{\mathbb{Q}}(\mathfrak{m})$ remains the same as $I_{\mathbb{Q}}(m\mathbb{Z})$. The condition $\frac{a}{b} \equiv^* 1 \mod \mathfrak{m}$ translates as $ab^{-1} \equiv 1 \mod m$ and $\frac{a}{b} > 0$. Thus $P_{\mathbb{Q},1}(\mathfrak{m})$ consists of principal fractional ideals which can be expressed as $a/b\mathbb{Z}$ with $ab^{-1} \equiv 1 \mod m$ and $\frac{a}{b} > 0$. Denote by $(a/b)_+$ the positive generator of the ideal $a/b\mathbb{Z}$. Consider the following map

$$I_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*, \qquad \left(\frac{a}{b}\right)_+ \longmapsto [ab^{-1}].$$

This is a well-defined surjective homomorphism of groups with kernel equal to $P_{\mathbb{Q},1}(\mathfrak{m})$. We therefore have an isomorphism of groups

$$\mathrm{Cl}_{\mathbb{Q}}(m\mathbb{Z}v_\infty) \cong (\mathbb{Z}/m\mathbb{Z})^*.$$

2.2 Finite Galois Extensions of Number Fields

We quickly review the main results concerning finite Galois extensions of number fields and define the Frobenius element associated to a prime ideal. More details are available in [Sam], VI or [Lil] Appendix B.3.

2.2.1 Decomposition and Inertia Groups

Let K/k be a finite Galois extension of number fields of degree n and let $G = \mathrm{Gal}(K/k)$. Let $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_k$. The Galois group G act transitively on the prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ that lie above $\mathfrak{p}$. If $\mathfrak{P}$ divides $\mathfrak{p}$ and $\sigma \in G$, then we have the relation

$$|x|_{\sigma(\mathfrak{P})} = |\sigma^{-1}(x)|_{\mathfrak{P}}, \text{ for } x \in K.$$

We define the decomposition group $D_{\mathfrak{P}/\mathfrak{p}}$ associated to $\mathfrak{P}$ to be the subgroup of G given by

$$D_{\mathfrak{P}/\mathfrak{p}} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

It is the stabilizer of $\mathfrak{P}$. One has a surjective homomorphism of groups

$$D_{\mathfrak{P}/\mathfrak{p}} \longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$$

where $\mathbb{F}_{\mathfrak{P}}$ and $\mathbb{F}_{\mathfrak{p}}$ respectively denote the residue field of K at $\mathfrak{P}$ and k at $\mathfrak{p}$. The map is given by sending σ to the automorphism of $\mathbb{F}_{\mathfrak{P}}$ which sends $x \mod \mathfrak{P}$ to $\sigma(x) \mod \mathfrak{P}$ for $x \in \mathcal{O}_K$. We define the inertia group $I_{\mathfrak{P}/\mathfrak{p}}$ of $\mathfrak{P}$ to be the kernel of this map so that we have the exact sequence

$$1 \longrightarrow I_{\mathfrak{P}/\mathfrak{p}} \longrightarrow D_{\mathfrak{P}/\mathfrak{p}} \longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \longrightarrow 1.$$

Remark 7. When the context is clear and there is no possible risk of confusion we shall use the notation $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ instead of the more tedious $D_{\mathfrak{P}/\mathfrak{p}}$ and $I_{\mathfrak{P}/\mathfrak{p}}$.

Because G acts transitively on the prime ideals above $\mathfrak{p}$, these all have the same ramification and residual degrees that we therefore simply denote by $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ respectively. We thus have the following decomposition

$$\mathfrak{p}\mathcal{O}_K = \prod_{\sigma \in G/D_{\mathfrak{P}}} \sigma(\mathfrak{P})^{e_{\mathfrak{p}}}$$

and we have the degree formula $n = e_{\mathfrak{p}} f_{\mathfrak{p}} |G/D_{\mathfrak{P}}|$ so that $|D_{\mathfrak{P}}| = e_{\mathfrak{p}} f_{\mathfrak{p}}$. But $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is isomorphic to $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ which has order $f_{\mathfrak{p}}$ by definition of the residual degree. Therefore $|I_{\mathfrak{P}}| = e_{\mathfrak{p}}$. It follows that $\mathfrak{P}$ is unramified in K/k if and only if the inertia group $I_{\mathfrak{P}}$ is trivial.

The next lemma shows that the decomposition and inertia groups of two primes lying above the same prime in $\mathcal{O}_k$ are conjugates:

Proposition 10. *With the above notations, we have $D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}$ and $I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$ for all $\sigma \in G$ and all prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$.*

Proof. Fix $\sigma \in G$ and a prime $\mathfrak{P} \subset \mathcal{O}_K$. Let τ be an element of the decomposition group $D_{\mathfrak{P}}$. Then

$$\sigma\tau\sigma^{-1}(\sigma(\mathfrak{P})) = \sigma(\tau(\mathfrak{P})) = \sigma(\mathfrak{P})$$

so that $\sigma\tau\sigma^{-1}$ belong to $D_{\sigma(\mathfrak{P})}$. This proves that $\sigma G_{\mathfrak{P}} \sigma^{-1} \subset G_{\sigma(\mathfrak{P})}$. This holds for all σ. Applying this with the inverse σ^{-1} to $\sigma(\mathfrak{P})$, we see that $\sigma^{-1} G_{\sigma(\mathfrak{P})} \sigma \subset G_{\mathfrak{P}}$ which implies that $G_{\sigma(\mathfrak{P})} \subset \sigma G_{\mathfrak{P}} \sigma^{-1}$ and we therefore obtain equality.

Let τ be an element of the inertia group $I_{\mathfrak{P}}$. Then for all $x \in \mathcal{O}_K$,

$$\sigma\tau\sigma^{-1}(x) - x = \sigma(\tau(\sigma^{-1}(x)) - \sigma^{-1}(x)) \in \sigma(\mathfrak{P}).$$

This proves that $\sigma\tau\sigma^{-1}$ belongs to $I_{\sigma(\mathfrak{P})}$ and thus $\sigma I_{\mathfrak{P}} \sigma^{-1} \subset I_{\sigma(\mathfrak{P})}$. By the same argument as before we obtain equality. □

We will now study the relation between different inertia and decomposition groups in finite Galois towers of number fields. Let $L/K/k$ be such a tower. Let $\mathfrak{p}$ be a prime ideal in k, let $\mathfrak{P}$ be one of K that lies above $\mathfrak{p}$ and let $\wp$ denote a prime ideal of L that lies above $\mathfrak{P}$. We have the tower of prime ideals $\wp|\mathfrak{P}|\mathfrak{p}$. It is not difficult to see that both the ramification and residual degrees behave multiplicatively, that is,

$$e(\wp/\mathfrak{p}) = e(\wp/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p}) \text{ and } f(\wp/\mathfrak{p}) = f(\wp/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p}).$$

Proposition 11. *With the above notation, the restriction map from* $\mathrm{Gal}(L/k)$ *to* $\mathrm{Gal}(K/k)$ *induces isomorphisms*

$$D_{\wp/\mathfrak{p}}/D_{\wp/\mathfrak{P}} \cong D_{\mathfrak{P}/\mathfrak{p}} \quad \text{ and } \quad I_{\wp/\mathfrak{p}}/I_{\wp/\mathfrak{P}} \cong I_{\mathfrak{P}/\mathfrak{p}}.$$

Proof. The restriction map $\mathrm{Res} : \mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K/k)$ is a surjective group homomorphism with kernel $\mathrm{Gal}(L/K)$.

Consider the restriction of the above map to the decomposition group $D_{\wp/\mathfrak{p}}$. We claim that the image of this map lies in $D_{\mathfrak{P}/\mathfrak{p}}$. In fact, let $\sigma \in D_{\wp/\mathfrak{p}}$. We must prove that $\mathrm{Res}(\sigma)(\mathfrak{P}) = \mathfrak{P}$. We have $\sigma(\wp) = \wp$ and

$$\mathrm{Res}(\sigma)(\mathfrak{P}) = \sigma(\mathfrak{P} \cap \mathcal{O}_K) \subset \wp \cap \mathcal{O}_K = \mathfrak{P}$$

because K is a normal extension of k and σ is a k-homomorphism so that $\sigma(\mathcal{O}_K) = \mathcal{O}_K$. Applying this with the inverse of sigma we obtain $\mathrm{Res}(\sigma)^{-1}(\mathfrak{P}) \subset \mathfrak{P}$ so that $\mathfrak{P} \subset \mathrm{Res}(\sigma)(\mathfrak{P})$. This prove that $\mathrm{Res}(\sigma) \in D_{\mathfrak{P}/\mathfrak{p}}$ whenever $\sigma \in D_{\wp/\mathfrak{p}}$. Consequently, we have a homomorphism $\mathrm{Res} : D_{\wp/\mathfrak{p}} \longrightarrow D_{\mathfrak{P}/\mathfrak{p}}$ with kernel equal to $D_{\wp/\mathfrak{p}} \cap \mathrm{Gal}(L/K) = D_{\wp/\mathfrak{P}}$. Therefore we have an injective homomorphism of groups

$$D_{\wp/\mathfrak{p}}/D_{\wp/\mathfrak{P}} \longrightarrow D_{\mathfrak{P}/\mathfrak{p}}.$$

Using the fact that the ramification and residual degrees behave mutiplicatively we see that the cardinalities of the two groups are equal and therefore the above map is an isomorphism.

We further restrict the map Res to the inertia group $I_{\wp/\mathfrak{p}}$. We claim that the image of this map lies in $I_{\mathfrak{P}/\mathfrak{p}}$. In fact, let $\sigma \in I_{\wp/\mathfrak{p}}$ and let $x \in \mathcal{O}_K$. By the above we know that $\mathrm{Res}(\sigma) \in D_{\mathfrak{P}/\mathfrak{p}}$. We have $\sigma(x) - x \in \wp$. We also have $\sigma(x) - x \in \mathcal{O}_K$ and therefore $\sigma(x) - x \in \mathfrak{P}$. This proves that $\mathrm{Res}(\sigma) \in I_{\mathfrak{P}/\mathfrak{P}}$. We therefore have a homomorphism $\mathrm{Res} : I_{\wp/\mathfrak{p}} \longrightarrow I_{\mathfrak{P}/\mathfrak{p}}$. The kernel of this homomorphism is $I_{\wp/\mathfrak{p}} \cap \mathrm{Gal}(L/K) = I_{\wp/\mathfrak{P}}$. We therefore have an injective homomorphism of groups

$$I_{\wp/\mathfrak{p}}/I_{\wp/\mathfrak{P}} \longrightarrow I_{\mathfrak{P}/\mathfrak{p}}.$$

Again by comparing cardinalities, this map must be an isomorphism. □

2.2.2 The Frobenius Element

Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_K$ above $\mathfrak{p}$. The extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is a finite extension of finite fields of degree $f_{\mathfrak{p}}$. The order of $\mathbb{F}_{\mathfrak{p}}$ is $N(\mathfrak{p})$. By general theory of finite field extensions, the Galois group of this extension is generated by the $N(\mathfrak{p})$-th power Frobenius automorphism of $\mathbb{F}_{\mathfrak{P}}$ which is defined by $x \longmapsto x^{N(\mathfrak{p})}$. Since $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is isomorphic to $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, this element corresponds to an element in $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ which we call the Frobenius element of K/k at $\mathfrak{P}$ and which we denote by $(\mathfrak{P}, K/k)$. It generates the quotient group $D_{\mathfrak{P}}/I_{\mathfrak{P}}$. A representative of $(\mathfrak{P}, K/k)$ in $D_{\mathfrak{P}}$ will be denoted $\sigma_{\mathfrak{P}}$ and is characterized by $\sigma_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$ for all $x \in \mathcal{O}_K$. Note that if $\mathfrak{p}$ is unramified, then $(\mathfrak{P}, K/k)$ is an actual element of G and we will interchangeably use the notations $(\mathfrak{P}, K/k)$ and $\sigma_{\mathfrak{P}}$ in this case. The Frobenius element is then uniquely determined by the congruence condition above and the fact that it belongs to $D_{\mathfrak{P}}$. We have the following result:

Proposition 12. *Let $\mathfrak{p}$ be a prime ideal of k and let $\mathfrak{P}$ be a prime ideal of K above $\mathfrak{p}$. Let $\sigma_{\mathfrak{P}}$ denote a representative of $(\mathfrak{P}, K/k)$ in $D_{\mathfrak{P}}$. For all $\sigma \in G$, we have $\sigma\sigma_{\mathfrak{P}}\sigma^{-1}$ is a representative of $(\sigma(\mathfrak{P}), K/k)$ in $D_{\sigma(\mathfrak{P})}$.*

Proof. First of all, by Proposition 10 we know that $\sigma\sigma_{\mathfrak{P}}\sigma^{-1}$ does indeed belong to $D_{\sigma(\mathfrak{P})}$. Let $x \in \mathcal{O}_K$. We have $\sigma_{\mathfrak{P}}(x) - x \in \mathfrak{P}$. We have $\sigma^{-1}(x) \in \mathcal{O}_K$ and thus $\sigma_{\mathfrak{P}}\sigma^{-1}(x) - \sigma^{-1}(x) \in \mathfrak{P}$. Consequently, we have

$$\sigma\sigma_{\mathfrak{P}}\sigma^{-1}(x) - x = \sigma(\sigma_{\mathfrak{P}}\sigma^{-1}(x) - \sigma^{-1}(x)) \in \sigma)(\mathfrak{P}).$$

By definition, this shows that $\sigma\sigma_{\mathfrak{P}}\sigma^{-1}$ is a representative of $(\sigma(\mathfrak{P}), K/k)$ in $D_{\sigma(\mathfrak{P})}$. □

Remark 8. If K/k is an abelian extension, meaning that G is an abelian group, then for any prime ideal $\mathfrak{p}$ in $\mathcal{O}_k$ there is only one decomposition group and one inertia group above $\mathfrak{p}$ since by Proposition 10 these are all conjugates. We will therefore simply write $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ in this case. Also, if $\mathfrak{p}$ is unramified, then there is also only one Frobenius element above $\mathfrak{p}$ by Proposition 12 and we will denote this element by $(\mathfrak{p}, K/k)$ or $\sigma_{\mathfrak{p}}$.

We have the following result concerning the behavior of Frobenius elements in towers:

Proposition 13. *Let $L/K/k$ be a tower of finite Galois extensions of number fields. Let $\wp|\mathfrak{P}|\mathfrak{p}$ be a corresponding tower of prime ideals. Denote by* Res *the restriction map* $\mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K/k)$*. If $\sigma_{\wp}$ denotes a representative of $(\wp, L/k)$ in $D_{\wp/\mathfrak{p}}$, then* $\mathrm{Res}(\sigma_{\wp})$ *is a representative of $(\mathfrak{P}, K/k)$ in $D_{\mathfrak{P}/\mathfrak{p}}$.*

Proof. By Proposition 11, we have $\mathrm{Res}(D_{\wp/\mathfrak{p}}) = D_{\mathfrak{P}/\mathfrak{p}}$. Let $x \in \mathcal{O}_L$. Then $\sigma_{\wp}(x) - x^{N(\mathfrak{p})} \in \wp$. If $x \in \mathcal{O}_K$ then $\sigma_{\wp}(x) \in \mathcal{O}_K$ because K/k is normal. Thus $\sigma_{\wp}(x) - x \in \mathcal{O}_K \cap \wp = \mathfrak{P}$. Thus $\mathrm{Res}(\sigma_{\wp})$ is indeed a representative of $(\mathfrak{P}, K/k)$. □

Let K/k be a finite Galois extension of number fields. Let $G = \mathrm{Gal}(K/k)$ and let H be a subgroup of G. We set $F = K^H$. Note that F/k is Galois if and only if H is a normal subgroup of G. We fix a prime $\mathfrak{p}$ in k. In F we have the following decomposition $\mathfrak{p}\mathcal{O}_F = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_r^{e_r}$. For each i, we let f_i denote the residual degree of $\mathfrak{q}_i$ over $\mathfrak{p}$. For each $\mathfrak{q}_i$ we let $\mathfrak{P}_i$ denote a prime of K that lies above $\mathfrak{q}_i$ and we denote by e'_i and f'_i the associated ramification and residual degrees of $\mathfrak{P}_i$ over $\mathfrak{q}_i$. We let e and f be the ramification and residual degrees of $\mathfrak{P}_i$ over $\mathfrak{p}$. We have the following formulas:

$$\sum_{i=1}^{r} e_i f_i = [F : k] \qquad e = e_i e'_i \qquad f = f_i f'_i.$$

The prime ideal $\mathfrak{P}_i$ all lie above $\mathfrak{p}$ and G acts transitively on the prime ideals of $\mathcal{O}_K$ that lie above $\mathfrak{p}$. We let $\eta_i \in G$ be such that $\eta_i(\mathfrak{P}_1) = \mathfrak{P}_i$. Let D_i and I_i be respectively the decomposition and inertia groups of $\mathfrak{P}_i$ over $\mathfrak{p}$. Then by Proposition 10 we have $D_i = \eta_i D_1 \eta_i^{-1}$ and $I_i = \eta_i I_1 \eta_i^{-1}$. Let $\sigma_1 \in D_1$ be an element such that $(\mathfrak{P}_1, K/k) = \sigma_1 I_1$ and choose $\sigma_i \in D_i$ such that $\sigma_i = \eta_i \sigma_1 \eta_i^{-1}$ by Proposition 12. Note that $D_i \cap H$ and $I_i \cap H$ are respectively the decomposition and inertia groups of $\mathfrak{P}_i$ over $\mathfrak{q}_i$. The order of the group D_i is ef and the order of $D_i \cap H$ is $e'_i f'_i$ and thus the index of $D_i \cap H$ in D_i is $e_i f_i$. Let $\{\gamma_{i,\nu}\}$ for $\nu = 1, \dots, e_i f_i$ be a system of right coset representatives of the quotient $D_i/(D_i \cap H)$.

Lemma 3. *With the above notations, the family $\{\gamma_{i,\nu}\eta_i\}$ for $i = 1, \ldots, r$ and $\nu = 1, \ldots, e_i f_i$ is a system of distinct right coset representatives of the quotient $H \setminus G$.*

Proof. We first prove that they each represent a distinct coset. Suppose that $H\gamma_{i,\nu}\eta_i = H\gamma_{j,\mu}\eta_j$. Then $\gamma_{i,\nu}\eta_i\eta_j^{-1}\gamma_{j,\mu}^{-1} \in H$. Since $\gamma_{j,\mu}$ belongs to D_j we have $\gamma_{j,\mu}^{-1}(\mathfrak{P}_j) = \mathfrak{P}_j$ and thus $\eta_j^{-1}\gamma_{j,\mu}^{-1}(\mathfrak{P}_j) = \mathfrak{P}_1$. Since $\eta_i(\mathfrak{P}_1) = \mathfrak{P}_i$ and $\gamma_{i,\mu}$ belongs to D_i, we see that $\gamma_{i,\nu}\eta_i\eta_j^{-1}\gamma_{j,\mu}^{-1}(\mathfrak{P}_j) = \mathfrak{P}_i$. But elements of H permute divisors of prime ideals in $\mathcal{O}_F$ and therefore we must have that $\mathfrak{P}_i$ divides $\mathfrak{q}_j$ which implies that $i = j$. But then $\gamma_{i,\nu}\gamma_{i,\mu}^{-1} \in H$ so that $\gamma_{i,\nu}$ and $\gamma_{i,\mu}$ represent the same element in the quotient $(D_i \cap H) \setminus D_i$ and this implies $\nu = \mu$. This proves that each element of our system represents distinct cosets. Since our system is comprised of $\sum_{i=1} e_i f_i = [F : k] = [G : H]$ elements we have proved our claim. □

Lemma 4. *With the above notations, for each i we let ϕ_i be an element of the decomposition group $D_i \cap H$ of $\mathfrak{P}_i$ over $\mathfrak{q}_i$ such that $(\mathfrak{P}_i, K/F) = \phi_i(I_i \cap H)$. For any integer j, the intersection $\sigma_i^j I_i \cap H$ is non-empty if and only if f_i divides j. Moreover, if this is the case, then*

$$\sigma_i^j I_i \cap H = \phi_i^{j/f_i}(I_i \cap H).$$

Proof. Suppose that $\sigma_i^j\tau$ belongs to H for some τ in I_i. Then by definition of the inertia group, for all $x \in \mathcal{O}_K$, we have $\sigma_i^j\tau(x) \equiv \sigma_i^j(x) \mod \mathfrak{P}_i$. The residue field $\mathcal{O}_K/\mathfrak{P}_i$ is an extension of $\mathcal{O}_F/\mathfrak{q}_i$ of degree f_i' and since $\sigma_i^j\tau$ belongs to H, $\sigma_i^j\tau(x) = x$ for all x in $\mathcal{O}_F$. By definition of the Frobenius element, $\sigma_i(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}_i$ for all x in $\mathcal{O}_K$. By composition, $\sigma_i^j(x) \equiv x^{N(\mathfrak{p})^j} \mod \mathfrak{P}_i$. But we just saw that $\sigma_i^j\tau$ corresponds to an element of the Galois group of the extension $(\mathcal{O}_K/\mathfrak{P}_i)/(\mathcal{O}_F/\mathfrak{q}_i)$ which is a cyclic group generated by the Frobenius automorphism $\phi_i : x \mapsto x^{N(\mathfrak{p})^{f_i}}$. Thus $\sigma_i^j\tau$ is some power of ϕ_i. This implies that f_i divides j.

Suppose that this is the case. The element ϕ_i is characterized by the fact that $\phi_i(x) \equiv x^{N(\mathfrak{p})^{f_i}} \mod \mathfrak{P}_i$ for x in $\mathcal{O}_K$. Thus $\sigma_i^j\tau$ and ϕ^{j/f_i} have the exact same effect on $\mathcal{O}_K/\mathfrak{P}_i$ and they both belong to $D_i \cap H$. They therefore share the same coset of $I_i \cap H$. This implies that

$$\sigma_i^j I_i \cap H \subset \phi_i^{j/f_i}(I_i \cap H).$$

If τ belongs to $I_i \cap H$ then for all $x \in \mathcal{O}_K$, $\phi_i^{k/f_i}\tau(x) \equiv \phi_i^{k/f_i}(x) \mod \mathfrak{P}_i \equiv x^{N(p)^j} \mod \mathfrak{P}_i$ and therefore $\phi_i^{j/f_i}\tau$ has the same effect as σ_i^j. Both belong to D_i and thus share the same coset of I_i. Since $\phi_i^{j/f_i}\tau$ also belongs to H, we get $\phi_i^{j/f_i}(I_i \cap H) \subset \sigma_i^j I_i \cap H$ and this finishes the proof. □

2.3 The Artin Map

Let K/k be a finite abelian extension of number fields with Galois group G. Let $\mathfrak{p}$ be an unramified prime ideal of k. By Proposition 10 and Proposition 12, the decomposition group $D_{\mathfrak{P}}$, the inertia group $I_{\mathfrak{P}}$ and the Frobenius element $(\mathfrak{P}, K/k)$ do not depend on the prime $\mathfrak{P}$ dividing $\mathfrak{p}$ since we are in the case where G is an abelian group. We will therefore use the notation $D_{\mathfrak{p}}$, $I_{\mathfrak{p}}$ and $(\mathfrak{p}, K/k)$.

Let $\mathfrak{m}$ be a modulus of K that is divisible by all prime ideals of $\mathcal{O}_k$ that ramify in k. Let $\mathfrak{p}$ be a prime ideal that does not divide $\mathfrak{m}$. Since it is unramified in K, the inertia group $I_{\mathfrak{p}}$ is trivial and the Frobenius element $(\mathfrak{p}, L/K)$ is an element of the decomposition group $D_{\mathfrak{p}}$. In this case, $(\mathfrak{p}, K/k)$ is also called the Artin symbol of $\mathfrak{p}$. We extend the notion of Artin symbol to $I_k(\mathfrak{m})$ multiplicatively. Explicitly, if $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$ is a fractional ideal in $I_k(\mathfrak{m})$, then all the primes in its decomposition are unramified and we may define its Artin symbol by

$$(\mathfrak{a}, K/k) = \prod_{\mathfrak{p}} (\mathfrak{p}, K/k)^{v_{\mathfrak{p}}(\mathfrak{a})} \in G.$$

Definition 8. With the above notations, the group homomorphism

$$\Phi_{K/k,\mathfrak{m}} : I_k(\mathfrak{m}) \longrightarrow \mathrm{Gal}(K/k), \qquad \mathfrak{a} \longmapsto (\mathfrak{a}, K/k)$$

is called the reciprocity law map or the Artin map of K/k relative to the modulus $\mathfrak{m}$.

Notice that if $\mathfrak{p}$ is unramified in K/k, then $(\mathfrak{p}, K/k)$ is trivial if and only if $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$ is trivial, that is, if and only if $f_{\mathfrak{p}} = 1$. So $\mathfrak{p}$ has trivial Artin symbol if and only if $\mathfrak{p}$ splits completely in K/k.

2.4 Main Results

Before stating the theorems, we make the following definition:

Definition 9. Let K/k be a finite extension of number fields. If v is an infinite real prime of k, then we say that v is unramified or that it splits in K/k if for every extension τ of σ_v to K we have $\tau(K) \subset \mathbb{R}$. A complex infinite prime of k is always said to be unramified or split.

The first theorem of class field theory is due to Artin and says that the Galois group of any finite abelian extension of number fields is a generalized ideal class group for some modulus of k. The precise statement is as follows:

Theorem 2.4.1 (Artin Reciprocity)**.** *Let K/k be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus of k containing all primes, finite or infinite, that ramify in K. The following statements concerning the Artin map are true:*

(i) The map $\Phi_{K/k,\mathfrak{m}}$ is surjective.

(ii) If the exponents $m(v)$ of the modulus $\mathfrak{m}$ are sufficiently large, then the kernel of $\Phi_{K/k,\mathfrak{m}}$ is a congruence subgroup for $\mathfrak{m}$, that is,

$$P_{k,1}(\mathfrak{m}) \subset \ker(\Phi_{K/k,\mathfrak{m}}) \subset I_k(\mathfrak{m}).$$

The isomorphism

$$I_k(\mathfrak{m})/\ker(\Phi_{K/k,\mathfrak{m}}) \xrightarrow{\sim} \mathrm{Gal}(K/k)$$

shows that $\mathrm{Gal}(K/k)$ *is a generalized ideal class group for* $\mathfrak{m}$.

Suppose that K/k is a finite abelian extension and that $\mathrm{Gal}(K/k)$ is a generalized ideal class group for a modulus $\mathfrak{m}$. Let $\mathfrak{n}$ be a modulus of k that is divisible by $\mathfrak{m}$. It is clear that $P_{k,1}(\mathfrak{n}) \subset P_{k,1}(\mathfrak{m})$ and $I_k(\mathfrak{n}) \subset I_k(\mathfrak{m})$. The map $\Phi_{K/k,\mathfrak{n}}$ is the restriction of the map $\Phi_{K/k,\mathfrak{m}}$ to $I_k(\mathfrak{n})$ so that $\ker(\Phi_{K/k,\mathfrak{n}}) = \ker(\Phi_{K/k}, \mathfrak{m}) \cap I_k(\mathfrak{n})$ contains $P_{k,1}(\mathfrak{m}) \cap I_k(\mathfrak{n})$ which contains $P_{k,1}(\mathfrak{n})$. Therefore, we have

$$P_{k,1}(\mathfrak{n}) \subset \ker(\Phi_{K/k,\mathfrak{n}}) \subset I_k(\mathfrak{n}).$$

This proves that $\mathrm{Gal}(K/k)$ is a generalized ideal class group for infinitely many moduli. But as the following theorem shows, there is a preferred modulus.

Theorem 2.4.2 (Conductor Theorem)**.** *Let K/k be a finite abelian extension of number fields. There exists a modulus $\mathfrak{f} = \mathfrak{f}(K/k)$, called the conductor of K/k, such that:*

(i) A prime of k, finite or infinite, ramifies in K if and only if it divides $\mathfrak{f}$.

(ii) Let $\mathfrak{m}$ be a modulus of k divisible by all primes, finite or infinite, that ramify in K. Then $\ker(\Phi_{K/k}, \mathfrak{m})$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f}$ divides $\mathfrak{m}$.

To the Galois group of any finite abelian extension of number fields, one can associate a congruence subgroup given a suitable choice of modulus. The following theorem gives a converse result:

Theorem 2.4.3 (Existence Theorem)**.** *Let k be a number field, $\mathfrak{m}$ a modulus of k and H a congruence subgroup for $\mathfrak{m}$. There exists a unique abelian extension K/k all of whose primes that ramify divide $\mathfrak{m}$ and such that $H = \ker(\Phi_{K/k,\mathfrak{m}})$.*

Given the above results of class field theory we deduce the following.

Corollary 7. *Let K/k and L/k be two finite abelian extension of the number field k. Then $K \subset L$ if and only if there exists a modulus $\mathfrak{m}$ of k divisible by all primes in k that ramify in either K or L such that*

$$P_{k,1}(\mathfrak{m}) \subset \ker(\Phi_{L/k}, \mathfrak{m}) \subset \ker(\Phi_{K/k}, \mathfrak{m}).$$

Proof. Suppose that $K \subset L$ and consider the restriction map

$$r_K : \mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K/k)$$

that has kernel equal to $\mathrm{Gal}(L/K)$. By Theorem 2.4.1, there exists a modulus $\mathfrak{m}$ of k divisible by all primes that ramify in L and such that

$$P_{k,1}(\mathfrak{m}) \subset \ker(\Phi_{L/k,\mathfrak{m}}).$$

If a prime of k ramifies in K, then it also ramifies in L. Thus $\mathfrak{m}$ contains all primes that ramify in K. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_k$ that is unramified in L. Then it is also unramified in K and by Proposition 13 we have $r_K((\mathfrak{p}, L/k)) = (\mathfrak{p}, K/k)$. This implies that $r_K \circ \Phi_{L/k,\mathfrak{m}} = \Phi_{K/k,\mathfrak{m}}$ and therefore $\ker(\Phi_{K/k,\mathfrak{m}}) = \Phi^{-1}_{L/k,\mathfrak{m}}(\mathrm{Gal}(L/K))$. The latter implies in particular that $\ker(\Phi_{K/k,\mathfrak{m}})$ contains $\ker(\Phi_{L/k,\mathfrak{m}})$. This proves that

$$P_{k,1}(\mathfrak{m}) \subset \ker(\Phi_{L/k,\mathfrak{m}}) \subset \ker(\Phi_{K/k,\mathfrak{m}})$$

as desired.

Conversely, suppose that the above inclusions hold for a certain modulus $\mathfrak{m}$. This implies that $\ker(\Phi_{K/k,\mathfrak{m}})$ is a congruence subgroup for the modulus $\mathfrak{m}$. Define $H = \Phi_{L/k,\mathfrak{m}}(\ker(\Phi_{K/k,\mathfrak{m}}))$. This is a normal subgroup of the group $\mathrm{Gal}(L/k)$ since the latter is abelian. Hence the fixed field $L^H \subset L$ is an abelian extension of k. By the reasoning of the first part,

$$\ker(\Phi_{L^H/k}, \mathfrak{m}) = \Phi_{L/k,\mathfrak{m}}^{-1}(H) = \ker(\Phi_{L/k,\mathfrak{m}}).\ker(\Phi_{K/k,\mathfrak{m}}) = \ker(\Phi_{K/k,\mathfrak{m}}),$$

where in the last equality we used the inclusion $\ker(\Phi_{L/k,\mathfrak{m}}) \subset \ker(\Phi_{K/k,\mathfrak{m}})$. By the uniqueness part of Theorem 2.4.3, we must have $K = L^H$ and in particular $K \subset L$. □

2.5 Ray Class Fields

Let k be a number field and let $\mathfrak{m}$ be a modulus of k. Then $P_{k,1}(\mathfrak{m})$ is a particularly simple example of a congruence subgroup for $\mathfrak{m}$. Theorem 2.4.3 ensures that there exists a unique abelian extension of k, say $k(\mathfrak{m})$, that has the following properties:

- All primes of k that ramify in $k(\mathfrak{m})$ divide $\mathfrak{m}$.
- The kernel of the Artin map $\Phi_{k(\mathfrak{m})/k,\mathfrak{m}}$ is $P_{k,1}(\mathfrak{m})$.

The second property and Theorem 2.4.1 ensure that we have the exact sequence

$$1 \longrightarrow P_{k,1}(\mathfrak{m}) \longrightarrow I_k(\mathfrak{m}) \longrightarrow \mathrm{Gal}(k(\mathfrak{m})/k) \longrightarrow 1.$$

In particular, the $\mathfrak{m}$-ray class group $\mathrm{Cl}_k(\mathfrak{m})$ is isomorphic via the Artin map to $\mathrm{Gal}(K(\mathfrak{m})/K)$. As a consequence, the field $k(\mathfrak{m})$ is referred to as the $\mathfrak{m}$-ray class field of k.

Proposition 14. *Let K/k be a finite abelian extension of number fields. There exists a modulus $\mathfrak{m}$ of k such that $K \subset k(\mathfrak{m})$. In particular, K is a subfield of $k(\mathfrak{n})$ for any modulus $\mathfrak{n}$ divisible by $\mathfrak{m}$. Moreover, the conductor of K/k is the smallest modulus for which K is a subfield of the corresponding ray class field.*

Proof. By Theorem 2.4.1, there exists a modulus $\mathfrak{m}$ such that

$$P_{k,1}(\mathfrak{m}) = \ker(\Phi_{k(\mathfrak{m})/k,\mathfrak{m}}) \subset \ker(\Phi_{K/k,\mathfrak{m}})$$

and then by Corollary 7 K is a subfield of $k(\mathfrak{m})$. This proves that if $\mathrm{Gal}(K/k)$ is a congruence subgroup for some modulus, then K is a subfield of the corresponding ray class field. Since $\mathrm{Gal}(K/k)$ is a congruence subgroup for any modulus $\mathfrak{n}$ divisible by $\mathfrak{m}$ the result follows. The final statement is clear from Theorem 2.4.2. □

A consequence of Proposition 14 is that the description of the ray class fields of a given number field provide a good description of the finite abelian extensions of this field. In the next example, we shall give the ray class fields in the simplest case $k = \mathbb{Q}$.

Example 2. Let m be an integer larger or equal to 3 that is either odd or divisible by 4 so that $\phi(m)$ is even. Here, ϕ denotes the Euler totient function. Let ζ be a primitive m-th root of unity and consider the cyclotomic extension

$\mathbb{Q}(\zeta)/\mathbb{Q}$. It is well known that this extension is abelian of degree $\phi(m)$ with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$. Also, it is known that $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ and the absolute discriminant is

$$d_{\mathbb{Q}(\zeta)} = \frac{(-1)^{\phi(m)/2} m^{\phi(m)}}{\prod_{p|m} p^{\phi(m)/(p-1)}}. \tag{2.5.0.1}$$

The latter implies that the primes p that ramify in $\mathbb{Q}(\zeta)$ all divide m. Moreover, since m is greater than 3, the infinite place v_∞ of $\mathbb{Q}$ ramifies in $\mathbb{Q}(\zeta)$. Therefore, the modulus $\mathfrak{m} = m\mathbb{Z}v_\infty$ contains all ramified primes of $\mathbb{Q}$ in $\mathbb{Q}(\zeta)$. Consider the composition map

$$\begin{array}{ccccc} I_{\mathbb{Q}}(\mathfrak{m}) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ \left(\frac{a}{b}\right)_+ \mathbb{Z} & \longmapsto & ab^{-1} \mod m & & \\ & & a \mod m & \longmapsto & (\sigma_a : \zeta \mapsto \zeta^a). \end{array}$$

This is the Artin map $\Phi_{\mathbb{Q}(\zeta)/\mathbb{Q},\mathfrak{m}}$. By Example 1, its kernel is $P_{\mathbb{Q},1}(\mathfrak{m})$. Thus $\mathbb{Q}(\zeta)$ is the $(m\mathbb{Z}v_\infty)$-ray class field of $\mathbb{Q}$.

Let $K = \mathbb{Q}(\zeta)^+$ be the maximal real subfield of $\mathbb{Q}(\zeta)$. Every field homomorphism of K into $\bar{K}$ is obtained by restricting $\sigma_a : \zeta \mapsto \zeta^a$ to K for some $a \in (\mathbb{Z}/m\mathbb{Z})^*$. A basis of $\mathbb{Q}(\zeta)$ as a $\mathbb{Q}$-vector space is given by $1, \zeta, \ldots, \zeta^{\phi(m)-1}$. If $x \in K$, then there exist rational numbers λ_l such that $x = \sum_l \lambda_l \zeta^l$. If τ denotes complex conjugation, then

$$\tau(\sigma_a(x)) = \tau\left(\sum_l \lambda_l \zeta^{la}\right) = \sum_l \lambda_l \tau(\zeta)^{la} = \sigma_a(\tau(x)). \tag{2.5.0.2}$$

Since x is real we have $\tau(x) = x$ and therefore $\tau(\sigma_a(x)) = \sigma_a(x)$ so that $\sigma_a(x)$ is also real. Thus $\sigma_a(K)$ is a real subfield of $\mathbb{Q}(\zeta)$ and must therefore by definition of K be contained in K. This proves that $K/\mathbb{Q}$ is a normal extension and thus abelian. Moreover, since ζ is a root of unity its absolute value is 1 and its inverse is $\tau(\zeta)$. By (2.5.0.2) it follows that $\sigma_a(x) = \sigma_{-a}(x)$ so that $\sigma_a|_K = \sigma_{-a}|_K$. As a consequence, the Galois group G of $K/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$ and the degree of the extension is $\phi(m)/2$. Let p be a prime number. If p does not divide m, then p is unramified in $\mathbb{Q}(\zeta)$ and therefore also unramified in K. Thus a prime that ramifies in K must divide m. Moreover, since K is totally real the infinite prime v_∞ is unramified in K. Thus, all primes that ramify in K divide m. Finally, the composition map

$$\begin{array}{ccccc} I_{\mathbb{Q}}(m\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\} & \longrightarrow & \mathrm{Gal}(K/\mathbb{Q}) \\ \frac{a}{b}\mathbb{Z} & \longmapsto & [ab^{-1} \mod m] & & \\ & & [a \mod m] & \longmapsto & (\sigma_a|_K : \zeta \mapsto \zeta^a). \end{array}$$

is the Artin map $\Phi_{K/\mathbb{Q},m\mathbb{Z}}$ and by Example 1 its kernel is $P_{\mathbb{Q},1}(m\mathbb{Z})$. We conclude that K is the $m\mathbb{Z}$-ray class field of $\mathbb{Q}$.

We now show how class field theory can be used to prove the famous:

Theorem 2.5.1 (Kronecker-Weber)**.** *Any finite abelian extension of $\mathbb{Q}$ is a subfield of some cyclotomic field $\mathbb{Q}(\zeta)$.*

Proof. Let $K/\mathbb{Q}$ be a finite abelian extension. By Proposition 14 there exists a modulus $\mathfrak{m}$ of $\mathbb{Q}$ such that K is a subfield of $\mathbb{Q}(\mathfrak{m})$ and this is true for all moduli divisible by $\mathfrak{m}$. In particular, it is true for some modulus of the form $(m\mathbb{Z}v_\infty)$. By Example 2, $\mathbb{Q}(m\mathbb{Z}v_\infty) = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity and the proof is complete. □

We remark that the Kronecker-Weber Theorem was proved long before the development of the theory of class fields. The result was stated by Kronecker in 1853 and proved by Weber in 1886. It can be viewed as the starting point of what is today known as class field theory.

If k is a number field, a particularly interesting ray class field is the one corresponding to the empty modulus $\mathtt{1}$ of k. This field is called the Hilbert class field of k and is often denoted by H_k or simply H when there is no risk of confusion.

Proposition 15. *Let k be a number field. The Hilbert class field H_k has the following properties:*

(i) It is the maximal everywhere unramified abelian extension of k.

(ii) Its Galois group $\mathrm{Gal}(H_k/k)$ is isomorphic to the ideal class group $\mathrm{Cl}(\mathcal{O}_k)$ of k via the Artin map.

(iii) A prime ideal splits completely in H_k/k if and only if it is a principal ideal of $\mathcal{O}_k$.

Proof. By definition of the ray class field, every prime that ramifies in H_k must divide the modulus $\mathtt{1}$. Thus, no prime of k is ramified in H_k. In other words, H_k is totally unramified. If K is any finite abelian extension of k that is unramified everywhere, then by Theorem 2.4.2 (*i*), the conductor of K/k must be $\mathtt{1}$. By Proposition 14, K is a subfield of H_k. Therefore, H_K is indeed the maximal totally unramified abelian extension of K.

The second claim follows from the fact that $I_k(\mathtt{1}) = I_k$ and $P_{k,1}(\mathtt{1}) = P_k$ so that $\mathrm{Cl}_k(\mathtt{1}) = \mathrm{Cl}(\mathcal{O}_k)$.

A prime splits completely if and only if its Artin symbol $(\mathfrak{p}, H_k/k)$ is trivial which is true if and only if $\mathfrak{p}$ belongs to the kernel of the Artin map $\Phi_{H_k/k,\mathtt{1}}$. But this kernel is P_k hence the result. □

Chapter 3

Linear Representations of Finite Groups

We give an introduction to the theory of finite-dimensional complex linear representations of finite groups. We closely follow the exposition in [Se1]. In this section, by representation or linear representation we mean finite-dimensional complex linear representation.

3.1 Definition and First Properties

Let G be a finite group. A linear representation of G is a finite-dimensional complex vector space V together with a homomorphism of groups $\rho : G \longrightarrow \mathrm{GL}(V)$. A representation of G will most often simply be referred to by V, keeping the homomorphism ρ implicit. When in need of specifying the homomorphism we will talk about the representation (ρ, V).

The homomorphism ρ gives a left action of G on V defined by

$$G \times V \longrightarrow V, \qquad (\sigma, v) \longmapsto \rho(\sigma)(v).$$

We will often denote the action of σ on v simply by σv. Consequently V has the structure of a finite-dimensional complex vector space and a left G-module and these two actions commute: V is a finite-dimensional left $\mathbb{C}[G]$-module where $\mathbb{C}[G]$ denotes the group ring of G over $\mathbb{C}$. This is a free $\mathbb{C}$-vector space whose basis is one-to-one with G. It is a ring with multiplication extending linearly the one of G. As a $\mathbb{C}$-algebra it is isomorphic to $\bigoplus_{\sigma \in G} \mathbb{C}\sigma$.

Conversely, a finite-dimensional $\mathbb{C}[G]$-module is a linear representation of G. Both points of view will turn out to have their advantages. The words $\mathbb{C}[G]$-module and representation will be used interchangeably and both will implicitly contain "finite-dimensional".

Remark 9. Let V be a $\mathbb{C}[G]$-module. An element α of $\mathbb{C}[G]$ can be viewed a $\mathbb{C}$-linear map $\alpha : V \longrightarrow V$. In order for this map to be a $\mathbb{C}[G]$-homomorphism, it is necessary and sufficient that α be central in $\mathbb{C}[G]$, that is, for all $\beta \in \mathbb{C}[G]$, we have $\alpha\beta = \beta\alpha$. It even suffices to check this only in the case $\beta \in G$ since $\mathbb{C}$ is commutative.

Let G be a group. Two representations V_1 and V_2 of G are said to be isomorphic if they are isomorphic as $\mathbb{C}[G]$-modules. In other words, there exists an isomorphism $f : V_1 \longrightarrow V_2$ of $\mathbb{C}$-vector spaces such that for all $\sigma \in G$ and all $x \in V_1$, we have $\sigma f(x) = f(\sigma x)$.

Another remark concerning the definition of a linear representation is that upon choosing a basis for the n-dimensional complex vector space V, we can identify $\mathrm{GL}(V)$ with $\mathrm{GL}_n(\mathbb{C})$, the set of all $n \times n$ invertible matrices with coefficients in $\mathbb{C}$.

Let V_1 and V_2 be two representations of G and let $f : V_1 \longrightarrow V_2$ be an isomorphism. Choose bases for V_1 and V_2 and let $R_1(\sigma)$ and $R_2(\sigma)$ denote the respective matrices in $\mathrm{GL}(V_1)$ and in $\mathrm{GL}(V_2)$ of $\sigma \in G$. Let A denote the matrix of f with respect to these bases. Then the fact that f is an isomorphism of representations tells us that $R_1(\sigma) = A^{-1}R_2(\sigma)A$ for all $\sigma \in G$.

Let G be a finite group and let V be a representation. A subrepresentation W of V is a sub-$\mathbb{C}[G]$-module of V. In other words, W is a sub-vector space of V that is stable under the action of G.

Proposition 16. *Let G be a finite group. Then $\mathbb{C}[G]$ is a semisimple ring.*

Proof. It is enough to prove that any left $\mathbb{C}[G]$-module is semisimple (cf. [Ro2], Chapter 4, Proposition 4.5). So let V be a left $\mathbb{C}[G]$-module. Showing that V is semisimple is equivalent to proving that every sub-module of V is a direct summand (cf. [Ro2], Chapter 4, Proposition 4.1). Let therefore W be a sub-$\mathbb{C}[G]$-module of V. In particular, W is a sub-vector space of V so there is a projection map $p : V \longrightarrow W$, that is, a $\mathbb{C}$-linear map such that $p(x) = x$ for all $x \in W$ and $p(V) = W$. Let g denote the order of G and define

$$p^0 = \frac{1}{g}\sum_{\sigma\in G} \sigma p \sigma^{-1} : V \longrightarrow V.$$

We claim that $p^0(V) = W$. In fact, let $v \in V$. Then $p(\sigma^{-1}v) \in W$ since p is a projection and $\sigma(p(\sigma^{-1}v)) \in W$ since W is stable under the action of σ. Let $w \in W$. Since W is stable under the action of σ^{-1}, we have $\sigma^{-1}w \in W$. Since p is a projection onto W we have $p(\sigma^{-1}w) = \sigma^{-1}w$ so that $p^0(w) = w$. This proves that p^0 is a projection onto W.

We now prove that p^0 is a $\mathbb{C}[G]$-module homomorphism. The actions of $\mathbb{C}$ and of G on V commute and p is $\mathbb{C}$-linear. We conclude that p^0 is also $\mathbb{C}$-linear. Let $\tau \in G$. Then for all $v \in V$ we have

$$\tau p^0(v) = \frac{1}{g}\sum_{\sigma\in G} \tau\sigma p(\sigma^{-1}v) = \frac{1}{g}\sum_{\eta\in G} \eta p \eta^{-1}\tau v = p^0(\tau v)$$

where we performed the change of variables $\eta = \tau\sigma$. We conclude that p^0 is a $\mathbb{C}[G]$-module homomorphism. If $W^0 = \ker(p^0)$, then we have an exact sequence of $\mathbb{C}[G]$-modules

$$0 \longrightarrow W^0 \longrightarrow V \xrightarrow{p^0} W \longrightarrow 0.$$

Let $i : W \hookrightarrow V$ be the inclusion. Then $p^0 \circ i = \mathrm{id}|_W$ so i is a section and the sequence splits and $V = W \oplus W^0$. We conclude that W is a direct summand of V. □

Remark 10. Semisimple rings R are specially nice to work with since every short exact sequence of left (or right) R-modules splits and every left (or right) R-module is semisimple and projective (cf. [Ro2], Chapter 4, Proposition 4.5). In particular, every left (or right) R-module is flat.

Definition 10. Let G be a finite group. A representation V of G is said to be irreducible if it is simple as a $\mathbb{C}[G]$-module.

Corollary 8. *Every representation V of G can be written as a finite direct sum of irreducible representations.*

Proof. In fact, $\mathbb{C}[G]$ is a semisimple ring so the $\mathbb{C}[G]$-module V is semisimple as a module. By definition of semisimplicity, it can be written as a direct sum of simple sub-modules (or irreducible representations). Since V is finite dimensional over $\mathbb{C}$, the representation V can be written as a finite sum. □

Remark 11. One can ask if the decomposition of a representation V into a direct sum of irreducible representations is unique. We quickly realize that this is not the case: suppose that the action of G on V is trivial. Then each irreducible component of V is a one-dimensional complex vector space and there are many ways to decompose a vector space into a direct sum of lines.

3.2 Character of a Representation

Let G be a finite group. Let (ρ, V) be a representation of G of dimension n. If we choose a basis of V over $\mathbb{C}$, then $\rho(\sigma)$ becomes an $n \times n$ invertible matrix with coefficients in $\mathbb{C}$ and we can define the trace and the determinant of $\rho(\sigma)$ as a matrix. These quantities associated to σ are independent of the choice of basis since changing basis leads to a matrix that is conjugated with respect to the previous one. We can therefore speak of the trace and the determinant of $\rho(\sigma)$ without ambiguity.

With this in mind, we define the character associated to the representation (ρ, V) to be the complex valued function

$$\chi : G \longrightarrow \mathbb{C}, \qquad \sigma \longmapsto \mathrm{tr}(\rho(\sigma)).$$

If the dimension of V is n, then χ is a said to be of dimension n and if V is irreducible as a representation, then χ is said to be an irreducible character.

Note that if (ρ_1, V_1) and (ρ_2, V_2) are two isomorphic representations of G with respective characters χ_1 and χ_2, then $\chi_1 = \chi_2$. In fact, we noted in the previous section that in the given case, the matrices $\rho_1(\sigma)$ and $\rho_2(\sigma)$ are conjugates and therefore their traces coincide. Later we will see the converse: if two representations of G have the same character, then they are isomorphic as representations. Thus the study of representations reduces to the study of characters of G.

We remark that a representation V of dimension 1 coincides with its character χ. In this case, $\chi : G \longrightarrow \mathbb{C}^*$ is a homomorphism of groups which takes values on the unit circle S^1 since G is finite.

In what follows we use the notation $\bar{z}$ to mean the complex conjugate of the element z.

Proposition 17. *Let G be a finite group and let (ρ, V) be a representation with character χ. We have the following properties:*

(i) $\chi(1) = \dim_{\mathbb{C}} V$.

(ii) $\chi(\sigma^{-1}) = \bar{\chi}(\sigma)$ *for all* $\sigma \in G$.

(iii) $\chi(\tau\sigma\tau^{-1}) = \chi(\sigma)$ *for all* $\sigma, \tau \in G$.

Proof. By definition we have $\chi(1) = \operatorname{tr}(\rho(1)) = \operatorname{tr}(\mathrm{id}) = \dim_{\mathbb{C}} V$. For the second assertion, let $\lambda_i(\sigma)$ denote the eigenvalues of $\rho(\sigma)$ for $\sigma \in G$. Since ρ is a homomorphism and G is finite, the matrix $\rho(\sigma)$ is of finite order and it follows that the same is true for the eigenvalues. In particular, $|\lambda_i(\sigma)| = 1$ so that $\lambda_i(\sigma)^{-1} = \overline{\lambda_i(\sigma)}$. Thus,

$$\chi(\sigma^{-1}) = \operatorname{tr}(\rho(\sigma)^{-1}) = \sum_i \lambda_i(\sigma)^{-1} = \sum_i \overline{\lambda_i(\sigma)} = \bar{\chi}(\sigma).$$

The last assertion follows directly from the fact that the trace operator commutes pairs of elements. □

Let χ be a character of G and denote by $\mathbb{Q}(\chi)$ the finite field extension of $\mathbb{Q}$ obtained by adjoining to $\mathbb{Q}$ all the values $\chi(\sigma)$ for $\sigma \in G$.

Proposition 18. *Let* χ *be a character of a representation* (ρ, V) *of* G. *Then* $\mathbb{Q}(\chi)$ *is an abelian extension of* $\mathbb{Q}$.

Proof. Denote by $\lambda_i(\sigma)$ the eigenvalues of $\rho(\sigma)$. Let g denote the order of G. Then $\lambda_i(\sigma)$ is a g-th root of unity for all i and all σ. Let ζ denote a primitive g-th root of unity. Then $\mathbb{Q}(\chi)$ is contained in the cyclotomic field $\mathbb{Q}(\zeta)$ and every embedding of $\mathbb{Q}(\chi)$ into $\mathbb{C}$ is the restriction to $\mathbb{Q}(\chi)$ of $\sigma_a : \zeta \longmapsto \zeta^a$ for some $a \in (\mathbb{Z}/g\mathbb{Z})^*$. We have

$$\sigma_a(\chi(\sigma)) = \sum_i \sigma_a(\lambda_i(\sigma)) = \sum_i \lambda_i(\sigma)^a = \chi(\sigma^a) \in \mathbb{Q}(\chi)$$

so that $\mathbb{Q}(\chi)/\mathbb{Q}$ is a normal extension and thus Galois. It is a subextension of the abelian extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ and is therefore itself abelian. □

3.3 Representations of Quotient Groups

Let G be a finite group and let H be a normal subgroup of G. Let V be a representation of the group G/H. This is a finite-dimensional $\mathbb{C}[G/H]$-module. The natural quotient map $G \longrightarrow G/H$ endows G/H with the structure of a G-module. This G-module structure on G/H gives a G-module structure on V, making it into a representation of G. Denote this new representation by $\mathrm{Infl}_H^G V$ or simply $\mathrm{Infl}V$ and call it the inflation of V. Note that

$$\mathrm{Infl} : {}_{\mathbb{C}[G/H]}\mathbf{Mod} \longrightarrow {}_{\mathbb{C}[G]}\mathbf{Mod}$$

is an exact functor from the category of left $\mathbb{C}[G/H]$-modules to the category of left $\mathbb{C}[G]$-modules.

We denote by $\mathrm{Infl}\chi$ the character of $\mathrm{Infl}V$ which is given by the diagram

$$\mathrm{Infl}\chi : G \longrightarrow G/H \xrightarrow{\chi} \mathbb{C}.$$

Conversely, starting with a representation V of G we would like to define a representation of G/H. Consider the subspace V^H of H-invariants. Explicitly, we have

$$V^H = \{v \in V \; : \; \sigma x = x \text{ for all } \sigma \in H\}.$$

This is a sub-$\mathbb{C}[G]$-module of V. In fact, let $\sigma \in H$ and $\tau \in G$. Since H is normal in G, there exists $\sigma' \in H$ such that $\sigma\tau = \tau\sigma'$. Hence, if $v \in V^H$ then $\sigma(\tau v) = \tau(\sigma' v) = \tau v$ and $\tau v \in V^H$. So we have a homomorphism $G \longrightarrow \mathrm{GL}(V^H)$. The kernel of this map contains H so this map factors through H and gives a homomorphism $G/H \longrightarrow \mathrm{GL}(V^H)$. In other words, V^H is a representation of G/H. If χ is the character of V, then we denote by χ^H the character of V^H. If $\sigma \in G$, then we shall use the notation $[\sigma]$ to denote the image of σ in G/H.

Consider $\mathbb{Z}$ as an H-module, the action of H being trivial. Let $\mathrm{Hom}_H(\mathbb{Z}, V)$ denote the set of H-module homomorphisms $f : \mathbb{Z} \longrightarrow V$. This a group under addition and inherits the structure of a $\mathbb{C}[G]$-module from V. Explicitly, the action of an element $x \in \mathbb{C}[G]$ is defined by $(xf)(n) = xf(n)$ where the right hand side makes use of the action of $\mathbb{C}[G]$ on V. The action of H on $\mathrm{Hom}_H(\mathbb{Z}, V)$ is trivial since for $\sigma \in H$ we have $(\sigma f)(n) = f(\sigma n) = f(n)$. Therefore $\mathrm{Hom}_H(\mathbb{Z}, V)$ has the structure of a G/H-module. Note that an element $f \in \mathrm{Hom}_H(\mathbb{Z}, V)$ is uniquely determined by the image $f(1)$ in V. Moreover, as an element of V, $f(1)$ is fixed by H. We therefore have a bijection of sets between $\mathrm{Hom}_H(\mathbb{Z}, V)$ and V^H which is a $\mathbb{C}[G/H]$-module isomorphism.

Note that

$$(-)^H = \mathrm{Hom}_H(\mathbb{Z}, -) : \;{}_{\mathbb{C}[G]}\mathbf{Mod} \longrightarrow \;{}_{\mathbb{C}[G/H]}\mathbf{Mod}$$

is a covariant left-exact functor from the category of left $\mathbb{C}[G]$-modules to the category of left $\mathbb{C}[G/H]$-modules.

Proposition 19. *Let G be a finite group and H a normal subgroup of G. Define*

$$N_H = \frac{1}{|H|} \sum_{\tau \in H} \tau \in \mathbb{C}[H].$$

This is a central element of $\mathbb{C}[G]$. Moreover, if V is a representation of G, then N_H acts on V as the projection onto V^H.

Proof. We check that this is a central element of $\mathbb{C}[G]$. In fact, if $\sigma \in G$ then we have

$$\sigma N_H = \frac{1}{|H|} \sum_{\tau \in H} \sigma\tau = \frac{1}{|H|} \sum_{\tau' \in G} \tau'\sigma = N_H \sigma$$

where we performed the change of variables $\tau' = \sigma\tau\sigma^{-1}$ and used the fact that the subgroup H is normal to deduce that $\tau' \in H$. Note that if $\sigma \in H$, then $\sigma N_H = N_H \sigma = N_H$. Moreover, if $v \in V^H$ then $N_H v = v$. Thus the action of N_H on V is the projection onto V^H. □

Corollary 9. *Let G be a finite group and H a normal subgroup of G. Let V be a representation of G with character χ. For $\sigma \in G$ we have*

$$\chi^H([\sigma]) = \frac{1}{|H|} \sum_{\tau \in H} \chi(\tau\sigma) = \frac{1}{|H|} \sum_{\tau \in H} \chi(\sigma\tau).$$

Proof. We compute that

$$\chi^H([\sigma]) = \mathrm{tr}([\sigma]N_H) = \mathrm{tr}(N_H\sigma) = \frac{1}{|H|}\sum_{\tau\in H}\mathrm{tr}(\tau\sigma) = \frac{1}{|H|}\sum_{\tau\in H}\chi(\tau\sigma).$$

The last equality is obtained by change of variables and by using the fact that H is a normal subgroup. □

Corollary 10. *Let G be a finite group and H a normal subgroup of G. Let V be a representation of G with character χ. We have*

$$\dim_{\mathbb{C}} V^H = \frac{1}{|H|}\sum_{h\in H}\chi(h).$$

Proof. By Corollary 9 we have $\chi^H([\sigma]) = \frac{1}{|H|}\sum_{\tau\in H}\chi(\sigma\tau)$ and by Proposition 17 (i) we have

$$\dim_{\mathbb{C}} V^H = \chi^H([1]) = \frac{1}{|H|}\sum_{\tau\in H}\chi(\tau).$$

□

3.4 Representations of Subgroups

Let G be a finite group and let H be a subgroup of G. Let V be a representation of G. This is a $\mathbb{C}[G]$-module. The natural inclusion $H \hookrightarrow G$ endows G with an H-module structure. Consequently, this inclusion gives V the structure of a $\mathbb{C}[H]$-module. In other words, V is a representation of H. This representation will be denoted $\mathrm{Res}V$ or $\mathrm{Res}_H^G V$. Note that

$$\mathrm{Res} : {}_{\mathbb{C}[G]}\mathbf{Mod} \longrightarrow {}_{\mathbb{C}[H]}\mathbf{Mod}$$

is an exact functor from the category of left $\mathbb{C}[G]$-modules to the category of left $\mathbb{C}[H]$-modules. If χ is the character of V, then we denote by $\mathrm{Res}\chi$ the character of $\mathrm{Res}V$ given by the diagram

$$\mathrm{Res}\chi : H \hookrightarrow G \xrightarrow{\chi} \mathbb{C}.$$

Conversely, given a representation V of H we would like to define a representation of G. In other words, given a $\mathbb{C}[H]$-module V, we would like to give it a $\mathbb{C}[G]$-module structure. The answer to this problem is provided by the tensor product of modules and we define the induced representation $\mathrm{Ind}V$ or $\mathrm{Ind}_H^G V$ to be

$$\mathrm{Ind}V := \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V.$$

By properties of the tensor product, $\mathrm{Ind}V$ is uniquely defined up to isomorphism. Note that

$$\mathrm{Ind} = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} - : {}_{\mathbb{C}[H]}\mathbf{Mod} \longrightarrow {}_{\mathbb{C}[G]}\mathbf{Mod}$$

is an exact functor from the category of left $\mathbb{C}[H]$-modules to the category of left $\mathbb{C}[G]$-modules by Remark 10.

If χ is the character of V then we denote by $\mathrm{Ind}\chi$ the character of $\mathrm{Ind}V$. In order to give an expression for $\mathrm{Ind}\chi(\sigma)$ with $\sigma \in G$ and actually be able to do computations, we need a more explicit description of Ind$V$. We have the following decomposition of $\mathbb{C}[G]$ as a complex vector space:

$$\mathbb{C}[G] \cong \bigoplus_{\sigma\in G} \mathbb{C}\sigma \cong \bigoplus_{r\in H\setminus G}\bigoplus_{\sigma\in Hr} \mathbb{C}\sigma \cong \bigoplus_{r\in H\setminus G}\bigoplus_{\tau\in H} \mathbb{C}\tau r \cong \bigoplus_{r\in H\setminus G} \mathbb{C}[H]r.$$

Denote by $\psi : \mathbb{C}[G] \longrightarrow \bigoplus_{r\in H\setminus G} \mathbb{C}[H]r$ this isomorphism. Define a G-action on $\bigoplus_{r\in H\setminus G} \mathbb{C}[H]r$ as follows: if $\sigma \in G$ and $v \in \bigoplus_{r\in H\setminus G} \mathbb{C}[H]r$, then we define

$$\sigma(v) = \psi(\sigma(\psi^{-1}(v))).$$

Then the map ψ becomes an isomorphism of $\mathbb{C}[G]$-modules.

One can explicitly write down this action: let $\sigma \in G$ and let $r \in H \setminus G$. Then $\sigma r \in Hr'$ for some $r' \in H \setminus G$ and therefore there exists $\tau \in H$ such that $\sigma r = \tau r'$. The action of σ on $\mathbb{C}[H]r$ is given by $\sigma(\alpha r) = \tau(\alpha)r'$ for $\alpha \in \mathbb{C}[H]$. Extend this linearly to $\bigoplus_{r\in H\setminus G} \mathbb{C}[H]r$.

By general properties of the tensor product, we see that

$$\mathrm{Ind}V \cong \bigoplus_{r\in H\setminus G} Vr \tag{3.4.0.1}$$

as $\mathbb{C}[G]$-modules. In particular, $\dim_{\mathbb{C}} \mathrm{Ind}V = |H \setminus G| \dim_{\mathbb{C}} V$.

Theorem 3.4.1. *Let G be a finite group and H a subgroup of G. Let V be a representation of H with character χ. Let R be a full set of representatives of the right cosets of $H \setminus G$. Then for $\sigma \in G$ we have the formula*

$$\mathrm{Ind}\chi(\sigma) = \sum_{\substack{r\in R\\ r^{-1}\sigma r\in H}} \chi(r^{-1}\sigma r) = \frac{1}{|H|}\sum_{\substack{\tau\in G\\ \tau^{-1}\sigma\tau\in H}} \chi(\tau^{-1}\sigma\tau).$$

Proof. Let $R = \{r_1, \dots, r_k\}$. Take as basis for Ind$V$ the one of $\bigoplus_{i=1}^k Vr_i$. Then if $\sigma \in G$ we have

$$\sigma\left(\sum_{i=1}^k v_i r_i\right) = \sum_{i=1}^k \tau_i(v_i) r_{s(i)}$$

where $\sigma r_i = \tau_i r_{s(i)}$ with $\tau_i \in H$ and s an element of the permutation group S_n of $n$elements. Express σ in matrix form in this basis. If $r_{s(i)} \neq r_i$, then we get only zeroes on the diagonal in the part of the matrix where we plug in the image of the basis vectors of Vr_i. So the trace only takes into account the i's for which $r_{s(i)} = r_i$. This happens exactly whenever $r_i^{-1}\sigma r_i = \tau_i \in H$ and the sum of the diagonal terms in this part of the matrix is $\chi(\tau_i)$. Taking the trace of the whole matrix we get

$$\mathrm{Ind}\chi(\sigma) = \sum_{\substack{i=1\\ r_i^{-1}\sigma r_i\in H}}^k \chi(\tau_i) = \sum_{\substack{i=1\\ r_i^{-1}\sigma r_i\in H}}^k \chi(r_i^{-1}\sigma r_i).$$

To prove the second formula, note that if τ is in the coset defined by r_i, then $\tau = r_i h$ for some $h \in H$ and by Proposition 17 (*iii*), $\chi(\tau^{-1}\sigma\tau) = \chi(h^{-1}r_1^{-1}\sigma r_1 h) = \chi(r_i^{-1}\sigma r_i)$. Since there are $|H|$ elements in each coset, we see that

$$\sum_{\substack{\tau\in Hr_i\\ \tau^{-1}\sigma\tau\in H}} \chi(\tau^{-1}\sigma\tau) = |H|\chi(r_i^{-1}\sigma r_i)$$

and the second formula follows. □

3.5 The Dual Representation

Let G be a finite group and let V be a representation of G. Denote by $V^\vee$ the dual vector space $\mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ of V.

Proposition 20. *Let G be a finite group and let V be a representation of G with character χ. The dual $V^\vee$ has the structure of a left $\mathbb{C}[G]$-module and is therefore a representation of G. Moreover, its dimension is the one of V and its character is $\bar{\chi}$. Finally, V is irreducible if and only if $V^\vee$ is irreducible.*

Proof. Let $\sigma \in G$. Then we define a left action on $V^\vee$ by setting $(\sigma.f)(v) = f(\sigma^{-1}v)$ for $f \in V^\vee$ and $v \in V$. One easily checks that this is indeed an action. Let $x_1, \ldots, x_n$ be a basis for V as a $\mathbb{C}$-vector space and denote by $x^1, \ldots, x^n$ the corresponding dual basis. Explicitly, we have

$$x^j(\sum_{i=1}^{n} \lambda_i x_i) = \lambda_j.$$

Let $M(\sigma)$ be the matrix expression of σ in the basis $x_1, \ldots, x_n$. Then the matrix expression of σ in the dual basis is the transposed matrix $M(\sigma^{-1})^t$. It follows that the character of $V^\vee$ is given by $\sigma \longmapsto \chi(\sigma^{-1})$. By Proposition 17 (ii), this is $\bar{\chi}$.

Finally, suppose that $V^\vee$ is reducible. Then its character can be written as a sum of character $\theta_1 + \theta_2$. Since its character is $\bar{\chi}$, we obtain $\chi = \bar{\theta}_1 + \bar{\theta}_2$ which is a contradiction. The converse is similar. □

Proposition 21. *Let G be a finite group and let V and W be two representations of G. Then we have an isomorphism of $\mathbb{C}[G]$-modules*

$$V^\vee \otimes_{\mathbb{C}} W \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(V, W).$$

Proof. Define

$$F : V^\vee \times W \longrightarrow \mathrm{Hom}_{\mathbb{C}}(V, W), \qquad (f, w) \longmapsto (v \longmapsto f(v)w).$$

We check that this map is biadditive. If $f_1, f_2 \in V^\vee$, then

$$F((f_1 + f_2, w))(v) = (f_1 + f_2)(v)w = F((f_1, w))(v) + F((f_2, w))(v)$$

so F is linear in the first variable. If $w_1 \in w_2$, then

$$F((f, w_1 + w_2))(v) = f(v)(w_1 + w_2) = F((f, w_1))(v) + F((f, w_2))(v)$$

so F is linear in the second variable.

Moreover, if $\lambda \in \mathbb{C}$, then

$$F((f.\lambda, w))(v) = (f.\lambda)(v)w = f(\lambda v)w = f(v)(\lambda w) = F((f, \lambda w))(v).$$

By the universal property of the tensor product, there is a unique $\mathbb{C}$-linear map

$$\tilde{F} : V^\vee \otimes_{\mathbb{C}} W \longrightarrow \mathrm{Hom}_{\mathbb{C}}(V, W)$$

such that $\tilde{F}(f \otimes w) = F((f, w))$.

We check that $\tilde{F}$ is injective. In fact, suppose that $\tilde{F}(f \otimes w) = 0$ for all f and w. Then $f(v)w = 0$ for all $v \in V$. If $w \neq 0$, then $f(v) = 0$ so that $f = 0$. in either case, $f \otimes w = 0$. Finally, since

$$\dim_{\mathbb{C}} V^{\vee} \otimes_{\mathbb{C}} W = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}}(V, W) = \dim_{\mathbb{C}} V \dim_{\mathbb{C}} W$$

we must have that $\tilde{F}$ is an isomorphism of $\mathbb{C}$-vector spaces.

Note that $V^{\vee} \otimes_{\mathbb{C}} W \in {}_{\mathbb{C}[G]}\mathbf{Mod}$ where the action is given for $\sigma \in G$ by

$$\sigma.(f \otimes w) = (f.\sigma^{-1}) \otimes (\sigma w).$$

Also, $\mathrm{Hom}_{\mathbb{C}}(V, W) \in {}_{\mathbb{C}[G]}\mathbf{Mod}$ where the action is given for $\sigma \in G$ by

$$(\sigma.\phi)(v) = \sigma\phi(\sigma^{-1}v).$$

Let $\sigma \in G$. Then

$$\tilde{F}(\sigma.(f \otimes w)) = F((f.\sigma^{-1}) \otimes (\sigma w)) = f(\sigma^{-1}v)(\sigma w) = (\sigma.\tilde{F}(f \otimes w))(v)$$

so that $\tilde{F}$ is a $\mathbb{C}[G]$-isomorphism. □

Corollary 11. *Let G be a finite group. Let V and W be two representations of G with respective characters χ_V and χ_W. Then the character of the representation* $\mathrm{Hom}_{\mathbb{C}}(V, W)$ *is* $\bar{\chi}_V \chi_W$.

Proof. By Proposition 20, the character of the dual representation $V^{\vee}$ is $\bar{\chi}_V$. One checks easily that the character of the tensor product of two representations is the product of their characters. Therefore the character of the representation $V^{\vee} \otimes_{\mathbb{C}} W$ is $\bar{\chi}_V \chi_W$. By Proposition 21, the representations $V^{\vee} \otimes_{\mathbb{C}} W$ and $\mathrm{Hom}_{\mathbb{C}}(V, W)$ are isomorphic and thus share the same character. □

Corollary 12. *Let G be a finite group and let V and W be two representations of G. Then we have an isomorphism of complex vector spaces*

$$V^{\vee} \otimes_{\mathbb{C}[G]} W \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}[G]}(V, W).$$

Proof. We have

$$\mathrm{Hom}_{\mathbb{C}[G]}(V, W) = \mathrm{Hom}_{\mathbb{C}}(V, W)^G \text{ and } V^{\vee} \otimes_{\mathbb{C}[G]} W = (V^{\vee} \otimes_{\mathbb{C}} W)^G.$$

Since $(-)^G$ is a functor we get the desired result by using Proposition 21. □

.

3.6 Orthogonality Relations for Characters

In order to talk about orthogonality we must first define a scalar product on characters. Let G be a finite group and define $\mathcal{F}(G, \mathbb{C})$ to be the space of complex valued function $\phi : G \longrightarrow \mathbb{C}$. This is a complex vector space of dimension $|G|$.

Definition 11. Let G be a finite group of order g. We define the bilinear symmetric operator

$$\langle \cdot, \cdot \rangle_G : \mathcal{F}(G, \mathbb{C}) \times \mathcal{F}(G, \mathbb{C}) \longrightarrow \mathbb{C}, \qquad \langle \phi, \psi \rangle_G = \frac{1}{g} \sum_{\sigma \in G} \phi(\sigma)\psi(\sigma^{-1})$$

and the inner product

$$(\cdot|\cdot)_G : \mathcal{F}(G, \mathbb{C}) \times \mathcal{F}(G, \mathbb{C}) \longrightarrow \mathbb{C}, \qquad (\phi|\psi)_G = \frac{1}{g} \sum_{\sigma \in G} \phi(\sigma)\bar{\psi}(\sigma).$$

Remark 12. Let $\phi, \psi \in \mathcal{F}(G, \mathbb{C})$. If we define $\check{\psi} : G \longrightarrow \mathbb{C}$ by $\sigma \mapsto \bar{\psi}(\sigma^{-1})$, then $(\phi|\psi)_G = \langle \phi, \check{\psi} \rangle_G$. In particular, if χ is a character of G, then $\check{\chi} = \chi$ by Proposition 17 *(ii)* and thus $(\phi|\chi)_G = \langle \phi, \chi \rangle_G$.

Lemma 5. *Let G be a finite group. Let V and W be two representations of G with respective character χ_V and χ_W. Then we have*

$$\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V, W) = (\chi_V|\chi_W)_G .$$

Proof. We have $\operatorname{Hom}_{\mathbb{C}[G]}(V, W) = \operatorname{Hom}_{\mathbb{C}}(V, W)^G$ and by Corollary 11 the character of the representation $\operatorname{Hom}_{\mathbb{C}}(V, W)$ is $\bar{\chi}_V \chi_W$. By Corollary 10, we have

$$\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}}(V, W)^G = \frac{1}{|G|} \sum_{\sigma \in G} \bar{\chi}_V(\sigma)\chi_W(\sigma) = (\chi_W|\chi_V)_G = \overline{(\chi_V|\chi_W)}_G.$$

Since $\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}}(V, W)^G$ is an integer, complex conjugation has no effect here and we obtain the desired result. □

Lemma 6 (Schur)**.** *Let G be a finite group and let V_1 and V_2 be two irreducible representations of G. Let $f : V_1 \longrightarrow V_2$ be a $\mathbb{C}[G]$-module homomorphism. Then*

(i) If the two representations are not isomorphic, then $f = 0$.

(ii) If $V_1 = V_2$, then f is a homotethy.

Proof. For the first assertion, we will show that if f is not zero, then it is necessarily an isomorphism. Suppose therefore that f is non-zero. Consider the sub-$\mathbb{C}[G]$-module ker$f$ of V_1. By simplicity of V_1 we have either $\ker f = 0$ or $\ker f = V_1$. The latter is not possible since f is not the zero map and therefore f is injective. Similarly, im$f$ is a sub-$\mathbb{C}[G]$-module of V_2 and by simplicity we have either im$f = V_2$ or im$f = 0$. Again the latter is not possible and we conclude that f is an isomorphism of $\mathbb{C}[G]$-modules.

For the second assertion, suppose that f is not the zero map and let λ be a non-zero eigenvalue of f. Define $\tilde{f} := f - \lambda \mathrm{id}$. For all $\sigma \in G$ and $v \in V$, we have

$$\tilde{f}(\sigma v) = f(\sigma v) - \lambda \sigma v = \sigma(f(v)) - \sigma(\lambda v) = \sigma(\tilde{f}(v)).$$

In other words, $\tilde{f}$ is a $\mathbb{C}[G]$-endomorphism of V. In particular, $\ker \tilde{f}$ is a non-zero sub-$\mathbb{C}[G]$-module of V and by simplicity we have $\ker \tilde{f} = V$. This proves that $f(v) = \lambda v$ for all $v \in V$. □

Corollary 13. *Let G be a finite group and let $\widehat{G}$ denote the set of irreducible characters of G. Then $\widehat{G}$ forms an orthonormal system with respect to the inner product $(\cdot|\cdot)_G$.*

Proof. Let χ and θ be irreducible characters of G. Let V and W be irreducible representations of G with respective characters χ and θ. By Lemma 5, we have

$$(\chi|\theta)_G = \dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V, W).$$

By Lemma 6, if V and W are non-isomorphic then $\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V, W) = 0$ and $\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V, V) = 1$. We conclude that

$$(\theta|\chi)_G = \begin{cases} 0 & \text{if } \chi \neq \theta \\ 1 & \text{if } \chi = \theta. \end{cases}$$

□

Corollary 14. *Let V and W be two irreducible representations of G with respective characters χ and θ. Then V and W are isomorphic if and only if $(\chi|\theta)_G = 1$.*

Proof. If $V \cong W$ then $\chi = \theta$ and by Corollary 13 we have $(\chi|\theta)_G = 1$. If V and W are not isomorphic, then by Corollary 13 we have $(\chi|\theta)_G = 0$. □

Proposition 22. *Let V be a representation of G with character ϕ and let*

$$V = W_1 \oplus \ldots \oplus W_k$$

be a decomposition of V into irreducible representations. Let χ_i be the character of W_i for each i. Let W be an irreducible representation of G with character χ. Then the number of W_i that are isomorphic to W is equal to $(\phi|\chi)_G$.

Proof. We have $\phi = \chi_1 + \ldots + \chi_k$ and therefore

$$(\phi|\chi)_G = \sum_{i=1}^{k} (\chi_i|\chi)_G$$

and by Corollary 13 this is equal to the number of i's such that $(\chi_i|\chi)_G = 1$ which is the number of W_i isomorphic to W by Corollary 14. □

Corollary 15. *Two representations of a finite group are isomorphic if and only if they have the same character.*

Proof. We already know that if two representations are isomorphic, then they have the same character. The converse follows Proposition 22. □

The following is a useful criterion to determine whether or not a representation is irreducible.

Proposition 23. *Let V be a representation of G with character ϕ. Then V is irreducible if and only if $(\phi|\phi)_G = 1$. Moreover, $(\phi|\phi)_G$ is always a positive integer.*

Proof. Let $\chi_1, \ldots, \chi_h$ denote the distinct irreducible characters of G with corresponding representations $W_1, \ldots, W_h$. Then the representation V has a decomposition

$$V = W_1^{\oplus m_1} \oplus \ldots \oplus W_h^{\oplus m_h}$$

where the m_i are natural numbers. Thus $\phi = m_1\chi_1 + \ldots + m_h\chi_h$ and by Corollary 13 we have $m_i = (\phi|\chi_i)_G$ for all i so that $\phi = \sum_{i=1}^{h} (\phi|\chi_i)_G \chi_i$.

We see that $(\phi|\phi)_G = \sum_{i,j} m_i m_j (\chi_i|\chi_j)_G = \sum_i m_i^2$ and this is a positive integer. If ϕ is irreducible, then we already saw that $(\phi|\phi)_G = 1$. On the other hand, if $(\phi|\phi)_G = 1$ then $\sum_i m_i^2 = 1$ and therefore there exists j such that $m_j = 1$ and $m_i = 0$ for $i \neq j$ and this implies that $\phi = \chi_j$ which is irreducible. □

3.7 The Canonical Decomposition

Let G be a finite group of order g. Let $\widehat{G}$ denote the set of distinct irreducible characters of G and for each $\chi \in \widehat{G}$ let n_χ be the dimension of χ.

If V is a representation of G with character θ, then by Corollary 8 we may decompose V into a finite direct sum of irreducible representations, say $V = \bigoplus_{i=1}^m U_i$. Define V_χ to be the direct sum of those U_i whose character is χ. By Proposition 22, each V_χ is a direct sum of $(\chi|\theta)_G$ irreducible representations. We now have a decomposition

$$V = \bigoplus_{\chi \in \widehat{G}} V_\chi .$$

This is called the canonical decomposition of V. It is canonical because as we will see in the next result the components V_χ do not depend on the choice of the U_i.

Proposition 24. *With the above notations, for each $\chi \in \widehat{G}$ we define*

$$p_\chi = \frac{n_\chi}{g} \sum_{\sigma \in G} \bar{\chi}(\sigma)\sigma \in \mathbb{C}[G].$$

The action of p_χ on V is the projection of V onto V_χ. Since p_χ does not depend on the original decomposition of V and p_χ determines V_χ completely, this shows that V_χ is independent of the original decomposition.

Proof. We start by checking that p_χ lies in the center of $\mathbb{C}[G]$. In fact, if $\tau \in G$ then

$$p_\chi \tau = \frac{n_\chi}{g} \sum_{\sigma \in G} \bar{\chi}(\sigma)\sigma\tau = \frac{n_\chi}{g} \sum_{\sigma \in G} \bar{\chi}(\tau^{-1}\sigma\tau) = \frac{n_\chi}{g} \sum_{\eta \in G} \bar{\chi}(\eta)\tau\eta = \tau p_\chi$$

where in the second equality we used Proposition 17 (iii).

Let W be an irreducible representation of dimension n with character ξ. The action of p_χ on W is a $\mathbb{C}[G]$-endomorphism of W. By Lemma 6 (*ii*), p_χ acts on W by multiplication by, say λ. Taking traces on both sides we obtain

$$n_\chi \left(\xi|\chi\right)_G = n\lambda \implies \lambda = \frac{n_\chi}{n} \left\langle \xi, \chi \right\rangle_G = \begin{cases} 1 & \text{if } \xi = \chi \\ 0 & \text{otherwise} \end{cases}$$

by Corollary 13.

Thus p_χ acts as the identity on representations with character equal to χ and as the zero map otherwise. Thus p_χ acts as the identity on V_χ and as the zero map on $V_{\chi'}$ for $\chi' \neq \chi$. In other words, p_χ acts as the projection of V onto V_χ. □

Let $\chi \in \widehat{G}$. Then the χ-component V_χ of V is the eigenspace

$$V_\chi = \{v \in V \;:\; p_\chi v = v\}.$$

Suppose now that χ has dimension 1 so that χ is a homomorphism. Let $v \in V_\chi$ and $\sigma \in G$. Then we have

$$\sigma v = \sigma p_\chi v = \frac{1}{g} \sum_{\tau \in G} \bar{\chi}(\tau)\sigma\tau v = \frac{1}{g} \sum_{\tau \in G} \bar{\chi}(\sigma^{-1}\tau)\tau(v) = \chi(\sigma)v.$$

Conversely, if $v \in V$ and $\sigma v = \chi(\sigma)v$ for all $\sigma \in G$, then

$$p_\chi v = \frac{1}{g}\sum_{\tau \in G} \bar{\chi}(\tau)\chi(\tau)v = \langle \chi, \chi \rangle v = v$$

so that $v \in V_\chi$. We have proved the following:

Proposition 25. *With the above notations, if $\chi \in \widehat{G}$ has dimension 1 then we have*

$$V_\chi = \{v \in V \ : \ \sigma v = \chi(\sigma)v, \ \forall \sigma \in G\}.$$

In other words, the χ-component of V consists of simultaneous eigenvectors for the action of $\sigma \in G$ with eigenvalues $\chi(\sigma)$.

3.8 The Regular Representation

Let G be a finite group. The (left) regular representation of G is the group ring $\mathbb{C}[G]$ seen as a left module over itself. This is a $\mathbb{C}$-vector space of dimension $|G|$ whose basis can be identified with G. Explicitly, the left action of G on $\mathbb{C}[G]$ is the one of left multiplication of G on itself extended $\mathbb{C}$-linearly. We denote this action by $R_G : G \longrightarrow \mathrm{GL}(\mathbb{C}[G])$.

Proposition 26. *Let G be a finite group and let r_G be the character of the representation $\mathbb{C}[G]$. Then $r_G(1) = |G|$ and $r_G(\sigma) = 0$ for $\sigma \neq 1$.*

Proof. From Proposition 17 (i) we know that $r_G(1) = \dim_{\mathbb{C}} \mathbb{C}[G]$ which is equal to $|G|$. Let $\sigma \neq 1$ be an element of G. If we write $R_G(\sigma)$ in matrix form with respect to the basis $(\sigma)_\tau$, then the diagonal of this matrix is zero and thus its trace is zero. Therefore we have $r_G(\sigma) = 0$. □

Corollary 16. *Let G be a finite group. Let $\widehat{G}$ denote set of distinct irreducible characters of G and for each $\chi \in \widehat{G}$ we let n_χ denote the dimension of χ. The regular character decomposes as follows:*

$$r_G = \sum_{\chi \in \widehat{G}} n_\chi \chi.$$

As a consequence, we have $\sum_{\chi \in \widehat{G}} n_\chi^2 = |G|$ and $\sum_{\chi \in \widehat{G}} n_\chi \chi(\sigma) = 0$ for all $\sigma \neq 1$.

Proof. We have $r_G = \sum_{\chi \in \widehat{G}} (r_G|\chi)_G \, \chi$. For each $\chi \in \widehat{G}$ we have

$$(r_G|\chi)_G = \langle r_G, \chi \rangle_G = \frac{1}{g}\sum_{\sigma \in G} r_G(\sigma)\chi(\sigma^{-1}) = \frac{1}{g} r_G(1)\chi(1) = \chi(1) = n_\chi,$$

by Proposition 26. This proves the first formula. We obtain the second and third formula by evaluating the first at 1 and then at $\sigma \neq 1$ respectively. □

3.9 The Space of Class Functions

Let G be a finite group. We say that a function $f \in \mathcal{F}(G, \mathbb{C})$ is a class function of G if is has the property that $f(\tau\sigma\tau^{-1}) = f(\sigma)$ for all $\sigma, \tau \in G$. We denote by $\mathcal{C}(G, \mathbb{C})$ the space of all class functions of G. It is a complex subvector space of $\mathcal{F}(G, \mathbb{C})$ of dimension the number of conjugacy classes of G, say h. By Proposition 17 (iii), all characters of G are class functions of G.

Proposition 27. *Let $f \in \mathcal{C}(G, \mathbb{C})$ and define $\rho_f = \sum_{\sigma \in G} f(\sigma)\sigma \in \mathbb{C}[G]$. Let V be an irreducible representation of G of dimension n with character χ. Then ρ_f acts on V as multiplication by $\frac{|G|}{n} (f|\bar{\chi})_G$.*

Proof. We check that ρ_f is central in $\mathbb{C}[G]$. In fact, if $\tau \in G$ then we have

$$\rho_f \tau = \sum_{\sigma \in G} f(\sigma)\sigma\tau = \sum_{\sigma \in G} f(\tau^{-1}\sigma\tau)\sigma\tau = \sum_{\eta \in G} f(\eta)\tau\eta = \tau\rho_f.$$

It follows that the action of ρ_f on V is a $\mathbb{C}[G]$-endomorphism of V. By Lemma 6 (*ii*) ρ_f therefore acts on V as multiplication by, say λ. Taking traces, we see that

$$n\lambda = \sum_{\sigma \in G} f(\sigma)\chi(\sigma) = |G| \, (f|\bar{\chi})_G \, .$$

□

Theorem 3.9.1. *The set of irreducible characters $\widehat{G}$ of G forms an orthonormal basis of $\mathcal{C}(G, \mathbb{C})$ with respect to the scalar product $(\cdot|\cdot)_G$.*

Proof. By Corollary 13 we already know that $\widehat{G}$ is an orthonormal system in $\mathcal{C}(G, \mathbb{C})$ with respect to the above scalar product. In order to show that this system spans $\mathcal{C}(G, \mathbb{C})$, it suffices to prove that the orthogonal complement of $\mathrm{Span}(\bar{\chi} \mid \chi \in \widehat{G})$ is trivial. So let $f \in \mathcal{C}(G, \mathbb{C})$ such that $(f|\bar{\chi})_G = 0$ for all $\chi \in \widehat{G}$ and consider $\rho_f = \sum_{\sigma \in G} f(\sigma)\sigma \in \mathbb{C}[G]$. By Proposition 27, if W is an irreducible representation of G of dimension n and character χ, then ρ_f acts on W by multiplication by $\frac{|G|}{n} (f|\bar{\chi})_G = 0$. Let V be any representation of G. It decomposes into irreducible components and the action of ρ_f being the zero map on each component, we must have that $\rho_f : V \longrightarrow V$ is the zero map. In particular, take V to be the regular representation and let $(e_\sigma)_{\sigma \in G}$ be a basis of V. Then

$$\rho_f(e_1) = \sum_{\sigma \in G} f(\sigma)e_\sigma = 0.$$

Since the e_σ are linearly independent over $\mathbb{C}$ this implies that $f(\sigma) = 0$ for all σ so that $f = 0$. The proof is complete. □

Corollary 17. *The number of irreducible representations of G (up to isomorphism) is equal to the number of conjugacy classes of G.*

Proof. The number of irreducible representations of G up to isomorphism is equal to the number of irreducible characters. By Theorem 3.9.1, these form a basis of the vector space $\mathcal{C}(G, \mathbb{C})$ which has dimension the number of conjugacy classes of G. □

Proposition 28. *For $\sigma \in G$ we let $c(\sigma)$ denote the order of the conjugacy class of σ in G. Then we have the following:*

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \bar{\chi}(\sigma)\chi(\tau) = \begin{cases} \frac{1}{c(\sigma)} & \textit{if } \sigma \textit{ and } \tau \textit{ are conjugates} \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Fix $\sigma \in G$ and consider the class function $f_\sigma : G \longrightarrow \mathbb{C}$ defined by

$$f_\sigma(\tau) = \begin{cases} 1 & \text{if } \sigma \text{ and } \tau \text{ are conjugates} \\ 0 & \text{otherwise.} \end{cases}$$

By Theorem 3.9.1, we can write $f_\sigma(\tau) = \sum_{\chi\in\widehat{G}} (f|\chi)_G\, \chi$. We compute that $(f|\chi)_G = \frac{c(\sigma)}{|G|}\bar{\chi}(\sigma)$. It follows that

$$f_\sigma(\tau) = \frac{c(\sigma)}{|G|} \sum_{\chi\in\widehat{G}} \bar{\chi}(\sigma)\chi(\tau)$$

and the result follows from the definition of f_σ. □

Proposition 29. *A finite group G is abelian if and only if all irreducible representations of G have degree* 1*.*

Proof. Let g be the order of G and let $h = |\widehat{G}|$. Denote by n_χ the dimension of $\chi \in \widehat{G}$. The group G is abelian if and only if G has g distinct conjugacy classes. By Corollary 17 the number of distinct conjugacy classes is h. Thus G is abelian if and only if $g = h$. By Corollary 16 we have $\sum_{\chi\in\widehat{G}} n_\chi^2 = g$. Thus G is abelian if and only if $n_\chi = 1$ for all $\chi \in \widehat{G}$. □

Combining this with Proposition 25 we get:

Corollary 18. *Let G be an abelian group and V a representation of G. The canonical decomposition of V is the following eigen-decomposition of V:*

$$V = \bigoplus_{\chi\in\widehat{G}} V_\chi, \qquad V_\chi = \{v \in V \ : \ \sigma v = \chi(\sigma)v,\ \forall \sigma \in G\}.$$

3.10 Frobenius Reciprocity

The close relation between the Hom functor and the tensor functor is illustrated in the following theorem, known as the Adjoint Isomorphism Theorem:

Theorem 3.10.1. *Let R and S be rings. Let $A \in {}_R\mathbf{Mod}$, $B \in {}_S\mathbf{Mod}_R$ and $C \in {}_S\mathbf{Mod}$. There is a natural isomorphism*

$$\tau_{A,B,C} = \tau : \mathrm{Hom}_S(B \otimes_R A, C) \longrightarrow \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

defined as follows: consider $f : B \otimes_R A \longrightarrow C$ and define the map

$$\tau(f) : A \longrightarrow \mathrm{Hom}_S(B, C), \qquad \tau(f)(a)(b) = f(b \otimes a).$$

Proof. Let us check that the above map is well-defined. If $s \in S$, then

$$\tau(f)(a)(sb) = f((sb) \otimes a) = f(s(b \otimes a)) = sf(b \otimes a) = s\tau(f)(a)(b)$$

since f is an S-map. So $\tau(f)(a) \in \mathrm{Hom}_S(B, C)$. Let $r \in R$. Then

$$\tau(f)(ra)(b) = f(b \otimes (ra)) = f((br) \otimes a) = \tau(f)(a)(br) = (r.\tau(f)(a))(b)$$

so that $\tau(f)(a) \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$.

Let us check that τ is a homomorphism of groups. Let $f, g \in \mathrm{Hom}_S(B \otimes_R A, C)$. Then

$$\tau(f + g)(a)(b) = (f + g)(b \otimes a) = f(b \otimes a) + g(b \otimes a) = \tau(f)(a)(b) + \tau(g)(a)(b).$$

This shows that $\tau(f + g) = \tau(f) + \tau(g)$.

Let us check that τ is injective. Suppose that $\tau(f) = 0$. Then for all $a \in A$ and all $b \in B$ we have $f(b \otimes a) = 0$ and thus $f = 0$ since it is zero on all generators of $B \otimes_R A$.

Let check that τ is surjective. Let $F : A \longrightarrow \mathrm{Hom}_S(B, C)$ be an R-map. Define $\phi : B \times A \longrightarrow C$ by $\phi((b, a)) = F(a)(b)$. Obviously ψ is biadditive. Also, if $r \in R$, then $\psi((br, a)) = F(a)(br) = F(ra)(b) = \psi((b, ra))$ since F is an R-map. By the universal property of the tensor product, there exists a unique S-map $\tilde{\psi} : B \otimes_R A \longrightarrow C$ such that $\tilde{\psi}(b \otimes a) = \psi((b, a))$. Then $\tau(\tilde{\psi}) = F$.

To check the naturality of the map, we fix for example B and C and show that

$$\tau : \mathrm{Hom}_S(B \otimes_R -, C) \longrightarrow \mathrm{Hom}_R(-, \mathrm{Hom}_S(B, C))$$

is a natural isomorphism of functors. Let $A, A' \in {}_R\mathbf{Mod}$ and $f \in \mathrm{Hom}_R(A, A')$. The only thing we need to check is that the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Hom}_S(B \otimes_R A, C) \arrow[r, "\tau_A"] & \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \\
\mathrm{Hom}_S(B \otimes_R A', C) \arrow[u, "(1_B \otimes f)^*"] \arrow[r, "\tau_{A'}"'] & \mathrm{Hom}_R(A', \mathrm{Hom}_S(B, C)). \arrow[u, "f^*"']
\end{tikzcd}$$

Let $F : B \otimes_R A' \longrightarrow C$ be an S-map. Then taking the right-up path we arrive at the R-map $\tau_{A'}(F) \circ f : A \longrightarrow \mathrm{Hom}_S(B, C)$ given by

$$\tau_{A'}(F)(f(a))(b) = F(b \otimes f(a)).$$

Taking the up $F \circ (1 \otimes f) : B \otimes_R A \longrightarrow C$ which maps $b \otimes a$ to $F(b \otimes f(a))$. Taking now the right path, we arrive at $\tau_A(F \circ (1 \otimes f)) : A \longrightarrow \mathrm{Hom}_S(B, C)$ given by

$$\tau_A(F \circ (1 \otimes f))(a)(b) = F \circ (1 \otimes f)(b \otimes a) = F(b \otimes f(a)).$$

We have proved that the diagram commutes.

One can similarly check the naturality of the map in the other variables. □

Corollary 19. *Let G be a finite group and let H be a subgroup of G. Let V be a representation of H and let W be a representation of G. We have a natural isomorphism*

$$\tau : \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}V, W) \longrightarrow \mathrm{Hom}_{\mathbb{C}[H]}(V, \mathrm{Res}W).$$

Proof. We have $\mathbb{C}[G] \in {}_{\mathbb{C}[G]}\mathbf{Mod}_{\mathbb{C}[H]}$, $V \in {}_{\mathbb{C}[H]}\mathbf{Mod}$ and $W \in {}_{\mathbb{C}[G]}\mathbf{Mod}$. Applying Theorem 3.10.1, we have a natural $\mathbb{C}$-linear isomorphism

$$\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V, W) \longrightarrow \mathrm{Hom}_{\mathbb{C}[H]}(V, \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], W)).$$

Note that $\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], W) \in {}_{\mathbb{C}[H]}\mathbf{Mod}$, the action being given by

$$(\lambda.f)(x) = f(x\lambda)$$

for $f : \mathbb{C}[G] \longrightarrow W$, $x \in \mathbb{C}[G]$ and $\lambda \in \mathbb{C}[H]$. Consider the group isomorphism

$$\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], W) \longrightarrow \mathrm{Res}W, \qquad f \longmapsto f(1).$$

If $\lambda \in \mathbb{C}[H]$, then we have

$$\lambda.f \mapsto (\lambda.f)(1) = f(1.\lambda) = f(\lambda.1) = \lambda f(1)$$

since f is a $\mathbb{C}[G]$-map. Therefore, the above map is a $\mathbb{C}[H]$-module isomorphism and we have a natural isomorphism of groups

$$\tau : \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}V, W) \longrightarrow \mathrm{Hom}_{\mathbb{C}[H]}(V, \mathrm{Res}W).$$

□

Theorem 3.10.2 (Frobenius Reciprocity)**.** *Let G be a finite group and let H be a subgroup of G. Let V be a representation of H and let W be a representation of G with respective characters χ and θ. Then we have*

$$\langle \mathrm{Ind}\chi, \theta\rangle_G = \langle \chi, \mathrm{Res}\theta\rangle_H .$$

Proof. By Corollary 19, we have

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}V, W)) = \dim_{\mathbb{C}[H]}(V, \mathrm{Res}W).$$

By Proposition 5 and Remark 12, this is the desired formula. □

3.11 A Theorem of Brauer

We will prove a refinement of a theorem of Brauer assuming the proof of Brauer's original theorem given below. Let G be a finite group. A character χ of G is said to be monomial if $\chi = \mathrm{Ind}\theta$ for some 1-dimensional character of a subgroup of G.

Theorem 3.11.1. *Every character of a finite group can be written as a $\mathbb{Z}$-linear combination of monomial characters.*

Proof. See Chapter 10 of [Se1]. □

Explicitly the theorem says the following: if χ is a character of G, then there exist integers n_i, subgroups H_i and 1-dimensional characters θ_i of H_i such that

$$\chi = \sum_i n_i \mathrm{Ind}_{H_i}^G \theta_i.$$

Let G be a finite group. Denote by $[G : G]$ the commutator subgroup of G and let $G_1 = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}^*)$ be the multiplicative group of 1-dimensional characters of G. We claim that

$$\mathrm{Infl} = \mathrm{Infl}_{[G:G]}^G : (G/[G : G])_1 \longrightarrow G_1$$

is an isomorphism of groups.

This map is obviously well-defined homomorphism of groups. Let $\chi \in G_1$. Then $\chi : G \longrightarrow \mathbb{C}^*$ is a homomorphism of groups and therefore its kernel contains the commutator subgroup. By the universal property of the quotient, there is a unique homomorphism $\tilde{\chi} : G/[G : G] \longrightarrow \mathbb{C}^*$ such that $\chi(\sigma) = \tilde{\chi}([\sigma])$. In other words, there is a unique $\tilde{\chi} \in (G/[G : G])_1$ such that $\mathrm{Infl}\tilde{\chi} = \chi$. This proves that the map Infl is a bijection.

In particular, we have $|G_1| = |(G/[G:G])_1|$. But $G/[G:G]$ is an abelian group and by Proposition 29, we have $(G/[G:G])_1 = \widehat{G/[G:G]}$, that is, the group of irreducible characters of $G/[G:G]$. In particular, we have $|(G/[G:G])_1| = |G/[G:G]|$. We conclude that

$$|G_1| = |G/[G:G]|. \tag{3.11.1.1}$$

Let $Z = Z(G)$ denote the center of G and let H be a subgroup of G. Then $[ZH:ZH] = [H:H]$ and therefore by (3.11.1.1) we have

$$|(ZH)_1| = |ZH/[ZH:ZH]| = |ZH/[H:H]| = [ZH:H]|H_1|.$$

Consider the homomorphism

$$\text{Res} : (ZH)_1 \longrightarrow H_1, \qquad \chi \longmapsto \chi|_H.$$

This map is surjective: for if $\chi \in H_1$, then we define $\tilde{\chi} \in (ZH)_1$ by setting $\tilde{\chi}(zh) = \chi(h)$ for $z \in Z$ and $h \in H$. This does indeed define a homomorphism since for $z_1, z_2 \in Z$ and $h_1, h_2 \in H$ we have

$$\tilde{\chi}((z_1h_1)(z_2h_2)) = \tilde{\chi}((z_1z_2)(h_1h_2)) = \chi(h_1h_2) = \chi(h_1)\chi(h_2) = \tilde{\chi}(z_1h_1)\tilde{\chi}(z_2h_2).$$

Finally we have $\text{Res}\tilde{\chi} = \chi$ and this proves that Res is surjective. By comparing cardinalities, we see that the kernel of this map must be of order $[ZH:H]$. We conclude that the map Res is a $[ZH:H]$-to-1 homomorphism.

Theorem 3.11.2. *Let G be a finite group with center $Z = Z(G)$ and let χ be an irreducible character of G. The restriction of χ to Z is a multiple of a 1-dimensional character ψ of Z and we may write*

$$\chi = \sum_i n_i \text{Ind}_{H_i}^G \theta_i$$

where, for every i, H_i is a subgroup of G containing Z, θ_i is a 1-dimensional character of H_i whose restriction to Z is ψ and the n_i are integers.

Proof. Let H be a subgroup of G. By the above discussion, the map

$$\text{Res} : (ZH)_1 \longrightarrow H_1$$

is a $[ZH:H]$-to-1 homomorphism of groups. In other words, there are exactly $[ZH:H]$ ways to extend an element of H_1 to $(ZH)_1$.

Let θ be in H_1 and let θ_i with $i = 1, \ldots, [CH:H]$ be the distinct extensions of θ to ZH. By Theorem 3.10.2 we have

$$\left\langle \text{Ind}_H^{ZH}\theta, \theta_i \right\rangle_{ZH} = \langle \theta, \text{Res}\theta_i \rangle_H = \langle \theta, \theta \rangle_H = 1$$

by Corollary 13. By Proposition 22 this means that every character θ_i appears in the decomposition of the character $\text{Ind}_H^{CH}\theta$ with multiplicity 1. Since $\text{Ind}_H^{CH}\theta$ is of dimension $[ZH:H]$ we must therefore have the decomposition

$$\text{Ind}_H^{ZH}\theta = \sum_{i=1}^{[ZH:H]} \theta_i.$$

For any left $\mathbb{C}[H]$-module M, we have

$$\mathbb{C}[G] \otimes_{\mathbb{C}[CH]} (\mathbb{C}[CH] \otimes_{\mathbb{C}[H]} M) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} M$$

by associativity of the tensor product. In other words, we have

$$\mathrm{Ind}_H^G M = \mathrm{Ind}_{CH}^G \mathrm{Ind}_H^{CH} M.$$

Since tensoring is an additive functor, this implies that

$$\mathrm{Ind}_H^G \theta = \sum_{i=1}^{[ZH:H]} \mathrm{Ind}_{ZH}^G \theta_i.$$

Combined with Theorem 3.11.1, this shows that we can choose the subgroups H_i in the statement of the present theorem to contain the center Z.

Let V be a representation of G with character χ. Then $\mathrm{Res}V = \mathrm{Res}_Z^G V$ is a representation of the center Z. Let W be a simple sub-$\mathbb{C}[Z]$-module of $\mathrm{Res}V$ with character ψ. Since Z is an abelian group, by Proposition 29, we have $\dim_{\mathbb{C}} W = 1$. Denote by $(\mathrm{Res}V)_\psi$ the ψ component in the canonical decomposition of $\mathrm{Res}V$. By Proposition 24, the element

$$p_\psi = \frac{1}{|Z|} \sum_{z \in Z} \bar{\psi}(z) z \in \mathbb{C}[Z] \subset \mathbb{C}[G]$$

acts on $\mathrm{Res}V$ as the projection onto $(\mathrm{Res}V)_\psi$. Let $\sigma \in G$. Using the definition of the center Z, we see that

$$p_\psi \sigma = \frac{1}{|Z|} \sum_{z \in Z} \bar{\psi}(z) z \sigma = \frac{1}{|Z|} \sum_{z \in Z} \bar{\psi}(z) \sigma z = \sigma p_\psi.$$

Thus, if $v \in (\mathrm{Res}V)_\psi$, we have $p_\psi(\sigma v) = \sigma v$. In other words, σv belongs to $(\mathrm{Res}V)_\psi$. This proves that $(\mathrm{Res}V)_\psi$ is a sub-$\mathbb{C}[G]$-module of V. But V is irreducible so that $\mathrm{Res}V = (\mathrm{Res}V)_\psi$ and $\mathrm{Res}\chi = \chi(1)\psi$. This proves the assertion that the restriction of χ to Z is a multiple of a 1-dimensional character of Z.

We write $\chi = \sum_i n_i \mathrm{Ind}_{H_i}^G \theta_i$ where the H_i are subgroups containing Z and the characters θ_i are 1-dimensional. Let θ be any irreducible character of G. By the above discussion, there exists a 1-dimensional character ψ_θ of Z and a positive integer m_θ such that $\mathrm{Res}_Z^G \theta = m_\theta \psi_\theta$. By Theorem 3.10.2 we have

$$\left\langle \mathrm{Ind}_{H_i}^G \theta_i, \theta \right\rangle_G = \left\langle \theta_i, \mathrm{Res}_{H_i}^G \theta \right\rangle_{H_i}.$$

If $\mathrm{Res}_Z^{H_i} \theta_i \neq \psi_\theta$, then θ_i cannot be a summand of $\mathrm{Res}_{H_i}^G \theta$. In other words, we have $\left\langle \theta_i, \mathrm{Res}_{H_i}^G \theta \right\rangle_{H_i} = 0$ by Proposition 22. Consequently, we have

$$\mathrm{Res}_Z^{H_i} \theta_i \neq \psi_\theta \implies \left\langle \mathrm{Ind}_{H_i}^G \theta_i, \theta \right\rangle_G = 0.$$

Perhaps more usefully, we have

$$\left\langle \mathrm{Ind}_{H_i}^G \theta_i, \theta \right\rangle_G > 0 \implies \mathrm{Res}_Z^{H_i} \theta_i = \psi_\theta. \tag{3.11.2.1}$$

We split the sum as follows:

$$\chi = \sum_{\mathrm{Res}_Z^{H_i}\theta_i=\psi} n_i \mathrm{Ind}_{H_i}^G \theta_i + \sum_{\mathrm{Res}_Z^{H_i}\theta_i\neq\psi} n_i \mathrm{Ind}_{H_i}^G \theta_i.$$

By (3.11.2.1), every irreducible character of G that appears in the first sum must be a multiple of ψ when restricted to Z and no irreducible character of G appearing in the second sum can be a multiple of ψ when restricted to Z. It follows that the sets of irreducible characters respectively appearing in the first sum and in the second sum are distinct sets. Since the appearance of χ is necessarily in the first sum, the second sum must be zero. This shows that

$$\chi = \sum_{\mathrm{Res}_Z^{H_i}\theta_i=\psi} n_i \mathrm{Ind}_{H_i}^G \theta_i$$

and finishes the proof. □

Chapter 4

Rationality of Characters

Until now we have only considered linear representations over the field of complex numbers $\mathbb{C}$ and their characters. But in fact all the results we have proved hold for algebraically closed fields of characteristic zero. Let K be any field of characteristic zero and let C be a fixed algebraic closure of K. As usual, G will denote a finite group. A linear representation of G over K is a $K[G]$-module V which is finite-dimensional as a K-vector space. A character of such a representation of G is the trace map $G \longrightarrow K$ associated to the action of G on V.

Let V be a representation of G over K with character χ. Define V_C to be the extension of scalars $C \otimes_K V$. It is a C-vector space of dimension equal to $\dim_K V$. Moreover, V_C has the structure of a left G-module given by $\sigma(c \otimes v) = c \otimes (\sigma v)$. Thus V_C is a left $C[G]$-module which is finite-dimensional over C. In other words, it is a representation of G over C. The action of G on V_C can be summarized by the diagram

$$G \xrightarrow{\sigma} \mathrm{GL}_K(V) \xrightarrow{1 \otimes \sigma} \mathrm{GL}_C(V_C).$$

The character of V_C is still $\chi : G \longrightarrow K$. A representation of G over C is said to be defined or rational over K if it is isomorphic to a representation V_C as constructed here for some representation V of G over K. This is equivalent to saying that a representation V of G over C is rational over K if there exists a basis of V in which the coefficients of the matrices of $\sigma \in G$ lie in K.

Starting with a representation of G over K we can produce a representation of G over C by extension of scalars. The question that we will answer in this chapter is how to determine when a representation of G over C is rational over some subfield K of C.

4.1 First Results

We start with some notations. We define $R(G) = R_C(G)$ to be the free abelian group on the irreducible characters of G over C. Explicitly, if $\chi_1, \ldots, \chi_h$ are the irreducible characters of G over C, then

$$R(G) = \mathbb{Z}\chi_1 \oplus \ldots \oplus \mathbb{Z}\chi_r.$$

An element of $R(G)$ is a character of G over C if and only if it is a $\mathbb{Z}$-linear combination of the χ_i with non-negative coefficients. A general element of $R(G)$ is called a virtual character of G over C. Since multiplying two characters results in a new character (realized by tensoring the corresponding representations), we see that $R(G)$ has a multiplication and actually forms a ring. By Theorem 3.9.1, the χ_i form an orthonormal basis of the C-vector space of class functions $\mathcal{C}(G,C)$ with respect to the symmetric bilinear form $\langle \phi, \psi \rangle_G = \frac{1}{|G|} \sum_{\sigma \in G} \phi(\sigma^{-1})\psi(\sigma)$. Therefore we have $\mathcal{C}(G,C) \cong C \otimes_{\mathbb{Z}} R(G)$ as C-vector spaces.

We let $R_K(G)$ denote the subring of $R(G)$ generated by characters of representations of G over K. We also let $R(G,K)$ denote the subring of $R(G)$ consisting of those elements that take values in K. Of course we have the inclusion $R_K(G) \subset R(G,K)$.

Proposition 30. *Let V_i, $i = 1, \dots, h$, be the distinct (up to isomorphism) irreducible representations of G over K with characters χ_i. Then the χ_i form an orthogonal basis of $R_K(G)$ with respect to the bilinear form $\langle \cdot, \cdot \rangle_G$. Moreover, we have $\langle \chi_i, \chi_i \rangle_G = \dim_K \operatorname{End}_{K[G]}(V_i)$.*

Proof. From the definition of $R_K(G)$ it is clear that it is generated by the χ_i. Let V and W be two representations of G over K with characters χ_V and χ_W. Then by Lemma 5 we have

$$\dim_K \operatorname{Hom}_{K[G]}(V,W) = \dim_C \operatorname{Hom}_{C[G]}(V_C, W_C) = \langle \chi_V, \chi_W \rangle_G .$$

Applying Shur's Lemma 6 (a), whose proof does not require K to be algebraically closed, we see that if $i \neq j$, then $\operatorname{Hom}_{K[G]}(V_i, V_j) = 0$. Combined with the above equality this implies that $\langle \chi_i, \chi_j \rangle_G = 0$ for $i \neq j$, proving orthogonality of the χ_i which in turn implies $\mathbb{Z}$-linear independence of the χ_i. We conclude that the χ_i form an orthogonal basis of $R_K(G)$. □

Remark 13. Let V be an irreducible representation of G over K with character χ. We have just proved that $\langle \chi, \chi \rangle_G = \dim_C \operatorname{End}_{C[G]}(V_C)$ which is an integer greater than or equal to 1. It is 1 if the representation V_C is irreducible by Corollary 13. But this is not always the case as illustrated in the next example.

Example 3. Let μ_3 be the group of third roots of unity. If $\zeta = e^{2\pi i/3}$, then $\mu_3 = \{1, \zeta, \zeta^2\}$. This group acts on $\mathbb{C}$ by multiplication. By choosing $\{(1,0),(0,i)\}$ as a basis of $\mathbb{C}$ as an $\mathbb{R}$-vector space of dimension 2, we get a 2-dimensional real representation of μ_3 given by the homomorphism $\rho : \mu_3 \longrightarrow \mathrm{GL}_2(\mathbb{R})$ defined by:

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho(\zeta) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \quad \rho(\zeta^2) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

The character χ of this representation is given by

$$\chi(1) = 2, \qquad \chi(\zeta) = -1, \qquad \chi(\zeta^2) = -1.$$

The characteristic polynomial of $\rho(\zeta)$ and $\rho(\zeta^2)$ is given by T^2+T+1 so that the eigenvalues of these matrices are ζ and ζ^2 which do not belong to $\mathbb{R}$. Therefore $\rho(\zeta)$ cannot be diagonalized over $\mathbb{R}$ and consequently the above representation is irreducible over $\mathbb{R}$. But even though it is irreducible, we have

$$\langle \chi, \chi \rangle_G = \frac{1}{3}(4+1+1) = 2.$$

If we now tensor this representation over $\mathbb{C}$, we get a 2-dimensional complex representation of μ_3. But μ_3 is abelian so by Corollary 29, this representation cannot be irreducible. For the sake of the example we here show how this representation decomposes over $\mathbb{C}$. By computation we find that the eigenspaces of $\rho(\zeta)$ for the eigenvalues ζ and ζ^2 are respectively given by

$$V_1 = \operatorname{Span}\left\{\begin{pmatrix}1\\ i\end{pmatrix}\right\} \subset \mathbb{C}^2 \qquad \text{and} \qquad V_2 = \operatorname{Span}\left\{\begin{pmatrix}1\\ -i\end{pmatrix}\right\} \subset \mathbb{C}^2.$$

Base changing $\{(1,0),(0,1)\}$ to $\{(1,i),(1,-i)\}$ we obtain an isomorphic representation $\rho : G \longrightarrow \mathrm{GL}_2(\mathbb{C})$ given by

$$\rho(1) = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad \rho(\zeta) = \begin{pmatrix}\zeta & 0\\ 0 & \zeta^2\end{pmatrix}, \quad \rho(\zeta^2) = \begin{pmatrix}\zeta^2 & 0\\ 0 & \zeta\end{pmatrix}.$$

The element ζ acts on V_1 by multiplication by ζ and on V_2 by multiplication by ζ^2. Our original representation decomposes over $\mathbb{C}$ as $V_1 \oplus V_2$.

Proposition 31. *Let V be a representation of G over K with character ϕ and let*

$$V = W_1 \oplus \ldots \oplus W_k$$

be a decomposition of V into irreducible representations of G over K. Let χ_i be the character of W_i for each i. Let W be an irreducible representation of G over K with character χ. Then the number n_W of W_i that are isomorphic to W independent of the above decomposition. In particular, two representations of G over K are isomorphic if and only if they share the same character.

Proof. We have $\phi = \sum_{i=1}^k \chi_i$. By Proposition 30 we have

$$\langle \phi, \chi \rangle_G = \sum_{i=1}^k \langle \chi_i, \chi \rangle_G .$$

This is equal to $n_W \dim_K \operatorname{End}_{K[G]}(W)$ so that n_w is independent of of the decomposition. □

Corollary 20. *Any representation of G over K has a canonical representation over K.*

Proposition 32. *A representation of G over C is defined over K if and only if its character belongs to $R_K(G)$.*

Proof. Let V be a representation of G over C with character χ. It is clear that if this representation is rational over K, then χ belongs to $R_K(G)$. On the other hand, suppose that χ belongs to $R_K(G)$. If $\chi_1, \ldots, \chi_h$ are the irreducible characters of G over K, then there exist integers n_i such that $\chi = \sum_{i=1}^h n_i\chi_i$ and by Proposition 30 we have $\langle \chi, \chi_i \rangle_G = n_i \langle \chi_i, \chi_i \rangle_G$. The bilinear form $\langle \cdot, \cdot \rangle_G$ is a scalar product on characters of G over C. Since χ and χ_i are both characters of G over C, we must therefore have $\langle \chi, \chi_i \rangle_G \geq 0$ so that $n_i \geq 0$. If $V_1, \ldots, V_h$ are irreducible representation of G over K with characters χ_i, then the latter implies that $W = \bigoplus V_i^{\oplus n_i}$ is a representation of G over K with character χ. In particular, W_C is isomorphic to V and therefore V is defined over K. □

Let V be a representation of G over C. We claim that V is always defined over some finite extension L of K. In fact, let $\chi_1, \ldots, \chi_h$ be the irreducible characters of G over C and let $(\rho_1, V_1), \ldots, (\rho_h, V_h)$ be corresponding irreducible representations of G over C. Choose bases for each V_i and write $\rho_i(\sigma)$ in matrix form with respect to the chosen basis for each $\sigma \in G$. Define L to be the finite extension of K obtained by adjoining to K all matrix coefficients of the $\rho_i(\sigma)$. Then each V_i is defined over L. In other words, $\chi_i \in R_L(G)$ for all $i = 1, \ldots, h$ and consequently we have $R_L(G) = R_C(G)$. By Proposition 32, every representation of G over C is defined over L. Let $d = [L : K]$.

Let V be a representation of G over L with character χ. Let V_K denote the restriction of scalars of V to K. As a set, V_K is the same as V but where we have forgotten the L-vector space structure on V. Since L is a K-vector space of degree d, the restriction of scalars V_K is a K-vector space of degree $d \deg_L V$. In particular, it is a representation of G over K. Let χ_K denote the character of V_K. One checks that $\chi_K = \mathrm{tr}_{L/K} \circ \chi : G \longrightarrow K$. We therefore have $\mathrm{tr}_{L/K}\chi \in R_K(G)$.

Now, if $\theta \in R_C(G) = R_L(G)$, then $\theta = \sum_i^h n_i \chi_i$. By linearity of $\mathrm{tr}_{L/K}$ we obtain

$$\mathrm{tr}_{L/K}\theta = \sum_{i=1}^{h} n_i \mathrm{tr}_{L/K}\chi_i \in R_K(G).$$

In particular, if $\theta \in R(G, K)$, then $\mathrm{tr}_{L/K}\theta = d\theta \in R_K(G)$. This proves that $dR(G, K) \subset R_K(G)$. As already noted, we have the trivial inclusion $R_K(G) \subset R(G, K)$. We therefore have the inclusions

$$dR(G, K) \subset R_K(G) \subset R(G, K).$$

This gives a surjective homomorphism of groups

$$R(G, K)/dR(G, K) \longrightarrow R(G, K)/R_K(G).$$

Since the first quotient group is finite, we have proved the following:

Proposition 33. *The group $R_K(G)$ has finite index in $R(G, K)$.*

Remark 14. Let V be a representation of G over C with character χ. In general, in order for V to be defined over K, it is not enough for χ to belong to $R(G, K)$ as the following example shows.

Example 4. Consider the Hamilton quaternion algebra H_K over a field K of characteristic 0. This is a 4-dimensional K-vector space with basis $\{1, i, j, k\}$ with the following multiplication rules:

$$i^2 = -1, \qquad j^2 = -1, \qquad ij = k, \qquad ji = -k.$$

One defines a norm form $N : H_K \longrightarrow K$ by defining $N(\alpha)$ to be the determinant of the multiplication-by-α map on H_K. It is not difficult to check that

$$N(x + yi + zj + tk) = x^2 + y^2 + z^2 + t^2.$$

The algebra H_K also comes equipped with an involution defined by

$$\overline{x + yi + zj + tk} = x - yi - zj - tk.$$

One now checks that $N(\alpha) = \alpha\bar{\alpha}$. This norm form is multiplicative and it becomes clear that $\alpha \in H_K^*$ if and only if $N(\alpha) \neq 0$. In particular, $H_{\mathbb{Q}}$ and $H_{\mathbb{R}}$ are skew-fields, that is, non-commutative division rings.

If -1 is a sum of two squares in K, that is, if there exist $\alpha, \beta \in K$ such that $\alpha^2 + \beta^2 = -1$, then we have a K-algebra isomorphism $\phi : H_K \longrightarrow M_2(K)$. This can be described by

$$\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \phi(i) = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}, \phi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \phi(k) = \begin{pmatrix} \beta & -\alpha \\ -\alpha & -\beta \end{pmatrix}.$$

In the case $K = \mathbb{C}$, one can for example take $\alpha = i$ and $\beta = 0$.

In particular, we get a homomorphism $G \longrightarrow \mathrm{GL}_2(K)$ and we thus have a 2-dimensional representation of G over K. This representation is defined over $\mathbb{Q}(\alpha, \beta)$. Its character χ is given by

$$\chi(\pm 1) = \pm 2, \chi(\pm i) = \chi(\pm j) = \chi(\pm k) = 0.$$

In particular, we see that $\chi \in R(G, \mathbb{Q})$. However, this representation is not defined over $\mathbb{Q}$ since the sum of any two squares in $\mathbb{Q}$ is non-negative.

4.2 Non-Commutative Algebra

We prove the structure theorem of simple left Artinian rings due to Wedderburn. A good reference for this section is [Ro1].

4.2.1 Semisimple Rings

Let R be a ring. It is not assumed to be commutative but we will assume that R has a multiplicative unit 1. We have already encountered semisimple rings: remember that the group ring $\mathbb{C}[G]$ is a semisimple ring for example. We start by recalling the definition of semisimplicity.

A left R-module is said to be simple if it has no left sub-R-modules other than (0) and itself. A left R-module M is said to be semisimple if it can be written as a direct product of of simple left sub-R-modules. A ring R is said to be left semisimple if it is semisimple when viewed as a left module over itself. A simple left sub-R-module of R is a minimal left ideal, that is, a non-zero left ideal of R that does not contain any left ideals other than (0) and itself. We say that a ring R is simple if it has no two-sided ideals other than (0) and itself. Note that a simple ring is not necessarily simple as a left module over itself. An example is the matrix ring $M_n(\mathbb{C})$ which has no proper two-sided ideals but the set $\mathrm{Col}(j)$ of matrices with entries only in the j-th column is a non-zero proper left ideal. Also, our definition of simple rings does not imply that they are semisimple.

Lemma 7. *If a ring R is a direct sum of left ideals, say $R = \bigoplus_{i \in I} L_i$, then only finitely many L_i are non-zero. In particular, a left semisimple ring is a finite direct sum of minimal left ideals.*

Proof. Since every element of the direct sum has finite support by definition, we may write $1 = e_1 + \ldots + e_n$ uniquely where $e_i \in L_i$. Let $a \in L_j$ for $j \neq 1, \ldots, n$. Then

$$a = a1 = ae_1 + \ldots + ae_n \in L_j \cap (L_1 \oplus \ldots \oplus L_n) = \{0\}.$$

This implies that $L_j = \{0\}$ and $R = \bigoplus_{i=1}^n L_i$.

If R is left semisimple, then R is semisimple as a left R-module. By definition this means that R is a direct sum of simple submodules. Thus R is a direct sum of minimal left ideals and by the above, this sum is finite. □

Let R be a ring. A left R-module M is said to be Artinian if it has the descending chain condition on left submodules. That is, any descending chain of left sub-R-modules of M

$$M_1 \supset M_2 \supset M_3 \supset \dots$$

stabilizes, meaning that there is a rank n such that $M_m = M_n$ for all $m \geq n$. Artinian modules have the property that any submodule contains a minimal submodule with respect to inclusion.

A ring R is said to be left Artinian if it is Artinian when viewed as a left module over itself. A left Artinian ring has the property that every non-zero left ideal of R contains a minimal left ideal.

Let R be a ring. We define the left Jacobson radical, $J(R)$, of R to be the intersection of all left maximal ideals of R. This is a left ideal of R.

Proposition 34. *Let R be a ring. The following statements are equivalent for $x \in R$:*

(i) $x \in J(R)$.

(ii) $1 - z$ *is left invertible for all* $z \in Rx$.

(iii) $xM = \{0\}$ *for every simple left R-module M.*

Proof. (i) implies (ii): Suppose that $x \in J(R)$ and by contradiction that there exists $r \in R$ such that $1 - rx$ is not left invertible. Then $R(1 - rx)$ is a proper left ideal of R and is contained in some maximal ideal I. But $rx \in J(R)$ since $J(R)$ is a left ideal and $J(R) \subset I$. Thus $1 = (1 - rx) + rx \in I$ so that $I = R$ and this is a contradiction.

(ii) implies (iii): Suppose that $1 - z$ is left invertible for all $z \in Rx$ and by contradiction that there is a simple left R-module M such that $xM \neq \{0\}$. Then there exists a non-zero $m \in M$ such that $xm \neq 0$ and thus the left ideal Rxm is non-zero. This is a non-zero submodule of M and by simplicity $Rxm = M$. Therefore, there exists $r \in R$ with $rxm = m$. In other words, $(1 - rx)m = 0$. Let $u \in R$ such that $1 = u(1 - rx)$. Then $m = u(1 - rx)m = 0$ which is a contradiction.

(iii) implies (i): For every maximal left ideal I of R, R/I is a simple left R-module. By assumption $x(R/I) = \{0\}$ which implies that $x \in I$. Thus $x \in J(R)$. □

An ideal I of R is said to be nilpotent if $I^m = \{0\}$ for some integer m.

Proposition 35. *Let R be a ring. The left Jacobson radical $J(R)$ contains all nilpotent left ideals of R.*

Proof. In fact, let I be a nilpotent left ideal and let m be such that $I^m = \{0\}$. Let $x \in I$. For all $r \in R$ we have $rx \in I$ and therefore $(rx)^m = 0$. In particular $1 - (rx)^m = 1$ which can be written as

$$(1 + (rx) + (rx)^2 + \ldots + (rx)^{m-1})(1 - rx) = 1.$$

This proves that $1 - rx$ is left invertible and thus $x \in J(R)$ by Proposition 34. □

Lemma 8. *A left semisimple ring R is left Artinian and $J(R) = \{0\}$.*

Proof. A simple left submodule of R, that is, a minimal left ideal of R, is certainly left Artinian. A finite direct sum of left Artinian modules is again left Artinian. Therefore, by Lemma 7, a left semisimple ring is left Artinian.

By Lemma 7, we may write $R = \bigoplus_i L_i$ where the L_i are minimal left ideals and the sum is finite. Let $M_j = \bigoplus_{i \neq j} L_i$. Then $R/M_j \cong L_j$ which is a simple left module. Thus M_j is a maximal left ideal of R. Finally, we have $J(R) \subset \bigcap_j M_j = \{0\}$. □

Proposition 36. *A left semisimple ring R is isomorphic as a ring to a direct product of simple left Artinian rings which are two-sided ideals of R.*

Proof. By Lemma 7, we may write $R = \bigoplus_i L_i$ where the L_i are minimal left ideals of R and the sum is finite. For each pair L_i and L_j, L_iL_j is a also a left ideal and it is contained in L_j since L_j is a left ideal. By minimality of L_j we must have that L_iL_j is either $\{0\}$ or L_j. Suppose that $L_iL_j = L_j$. Then there exists $x \in L_j$ such that $L_ix \neq \{0\}$. Then $m_x : L_i \longrightarrow L_j, y \longmapsto yx$ is a non-zero left R-module homomorphism. The kernel of this map is a left ideal and by simplicity of L_i it must be $\{0\}$ so m_x is injective. The image L_ix is non-zero and by simplicity of L_j we have $L_ix = L_j$. In particular, m_x is an isomorphism of left R-modules.

We claim that $L_iL_j \neq \{0\}$ is an equivalence relation on the set of ideals L_i. In fact, let us first prove that $L_i^2 \neq \{0\}$. Suppose that $L_i^2 = \{0\}$ by contradiction. Then L_i is a nilpotent left ideal and is contained in $J(R)$ by Proposition 35. By Lemma 8 we have $L_i = \{0\}$ which is the desired contradiction. Suppose that $L_iL_j \neq \{0\}$. Then $L_iL_j = L_j$ and $L_jL_iL_j = L_jL_j \neq \{0\}$ so that $L_jL_i \neq \{0\}$. Finally, if $L_iL_j \neq \{0\}$ and $L_jL_k \neq \{0\}$, then $L_iL_k = L_iL_jL_k = L_jL_k \neq \{0\}$.

Regroup the finite direct sum $R = \bigoplus_i L_i$ according to equivalence classes and for each class form the direct sum of all L_i in that class and call this A_j. This gives a decomposition $R = A_1 \oplus \ldots \oplus A_n$ for some n.

For each i, A_i is a direct sum of left ideals and is therefore itself a left ideal. We claim that it is also a right ideal of R. To see this we need to prove that $A_iR \subset A_i$. Let L and L' be two minimal left ideals such that $L \sim L_i$ and $L' \sim L_j$ for some $j \neq i$. Then we have $LL' = \{0\}$. Consequently, we see that for $j \neq i$ we have

$$A_iA_j = \left(\sum_{L \cong L_i} L\right)\left(\sum_{L' \cong L_j} L'\right) \subset \sum LL' = \{0\}.$$

We therefore have

$$A_iR = A_i(A_1 \oplus \ldots \oplus A_n) =\subset A_iA_1 + \ldots + A_iA_n = A_iA_i \subset A_i$$

since A_i is a left ideal. This proves that A_i is a right ideal.

Since A_i is a left ideal we have $A_iA_i \subset A_i$ which shows that A_i is closed under multiplication. In order for A_i to be a ring we only need to show that it has a unit element. Let $1 = e_1 + \ldots + e_n$ with $e_i \in A_i$. Then for any $a_i \in A_i$ we have

$$e_ia_i = e_1a_i + \ldots + e_na_i = 1a_i = a_i$$

since $e_ja_i = 0$ for all $j \neq i$ since $A_jA_i = \{0\}$. The same reasoning shows that $a_ie_i = a_i$. This proves that A_i is a ring. Moreover, the fact that $A_jA_i = \{0\}$ for $i \neq j$ shows that addition and multiplication in R is done componentwise. Therefore, as rings we have an isomorphism

$$R \cong A_1 \times \ldots \times A_n.$$

There is a surjective ring homomorphism $R \longrightarrow A_i$ for each i. Thus any left ideal of A_i is also a left R-module and therefore a left ideal of R. It follows that each A_i is left Artinian since by Proposition 8 R is left Artinian. It remains to prove that the A_i are simple rings.

By construction, we may write $A_i = \bigoplus_j L_j$ where the L_j are minimal left ideals of R such that $L_jL_k = L_k$. Let I be a two-sided ideal of A_i. Then IL_j is a left ideal contained in L_j. It is therefore either $\{0\}$ or L_j. Suppose that $IL_j = \{0\}$. Then for every k we have $IL_k = IL_jL_k = \{0\}$. In this case, $I = IA_i = \sum_k IL_k = \{0\}$. Otherwise, $IL_j = L_j$ for all j. But I is a right ideal so $IL_j \subset I$. It follows that $L_j \subset I$ and therefore $A_i \subset I$ which implies $I = A_i$. This proves that A_i has no two-sided ideals, that is, A_i is a simple ring. □

4.2.2 Division Rings

By a division ring D, we mean a not necessarily commutative ring with the property that every non-zero element of D is multiplicatively invertible. In other words, the set $D \setminus \{0\}$ with the multiplication law forms a not necessarily commutative group. A commutative division ring is a field and a non-commutative division ring is also sometimes called a skew-field. In Example 4 we saw that the Hamilton quaternion algebra over $\mathbb{Q}$ is an example of a non-commutative division ring.

Non-commutative division rings D share many properties with fields and many of the classical theorems of linear algebra do not make use of the commutativity of multiplication in fields. For example D-modules, which we shall call D-vector spaces, behave much like actual vector spaces. Note that because of the non-commutativity one needs to specify whether it is a left or right module. Any left (or right) D-vector space V has a basis and the number of elements in a basis is independent of the choice of basis. We call this number the dimension of V over D and denote it by $\dim_D V$. Any linearly independent set of elements in V can be completed to form a basis of V. If W is a sub-D-vector space, then there exists a complementary module W' so that $V = W \oplus W'$ and $\dim_D V = \dim_D W + \dim_D W'$. Finally, if $f : V_1 \longrightarrow V_2$ is a homomorphism between finite-dimensional left D-vector spaces, then

$$\dim_D V_1 = \dim_D \ker f + \dim_D \mathrm{im} f.$$

Let D be a division ring and let V be a left D-vector space of finite dimension. Let $\{x_1, \ldots, x_n\}$ be a basis of V. For any $f \in \mathrm{Hom}_D(V, V) = \mathrm{End}_D(V)$ we may write

$$f(x_j) = \sum_{i=1}^{n} a_{ij} x_i$$

and associate the $n \times n$ matrix $(a_{ij})^t$ to f with coefficients in D. This gives a map

$$\operatorname{End}_D(V) \longrightarrow M_n(D), \qquad f \longmapsto (a_{ij})^t.$$

This is an isomorphism of groups, it maps id_V to the identity matrix but it reverses multiplication in $M_n(D)$. We therefore have an isomorphism of rings

$$\operatorname{End}_D(V) \cong M_n(D)^{op} \cong M_n(D^{op}). \tag{4.2.0.1}$$

If V was a right D-vector space, we would write

$$f(x_j) = \sum_{i=1}^{n} x_i a_{ij}$$

and assign to f the matrix (a_{ij}). This gives a ring isomorphism $\operatorname{End}_D(V) \cong M_n(D)$.

Proposition 37. *Let D be a division ring. Then $M_n(D)$ is both a left (and right) semisimple ring and a simple left (and right) Artinian ring.*

Proof. For each $j = 1, \ldots, n$ we denote by $\mathrm{Col}(j)$ the subspace of $M_n(D)$ consisting of matrices with entries only in the j-th column. This is left ideal of $M_n(D)$. If E_{ij} denotes the matrix whose (i, j) entry is 1 and all other entries are zero, then $(E_{ij})_{i=1}^n$ is a basis for $\mathrm{Col}(j)$ as a left D-vector space. Let I be a non-zero left ideal of $M_n(D)$ that is contained in $\mathrm{Col}(j)$. Let B be a non-zero element in I. Then there exist elements d_i in D such that $B = \sum_{i=1}^n d_i E_{ij}$. Since B is non-zero, there exists an index i_0 such that d_{i_0} is non-zero and thus invertible in D. Therefore we have

$$E_{i_0 j} = d_{i_0}^{-1} E_{i_0 i_0} B \in I$$

since I is a left ideal. But then $E_{ij} = E_{ii_0} E_{i_0 j} \in I$ since I is a left ideal and this is true for all $i = 1, \ldots, n$. Thus I contains the basis $(E_{ij})_i$ of $\mathrm{Col}(j)$ so that $I = \mathrm{Col}(j)$. This proves that $\mathrm{Col}(j)$ is a minimal left ideal of $M_n(D)$. Since $M_n(D) = \bigoplus_{j=1}^n \mathrm{Col}(j)$ we have proved that $M_n(D)$ is left semisimple. One can similarly prove that $M_n(D)$ is right semisimple by using rows instead of columns in the above. By Lemma 8 $M_n(D)$ is both left and right Artinian.

Let $k \neq j$ and consider the map

$$\mathrm{Col}(j) \longrightarrow \mathrm{Col}(k), \qquad \sum_i d_i E_{ij} \longmapsto \sum_i d_i E_{ik}.$$

This is simply multiplication on the right by E_{jk} so that the left multiplication is preserved by this map. Therefore it is a left $M_n(D)$-module homomorphism. It is clearly an isomorphism.

Suppose that I is a non-zero two-sided ideal of $M_n(D)$. Let A be a non-zero matrix in I. Then it has a non-zero entry, say $a_{ij} \neq 0$. Since it is a two-sided ideal, I contains the matrix $E_{ki} A E_{jl} = a_{ij} E_{kl}$. Since D is a division ring, a_{ij} is invertible and thus I contains E_{kl} for all k, l. But this is a basis for $M_n(D)$ so that $I = M_n(D)$. This proves that $M_n(D)$ is simple. □

4.2.3 Classification of Simple Artinian Rings

We have just seen that a matrix ring over a division ring is a simple Artinian ring. We will now prove the converse: every simple Artinian ring is isomorphic to a matrix ring over a division ring. We need some lemmas.

Lemma 9 (Schur)**.** *Let R be a ring and let M be a simple left R-module. Then* $\mathrm{End}_R(M)$ *is a division ring.*

Proof. Let $f : M \longrightarrow M$ be a non-zero R-module homomorphism. Then $\ker f$ is a left sub-R-module of M. By simplicity, it is either trivial or all of M. Since f is not the zero map, the kernel must be trivial. This proves injectivity. The image $\mathrm{im} f$ is also a left sub-R-module of M and must be either trivial or all of M. Since f is not the zero map the latter must be true and this proves surjectivity. As a consequence f is an isomorphism and therefore invertible in $\mathrm{End}_R(M)$. □

Let R be a ring and let M be a left R-module. Let $D = \mathrm{End}_R(M)$. Note that M is a left D-module, the action being given by

$$D \times M \longrightarrow M, \qquad (f, m) \longmapsto f(m).$$

Define a map

$$\lambda : R \longrightarrow \mathrm{End}_D(M), \qquad r \longmapsto (\lambda_r : m \mapsto rm).$$

This is well-defined. In fact, if $f \in D$, then

$$\lambda_r(f(m)) = rf(m) = f(rm) = f(\lambda_r(m))$$

since f is a left R-module homomorphism. Therefore $\lambda_r \in \mathrm{End}_D(M)$ for all $r \in R$. Moreover, the map λ is a ring homomorphism. In fact, it is easily seen to be a group homomorphism. Also, $\lambda_1(m) = 1.m = m$ for all $m \in M$ so that $\lambda_1 = \mathrm{id}_M$. Finally, if $r, r' \in R$ then

$$\lambda_{rr'}(m) = (rr')(m) = r(r'm) = \lambda_r \circ \lambda_{r'}(m), \qquad \text{for all } m \in M$$

so that $\lambda_{rr'} = \lambda_r \circ \lambda_{r'}$.

Theorem 4.2.1 (Rieffel)**.** *Let R be a simple ring and let M be a non-zero left ideal of R. Let $D = \mathrm{End}_R(M)$. Then the above defined map $\lambda : R \longrightarrow \mathrm{End}_D(M)$ is a ring isomorphism.*

Proof. Since λ is a ring homomorphism, the kernel of λ is a two-sided ideal of R. Since $\lambda_1 = \mathrm{id}_M$, λ is not the zero map and this kernel can not be all of R. By simplicity of R we must have $\ker \lambda = \{0\}$. Is remains to prove that λ is surjective.

We claim that $\lambda(M)$ is a left ideal in $\mathrm{End}_D(M)$. Let $f \in \mathrm{End}_D(M)$ and $x \in M$. For $m \in M$ we have $f \circ \lambda(x)(m) = f(xm)$. Consider

$$L_m : M \longrightarrow M, \qquad u \longmapsto um.$$

This is a left R-module homomorphism. Indeed, if $r' \in R$ then $L_m(r'u) = (r'u)m = r'(um) = r'L_m(u)$. This shows that $L_m \in D$. But $f \in \mathrm{End}_D(M)$ and therefore we have

$$f \circ \lambda(x)(m) = f(xm) = f(L_m(x)) = L_m(f(x)) = f(x)m = \lambda_{f(x)}(m).$$

This proves that $f \circ \lambda(x) = \lambda \circ f(x) \in \lambda(M)$ for all $x \in M$. This proves that $\lambda(M)$ is indeed a left ideal in $\mathrm{End}_D(M)$.

Consider MR. Since M is a left ideal, this is a two-sided ideal of R. It is non-zero because M is non-zero and MR contains M. By simplicity of R we must have $MR = R$. Then $\lambda(R) = \lambda(MR) = \lambda(M)\lambda(R)$. This proves that $\lambda(R)$ is a left ideal of $\mathrm{End}_D(M)$ since $\lambda(M)$ is a left ideal. Since $1 \in \lambda(R)$ we obtain $\lambda(R) = \mathrm{End}_D(V)$. □

Lemma 10. *Let D be a division ring and let M be a left D-module. Then $\mathrm{End}_D(M)$ is left Artinian if and if $\dim_D M < \infty$.*

Proof. Suppose that $\dim_D M = n$. Then by (4.2.0.1) we have $\mathrm{End}_D(M) \cong M_n(D^{op})$ as rings and by Proposition 37 $M_n(D^{op})$ is left Artinian.

Suppose that $\dim_D M = \infty$. Then we can create an ascending chain of subspaces

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \dots$$

where M_i has dimension i over D. Define $L_i = \{f \in \mathrm{End}_D(M) \ : \ f(M_i) = 0\}$. This is a left ideal of $\mathrm{End}_D(M)$. Moreover, we have $L_i \supsetneq L_{i+1}$ since it is always possible to construct a linear form that vanishes on i basis elements but not on the other ones. We have therefore constructed an infinite descending chain of left ideals

$$L_1 \supsetneq L_2 \supsetneq L_3 \supsetneq \dots$$

and therefore M is not left Artinian. □

Theorem 4.2.2. *Let R be a simple left Artinian ring, let M be a minimal left ideal of R, let $D = \mathrm{End}_R(M)$ and $n = \dim_D M$. Then*

$$R \cong \mathrm{End}_D(M) \cong M_n(D^{op}).$$

Proof. By Lemma 9 D is a division ring. By Theorem 4.2.1, R is isomorphic to $\mathrm{End}_D(M)$ as a ring. Since R is left Artinian, the same is true for $\mathrm{End}_D(M)$. By Lemma 10 M is of finite dimension over D, say n. By (4.2.0.1), we have $\mathrm{End}_D(M) \cong M_n(D^{op})$ as rings. □

Corollary 21. *A ring is simple and left Artinian if and only if it is isomorphic to a matrix ring over a division ring.*

Corollary 22. *The center of an Artinian simple ring R is a field.*

Proof. By Theorem 4.2.2 R is of the form $M_n(D)$ where D is a division ring. The center $Z(D)$ of D is clearly a field and the center of $M_n(D)$ consists of scalar matrices with coefficients in $Z(D)$, that is, matrices of the form xI_n with $x \in Z(D)$ and where I_n denotes the size n identity matrix. Thus the center of R is isomorphic to $Z(D)$ which is a field. □

Corollary 23. *A ring is left semisimple if and only if it is isomorphic to a direct product of matrix rings over division ring.*

Proof. Let R be a left semisimple ring. By Proposition 36 R is isomorphic to a direct product of simple left Artinian rings, say $R \cong A_1 \times \dots \times A_m$. By Theorem 4.2.2, each A_i is isomorphic to a matrix ring over a division ring, say $A_i \cong M_{n_i}(\Delta_i)$. Thus

$$R \cong M_{n_1}(\Delta_1) \times \dots \times M_{n_m}(\Delta_m).$$

Conversely, let D be a division ring. By Proposition 37 $M_n(D)$ is left semisimple. A direct product of left semisimple rings is again left semisimple. □

Corollary 24. *A ring is left semisimple if and only if it is right semisimple.*

Proof. Follows from Proposition 37 which says that $M_n(D)$ is both left and right semisimple for a division ring D. □

4.2.4 Uniqueness of Decompositions

We have seen that simple Artinian rings are isomorphic to matrix rings over division rings. We now examine the uniqueness of the size of the matrix ring and the division ring.

Proposition 38. *Let R be a simple left Artinian ring. All non-zero simple left R-modules are isomorphic. In particular, if $R \cong M_n(D) \cong M_{n'}(D')$ where D and D' are division rings, then $n = n'$ and $D \cong D'$.*

Proof. Let M be a non-zero simple left R-module and let L be any minimal left ideal of R. Then LM is a left sub-R-module of M. By simplicity of M we either have $LM = \{0\}$ or $LM = M$. Suppose that the former is true. Then $L \subset \mathrm{Ann}_R(M)$. The annihilator of M is a two-sided ideal of R. By simplicity of R it must be $\{0\}$ and therefore $L = \{0\}$ which is not possible. Therefore we have $LM = M$. Let $x \in M$ be an element such that $Lx \neq \{0\}$. Then the multiplication-by-x map

$$L \longrightarrow M, \qquad y \mapsto yx$$

is a non-zero left R-module homomorphism. By simplicity of L and M it is an isomorphism.

Let $R = M_n(D)$ and $R' = M_{n'}(D')$ and let $\phi : R \longrightarrow R'$ be an isomorphism of rings. Let $L = \mathrm{Col}(1)$ in R and let $L' = \mathrm{Col}(1)$ in R'. By Proposition 37, L and L' are minimal left ideals of R and R' respectively. The preimage $\phi^{-1}(L')$ is a minimal left ideal of R and by the first part, there exists an isomorphism between L and $\phi^{-1}(L')$. We may view L' as a left R-module via ϕ. We then have an isomorphism $f : L \longrightarrow L'$ of left R-modules. Consider now the map

$$\mathrm{End}_R(L) \longrightarrow \mathrm{End}_R(L'), \qquad \alpha \longrightarrow f\alpha f^{-1}.$$

This is well-defined homomorphism of groups in that $f\alpha f^{-1}$ does indeed belong to $\mathrm{End}_R(L')$ whenever α belongs to $\mathrm{End}_R(L)$. It is injective and surjective because f is an isomorphism. Moreover, id_L is mapped to $\mathrm{id}_{L'}$ and $\alpha\alpha'$ is mapped to $f\alpha\alpha' f^{-1} = f\alpha f^{-1} f\alpha' f^{-1}$. We conclude that it is an isomorphism of rings.

The ideal L is a left D-module of dimension n. Let $\Delta = \mathrm{End}_D(L)$. Then $\Delta \cong M_n(D^{op})$ and $\mathrm{End}_\Delta(L) \cong \mathrm{End}_{M_n(D)}(L)^{op}$. By Theorem 4.2.1 we have $D \cong \mathrm{End}_{M_n(D)}(L)^{op} = \mathrm{End}_R(L)^{op}$. Similarly, one shows that $D' \cong \mathrm{End}_{R'}(L')^{op} = \mathrm{End}_R(L')^{op}$. We conclude that $D \cong D'$. Finally, the left R-module isomorphism $f : L \longrightarrow L'$ is in particular a left D-module isomorphism. Therefore $n = \dim_D L = \dim_D L' = n'$. □

Proposition 39. *Let $R = A_1 \oplus \ldots \oplus A_m$ be a decomposition of a ring R where each A_i is a minimal two-sided ideal of R. Any two such decomposition are the same up to permutation.*

Proof. Let I be a non-zero two-sided ideal of R. Then $IA_i \subset A_i$ is a two-sided ideal. By minimality we either have $IA_i = \{0\}$ or $IA_i = A_i$. Thus $IR = \sum_{i=1}^m IA_i = \sum A_i$ where the last sum is over those i for which $IA_i = A_i$. Thus any two-sided ideal is a sum of the A_i and therefore the minimal two-sided ideals of R are exactly the A_i. □

From Proposition 36 the minimal two-sided ideals A_i are simple rings and we have a ring isomorphism

$$R \cong A_1 \times \ldots \times A_m.$$

Moreover, we have $A_iA_j = \{0\}$ whenever $i \neq j$.

Corollary 25. *The decomposition of a semisimple ring into a direct product of simple rings is unique up to isomorphism.*

Proof. Suppose that $R = A_1 \times \ldots \times A_m$. Then $A_i' = \{0\} \times \ldots \times A_i \times \ldots \times \{0\}$ is a minimal two-sided ideal of R and $R = A_1' \oplus \ldots \oplus A_m'$ and this decomposition is unique up to order. □

4.3 Semisimple Algebras

A ring is central over a field k if k is exactly its center. A k-algebra is a ring with a copy of k in its center, making it into a k-vector space and a ring simultaneously. A k-algebra homomorphism is a k-linear ring homomorphism. By a finite-dimensional semisimple k-algebra, we mean a k-algebra which is of finite dimension over k and semisimple as a ring.

If A is an algebra, then we give it the Lie bracket

$$[\cdot,\cdot] : A \times A \longrightarrow A, \qquad [a,b] = ab - ba.$$

It is bilinear, skew-symmetric and satisfies the Jacobi identity. Note that if I is a two-sided ideal of A, then if $a \in I$ and $b \in B$, then $[a,b] \in I$. The Lie bracket is very useful in that the center of A is characterized as follows:

$$Z(A) = \{a \in A \,:\, [a,b] = 0, \text{ for all } b \in A\}.$$

Theorem 4.3.1. *Let A be a finite-dimensional semisimple k-algebra. Then A is isomorphic as a k-algebra to a finite product of matrix rings $M_{n_i}(\Delta_i)$ over division rings Δ_i whose center is a finite field extension of k. The integers n_i and the division rings Δ_i are unique up to k-algebra isomorphism and the decomposition of A is unique up to permutation.*

Proof. Since A is a semisimple ring, by Corollary 23 A is isomorphic as a ring to a finite product of matrix rings over division rings, say

$$A \cong A_1 \times \ldots \times A_m \cong M_{n_1}(\Delta_1) \times \ldots \times M_{n_m}(\Delta_m).$$

This decomposition is unique up to order and ring isomorphism. Here the A_i are the minimal two-sided ideals of A. They are simple rings. Each A_i contains k in its center and therefore each A_i is a simple k-algebra and the above isomorphisms are ones of k-algebras. For each i, the center of $M_{n_i}(\Delta_i)$ is the set of scalar matrices with coefficients in $Z(\Delta_i)$ and it is therefore isomorphic to the center $Z(\Delta_i)$. Since $M_{n_i}(\Delta_i)$ is a k-algebra, this implies that k is contained in $Z(\Delta_i)$. By Theorem 4.2.2, $\Delta_i \cong \mathrm{End}_{A_i}(L_i)^{op}$ where L_i is a minimal left ideal of A_i. Since A_i is finite-dimensional over k it is also true that Δ_i is finite-dimensional over k. It follows that $Z(\Delta_i)$ is a finite field extension of k. □

Proposition 40. *Let A be a central simple algebra over k and let B be a simple k-algebra. Then $A \otimes_k B$ is a simple k-algebra. Moreover, $Z(A \otimes_k B) = Z(B)$, that is, any element of the center of $A \otimes_k B$ has the form $1 \otimes b$ for some unique $b \in Z(B)$. In particular, if B is a central simple k-algebra, then so is $A \otimes_k B$.*

Proof. The tensor product $A \otimes_k B$ is a k-vector space. It has a ring structure given on basis elements by

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$$

and extended linearly to all elements.

We will now prove that it is simple. We assume here that the dimension of B over k is finite for simplicity. The proof in the general case is similar to the one we now produce.

Let $b_1, \ldots, b_r$ be a basis of B over k. Any element $x \in A \otimes_k B$ can be written as $\sum_{i=1}^r a_i \otimes b_i$ with $a_i \in A$. Define the length of $\sum_{i=1}^r a_i \otimes b_i$ to be $|\{i : a_i \neq 0\}|$. Let I be a non-zero two-sided ideal of $A \otimes_k B$ and choose $x \in I$ a non-zero element of minimal length. By reordering the b_i, we may assume that

$$x = 1 \otimes b_1 + \sum_{i=2}^r a_i \otimes b_i$$

with $a_i \in A$. For all $a \in A$ we compute that

$$[a \otimes 1, x] = \sum_{i=2}^r [a, a_i] \otimes b_i.$$

Since $x \in I$ we have $[a \otimes 1, x] \in I$. Since the length of $[a \otimes 1, x]$ is less than the one of x, by minimality we must have $[a \otimes 1, x] = 0$ for all $a \in A$. This implies that $[a, a_i] = 0$. In other words, $aa_i = a_i a$ for all $a \in A$ so that $a_i \in Z(A) = k$ for $i = 2, \ldots, r$. But then

$$x = 1 \otimes b_1 + \sum_{i=2}^r 1 \otimes (a_i b_i) = 1 \otimes b$$

where $b = b_1 + \sum_{i=2}^r a_i b_i \in B \setminus \{0\}$. For any $b_1, b_2 \in B$ we have

$$(1 \otimes b_1)x(1 \otimes b_2) = 1 \otimes (b_1 b b_2) \in I$$

since I is an ideal. Thus $BbB \subset B$ is a non-zero two-sided ideal of B. By simplicity $BbB = B$ and thus $1 \otimes B \subset I$ which implies that $A \otimes_k B = I$. This proves that $A \otimes_k B$ is simple.

Let $x = \sum_{i=1}^r a_i \otimes b_i$ be an element of $Z(A \otimes_k B)$. Then for all $a \in A$ we have

$$0 = [a \otimes 1, x] = \sum_{i=1}^r [a, a_i] \otimes b_i.$$

This implies that $[a, a_i] = 0$ for all $a \in A$ so that $a_i \in Z(A) = k$ for $i = 1, \ldots, r$. We may then write

$$x = 1 \otimes \left(\sum_{i=1}^{r} a_i b_i \right) =: 1 \otimes b.$$

For all $x \in B$ we have $0 = [1 \otimes y, x] = 1 \otimes [y, b]$ so that $b \in Z(B)$. □

Corollary 26. *Let A be a central simple k-algebra and let K be a field extension of k. Then $A \otimes_k K$ is a central simple K-algebra.*

Lemma 11. *There are no proper finite-dimensional division algebras over an algebraically closed field.*

Proof. Assume that k is algebraically closed and let D be a finite-dimensional division k-algebra. Let $x \in D \setminus k$. Since D is finite-dimensional over k and $k(x)$ is contained in D, the extension $k(x)/k$ must be finite and thus algebraic. Since k is algebraically closed, this forces $k(x) = k$ and thus $x \in k$. This proves that $D = k$. □

Definition 12. Let A be a central simple k-algebra. A field extension K of k is called a splitting field for A if $A \otimes_k K$ is isomorphic to a matrix ring over K.

Definition 13. Let A be a central simple k-algebra and let K be a splitting field of k. Let $\phi : A \otimes_k K \longrightarrow M_n(K)$ be a K-algebra isomorphism. Define the reduced trace and the reduced norm on A to be the composite maps

$$\mathrm{tr}_r : A \xrightarrow{\mathrm{id} \otimes 1} A \otimes_k K \xrightarrow{\phi} M_n(K) \xrightarrow{\mathrm{tr}} K$$

and

$$N_r : A \xrightarrow{\mathrm{id} \otimes 1} A \otimes_k K \xrightarrow{\phi} M_n(K) \xrightarrow{\det} K$$

Example 5. In Example 4, we saw that a splitting field of the 4-dimensional central division $\mathbb{Q}$-algebra $H_{\mathbb{Q}}$ is $K = \mathbb{Q}(\alpha, \beta)$ where $\alpha^2 + \beta^2 = -1$. An element of $\alpha = x + yi + zj + tk \in H_K = H_{\mathbb{Q}} \otimes_{\mathbb{Q}} K$ is expressed in matrix form as

$$\begin{pmatrix} x + y\alpha + z\beta & y\beta - z - t\alpha \\ y\beta + z - t\alpha & x - y\alpha - t\beta \end{pmatrix}.$$

Thus $\mathrm{tr}_r(\alpha) = 2x$ and $N_r(\alpha) = x^2 + y^2 + z^2 + t^2$.

Proposition 41. *Let A be a finite-dimensional central algebra A over a field k. Let $\bar{k}$ denote a fixed algebraic closure of k. Then $\bar{k}$ is a splitting field for A. In particular, $\dim_k A$ is a perfect square.*

Proof. Denote by $\bar{k}$ a fixed algebraic closure of k. By Corollary 26, $A \otimes_k \bar{k}$ is a finite-dimensional simple central $\bar{k}$-algebra. By Proposition 4.3.1, $A \otimes_k \bar{k}$ is isomorphic as a $\bar{k}$-algebra to a matrix algebra over a finite-dimensional division $\bar{k}$-algebra. By Lemma 11 there are no finite-dimensional division algebras over $\bar{k}$ other than $\bar{k}$ itself. Thus $A \otimes_k \bar{k}$ is isomorphic to $M_n(\bar{k})$ for some integer n. In other words, $\bar{k}$ is a splitting field for A. Consequently, we have

$$\dim_k A = \dim_{\bar{k}} A \otimes_k \bar{k} = \dim_{\bar{k}} M_n(\bar{k}) = n^2.$$

□

4.4 Schur Indices

We now relate our discussion of semisimple algebras to the theory of representations and more precisely to the question of rationality of representations. Here, K will denote a field of characteristic zero and C will denote a fixed algebraic closure of K. Let G be a finite group. Then the group ring $K[G]$ is a finite-dimensional K-algebra. It is semisimple by Proposition 16 whose proof does not require K to be algebraically closed. Therefore $K[G]$ decomposes into a direct sum of finite dimensional simple K-algebras by Proposition 4.3.1. Going through the proof of Proposition 36, we see that this decomposition corresponds to the canonical decomposition of $K[G]$ as a representation. But $K[G]$ is the regular representation of G over K and by Corollary 16 this decomposition is given by

$$K[G] \cong A_1 \times \ldots \times A_h$$

where A_i is the simple component of $K[G]$ corresponding the irreducible character χ_i of G over K. Let V_i be a representation of G with character χ_i and denote by n_i its dimension over K. Then A_i is isomorphic as a left $K[G]$-module to the direct sum of n_i copies of V_i. The representation V_i is the minimal left ideal of the simple ring A_i. We say the minimal left ideal because by Proposition 38 all minimal left ideals of A_i are isomorphic as left modules. By Proposition 4.3.1 and Proposition 38, each A_i is isomorphic as a K-algebra to a matrix ring over a division ring, say $M_{l_i}(\Delta_i)$, where $l_i = \dim_{\Delta_i} V_i$ and $\Delta_i \cong (\mathrm{End}_{A_i}(V_i))^{op}$. Note that $\mathrm{End}_{A_i}(V_i) = \mathrm{End}_{K[G]}(V_i)$ since the left action of $K[G]$ on V_i is left multiplication which is done componentwise with respect to the decomposition $K[G]$ into the direct product of the A_i. Summing this up, we have a K-algebra isomorphism

$$K[G] \cong M_{l_1}(\mathrm{End}_{K[G]}(V_1)^{op}) \times \ldots \times M_{l_h}(\mathrm{End}_{K[G]}(V_h)^{op}).$$

By Proposition 41, C is a splitting field of each A_i. It follows that we have an isomorphism of C-algebras

$$C[G] \cong M_{l_1}(C) \times \ldots \times M_{l_h}(C).$$

Definition 14. With the above notations, denote by $Z(\Delta_i)$ the center of Δ_i. Since Δ_i is of finite-dimension over K and $Z(\Delta_i)$ contains K as a subfield, Δ_i is of finite dimension over $Z(\Delta_i)$. Thus Δ_i is a finite-dimensional central division $Z(\Delta_i)$-algebra. By Proposition 41, we have $[\Delta_i : Z(\Delta_i)] := \dim_{Z(\Delta_i)} \Delta_i = m_i^2$ for some integer m_i. This integer m_i is called the Schur index of the character χ_i over K.

Proposition 42. *Let G be a finite group. Let $\chi_1, \ldots, \chi_h$ denote the irreducible characters of G over K and let m_i be their respective Schur indices. Then the family of characters $\{\chi_i/m_i\}_{i=1}^h$ forms a $\mathbb{Z}$-basis of $R(G, K)$.*

Proof. See § 12.2 Proposition 35 of [Se1]. □

Theorem 4.4.1. *Let χ be an irreducible character of G over C. Then there is an irreducible representation of G over $K(\chi)$ with character χ' such that $\chi' = m\chi$, where m is the Schur index of χ' over $K(\chi)$. Furthermore, the character $\phi = \mathrm{tr}_{K(\chi)/K} \circ \chi'$ is the character of an irreducible representation of G over K.*

Proof. Let V_i be the distinct (up to isomorphism) irreducible representations of G over $K(\chi)$ with characters χ_i. Let $D_i = \mathrm{End}_{K(\chi)[G]} V_i$ and denote by E_i the center of D_i so that the Schur index m_i of χ_i over $K(\chi)$ satsifies $m_i^2 = [D_i : E_i]$. Evidently χ takes values in $K(\chi)$ and thus $\chi \in R(G, K(\chi))$. By Proposition 42, there exist integers d_i such that $\chi = \sum_i d_i \frac{\chi_i}{m_i}$. By Proposition 30, we have

$$\langle \chi_i, \chi_j \rangle_G = \begin{cases} \dim_{K(\chi)} D_i & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Since χ is assumed to be irreducible, we obtain

$$\begin{aligned} 1 = \langle \chi, \chi \rangle_G &= \sum_i \frac{d_i^2}{m_i^2} \langle \chi_i, \chi_i \rangle_G = \sum_i \frac{d_i^2}{m_i^2} [D_i : K(\chi)] \\ &= \sum_i \frac{d_i^2}{m_i^2} [D_i : E_i][E_i : K(\chi)] = \sum_i d_i^2 [E_i : K(\chi)]. \end{aligned}$$

This implies that all d_i are zero except for one, say d_{i_0}, and moreover, $d_{i_0}^2 = 1$ and $E_{i_0} = K(\chi)$. As a consequence, we have $m_{i_0}\chi = d_{i_0}\chi_{i_0}$. Evaluating both sides at $1 \in G$, we see that $d_{i_0} > 0$ and this implies $d_{i_0} = 1$. This proves the first part of the theorem.

We rename $m = m_{i_0}$ and $\chi_{i_0} = \chi'$ as in the statement of the theorem and let (ρ, V) be a representation of G over $K(\chi)$ with character χ'. We also write $D' = D_{i_0}$ and $E' = E_{i_0} = K(\chi)$. Let Γ be the Galois group of $K(\chi)/K$ which is a Galois extension by Proposition 18 (the same proof works with $\mathbb{Q}$ and $\mathbb{C}$ replaced by K and C). Define $\phi = \mathrm{tr}_{K(\chi)/K}(\chi')$ and $\psi = \mathrm{tr}_{K(\chi)/K}(\chi)$. We have

$$m\psi = \sum_{\alpha \in \Gamma} m\chi^\alpha = \sum_{\alpha \in \Gamma} (m\chi)^\alpha = \phi.$$

The representation V is a $K(\chi)[G]$-module of finite dimension equal to, say n. Since $K(\chi)$ is a $|\Gamma|$-dimensional vector space over K, we can view V as a $K[G]$-module of dimension $n|\Gamma|$ over K by restriction of scalars. The character of the $K[G]$-module V obtained in this way is ϕ and therefore ϕ is realizable over K.

Let W be a realization of ϕ over K. We need to prove that the representation W is irreducible. Let therefore W_1 be a $K[G]$-submodule of W. By semisimplicity, there exists a $K[G]$-submodule W_2 of W such that $W = W_1 \oplus W_2$. By definition of realizability, the representation $K(\chi) \otimes_K W$ is a realization of ϕ over $K(\chi)$ and is therefore isomorphic as a $K(\chi)[G]$-module to the representation $\bigoplus_{\alpha \in \Gamma} V^\alpha$. By distributivity of the tensor product with respect to direct sums we have

$$(K(\chi) \otimes_K W_1) \oplus (K(\chi) \otimes_K W_2) \cong K(\chi) \otimes_K W \cong \bigoplus_{\alpha \in \Gamma} V^\alpha.$$

It follows that one of the two left summands contains an isomorphic copy of V, say the first. Since $K(\chi) \otimes_K W_1$ is stable under the action of Γ, it must contain at least one copy of each V^α. Now, if α is not 1, then we cannot have $(\chi')^\alpha = \chi'$ since otherwise α fixes $K(\chi')$ which is equal to $K(\chi)$ which implies $\alpha = 1$. Thus $\alpha \neq \beta$ in Γ implies that $(\chi')^\alpha \neq (\chi')^\beta$ so that V^α is not isomorphic to V^β. Thus $K(\chi) \otimes_K W_1 = \bigoplus_{\alpha \in \Gamma} V^\alpha$ and $K(\chi) \otimes_K W_2 = 0$ which implies that $W_2 = 0$. This proves that W is indeed irreducible. □

Chapter 5

L-Functions

Before Artin introduced his L-functions in his 1923 paper [Ar1], people had already studied other less general L-functions. The study of L-functions can be traced back to Leonard Euler who introduced and studied what is today known as the Riemann zeta-function. In particular, he proved that it admitted an expression as an Euler product in the region $\Re s > 1$. He also gave a modern proof of the infinity of the prime numbers. Bernard Riemann was the first to view this function as a complex variable function. He showed that his zeta-function admitted a functional equation and an analytic continuation to all of $\mathbb{C}$. He also discovered the deep link between the zeros of the Riemann zeta-function and the prime numbers and proved the explicit Weil formula for his function. In his study he was led to conjecture that the non-trivial zeros of the Riemann zeta-function all lie on the line $\Re s = 1/2$. This is now known as the Riemann Hypothesis.

Later, Dirichlet introduced what is known as Dirichlet L-functions by attaching what is called a Dirichlet character to the Riemann zeta-function. These L-function were also shown to possess a functional equation which gave them analytic continuation to $\mathbb{C}$. Finally, Dedekind introduced the Dedekind zeta-function of a number field, generalizing the Riemann zeta-function to number fields. It was Weber who generalized Dirichlet's methods and attached ray-class characters to the Dedekind zeta-function and created what is called Weber L-functions. Hecke was the one that proved that these L-functions admitted a functional equation and an analytic continuation. Later Hecke introduced his Grossencharakter, now known as a Hecke character, and attached to them a generalization of both Dirichlet and Weber L-functions in the form of a Dirichlet series that has an Euler product. The L-functions introduced by Artin generalize all of these previous L-functions.

5.1 L-Functions before Artin

We briefly introduce Dirichlet and Weber L-functions.

5.1.1 Dirichlet L-functions

Let $m \geq 1$ and let χ be 1-dimensional complex representation of the group $(\mathbb{Z}/m\mathbb{Z})^*$. We extend this to a function $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ by letting

$$\chi(n) = \begin{cases} \chi([n]) & \text{if } (n, m) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

This is called a Dirichlet character of modulus m.

Suppose that $m'|m$. Then we have an inclusion $m\mathbb{Z} \subset m'\mathbb{Z}$ and thus a surjective homomorphism $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m'\mathbb{Z}$. Moreover, $(a, m) = 1$ implies that $(a, m') = 1$ so that we have a surjective homomorphism $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m'\mathbb{Z})^*$.

The smallest $m^*|m$ such that χ factors through $(\mathbb{Z}/m^*\mathbb{Z})^*$ is called the conductor of χ and is denoted m^*. The extended character $\chi^* : (\mathbb{Z}/m^*\mathbb{Z})^* \longrightarrow \mathbb{C}$ is then called a primitive Dirichlet character.

One can check that if χ factors through $(\mathbb{Z}/m'\mathbb{Z})^*$ and $(\mathbb{Z}/m''\mathbb{Z})^*$ where both m' and m'' divide m, then χ factors through $(\mathbb{Z}/\gcd(m', m'')\mathbb{Z})^*$. Existence and uniqueness of the conductor m^* is proved by simply taking m^* to be the gcd of all divisors of m that χ factors through.

Once we have the definition of Dirichlet characters we can form Dirichlet L-functions. If χ is a Dirichlet character then we define this function, for $\Re s > 1$, to be

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

These are generalizations of the Riemann zeta-function which is obtained by taking the trivial character of modulus 1. One can show that Dirichlet L-functions admit a functional equation centered at $s = 1/2$ and extend analytically to holomorphic functions if χ is not trivial. If χ is the trivial character then the Dirichlet L-function is the Riemann zeta-function and has a simple pole at $s = 1$ with residue 1. Moreover, one can prove that the L-function of a non-trivial Dirichlet character has no zeros on the line $\mathcal{R}(s) = 1$ and actually no zeros in a region away from the line $s = 1$ except possibly one which is known as Siegel's exceptional zero. These functions are central when studying primes in arithmetic progression and primes in general. One for example studies these functions when proving the Maynard-Zhang Theorem on bounded gaps between primes.

If χ is a Dirichlet character of modulus m and χ^* is the corresponding primitive character of modulus m^*, then we have

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

Thus the L-function of χ only differs by finitely many factors from the L-function of χ^* and it therefore suffices to study only primitive Dirichlet L-functions.

5.1.2 Weber L-functions

Let k be a number field and $\mathfrak{m}$ a modulus of k. Let χ be a 1-dimensional complex representation of the $\mathfrak{m}$-ray class group $\mathrm{Cl}_k(\mathfrak{m})$ of k. Extend this to a function $\chi : I_K \longrightarrow \mathbb{C}$ by letting

$$\chi(\mathfrak{a}) = \begin{cases} \chi([\mathfrak{a}]) & \text{if } \mathfrak{a} \in I_k(\mathfrak{m}) \\ 0 & \text{otherwise.} \end{cases}$$

This is called a ray-class character of modulus $\mathfrak{m}$.

Suppose that $\mathfrak{m}'|\mathfrak{m}$ and let $\alpha \equiv 1 \mod {}^*\mathfrak{m}$. Then we have $\alpha \equiv 1 \mod {}^*\mathfrak{m}'$. As a consequence, we have the inclusion $P_\mathfrak{m} \subset P_{\mathfrak{m}'}$ and we have a homomorphism of groups $\mathrm{Cl}_k(\mathfrak{m}) \longrightarrow \mathrm{Cl}_k(\mathfrak{m}')$.

Definition 15. Let χ be a ray-class character of modulus $\mathfrak{m}$. The conductor $\mathfrak{f}(\chi)$ of χ is the smallest modulus $\mathfrak{m}'$ of k with the property that there exists a ray-class character χ' of modulus $\mathfrak{m}'|\mathfrak{m}$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Cl}_k(\mathfrak{m}) \arrow[r, "\chi"] \arrow[d] & \mathbb{C}^* \\
\mathrm{Cl}_k(\mathfrak{m}'). \arrow[ur, "\chi'"'] &
\end{tikzcd}$$

The corresponding Hecke character $\chi^* : \mathrm{Cl}_k(\mathfrak{f}(\chi)) \longrightarrow \mathbb{C}^*$ is said to be primitive.

The existence and uniqueness of the conductor of a ray-class character comes from constructing it again as the gcd of all moduli that divide $\mathfrak{m}$ and have the above property.

Definition 16. Let χ be a ray-class character over k of modulus $\mathfrak{m}$. The Weber L-function associated to χ is defined, for $\Re s > 1$, to be

$$L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1}$$

where the sum is over all non-zero integral ideals of k and the product is over all non-zero prime ideals of k.

Remark 15. By Example 1 a Dirichlet character of modulus m is a ray-class character for $\mathbb{Q}$ of modulus $m\mathbb{Z}v_\infty$ and their L-functions coincide.

Proposition 43. *Let χ be a ray-class character for k of modulus $\mathfrak{m}$. The Weber L-function $L(s,\chi)$ converges absolutely for $\Re s > 1$ and therefore defines a holomorphic function in this region which has no zeros.*

Proof. Since $\chi : \mathrm{Cl}(\mathfrak{m}) \longrightarrow \mathbb{C}^*$ is a homomorphism of groups, χ takes values on the unit circle. We therefore have, for $\Re s > 1$,

$$|L(s,\chi)| = \left| \sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} \right| \leq \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^{\Re s}} = \zeta_k(\Re s)$$

and we already know that the Dedekind zeta function converges absolutely for $\Re s > 1$. □

In view of Remark 15, these Weber L-functions are generalizations of Dirichlet L-functions. As in the previous section, if χ is a ray-class character and χ^* denotes the corresponding primitive character, then

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

Thus the Weber L-function of χ only differs by finitely many factors from the one of χ^*. It follows that in order to understand Weber L-functions it suffices to consider the case of primitive characters. Note that the Weber L-function associated to the primitive trivial character is exactly the Dedekind zeta-function ζ_k. Hecke proved that these L-functions can be analytically continued to the whole complex plane via a functional equation. In order to state this theorem we first need to complete $L(s,\chi)$ with local factors corresponding to the infinite places of K.

Definition 17. Let χ be a ray-class character of k with conductor $\mathfrak{f}$. If v denotes an infinite place of K, then we define the local factor at v as follows:

$$L_v(s,\chi) = \begin{cases} \Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) & \text{if } v \nmid \mathfrak{f} \text{ and is real} \\ \Gamma_{\mathbb{R}}(s+1) = \pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right) & \text{if } v|\mathfrak{f} \text{ and is real} \\ \Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = 2(2\pi)^{-s}\Gamma(s) & \text{if } v \text{ is complex.} \end{cases}$$

We also define $L_\infty(s,\chi) = \prod_{v\in M_K^\infty} L_v(s,\chi)$.

Theorem 5.1.1. *Let χ be a primitive ray-class character of k of conductor $\mathfrak{f}(\chi)$. The completed Weber L-function*

$$\Lambda(s,\chi) = (|d_k|N(\mathfrak{f}(\chi)_0))^{\frac{s}{2}} L_\infty(s,\chi)L(s,\chi)$$

extends holomorphically to $\mathbb{C}$ (unless χ is trivial in which case it has simple poles at $s = 0,1$) and has a functional equation

$$\Lambda(s,\chi) = \epsilon(\chi)\Lambda(1-s,\bar{\chi})$$

where $|\epsilon(\chi)| = 1$.

Proof. The proof, which is due to Hecke, is inspired by the proof of the functional equation for Dirichlet L-functions but uses more general and complicated Hecke Θ-functions. See Chapter XIII, § 3 of [Lan]. □

Corollary 27. *The Weber L-function of a non-trivial ray-class character is holomorphic on $\mathbb{C}$.*

Proof. Let χ be a non-trivial ray-class character of modulus $\mathfrak{m}$ and let χ^* be the corresponding primitive character. As already noted, we have

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

and as a consequence holomorphicity of $L(s,\chi)$ only depends on holomorphicity of $L(s,\chi^*)$ since the finite product is holomorphic.

We may therefore suppose that χ is a primitive non-trivial Weber character with conductor $\mathfrak{f}(\chi)$. By the functional equation we have

$$L(s,\chi) = \epsilon(\chi)\frac{\Lambda(1-s,\bar{\chi})}{(|d_k|N(\mathfrak{f}(\chi)_0))^{\frac{s}{2}}L_\infty(s,\chi)}.$$

Looking at the definition of the Γ-factors in Definition 17 and using the fact that Γ has a simple poles at $s=-n$ for non-negative integers n and no zeros it becomes clear that $L(s,\chi)$ is holomorphic on $\mathbb{C}$. □

Corollary 28. *Let k be a number field. The completed Dedekind zeta-function*

$$\Lambda_k(s) = |d_k|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_k(s).$$

extends meromorphically to $\mathbb{C}$ with two simple poles at $s=0,1$ with polar part given by

$$\frac{2^{r_1}h_kR_k}{\omega_k}\left(\frac{1}{s-1}-\frac{1}{s}\right)$$

and satisfies the functional equation $\Lambda_k(s)=\Lambda_k(1-s)$.

Proof. This is a consequence of our observation that $\zeta_k(s)$ is the Weber L-function for the trivial primitive ray-class character. Therefore $N(\mathfrak{f}(\chi)_0)=1$ and $L_\infty = \Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}$. The polar part result is a consequence of Theorem 1.5.1. □

5.2 Artin L-functions

Weber L-functions were a great tool in proving global class field theory. But we only have a class field theory for abelian extensions of number fields. Meanwhile, Weber L-functions are functions associated to characters of abelian groups. Artin was interested in L-functions more general than the ones of Weber and Hecke that may be associated with not necessarily abelian Galois extensions of number fields. He introduced his L-functions in his 1923 paper [Ar1] and completed his work on them in his 1930 and 1931 papers [Ar2] and [Ar3].

5.2.1 Definition

Let K/k be a finite Galois extension of number fields and let $G=\mathrm{Gal}(K/k)$. Let $v=\mathfrak{p}$ be a finite place of M_k. Pick a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ that divides $\mathfrak{p}$ and let $e_{\mathfrak{P}}$ and $f_{\mathfrak{P}}$ be the ramification and residual degrees of $\mathfrak{P}$ over $\mathfrak{p}$. Denote by $(\mathfrak{P},K/k)$ the Frobenius element of $\mathfrak{P}$. This is an element of the quotient group $D_{\mathfrak{P}}/I_{\mathfrak{P}}$.

Let (ρ,V) be a finite-dimensional complex representation of G and consider the representation $(\rho_{\mathfrak{P}},V^{I_{\mathfrak{P}}})$ of the quotient group $D_{\mathfrak{P}}/I_{\mathfrak{P}}$. For any $s\in\mathbb{C}$ with $\Re s>1$, consider the element $1-\rho_{\mathfrak{P}}((\mathfrak{P},K/k))N(\mathfrak{p})^{-s}$ of $\mathrm{End}_{\mathbb{C}}(V^{I_{\mathfrak{P}}})$. Since the order of $\rho_{\mathfrak{P}}((\mathfrak{P},K/k))$ is $f=f_{\mathfrak{P}}$, the above element has an inverse given by

$$(1-N(\mathfrak{p})^{-sf})^{-1}\sum_{j=1}^{f-1}\rho_{\mathfrak{P}}((\mathfrak{P},K/k))^jN(\mathfrak{p})^{-sj}.$$

In particular, $1-\rho_{\mathfrak{P}}((\mathfrak{P},K/k))N(\mathfrak{p})^{-s}$ belongs to $\mathrm{GL}(V^{I_{\mathfrak{P}}})$ and its determinant is non-zero.

Definition 18. Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let (ρ, V) be a finite-dimensional complex representation of G. The Artin L-function of V is defined, for $s \in \mathbb{C}$ with $\Re s > 1$, by the product

$$L(s, V, K/k) = \prod_{\mathfrak{p} \in M_k^0} \det(1 - \rho_{\mathfrak{P}}((\mathfrak{P}, K/k))N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}})^{-1}$$

where $\mathfrak{P}$ denotes any prime ideal of K that divides $\mathfrak{p}$.

Remark 16. We claim that this definition does not depend on the choice of the prime $\mathfrak{P}|\mathfrak{p}$. For, any other prime that divides $\mathfrak{p}$ is of the form $\sigma(\mathfrak{P})$ for some element σ of G. Let $\sigma_{\mathfrak{P}}$ denote a representative of $(\mathfrak{P}, K/k)$ in $D_{\mathfrak{P}}$. By Proposition 12, $\sigma\sigma_{\mathfrak{P}}\sigma^{-1}$ is a representative of $\sigma(\mathfrak{P}, K/k)$ in $D_{\sigma(\mathfrak{P})}$. Then by definition of the quotient representation we have

$$\rho_{\sigma(\mathfrak{P})}((\sigma(\mathfrak{P}), K/k)) = \rho(\sigma\sigma_{\mathfrak{P}}\sigma^{-1}) = \rho(\sigma)\rho_{\mathfrak{P}}((\mathfrak{P}, K/k))\rho(\sigma)^{-1}.$$

It follows that

$$1 - \rho_{\sigma(\mathfrak{P})}((\sigma(\mathfrak{P}), K/k))N(\mathfrak{p})^{-s} = \rho(\sigma)(1 - \rho_{\mathfrak{P}}((\mathfrak{P}, K/k))N(\mathfrak{p})^{-s})\rho(\sigma)^{-1}.$$

As a consequence, we have

$$\det(1 - \rho_{\sigma(\mathfrak{P})}((\sigma(\mathfrak{P}), K/k))N(\mathfrak{p})^{-s}) = \det(1 - \rho_{\mathfrak{P}}((\mathfrak{P}, K/k))N(\mathfrak{p})^{-s}).$$

Remark 17. Let (ρ', V') be an isomorphic representation. Then there exists an isomorphism of complex vector spaces $f : V \longrightarrow V'$ such that $f \circ \rho(\sigma) = \rho'(\sigma) \circ f$ for all $\sigma \in G$. It follows that $\rho(\sigma) = f^{-1} \circ \rho'(\sigma) \circ f$ and $\det(1 - \rho(\sigma)) = \det(1 - \rho'(\sigma))$. We conclude that

$$L(s, V, K/k) = L(s, V', K/k).$$

Thus, the Artin L-function is actually defined for isomorphism classes of representation. This last observation hints toward the fact that we should be able to get an expression of the L-function that only depends on the character of the representation.

Remark 18. When the context is clear and no confusion is possible, we shall write $L(s, V)$ instead of $L(s, V, K/k)$ for the Artin L-function of V.

Proposition 44. *Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let (ρ, V) be a representation of G over $\mathbb{C}$. The Artin L-function $L(s, V)$ converges absolutely in the region $\Re s > 1$.*

Proof. For each prime $\mathfrak{p}$ of k and any choice of a prime $\mathfrak{P}$ in K that divides $\mathfrak{p}$, we denote by $\dim(\mathfrak{P})$ the degree of the representation $V^{I_{\mathfrak{P}}}$. Also, we denote by $\lambda_i^{\mathfrak{P}}$ the eigenvalues of the matrix $\rho_{\mathfrak{P}}((\mathfrak{P}, K/k))$ for $i = 1, \ldots, \dim(\mathfrak{P})$. For the following computation we drop the $V^{I_{\mathfrak{P}}}$ in the determinant notation. With these notations, we have

$$\begin{aligned}|L(s,V)| &= \prod_{\mathfrak{p}} |\det(1-\rho_{\mathfrak{P}}((\mathfrak{P},K/k))N(\mathfrak{p})^{-s})|^{-1}\\ &= \prod_{\mathfrak{p}} \prod_{i=1}^{\dim(\mathfrak{P})} |1-\lambda_i^{\mathfrak{P}}N(\mathfrak{p})^{-s}|^{-1}\\ &\leq \prod_{\mathfrak{p}} \prod_{i=1}^{\dim(\mathfrak{P})} (1-|\lambda_i^{\mathfrak{P}}|N(\mathfrak{p})^{-\Re s})^{-1}\\ &= \prod_{\mathfrak{p}} \prod_{i=1}^{\dim(\mathfrak{P})} (1-N(\mathfrak{p})^{-\Re s})^{-1}\\ &\leq \prod_{\mathfrak{p}} (1-N(\mathfrak{p})^{-\Re s})^{\dim_{\mathbb{C}} V}\\ &= \zeta_k(\Re s)^{\dim_{\mathbb{C}} V},\end{aligned}$$

where ζ_k denotes the Dedekind zeta-function of k. Note that we made use of the fact that the absolute value of the eigenvalues of $\rho_{\mathfrak{P}}((\mathfrak{P},K/k))$ is 1. This is due to the fact that $\rho_{\mathfrak{P}}$ is a homomorphism of groups and therefore of finite order since $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ is finite. Since ζ_k converges for $\Re s > 1$ we get the desired result. □

Proposition 45. *Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let (ρ, V) be a representation of G over $\mathbb{C}$ with character χ. For $\mathfrak{P}|\mathfrak{p}$ we denote by $\chi_{\mathfrak{P}}$ the character of the representation $V^{I_{\mathfrak{P}}}$. Then, for $\Re s > 1$, we have*

$$\log L(s,V) = \sum_{\mathfrak{p}} \sum_{j=1}^{\infty} \frac{\chi_{\mathfrak{P}}((\mathfrak{P},K/k)^j)}{jN(\mathfrak{p})^{js}}$$

where $\sigma_{\mathfrak{P}}$ denotes any representative of the Frobenius element $(\mathfrak{P},L/K)$ in $D_{\mathfrak{P}}$.

Proof. We use the same notations as in the previous proof. Taking the logarithm of the L-function, we obtain

$$\begin{aligned}\log L(s,V) &= \sum_{\mathfrak{p}} -\log\det(1-(\mathfrak{P},L/K)N(\mathfrak{p})^{-s}))\\ &= \sum_{\mathfrak{p}} -\log \prod_{i=1}^{\dim\mathfrak{P}} (1-\lambda_i^{\mathfrak{P}}N(\mathfrak{p})^{-s}) = \sum_{\mathfrak{p}} \sum_{i=1}^{\dim\mathfrak{P}} -\log(1-\lambda_i^{\mathfrak{P}}N(\mathfrak{p})^{-s}).\end{aligned}$$

Using the Taylor expansion of $-\log(1-x)$, we see that

$$\log L(s,V) = \sum_{\mathfrak{p}} \sum_{i=1}^{\dim\mathfrak{P}} \sum_{k=1}^{\infty} \frac{(\lambda_i^{\mathfrak{P}})^j}{jN(\mathfrak{p})^{js}} = \sum_{\mathfrak{p}} \sum_{j=1}^{\infty} \frac{\sum_{i=1}^{\dim\mathfrak{P}}(\lambda_i^{\mathfrak{P}})^j}{jN(\mathfrak{p})^{js}}.$$

But the $(\lambda_i^{\mathfrak{P}})^j$ are the eigenvalues of the j^{th} power of $\rho_{\mathfrak{P}}((\mathfrak{P},L/K))$ and thus their sum is $\chi_{\mathfrak{P}}((\mathfrak{P},L/K)^j)$ and this concludes the proof of the first equality. The second equality is a direct consequence of Proposition 9. □

Remark 19. Proposition 45 shows that the Artin L-function of a Galois representation only depends on the character of this representation. We will therefore speak about the Artin L-function of a character and we will interchangeably use the notations $L(s, V)$ and $L(s, \chi)$.

By Proposition 9 we have

$$\log L(s,\chi) = \sum_{\mathfrak{p}} \sum_{j=1}^{\infty} \frac{\frac{1}{e_{\mathfrak{P}}} \sum_{\tau \in I_{\mathfrak{P}}} \chi(\sigma_{\mathfrak{P}}^{j} \tau)}{jN(\mathfrak{p})^{js}}.$$

We use this expression to extend the definition of Artin L-functions to class functions of G.

Definition 19. Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/)k$. For any class function $\phi \in R(G, \mathbb{C})$, we define the Artin L-function of ϕ for $\Re s > 1$ to be

$$\log L(s,\phi) = \sum_{\mathfrak{p}} \sum_{j=1}^{\infty} \frac{\frac{1}{e_{\mathfrak{P}}} \sum_{\tau \in I_{\mathfrak{P}}} \phi(\sigma_{\mathfrak{P}}^{j} \tau)}{jN(\mathfrak{p})^{js}}$$

where $\sigma_{\mathfrak{P}}$ denotes any coset representative of the Frobenius automorphism $(\mathfrak{P}, K/k)$ in $D_{\mathfrak{P}}$.

5.2.2 First Properties

We study the behavior of Artin L-functions with respect to the operations of addition, induction and inflation on representations and their characters.

Proposition 46. *Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let 1_G denote the trivial character of G. Then, for $\Re s > 1$, we have*

$$L(s, 1_G) = \zeta_k(s).$$

Proof. By Proposition 45 we have

$$\log L(s, 1_G) = \sum_{\mathfrak{p}} \sum_{j=1}^{\infty} \frac{1}{jN(\mathfrak{p})^{js}}.$$

Using the Taylor series of $\log(1-x)$ we get

$$\log L(s, 1_G) = \sum_{\mathfrak{p}} -\log(1 - N(\mathfrak{p})^{-s}) = \log \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} = \log \zeta_k(s).$$

□

Proposition 47 (Additivity)**.** *Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let χ_1 and χ_2 be two characters of G. Then, for $\Re s > 1$,*

$$L(s, \chi_1 + \chi_2) = L(s, \chi_1) L(s, \chi_2).$$

Proof. By Proposition 45 and using absolute convergence of the Artin L-function in the region $\Re s > 1$ we see that

$$\log L(s, \chi_1 + \chi_2) = \log L(s, \chi_1) + \log L(s, \chi_2).$$

□

Proposition 48 (Inflation). *Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let H be a normal subgroup of G and let χ be a character of the quotient group G/H. Then, for $\Re s > 1$, we have*

$$L(s, \mathrm{Infl}_H^G \chi, K/k) = L(s, \chi, K^H/k).$$

Proof. Let $K' = K^H$ and let $\Gamma = \mathrm{Gal}(K'/k)$. By Proposition 11, the restriction map $\mathrm{Res} : G \longrightarrow \Gamma$ induces and isomorphism $I_{\mathfrak{P}}/(I_{\mathfrak{P}} \cap H) \cong I_{\mathfrak{P}'}$.

If $\sigma_{\mathfrak{P}'}$ and $\sigma_{\mathfrak{P}}$ denote representatives of the respective Frobenius elements, then for any positive integer j we have

$$\frac{1}{e_{\mathfrak{P}'}} \sum_{\tau' \in I_{\mathfrak{P}'}} \chi(\sigma_{\mathfrak{P}'}^j \tau') = \frac{1}{e_{\mathfrak{P}'} |I_{\mathfrak{P}} \cap H|} \sum_{\tau \in I_{\mathfrak{P}}} \chi(\sigma_{\mathfrak{P}'}^j \mathrm{Res}(\tau)).$$

Note that $|I_{\mathfrak{P}} \cap H| = e_{\mathfrak{P}}/e_{\mathfrak{P}'}$. By Proposition 13, we may suppose that $\mathrm{Res}(\sigma_{\mathfrak{P}}) = \sigma_{\mathfrak{P}'}$. Thus

$$\frac{1}{e_{\mathfrak{P}'}} \sum_{\tau' \in I'_{\mathfrak{P}}} \chi(\sigma_{\mathfrak{P}'}^j \tau') = \frac{1}{e_{\mathfrak{P}}} \sum_{\tau \in I_{\mathfrak{P}}} \chi(\mathrm{Res}(\sigma_{\mathfrak{P}}^j \tau)) = \frac{1}{e_{\mathfrak{P}}} \sum_{\tau \in I_{\mathfrak{P}}} \mathrm{Infl}_H^G \chi(\sigma_{\mathfrak{P}}^j \tau).$$

By Proposition 45, we obtain equality between the L-functions. □

Proposition 49 (Induction). *Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let H be a subgroup of G and let χ be a character of H. Then, for $\Re s > 1$, we have*

$$L(s, \mathrm{Ind}_H^G \chi, K/k) = L(s, \chi, K/K^H).$$

Proof. By Proposition 45 it suffices to prove the following: for all $\mathfrak{p}$ prime in k with $\mathfrak{P}$ a prime in K that divides $\mathfrak{p}$ we have

$$\sum_{j \geq 1} \frac{\mathrm{Ind}_H^G \chi_\beta((\mathfrak{P}, K/k)^j)}{j N(\mathfrak{p})^{js}} = \sum_{\mathfrak{q}|\mathfrak{p}} \sum_{n \geq 1} \frac{\chi_\wp((\wp, K/K^H)^n)}{n N(\mathfrak{q})^{ns}}$$

where the right-hand side sum is over prime ideals $\mathfrak{q}$ of K^H that divide $\mathfrak{p}$ and $\wp$ is any prime ideal of K that divides $\mathfrak{q}$.

We set $F = K^H$. We fix a prime $\mathfrak{p}$ in k. In F, we have a decomposition of $\mathfrak{p}$, say $\mathfrak{p}\mathcal{O}_F = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_r^{e_r}$. For each i, we let f_i denote the residual degree of $\mathfrak{q}_i$ over $\mathfrak{p}$. For each $\mathfrak{q}_i$ we let $\mathfrak{P}_i$ denote a prime of K that lies above $\mathfrak{q}_i$ and we denote by e'_i and f'_i the associated ramification and residual degrees of $\mathfrak{P}_i$ over $\mathfrak{q}_i$. We let e and f be the ramification and residual degrees of $\mathfrak{P}_i$ over $\mathfrak{p}$. The prime ideal $\mathfrak{P}_i$ all lie above $\mathfrak{p}$ and G acts transitively on the prime ideals of $\mathcal{O}_K$ that lie above $\mathfrak{p}$. We let $\eta_i \in G$ be such that $\eta_i(\mathfrak{P}_1) = \mathfrak{P}_i$. Let D_i and I_i be respectively the decomposition and inertia groups of $\mathfrak{P}_i$ over $\mathfrak{p}$. Then by Proposition 10 we have $D_i = \eta_i D_1 \eta_i^{-1}$ and $I_i = \eta_i I_1 \eta_i^{-1}$. Let $\sigma_1 \in D_1$ be an element such that $(\mathfrak{P}_1, K/k) = \sigma_1 I_1$ and choose $\sigma_i \in D_i$ such that $\sigma_i = \eta_i \sigma_1 \eta_i^{-1}$ by Proposition 12. Note that $D_i \cap H$ and $I_i \cap H$ are respectively the decomposition and inertia groups of $\mathfrak{P}_i$ over $\mathfrak{q}_i$. The order of the group D_i is ef and the order of $D_i \cap H$ is $e'_i f'_i$ and thus the index of $D_i \cap H$ in D_i is $e_i f_i$. Let $\{\gamma_{i,\nu}\}$ for $\nu = 1, \ldots, e_i f_i$ be a system of right coset representatives of the quotient $D_i/(D_i \cap H)$. By Lemma

3, the family $\{\gamma_{i,\nu}\eta_i\}$ for $i = 1, \ldots, r$ and $\nu = 1, \ldots, e_i f_i$ is a system of distinct right coset representatives of the quotient $H \setminus G$.

Using Theorem 3.4.1, we see that if τ is an element of G, we have

$$\mathrm{Ind}_H^G \chi(\tau) = \sum_{i=1}^{r}{}' \sum_{\nu=1}^{e_i f_i}{}' \chi(\gamma_{i,\nu}\eta_i\tau\eta_i^{-1}\gamma_{i,\nu}^{-1})$$

where the symbol $'$ in the sums means that the sums are over all i and ν such that $\gamma_{i,\nu}\eta_i\tau\eta_i^{-1}\gamma_{i,\nu}^{-1}$ belongs to H. It follows from Proposition 9 that

$$\begin{aligned}
\mathrm{Ind}_H^G \chi_{\mathfrak{P}}((\mathfrak{P}, K/k)^j) = \mathrm{Ind}_H^G \chi_{\mathfrak{P}_1}(\sigma_1^j I_1) &= \frac{1}{e} \sum_{\tau \in I_1} \mathrm{Ind}_H^G \chi(\sigma_1^j \tau) \\
&= \frac{1}{e} \sum_{\tau \in I_1} \sum_{i=1}^{r}{}' \sum_{\nu=1}^{e_i f_i}{}' \chi(\gamma_{i,\nu}\eta_i\sigma_1^j\tau\eta_i^{-1}\gamma_{i,\nu}^{-1}) \\
&= \frac{1}{e} \sum_{\tau \in I_1} \sum_{i=1}^{r}{}' \sum_{\nu=1}^{e_i f_i}{}' \chi(\gamma_{i,\nu}\eta_i\sigma_1^j\eta_i^{-1}\eta_i\tau\eta_i^{-1}\gamma_{i,\nu}^{-1}) \\
&= \frac{1}{e} \sum_{i=1}^{r}{}' \sum_{\nu=1}^{e_i f_i}{}' \sum_{\tau_i \in I_i} \chi(\gamma_{i,\nu}\sigma_i^j\tau_i\gamma_{i,\nu}^{-1}).
\end{aligned}$$

Since I_i is a normal subgroup of G_i and G_i/I_i is abelian, conjugation of $\sigma_i^j I_i$ by elements of G_i does not affect $\sigma_i^j I_i$. It follows that

$$\mathrm{Ind}_H^G \chi_{\mathfrak{P}}((\mathfrak{P}, K/k)^j) = \sum_{i=1}^{r}{}' \frac{e_i f_i}{e} \sum_{\tau \in I_i} \chi(\sigma_i^j \tau)$$

where the sum is over the i's and the τ for which $\sigma_i^j\tau$ belongs to H. By Lemma 4, the intersection $\sigma_i^j I_i \cap H$ is non-empty if and only if f_i divides j. Moreover, if ϕ_i is a representative of $(\mathfrak{P}_i, K/F)$ in the decomposition group $D_i \cap H$ of $\mathfrak{P}_i$ over $\mathfrak{q}_i$, then if f_i divides j we have

$$\sigma_i^j I_i \cap H = \phi_i^{j/f_i}(I_i \cap H).$$

It follows that

$$\begin{aligned}
\mathrm{Ind}_H^G \chi_{\mathfrak{P}}((\mathfrak{P}, K/k)^j) &= \sum_{i=1}^{r} \frac{e_i f_i}{e} \sum_{\substack{\tau \in I_i \\ \sigma_i^j \tau \in H}} \chi(\sigma_i^j \tau) \\
&= \sum_{i=1}^{r} \frac{e_i f_i}{e} \sum_{\tau \in I_i \cap H} \chi(\phi_i^{j/f_i} \tau) \\
&= \sum_{i=1}^{r} \frac{e_i' e_i f_i}{e} \chi_{\mathfrak{P}_i}((\mathfrak{P}_i, K/F)^{j/f_i})
\end{aligned}$$

since $e_i' = |I_i \cap H|$. Since $e = e_i e_i'$, we get

$$\mathrm{Ind}_H^G \chi_{\mathfrak{P}}((\mathfrak{P}, K/k)^j) = \sum_{i=1}^{r} f_i \chi_{\mathfrak{P}_i}((\mathfrak{P}_i, K/F)^{j/f_i}).$$

We can now compute

$$\begin{aligned}\sum_{j\geq 1}\frac{\mathrm{Ind}_H^G\chi_\beta((\mathfrak{P},K/k)^j)}{jN(\mathfrak{p})^{js}} &= \sum_{i=1}^{r}\sum_{j:f_i|j} f_i\frac{\chi_{\mathfrak{P}_i}((\mathfrak{P}_i,K/F)^{j/f_i})}{jN(\mathfrak{p})^{js}}\\ &= \sum_{i=1}^{r}\sum_{n\geq 1} f_i\frac{\chi_{\mathfrak{P}_i}((\mathfrak{P}_i,K/F)^{n})}{nf_iN(\mathfrak{p})^{nf_is}}\\ &= \sum_{i=1}^{r}\sum_{n\geq 1} \frac{\chi_{\mathfrak{P}_i}((\mathfrak{P}_i,K/F)^{n})}{nN(\mathfrak{q})^{ns}}\end{aligned}$$

as promised. □

Proposition 50. *Let K/k be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/k)$. Let $\widehat{G}$ denote the set of irreducible characters of G over $\mathbb{C}$. For $\Re s > 1$, we have the formula*

$$\zeta_K(s) = \prod_{\chi\in\widehat{G}} L(s,\chi)^{\chi(1)}.$$

In particular, if 1_G denotes the trivial character of G, then we have the formula

$$\frac{\zeta_K(s)}{\zeta_k(s)} = \prod_{\chi\neq 1_G} L(s,\chi)^{\chi(1)}.$$

Proof. Consider the trivial subgroup $\{1\}$ of G. It has only one irreducible character, namely the trivial character $1_{\{1\}}$. By Theorem 3.4.1, the induced character on G is given by

$$\mathrm{Ind}_{\{1\}}^G 1_{\{1\}}(\sigma) = \sum_{\substack{\tau\in G\\ \tau^{-1}\sigma\tau=1}} 1 = \begin{cases}|G| & \text{if } \sigma = 1\\ 0 & \text{otherwise.}\end{cases}$$

By Proposition 26, this is equal to the regular character r_G of G. By Corollary 16 we have $r_G = \sum_{\chi\in\widehat{G}}\chi(1)\chi$. By Proposition 47 applied repeatedly we have, for $\Re s > 1$, the formula

$$L(s,r_G) = \prod_{\chi\in\widehat{G}} L(s,\chi)^{\chi(1)}.$$

By Proposition 49 and Proposition 46, we have

$$L(s,\mathrm{Ind}_{\{1\}}^G 1_{\{1\}},K/k) = L(s,1_{\{1\}},K/K) = \zeta_K(s).$$

We thus obtain

$$\zeta_K(s) = \prod_{\chi\in\widehat{G}} L(s,\chi)^{\chi(1)}$$

which proves the first formula. By Proposition 46, we have $L(s,1_G,L/K) = \zeta_k(s)$ so that

$$\zeta_K(s) = \zeta_k(s)\prod_{\chi\neq 1_G} L(s,\chi)^{\chi(1)}.$$

By Remark 5 the function $\zeta_k(s)$ can be expressed as an Euler product for $\Re s > 1$ and therefore has no zeros in this region of the complex plane. We can therefore divide the previous expression by $\zeta_k(s)$ on both sides to obtain the desired formula. □

5.3 Artin L-Functions of 1-dimensional Characters

Let K/k be a finite Galois extension of number fields with Galois group G. Let χ be a 1-dimensional character of G. Then χ factors through it kernel. Explicitly, there exists a homomorphism $\chi' : G/\ker\chi \longrightarrow \mathbb{C}^*$ such that the following diagram

$$\begin{tikzcd}
G \arrow[r, "\chi"] \arrow[d] & \mathbb{C}^* \\
G/\ker\chi \arrow[ur, "\chi'"'] &
\end{tikzcd}$$

commutes. In other words, we have $\chi = \mathrm{Infl}^{G}_{\ker\chi}\chi'$. Since $\ker\chi$ is a normal subgroup of G, the extension $K^{\ker\chi}/k$ is a Galois extension. Moreover, it is abelian. The latter is because the kernel of χ contains the commutator $[G:G]$, whence $K^{\ker(\chi)}$ is a subfield of $K^{[G:G]}$. Since $K^{\ker(\chi)}$ is Galois over k, its Galois group is a quotient of the abelian group $G/[G:G]$ and is therefore abelian. By Proposition 48, we have

$$L(s,\chi,K/k) = L(s,\chi',K^{\ker\chi}/k).$$

Thus the L-function of a 1-dimensional character is the L-function of a 1-dimensional injective character of an abelian extension of k.

Assume now that K/k is an abelian extension with Galois group G. Let χ be a 1-dimensional injective character of G. The conductor $\mathfrak{f} = \mathfrak{f}(K/k)$ of K/k is the smallest modulus of k for which K is a subfield of the corresponding ray class field by Proposition 14. Let Res denote the restriction map

$$\mathrm{Gal}(k(\mathfrak{f})/k) \longrightarrow G.$$

It induces an isomorphism of groups

$$\mathrm{Gal}(k(\mathfrak{f})/k)/\mathrm{Gal}(k(\mathfrak{f})/K) \longrightarrow G.$$

Define the character

$$\chi_{\mathfrak{f}} := \mathrm{Infl}^{\mathrm{Gal}(k(\mathfrak{f})/k)}_{\mathrm{Gal}(k(\mathfrak{f})/K)}(\chi \circ \mathrm{Res}) : \mathrm{Gal}(k(\mathfrak{f})/k) \longrightarrow \mathbb{C}^*.$$

Composing with the Artin map we get a character $\chi'_{\mathfrak{f}} = \chi_{\mathfrak{f}} \circ \Phi_{k(\mathfrak{f})/k,\mathfrak{f}}$ of $\mathrm{Cl}_k(\mathfrak{f})$. We extend $\chi'_{\mathfrak{f}}$ to a ray-class character $\chi'_{\mathfrak{f}} : I_k \longrightarrow \mathbb{C}$ of modulus $\mathfrak{f}$ by setting

$$\chi'_{\mathfrak{f}}(\mathfrak{a}) = \begin{cases} \chi'_{\mathfrak{f}}([\mathfrak{a}]) & \text{if } \mathfrak{a} \in I_k(\mathfrak{f}) \\ 0 & \text{otherwise.} \end{cases}$$

We consider the Weber L-function associated to this ray-class character

$$L_W(s,\chi'_{\mathfrak{f}}) = \prod_{\mathfrak{p}\nmid\mathfrak{f}} \left(1 - \chi'_{\mathfrak{f}}(\mathfrak{p})N(\mathfrak{p})^{-s}\right)^{-1}.$$

We have

$$L(s,\chi,K/k) = \prod_{\mathfrak{p}} (1 - \chi_{\mathfrak{p}}((\mathfrak{p},K/k))N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{p}}})^{-1}.$$

We have $V^{I_\mathfrak{p}} \neq \{0\}$ if and only if $\chi(I_\mathfrak{p}) = 1$. By injectivity of χ this implies that $I_\mathfrak{p}$ is trivial which is equivalent to $\mathfrak{p}$ being unramified. By Theorem 2.4.2, $\mathfrak{p}$ is ramified if and only if $\mathfrak{p}$ divides $\mathfrak{f}$. We conclude that

$$L(s, \chi, K/k) = \prod_{\mathfrak{p} \nmid \mathfrak{f}} (1 - \chi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}.$$

If $\mathfrak{p}$ is unramified, then

$$\chi'_\mathfrak{f}(\mathfrak{p}) = \chi_\mathfrak{p}((\mathfrak{p}, k(\mathfrak{f})/k)) = \chi(\mathrm{Res}((\mathfrak{p}, k(\mathfrak{f}/k)))) = \chi(\sigma_\mathfrak{p})$$

where we used Proposition 13 in the last equality. We conclude that

$$L(s, \chi, K/k)) = L_W(s, \chi'_\mathfrak{f}). \tag{5.3.0.1}$$

To recapitulate, using class field theory and the properties of Artin L-functions we have shown that the Artin L-function of a 1-dimensional character of a finite Galois extension is equal to a Weber L-function. By Theorem 5.1.1 all Weber L-functions admit a functional equation centered at $\frac{1}{2}$. By Corollary 27, these L-functions are holomorphic on $\mathbb{C}$ if the ray-class character is not trivial and meromorphic with a pole at $s = 1$ if the character is trivial. In conclusion, we have proved the following:

Theorem 5.3.1. *The Artin L-function of a 1-dimensional characters of finite Galois extensions admits a meromorphic continuation to $\mathbb{C}$ and a functional equation centered at $s = \frac{1}{2}$.*

Theorem 5.3.2. *Let χ be a 1-dimensional non-trivial character of a finite Galois extension K/k with Galois group G. Then $L(s, \chi, K/k)$ is non-zero at $s = 1$.*

Proof. We have just proved that $L(s, \chi, K/k)$ is actually the Artin L-function of a 1-dimensional character of an abelian extension. It thus suffices to prove the result in the special case where K/k is abelian. Every irreducible character of K/k is then 1-dimensional and by Proposition 50 we have the formula

$$\frac{\zeta_K(s)}{\zeta_k(s)} = \prod_{\chi' \neq 1_G} L(s, \chi', K/k)$$

where the product runs over all irreducible characters of K/k that are not the trivial character 1_G. By our above discussion, each $L(s, \chi', K/k)$ is a Weber L-function and extends holomorphically to $\mathbb{C}$ by Theorem 5.1.1. On the other hand, by Theorem 1.5.1, both ζ_K and ζ_k have a simple pole at $s = 1$ and thus the quotient $\frac{\zeta_K(s)}{\zeta_k(s)}$ has neither zero nor pole at $s = 1$. Since all $L(s, \chi', K/k)$ on the right hand side are holomorphic, if one factor has a zero at $s = 1$ then it cannot be balanced out by the other factors and the right hand side would have a zero of order at least 1 at $s = 1$ which is a contradiction. Thus $L(1, \chi', K/k) \neq 0$ and in particular this proves that $L(1, \chi, K/k) \neq 0$ as desired. □

5.4 Functional Equation of Artin L-Functions

Let K/k be a finite Galois extension of number fields with Galois group G and let χ be a character of G. By Brauer's Theorem 3.11.1, there exist subgroups

H_i with one-dimensional characters θ_i and integers n_i such that

$$\chi = \sum_i n_i \mathrm{Ind}_{H_i}^G \theta_i.$$

By Proposition 47 and Proposition 49 we have the equality

$$L(s, \chi, K/k) = \prod_i L(s, \theta_i, K/K^{H_i})^{n_i}.$$

By Theorem 5.3.1, each $L(s, \theta_i, K/K^{H_i})$ satisfies a functional equation centered at $\frac{1}{2}$. Therefore the same is true for $L(s, \chi, K/k)$ and therefore Artin L-functions extend to meromorphic functions on $\mathbb{C}$ via a functional equation centered at $s = \frac{1}{2}$. Since the functional equations of Artin L-functions of 1-dimensional characters relate the completed L-function of the character with the one of the conjugate character and the conjugate of a $\mathbb{Z}$-linear combination of characters is the same $\mathbb{Z}$-linear combination of the conjugates of the characters, the functional equation of a general Artin L-function will also relate the completed L-function of χ with the one of $\bar{\chi}$. But how do we get an explicit well-defined completed Artin L-function? One way to obtain this completed L-function would be to write the Artin L-function as a $\mathbb{Z}$-linear combination of monomial characters using Brauer's Theorem 3.11.1 and then defining the completed Artin L-function as the product of the completed L-functions of the monomial characters. But the expression obtained via Brauer's Theorem 3.11.1 is not unique and one cannot a priori guarantee that the completed Artin L-function obtained in this way is consistent with the different expressions. Moreover, the completed L-function would have to satisfy properties consistent with the addition, induction and inflation properties of Artin L-functions. Having made this observation we will not dwell on this problem any further but simply give the completed Artin L-function and state the functional equation.

In order to accomplish this, we need some notation and the definition of the Artin conductor. Let K/k be a Galois extension of number fields with Galois group G. Let V be a finite-dimensional complex linear representation of G with character χ. Having fixed the field extension K/k, we will simply write $L(s, \chi)$ for the Artin L-function of χ.

We start by adding in Gamma factors corresponding to the infinite places of k. The Galois group G acts on infinite places w of K in the following way:

$$|x|_{\sigma(w)} = |\sigma^{-1}(x)|_w.$$

Suppose that w lies above the infinite place v of k. Since σ fixes k, the infinite place $\sigma(w)$ also lies above v. It is not difficult to see that G acts transitively on the places above v.

Let v be an infinite place of k and let w be a place in K that lies above v. Define the decomposition group of w over v to be

$$D_w = D_{w/v} = \{\sigma \in G \,:\, \sigma(w) = w\}.$$

If w is a complex place and v a real place, then D_w is of order 2 and contains the identity and complex conjugation. Otherwise, D_w is the trivial group.

If D_w is non-trivial, then let χ_+ and χ_- respectively be the trivial and the non-trivial irreducible character of D_w. Since D_w is abelian, both characters have dimension 1. Decomposing χ into irreducible characters of D_w yields

$$\mathrm{Res}^G_{G_w}\chi = n_+(w)\chi_+ + n_-(w)\chi_-.$$

We have $n_+(w) = \left\langle \mathrm{Res}^G_{G_w}, \chi_+ \right\rangle_{G_w} = \dim_{\mathbb{C}} V^{D_w}$. Evaluating the above equation at the identity yields $\dim_{\mathbb{C}} V = n_+(w) + n_-(w)$ by Proposition 17 (i) so that $n_-(w) = \mathrm{codim}_{\mathbb{C}} V^{D_w}$. The particular choice of a place w above v does not affect the above decomposition since the decomposition groups of two places above v are conjugate (same proof as Proposition 10). We therefore write $n_+(v)$ and $n_-(v)$. We define

$$\begin{cases} L_v(s,\chi_+) = \Gamma_{\mathbb{C}}(s) & \text{if } v \text{ is complex} \\ L_v(s,\chi_+) = \Gamma_{\mathbb{R}}(s) & \text{if } v \text{ is real} \\ L_v(s,\chi_-) = \Gamma_{\mathbb{R}}(s+1) & \text{if } v \text{ is real.} \end{cases}$$

We define the local factor at v by

$$L_v(s,\chi) = L_v(s,\chi_+)^{n_+(v)} L_v(s,\chi_-)^{n_-(v)}.$$

For the definition of $\Gamma_{\mathbb{R}}$ and $\Gamma_{\mathbb{C}}$ see Definition 17.

We also define

$$a_1(\chi) = \sum_{v \text{ real}} n_+(v) \quad \text{and} \quad a_2(\chi) = \sum_{v \text{ real}} n_-(v).$$

It follows that

$$n = [k:\mathbb{Q}] = \frac{1}{\chi(1)}(a_1(\chi) + a_2(\chi) + 2r_2\chi(1)). \tag{5.4.0.1}$$

Explicitly, we then have

$$\prod_{v|\infty} L_v(s,\chi) = 2^{r_2\chi(1)(1-s)}\pi^{-\frac{a_2(\chi)}{2}-n\chi(1)\frac{s}{2}}\Gamma(s)^{r_2\chi(1)}\Gamma\left(\frac{s}{2}\right)^{a_1(\chi)}\Gamma\left(\frac{s+1}{2}\right)^{a_2(\chi)}.$$

Our next task is to define the exponential factor of the completed L-function. Let $\mathfrak{p}$ be a finite place of k and let $\mathfrak{P}$ be a place above $\mathfrak{p}$. For all $i \geq 0$ we define the i^{th} ramification group G_i to be the subgroup of $D_{\mathfrak{P}}$ consisting of elements that act trivially on $\mathcal{O}_K/\mathfrak{P}^{i+1}$. Explicitly, we have

$$G_i = \{\sigma \in D_{\mathfrak{P}} \ : \ v_{\mathfrak{P}}(\sigma(x) - x) \geq i+1 \text{ for all } x \in \mathcal{O}_K\}.$$

This gives a filtration

$$I_{\mathfrak{P}} = G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots$$

with $G_i = \{1\}$ for i large enough. If g_i denotes the order of G_i then we define

$$f(\chi,\mathfrak{p}) = \sum_{i=0}^{\infty} \frac{g_i}{g_0}\mathrm{codim}_{\mathbb{C}} V^{G_i}.$$

This definition does not depend on the choice of $\mathfrak{P}$. In fact, if $\mathfrak{P}'$ is another place above $\mathfrak{p}$ then $\mathfrak{P}' = \sigma(\mathfrak{P})$ for some $\sigma \in G$ and if G'_i denotes the ith ramification group of $\mathfrak{P}'$, then $G_i' = \sigma G_i \sigma^{-1}$. In fact, if τ is an element of G_i, then for $x \in \mathcal{O}_K$, we have

$$\sigma\tau\sigma^{-1}(x) - x = \sigma(\tau(\sigma^{-1}(x)) - \sigma^{-1}(x)) \in \sigma(\mathfrak{P}^{i+1}) = \mathfrak{P}'^{i+1}.$$

This proves that $G_i' \supseteq \sigma G_i \sigma^{-1}$. Applying this inclusion with σ^{-1} gives the desired equality.

Furthermore, if $\mathfrak{p}$ is unramified, then $f(\chi, \mathfrak{p}) = 0$ and one can prove that $f(\chi, \mathfrak{p})$ is an integer for any $\mathfrak{p}$.

Definition 20. The Artin conductor of χ is the ideal of $\mathcal{O}_k$ defined by

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

Definition 21. The completed Artin L-function of χ is defined, for $\Re s > 1$, by

$$\Lambda(s,\chi) = (|d_k|^{\chi(1)} N(f(\chi)))^{\frac{s}{2}} \prod_{v|\infty} L_v(s,\chi) L(s,\chi).$$

Theorem 5.4.1. *The completed Artin L-function of χ admits a meromorphic continuation to the whole complex plane and satisfies the functional equation*

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\bar{\chi})$$

where $|W(\chi)| = 1$.

Remark 20. We have seen that Artin L-functions satisfy additivity, inflation and induction properties in the region $\Re s > 1$. One can check that these properties extend to all of $\mathbb{C}$.

Artin did not prove Theorem 5.4.1. He proved Artin Reciprocity which is Theorem 2.4.1 and Theorem 2.4.2 and hereby completed global class field theory. This enabled him to prove the relation between Artin L-functions of 1-dimensional characters and Weber L-series which was established in the previous section. He also proved the following:

Theorem 5.4.2 (Artin)**.** *Any character of a finite group can be expressed as a $\mathbb{Q}$-linear combination of monomial characters.*

This enabled him to decompose his Artin L-functions into the product of rational powers of Artin L-functions of 1-dimensional characters which he knew by Hecke's work could be extended meromorphically to $\mathbb{C}$ via a functional equation centered at $s = \frac{1}{2}$. However, since the powers were rational, he could not conclude that his Artin L-functions could be extended meromorphically to $\mathbb{C}$. Suspecting however that this was true, he conjectured the following:

Conjecture 1 (Artin)**.** *Any character of a finite group can be expressed as a $\mathbb{Z}$-linear combination of monomial characters.*

This became known as Brauer's Theorem in 1946 when Brauer confirmed Artin's intuition. As we discussed in the beginning of this section, this result ensured that Artin L-functions admit a meromorphic continuation to $\mathbb{C}$. But Artin went even furtherand conjectured the following:

Conjecture 2 (Artin). *Every Artin L-function, except those associated to trivial characters, can be extended to a holomorphic function on $\mathbb{C}$.*

This result is commonly referred to as "Artin's Conjecture". It is known to hold, as we have already seen, in the case of one-dimensional characters. But for higher dimensional characters this is still an open problem and an active area of research today. Progress has been made in the 2-dimensional case by considering L-functions attached to certain modular forms of weight 2.

Chapter 6

Stark's Conjectures

The Stark Conjecture was introduced by Stark in the 1970's in his series of papers [StI], [StII], [StIII] and [StIV] and was later expanded by Tate in his book [Ta1]. It gives conjectural information concerning the leading term of the Taylor expansion of Artin L-function around $s = 0$ and generalizes the analytic class number formula of the Dedekind zeta-function. In the abelian rank 1 case Stark gave a more refined version of his conjecture. That is why this section is called Stark's conjectures in plural. We shall follow the exposition in [Ta1].

6.1 Preliminaries

The idea here is to present the motivation behind Stark's conjecture as well as defining the ingredients needed to state the conjecture.

6.1.1 The Class Number Formula at $s = 0$

Let k be a number field. In chapter 1 we proved Theorem 1.5.1, known as the class number formula, which states that the Dedekind zeta-function has a simple pole at $s = 1$ with residue given by

$$\mathrm{Res}_{s=1}(\zeta_k(s)) = \frac{2^{r_1}(2\pi)^{r_2}R_k}{\omega_k|d_k|^{\frac{1}{2}}}h_k.$$

By Corollary 28, the completed zeta-function $\Lambda_k(s)$ extends to all of $\mathbb{C}$ with simple poles at $s = 0$ and $s = 1$ and satisfies a functional equation $\Lambda_k(s) = \Lambda_k(1-s)$. We will use this to translate the above formula into information about ζ_k at $s = 0$.

Proposition 51. *The Dedekind zeta-function $\zeta_k(s)$ admits a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ with residue given by the class number formula. The Taylor expansion of $\zeta_k(s)$ at $s = 0$ is*

$$\zeta_k(s) = -\frac{h_k}{\omega_k}R_k s^{r_1+r_2-1} + O(s^{r_1+r_2}).$$

Proof. Using Theorem 28, we see that

$$\zeta_k(s) = |d_k|^{\frac{1}{2}-s}\pi^{(s-1/2)n}2^{(2s-1)r_2}\left(\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}\right)^{r_1}\left(\frac{\Gamma(1-s)}{\Gamma(s)}\right)^{r_2}\zeta_k(1-s).$$

Since $\Gamma_k(s)$ has a simple pole at $s = 0$ we see that $\zeta_k(s)$ is indeed holomorphic at $s = 0$ and the order of annulation of $\zeta_k(s)$ at $s = 0$ is $r_1 + r_2 - 1$. We compute that $\lim_{s\to 0} \frac{\zeta_k(s)}{s^{r_1+r_2-1}}$ is equal to

$$|d_k|^{\frac{1}{2}} \pi^{-\frac{n}{2}} 2^{-r_1-r_2} \Gamma\left(\frac{1}{2}\right)^{r_1} \Gamma(1)^{r_2} \lim_{s\to 0} \left(\frac{s}{2}\Gamma\left(\frac{s}{2}\right)\right)^{-r_1} (s\Gamma(s))^{-r_2} \lim_{s'\to 1} -(s'-1)\zeta_k(s').$$

Using the fact that $\Gamma(s)$ has a simple pole at $s = 0$ with residue 1, that the value of $\Gamma(s)$ at $s = 1/2$ is $\pi^{-1/2}$ and the class number formula 1.5.1, we see that

$$\lim_{s\to 0} \frac{\zeta_k(s)}{s^{r_1+r_2-1}} = -\frac{h_k}{\omega_k} R_k.$$

□

Remark 21. This result is truly remarkable. First of all, the leading coefficient of the Taylor series of $\zeta_k(s)$ around $s = 0$ is given by a global invariant of the field k, namely its regulator, times a rational number. Secondly, the order of annulation of $\zeta_k(s)$ at $s = 0$ is the rank of the unit group U_k by Theorem 1.4.2.

Definition 22. Let S be a finite subset of M_k containing M_k^∞. We define the S-modified Dedekind zeta-function, for $\Re s > 1$, by the Euler product

$$\zeta_{k,S}(s) = \prod_{\mathfrak{p}\notin S} (1 - N(\mathfrak{p})^{-s})^{-1} = \zeta_k(s) \prod_{\mathfrak{p}\in S\setminus M_k^\infty} (1 - N(\mathfrak{p})^{-s}).$$

Using the functional equation of $\zeta_k(s)$ we see that $\zeta_{k,S}(s)$ also admits a meromorphic continuation to the whole of the complex plane.

Proposition 52. *Let S be a finite subset of M_k containing M_k^∞. Let $\mathfrak{p} \notin S$ and define $S' = S \cup \{\mathfrak{p}\}$. Then, as $s \to 0$, we have*

$$\zeta_{K,S'}(s) \sim \log N(\mathfrak{p}) s \zeta_{K,S}(s)$$

meaning that the ratio tends to 1 *as $s \to 0$.*

Proof. We have $\zeta_{k,S'}(s) = (1 - N(\mathfrak{p})^{-s})\zeta_{k,S}(s)$. Thus

$$\lim_{s\to 0} \frac{\zeta_{k,S'}(s)}{\log N(\mathfrak{p}) s \zeta_{k,S}(s)} = \lim_{s\to 0} \frac{1 - N(\mathfrak{p})^{-s}}{s \log N(\mathfrak{p})} = \lim_{s\to 0} \frac{1}{1 + s \log N(\mathfrak{p})} = 1$$

where we used the rule of l'Hospital in the second equality. □

Corollary 29. *Let S be a finite subset of M_k containing M_k^∞. The Taylor expansion of $\zeta_{k,S}(s)$ at $s = 0$ is*

$$\zeta_{k,S}(s) = -\frac{h_{k,S}}{\omega_k} R_{k,S} s^{|S|-1} + O(s^{|S|}).$$

Proof. We prove this by induction on $n = |S \setminus M_K^\infty|$. The case $n = 0$ is Proposition 51. Suppose the result true for $n - 1$. Let $\mathfrak{p}$ be a prime in S and consider $S' = S \setminus \{\mathfrak{p}\}$. By induction hypothesis, we have

$$\lim_{s\to 0} \frac{\zeta_{k,S'}(s)}{s^{|S|-2}} = -\frac{h_{k,S'}}{\omega_k} R_{k,S'}.$$

If m denotes the order of $[\mathfrak{p}]$ in $\mathrm{Cl}(\mathcal{O}_{k,S'})$, then by Lemma 1 we have $h_{k,S'} = mh_{k,S}$ and by Proposition 7 we have $R_{k,S} = m\log N(\mathfrak{p})R_{k,S'}$. Thus

$$\lim_{s\to 0}\frac{\zeta_{k,S'}(s)}{s^{|S|-2}} = -\frac{h_{k,S}}{\log N(\mathfrak{p})\omega_k}R_{k,S}.$$

Finally, by Proposition 52, we have

$$\lim_{s\to 0}\frac{\zeta_{k,S}(s)}{s^{|S|-1}} = \log N(\mathfrak{p})\lim_{s\to 0}\frac{\zeta_{k,S'}(s)}{s^{|S|-2}} = -\frac{h_{k,S}}{\omega_k}R_{k,S}$$

and the proof is complete. □

Remark 22. We see that the leading term of the Taylor expansion of $\zeta_{k,S}(s)$ around $s = 0$ is the product of a rational number with the S-regulator of k. The latter is the determinant of a $(|S|-1)$-dimensional matrix with coefficient that are logarithmic. The order of $\zeta_{k,S}(s)$ at $s = 0$ is the rank of the S-unit group $U_{k,S}$ by Theorem 1.4.1.

6.1.2 The Order of Artin L-Functions at $s = 0$

Let K/k be a finite Galois extension of number fields with Galois group G. Let (ρ, V) be a complex representation of G with character χ. Let S be a finite subset of M_k that contains M_k^∞.

Definition 23. With the above notations, we define the S-modified Artin L-function of χ, for $\Re s > 1$, by

$$L_S(s,\chi,K/k) = \prod_{\mathfrak{p}\notin S}(\det(1-\rho_{\mathfrak{P}}((\mathfrak{P},K/k))N(\mathfrak{p})^{-s})|V^{I_{\mathfrak{P}}}))^{-1}.$$

This function admits a meromorphic continuation to the whole complex plane by Theorem 5.4.1. We write its Taylor expansion around $s = 0$ as follows:

$$L_S(s,\chi,K/k) = c_S(\chi,K/k)^{r_S(\chi,K/k)} + O(s^{r_S(\chi,K/k)+1}).$$

Having fixed the extension K/k we will write $L_S(s,\chi)$ instead of $L_S(s,\chi,K/k)$ in the rest of this section. Similarly, we write $c_S(\chi)$ and $r_S(\chi)$. In this section we shall compute $r_S(\chi)$. First, we fix some notations.

Let S_K be the finite subset of M_K consisting of the places that lie above the ones in S. Recall from Section 1.4 that Y_{K,S_K} denotes the free abelian group on the set S_K and X_{K,S_K} fits in the exact sequence of groups

$$0 \longrightarrow X_{K,S_K} \longrightarrow Y_{K,S_K} \xrightarrow{\text{aug}} \mathbb{Z} \longrightarrow 0.$$

The Galois group G acts on the left on the set of valuations S_K and for any $v \in S$, G acts transitively on the places $w \in S_K$ that lie above v. By giving $\mathbb{Z}$ the trivial G-action, the groups $Y_{K,S}$ and $X_{K,S}$ naturally come with a left action of G. Thus both $Y_{K,S}$ and $X_{K,S}$ have the structure of a left $\mathbb{Z}[G]$-module. It is an easy exercise to check that the above exact sequence of groups is an exact sequence in the category of left $\mathbb{Z}[G]$-modules.

By tensoring with $\mathbb{C}$ over $\mathbb{Z}$ we get an exact sequence in the category of left $\mathbb{C}[G]$ modules

$$0 \longrightarrow \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}Y_{K,S_K} \xrightarrow{\text{aug}} \mathbb{C} \longrightarrow 0.$$

By Proposition 16, $\mathbb{C}[G]$ is a semisimple ring, and by Remark 10 the above exact sequence splits. Consequently, as left $\mathbb{C}[G]$-modules, we have

$$\mathbb{C}Y_{K,S_K} \cong \mathbb{C}X_{K,S_K} \oplus \mathbb{C}. \tag{6.1.0.1}$$

As a consequence, if $\chi_{Y_{K,S_K}}$ and $\chi_{X_{K,S_K}}$ denote respectively the characters of the representations $\mathbb{C}Y_{K,S_K}$ and $\mathbb{C}X_{K,S_K}$, then we have

$$\chi_{Y_{K,S_K}} = \chi_{X_{K,S_K}} + 1_G.$$

By distributivity of the tensor product with respect to direct sums, we have the following isomorphisms of left $\mathbb{C}[G]$-modules:

$$\mathbb{C}Y_{K,S_K} \cong \bigoplus_{w\in S_K} \mathbb{C}w \cong \bigoplus_{v\in S}\bigoplus_{w|v} \mathbb{C}w.$$

If $v \in S$, then G acts transitively on the set $\{w \in S_K : w|v\}$. Pick one $w \in S_K$ that lies above v. Then, as left $\mathbb{C}[G]$-modules, we have

$$\bigoplus_{w|v} \mathbb{C}w \cong \bigoplus_{[\sigma]\in G/D_w} \mathbb{C}\sigma(w) \cong \operatorname{Ind}_{D_w}^G \mathbb{C}$$

where we used (3.4.0.1) for the last isomorphism. We have proved the following:

Proposition 53. *With the above notations, we have*

$$\chi_{Y_{K,S_K}} = \chi_{X_{K,S_K}} + 1_G = \sum_{v\in S} \operatorname{Ind}_{D_w}^G 1_{D_w}.$$

In particular, $\chi_{Y_{K,S_K}}$ and $\chi_{X_{K,S_K}}$ belong to $R(G,\mathbb{Q})$.

Proposition 54. *Let K/k be a finite Galois extension of number fields with Galois group G. Let V be a complex representation of G with character χ. With the above notations, we have*

$$\begin{aligned} r_S(\chi) &= \sum_{v\in S} \dim_{\mathbb{C}} V^{D_w} - \dim_{\mathbb{C}} V^G \\ &= \left\langle \chi, \chi_{X_{K,S_K}} \right\rangle_G \\ &= \dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \end{aligned}$$

where w is any place of S_K that lies above v.

Proof. The choice of $w \in S_K$ does not matter. In fact, let w' be another place above v. Then there exists $\sigma \in G$ such that $w' = \sigma(w)$. By Proposition 10 we have $D_{\sigma(w)} = \sigma D_w \sigma^{-1}$ and thus $V^{D_{\sigma(w)}} = \sigma(V^{D_w})$. As a consequence, $\dim_{\mathbb{C}} V^{D_{\sigma(w)}} = \dim_{\mathbb{C}} V^{D_w}$.

We now turn to the proof of the proposition. For simplicity in this proof we drop the subscripts K and S_K in our notations. Thus X_{K,S_K} becomes X and $\chi_{X_{K,S_K}}$ becomes χ_X.

By Proposition 20 the character of $V^\vee$ is $\bar{\chi}$. By Lemma 5 we have

$$\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X) = \langle \bar{\chi}, \chi_X \rangle_G.$$

But $\langle\bar{\chi}, \chi_X\rangle_G = \langle\chi, \bar{\chi}_X\rangle_G$ and by Proposition 53 we have $\chi_X \in R(G,\mathbb{Q})$ so that $\bar{\chi}_X = \chi_X$. We conclude that

$$\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X) = \langle\chi, \chi_X\rangle_G .$$

By Proposition 53, we have

$$\chi_X = \sum_{v\in S} \operatorname{Ind}_{D_w}^G 1_{D_w} - 1_G.$$

Using Theorem 3.10.2 we have

$$\langle\chi, \chi_X\rangle_G = \sum_{v\in S} \left\langle \chi, \operatorname{Ind}_{D_w}^G 1_{D_w} \right\rangle_G - \langle\chi, 1_G\rangle_G = \sum_{v\in S} \left\langle \operatorname{Res}_{G_w}^G \chi, 1_{D_w} \right\rangle_{D_w} - \langle\chi, 1_G\rangle_G .$$

By Lemma 5 we obtain

$$\langle\chi, \chi_X\rangle_G = \sum_{v\in S} \dim_{\mathbb{C}} V^{D_w} - \dim_{\mathbb{C}} V^G.$$

It remains to prove equality between $r_S(\chi)$ and any of the three quantities. By Theorem 3.11.1, there exist subgroups H_i of G with 1-dimensional characters θ_i and integers n_i for $i = 1, \ldots, m$ such that

$$\chi = \sum_{i=1}^m n_i \operatorname{Ind}_{H_i}^G \theta_i.$$

By Proposition 47 and Proposition 49, we have

$$L_S(s,\chi) = \prod_{i=1}^m L_S(s, \operatorname{Ind}_{H_i}^G \theta_i)^{n_i} = \prod_{i=1}^m L_S(s, \theta_i)^{n_i}.$$

If $r_S(\theta_i)$ denotes the order of $L_S(s,\theta_i)$ at $s = 0$, then we have

$$r_S(\chi) = \sum_{i=1}^m n_i r_S(\theta_i).$$

On the other hand, by linearity of the scalar product and by Theorem 3.10.2, we have

$$\langle\chi, \chi_X\rangle_G = \sum_{i=1}^m n_i \left\langle \operatorname{Ind}_{H_i}^G \theta_i, \chi_X \right\rangle_G = \sum_{i=1}^m n_i \left\langle \theta_i, \operatorname{Res}_{H_i}^G \chi_X \right\rangle_{H_i} .$$

It thus suffices to prove that $r_S(\theta_i) = \left\langle \theta_i, \operatorname{Res}_{H_i}^G \chi_X \right\rangle_{H_i}$ for each i in order to conclude the proof.

We have reduced the proof to the case where χ is a 1-dimensional character of G. We will prove that $r_S(\chi) = \langle\chi, \chi_X\rangle_G$. We distinguish two cases:

- $\chi = 1_G$: By Proposition 46 we have $L_S(s,\chi) = \zeta_{K,S}(s)$ and by Corollary 29 we have $r_S(1_G) = |S| - 1$. Moreover, we have $V^G = V$ so that $\dim_{\mathbb{C}} V^G = \dim_{\mathbb{C}} V = 1$. If $v \in S$ and $w \in S_K$ lies above v, then

$$\dim_{\mathbb{C}} V^{D_w} = \left\langle \operatorname{Res}_{D_w}^G \chi, 1_{D_w} \right\rangle_{D_w} = \langle 1_{G_w}, 1_{G_w}\rangle_{G_w} = 1.$$

  We conclude that $\sum_{v\in S} \dim_{\mathbb{C}} V^{D_w} - \dim_{\mathbb{C}} V^G = |S| - 1 = r_S(\chi)$.

- $\chi \neq 1_G$: We have $\dim_{\mathbb{C}} V^G = \langle \chi, 1_G \rangle_G = 0$ by orthogonality. By Theorem 5.3.2, $L(s,\chi)$ neither has a pole nor a zero at $s=1$. By Theorem 5.4.1, the completed Artin L-function $\Lambda(s,\chi)$ is equal to

$$W(\chi)(|d_k|^{\chi(1)}N(f(\chi)))^{\frac{s}{2}} \prod_{v|\infty} L_v(1-s,\bar{\chi}).L(1-s,\bar{\chi}).$$

By equating the orders at $s=0$, we obtain

$$-r_2 - a_1(\chi) + r(\chi) = 0$$

where $r(\chi)$ denotes the order of $L(s,\chi)$ at $s=0$. This implies, by (5.4.0.1), that

$$r(\chi) = r_2 + a_1(\chi) = n - a_2(\chi) - r_2 = r_1 + r_2 - a_2(\chi).$$

But $r_1+r_2 = |M_k^\infty|$ and since $\dim_{\mathbb{C}} V = 1$ this is equal to $\sum_{v\in M_k^\infty} \dim_{\mathbb{C}} V$. It follows that

$$r(\chi) = \sum_{v\in M_k^\infty} (\dim_{\mathbb{C}} V - \mathrm{codim}_{\mathbb{C}} V^{D_w}) = \sum_{v\in M_k^\infty} \dim_{\mathbb{C}} V^{D_w}$$

which is the desired formula in the case $S = M_k^\infty$.

We have

$$L_S(s,\chi) = L(s,\chi) \prod_{\mathfrak{p}\in S\setminus M_k^\infty} \det(1 - \chi_{\mathfrak{P}}((\mathfrak{P}, K/k))N(\mathfrak{p})^{-s})|V^{I_{\mathfrak{P}}}).$$

But $V^{I_{\mathfrak{P}}}$ is either V or 0 since V is of dimension 1 and we have $V^{I_{\mathfrak{P}}} = V$ exactly when $\chi(I_{\mathfrak{P}}) = 1$. Since V is of dimension 1, the character χ is a homomorphism from G to $\mathbb{C}^*$. Thus, if $\sigma_{\mathfrak{P}}$ is a representative of $(\mathfrak{P}, K/k)$ in $D_{\mathfrak{P}}$, then by Proposition 9 we have

$$\chi_{\mathfrak{P}}((\mathfrak{P}, K/k)) = \frac{1}{e_{\mathfrak{p}}} \sum_{\tau\in I_{\mathfrak{P}}} \chi(\sigma_{\mathfrak{P}}\tau) = \chi(\sigma_{\mathfrak{P}}) \left\langle \mathrm{Res}^G_{I_{\mathfrak{P}}} \chi, 1_{I_{\mathfrak{P}}} \right\rangle_{I_{\mathfrak{P}}}.$$

Hence if $\chi(I_{\mathfrak{P}}) = 1$, then $\chi_{\mathfrak{P}}((\mathfrak{P}, K/k)) = \chi(\sigma_{\mathfrak{P}})$. As a consequence, we have

$$L_S(s,\chi) = L(s,\chi) \prod_{\substack{\mathfrak{p}\in S\setminus M_k^\infty \\ \chi(I_{\mathfrak{P}})=1}} \left(1 - \frac{\chi(\sigma_{\mathfrak{P}})}{N(\mathfrak{p})^s}\right).$$

So we collect a zero at $s=0$ in the product exactly when $\chi(\sigma_{\mathfrak{P}}) = 1$. But since $\chi(I_{\mathfrak{P}}) = 1$ and $[\sigma_{\mathfrak{P}}]$ generates $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ we get $\chi(D_{\mathfrak{P}}) = 1$. Thus

$$\begin{aligned} r_S(\chi) &= r(\chi) + |\{\mathfrak{p} \in S \setminus M_k^\infty \ : \ \chi(D_{\mathfrak{P}}) = 1\}| \\ &= \sum_{v\in M_k^\infty} \dim_{\mathbb{C}} V^{D_w} + \sum_{\mathfrak{p}\in S\setminus M_k^\infty} \left\langle \mathrm{Res}^G_{G_{\mathfrak{P}}} \chi, 1_{D_{\mathfrak{P}}} \right\rangle_{D_w} \\ &= \sum_{v\in M_k^\infty} \dim_{\mathbb{C}} V^{D_w} + \sum_{\mathfrak{p}\in S\setminus M_k^\infty} \dim_{\mathbb{C}} V^{D_{\mathfrak{P}}} \\ &= \sum_{v\in S} \dim_{\mathbb{C}} V^{D_w}. \end{aligned}$$

□

In the course of the proof we proved the following result which we record as a corollary for future use:

Corollary 30. *Let K/k be a finite Galois extension of number fields with Galois group G. If χ is a 1-dimensional character of G, then*

$$r_S(\chi) = \begin{cases} |S| - 1 & \textit{if } \chi = \mathbf{1}_G \\ |\{v \in S \ : \ \chi(D_w) = 1\}| & \textit{otherwise.} \end{cases}$$

6.1.3 Partial Zeta-Functions

Let K/k be a finite abelian extension of number fields with Galois group G.

Definition 24. Let S be a finite subset of M_k containing M_k^∞ and containing all finite ramified places of k. Let $\mathfrak{s}$ denote the product of all finite places in S. This is an ideal of $\mathcal{O}_k$. Let $\sigma \in G$ and define, for $\Re s > 1$, the function

$$\zeta_S(s, \sigma) = \sum_{\substack{(\mathfrak{a}, \mathfrak{s}) = 1 \\ \Phi_{K/k, \mathfrak{s}}(\mathfrak{a}) = \sigma}} N(\mathfrak{a})^{-s},$$

where the sum is over all integral ideals of k coprime to $\mathfrak{s}$ whose Artin symbol is σ.

Remark 23. By comparing with the Dedekind zeta function ζ_k one sees immediately that the above sum is absolutely convergent for $\Re s > 1$. Moreover, one can show that these functions admit a meromorphic continuation to the whole complex plane and satisfy a functional equation. These extended functions are known as partial zeta functions of K/k relative to σ.

Proposition 55. *Let K/k be a finite abelian extension with Galois group G. Let S be a finite subset of M_k containing M_k^∞ as well as all finite places that ramify in K/k. The functions $\zeta_S(s, \cdot) : G \longrightarrow \mathbb{C}$ and $L_S(s, \cdot) : \widehat{G} \longrightarrow \mathbb{C}$ are Fourier and inverse Fourier transforms of one-another for the group $\widehat{G}$. That is,*

$$\zeta_S(s, \sigma) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \bar{\chi}(\sigma) L_S(s, \chi, K/k), \qquad L_S(s, \chi, K/k) = \sum_{\sigma \in G} \chi(\sigma) \zeta_S(s, \sigma).$$

Proof. Let $\mathfrak{s}$ be a modulus of k with factors all finite places in S and all real places of S and such that the conductor $\mathfrak{f}$ of K/k divides $\mathfrak{s}$. By Theorem 2.4.2, K is a subfield of the ray class field $k(\mathfrak{s})$. Denote by Res the restriction map $\mathrm{Gal}(k(\mathfrak{s})/k) \longrightarrow G$. It induces an isomorphism of groups

$$\mathrm{Gal}(k(\mathfrak{s})/K)/\mathrm{Gal}(k(\mathfrak{s})/K) \longrightarrow G.$$

Let $\chi \in \widehat{G}$. By Corollary 29, χ is a 1-dimensional character of G. We define

$$\chi_{\mathfrak{s}} := \mathrm{Infl}_{\mathrm{Gal}(k(\mathfrak{s})/K)}^{\mathrm{Gal}(k(\mathfrak{s})/k)} (\chi \circ \mathrm{Res}) : \mathrm{Gal}(k(\mathfrak{s})/k) \longrightarrow \mathbb{C}^*$$

and $\chi'_{\mathfrak{s}} = \chi_{\mathfrak{s}} \circ \Phi_{k(\mathfrak{s})/k, \mathfrak{f}}$. The latter is a character of $\mathrm{Cl}_k(\mathfrak{s})$. We claim that

$$L_S(s, \chi, K/k) = L_W(s, \chi'_{\mathfrak{s}}). \qquad (6.1.0.2)$$

In fact, let $\mathfrak{p} \notin S$. Then $\mathfrak{p}$ is unramified and its Frobenius element $\sigma_{\mathfrak{p}}$ belongs to G. Since we are in the abelian case, the Frobenius element is independent of the choice of a prime $\mathfrak{P}$ over $\mathfrak{p}$. On one hand we have

$$L_S(s,\chi,K/k) = \prod_{\mathfrak{p}\notin S}(1-\chi(\sigma_{\mathfrak{p}})N(\mathfrak{p})^{-s})^{-1}.$$

On the other hand we have

$$L_W(s,\chi'_{\mathfrak{s}}) = \prod_{\mathfrak{p}\notin S}(1-\chi'_{\mathfrak{s}}(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}.$$

But if $\mathfrak{p} \notin S$, then by Proposition 13 we have

$$\chi'_{\mathfrak{s}}(\mathfrak{p}) = \chi_{\mathfrak{s}}((\mathfrak{p},k(\mathfrak{s})/k)) = \chi(\mathrm{Res}((\mathfrak{p},k(\mathfrak{s})/k))) = \chi((\mathfrak{p},K/k)) = \chi(\sigma_{\mathfrak{p}}).$$

This proves (6.1.0.2).

If $\mathfrak{p} \notin S$, then by Proposition 13 we have

$$\mathrm{Res}((\mathfrak{p},k(\mathfrak{s})/k)) = (\mathfrak{p},K/k).$$

It follows that for any $\mathfrak{a}$ coprime to $\mathfrak{s}$ we have

$$\mathrm{Res}((\mathfrak{a},k(\mathfrak{s})/k)) = (\mathfrak{a},K/k).$$

Let $\sigma \in G$ and suppose that $(\mathfrak{a},K/k) = \sigma$. Then we have

$$\chi(\sigma) = \chi((\mathfrak{a},K/k)) = \chi((\mathrm{Res}((\mathfrak{a},k(\mathfrak{f})/k)))) = \chi_{\mathfrak{s}}((\mathfrak{a},k(\mathfrak{s})/k)) = \chi'_{\mathfrak{s}}(\mathfrak{a}).$$

We now compute that

$$\sum_{\sigma\in G}\chi(\sigma)\zeta_S(s,\sigma) = \sum_{\sigma\in G}\sum_{\substack{(\mathfrak{a},\mathfrak{s})=1\\ (\mathfrak{a},K/k)=\sigma}}\frac{\chi'_{\mathfrak{s}}(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{(\mathfrak{a},\mathfrak{s})=1}\frac{\chi'_{\mathfrak{s}}(\mathfrak{a})}{N(\mathfrak{a})^s} = L_W(s,\chi'_{\mathfrak{s}}).$$

By (6.1.0.2) the proof of the second formula is complete.

Using this formula and Proposition 28, we also have

$$\begin{aligned}\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\bar{\chi}(\sigma)L_S(s,\chi,K/k) &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\bar{\chi}(\sigma)\sum_{\tau\in G}\chi(\tau)\zeta_S(s,\tau)\\ &= \sum_{\tau\in G}\zeta_S(s,\tau)\left(\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\bar{\chi}(\sigma)\chi(\tau)\right)\\ &= \zeta_S(s,\sigma).\end{aligned}$$

□

The following theorem is due to Siegel. We do not prove it in this paper.

Theorem 6.1.1 (Siegel). *Let K/k be a finite abelian extension of number fields with Galois group G. Let S be a finite subset of M_k containing M_k^∞ as well as all finite places that ramify in K/k. For any $\sigma \in G$, we have*

$$\zeta_S(0,\sigma) \in \mathbb{Q}.$$

Proof. See p. 101-102 of [Sie]. □

6.2 The Stark Regulator

6.2.1 Motivation and Definition

Let K/k be a finite Galois extension of number fields with Galois group G. Let S be a finite subset of M_k containing M_k^∞ and let S_K denote the finite subset of M_K consisting of those places that divide the ones in S. Corollary 29 says that, as $s \to 0$, we have

$$\zeta_{K,S_K}(s) \sim -\frac{h_{K,S_K}}{\omega_K} R_{K,S_K} s^{|S_K|-1}.$$

This is the analytic class number formula. By Remark 3, the S_K-regulator is the absolute value of the determinant of the map

$$\lambda_{K,S_K} : \mathbb{C}U_{K,S_K} \longrightarrow \mathbb{C}X_{K,S_K}, \quad u \longrightarrow \sum_{w \in S_K} \log |u|_w w$$

with respect to a basis $\{u_1, \ldots, u_{|S_K|-1}\}$ of U_{K,S_K} and a basis $\{w - w_0\}_{w \in S_K \setminus \{w_0\}}$ for some $w_0 \in S_K$.

By Proposition 50, we have

$$\zeta_{K,S_K}(s) = \prod_{\chi \in \widehat{G}} L_S(s, \chi, K/k)^{\chi(1)}.$$

Since ζ_{K,S_K} has the analytic class number formula, it occurred to Stark in view of this decomposition that it might be possible to break this formula up into pieces. Hence, the Artin L-function of an irreducible character χ should have an analogue of the class number formula corresponding to a piece of the formula for the zeta-function. Moreover, the class number formula that we know for ζ_{K,S_K} should be the result of a piecing together of the formulas for Artin L-functions.

Finally, if θ is any character of G, then by the canonical decomposition, it may be written uniquely as

$$\theta = \sum_{\chi \in \widehat{G}} m_\chi \chi$$

where the m_χ are non-negative integers. By Proposition 47, we obtain

$$L(s, \theta) = \prod_{\chi \in \widehat{G}} L(s, \chi)^{m_\chi}.$$

If the Artin L-functions of irreducible characters had an analogue of the class number formula, by piecing these together one should be able to deduce such a formula for the Artin L-function of θ.

The class number formula of ζ_{K,S_K} relates the leading coefficient of its Taylor expansion around $s = 0$ to the product of a rational number with the determinant of a matrix of size the rank of ζ_{K,S_K} at $s = 0$. Stark was lead to conjecture that the leading coefficient of the Artin L-function of a character θ of G should be the product of some algebraic number with the determinant of a matrix of size the rank of $L(s, \theta)$ at $s = 0$. By Proposition 54, this rank is equal to

$r_S(\theta) = \dim_{\mathbb{C}} \operatorname{Hom}(V^\vee, \mathbb{C}X_{K,S_K})$. In this section, we present the type of regulator introduced by Stark to play the role of the determinant of the matrix of size $r_S(\theta)$, which is accordingly called the Stark regulator.

We consider the group homomorphism

$$\lambda_{K,S_K} : U_{K,S_K} \longrightarrow \mathbb{R}X_{K,S_K}, \qquad u \longmapsto \sum_{w \in S_K} \log |u|_w w.$$

The kernel of this map is μ_K and the image sits as a lattice in $\mathbb{R}X_{K,S_K}$ (cf. § 1.4).

The group G acts on the left on U_{K,S_K} and X_{K,S_K}. By letting G act trivially on $\mathbb{R}$, the real vector space $\mathbb{R}X_{K,S_K}$ acquires the structure of a left G-module. We claim that λ_{K,S_K} is a homomorphism of left G-modules. In fact, if $\sigma \in G$ and $u \in U_{K,S_K}$, then

$$\begin{aligned}\sigma(\lambda_{K,S_K}(u)) &= \sum_{w \in S_K} \log |u|_w \sigma(w) = \sum_{w \in S_K} \log |u|_{\sigma^{-1}(w)} w \\ &= \sum_{w \in S_K} \log |\sigma(u)|_w w = \lambda(\sigma(u)).\end{aligned}$$

We therefore have a short exact sequence of left $\mathbb{Z}[G]$-modules

$$1 \longrightarrow \mu_K \longrightarrow U_{K,S_K} \longrightarrow \lambda_{K,S_K}(U_{K,S_K}) \longrightarrow 1.$$

Tensoring with $\mathbb{C}$ over $\mathbb{Z}$, we get an exact sequence of left $C[G]$-modules

$$1 \longrightarrow \mathbb{C}\mu_K \longrightarrow \mathbb{C}U_{K,S_K} \longrightarrow \mathbb{C}\lambda_{K,S_K}(U_{K,S_K}) \longrightarrow 1.$$

Since μ_K is finite, we have $\mathbb{C}\mu_K = \{1\}$. Since $\lambda_{K,S}(U_{K,S})$ is a lattice in $\mathbb{R}X_{K,S_K}$ we have $\mathbb{R}\lambda_{K,S}(U_{K,S}) = \mathbb{R}X_{K,S_K}$. We conclude that we have an isomorphism of left $\mathbb{C}[G]$-modules

$$\lambda_{K,S_K} : \mathbb{C}U_{K,S_K} \longrightarrow \mathbb{C}X_{K,S_K}.$$

As a consequence, the character of the representation $\mathbb{C}U_{K,S_K}$ of G is $\chi_{X_{K,S_K}}$. By Proposition 53 we know that

$$\chi_{X_{K,S_K}} = \sum_{v \in S} \operatorname{Ind}_{D_w}^G 1_{D_w} - 1_G \in R(G, \mathbb{Q}).$$

Notice that $1_{D_w} \in R_{\mathbb{Q}}(D_w)$ and $1_G \in R_{\mathbb{Q}}(G)$. Moreover the $\mathbb{Q}$-representation $\mathbb{Q}[G] \otimes_{\mathbb{Q}[D_w]} \mathbb{Q}$ of G has character $\operatorname{Ind}_{D_w}^G 1_{D_w}$. As a consequence, $\operatorname{Ind}_{D_w}^G 1_{D_w} \in R_{\mathbb{Q}}(G)$ and we conclude that $\chi_{X_{K,S_K}} \in R_{\mathbb{Q}}(G)$. By Proposition 32, the representations $\mathbb{C}U_{K,S_K}$ and $\mathbb{C}X_{K,S_K}$ are defined over $\mathbb{Q}$.

The rational representations $\mathbb{Q}U_{K,S_K}$ and $\mathbb{Q}X_{K,S_K}$ share the same character $\chi_{X_{K,S_K}}$ and therefore they must be isomorphic as left $\mathbb{Q}[G]$-modules. But there is no canonical way to define an isomorphism. Let

$$f : \mathbb{Q}X_{K,S_K} \longrightarrow \mathbb{Q}U_{K,S_K}$$

be such an isomorphism. By tensoring get an isomorphism of left $\mathbb{C}[G]$-modules

$$f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$$

which is defined over $\mathbb{Q}$. By composition we get a left $\mathbb{C}[G]$-module isomorphism

$$\lambda_{K,S_K} \circ f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}X_{K,S_K}$$

Let V be a complex representation of G with character χ. By applying the functor $\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, -)$, we get a $\mathbb{C}$-linear isomorphism

$$\begin{array}{rccc} (\lambda_{K,S_K} \circ f)_V : & \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) & \longrightarrow & \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \\ & \phi & \longmapsto & \lambda_{K,S_K} \circ f \circ \phi. \end{array}$$

Definition 25. With the above notations, we define the Stark regulator of χ relative to f by

$$R_S(\chi, f, K/k) = \det((\lambda_{K,S_K} \circ f)_V).$$

Remark 24. The definition of the Stark regulator does not depend on the choice of the realization V of χ. In fact, suppose that W is another realization of G. Then there exists an isomorphism $\psi : V \longrightarrow W$ of left $\mathbb{C}[G]$-modules which induces an isomorphism of left $\mathbb{C}[G]$-modules $\psi^* : W^\vee \longrightarrow V^\vee$ defined by $g \mapsto g \circ \psi$. By naturality of the Hom functor, we have the following commutative diagram:

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \arrow[r, "(\lambda_{K,S_K} \circ f)_V"] \arrow[d, "\mathrm{Hom}_{\mathbb{C}[G]}(\psi^*, \mathbb{C}X_{K,S_K})"'] & \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \arrow[d, "\mathrm{Hom}_{\mathbb{C}[G]}(\psi^*, \mathbb{C}X_{K,S_K})"] \\ \mathrm{Hom}_{\mathbb{C}[G]}(W^\vee, \mathbb{C}X_{K,S_K}) \arrow[r, "(\lambda_{K,S} \circ f)_W"'] & \mathrm{Hom}_{\mathbb{C}[G]}(W^\vee, \mathbb{C}X_{K,S_K}). \end{tikzcd}$$

In fact, if $\phi \in \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S}))$, then both paths map ϕ to $\lambda_{K,S_K} \circ f \circ \phi \circ \psi^*$. This implies that

$$(\lambda_{K,S_K} \circ f)_V = \mathrm{Hom}_{\mathbb{C}[G]}(\psi^*, \mathbb{C}X_{K,S_K}))^{-1} \circ (\lambda_{K,S_K} \circ f)_W \circ \mathrm{Hom}_{\mathbb{C}[G]}(\psi^*, \mathbb{C}X_{K,S_K})$$

and the determinants are equal.

Proposition 56. *Let V be a representation of G with character χ. With the above notations, we have*

$$R_S(\chi, f, K/k) = \det(1_V \otimes (\lambda_{K,S} \circ f) | (V \otimes_{\mathbb{C}} \mathbb{C}X_{K,S})^G).$$

Proof. By Corollary 12, there is an isomorphism of $\mathbb{C}$-vector spaces

$$\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \cong (V \otimes_{\mathbb{C}} \mathbb{C}X_{K,S_K})^G.$$

We claim that the diagram

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \arrow[r, "(\lambda_{K,S_K} \circ f)_V"] & \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \\ (V \otimes_{\mathbb{C}} \mathbb{C}X_{K,S_K})^G \arrow[u, "\cong"] \arrow[r, "1_{\mathbb{V}} \otimes (\lambda_{K,S_K} \circ f)"'] & (V \otimes_{\mathbb{C}} \mathbb{C}X_{K,S_K})^G \arrow[u, "\cong"'] \end{tikzcd}$$

commutes.

In fact, let $v \in V$ and $x \in \mathbb{C}X_{K,S_K}$. Taking the up-right path we arrive at

$$\lambda_{K,S_K} \circ f \circ F_{v \otimes x} : g \mapsto \lambda_{K,S_K} \circ f(g(v)x) = g(v)\lambda_{K,S_K} \circ f(x)$$

and taking the right-up path we arrive at

$$F_{v\otimes(\lambda_{K,S_K}\circ f(x))} : g \mapsto g(v)\lambda_{K,S_K}\circ f(x).$$

Thus $R_S(\chi, f, K/k) = \det(1_V \otimes (\lambda_{K,S}\circ f))$. □

Remark 25. Recall that we have an isomorphism of left $\mathbb{C}[G]$-modules

$$\lambda_{K,S_K} : \mathbb{C}U_{K,S_K} \longrightarrow \mathbb{C}X_{K,S_K}.$$

An idea would have been to apply the functor $\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, -)$ and get a $\mathbb{C}$-linear isomorphism

$$\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \lambda_{K,S_K}) : \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}U_{K,S_K}) \longrightarrow \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}).$$

Then one would take the determinant of this isomorphism. But this determinant depends on the choices of bases that we make. This makes this definition very difficult to manipulate. Choosing a non-canonical left $\mathbb{C}[G]$-isomorphism $f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$ defined over $\mathbb{Q}$ enables us to define without ambiguity the determinant of $(\lambda_{K,S_K}\circ f)_V$ since this is now an $\mathbb{C}$-linear automorphism of a vector space. Basically, choosing f amounts to making a choice of basis but this description due to Tate is much easier to use.

6.2.2 Compatibility of the Map λ in Towers

Let $K/K'/k$ be a tower of finite Galois extensions of number fields. Let $G = \mathrm{Gal}(K/k)$ and let $H = \mathrm{Gal}(K/K')$ so that $\mathrm{Gal}(K'/k) \cong G/H$. Let S be a finite subset of M_k containing M_k^∞. Let S_K and $S_{K'}$ be respectively the finite subsets of M_K and $M_{K'}$ consisting of those places that lie above the ones in S.

For simplicity in this section, we remove the indices K, S_K and $K', S_{K'}$ and simply write $\lambda = \lambda_{K,S_K}, U = U_{K,S_K}, X = X_{K,S_K}$ and similarly $\lambda' = \lambda_{K',S_{K'}}, U' = U_{K',S_{K'}}, X' = X_{K',S_{K'}}$.

Let $\mathfrak{p}$ be a finite place in S. Let $\mathfrak{P}'$ be a place of $S_{K'}$ above $\mathfrak{p}$ and let $\mathfrak{P}$ be a place of S_K above $\mathfrak{P}'$. Denote by $K_{\mathfrak{P}}, K'_{\mathfrak{P}'}$ and $k_{\mathfrak{p}}$ the respective completions and let $[\mathfrak{P} : \mathfrak{P}']$ denote the degree of the extension $K_{\mathfrak{P}}/K'_{\mathfrak{P}'}$. Let $(e_{\mathfrak{P}}, f_{\mathfrak{P}}), (e_{\mathfrak{P}'}, f_{\mathfrak{P}'})$ and $(e'_{\mathfrak{P}}, f'_{\mathfrak{P}})$ be respectively the ramification index and residual degree of $\mathfrak{P}/\mathfrak{p}$, $\mathfrak{P}'/\mathfrak{p}$ and $\mathfrak{P}/\mathfrak{P}'$. By multiplicativity we have $e_{\mathfrak{P}} = e'_{\mathfrak{P}}e_{\mathfrak{P}'}$ and $f_{\mathfrak{P}} = f'_{\mathfrak{P}}f_{\mathfrak{P}'}$. We also have $[\mathfrak{P} : \mathfrak{P}'] = e'_{\mathfrak{P}}f'_{\mathfrak{P}}$. It follows that

$$\sum_{\mathfrak{P}|\mathfrak{P}'} [\mathfrak{P} : \mathfrak{P}'] = [K : K']. \tag{6.2.0.1}$$

Lemma 12. *With the previous notations, the restriction of* $|\cdot|_{\mathfrak{P}}$ *to* K' *is equal to* $|\cdot|_{\mathfrak{P}'}^{[\mathfrak{P}:\mathfrak{P}']}$.

Proof. For any $x \in K'$, we have

$$\begin{aligned}
|x|_{\mathfrak{P}} &= N(\mathfrak{P})^{-v_{\mathfrak{P}}(x)} = N(\mathfrak{P})^{-e'_{\mathfrak{P}}v_{\mathfrak{P}'}(x)} \\
&= N(\mathfrak{p})^{-f_{\mathfrak{P}}e'_{\mathfrak{P}}v_{\mathfrak{P}'}(x)} = N(\mathfrak{P}')^{-\frac{f_{\mathfrak{P}}e'_{\mathfrak{P}}}{f_{\mathfrak{P}'}}v_{\mathfrak{P}'}(x)} \\
&= N(\mathfrak{P}')^{-f'_{\mathfrak{P}}e'_{\mathfrak{P}}v_{\mathfrak{P}'}(x)} = |x|_{\mathfrak{P}'}^{[\mathfrak{P}:\mathfrak{P}']}.
\end{aligned}$$

□

Remark 26. A similar result is true for archimedean places. Suppose that $v \in M_k^\infty$ and w, w' are places above v such that $w|w'$. Denote by K_w and $K'_{w'}$ the completions and by $[w : w']$ the degree of $K_w/K'_{w'}$. This is equal to either 1 or 2. It is immediately verified that if $x \in K'$, then similarly we have $|x|_w = |x|_{w'}^{[w:w']}$.

Moreover, since K/K' is Galois, we have $[w_1 : w'] = [w_2 : w']$ for all places w_1 and w_2 that lies above w' and we have the formula

$$\sum_{w|w'} [w : w'] = [K : K']. \tag{6.2.0.2}$$

Proposition 57. *Let E be a field of characteristic zero. With the above notations, there exists a left $E[G/H]$-module isomorphism*

$$j = j_{K/K',S} : EX' \longrightarrow (EX)^H.$$

Proof. Consider the map

$$j : X' \longrightarrow X, \qquad w' \longmapsto \sum_{w|w'} [w : w']w.$$

This is well-defined. In fact, if $\sum_{w' \in S_{K'}} n_{w'} w' \in X'$ then by definition we have $\sum_{w' \in S_{K'}} n_{w'} = 0$. We have

$$j\left(\sum_{w' \in S_{K'}} n_{w'} w'\right) = \sum_{w' \in S_{K'}} \sum_{w|w'} [w : w'] n_{w'} w.$$

By (6.2.0.1) and (6.2.0.2) we have

$$\sum_{w' \in S_{K'}} \sum_{w|w'} [w : w'] n_{w'} = [K : K'] \sum_{w' \in S_{K'}} n_{w'} = 0$$

which proves that $j\left(\sum_{w' \in S_{K'}} n_{w'} w'\right) \in X$.

It is easily seen that the map j is an injective homomorphism of groups. Note that if $w' \in S_{K'}$ and w_0 is some place in S_K that lies above w', then we have

$$j(w') = \sum_{[h] \in H/D_{w_0/w'}} [h(w_0) : w']h(w_0)$$

since H acts transitively on the places that lie above w'. The order of the decomposition group $D_{w_0/w'}$ is $[w_0 : w']$ and for all places $w|w'$ we have $[w : w'] = [w_0 : w']$ since K/K' is Galois. Hence, we have

$$j(w') = |D_{w_0}| \sum_{[h] \in H/D_{w_0}} h(w_0) = \sum_{h \in H} h(w_0).$$

It follows that $j(X') = N_H X$ where $N_H = \sum_{h \in H} h \in \mathbb{Z}[G]$. We have shown that we have an isomorphism of groups

$$j : X' \longrightarrow N_H X.$$

We claim that $N_H X$ is a subgroup of X^H of finite index. It is easily seen that it is indeed a subgroup. Let $\alpha = \sum_{w \in S_K} n_w w$ be an element of X^H. Then for all $h \in H$, we must have

$$\alpha = h(\alpha) = \sum_{w \in S_K} n_w h(w) = \sum_{w \in S_K} n_{h^{-1}(w)} w.$$

By comparing the coefficients, we see that α belongs to X^H if and only if $n_w = n_{h(w)}$ for all $h \in H$. In other words, all w that lie over the same w' in $S_{K'}$ must share the same coefficient n_w which consequently only depends on w'. We may therefore write $n_{w'} = n_w$ for all $w|w'$. It follows that α can be written as

$$\alpha = \sum_{w' \in S_{K'}} n_{w'} \sum_{w|w'} w = \sum_{w' \in S_{K'}} n_{w'} \sum_{[h] \in H/G_{w_0}} h(w_0)$$

for some choice of valuation w_0 that lies above w'. But we have

$$\sum_{[h] \in H/G_{w_0}} h(w_0) = \frac{1}{[w_0 : w']} \sum_{h \in H} h(w_0).$$

Thus α belongs to $N_H X$ if and only if $[w_0 : w']$ divides $n_{w'}$ for each w' in which case we have

$$\alpha = N_H \left(\sum_{w'} \frac{n_{w'}}{[w_0 : w']} w_0 \right).$$

We conclude that

$$N_H X = \{ \sum_{w \in S_K} n_w w \in X^H \ : \ [w : w|_{K'}] | n_w, \forall w \in S_K \}.$$

We consider the map

$$\phi : X^H \longrightarrow \bigtimes_{w' \in S_{K'}} \mathbb{Z}/[w_0 : w']\mathbb{Z}, \qquad \sum_w n_w w \longmapsto (n_{w_0} \mod [w_0 : w'])_{w' \in S_{K'}}$$

where w_0 denotes an arbitrary place of S_K that lies above w'. This map is well-defined by our characterization of X^H. Moreover, ϕ is clearly a surjective homomorphism of groups and its kernel is exactly $N_H X$ by our characterization of $N_H X$. We conclude that we have an isomorphism of groups

$$X^H / N_H X \longrightarrow \bigtimes_{w' \in S_{K'}} \mathbb{Z}/[w_0 : w']\mathbb{Z}.$$

In particular, $N_H X$ has finite index in X^H.

Let E be a field of characteristic zero. Tensoring with E over $\mathbb{Z}$ we get an exact sequence of E-vector spaces

$$0 \longrightarrow E(N_H X) \longrightarrow EX^H \longrightarrow E(X^H / N_H X) \longrightarrow 0.$$

Since $X^H / N_H X$ is finite we have $E(X^H / N_H X) = 0$ and therefore we have an isomorphism of E-vector spaces

$$E(N_H X) \longrightarrow EX^H$$

induced by the inclusion map. Since X' is isomorphic to $N_H X$ via j we get an isomorphism of E-vector spaces

$$j : EX' \longrightarrow EX^H.$$

It remains only to check that this is also a homomorphism of left G/H-modules: if $[\sigma] \in G/H, w' \in S_{K'}$ and w_0 is a place in S_K that lies above w', then we have

$$j([\sigma](w')) = \sum_{h \in H} h(\sigma(w_0)) = \sum_{h \in H} \sigma(h(w_0)) = [\sigma](j(w'))$$

by normality of H. We conclude that the map j is a left $E[G/H]$-module isomorphism. □

Remark 27. By tensoring with $\mathbb{R}$ over $\mathbb{Z}$ we get an injective homomorphism of $\mathbb{R}$-vector spaces $j_{K/K',S} : \mathbb{R}X_{K',S_{K'}} \longrightarrow \mathbb{R}X_{K,S_K}$ which is a left $\mathbb{R}[G/H]$-isomorphism on its image $\mathbb{R}X^H_{K,S_K}$. We claim that the following diagram commutes:

$$\begin{tikzcd}
U_{K,S_K} \arrow[r, "\lambda_{K,S_K}"] & \mathbb{R}X_{K,S_K} \\
U'_{K',S_{K'}} \arrow[u, hook] \arrow[r, "\lambda_{K',S_{K'}}"'] & \mathbb{R}X_{K',S_{K'}}. \arrow[u, "j_{K/K',S}"']
\end{tikzcd}$$

Let $u' \in U_{K',S_{K'}}$. Then, by Lemma 12, we have

$$\begin{aligned}
j_{K/K',S}(\lambda_{K',S_{K'}}(u')) &= j_{K/K',S}\left(\sum_{w' \in S_{K'}} \log|u'|_{w'} w'\right) \\
&= \sum_{w' \in S_{K'}} \log|u'|_{w'} \sum_{w|w'} [w : w'] w \\
&= \sum_{w' \in S_{K'}} \sum_{w|w'} \log|u'|_{w'}^{[w:w']} w \\
&= \sum_{w' \in S_{K'}} \sum_{w|w'} \log|u'|_w w \\
&= \sum_{w \in S_K} \log|u'|_w . w \\
&= \lambda_{K,S_K}(u').
\end{aligned}$$

It follows by tensoring that the diagram

$$\begin{tikzcd}
\mathbb{C}U_{K,S_K} \arrow[r, "\lambda_{K,S_K}", "\cong"'] & \mathbb{C}X_{K,S_K} \\
\mathbb{C}U_{K',S_{K'}} \arrow[u, hook] \arrow[r, "\cong", "\lambda_{K',S_{K'}}"'] & \mathbb{C}X_{K',S_{K'}} \arrow[u, "j_{K/K',S}"']
\end{tikzcd}$$

is also commutative.

6.2.3 Properties of the Stark Regulator

Let K/k be a finite Galois extension of number fields with Galois group G. Let S be a finite subset of M_k containing M_k^∞ and let S_K be the finite subset of M_K consisting of the places that lies above the ones in S.

Definition 26. Let V be a complex representation of G with character χ. For any left $\mathbb{C}[G]$-endomorphism θ of $\mathbb{C}X_{K,S}$ we denote by θ_V the $\mathbb{C}$-linear endomorphism $\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \theta)$ of $\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K})$ and we define

$$\delta_S(\chi, \theta, K/k) = \det(\theta_V)$$

which is independent of the realization V of χ by naturality of the Hom functor.

Remark 28. With the notations of the previous section, we have

$$R_S(\chi, f, K/k) = \delta_S(\chi, \lambda_{K,S} \circ f, K/k).$$

Proposition 58. *The function δ_S satisfies the following properties:*

(i) If χ and χ' are two characters of G then we have

$$\delta_S(\chi + \chi', \theta, K/k) = \delta_S(\chi, \theta, K/k)\delta_S(\chi', \theta, K/k).$$

(ii) If H is a subgroup of G with character χ then we have

$$\delta_S(\mathrm{Ind}_H^G \chi, \theta, K/k) = \delta_{S_{K^H}}(\chi, \theta, K/K^H).$$

(iii) Let $K/K'/k$ is a tower of finite Galois extensions of number fields. Let $G = \mathrm{Gal}(K/k)$, $H = \mathrm{Gal}(K/K')$ and let χ be a character of G/H. Then we have

$$\delta_S(\mathrm{Infl}_H^G \chi, \theta, K/k) = \delta_S(\chi, \theta', K'/k)$$

where $\theta' = j_{K/K',S}^{-1} \circ \theta|_{\mathbb{C}X_{K,S_K}^H} \circ j_{K/K',S}$.

(iv) If θ and θ' are two left $\mathbb{C}[G]$-endomorphisms of $\mathbb{C}X_{K,S_K}$, then

$$\delta_S(\chi, \theta \circ \theta', K/k) = \delta_S(\chi, \theta, K/k)\delta_S(\chi, \theta', K/k).$$

Proof. Proof of (i): Let V and V' be representations of G with respective characters χ and χ'. Then $V \oplus V'$ is a representation of G with character $\chi + \chi'$ and we have an isomorphism of $\mathbb{C}$-vector spaces between $\mathrm{Hom}_{\mathbb{C}[G]}((V \oplus V')^\vee, \mathbb{C}X_{K,S_K})$ and

$$\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K}) \oplus \mathrm{Hom}_{\mathbb{C}[G]}((V')^\vee, \mathbb{C}X_{K,S_K})$$

so that $\det(\theta_{V \oplus V'}) = \det(\theta_V \oplus \theta_{V'})$ and the result follows.

Proof of (ii): Let W be a representation of H with character χ. We have

$$(\mathrm{Ind}_H^G W)^\vee = \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, \mathbb{C}).$$

By Theorem 3.10.1, Proposition 21 and Corollary 12 we have left $\mathbb{C}[G]$-module isomorphisms

$$(\mathrm{Ind}_H^G W)^\vee \cong \mathrm{Hom}_{\mathbb{C}[H]}(W, \mathbb{C}[G]^\vee) \cong W^\vee \otimes_{\mathbb{C}[H]} \mathbb{C}[G]^\vee.$$

By Proposition 21, the character of $\mathbb{C}[G]^\vee$ is $\bar{r}_G$ where r_G denotes the regular character of G. By Corollary 16 this character takes values in $\mathbb{Q}$ so that $\bar{r}_G = r_G$ and therefore, as left $\mathbb{C}[G]$-modules, we have $\mathbb{C}[G] \cong \mathbb{C}[G]^\vee$. Finally we have an isomorphism of left $\mathbb{C}[G]$-modules

$$(\mathrm{Ind}_H^G W)^\vee \cong \mathbb{C}[G]^\vee \otimes_{\mathbb{C}[H]} W^\vee \cong \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W^\vee = \mathrm{Ind}_H^G (W^\vee).$$

By Proposition 19 we have a natural isomorphism of $\mathbb{C}$-vector spaces

$$\mathrm{Hom}_{\mathbb{C}[G]}((\mathrm{Ind}_H^G W)^\vee, \mathbb{C}X_{K,S_K}) \cong \mathrm{Hom}_{\mathbb{C}[H]}(W^\vee, \mathbb{C}X_{K,S_K}).$$

By naturality we get the desired result.

Proof of (iii): Let V be a representation of G/H with character χ and let M be a representation of G with character ϕ. We claim that there is a natural isomorphism of $\mathbb{C}$-vector spaces

$$\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), M) \cong \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, M^H).$$

Let $N_H = \frac{1}{|H|}\sum_{h\in H} h \in \mathbb{C}[H]$. By proposition 19 N_H belongs to the center of $\mathbb{C}[G]$ and acts on M as the projection onto M^H. Moreover, N_H commutes with the action of G/H on M^H. Thus we obtain a well-defined homomorphism of $\mathbb{C}$-vector spaces

$$(N_H)_V : \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), M) \longrightarrow \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, M^H)$$

defined by $f \longmapsto N_H \circ f$. This map is easily seen to be surjective. By Corollary 11 and Proposition 21 we have

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), M) = \left\langle \mathrm{Infl}_H^G \bar{\chi}, \phi \right\rangle_G$$

and

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, M^H) = \left\langle \bar{\chi}, \phi^H \right\rangle_{G/H}.$$

Denoting by $[g]$ the class of an element g in G/H, we compute that

$$\begin{aligned}\left\langle \mathrm{Infl}_H^G \bar{\chi}, \phi \right\rangle_G &= \frac{1}{|G|}\sum_{g\in G} \mathrm{Infl}_H^G \bar{\chi}(g)\bar{\phi}(g) = \frac{1}{|G||H|}\sum_{g\in G}\sum_{h\in H} \mathrm{Infl}_H^G \bar{\chi}(gh)\bar{\phi}(g) \\ &= \frac{1}{|G||H|}\sum_{g\in G}\sum_{h\in H} \mathrm{Infl}_H^G \bar{\chi}(g)\bar{\phi}(gh) = \frac{1}{|G|}\sum_{g\in G} \bar{\chi}([g])\bar{\phi}^H([g]) \\ &= \frac{|H|}{|G|}\sum_{\sigma\in G/H} \bar{\chi}(\sigma)\bar{\phi}^H(\sigma) = \left\langle \chi, \phi^H \right\rangle_{G/H}.\end{aligned}$$

Thus the dimensions are equal and $(N_H)_V$ is an isomorphism of $\mathbb{C}$-vector spaces.

We now prove naturality. Let $f : M \longrightarrow N$ be a left $\mathbb{C}[G]$-module homomorphism. We claim that the following diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), M) \arrow[r, "(N_H)_V"] \arrow[d, "\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), f)"'] & \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, M^H) \arrow[d, "\mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, f|_{M^H})"] \\
\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), N) \arrow[r, "(N_H)_V"'] & \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, N^H)
\end{tikzcd}$$

commutes. In fact, let $\omega \in \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), M)$. Both paths send ω to the map $V^\vee \longrightarrow N^H$ given by

$$g \mapsto \frac{1}{|H|} \sum_{h \in H} h \cdot (f \circ \omega(g)).$$

Applying this to the present situation we have a natural isomorphism of $\mathbb{C}$-vector spaces

$$\mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Infl}_H^G(V^\vee), \mathbb{C}X_{K,S_K}) \cong \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, \mathbb{C}X_{K,S_K}^H).$$

The naturality property applied with $M = N = \mathbb{C}X_{K,S}$ and $f = \theta$ implies that $\delta_S(\mathrm{Infl}_H^G \chi, \theta, K/k) = \det((\theta|_{\mathbb{C}X_{K,S_K}^H})_V)$. Meanwhile, by definition of θ', the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, \mathbb{C}X_{K',S_{K'}}) \arrow[r, "\theta'_V"] & \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, \mathbb{C}X_{K',S_{K'}}) \\
\mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, \mathbb{C}X_{K,S_K}^H) \arrow[r, "(\theta|_{\mathbb{C}X_{K,S_K}^H})_V"'] \arrow[u, "\mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, j_{K/K',S}^{-1})", "\cong"'] & \mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, \mathbb{C}X_{K,S_K}^H). \arrow[u, "\cong", "\mathrm{Hom}_{\mathbb{C}[G/H]}(V^\vee, j_{K/K',S}^{-1})"']
\end{tikzcd}$$

Hence $\det((\theta|_{\mathbb{C}X_{K,S}^H})_V) = \delta_S(\chi, \theta', K'/k)$ and we conclude that

$$\delta_S(\mathrm{Infl}_H^G \chi, \theta, K/k) = \delta_S(\chi, \theta', K'/k).$$

Proof of (iv): By functoriality, $(\theta \circ \theta')_V = \theta_V \circ \theta'_V$ and the result follows. □

Let $\alpha \in \mathrm{Aut}(\mathbb{C})$. Then α must fix $\mathbb{Q}$ and we see that $\mathrm{Aut}(\mathbb{C}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$. Note that $\mathbb{C}$ can be viewed as a $\mathbb{C}$-vector space with scalar multiplication via α. We specify this by using the notation $\mathbb{C}^\alpha$. If W is any finite-dimensional complex vector space, we denote by W^α the tensor product $\mathbb{C}^\alpha \otimes_{\mathbb{C}} W$. In other words, W^α is a $\mathbb{C}$-vector space with the same elements as W but where scalar multiplication goes through α. If θ is an endomorphism of W, then we denote by θ^α the endomorphism $1 \otimes_\alpha \theta$ of W^α.

Proposition 59. *Let V be a representation of G with character χ. If $\alpha \in \mathrm{Aut}(\mathbb{C})$, then V^α is a representation of G with character $\chi^\alpha = \alpha \circ \chi$.*

Proof. In fact, let $v_1, \ldots, v_n$ be a basis of V as a $\mathbb{C}$-vector space. Let ρ be the homomorphism $G \longrightarrow \mathrm{GL}(V)$ associated to the representation V and denote by $(a_{ij}(\sigma))$ the matrix of $\rho(\sigma)$ with respect to this basis for $\sigma \in G$. By definition, we have

$$\rho(\sigma)(\sum_{i=1}^n \lambda_i v_i) = \sum_{i,j} a_{ij}(\sigma)\lambda_j v_i.$$

A basis of V^α is given by $1 \otimes v_1, \ldots, 1 \otimes v_n$ and we denote by $(a'_{ij}(s))$ the matrix of the automorphism $\rho(\sigma)^\alpha$ of V^α corresponding to this basis. We have

$$\sum_{j=1}^n a'_{ji}(\sigma)(1 \otimes v_j) = \rho(\sigma)^\alpha(1 \otimes v_i) = 1 \otimes \rho(\sigma)(v_i) = 1 \otimes \left(\sum_{j=1}^n a_{ji}(\sigma) v_j\right)$$

$$= \sum_{j=1}^n (\alpha(a_{ji}(\sigma))) \otimes v_j = \sum_{j=1}^n \alpha(a_{ji}(\sigma))(1 \otimes v_j).$$

Thus $a'_{ij}(\sigma) = \alpha \circ a_{ij}(\sigma)$ for all $\sigma \in G$ and all i, j. In particular, the character of V^α is $\alpha \circ \chi$ and we have $\det(\rho(\sigma)^\alpha) = \alpha(\det(\rho(\sigma)))$. $\square$

Proposition 60. *Let $\alpha \in \mathrm{Aut}(\mathbb{C})$ and let V be a representation of G with character χ. We have*

$$\delta_S(\chi, \theta, K/k)^\alpha = \delta_S(\chi^\alpha, \theta^\alpha, K/k).$$

Proof. By Proposition 59, the representation V^α has character χ^α. We have the identification

$$\mathrm{Hom}_{\mathbb{C}[G]}((V^\alpha)^\vee, (\mathbb{C}X_{K,S_K})^\alpha) = \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S_K})^\alpha.$$

Therefore $(\theta^\alpha)_{V^\alpha} = 1 \otimes_\alpha \theta_V$. Taking determinants we get $\det((\theta^\alpha)_{V^\alpha}) = \det(\theta_V)^\alpha$ as desired. $\square$

Corollary 31. *The Stark regulator satisfies the following properties:*

(i) $R_S(\chi + \chi', f, K/k) = R_S(\chi, f, K/k) R_S(\chi', f, K/k)$.

(ii) $R_S(\mathrm{Ind}_H^G \chi, f, K/k) = R_{S_{K^H}}(\chi, f, K/K^H)$.

(iii) Let H be a normal subgroup of G and write $K' = K^H$. Let χ be a character of G/H. Let f' be a left $\mathbb{Q}[G/H]$-isomorphism $\mathbb{Q}X_{K',S_{K'}} \longrightarrow \mathbb{Q}U_{K',S_{K'}}$ and suppose that there exists a $\mathbb{Q}[G]$-isomorphism

$$f : \mathbb{Q}X_{K,S_K} \longrightarrow \mathbb{Q}U_{K,S_K}$$

making the following diagram commute:

$$\begin{tikzcd}
\mathbb{Q}X_{K,S_K} \arrow[r, "f"] & \mathbb{Q}U_{K,S_K} \\
\mathbb{Q}X_{K',S_{K'}} \arrow[u, "j_{K/K',S}"] \arrow[r, "f'"'] & \mathbb{Q}U_{K',S_{K'}} \arrow[u, hook]
\end{tikzcd}$$

Then $R_S(\mathrm{Infl}_H^G \chi, f, K/k) = R_S(\chi, f', K'/k)$.

Proof. Properties (i) and (ii) are direct consequences of Proposition 58 and Remark 28. We now prove the third property. By tensoring and using the commutative diagram in the end of the previous section we get a commutative diagram:

$$\begin{tikzcd}
\mathbb{C}X_{K,S_K} \arrow[r, "f", "\cong"'] & \mathbb{C}U_{K,S_K} \arrow[r, "\lambda_{K,S_K}", "\cong"'] & \mathbb{C}X_{K,S_K} \\
\mathbb{C}X_{K',S_{K'}} \arrow[u, "j_{K/K',S}"] \arrow[r, "\cong", "f'"'] & \mathbb{C}U_{K',S_{K'}} \arrow[u, hook] \arrow[r, "\cong", "\lambda_{K',S_{K'}}"'] & \mathbb{C}X_{K',S_{K'}} \arrow[u, "j_{K/K',S}"']
\end{tikzcd}$$

which by restriction gives a commutative diagram

$$\begin{tikzcd}
\mathbb{C}X^H_{K,S_K} \arrow[r, "\lambda_{K,S_K} \circ f", "\cong"'] & \mathbb{C}X^H_{K,S_K} \\
\mathbb{C}X_{K',S_{K'}} \arrow[u, "j_{K/K',S}", "\cong"'] \arrow[r, "\cong", "\lambda_{K',S_{K'}} \circ f'"'] & \mathbb{C}X_{K',S_{K'}} \arrow[u, "\cong", "j_{K/K',S}"']
\end{tikzcd}$$

so that

$$\lambda_{K',S_{K'}} \circ f' = j_{K/K',S}^{-1} \circ (\lambda_{K,S_K} \circ f)|_{\mathbb{C}X_{K,S}^H} \circ j_{K/K',S}$$

and by Proposition 58 (*iii*) and Remark 28 we obtain the desired result. □

Remark 29. Given a left $\mathbb{Q}[G/H]$-isomorphism $f' : \mathbb{Q}X_{K',S_{K'}} \longrightarrow \mathbb{Q}U_{K',S_{K'}}$ we can always find a left $\mathbb{Q}[G]$-isomorphism $f : \mathbb{Q}X_{K,S_K} \longrightarrow \mathbb{Q}U_{K,S_K}$ making the diagram in Proposition 31 (*iii*) commute. In fact, by semisimplicity of $\mathbb{Q}[G]$ (cf. Proposition 16), there exists a left $\mathbb{Q}[G]$-submodule M of $\mathbb{Q}X_{K,S_K}$ such that

$$\mathbb{Q}X_{K,S_K} = \mathbb{Q}X_{K,S_K}^H \oplus M \cong \mathbb{Q}X_{K',S_{K'}} \oplus M$$

as $\mathbb{Q}[G]$-modules. Also by semisimplicity, there exists a left $\mathbb{Q}[G]$-submodule N of $\mathbb{Q}U_{K,S_K}$ such that $\mathbb{Q}U_{K,S_K} = \mathbb{Q}U_{K',S_{K'}} \oplus N$. Necessarily M and N are isomorphic as left $\mathbb{Q}[G]$-modules. Choose a $\mathbb{Q}[G]$-isomorphism $h : M \longrightarrow N$ and take f to be $(f' \circ j_{K/K',S}^{-1}) \oplus h$.

6.3 The Main Conjecture

6.3.1 Statement

We give the statement of Stark's main conjecture as formulated by Tate in [Ta1]. Let K/k be a finite Galois extension of number fields with Galois group G. Let S be a finite subset of M_k containing M_k^∞. Let S_K be the finite subset of M_K consisting of the places that lie above the ones in S. Let

$$f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$$

be a left $\mathbb{C}[G]$-module isomorphism that is defined over $\mathbb{Q}$. Let χ be a character of G and denote by $c_S(\chi, K/k)$ the leading coefficient of the Taylor expansion of the Artin L-function $L(s,\chi,K/k)$ around $s = 0$. We define

$$A_S(\chi, f, K/k) = \frac{R_S(\chi, f, K/k)}{c_S(\chi, K/k)} \in \mathbb{C}.$$

Conjecture 3 (Stark)**.** *With the above notations, for all $\alpha \in \mathrm{Aut}(\mathbb{C})$, we have*

$$A_S(\chi, f, K/k)^\alpha = A_S(\chi^\alpha, f, K/k).$$

Remark 30. By Proposition 18, $\mathbb{Q}(\chi)$ is a finite abelian extension of $\mathbb{Q}$. Let $\alpha \in \mathrm{Aut}_{\mathbb{Q}(\chi)}(\mathbb{C})$. Then $\chi^\alpha = \chi$ and therefore Conjecture 3 implies that

$$A_S(\chi, f, K/k)^\alpha = A_S(\chi, f, K/k).$$

This implies that $A_S(\chi, f, K/k) \in \mathbb{Q}(\chi)$. Also, every $\alpha \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ is the restriction of some element of $\mathrm{Aut}(\mathbb{C})$ so that $A_S(\chi, f, K/k)^\alpha = A_S(\chi^\alpha, f, K/k)$.

Conversely, if $A_S(\chi, f, K/k) \in \mathbb{Q}(\chi)$ and $A_S(\chi, f, K/k)^\alpha = A_S(\chi^\alpha, f, K/k)$ for all $\alpha \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$, then Conjecture 3 holds true.

From this remark it follows that Conjecture 3 is equivalent to the following:

Conjecture 4. *With the above notations, we have*

$$\begin{cases} A_S(\chi, f, K/k) \in \mathbb{Q}(\chi), \\ A_S(\chi, f, K/k)^\alpha = A_S(\chi^\alpha, f, K/k), \quad \text{for all } \alpha \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}). \end{cases}$$

Remark 31. Conjecture 4 says that the leading coefficient of the Taylor expansion of $L(s,\chi,K/k)$ is equal to $A_S(\chi,f,K/k)^{-1}R_S(\chi,f,K/k)$ which is the product of am algebraic number with the determinant of a matrix of size the order of $L(s,\chi,K/k)$ at $s=0$. In this sense, the conjecture generalizes the class number formula at $s=0$.

6.3.2 Independence of the Choice of f

Another equivalent statement of Conjecture 3 was formulated by Deligne. Instead of requiring f to be defined over $\mathbb{Q}$, we consider any field E of characteristic zero which can be embedded in $\mathbb{C}$. Let V be a representation of G over E with character χ. Let $f : EX_{K,S_K} \longrightarrow EU_{K,S_K}$ be a left $E[G]$-module homomorphism. Any embedding $\alpha : E \hookrightarrow \mathbb{C}$ fixes $\mathbb{Q}$ and gives $\mathbb{C}$ the structure of a vector space over E. We use the notation $\mathbb{C}^\alpha$ to denote $\mathbb{C}$ with its structure of E-vector space coming from α. Note that for any $\mathbb{Z}$-module A, we have

$$\mathbb{C}^\alpha \otimes_E EA = \mathbb{C}^\alpha \otimes_E (E \otimes_{\mathbb{Z}} A) \cong \mathbb{C}A.$$

Consider the complex character χ^α and its complex realization $V^\alpha := \mathbb{C}^\alpha \otimes_E V$. To the character χ^α corresponds the Artin L-function $L_S(s,\chi^\alpha,K/k)$. Define f^α to be the left $\mathbb{C}[G]$-module homomorphism

$$1 \otimes_\alpha f : \mathbb{C}^\alpha \otimes_E EX_{K,S_K} \longrightarrow \mathbb{C}^\alpha \otimes_E EU_{K,S_K}.$$

Explicitly we have

$$f^\alpha(s \otimes (e \otimes x)) = s \otimes f(e \otimes x) = s \otimes ef(1 \otimes x) = s\alpha(e) \otimes f(1 \otimes x).$$

Composing with λ_{K,S_K} gives a left $\mathbb{C}[G]$-homomorphism

$$\lambda_{K,S_K} \circ f^\alpha : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}X_{K,S_K}$$

which induces a $\mathbb{C}$-endomorphism $(\lambda_{K,S} \circ f^\alpha)_{V^\alpha}$ of $\mathrm{Hom}_{\mathbb{C}[G]}((V^\alpha)^\vee, \mathbb{C}X_{K,S_K})$. Define

$$R_S(\chi^\alpha, f^\alpha, K/k) = \det((\lambda_{K,S} \circ f^\alpha)_{V^\alpha}).$$

Conjecture 5 (Deligne)**.** *With the above notations, there exists an element $A_S(\chi,f,K/k) \in E$ such that for all $\alpha : E \hookrightarrow \mathbb{C}$ we have*

$$R_S(\chi^\alpha, f^\alpha, K/k) = A(\chi,f,K/k)^\alpha c_S(\chi^\alpha, K/k).$$

Proposition 61. *Conjecture 5 implies Conjecture 3.*

Proof. Consider the case where $E=\mathbb{C}$ and take $f_{\mathbb{Q}} : \mathbb{Q}X_{K,S_K} \longrightarrow \mathbb{Q}U_{K,S_K}$ to be a left $\mathbb{Q}[G]$-isomorphism. Tensor it to get a left $\mathbb{C}[G]$-module isomorphism $f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$. Let α be any $\mathbb{C}$-automorphism. Now,

$$f^\alpha = 1 \otimes_\alpha f = 1 \otimes_\alpha (1 \otimes_{\mathbb{Q}} f_{\mathbb{Q}}) = 1 \otimes_{\mathbb{Q},\alpha|_{\mathbb{Q}}} f_{\mathbb{Q}}.$$

But the restriction of α to $\mathbb{Q}$ is the identity so the latter is simply f. Thus $f^\alpha = f$ and the statement of Conjecture 5 in this case is exactly the statement of Conjecture 3. □

Remark 32. In the course of the proof we showed that if $f : \mathbb{C}X_{K,S} \longrightarrow \mathbb{C}U_{K,S}$ is defined over $\mathbb{Q}$, then $f^\alpha = f$ for all $\alpha \in \mathrm{Aut}(\mathbb{C})$.

Proposition 62. *Let $E = \mathbb{C}$ and suppose that Conjecture 5 is true for one particular left $\mathbb{C}[G]$-isomorphism $f_0 : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$. Then it is true for all left $\mathbb{C}[G]$-homomorphisms $f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$. In particular, Conjecture 3 implies Conjecture 5 in the case $E = \mathbb{C}$.*

Proof. There exists $A_S(\chi, f_0, K/k)$ in $\mathbb{C}$ such that for all $\alpha \in \mathrm{Aut}(\mathbb{C})$ we have $R_S(\chi^\alpha, f_0^\alpha, K/k) = A_S(\chi, f_0, K/k)^\alpha c_S(\chi^\alpha, K/k)$. Let $f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$ be a left $\mathbb{C}[G]$-module homomorphism and define

$$A_S(\chi, f, K/k) := A_S(\chi, f_0, K/k)\delta_S(\chi, \theta, K/k) \in \mathbb{C}$$

where $\theta = f_0^{-1} \circ f$. By Proposition 58 (iv) and Proposition 60 we have

$$\begin{aligned} A_S(\chi, f, K/k)^\alpha &= A_S(\chi, f_0, K/k)^\alpha \delta_S(\chi, \theta, K/k)^\alpha \\ &= \frac{R_S(\chi^\alpha, f_0^\alpha, K/k)}{c_S(\chi^\alpha, K/k)} \delta_S(\chi^\alpha, \theta^\alpha, K/k) \\ &= \frac{\delta_S(\chi^\alpha, \lambda_{K,S_K} \circ f_0^\alpha), K/k}{c_S(\chi^\alpha, K/k)} \delta_S(\chi^\alpha, (f_0^{-1} \circ f)^\alpha, K/k) \\ &= \frac{\delta_S(\chi^\alpha, \lambda_{K,S_K} \circ f^\alpha, K/k)}{c_S(\chi^\alpha, K/k)} \\ &= \frac{R_S(\chi^\alpha, f^\alpha, K/k)}{c_S(\chi^\alpha, K/k)}. \end{aligned}$$

Thus Conjecture 5 is true for f.

Suppose that Conjecture 3 is true for some left $\mathbb{C}[G]$-isomorphism

$$g : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$$

defined over $\mathbb{Q}$. Since it is defined over $\mathbb{Q}$, by Remark 32, $g^\alpha = g$ for all $\alpha \in \mathrm{Aut}(\mathbb{C})$ and therefore Conjecture 5 is true for g and therefore in general in the case $E = \mathbb{C}$. □

Corollary 32. *Conjecture 3 is equivalent to Conjecture 5 with $E = \mathbb{C}$.*

Corollary 33. *The truth of Conjecture 3 is independent of the choice of the left $\mathbb{C}[G]$-module isomorphism $f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$ defined over $\mathbb{Q}$.*

Remark 33. It is true that Conjecture 3 is equivalent to Conjecture 5 for any E. We refer the reader to Chapter I, § 6 of [Ta1] for the proof of this.

6.3.3 Independence of the Choice of S

Having proved that the truth of Stark's conjecture does not depend on the choice of a left $\mathbb{C}[G]$-module isomorphism $f : \mathbb{C}X_{K,S_K} \longrightarrow \mathbb{C}U_{K,S_K}$ defined over $\mathbb{Q}$, we now prove that it neither depends on the choice of the set S. First we give some properties of $A_S(\chi, f, K/k)$.

Proposition 63. *The following properties are true:*

(i) If χ and χ' are two characters of G then we have

$$A_S(\chi + \chi', f, K/k) = A_S(\chi, f, K/k)A_S(\chi', f, K/k).$$

(ii) If H is a subgroup of G with character χ then we have

$$A_S(\mathrm{Ind}_H^G\chi, f, K/k) = A_{S_{K^H}}(\chi, f, K/K^H).$$

(iii) Let H be a normal subgroup of G and write $K' = K^H$. Let χ be a character of G/H. Let f' be a left $\mathbb{Q}[G/H]$-isomorphism $\mathbb{Q}X_{K',S_{K'}} \longrightarrow \mathbb{Q}U_{K',S_{K'}}$ and by Remark 29 let $f : \mathbb{Q}X_{K,S_K} \longrightarrow \mathbb{Q}U_{K,S_K}$ be a left $\mathbb{Q}[G]$-isomorphism making the following diagram commute:

$$\begin{tikzcd}
\mathbb{Q}X_{K,S_K} \arrow[r, "f"] & \mathbb{Q}U_{K,S_K} \\
\mathbb{Q}X_{K',S_{K'}} \arrow[u, "j_{K/K',S}"] \arrow[r, "f'"'] & \mathbb{Q}U_{K',S_{K'}}. \arrow[u, hook]
\end{tikzcd}$$

Then we have $A_S(\mathrm{Infl}_H^G\chi, f, K/k) = A_S(\chi, f', K'/k)$.

Proof. By Proposition 47 we have

$$L_S(s, \chi + \chi', K/k) = L_S(s, \chi, K/k)L_S(s, \chi', K/k)$$

so that $c_S(\chi + \chi', K/k) = c_S(\chi, K/k)c_S(\chi', K/k)$ and the first property follows from Corollary 31 (i).

By Proposition 49 we have $L_S(s, \mathrm{Ind}_H^G\chi K/k) = L_{S_{K^H}}(s, \chi, K/K^H)$ so that $c_S(\mathrm{Ind}_H^G\chi, K/k) = c_S(\chi, K/K^H)$ and the second property therefore follows from Corollary 31 (ii).

By Proposition 48 we have $L_S(s, \mathrm{Infl}_H^G\chi, K/k) = L_S(s, \chi, K'/k)$ so that $c_S(\mathrm{Infl}_H^G\chi, K/k) = c_S(\chi, K'/k)$ and the third property therefore follows from Corollary 31 (iii). □

Proposition 64. *As a consequence we have:*

(i) If Conjecture 3 holds for all finite Galois extensions $K/\mathbb{Q}$, then it holds in general.

(ii) If Conjecture 3 holds for all 1-dimensional characters of all finite Galois extensions K/k, then it holds in general.

Proof. Let K/k be a finite Galois extension of number fields with Galois group G and denote by K^{Gal} the normal closure of K over $\mathbb{Q}$. Let χ be a character of G. We have an isomorphism of groups $G \cong \mathrm{Gal}(K^{\mathrm{Gal}}/k)/\mathrm{Gal}(K^{\mathrm{Gal}}/K)$ and therefore by Proposition 63 (iii) and (ii) we have

$$\begin{aligned} A_S(\chi, f, K/k) &= A_S(\mathrm{Infl}_{\mathrm{Gal}(K^{\mathrm{Gal}}/K)}^{\mathrm{Gal}(K^{\mathrm{Gal}}/k)}\chi, f', K^{\mathrm{Gal}}/k) \\ &= A_{S|_{\mathbb{Q}}}(\mathrm{Ind}_{\mathrm{Gal}(K^{\mathrm{Gal}}/k)}^{\mathrm{Gal}(K^{\mathrm{Gal}}/\mathbb{Q})}\mathrm{Infl}_{\mathrm{Gal}(K^{\mathrm{Gal}}/K)}^{\mathrm{Gal}(K^{\mathrm{Gal}}/k)}\chi, f', K^{\mathrm{Gal}}/\mathbb{Q}) \end{aligned}$$

for a suitable f'. This proves (i).

By Theorem 3.11.1 there exist integers n_i and subgroups H_i with characters θ_i of dimension 1 such that

$$\chi = \sum_i n_i \mathrm{Ind}_{H_i}^G \theta_i.$$

By Proposition 63 we have

$$A_S(\chi, f, K/k) = \prod_i A_S(\mathrm{Ind}_{H_i}^G \theta_i, f, K/k)^{n_i} = \prod_i A_{S_{K^{H_i}}}(\theta_i, f, K/K^{H_i})^{n_i}.$$

Since $(\mathrm{Ind}_{H_i}^G \theta_i)^\alpha = \mathrm{Ind}_{H_i}^G \theta_i^\alpha$ for all $\alpha \in \mathrm{Aut}(\mathbb{C})$ the result follows. □

Proposition 65. *Conjecture 3 is independent of the choice of the set S.*

Proof. Let K/k be a finite Galois extension of number fields with Galois group G and let S be a finite set of places of k containing M_k^∞. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$ that is not contained in S and define $S' = S \cup \{\mathfrak{p}\}$. Let χ be a character of G and let V be a representation of G with character χ. By Proposition 64, we may suppose that χ is a 1-dimensional character. Since χ is 1-dimensional and therefore a homomorphism of groups, χ factors through its kernel. That is, there exists by universal property of the quotient, a unique homomorphism of groups $\chi' : G/\mathrm{ker}\chi \longrightarrow \mathbb{C}^*$ such that the diagram

$$\begin{tikzcd} G \arrow[r, "\chi"] \arrow[d, "q"] & \mathbb{C}^* \\ G/\mathrm{ker}(\chi) \arrow[ur, "\exists! \chi'"'] & \end{tikzcd}$$

commutes. In other words, $\chi = \mathrm{Infl}_{\mathrm{ker}(\chi)}^G \chi'$ and by Proposition 63 (iii) we can work with the character χ' instead of χ. We will therefore assume that χ is an injective 1-dimensional character.

For simplicity we shall drop the indices K and S in our usual notations and use $'$ to denote objects defined for S'. For example, we shall write $c'(\chi)$ instead of $c_{S'}(\chi, K/k)$ and U' instead of U_{K,S'_K}.

Let $f : \mathbb{Q}X \longrightarrow \mathbb{Q}U$ be a left $\mathbb{Q}[G]$-isomorphism. By semisimplicity of $\mathbb{Q}[G]$ we may view $\mathbb{Q}X$ and $\mathbb{Q}U$ as direct summands of $\mathbb{Q}X'$ and $\mathbb{Q}U'$ and extend f to a left $\mathbb{Q}[G]$-isomorphism $f' : \mathbb{Q}X' \longrightarrow \mathbb{Q}U'$. We define the quantity

$$\Theta(\chi) = \frac{A(\chi, f)}{A'(\chi, f')}.$$

It suffices to prove that $\Theta(\chi)^\alpha = \Theta(\chi^\alpha)$ for all $\alpha \in \mathrm{Aut}(\mathbb{C})$. In fact, if this is true, then

$$\frac{A(\chi, f)^\alpha}{A'(\chi, f')^\alpha} = \frac{A(\chi^\alpha, f)}{A'(\chi^\alpha, f')}$$

so that Conjecture 3 is true for S if and only if it is true for S'.

Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_K$ that lies above $\mathfrak{p}$. We consider two cases:

- $\chi(D_\mathfrak{P}) \neq 1$: In this case, by Corollary 30, we have $r'(\chi) = r(\chi)$. By Proposition 54 this implies that $\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X')$ and $\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X)$ have the same dimension as complex vector spaces. But since $\mathbb{C}X$ is a $\mathbb{C}[G]$-submodule of $\mathbb{C}X'$ we have an injective $\mathbb{C}$-linear map

$$\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X) \longrightarrow \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X')$$

which must in turn be an isomorphism of vector spaces. We have the following commutative diagram:

$$\begin{tikzcd}
\mathbb{C}X' \arrow[r, "f'"] & \mathbb{C}U' \arrow[r, "\lambda'"] & \mathbb{C}X' \\
\mathbb{C}X \arrow[u, hook] \arrow[r, "f"'] & \mathbb{C}U \arrow[u, hook] \arrow[r, "\lambda"'] & \mathbb{C}X. \arrow[u, hook]
\end{tikzcd}$$

In fact, the left square commutes by choice of f' and for the right square, if $u \in U$ then

$$\lambda'(u) = \sum_{w \in S'_K} \log |u|_w w = \lambda(u) + \sum_{w | \mathfrak{p}} \log |u|_w w = \lambda(u)$$

since $|u|_w = 1$ for all $w \notin S_K$. This induces a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X') \arrow[r, "(\lambda' \circ f')_V"] & \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X') \\
\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X) \arrow[u, "\cong"] \arrow[r, "(\lambda \circ f)_V"'] & \mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X). \arrow[u, "\cong"']
\end{tikzcd}$$

so that $R(\chi, f) = R'(\chi, f')$.

Moreover, if $\chi(I_{\mathfrak{P}})$ is non-trivial, then $L_{S'}(s, \chi) = L_S(s, \chi)$ and thus $c'(\chi) = c(\chi)$, whence $\Theta(\chi) = 1$. If $\alpha \in \mathrm{Aut}(\mathbb{C})$, then the character χ^α is also 1-dimensional with $\chi^\alpha(G_{\mathfrak{P}})$ and $\chi^\alpha(I_{\mathfrak{P}})$ non-trivial since α is injective. The same argument shows that $\Theta(\chi^\alpha) = 1$ so that $\Theta(\chi)^\alpha = 1 = \Theta(\chi^\alpha)$.

On the other hand, if $\chi(I_{\mathfrak{P}})$ is trivial, then by injectivity of χ we see that $I_{\mathfrak{P}}$ is trivial so that $\mathfrak{P}$ is unramified over $\mathfrak{p}$. In this case we have

$$L_{S'}(s, \chi) = (1 - \chi(\sigma_{\mathfrak{P}}) N(\mathfrak{p})^{-s}) L_S(s, \chi)$$

where $\sigma_{\mathfrak{P}}$ denotes the Frobenius element of $\mathfrak{P}$ which lies in $D_{\mathfrak{P}}$. Notice that $\chi(\sigma_{\mathfrak{P}}) \neq 1$ since otherwise we would have $\chi(D_{\mathfrak{P}}) = 1$ because the Frobenius element generates the decomposition group in the unramified case. Thus $c'(\chi) = (1 - \chi(\sigma_{\mathfrak{P}}))c(\chi)$ and as a result $\Theta(\chi) = (1 - \chi(\sigma_{\mathfrak{P}}))^{-1}$. Again, the character χ^α has the same properties, that is, $\chi^\alpha(I_{\mathfrak{P}})$ is trivial, so that the exact same argument shows that $\Theta(\chi^\alpha) = (1 - \chi^\alpha(\sigma_{\mathfrak{P}}))^{-1}$ which is equal to $\Theta(\chi)^\alpha$.

- $\chi(D_{\mathfrak{P}}) = 1$: By injectivity of χ this implies that $D_{\mathfrak{P}}$ is trivial. By Proposition 54 we then have

$$r'(\chi) = r(\chi) + \dim_{\mathbb{C}} V^{D_{\mathfrak{P}}} = r(\chi) + 1.$$

Moreover, $\mathfrak{p}$ splits completely in K/k meaning that each $\mathfrak{P}$ dividing $\mathfrak{p}$ is unramified and has residual degree equal to 1. We have

$$L_{S'}(s, \chi) = (1 - N(\mathfrak{p})^{-s}) L_S(s, \chi)$$

and

$$c'(\chi) = \lim_{s \to 0} s^{-(r(\chi)+1)} L_{S'}(s, \chi) = \lim_{s \to 0} \frac{1 - N(\mathfrak{p})^{-s}}{s} c(\chi) = \log N(\mathfrak{p}) c(\chi)$$

by the rule of l'Hospital.

Suppose that $\mathfrak{P}$ is of order m in $\mathrm{Cl}(\mathcal{O}_{K,S_K})$ and let π be a generator of the principal ideal $\mathfrak{P}^m\mathcal{O}_{K,S_K}$. Then $\sigma(\mathfrak{P})^m\mathcal{O}_{K,S_K}$ is generated by $\sigma(\pi)$. Since $\mathfrak{p}$ splits, S'_K contains $|G|$ more elements than S_K, namely the conjugates of $\mathfrak{P}$ and by Lemma 2 we know that the family $(\sigma(\pi))_{\sigma\in G}$ generates U'/U as a free $\mathbb{Z}$-module so that

$$U' \cong U \oplus \bigoplus_{\sigma\in G} \mathbb{Z}\sigma(\pi) \cong U \oplus \mathbb{Z}[G]\pi$$

as $\mathbb{Z}[G]$-modules. Tensoring with $\mathbb{Q}$ we get the following $\mathbb{Q}[G]$-isomorphism

$$\mathbb{Q}U' \cong \mathbb{Q}U \oplus \mathbb{Q}[G]\pi.$$

On the other hand, let w_0 denote any place in S_K, let

$$N_G = \frac{1}{|G|}\sum_{\sigma\in G}\sigma \in \mathbb{Q}[G]$$

and define $x = (\mathfrak{P} - N_G(w_0)) \in X'$.

Note that if $\tau \in G$, then $\tau(x) = (\tau(\mathfrak{P}) - N_G(w_0))$ since N_G is invariant under left multiplication by G. We now verify that $\mathbb{Q}[G]x$ is a $\mathbb{Q}[G]$-submodule of $\mathbb{Q}X'$. First of all we have the inclusion $\mathbb{Q}[G]x \subset \mathbb{Q}X'$. In fact, if $\alpha = (\sum_{\tau\in G}\lambda_\tau\tau)x$ is an element of $\mathbb{Q}[G]$ we see that

$$\alpha = \sum_{\tau\in G}\lambda_\tau(\tau(\mathfrak{P}) - N_G w_0).$$

Summing the coefficients we get

$$\sum_{\tau\in G}\lambda_\tau - \frac{1}{|G|}\sum_{\tau,\sigma\in G}\lambda_\tau = 0$$

and this proves that $\alpha \in \mathbb{Q}X'$. We notice also that if $\eta \in G$ then

$$\eta(\alpha) = \left(\sum_{\tau\in G}\lambda_{\tau\eta^{-1}}\tau\right)x \in \mathbb{Q}[G]x$$

so that $\mathbb{Q}[G]$ is stable under the action of G. We have proved that $\mathbb{Q}[G]x$ is a sub-$\mathbb{Q}[G]$-module of $\mathbb{Q}X'$.

But $\mathbb{Q}X$ is also a $\mathbb{Q}[G]$-submodule of $\mathbb{Q}X'$ and clearly $\mathbb{Q}X \cap \mathbb{Q}[G]x = \{0\}$. Moreover, since $\mathfrak{p}$ is split, we have

$$\dim_{\mathbb{Q}}\mathbb{Q}X' = |S'_K| - 1 = (|S_K| - 1) + |G| = \dim_{\mathbb{Q}}\mathbb{Q}X + \dim_{\mathbb{Q}}\mathbb{Q}[G]x.$$

We conclude that $\mathbb{Q}X' = \mathbb{Q}X \oplus \mathbb{Q}[G]x$.

By tensoring with $\mathbb{C}$ we get isomorphism of left $\mathbb{C}[G]$-modules:

$$\begin{cases}\mathbb{C}U' \cong \mathbb{C}U \oplus \mathbb{C}[G]\pi \\ \mathbb{C}X' \cong \mathbb{C}X \oplus \mathbb{C}[G]x.\end{cases}$$

Let $\omega : \mathbb{Q}[G]x \longrightarrow \mathbb{Q}[G]\pi$ be the left $\mathbb{Q}[G]$-module isomorphism that sends x to π. By Corollary 33, we may and will assume that $f' = f \oplus \omega$. We choose bases for $\mathbb{Q}X$ and $\mathbb{Q}U$ as $\mathbb{Q}$-vector spaces and complete them with $\{\sigma(x)\}_{\sigma\in G}$ and $\{\sigma(\pi)\}_{\sigma\in G}$ (where G has been given an ordering which is respected between these two bases) in order to form bases for $\mathbb{Q}X'$ and $\mathbb{Q}U'$ with respect to their respective decomposition. These also serve as bases for the complex vector spaces obtained by tensoring with $\mathbb{C}$. Let $M(f)$, $M(f')$, $M(\lambda)$ and $M(\lambda')$ denote the matrices of f, f', λ, λ' with respect to these bases. Then by the choice of our bases and by choice of f', we claim that

$$M(f') = \begin{pmatrix} M(f) & 0 \\ 0 & I_{|G|} \end{pmatrix} \quad \text{and} \quad M(\lambda') = \begin{pmatrix} M(\lambda) & * \\ 0 & \log|\pi|_{\mathfrak{P}} I_{|G|} \end{pmatrix}.$$

The expression for $M(f')$ is clear. The first $|S_K|-1$ columns of $M(\lambda')$ come from the fact that λ' and λ commute with the inclusions (see diagram earlier in this proof). The last $|G|$ columns of $M(\lambda')$ come from the computation:

$$\begin{aligned}\lambda'(\sigma(\pi)) &= \sum_{w\in S'_K} \log|\sigma(\pi)|_w w \\ &= \sum_{w\in S_K} \log|\sigma(\pi)|_w w + \sum_{\tau\in G} \log|\sigma(\pi)|_{\tau(\mathfrak{P})}\tau(\mathfrak{P}) \\ &= \lambda(\sigma(\pi)) + \sum_{\tau\in G} \log|\sigma(\pi)|_{\tau(\mathfrak{P})}\tau(x) + \sum_{\tau\in G} \log|\sigma(\pi)|_{\tau(\mathfrak{P})} N_G(w_0) \\ &\equiv \sum_{\tau\in G} \log|\sigma(\pi)|_{\tau(\mathfrak{P})}\tau(x) \mod \mathbb{C}X \\ &\equiv \log|\sigma(\pi)|_{\sigma(\mathfrak{P})}\sigma(x) \mod \mathbb{C}X \\ &\equiv \log|\pi|_{\mathfrak{P}}\sigma(x) \mod \mathbb{C}X\end{aligned}$$

where in the second last equality we use the fact that $|\sigma(\pi)|_{\tau(\mathfrak{P})} = 1$ for all $\tau \neq \sigma$ by definition of π and the last equality is the definition of the valuation $\sigma(\mathfrak{P})$.

As a consequence we have

$$M(\lambda'\circ f') = \begin{pmatrix} M(\lambda\circ f) & * \\ 0 & \log|\pi|_{\mathfrak{P}} I_{|G|} \end{pmatrix}.$$

With the above decomposition we have isomorphisms of $\mathbb{C}$-vector spaces

$$\operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X') \cong \operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X) \oplus \operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}[G]x).$$

Moreover, $\mathbb{C}[G]x$ is isomorphic as a left $\mathbb{C}[G]$-module to $\mathbb{C}[G]$. If r_G denotes the regular character of G, then by Lemma 5 we have

$$\dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}[G]x) = \langle \bar{\chi}, r_G\rangle_G = \langle r_G, \chi\rangle_G = \dim_{\mathbb{C}} V^\vee = 1.$$

Choose a basis of $\operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X)$ as a vector space over $\mathbb{C}$ and complete it with a non-zero element of $\operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}[G]x)$ to form a basis of $\operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X')$. With this choice of basis for $\operatorname{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X')$ we get

$$M((\lambda'\circ f')_V) = \begin{pmatrix} M((\lambda\circ f)_V) & * \\ 0 & \log|\pi|_{\mathfrak{P}} \end{pmatrix}.$$

We deduce that $R'(\chi, f') = \log|\pi|_{\mathfrak{P}} R(\chi, f)$.

We conclude that

$$\Theta(\chi) = \frac{\log N(\mathfrak{p})}{\log|\pi|_{\mathfrak{P}}} = \frac{\log N(\mathfrak{p})}{\log N(\mathfrak{P})^{-m}} = -\frac{1}{m}$$

since $\mathfrak{p}$ is split and thus $N(\mathfrak{p}) = N(\mathfrak{P})$. Hence $\Theta(\chi)$ is a rational number that is independent of χ so the proof is complete.

□

6.4 Special Cases

We prove Conjecture 3 in the the case where the Artin L-function has rank zero at $s = 0$. We then analyze the still unproven case of rank 1. In the abelian case, we present a refinement of Conjecture 3 and introduce the notion of Stark unit.

6.4.1 The Trivial Case

We prove that Stark's Conjecture 3 is true for the trivial character. Let K/k be a finite Galois extension of number fields with Galois group G. By Proposition 65 we may without loss of generality take $S = M_k^\infty$. We shall write X_K for X_{K,M_K^∞} and U_K for U_{K,M_K^∞}. We accordingly adjust other notations involving subscripts.

Let f be a left $\mathbb{Q}[G]$-module isomorphism $\mathbb{Q}X_K \longrightarrow \mathbb{Q}U_K$. We have $1_G = \mathrm{Infl}_{\{1\}}^G 1_{\{1\}}$. Thus, by Proposition 63, we have

$$A(f, 1_G, K/k) = A(f', 1_{\{1\}}, k/k)$$

where $f' : \mathbb{Q}X_k \longrightarrow \mathbb{Q}U_k$ is a left $\mathbb{Q}[G]$-module isomorphism such that f extends f'. We may therefore suppose that $K = k$.

Consider the isomorphism $\lambda_k : \mathbb{C}U_k \longrightarrow \mathbb{C}X_k$ of left $\mathbb{C}[G]$-modules. Let $u_1, \ldots, u_r$ be a system of fundamental units of U_k. Let v_0 be an archimedean place of k and choose as basis for $\mathbb{C}X_k$ the family $\{v - v_0 : v \in M_k^\infty \setminus \{v_0\}\}$. By Remark 3, the regulator of k is the absolute value of the determinant of λ_k with respect to these bases. We conclude that with choice of bases we have $\det(\lambda_k \circ f) = \pm R_k \det f$. Since

$$\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^\vee, \mathbb{C}X_k) \cong \mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}X_k \cong \mathbb{C}X_k$$

we see that $R(1_{\{1\}}, k/k) = \det(\lambda_k \circ f)$.

Meanwhile, $L(s, 1_{\{1\}}, k/k) = \zeta_k(s)$ by Proposition 46 and by Proposition 51 we have

$$c(1_{\{1\}}, k/k) = -\frac{h_k R_k}{\omega_k}.$$

It follows that

$$A(f, 1_{\{1\}}, k/k) = \pm\frac{\omega_k \det f}{h_k}.$$

This is a rational number since f is defined over $\mathbb{Q}$. Therefore Conjecture 3 is true for the trivial character.

6.4.2 The Rank 0 Case

We show how this case reduces to a result of Siegel on partial zeta-functions (Theorem 6.1.1) by using a refined version of Brauer's Theorem (Theorem 3.11.2).

With notations as in Conjecture 3, we assume in this section that

$$r_S(\chi, K/k) = 0.$$

By Proposition 54, we then have

$$\mathrm{Hom}_{\mathbb{C}[G]}(V^\vee, \mathbb{C}X_{K,S}) = 0$$

so that the Stark regulator equals 1 in this case for any choice of f. Also by Proposition 54, we see that $S \subset S'$ implies that $r_S(\chi) \leq r_{S'}(\chi)$. So if $r_S(\chi, K/k) = 0$, then $r_{M_k^\infty}(\chi, K/k) = 0$. By Proposition 65 we may therefore assume without loss of generality that $S = M_k^\infty$. For simplicity we will write $L(s,\chi)$ instead of $L_{M_k^\infty}(s,\chi,K/k)$ and $r(\chi)$ instead of $r_{M_k^\infty}(\chi, K/k)$. Since $r(\chi) = 0$, we know that $L(0,\chi)$ is non-zero. In our present case, Conjecture 3 can be restated as follows:

$$L(0,\chi)^\alpha = L(0,\chi^\alpha), \qquad \text{for all } \alpha \in \mathrm{Aut}(\mathbb{C}). \tag{6.4.0.1}$$

We start by simplifying the situation. Let (ρ, V) be a realization of χ. Quotienting out by $\ker(\rho)$ we get an injective homomorphism of group

$$\rho' : G/\ker(\rho) \longrightarrow \mathrm{GL}(V)$$

with character $\chi' : G/\ker(\rho) \longrightarrow \mathbb{C}$ such that $\chi = \mathrm{Infl}_{\ker(\rho)}^G \chi'$. By Proposition 48, we have $L(s,\chi,K/k) = L(s,\chi',K^{\ker(\rho)}/k)$. In particular $r(\chi') = 0$. Since $\chi^\alpha = \mathrm{Infl}_{\ker(\rho)}^G (\chi')^\alpha$, it suffices to prove (6.4.0.3) for χ'. So by replacing K with $K^{\ker(\rho)}$, we may assume that the representation is faithful, that is, ρ is an injective homomorphism.

Suppose that $\chi = \chi_1 + \chi_2$. By Proposition 47 we have $r(\chi) = r(\chi_1) + r(\chi_2)$ so that $r(\chi_1) = r(\chi_2) = 0$. As a consequence, $L(0,\chi_i) \neq 0$ and we have $L(0,\chi) = L(0,\chi_1)L(0,\chi_2)$ and it suffices to check (6.4.0.3) for each χ_i. We may therefore assume that χ is irreducible.

If χ is the trivial character on G, then we know from the previous section that Conjecture 3 is true. We therefore assume that χ is non-trivial.

After simplifications, we are in the case where χ is the character of a non-trivial irreducible and faithful representation (ρ, V) of G. We have $V^G = 0$ and by Proposition 54 we have

$$r(\chi) = \sum_{v \in M_k^\infty} \dim_{\mathbb{C}} V^{D_w} = 0$$

so that $V^{D_w} = 0$ for all w. This implies that $G_w = \{1, \tau_w\}$ for all w. Moreover, by considerations discussed in Section 5.4, the fact that D_w is of order 2 implies that k is totally real and K is totally complex. Since τ_w is of order 2 and $V^{D_w} = 0$, τ_w must act on V as $-\mathrm{id}_V$. The faithfulness of ρ then implies that $\tau_w = \tau$ for all w. Thus K is an imaginary quadratic extension of $K^{\langle\tau\rangle}$. As a consequence, τ is complex conjugation and this implies that $K^{\langle\tau\rangle}$ is totally real.

If σ is an element of G, then $D_{\sigma(w)} = \sigma D_w \sigma^{-1}$ and

$$\sigma\tau\sigma^{-1} = \sigma\tau_w\sigma^{-1} = \tau_{\sigma(w)} = \tau.$$

As a consequence, τ lies in the center $Z(G)$ of G. By Theorem 3.11.2, there exists a 1-dimensional character $\psi : Z(G) \longrightarrow \mathbb{C}^*$ such that $\chi|_{Z(G)} = \chi(1)\psi$ and

$$\chi = \sum_i n_i \mathrm{Ind}_{H_i}^G \chi_i$$

where the χ_i are 1-dimensional characters of subgroups H_i that contain $Z(G)$ such that $\chi_i|_{Z(G)} = \psi$ and $n_i \in \mathbb{Z}$.

For all i, we have

$$\chi_i(\tau) = \psi(\tau) = \frac{\chi(\tau)}{\chi(1)} = -1.$$

Let V_i be a representation of H_i over $\mathbb{C}$ with character χ_i. This is a 1-dimensional complex vector-space. Since K^{H_i} is a subfield of $K^{\langle\tau\rangle}$, it is totally real. Thus the decomposition groups D_w of K/K^{H_i} are generated by τ which acts as -1 so that $V_i^{D_w} = 0$ for all w. By Proposition 54 this implies that $r(\chi_i) = 0$. As a consequence, $L(0, \chi_i, K/K^{H_i}) \neq 0$ so that by Propositions 47 and 49, we have

$$L(0,\chi) = \prod_i L(0, \chi_i, K/K^{H_i})^{n_i}.$$

Since $(\mathrm{Ind}_H^G \chi)^\alpha = \mathrm{Ind}_H^G \chi^\alpha$, it suffices to prove (6.4.0.3) for each χ_i.

We are reduced to proving (6.4.0.3) in the case where χ is 1-dimensional and k is totally real. Using Proposition 48 we may replace K by $K^{\ker(\chi)}$ and assume that χ is injective and that K/k is abelian. The latter is because the kernel of χ contains the commutator subgroup $[G : G]$, whence $K^{\ker(\chi)}$ is a subfield of $K^{[G:G]}$. Since $K^{\ker(\chi)}$ is Galois over k, its Galois group is a quotient of the abelian group $G/[G : G]$ and is therefore abelian.

We are finally in the following situation: K/k is a finite abelian extension of number fields with Galois group G and χ is a 1-dimensional injective character of G. Let $\mathfrak{f}$ denote the conductor of K/k. Let S denote the finite subset of M_k consisting of M_k^∞ and all finite prime divisors of $\mathfrak{p}$. By Theorem 2.4.2, the finite places of S are exactly the ones that ramify in K/k. We have

$$L(s,\chi) = L_S(s,\chi) \prod_{\text{ramified } \mathfrak{p}} (1 - \chi_{\mathfrak{p}}((\mathfrak{p}, K/k))N(\mathfrak{p}) - s \mid V^{I_{\mathfrak{p}}})^{-1}.$$

But $V^{I_{\mathfrak{p}}} \neq \{0\}$ if and only if $\chi(I_{\mathfrak{p}}) = 1$. By injectivity of χ, this implies that $I_{\mathfrak{p}}$ is trivial which is to say that $\mathfrak{p}$ is unramified in K/k. We conclude that whenever $\mathfrak{p}$ is ramified we have $V^{I_{\mathfrak{p}}} = \{0\}$. As a consequence, we have

$$L(s,\chi) = L_S(s,\chi).$$

Let $\alpha \in \mathrm{Aut}(\mathbb{C})$. By Proposition 28 we then have

$$L(s,\chi) = \sum_{\sigma \in G} \chi(\sigma)\zeta_S(s,\sigma) \qquad \text{and} \qquad L(s,\chi^\alpha) = \sum_{\sigma \in G} \chi^\alpha(\sigma)\zeta_S(s,\sigma).$$

Thus (6.4.0.3) reduces to proving that $\zeta_S(0,\sigma)^\alpha = \zeta_S(0,\sigma)$ for all $\alpha \in \mathrm{Aut}(\mathbb{C})$. In other words, it reduces to proving that

$$\zeta_S(0,\sigma) \in \mathbb{Q}, \text{ for all } \sigma \in G.$$

This is Theorem 6.1.1 and thus Conjecture 3 is true in this case.

6.4.3 The Rank 1 Case

With notations as in Conjecture 3, we assume in this section that

$$r_S(\chi, K/k) = 1.$$

The conjecture remains unproven in this case but we will define Stark units and see how this leads to a refinement of the conjecture in the case where K/k is abelian.

The Non-Abelian Stark Conjecture

Let K/k be a finite Galois extension of number fields with Galois group G. Let S be a finite subset of M_k containing M_k^∞. Let S_K denote the finite subset of M_K consisting of the places of K that lie above the ones in S. Let χ be a character of G and suppose that the rank of the Artin L-function $L(s,\chi,K/k)$ at $s=0$ is 1, that is, $r_S(\chi,K/k)=1$. Let V be a representation of G over $\mathbb{C}$ with character χ. As usual, for simplicity we will drop the K/k in the notations. We begin with some simplifications and some observations.

Suppose that we can decompose χ as $\chi = \chi_1 + \chi_2$. By Proposition 47, we see that $r_S(\chi) = r_S(\chi_1) + r_S(\chi_2)$. Then one of these terms is 1, say $r_S(\chi_1)$, and the other one is 0. By Proposition 63 (i) we have

$$A_S(\chi, f) = A_S(\chi_1, f)A_S(\chi_2, f).$$

In order to prove Conjecture 3 it suffices therefore to prove it for χ_1 and χ_2. By the previous section, Conjecture 3 is true for χ_2. We therefore only need to be concerned with χ_1. We conclude that without loss of generality we may suppose that χ is irreducible.

By Proposition 54 we have $r_S(\chi) = \langle \chi, \chi_{X_K} \rangle_G$. By Proposition 53 we have $\chi_{X_K} \in R(G,\mathbb{Q})$. Consequently, for all $\alpha \in \mathrm{Aut}(\mathbb{C})$ we have $\chi_{X_K}^\alpha = \chi_{X_K}$. It follows that

$$r_S(\chi^\alpha) = \langle \chi^\alpha, \chi_{X_K} \rangle_G = \langle \chi, \chi_{X_K} \rangle_G^\alpha = r_S(\chi)^\alpha = 1.$$

Therefore we have $c_S(\chi^\alpha) = L'_S(0,\chi^\alpha)$ which is non-zero for all α.

Let $E = \mathbb{Q}(\chi)$. By Proposition 18 this is a finite abelian extension of $\mathbb{Q}$. We denote by Γ the Galois group of $E/\mathbb{Q}$. By Theorem 4.4.1, there exists an irreducible representation V' of G over E with character χ' such that $\chi' = m\chi$, where m is the Schur index of χ' over E. We have

$$\langle \chi', \chi_{X_K} \rangle_G = m r_S(\chi) = m > 0$$

so that V' appears as a subrepresentation of the representation EX_K of G over E. This implies that the left $\mathbb{C}[G]$-module $\mathbb{C}V' := \mathbb{C} \otimes_E V'$ appears as a subrepresentation of $\mathbb{C}X_K$. Since $\mathbb{C}V'$ has character $\chi' = m\chi$, it is isomorphic as a left $\mathbb{C}[G]$-module to $V^{\oplus m}$. As a consequence, the irreducible character χ appears at least m times in the decomposition of χ_X. Explicitly, we have

$$m \leq \langle \chi, \chi_{X_K} \rangle_G = r_S(\chi) = 1.$$

This implies that $m = 1$. In other words, χ is realizable as an irreducible character over E.

Define $\psi = \mathrm{tr}_{E/\mathbb{Q}} \circ \chi$. By Theorem 4.4.1, there exists an irreducible representation W of G over $\mathbb{Q}$ with character ψ. We have

$$\langle \psi, \chi_{X_K} \rangle_G = \sum_{\alpha \in \Gamma} r(\chi^\alpha) = |\Gamma| > 0$$

so that W appears as a subrepresentation of the representation $\mathbb{Q}X_K$ of G over $\mathbb{Q}$. This implies that the left $\mathbb{C}[G]$-module $\mathbb{C}W := \mathbb{C} \otimes_{\mathbb{Q}} W$ appears as a subrepresentation of the representation $\mathbb{C}X_K$. Since $\mathbb{C}W$ has character $\mathrm{tr}_{E/\mathbb{Q}}\chi$, it is isomorphic as a left $\mathbb{C}[G]$-module to $\bigoplus_{\alpha \in \Gamma} V^\alpha$. Thus, all the irreducible character χ^α appear at least once in the decomposition of χ_{X_K}. Moreover, these are all distinct since $\chi^\alpha = \chi^\beta$ implies that $\alpha\beta^{-1}$ fixes E and is therefore the identity. Since $\langle \chi^\alpha, \chi_{X_K} \rangle_G = 1$ they appear exactly once. We conclude that there is a unique subrepresentation of G over $\mathbb{Q}$ of $\mathbb{Q}X_K$ that is isomorphic to W. Denote this subrepresentation by X_W. Similarly, since $\mathbb{Q}X_K$ and $\mathbb{Q}U_K$ are (non-canonically) isomorphic as left $\mathbb{Q}[G]$-modules, there is a unique subrepresentation of G over $\mathbb{Q}$ of $\mathbb{Q}U_K$ that is isomorphic to W. We denote this subrepresentation by U_W.

Consider the element

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{\sigma \in G} \bar{\chi}(\sigma)\sigma \in \mathbb{C}[G].$$

By Proposition 24 it is a central element of $\mathbb{C}[G]$ which acts as the projection on the χ-component of the canonical decomposition of any representation of G over $\mathbb{C}$. In particular, it is a central idempotent element of $\mathbb{C}[G]$.

Definition 27. If a is a non-zero element of E, we define

$$\pi(a, \chi) = \sum_{\alpha \in \Gamma} a^\alpha L'_S(0, \chi^\alpha) e_{\bar{\chi}^\alpha} \in \mathbb{C}[G].$$

Note that this element is central since this is the case of the projections $e_{\bar{\chi}^\alpha}$ so that left multiplication by $\pi(a, \chi)$ is a $\mathbb{C}[G]$-endomorphism of $\mathbb{C}X_K$.

Remark 34. Suppose that $r_S(\chi) = 0$. By Proposition 54 we have $\langle \chi, \chi_{X_K} \rangle_G = 0$ and for all $\alpha \in \Gamma$ we have $\langle \chi^\alpha, \chi_{X_K} \rangle_G = 0$. Since $\chi_{X_K} \in R(G, \mathbb{Q})$ we have

$$\langle \bar{\chi}^\alpha, \chi_{X_K} \rangle_G = \overline{\langle \chi^\alpha, \chi_{X_K} \rangle_G} = 0.$$

As a consequence, the representation EX_K contains no subrepresentation that is isomorphic to $(V^\vee)^\alpha$. It follows that $\pi(a,\chi)EX_K = \{0\}$ which implies that $\pi(a,\chi)\mathbb{Q}X_K = \{0\}$. Suppose that $r_S(\chi) > 1$, then $r_S(\chi^\alpha) > 1$ and thus $L'_S(0,\chi^\alpha) = 0$ so that $\pi(a,\chi) = 0$. Consequently, $\pi(a,\chi)\mathbb{Q}X_K \neq \{0\}$ implies that $r_S(\chi) = 1$.

Proposition 66 (Tate). *Let χ be an irreducible character of G with $r_S(\chi) = 1$. Let V be a representation of G with character χ. If a is a non-zero element of E, then the following statements are equivalent:*

(i) $\pi(a,\chi)\mathbb{Q}X_K \cap \lambda_K(\mathbb{Q}U_K) \neq \{0\}$

(ii) $\pi(a,\chi)\mathbb{Q}X_K = \lambda_K(U_W)$

(iii) Conjecture 3 is true for χ.

Proof. We start by proving the equivalence between (i) and (ii). The representation $\mathbb{Q}X_K$ has a canonical representation over $\mathbb{Q}$ given by, say

$$\mathbb{Q}X_K = X_W \oplus \bigoplus_i W_i.$$

None of the W_i contains a subrepresentation that is isomorphic to W over $\mathbb{Q}$. Tensoring with $\mathbb{C}$ over $\mathbb{Q}$ gives a finer decomposition

$$\mathbb{C}X_K = \mathbb{C}X_W \oplus \bigoplus_i \bigoplus_j W_{ij}.$$

Here, $\mathbb{C} \otimes_{\mathbb{Q}} W_i = \bigoplus_j W_{ij}$ is the canonical decomposition of $\mathbb{C} \otimes_{\mathbb{Q}} W_i$ over $\mathbb{C}$. Since ψ takes values in $\mathbb{Q}$, we have $\bar{\psi} = \psi$ which implies that $\psi = \sum_{\alpha\in\Gamma} \bar{\chi}^\alpha$. As left $\mathbb{C}[G]$-modules, we therefore have

$$\mathbb{C}X_W \cong \bigoplus_{\alpha\in\Gamma} V^\alpha \cong \bigoplus_{\alpha\in\Gamma} (V^\vee)^\alpha.$$

We conclude that

$$\mathbb{C}X \cong \bigoplus_{\alpha\in\Gamma} (V^\vee)^\alpha \oplus \bigoplus_i \bigoplus_j W_{ij}. \tag{6.4.0.2}$$

We have $1 = r_S(\chi^\sigma) = \langle \chi^\sigma, \chi_{X_K}\rangle_G$ for any $\sigma \in \mathrm{Aut}(\mathbb{C})$. In particular, we have $\langle \bar{\chi}^\alpha, \chi_{X_K}\rangle = 1$ for all $\alpha \in \Gamma$. This implies that the representation $\mathbb{C}X_K$ has a unique subrepresentation that is isomorphic to $(V^\vee)^\alpha$. Thus, none of the W_{ij} contain a subrepresentation isomorphic to $(V^\vee)^\alpha$ for any α. Therefore the W_{ij} are annihilated by $\pi(a,\chi)$. Consequently, we have

$$\pi(a,\chi)\mathbb{Q}X_K = \pi(a,\chi)X_W.$$

Recall that $\pi(a,\chi)$ is a central idempotent element of $\mathbb{C}[G]$ and therefore is a left $\mathbb{Q}[G]$-module endomorphism of X_W. But X_W is a simple left $\mathbb{Q}[G]$-module and by Lemma 6, the action of $\pi(a,\chi)$ on X_W is either zero or an isomorphism. Thus $\pi(a,\chi)X_W$ is either 0 or a left $\mathbb{Q}[G]$-module isomorphic to W.

Consider the left $\mathbb{Q}[G]$-module isomorphism $\lambda_K^{-1} : \mathbb{R}X_K \longrightarrow \mathbb{Q}U_K$. For the same reason, $\lambda_K^{-1}(\pi(a,\chi)X_W)$ is either zero or a left $\mathbb{Q}[G]$-submodule of $\mathbb{Q}U$ which is isomorphic to W and must therefore be equal to U_W.

So if (i) holds, then $\lambda_K^{-1}(\pi(a,\chi)X_W)$ is non-zero and thus equal to U_W which means that $\pi(a,\chi)X_W = \lambda_K(U_W)$ which is the statement of (ii). On the other hand, if (i) does not hold, then it is clear that $\pi(a,\chi)X_W = 0$. We have proved the equivalence between (i) and (ii).

Before proving the remaining equivalence, we make a few definitions. By left semisimplicity of $\mathbb{Q}[G]$, there exist complementary left $\mathbb{Q}[G]$-modules X' and U' such that $\mathbb{Q}X_K = X_W \oplus X'$ and $\mathbb{Q}U_K = U_W \oplus U'$. Since $\mathbb{Q}X_K \cong \mathbb{Q}U_K$ and $X_W \cong W \cong U_W$ as left $\mathbb{Q}[G]$-modules, X' and U' must be isomorphic as left $\mathbb{Q}[G]$-modules. Let $f' : X' \longrightarrow U'$ be such a left $\mathbb{Q}[G]$-module isomorphism.

We have the $\mathbb{C}[G]$-endomorphism $\pi(a,\chi)$ of $\mathbb{C}X_W$ and

$$\lambda_K : \mathbb{C}U_W \longrightarrow \mathbb{C}X_W$$

is a left $\mathbb{C}[G]$-isomorphism. We define a left $\mathbb{C}[G]$-homomorphism $f(a,\chi)$ from $\mathbb{C}X_K$ to $\mathbb{C}U_K$ as follows:

$$f(a,\chi) = \begin{cases} \lambda_K^{-1} \circ \pi(a,\chi) & \text{on } \mathbb{C}X_W \\ 1 \otimes f' & \text{on } \mathbb{C}X'. \end{cases}$$

By Proposition 54, we have $r_S(\chi^\alpha) = \dim_{\mathbb{C}} \operatorname{Hom}_{\mathbb{C}[G]}((V^\vee)^\alpha, \mathbb{C}X_K)$. Let

$$\varphi : (V^\vee)^\alpha \longrightarrow \mathbb{C}X_K$$

be a non-zero left $\mathbb{C}[G]$-homomorphism. Its image is a simple left $\mathbb{C}[G]$-module isomorphic to $(V^\vee)^\alpha$ by Lemma 6. By the decomposition (6.4.0.4), $\mathbb{C}X'$ contains no subrepresentation that is isomorphic to $(V^\vee)^\alpha$. Thus φ takes its values in $\mathbb{C}X_W$. The $\mathbb{C}$-vector space endomorphism of the space $\operatorname{Hom}_{\mathbb{C}[G]}((V^\vee)^\alpha, \mathbb{C}X_K)$ that is induced by the left $\mathbb{C}[G]$-endomorphism $\lambda_K \circ f(a,\chi)$ of $\mathbb{C}X_K$ maps φ to $\lambda \circ f(a,\chi) \circ \varphi$. Let $x \in (V^\vee)^\alpha$. Since the image of φ is in $\mathbb{C}X_W$, by definition of $f(a,\chi)$, we see that

$$\lambda_K \circ f(a,\chi) \circ \varphi(x) = \pi(a,\chi)(\varphi(x)).$$

Since φ is a left $\mathbb{C}[G]$-module homomorphism and $\pi(a,\chi)$ is an element of $\mathbb{C}[G]$, we obtain

$$\lambda_K \circ f(a,\chi) \circ \varphi(x) = \varphi(\pi(a,\chi)x) = \varphi(a^\alpha L'_S(0,\chi^\alpha)x) = a^\alpha L'_S(0,\chi^\alpha)\varphi(x)$$

by definition of $\pi(a,\chi)$. Thus $\lambda_K \circ f(a,\chi)$ acts on $\operatorname{Hom}_{\mathbb{C}[G]}((V^\vee)^\alpha, \mathbb{C}X_K)$ as $\pi(a,\chi)$ acts on $(V^\vee)^\alpha$, that is, by left multiplication by $a^\alpha L'_S(0,\chi^\alpha)$. Since $\operatorname{Hom}_{\mathbb{C}[G]}((V^\vee)^\alpha, \mathbb{C}X_K)$ is of dimension 1, we see that

$$\delta_S(\chi^\alpha, \lambda_K \circ f(a,\chi)) = a^\alpha L'_S(0,\chi^\alpha), \qquad \text{for all } \alpha \in \Gamma. \tag{6.4.0.3}$$

We now prove the remaining equivalence. Suppose that (ii) holds. Then $\lambda_K^{-1} \circ \pi(a,\chi)(\mathbb{C}X_W) = \mathbb{C}U_W$ so that $f(a,\chi)$ is a left $\mathbb{C}[G]$-module isomorphism from $\mathbb{C}X_K$ to $\mathbb{C}U_K$. In this case we have

$$\delta_S(\chi^\alpha, \lambda \circ f(a,\chi)) = R_S(\chi^\alpha, f(a,\chi))$$

and (6.4.0.5) translates as

$$A_S(\chi^\alpha, f(a,\chi)) = \frac{R_S(\chi, f(a,\chi))}{L'_S(0,\chi^\alpha)} = a^\alpha = A_S(\chi, f(a,\chi))^\alpha, \qquad \text{for all } \alpha \in \Gamma$$

and $A_S(\chi, f(a,\chi)) = a \in \mathbb{Q}(\chi)$. Therefore Conjecture 4 is true for χ. Since Conjecture 3 and Conjecture 4 are equivalent we have proved that *(ii)* implies *(iii)*.

Conversely, suppose that Conjecture 3 is true. By Corollary 32 this is equivalent to Conjecture 5 being true in the case "$E = \mathbb{C}$". Then

$$A_S(\chi, f(a,\chi)) := \delta_S(\chi, f(a,\chi))/L'_S(0,\chi)$$

satisfies the following: for all $\alpha, \beta \in \mathrm{Aut}(\mathbb{C})$ we have

$$A(\chi^\alpha, f(a,\chi)^\beta) = A(\chi^{\beta^{-1}\alpha}, f(a,\chi))^\beta = (a^{\beta^{-1}\alpha})^\beta = a^\alpha = A_S(\chi^\alpha, f(a,\chi))$$

where we used (6.4.0.5) twice. As a consequence, $(\lambda_K \circ f(a,\chi)^\beta)_{V^\alpha}$ and $(\lambda_K \circ f(a,\chi))_{V^\alpha}$ have the same determinant as endomorphisms of the 1-dimensional space $\mathrm{Hom}_{\mathbb{C}[G]}((V^\vee)^\alpha, \mathbb{C}X_K)$. They must therefore be equal on $\mathbb{C}X_W$. Since $1 \otimes f'$ is defined over $\mathbb{Q}$ we have $(1 \otimes f')^\beta = 1 \otimes f'$ by Remark 32. Therefore $f(a,\chi) = f(a,\chi)^\beta$ on $\mathbb{C}X_K$. This is true for all $\beta \in \mathrm{Aut}(\mathbb{C})$ and therefore $f(a,\chi)$ must be defined over $\mathbb{Q}$. It therefore maps $\mathbb{Q}X_K$ to $\mathbb{Q}U_K$ and X_W to U_W. In particular $\pi(a,\chi)\mathbb{Q}X_K \subset \lambda(U_W)$. Moreover, $\pi(a,\chi)X_W$ is non-zero since a and $L'_S(0,\chi^\alpha)$ are non-zero. We must therefore have $\pi(a,\pi)\mathbb{Q}X_K = \lambda(U_W)$. □

We now examine how Conjecture 3 implies the existence of certain special units called Stark units. Let Ψ be a set of irreducible characters of G with the following three properties:

- $1_G \notin \Psi$
- If $\chi \in \Psi$, then $\chi^\alpha \in \Psi$ for all $\alpha \in \mathrm{Aut}(\mathbb{C})$
- $r_S(\chi) = 1$ for all $\chi \in \Psi$.

Let $\chi_1, \dots, \chi_s$ be elements of Ψ such that for all i, j and for all $\alpha \in \mathrm{Aut}(\mathbb{C})$, $\chi_i \neq \chi_j^\alpha$. Let $(a_\chi)_{\chi \in \Psi}$ be a family of elements in $\mathbb{Q}(\chi)$ with the property that $a_{\chi^\alpha} = a_\chi^\alpha$ for all $\alpha \in \mathrm{Aut}(\mathbb{C})$. Note that the restriction $\alpha|_{\mathbb{Q}(\chi)}$ is an element of $\Gamma_\chi := \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ by Proposition 18. Consider the element

$$\sum_{\chi \in \Psi} a_\chi L'_S(0,\chi) e_{\bar{\chi}} = \sum_{i=1}^{s} \sum_{\alpha \in \Gamma_{\chi_i}} a_{\chi_i^\alpha} L'_S(0,\chi_i^\alpha) e_{\bar{\chi}_i^\alpha} = \sum_{i=1}^{s} \pi(a_{\chi_i}, \chi_i) \in \mathbb{C}[G].$$

Suppose that Conjecture 3 is true. By Proposition 66, it is equivalent to

$$\pi(a_{\chi_i}, \chi_i)\mathbb{Q}X_K = \lambda_K(U_{W_i}), \qquad \text{for all } i = 1, \dots, s.$$

In particular, $\pi(a_{\chi_i}, \chi_i)X_K \subset \lambda_K(\mathbb{Q}U_K)$ and since $\lambda_K(\mathbb{Q}U_K) = \mathbb{Q}\lambda_K(U_K)$ we obtain

$$\sum_{\chi \in \Psi} a_\chi L'_S(0,\chi) e_{\bar{\chi}} X_K \subset \mathbb{Q}\lambda_K(U_K). \tag{6.4.0.4}$$

Remark 35. Note that this even holds if Ψ contains characters with $r_S(\chi) \neq 1$ since if $r_S(\chi) > 1$ then $L'_S(0,\chi) = 0$ and if $r_S(\chi) = 0$, then $e_{\bar{\chi}}\mathbb{Q}X_K = 0$ by Remark 34.

By Proposition 53 we have $\chi_{X_K} = \chi_{Y_K} - 1_G$. Thus for all non-trivial irreducible character χ of G we have $\langle \chi, \chi_{X_K} \rangle_G = \langle \chi, \chi_{Y_K} \rangle_G$ and $\mathbb{C}X_K$ and $\mathbb{C}Y_K$ have the same χ-component and therefore the effect of the projection e_χ is the same on X_K as on Y_K. In particular, since $1_G \notin \Psi$, this is true for all $\chi \in \Psi$ and we can replace X_K in (6.4.0.6) by Y_K to obtain

$$\sum_{\chi \in \Psi} a_\chi L'_S(0, \chi) e_{\bar{\chi}} Y_K \subset \mathbb{Q}\lambda_K(U_K). \tag{6.4.0.5}$$

An element of $\mathbb{Q}\lambda_K(U_K)$ is of the form $\sum_i^n \frac{a_i}{b_i} \otimes \lambda_K(\epsilon_i)$ and since λ_K is a homomorphism and the tensor product is over $\mathbb{Z}$, this is equal to

$$\sum_{i=1}^n \frac{1}{b_i} \left(1 \otimes \lambda_K \left(\prod_{j=1}^n \epsilon_j^{a_j} \right) \right).$$

Therefore, any element of $\mathbb{Q}\lambda_K(U_K)$ is of the form

$$\frac{1}{m}(1 \otimes \lambda_K(\epsilon)) =: \frac{\lambda_K(\epsilon)}{m}$$

for some $\epsilon \in U_K$ and some integer m.

As a consequence of (6.4.0.7), given any place $v \in S$ and any place $w \in S_K$ lying above v, there exists an integer m and a unit ϵ of K such that

$$m \sum_{\chi \in \Psi} a_\chi L'_S(0, \chi) e_{\bar{\chi}} w = \lambda_K(\epsilon). \tag{6.4.0.6}$$

Remark 36. Note that this equation is note possible with only (6.4.0.6) since $w \notin X_K$. Hence the importance of excluding 1_G form the set Ψ. Note also that this exclusion is only necessary when $r_S(1_G) = 1$.

Definition 28. A unit ϵ that satisfies (6.4.0.8) for some $w \in S_K$ and some integer m is called a Stark unit.

Remark 37. Once we fix the integer m, a Stark unit satisfying (6.4.0.8) is uniquely determined up to a root of unity contained in K since the kernel of λ_K is μ_K.

Proposition 67. *Let $v \in S$ and let w be a place of K that lies above v. If a Stark unit exists for w, then there exists a Stark unit for w that belongs to K^{D_w}.*

Proof. Note, by looking at the definition of $e_{\bar{\chi}}$, that ϵ is supported only at places in S_K that divide v. Let σ be an element of the decomposition group D_w of w over v. Since G acts transitively on the places above v, we have

$$\begin{aligned}
\lambda_K(\epsilon) &= \sum_{[\tau] \in G/D_w} \log |\epsilon|_{\tau(w)} \tau(w) \\
&= \sum_{[\tau] \in G/D_w} \log |\epsilon^\sigma|_{\sigma\tau(w)} \tau(w) \\
&= \sum_{[\tau] \in G/D_w} \log |\epsilon^\sigma|_{\tau(w)} \tau\sigma^{-1}(w) \\
&= \sum_{[\tau] \in G/D_w} \log |\epsilon^\sigma|_{\tau(w)} \tau(w) \\
&= \lambda_K(\epsilon^\sigma).
\end{aligned}$$

Since $\epsilon^\sigma = \epsilon^\sigma\epsilon^{-1}\epsilon$, we must have that $\epsilon^\sigma\epsilon^{-1}$ is a root of unity in K. Denote this element by $\zeta(\sigma) \in \mu_K$. This defines a function $\zeta : D_w \longrightarrow \mu_K$. Note that if $\sigma, \tau \in D_w$, then we have

$$\zeta(\sigma\tau) = \epsilon^{\sigma\tau}\epsilon^{-1} = \sigma\tau(\epsilon)\epsilon^{-1} = \sigma(\tau(\epsilon)\epsilon^{-1})\sigma(\epsilon)\epsilon^{-1} = \zeta(\tau)^\sigma\zeta(\sigma).$$

This proves that ζ is a crossed homomorphism and therefore defines a 1-cocycle from D_w to μ_K. Denote by $[\zeta]$ the class of ζ in the first cohomology group $H^1(D_w, \mu_K)$. The class $[\zeta]$ is zero if and only if it is a 1-coboundary, that is, if there exists $\xi \in \mu_K$ such that $\zeta(\sigma) = \xi^\sigma\xi^{-1}$. If this is the case, then $\xi^\sigma\xi^{-1} = \epsilon^\sigma\epsilon^{-1}$ which implies that $\epsilon\xi^{-1} = (\epsilon\xi^{-1})^\sigma$ for all $\sigma \in D_w$ so that $\epsilon\xi^{-1} \in K^{D_w}$.

By general theory of group cohomology (cf. Chapter IV of [CF]), if H is a normal subgroup of D_w, then the composition map

$$H^q_T(D_w, \mu_K) \xrightarrow{\text{Res}} H^q_T(H, \mu_K) \xrightarrow{\text{Cor}} H^q_T(D_w, \mu_K)$$

is multiplication by $[G : H]$. Here, the subscript T denotes Tate cohomology and q is any integer. In particular, if we apply this with the trivial subgroup $H = \{1\}$, then the above map is multiplication by $|G|$ and $H^q_T(H, \mu_K) = \{0\}$. Therefore $H^q_T(D_w, \mu_K)$ is annihilated by $|G|$. Taking $q = 1$, we get that $H^1(D_w, \mu_K)$ is annihilated by $|G|$ since $H^1_T(D_w, \mu_K) = H^1(D_w, \mu_K)$. Because μ_K is finite, it is clear that $H^1(D_w, \mu_K)$ is annihilated by $\omega_K = |\mu_K|$. Thus $H^1(D_w, \mu_K)$ has exponent dividing $n := \gcd(|G|, \omega_K)$. Taking m to be nm in (6.4.0.8), $\epsilon' = \epsilon^n$ satisfies the new equation and the associated 1-cocycle becomes ζ^n whose class in $H^1(D_w, \mu_K)$ is zero. Thus, multiplying the Stark unit ϵ' by an appropriate element of μ_K, we may suppose that $\epsilon' \in K^{D_w}$. □

Remark 38. By comparing coefficients in (6.4.0.8) and using the definition of the projection e_χ, we can rewrite this equation as

$$\log|\epsilon|_{\sigma(w)} = \log|\epsilon^{\sigma^{-1}}|_w = \frac{m}{|G|}\sum_{\chi\in\Psi} a_\chi L'_S(0,\chi)\chi(1)\sum_{\tau\in D_w}\chi(\sigma\tau), \text{ for all } \sigma \in G.$$

and

$$|\epsilon|_{w'} = 1, \text{ for all } w' \nmid v$$

Conjecture 3 in the rank 1 case therefore implies that the values $L'_S(0,\chi)$ for $\chi \in \Psi$ are related in a linear relationship with coefficients in $\mathbb{Q}(\chi)$ to the logarithm of the absolute value of a Stark unit that belongs to K^{D_w}.

Example 6. Suppose that Conjecture 3 is true in the rank 1 case. Suppose that K/k is a finite abelian extension, that $|S| \geq 3$ and that the place v of k lying below w splits in K. The latter implies that the residual degree $f_{w/v}$ of w is 1 and therefore $D_w = \{1\}$. Let $\widehat{G}$ denote the irreducible characters of G over $\mathbb{C}$ which are all of dimension 1 by Corollary 29. Then $r_S(1_G) = |S| - 1 \geq 2$ so that $L'_S(0, 1_G) = 0$. Therefore there is no need to exclude the trivial character from Ψ by Remark 35. Taking Ψ to be $\widehat{G}$ and $a_\chi = 1$ for all $\chi \in \widehat{G}$, the equation of Remark 38 becomes

$$\begin{aligned}
\log|\epsilon^{\sigma^{-1}}|_w &= \frac{m}{|G|}\sum_{\chi\in\widehat{G}}\chi(\sigma)L'_S(0,\chi)\sum_{\tau\in G_w}\chi(\tau)\\
&= \frac{m}{|G|}\sum_{\chi\in\widehat{G}}\chi(\sigma)L'_S(0,\chi)|D_w|\chi^{D_w}([1])\\
&= \frac{m}{|G|}\sum_{\chi\in\widehat{G}}\chi(\sigma)L'_S(0,\chi).
\end{aligned}$$

If $\chi\in\widehat{G}$, then we have

$$\frac{1}{m}\sum_{\sigma\in G}\chi(\sigma)\log|\epsilon^{\sigma}|_w = \frac{1}{|G|}\sum_{\substack{\sigma\in G\\ \chi'\in\widehat{G}}}\chi(\sigma)\chi'(\sigma^{-1})L'_S(0,\chi') = \sum_{\chi'\in\widehat{G}}L'_S(0,\chi')\left\langle\chi,\chi'\right\rangle_G.$$

We therefore obtain the formula

$$L'_S(0,\chi) = \frac{1}{m}\sum_{\sigma\in G}\chi(\sigma)\log|\epsilon^{\sigma}|_w. \tag{6.4.0.7}$$

A Refined Conjecture in the Abelian Case

In the abelian case with some special conditions on S, we saw in Example 6 that Conjecture 3 implies the formula (6.4.0.9). Stark's abelian conjecture is a refinement of Conjecture 3 in the case of rank 1. It states that, under certain conditions on the set of places S, equation (6.4.0.9) holds with $m=-\omega_K$ and $K(\epsilon^{1/\omega_K})$ is an abelian extension of k. Before we can state this conjecture precisely we first fix some notations.

Let K/k be a finite abelian extension of number fields with Galois group G. Let $\widehat{G}$ denote the group of irreducible characters of G over $\mathbb{C}$. Note that these are all of dimension 1 by Corollary 29. Let S be a finite set of places of k that satisfies the following three conditions:

- S contains all archimedean places of k as well as all finite places of k that ramify in K,
- S contains at least one place that splits completely in K,
- $|S|\geq 2$.

As usual, we let S_K denote the set of places of K lying above those in S. Let v be a split prime in S and let w be any place in K above v. We define

$$U^{(v)} = \begin{cases}\{u\in U_{K,S_K}\ :\ |u|_{w'}=1,\forall w'\nmid v\} & \text{if } |S|\geq 3\\ \{u\in U_{K,S_K}\ :\ |u|_{\sigma(w')}=|u|_{w'},\forall\sigma\in G\} & \text{if } S=\{v,v'\} \text{ and } w'|v'.\end{cases}$$

Also, we define

$$U^{ab}_{K/k} = \{u\in U_{K,S_K}\ :\ K(u^{1/\omega_K})/k \text{ is abelian}\}.$$

The abelian rank one Stark conjecture, which we refer to as $\mathrm{St}(K/k,S,v)$, can now be formulated:

Conjecture 6 (St$(K/k,S,v)$)**.** *With notations as above, there exists a Stark unit $\epsilon \in U_{K/k}^{ab} \cap U^{(v)}$ such that*

$$\log|\epsilon^\sigma|_w = -\omega_K \zeta_S'(0,\sigma), \qquad \forall \sigma \in G \tag{6.4.0.8}$$

or, equivalently,

$$L_S'(0,\chi) = -\frac{1}{\omega_K}\sum_{\sigma\in G}\chi(\sigma)\log|\epsilon^\sigma|_w, \qquad \forall \chi \in \widehat{G}. \tag{6.4.0.9}$$

Remark 39. To see that the first statement implies the second, we use the first formula of Proposition 55 to compute that for all $\chi \in \widehat{G}$ we have

$$L_S'(0,\chi) = \sum_{\sigma\in G}\chi(\sigma)\zeta_S'(0,\sigma) = -\frac{1}{\omega_K}\sum_{\sigma\in G}\chi(\sigma)\log|\epsilon^\sigma|_w.$$

For the other implication, we use the second formula of Proposition 55 to compute that for all $\sigma \in G$ we have

$$\zeta_S'(0,\sigma) = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\bar{\chi}(\sigma)L_S'(0,\chi) = -\frac{1}{\omega_K}\sum_{\tau\in G}\log|\epsilon^\tau|_w\left(\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\bar{\chi}(\sigma)\chi(\tau)\right).$$

By Proposition 28 the latter is equal to $-\frac{\log|\epsilon^\sigma|_w}{\omega_K}$.

Remark 40. We make several comments concerning St$(K/k,S,v)$:

- St$(K/k,S,v)$ is independent of the place w above v. Indeed, if $\tilde{w}$ is another place above v, let $\tau \in G$ such that $\tilde{w} = \tau(w)$. Then, if St$(K/k,S,v)$ is true for w, we have

  $$L_S'(0,\chi) = -\frac{1}{\omega_K}\sum_{\sigma\in G}\chi(\sigma)\log|(\epsilon^\tau)^\sigma|_{\tilde{w}}$$

  and $K((\epsilon^\tau)^{1/\omega_K}) = K(\epsilon^{1/\omega_K})$. If $|S| \geq 3$, then for all $w' \nmid v$, we have

  $$|\epsilon^\tau|_{w'} = |\epsilon|_{\tau^{-1}(w')} = 1$$

  since $\tau^{-1}(w') \nmid v$ and $\epsilon \in U^{(v)}$. If $S = \{v,v'\}$, then for all $\sigma \in G$, $|\epsilon^\tau|_{\sigma(w')} = |\epsilon|_{\tau^{-1}\sigma(w')} = |\epsilon|_{w'}$ since $\epsilon \in U^{(v)}$. Therefore $\epsilon^\tau \in U_{K/k}^{ab} \cap U^{(v)}$. We can thus take ϵ^τ to be the desired Stark unit for w' and St$(K/k,S,v)$ is true for w'.

- The valuations of ϵ at places above v are given by (6.4.0.10) and the valuations at places outside S_K are all 1. If $|S| \geq 3$, then ϵ is a v-unit so that the valuation of ϵ at places not above v is 1. If $S = \{v,v'\}$, then by the product formula and the fact that $\epsilon \in U^{(v)}$, we have

  $$|\epsilon|_{w'}^{[G:D_{w'}]}\prod_{\sigma\in G/D_w}|\epsilon|_{\sigma(w)} = 1$$

  so that the valuation of ϵ at places above v' is known. In conclusion, all valuations of ϵ are known and therefore St$(K/k,S,v)$ specifies ϵ up to a root of unity.

Proposition 68. *Suppose that S contains only one place v that splits completely in K. Suppose that there exists an injective irreducible character χ of G. Suppose that there exists a Stark unit ϵ such that $\mathrm{St}(K/k,S,v)$ is true. Then $K = k(\epsilon)$.*

Proof. We clearly have $k(\epsilon) \subset K$. We need to show that $k(\epsilon)$ is only fixed by the identity in G. By Corollary 30, we have

$$r_S(\chi, K/k) = \{v \in S \mid \chi(D_w) = 1\}.$$

But $\chi(D_w) = 1$ implies by the injectivity of χ that $D_w = \{1\}$. In other words, v splits completely in K. By assumption S only contains one place that splits completely and therefore we have $r_S(\chi) = 1$ and $L'_S(0,\chi) \neq 0$. Let σ be a generator of G. Let $\tau \in G$ such that $\epsilon^\tau = \epsilon$. By (6.4.0.11) we have

$$\begin{aligned} L'_S(0,\chi) &= -\frac{1}{\omega_K}\sum_{\eta\in G}\chi(\eta)\log|(\epsilon^\tau)^\eta|_w \\ &= -\frac{1}{\omega_K}\sum_{\eta\in G}\chi(\eta)\log|\epsilon^{\eta\tau}|_w \\ &= -\frac{1}{\omega_K}\sum_{\eta\in G}\chi(\eta\tau^{-1})\log|\epsilon\eta|_w \\ &= \chi(\tau)^{-1}L'_S(0,\chi). \end{aligned}$$

Thus $\chi(\tau) = 1$ and by injectivity of χ we have $\tau = 1$. As a consequence, $k(\epsilon) = K$. □

Corollary 34. *Suppose that k is real and that there exists an irreducible injective character χ of G. Suppose that S contains only one place v that splits completely in K and suppose that v is a real archimedean place. Suppose that there exists a Stark unit ϵ such that $\mathrm{St}(K/k,S,v)$ is true. Then*

$$K = k(\exp(-2\zeta'_S(0,1))).$$

Proof. Let w be a place above v and fix an embedding $k \subset K \subset K_w = \mathbb{R}$. We may choose ϵ to be positive. By (6.4.0.10) we have

$$\log\epsilon = -2\zeta'_S(0,1).$$

By Proposition 68 we have $K = k(\epsilon) = k(\exp(-2\zeta'_S(0,1)))$. □

Remark 41. This corollary shows that in certain specific cases, Stark's conjecture enables one to construct an abelian extension of k by adjoining the value at $s = 0$ of an analytic function. This gives reason to believe that Stark's conjectures could provide an insight in Hilbert's 12th problem which is concerned with explicitly constructing a class field theory for number fields.

We will now prove that $\mathrm{St}(K/k,S,v)$ is actually independent of the choice of a prime v that splits in K. In order to accomplish this, we will make use of the following lemma which follows from class field theory.

Lemma 13. *Suppose that K/k is a totally unramified finite abelian extension and let S be a finite set of primes containing all infinite primes of K and such that all elements of S split completely in K. Then $[K:k]$ divides the ideal class number $h_{k,S}$.*

Proof. Let $\mathfrak{m}$ be the modulus obtained by taking the product of all finite primes in S. The primes of $\mathcal{O}_{k,S}$ are in bijection with the primes of $\mathcal{O}_k$ that do not belong to S. The prime ideals of $\mathcal{O}_k$ that do not belong to S are exactly those that do not divide $\mathfrak{m}$. Since $\mathcal{O}_{k,S}$ is a Dedekind domain, the group of fractional ideals $I(\mathcal{O}_{k,S})$ has unique factorization into prime components. We therefore get an obvious group isomorphism $I_k(\mathfrak{m}) \cong I_{\mathcal{O}_{k,S}}$. The subgroup $P_{k,S}$ of $I(\mathcal{O}_{k,S})$ consisting of the principal fractional ideals corresponds via this isomorphism to a subgroup $P'(\mathfrak{m})$ of $I_k(\mathfrak{m})$. This subgroup consists of elements of the form $\mathfrak{a}.(x)$ where $(x) \in P(\mathfrak{m})$ and $\mathfrak{a}$ only has primes of S in its decomposition.

Clearly, we have the inclusion $P_{k,1}(\mathfrak{m}) \subset P'(\mathfrak{m})$, that is, $P'(\mathfrak{m})$ is a congruence subgroup for $\mathfrak{m}$. By Theorem 2.4.3, there exists a unique abelian extension H_S of k such that $P'(\mathfrak{m}) = \ker(\Phi_{H_S/k}, \mathfrak{m})$. Thus the Artin map induces an isomorphism

$$\Phi_{H_S/k,\mathfrak{m}} : I_k(\mathfrak{m})/P'(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(H_S/k).$$

In particular, H_S/k is an extension of degree $h_{k,S}$. The proof has been reduced to showing that K is a subfield of H_S. By Corollary 7 this is equivalent to proving that

$$P_{k,1}(\mathfrak{m}) \subset \ker(\Phi_{H_S/k,\mathfrak{m}}) \subset \ker(\Phi_{K/k,\mathfrak{m}}). \tag{6.4.0.10}$$

But K/k is totally unramified and therefore K/k has conductor the empty modulus $\mathfrak{1}$ and K is contained in the Hilbert class field H_k of k. By Corollary 7 the latter implies that

$$P_k = \ker(\Phi_{H_k/k,\mathfrak{1}}) \subset \ker(\Phi_{K/k,\mathfrak{1}}). \tag{6.4.0.11}$$

Moreover, $\ker(\Phi_{K/k,\mathfrak{m}}) = \ker(\Phi_{K/k,\mathfrak{1}}) \cap I_k(\mathfrak{m})$. Since $\ker(\Phi_{H_S/k,\mathfrak{m}})$ is a subgroup of $I_k(\mathfrak{m})$, in order to prove (6.4.0.12), it suffices to prove that

$$P'(\mathfrak{m}) \subset \ker(\Phi_{K/k,\mathfrak{1}}).$$

Let $\mathfrak{a}.(x)$ be an element of $P'(\mathfrak{m})$. By (6.4.0.13) we see that $\Phi_{K/k,\mathfrak{1}}(x\mathcal{O}_k) = 1$. All primes that divide $\mathfrak{a}$ belong to S and these primes split in K. Thus their Artin symbol in K/k is trivial which implies by multiplicativity of the Artin symbol that $(\mathfrak{a}, K/k)$ is also trivial. We conclude that $P'(\mathfrak{m})$ does indeed lie in the kernel of $\Phi_{K/k,\mathfrak{1}}$. □

Proposition 69. *The conjecture* $\mathrm{St}(K/k,S,v)$ *is true if S contains at least two places which split in K. In particular,* $\mathrm{St}(K/k,S,v)$ *is independent of v and we shall in the future write* $\mathrm{St}(K/k,S)$.

Proof. If v is a place that splits and w lies above v, then $D_w = \{1\}$. If $|S| \geq 3$, then $r_S(1_G) = |S| - 1 \geq 2$ and by Corollary 30, $r_S(\chi) \geq 2$ if χ is of dimension 1. Thus, $r_S(\chi) \geq 2$ for all $\chi \in \widehat{G}$ which implies that $L'_S(0,\chi) = 0$. Therefore $\mathrm{St}(K/k,S,v)$ is true for the Stark unit $\epsilon = 1$.

Suppose now that $S' = \{v, v'\}$ where both v and v' are split in K. In this case, we have $r_S(1_G) = 1$ and $r_S(\chi) = 2$ for all non-trivial $\chi \in \widehat{G}$. In particular, $L'_S(0,\chi) = 0$ for non-trivial χ. Moreover, the rank of the S-unit group $U_{k,S}$ of k is 1 and we pick η to be a fundamental unit such that $|\eta|_v > 1$. By Proposition 46, we have $L_S(s,1_G) = \zeta_{k,S}$, the Dedekind zeta function of k relative to S. By the analytic class number formula at $s = 0$, Corollary 29, we have

$$L'_S(0,1_G) = \zeta'_{k,S}(0) = -\frac{h_{k,S}\log|\eta|_v}{\omega_k}.$$

Since μ_k is a subgroup of μ_K, ω_k divides ω_K. Since S contains all primes that ramify in K and no prime in S ramifies in K, we deduce that K/k is totally unramified. We may therefore apply Lemma 13 which says that $[K:k]$ divides $h_{k,S}$. Consequently

$$m = \frac{\omega_K h_{k,S}}{\omega_k [K:k]}$$

is a positive integer.

Now set $\epsilon = \eta^m \in U_{k,S}$. For all $\sigma \in G$, $\epsilon^\sigma = \epsilon$ so that $|\epsilon^\sigma|_{w'} = |\epsilon|_{w'}$ and $\epsilon \in U^{(v)}$. Also, $\epsilon^{1/\omega_K} = (\eta^{1/\omega_k})^{h_{k,S}/[K:k]}$ so that $K(\epsilon^{1/\omega_K})$ is a subfield of $K(\eta^{1/\omega_k})$. The latter is the compositum of the abelian extension K/k with the abelian Kummer extension $k(\eta^{1/\omega_k})/k$ so it is abelian over k. Thus $\epsilon \in U^{ab}_{K/k} \cap U^{(v)}$. It remain to check (6.4.0.11). We have

$$L'_S(0, 1_G) = -\frac{h_{k,S}}{\omega_k} \log|\eta|_v = -\frac{[K:k]}{\omega_K} \log|\epsilon|_v = -\frac{1}{\omega_K} \sum_{\sigma \in G} 1_G(\sigma) \log|\epsilon^\sigma|_v.$$

For $\chi \in \widehat{G}$ non-trivial, we have

$$-\frac{1}{\omega_K} \sum_{\sigma \in G} \chi(\sigma) \log|\epsilon^\sigma|_w = -\frac{\log|\epsilon|_v}{\omega_K} \sum_{\sigma \in G} \chi(\sigma) = -\frac{\log|\epsilon|_v}{\omega_K} |G| \left\langle \chi, 1_G \right\rangle_G = 0$$

and $L'_S(0, \chi) = 0$. □

From this result we get some easy corollaries.

Corollary 35. *The conjecture* $\mathrm{St}(k/k, S)$ *is true.*

Proof. All primes of k are split in k. Since $|S|$ is required to have at least two elements it contains at least two elements that split and the previous result applies. □

Corollary 36. *The conjecture* $\mathrm{St}(K/k, S)$ *is true if* k *contains at least two complex archimedean places.*

Proposition 70. *If* S' *contains* S*, then* $\mathrm{St}(K/k, S)$ *implies* $\mathrm{St}(K/k, S')$*.*

Proof. First, if S satisfies the three conditions imposed in the beginning of this section, then S' clearly also satisfies them. If $S = S'$ there is nothing to prove.

Suppose that $S' = S \cup \{\mathfrak{p}\}$. Then $\mathfrak{p}$ is necessarily a finite unramified prime of k. Let v be an element of S that splits in K and suppose that there exists a Stark unit $\epsilon \in U^{ab}_{K/k,S} \cap U^{(v)}_{K,S}$ that satisfies $\mathrm{St}(K/k, S)$. Let $\sigma_{\mathfrak{p}}$ denote the Frobenius element of any $\mathfrak{P}$ above $\mathfrak{p}$. This element is independent of $\mathfrak{P}$ since we are in the abelian case. Define

$$\epsilon' = \frac{\epsilon}{\epsilon^{\sigma_{\mathfrak{p}}^{-1}}}.$$

Suppose that $|S| \geq 3$. Then for any $w' \nmid v$ we have $|\epsilon|_{w'} = |\epsilon|_{\sigma_{\mathfrak{p}}(w')}$ since $\sigma_{\mathfrak{p}}(w') \nmid v$ and $\epsilon \in U^{(v)}$. If $S = \{v, v'\}$ and $w'|v$, then

$$|\epsilon^{\sigma_{\mathfrak{p}}^{-1}}|_{\sigma(w')} = |\epsilon|_{\sigma_{\mathfrak{p}}\sigma^{-1}(w')} = |\epsilon|_{w'}$$

for all $\sigma \in G$ since $\epsilon \in U^{(v)}$. Thus $|(\epsilon')^\sigma|_{w'} = 1$ and $\epsilon' \in U^{(v)}$. Since $(\epsilon')^{1/\omega_K} \in K(\epsilon^{1/\omega_K})$ we also have $\epsilon' \in U^{ab}_{K,S'}$.

We have

$$L_{S'}(s,\chi) = (1-\chi(\sigma_{\mathfrak{p}})N(\mathfrak{p})^{-s})L_S(s,\chi).$$

Since $L_S(0,\chi)=0$, we obtain

$$L'_{S'}(0,\chi) = (1-\chi(\sigma_{\mathfrak{p}}))L'_S(0,\chi).$$

Using (6.4.0.11), we compute that

$$\begin{aligned} L'_{S'}(0,\chi) &= -\frac{1-\chi(\sigma_{\mathfrak{p}})}{\omega_K}\sum_{\sigma\in G}\chi(\sigma)\log|\epsilon^{\sigma}|_w \\ &= -\frac{1}{\omega_K}\sum_{\sigma\in G}\chi(\sigma)(\log|\epsilon^{\sigma}|_w - \log|(\epsilon^{\sigma_{\mathfrak{p}}^{-1}})^{\sigma}|_w) \\ &= -\frac{1}{\omega_K}\sum_{\sigma\in G}\chi(\sigma)\log|(\epsilon')^{\sigma}|_w. \end{aligned}$$

Thus $\mathrm{St}(K/k,S')$ is true.

The result for a general S' trivially follows. □

One can prove the following result which describes how $\mathrm{St}(K/k,S)$ behaves with respect to intermediate extensions. We will not prove this here because it requires developing more theory.

Proposition 71. *If $K/K'/k$ is a tower of finite abelian extensions of number fields, then* $\mathrm{St}(K/k,S)$ *implies* $\mathrm{St}(K'/k,S)$.

Proof. See [Ta1], § 3.5, p. 92. □

An Example with Cyclotomic Units

The aim of this section is to present an example where the existence of Stark units is known. We begin with a brief introduction to cyclotomic units.

Let m be a positive integer. We will be working with the cyclotomic field $K=\mathbb{Q}(\zeta)$ where ζ is a primitive m-th root of unity. We treat several cases.

- Suppose that $m=p$ is a prime. Define

  $$f(X) = \frac{X^p-1}{X-1} = X^{p-1}+\ldots+X+1 \in \mathbb{Z}[X].$$

  This is the minimal polynomial of ζ. The roots of f are precisely the ζ^i where $\gcd(i,p)=1$. Thus we can write

  $$f(X) = \prod_{(i,p)=1}(X-\zeta^i). \tag{6.4.0.12}$$

  Consider the element $\pi = 1-\zeta$. If ω is any primitive p-th root of unity and $(i,n)=1$, then we have

  $$\frac{1-\omega^i}{1-\omega} = \omega^{i-1}+\ldots+\omega+1 \in \mathcal{O}_K = \mathbb{Z}[\zeta]. \tag{6.4.0.13}$$

In particular, $\frac{1-\zeta^i}{1-\zeta} \in \mathcal{O}_K$. Let $(j,p) = 1$ such that $ij \equiv 1 \mod p$. Then $\zeta^{ij} = \zeta$. Thus, by (6.4.0.15), we have

$$\frac{1-\zeta}{1-\zeta^i} = \frac{1-(\zeta^i)^j}{1-\zeta^i} \in \mathcal{O}_K.$$

We conclude that $\frac{1-\zeta^i}{1-\zeta}$ is a unit in $\mathcal{O}_K$ for all i such that $(i,p) = 1$. This implies that for i and j prime to p, $\frac{1-\zeta^i}{1-\zeta^j}$ is a unit of $\mathcal{O}_K$. Let $\mathfrak{q}$ be any prime ideal in $\mathcal{O}_K$. Then

$$0 = v_{\mathfrak{q}}\left(\frac{1-\zeta^i}{1-\zeta^j}\right) = v_{\mathfrak{q}}(1-\zeta^i) - v_{\mathfrak{q}}(1-\zeta^j).$$

We conclude that all the $1-\zeta^i$ share the same valuation at all primes of $\mathcal{O}_K$. By evaluating (6.4.0.14) at $X = 1$, we obtain $p = \prod_{(i,p)=1}(1-\zeta^i)$ and taking valuations we see that

$$v_{\mathfrak{q}}(p) = (p-1)v_{\mathfrak{q}}(\pi).$$

If $\mathfrak{q} \nmid p$, then $v_{\mathfrak{q}}(\pi) = 0$. If $\mathfrak{q} = \mathfrak{p}$ is a prime that divides p, then the left hand side is the ramification index $e_{\mathfrak{p}}$ of $\mathfrak{p}$ over p. But $[K : \mathbb{Q}] = p - 1 = rf_pe_p$ where f_p is the residual degree of $\mathfrak{p}$ over p and r is the number of primes above p. Since $v_{\mathfrak{p}}(\pi)$ cannot be zero, we must have $e_p \geq re_pf_p$ which implies $r = f = 1$ so that p is totally ramified in K. In conclusion, π is a $\mathfrak{p}$-unit of K.

- Suppose that $m = p^r$ is a prime power. Consider the polynomial $X^{p^r} - 1$ and let $Y = X^{p^{r-1}}$. Then

$$X^{p^r} - 1 = Y^p - 1 = (Y-1)(Y^{p-1} + \ldots + Y + 1).$$

Define the polynomial

$$f(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = Y^{p-1} + \ldots + Y + 1 \in \mathbb{Z}[X].$$

This is the minimal polynomial of ζ and therefore it factors as

$$f(X) = \prod_{(i,p^r)=1} (X - \zeta^i). \tag{6.4.0.14}$$

In the exact same way as before, one shows that $\frac{1-\zeta^i}{1-\zeta}$ is a unit in $\mathcal{O}_K$ and therefore all $1-\zeta^i$ have the same valuations. Evaluating (6.4.0.16) at $X = 1$ and taking valuations we obtain

$$v_{\mathfrak{q}}(p) = \phi(p^r)v_{\mathfrak{q}}(\pi).$$

Just as before, we conclude that p is totally ramified in K and that π is a $\mathfrak{p}$-unit of K.

- Suppose that n is not a prime power. In this case we claim that

$$\prod_{i=1}^{n-1}(1-\zeta^i) = \pm 1$$

which implies that all $1-\zeta^i$ are units in $\mathcal{O}_K$.

Let S_d denote the set of all primitive d-th roots of unity and consider the polynomials

$$f_d(X) = \prod_{\omega \in S_d} (X-\omega) \in \mathbb{Z}[X].$$

Consider also the polynomial $f(X) = \frac{X^n-1}{X-1}$ which has roots all non-trivial n-th roots of unity. These are exactly the elements of S_d for $d|n$ and $d>1$. We therefore have the decomposition

$$f(X) = \prod_{\substack{d|n \\ d>1}} f_d(X).$$

Evaluating at $X=1$ gives $n = \prod_{\substack{d|n \\ d>1}} f_d(1)$. We just saw in the previous case that $f_{p^r}(1) = p$ for any prime p and any positive integer r. Let $n = \prod_{p|n} p^{v_p(n)}$ be the prime factor decomposition of n. For each p, p^r with $r = 1, \dots, v_p(n)$ appears in the above product and contribute with a factor p. Thus the prime power divisors of n suffice to yield n. In other words, if d is a composite divisor of n, then $f_d(1) = \pm 1$. In particular, $f_n(1) = \pm 1 = \prod_{i=1}^{n-1}(1-\zeta^i)$.

We are now ready to construct the example. Let m be an integer greater or equal to 3 which is either odd or divisible by 4. In particular, $\phi(m)$ is even. Let ζ be a primitive m-th root of unity. Let $L = \mathbb{Q}(\zeta)$ and let $K = \mathbb{Q}(\zeta)^+$ be the maximal totally real subfield of K. Take S to be the union $\{v_\infty\} \cup \{p|m\}$. Note that v_∞ splits in K, that $|S| \geq 2$ and that all primes that ramify in K belong to S by (2.5.0.1). Recall from Example 2 that K is the $m\mathbb{Z}$-ray class field of $\mathbb{Q}$ whereas L is the $m\mathbb{Z}v_\infty$-ray class field of $\mathbb{Q}$.

Consider the automorphism σ_a of L which is the restriction to L of $(\zeta \mapsto \zeta^a)$. Consider the partial zeta-function

$$\zeta_S(s,\sigma_a) = \sum_{\substack{n \geq 1 \\ n \equiv \pm a (m)}} |n|^{-s} = \sum_{\substack{n \in \mathbb{Z} \\ n \equiv \pm a (m)}} |n|^{-s}.$$

Consider $\mathbb{Q}(\zeta)$ as embedded in $\mathbb{C}$ by identifying ζ with $e^{\frac{2i\pi}{m}}$ and let

$$\epsilon = (1-\zeta)(1-\zeta^{-1}) = 2 - \cos(2\pi/m) \in \mathcal{O}_K.$$

If $|S| \geq 3$, then m is not a prime power so by the above discussion, $1-\zeta$ and $1-\zeta^{-1}$ are both units of $\mathcal{O}_L$, whence ϵ is a unit of $\mathcal{O}_K$. Thus $\epsilon \in U^{(v_\infty)}$. If $S = \{v_\infty, p\}$, then m is a power of p and by the above discussion p is totally ramified in K. Therefore ϵ is automatically in $U^{(v_\infty)}$. We have

$$\epsilon^{\sigma_a} = (1-\zeta^a)(1-\zeta^{-a}) = 2 - 2\cos(2\pi a/m).$$

One can compute (cf. [StIV]) that the derivative of the partial zeta function $\zeta_S(s,\sigma_a)$ at $s=0$ is

$$\zeta_S'(0,\sigma_a) = -\frac{1}{2}\log(2-2\cos(2\pi a/m)) = -\frac{1}{2}\log \epsilon^{\sigma_a}. \qquad (6.4.0.15)$$

Since $\omega_K = 2$, this equation is exactly (6.4.0.10).

For any integer q, set $\zeta_q = e^{\frac{2i\pi}{q}}$ and let $L_q = \mathbb{Q}(\zeta_q)$. We have

$$\epsilon = 2 - \zeta_m - \zeta_m^{-1} = -(\zeta_{2m} - \zeta_{2m}^{-1})^2 = [\zeta_4(\zeta_{2m} - \zeta_{2m}^{-1})]^2.$$

If m is odd, then $2m$ is composite and $\zeta_{2m} - \zeta_{2m}^{-1} = \zeta_{2m}(1 - \zeta_{2m}^{-2})$ is a unit of $\mathcal{O}_{L_{2m}}$ by our above discussion. In particular, it is a unit of $\mathcal{O}_{L_{4m}}$, as is ζ_4. Thus, in the case of an odd m, ϵ is the square of a unit of L_{4m}. In particular, $K(\sqrt{\epsilon}) \subset L_{4m}$ and $K(\sqrt{\epsilon})$ is therefore abelian over $\mathbb{Q}$.

If m is even, then by assumption m is divisible by 4. If m is composite then by the above reasoning, ϵ is the square of a unit in L_{2m}. If m is a power of 2, then ϵ is the square of an S-unit of L_{2m}. Either way, $K(\sqrt{\epsilon})$ is a subfield of L_{2m} and therefore abelian over $\mathbb{Q}$.

We conclude that $\epsilon \in U_K^{ab}$ and consequently that ϵ is a Stark unit for K so that $\mathrm{St}(K/\mathbb{Q}, S)$ is true.

Remark 42. This partially proves the abelian Stark conjecture in the case $k = \mathbb{Q}$. In general, when we explicitly know the class field theory of k, it is possible to prove the conjecture. The class field theory is known in the case $k = \mathbb{Q}$ and the case if k is quadratic imaginary. We have the following result that we give without proof. A partial proof can be found in [Ta1], § 3.9, p. 95.

Theorem 6.4.1. *The conjecture* $\mathrm{St}(K/k, S)$ *is true for* $k = \mathbb{Q}$ *or if* k *is quadratic imaginary.*

Chapter 7

The Birch and Swinnerton-Dyer Conjecture

In the 1960's, Peter Swinnerton-Dyer used the EDSAC computer at the University of Cambridge to calculate the number of points modulo p on elliptic curves with known rank. From these numerical results he was led with Bryan Birch to their famous conjecture which they proposed in [BSD]. It says that the rank of the Hasse-Weil L-function of an elliptic curve at $s = 0$ is the rank of the Mordell-Weil group of the curve. A refined version of the conjecture also gives a formula for the leading term in the Taylor expansion of this L-function around $s = 1$ in terms of arithmetic invariants of the elliptic curve. The aim of this chapter is to state this refined version of the conjecture. We follow the paper of Gross [Gr2] and supplement it with the book of Silverman [Sil].

7.1 The Riemann-Roch Theorem

By a curve defined over a field k we mean a projective variety defined over k of dimension 1. Let C/k be a smooth curve. We will always assume that k is perfect field. We fix an algebraic closure $\bar{k}$ of k and let G denote the absolute Galois group of k. We will call P a point of C and write $P \in C$ if $P \in C(\bar{k})$. We review some notations.

Let $\mathrm{Div}(C)$ denote the divisor group of C. This is the free abelian group on the points of C. We note by $\mathrm{Div}^0(C)$ the subgroup of degree zero divisors. The Galois group G acts on points of C by acting on their coordinates and therefore naturally acts on $\mathrm{Div}(C)$. We let $\mathrm{Div}_k(C)$ denote the subgroup of $\mathrm{Div}(C)$ fixed by the action of G and we let $\mathrm{Div}_k^0(C)$ denote the subgroup of $\mathrm{Div}^0(C)$ fixed by the action of G.

If $f \in \bar{k}(C)$, then we define $\mathrm{div} f = \sum_{P \in C} \mathrm{ord}_P(f)(P)$. This is an element of $\mathrm{Div}^0(C)$ and divisors of the form $\mathrm{div} f$ are called principal divisors. Let P denote the subgroup of principal divisors. We form the Picard group of C to be $\mathrm{Pic}(C) = \mathrm{Div}(C)/P$. We define $\mathrm{Pic}_k(C)$ to be the subgroup of $\mathrm{Pic}(C)$ that is fixed by G. We write $D_1 \sim D_2$ and say that D_1 and D_2 are linearly equivalent if $D_1 = D_2$ in $\mathrm{Pic}(C)$.

Let $D = \sum_{P \in C} n_P(P) \in \mathrm{Div}(C)$. We say that D is efficient and write

$D \geq 0$ if $n_P \geq 0$ for all $P \in C$. We then write $D_1 \geq D_2$ if the divisor $D_1 - D_2$ is efficient. We define

$$\mathcal{L}(D) = \{f \in \bar{k}(C)^* \ : \ \mathrm{div} f \geq -D\} \cup \{0\}.$$

This is a finite-dimensional $\bar{k}$-vector space (cf. [Sil], II.5.2) and we denote by $\ell(D)$ its dimension over $\bar{k}$.

Let Ω_C denote the space of differential forms on C. This is a $\bar{k}(C)$-vector space of dimension 1 (cf. [Sil], II.4.2). Let $\omega \in \Omega_C$. Let $P \in C$ and let t_P denote a uniformizer of $\bar{k}(C)$ at P. Then there exists a unique $g \in \bar{k}(C)$ such that $\omega = g dt_P$. We denote this element by ω/dt_P. One can check that $\mathrm{ord}_P(\omega/dt_P)$ does not depend on the choice of t_P. We define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(\omega/dt_P)$. and associate to ω the divisor

$$\mathrm{div}\omega = \sum_{P \in E} \mathrm{ord}_P(\omega)(P).$$

The differential ω is said to be holomorphic if $\mathrm{div}\omega \geq 0$.

Let ω, ω' be two non-zero differentials. Then there exists $f \in \bar{k}(C)^*$ such that $\omega' = f\omega$. We have $\mathrm{div}\omega' = \mathrm{div} f + \mathrm{div}\omega$ so that $\mathrm{div}\omega' = \mathrm{div}\omega$ in $\mathrm{Pic}(C)$. The canonical divisor class on C is the image of $\mathrm{div}\omega$ in $\mathrm{Pic}(C)$ for any non-zero differential ω. Any representative of this class is called a canonical divisor on C and is typically denoted by K_C.

Suppose that $f \in \mathcal{L}(K_C)$. Then $\mathrm{div} f\omega \geq 0$ so that $f\omega$ is a holomorphic differential. On the other hand, let ω' be a holomorphic differential. Then $\omega' = f\omega$ for some $f \in \bar{k}(C)$ and $f \in \mathcal{L}(K_C)$. This establishes an isomorphism of $\bar{k}$-vector spaces

$$\mathcal{L}(K_C) \cong \{\omega \in \Omega_C \ : \ \omega \text{ is holomorphic}\}.$$

Theorem 7.1.1 (Riemann-Roch)**.** *Let C/k be a smooth curve and let K_C be a canonical divisor on C. There exists a non-negative integer g, the genus of C, such that for all $D \in \mathrm{Div}(C)$ we have*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Proof. See [Sil], II.5.4. □

Corollary 37. *Let C/k be a smooth curve and let K_C be a canonical divisor on C. Then we have*

(i) $\ell(K_C) = g$.

(ii) $\deg K_C = 2g - 2$.

(iii) If $D \in \mathrm{Div}(C)$ and $\deg D > 2g - 2$ then

$$\ell(D) = \deg D - g + 1.$$

Proof. By Theorem 7.1.1 we have

$$\ell(0) - \ell(K_C) = \deg 0 - g + 1.$$

But $\mathcal{L}(0)$ consists of the functions $f \in \bar{k}(C)$ that have no poles. Since $\deg \mathrm{div} f = 0$, f has no zeros either so that $f \in \bar{k}$. Thus $\ell(0) = 1$ and $\ell(K_C) = g$.

By Theorem 7.1.1 we have

$$\ell(K_C) - \ell(0) = \deg K_C - g + 1$$

so that $\deg K_C = 2g - 2$.

If $D \in \mathrm{Div}(C)$ and $\deg D > 2g - 2$ then by Theorem 7.1.1 we have

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

By (ii) we have $\deg(K_C - D) = 2g - 2 - \deg D < 0$. Let $f \in \mathcal{L}(K_C - D)$. Then

$$0 = \deg \mathrm{div} f \geq -\deg(K_C - D) > 0$$

so that $f = 0$ and $\ell(K_C - D) = 0$. □

Lemma 14. *Let C/k be a non-singular curve of genus 1. If $P, Q \in C$, then $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. Suppose that there exists $f \in \bar{k}(C)^*$ such that $\mathrm{div}(f) = (P) - (Q)$. Then $\mathrm{div}(f) + (Q) = (P) \geq 0$ so that $f \in \mathcal{L}((Q))$. We have $\deg(Q) = 1 > 2g - 2 = 0$ so that by Corollary 37 (iii) we have $\ell((Q)) = 1$. But $\mathcal{L}((Q))$ already contains the constant functions and therefore $f \in \bar{k}$. In particular, $\mathrm{div}(f) = 0$ and thus $P = Q$. □

7.2 Elliptic Curves

An elliptic curve E defined over k is a non-singular curve over k of genus 1 together with a k-rational point $\mathcal{O}_E \in E(K)$.

A very interesting fact about elliptic curves is that one can define an operation on E, making it into an algebraic group defined over k.

7.2.1 The Algebraic Group Law

We show how one can transfer the group law on $\mathrm{Pic}^0(E)$ to $E(\bar{k})$.

Theorem 7.2.1. *For any $D \in \mathrm{Div}^0(E)$, there exists a unique point $P \in E(\bar{k})$ such that $D \sim (P) - (\mathcal{O}_E)$. This defines a map $\sigma : \mathrm{Div}^0(E) \longrightarrow E(\bar{k})$ by sending D to the corresponding point P. This map induces a bijection of sets*

$$\sigma : \mathrm{Pic}^0(E) \xrightarrow{\sim} E(\bar{k}).$$

For future reference, we denote the inverse of this map by κ.

Proof. Let D be a divisor of degree 0. Then $D + (\mathcal{O}_E)$ is a divisor of degree 1 and by Corollary 37 (iii) we have $\ell(D + (\mathcal{O}_E)) = 1$. Let f be a non-zero element of $\mathcal{L}(D + (\mathcal{O}_E))$. Then f is a basis of $\mathcal{L}(D + (\mathcal{O}_E))$ and $\mathrm{div}(f) \geq -D - (\mathcal{O}_E)$. We have $\deg(\mathrm{div}(f) + D + (\mathcal{O}_E)) = 1$ and all coefficients $\mathrm{div}(f) + D + (\mathcal{O}_E)$ are non-negative. Therefore there must exist $P \in E$ such that $\mathrm{div}(f) + D + (\mathcal{O}_E) = (P)$. In other words, $D \sim (P) - (\mathcal{O}_E)$. This proves the existence part. For uniqueness, suppose that we also have $D \sim (P') - (\mathcal{O}_E)$. Then $(P') \sim (P)$ and by Lemma 14 we get $P = P'$.

The map σ is surjective. Indeed, if $P \in E$, then $(P) - (\mathcal{O}_E)$ is an element of $\mathrm{Div}^0(E)$ whose image by σ is P. Moreover, if $D_1, D_2 \in \mathrm{Div}^0(E)$, then

$\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. In fact, let $P_i = \sigma(D_i)$ for $i = 1, 2$. Then $P_1 = P_2$ implies that $(P_1) - (\mathcal{O}_E) = (P_2) - (\mathcal{O}_E)$ from which it follows that $D_1 \sim D_2$. Conversely, $D_1 \sim D_2$ implies that $(P_1) - (\mathcal{O}_E) \sim (P_2) - (\mathcal{O}_E)$ which in turn implies $(P_1) \sim (P_2)$. By Lemma (14), $P_1 = P_2$ and the proof is complete. □

Definition 29. If $P, Q \in E$, then we define their sum to be

$$P + Q := \sigma(\kappa(P) + \kappa(Q)) = \sigma([(P) + (Q) - 2(\mathcal{O}_E)]).$$

With this law $E(\bar{k})$ is a group with zero element $\mathcal{O}_E$ and σ is an isomorphism of abelian groups.

Remark 43. If $\tau \in G$ and $D \in \mathrm{Div}^0(E)$ is such that $D \sim (P) - (\mathcal{O}_E)$, then $D^\tau \sim (P^\tau) - (\mathcal{O}_E)$ so that $\sigma([D^\tau]) = P^\tau = \sigma([D])^\tau$. This shows that σ is a left G-module isomorphism. The restriction of σ to $\mathrm{Pic}^0_k(E)$ is an injective group homomorphism. Moreover, if $[D] \in \mathrm{Pic}^0_k(E)$ and $D \sim (P) - (\mathcal{O}_E)$, then $D^\tau \sim D$ and $D^\tau \sim (P^\tau) - (\mathcal{O}_E)$. By uniqueness, we obtain $P = P^\tau$. This proves that $P \in E(k)$ and the image of the restriction of σ lies in $E(k)$. If $P \in E(k)$, then $(P) - (\mathcal{O}_E)$ certainly belongs to $\mathrm{Div}^0_k(E)$ and its image under σ is P. This proves surjectivity. Thus we get an isomorphism of abelian groups

$$\sigma : \mathrm{Pic}^0_k(E) \longrightarrow E(k).$$

In particular, $E(k)$ is a subgroup of $E(\bar{k})$ with the above defined group law.

Proposition 72. *Let E/k be an elliptic curve. Then we have the following exact sequence:*

$$1 \longrightarrow \bar{k}^* \longrightarrow \bar{k}(E)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E) \longrightarrow \mathrm{Pic}^0(E) \longrightarrow 0$$

Moreover, the sequence obtained by taking G-invariants

$$1 \longrightarrow k^* \longrightarrow k(E)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0_k(E) \longrightarrow \mathrm{Pic}^0_k(E) \longrightarrow 0$$

remains exact.

Proof. Let $f \in \bar{k}(E)^*$ and define a map $f : E \longrightarrow \mathbb{P}^1$ by $P \mapsto [f(P), 1]$ is f is regular at P and by $P \mapsto [1, 0]$ otherwise. This is a rational map and since E and $\mathbb{P}^1$ are both smooth curves it is a morphism of curves (cf. [Sil], II.2.1). If $\mathrm{div}(f) = 0$ then f has no poles and therefore the above map cannot be surjective. Consequently, it must be a constant map (cf. [Sil], II.2.3) so that $f \in \bar{k}^*$. This proves exactness at $\bar{k}(E)^*$. Exactness elsewhere is clear.

For the second part, we start by proving exactness at $k(E)^*$. If $P(E) = \mathrm{div}(\bar{k}(E)^*)$ is the subgroup of $\mathrm{Div}^0(E)$ of principal divisors, that is, the kernel of $\mathrm{Div}^0(E) \longrightarrow \mathrm{Pic}^0(E)$, then $P_k(E) = P(E) \cap \mathrm{Div}^0_k(E)$ is the kernel of $\mathrm{Div}^0_k(E) \longrightarrow \mathrm{Pic}^0_k(E)$. Proving exactness amounts to proving that $P_k(E) = \mathrm{div}(k(E)^*)$. Note that we clearly have the inclusion $\mathrm{div}(k(E)^*) \subset P_k(E)$ since $\mathrm{div}(f)^\tau = \mathrm{div}(f^\tau) = \mathrm{div}(f)$ for any $\tau \in G$ and any $f \in k(E)^*$. Now, if $f \in P_k(E)$, then for any $\tau \in G$, we have $\mathrm{div}(f)^\tau = \mathrm{div}(f^\tau) = \mathrm{div}(f)$. Thus $\mathrm{div}(f^\tau/f) = 0$ and therefore these two functions differ by a constant $c_\tau \in \bar{k}^*$. This gives a function $c : G \longrightarrow \bar{k}^*$. If $\omega \in G$, then

$$f^{\omega\tau} = (f^\tau)^\omega = c_\tau^\omega f^\omega = c_\tau^\omega c_\omega f$$

so that $c_{\omega\tau} = c_\tau^\omega c_\omega$. As a consequence, c is a crossed homomorphism and determines an element of the first cohomology group $H^1(G, \bar{k}^*)$. By Hilbert's Theorem 90, this cohomology group is trivial so c is a 1-coboundary, that is, there exists $x \in \bar{k}^*$ such that $c = (\tau \mapsto x^\tau / x)$. Then $(f/x)^\tau = f/x$ for all τ so that $f/x \in k(E)^*$. Since $\operatorname{div}(f/x) = \operatorname{div}(f)$, we see that $\operatorname{div}(f) \in \operatorname{div}(k(E)^*)$. This proves the inclusion $P_k(E) \subset \operatorname{div}(k(E)^*)$.

It is easily checked that the sequence

$$1 \longrightarrow k^* \longrightarrow k(E)^* \xrightarrow{\text{div}} \operatorname{Div}_k^0(E) \longrightarrow \operatorname{Pic}_k^0(E)$$

is exact.

It remains to show that $\operatorname{Div}_k^0(E) \longrightarrow \operatorname{Pic}_k^0(E)$ is surjective. Let $[D]$ be an element of $\operatorname{Pic}_k^0(E)$. By definition, for all $\tau \in G$, we have $[D^\tau] = [D]$ in $\operatorname{Pic}_k^0(E)$. In other words, $D^\tau \sim D$. Let $P = \sigma([D]) \in E(\bar{k})$, that is, the unique point such that $D \sim (P) - (\mathcal{O}_E)$. It follows that $D^\tau \sim (P^\tau) - (\mathcal{O}_E)$. But $D^\tau \sim D$ implies that $(P) \sim (P^\tau)$ and by Lemma 14 we have $P = P^\tau$. This being true for any τ, we have shown that $P \in E(k)$. But then $(P) - (\mathcal{O}_E) \in \operatorname{Div}_k^0(E)$ and $[D] = [(P) - (\mathcal{O}_E)]$. This proves surjectivity. □

7.2.2 The Geometric Group Law

Let E/k be an elliptic curve. Using the fact that the genus of E is 1 together with Theorem 7.1.1, one can show (cf. [Sil], III.3.1) that E embeds as a non-singular cubic curve in $\mathbb{P}^2$ given by a Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with coefficients in k. The point $\mathcal{O}_E$ is mapped to the unique intersection of the Weierstrass curve with the line at infinity. This point has projective coordinates $[0, 1, 0]$.

The embedding $E \longrightarrow \mathbb{P}^2$ is given by a morphism $\Phi = [x, y, 1]$ where $x, y \in k(E)$ are rational functions called Weierstrass coordinates for E. We have the equality $\bar{k}(E) = \bar{k}(x, y)$. The discriminant of the above Weierstrass equation is a certain polynomial $\Delta = \Delta(a_1, \ldots, a_6)$ in the coefficients of the equation. Note that a Weierstrass equation defines a non-singular curve in $\mathbb{P}^2$ if and only if $\Delta \neq 0$ (cf. [Sil] III.1.4 (a)). Conversely, every non-singular curve in $\mathbb{P}^2$ given by a Weierstrass equation is an elliptic curve.

If K/k is any field extension then the chord and tangent process turns $E(K)$ into an abelian group with zero element $\mathcal{O}_E$. This geometric addition law is determined by the following property:

$$P + Q + R = \mathcal{O}_E \iff P, Q, R \text{ are colinear.}$$

Note that it is not immediate that this actually defines a group law (associativity is not immediate). However, as we will see, this turns out to be true. One can derive addition and inverse formulas that turn out to be rational functions in the coefficients a_i of the Weierstrass equation. One can then show that both addition and taking inverse are morphisms of projective varieties defined over k (cf. [Sil], III.3.6).

Theorem 7.2.2. *The geometric group law on E and the algebraic group law on E coincide.*

Proof. Let $P, Q \in E(\bar{k})$. In this proof we use the symbol $\oplus$ to denote the geometric group law and the symbol $+$ to denote the algebraic group law. We want to prove that $P \oplus Q = P + Q$. This amounts to proving that

$$\kappa(P \oplus Q) = \kappa(P) + \kappa(Q)$$

where addition in the right hand side is the one of $\mathrm{Pic}^0(E)$. Let

$$f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$$

be the equation of the line L in $\mathbb{P}^2$ going through P, Q and let R be the third point of intersection with E. Let

$$f'(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$$

be the equation of the line L' in $\mathbb{P}^2$ going through R and $\mathcal{O}_E$. By definition of the geometric group law, the third point of intersection of L' with E is $P \oplus Q$. Counting intersection multiplicities, we see that

$$\begin{aligned} \mathrm{div}(f/Z) &= (P) + (Q) + (R) - 3(\mathcal{O}_E) \\ \mathrm{div}(f'/Z) &= (R) + (P \oplus Q) - 2(\mathcal{O}_E). \end{aligned}$$

It follows that

$$\mathrm{div}(f'/f) = ((P \oplus Q) - (\mathcal{O}_E)) - ((P) + (Q) - 2(\mathcal{O}_E)) \sim 0$$

and therefore $\kappa(P \oplus Q) = \kappa(P) + \kappa(Q)$. □

Remark 44. From this theorem it follows that the geometric group law is a group law and in particular we get associativity. On the other hand, it shows that the algebraic group law we defined is a morphism of varieties defined over k. From now on we will obviously not distinguish between the algebraic and geometric group laws and both will simply be denoted by the symbol $+$.

7.2.3 Torsion on Elliptic Curves

Having defined the operation of addition on the points of E we naturally define the multiplication-by-m map $[m]$ on E for any integer m inductively: if $m > 1$, then $[m+1](P) = [m](P) + P$ and if $m < 0$, then $[m](P) = [-m](-P)$. Since addition and taking inverse are morphisms, one verifies easily that $[m]$ is a morphism for all integer m. Since $[m]$ obviously maps $\mathcal{O}_E$ to itself, $[m]$ is an isogeny for all m.

If E_1 and E_2 are two elliptic curves, we denote by $\mathrm{Hom}(E_1, E_2)$ the additive group of isogenies $E_1 \longrightarrow E_2$. If $E_1 = E_2$ we can also compose isogenies. Thus if E is an elliptic curve, we let $\mathrm{End}(E) := \mathrm{Hom}(E, E)$ be the ring of isogenies $E \longrightarrow E$. This is called the endomorphism ring of E. If E_1 and E_2 are both defined over a field k, then we denote by $\mathrm{Hom}_k(E_1, E_2)$ and $\mathrm{End}_k(E)$ respectively the group and ring of isogenies defined over k.

Since addition and taking inverse are both defined over k, we see that

$$[m] \in \mathrm{End}_k(E)$$

for all m. There is more to be said about the multiplication-by-m isogeny:

Proposition 73. *Let E/k be an elliptic curve and assume that m is non-zero in k, that is, $m \neq 0$ if $\operatorname{char}(k) = 0$ and $(m,p) = 1$ if $\operatorname{char}(k) = p > 0$. Then $[m]$ is a finite separable endomorphism of degree m^2.*

Proof. Let $\omega \in \Omega_E$ be an invariant differential of E. Then $[0]^*\omega = 0$ and $[1]^*\omega = \omega$ since $[1]$ is the identity map. If m is an integer, then we have

$$[m+1]^*\omega = [m]^*\omega + [1]^*\omega = [m]^*\omega + \omega$$

(cf. [Sil], III.5.2). Now by ascending and descending induction, we get $[m]^*\omega = m\omega$ for all $m \in \mathbb{Z}$. In particular, since m is non-zero in k, $[m]^*\omega \neq 0$. Therefore we cannot have $[m] = [0]$. Thus $[m]$ is non-constant, hence surjective. In other words, $[m]$ is a finite map. Moreover, $[m]^*\omega \neq 0$ implies that $[m]$ is separable (cf. [Sil], II.4.2).

Denote by $\widehat{[m]}$ the dual isogeny of $[m]$. By convention, $\widehat{[0]} = [0]$ and since $\deg([1]) = 1$, we have $\widehat{[1]} = [1]$. We have

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]} = \widehat{[m]} + [1].$$

By ascending and descending induction, we obtain $\widehat{[m]} = [m]$. Let $d = \deg([m])$. Then

$$[d] = [\deg([m])] = \widehat{[m]} \circ [m] = [m^2].$$

Thus $[d - m^2] = [0]$ is constant. This implies that $d - m^2 = 0$ since otherwise $[d - m^2]$ is a finite map. □

Remark 45. It follows from this result that we have an injection of rings

$$\mathbb{Z} \hookrightarrow \operatorname{End}(E).$$

This is usually an isomorphism, but if the endomorphism ring of E is bigger than $\mathbb{Z}$, then E is said to have complex multiplication.

Definition 30. For any integer m we define the m-torsion subgroup of E, denoted by $E[m]$, to be $\ker([m])$. For any field extension K/k we denote by $E[m](K)$ the m-torsion points of E that are defined over K.

Remark 46. Since multiplication-by-m is an algebraic map, every m-torsion point has coordinates that are algebraic over k. Therefore we have

$$E[m] = E[m](\bar{k}).$$

We want to understand the structure of $E[m]$. In order to deal with the case of positive characteristic, we introduce the Frobenius map on an elliptic curve.

Let k be a perfect field of characteristic p and let $q = p^r$ for some $r \in \mathbb{N}$. Let E/k be an elliptic curve given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define a new curve $E^{(q)}/k$ by raising the coefficients of the Weierstrass equation for E to the q-th power, that is,

$$E^{(q)} : y^2 + a_1^qxy + a_3^qy = x^3 + a_2^qx^2 + a_4^qx + a_6^q.$$

Writing out the discriminant $\Delta(E)$ of E and using the fact that the q-th power map $k \longrightarrow k$ is a homomorphism, we see that $\Delta(E^{(q)}) = \Delta(E)^q$. Since E is non-singular, we find that $E^{(q)}$ is non-singular and therefore is an elliptic curve.

Definition 31. The q-th power Frobenius map of E is the map

$$\phi_q : E \longrightarrow E^{(q)}, \qquad (x,y) \longmapsto (x^q, y^q)$$

and $\phi_q(\mathcal{O}_E) = \mathcal{O}_{E^{(q)}} = \mathcal{O}_E$.

This is a rational map and since both E and $E^{(q)}$ are non-singular, ϕ is a morphism. The Frobenius morphism has the following properties:

Proposition 74. *Let ϕ_q be the q-th power Frobenius map of E.*

(i) $\phi_q^*(k(E^{(q)})) = k(E)^q$.

(ii) ϕ_q *is purely inseparable.*

(iii) $\deg(\phi_q) = q$.

Proof. See [Sil] II.2.11. □

Remark 47. Suppose that $k = \mathbb{F}_q$ is a finite field with q elements. Denote by ψ_q the q-th power map on $\overline{\mathbb{F}}_q$ so that $\phi_q(x,y) = (\psi_q(x), \psi_q(y))$. The restriction of ψ_q to k is the identity so that $E^{(q)} = E$. In particular, ϕ_q is an endomorphism of E, called the Frobenius endomorphism. Note that $E(\mathbb{F}_q)$ consists of the points of $E(\overline{\mathbb{F}}_q)$ that are fixed by $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. By definition, we have

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \varprojlim \langle \psi_q|_{\mathbb{F}_{q^n}} \rangle.$$

It becomes clear that the points fixed by $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ are exactly those fixed by ϕ_q. Stated more precisely, we have

$$\ker(1 - \phi_q) = E(\mathbb{F}_q).$$

Proposition 75. *Let $E/\mathbb{F}_q$ be an elliptic curve define over the finite field of cardinality q. Let $\phi : E \longrightarrow E$ denote the q-th power Frobenius isogeny. Then the map $1 - \phi$ is separable.*

Proof. Let ω be an invariant differential on E. Then

$$(1-\phi)^*\omega = [1]^*\omega - \phi^*\omega = \omega$$

because by Proposition 74 (*ii*) the map ϕ is purely inseparable and this is true if and only if $\phi^*\omega = 0$ (cf. [Sil], II.4.2). Therefore $(1-\phi)^*\omega \neq 0$ and $1 - \phi$ is separable. □

We are now almost ready to establish the structure of the m-torsion subgroup of E. All we need is the following easy lemma.

Lemma 15. *Let A be an abelian group of order m^r and suppose that for all d that divides m, the order of the d-torsion subgroup $A[d]$ is d^r. Then we have an isomorphism of groups*

$$A \cong (\mathbb{Z}/m\mathbb{Z})^r.$$

Proof. By the structure theorem for finite abelian groups, there exist positive integers $d_1, \ldots, d_n$ such that $A \cong C_{d_1} \times \ldots \times C_{d_n}$ where C_d denotes the cyclic group of order d. Moreover, we may suppose that $d_1|d_2|\ldots|d_n$. By comparing orders, we see that $m^r = d_1 \ldots d_n$. Furthermore, since the order of $A[m]$ is m^r, we must have the equality $A = A[m]$ and thus all elements of A are killed by m. This implies that d_n divides m.

We have $A[d_1] \cong C_{d_1} \times C_{d_2} \times \ldots \times C_{d_{n_1}}$ with $n_1 \leq n$ chosen to be the maximal index such that d_i divides d_1 for all $i \leq n_1$. But we already have that d_1 divides d_i for all i so that $d_1 = d_i$ for all $i \leq n_1$. Comparing orders we see that $d_1^r = d_1 \ldots d_{n_1} = d_1^{n_1}$ so that $n_1 = r$. We conclude that $A[d_1] \cong C_{d_1}^r$.

Relabeling everything, we now have an isomorphism

$$A \cong C_{d_1}^r \times C_{d_2} \times \ldots \times C_{d_n}$$

with $d_1|d_2|\ldots|d_n|m$ and $d_1 < d_2$. Proceeding as before we write

$$A[d_2] \cong C_{d_1}^r \times C_{d_2} \times \ldots \times C_{d_{n_2}}$$

where $n_2 \leq n$ is maximal such that d_i divides d_2 for all $i \leq n_2$. As before, this implies that $d_i = d_2$ for all $i = 2, \ldots, n_2$. Thus, we have $A[d_2] \cong C_{d_1}^r \times C_{d_2}^{n_2-1}$. Comparing order, we get $d_2^r = d_1^r d_2^{n_2-1}$. Since $d_1 < d_2$, this is a contradiction unless $n = 1$. This implies that $d_1 = m$ and finally $A \cong C_m^r$ as desired. □

Proposition 76. *Let E/k be an elliptic curve and $m \in \mathbb{Z}$ a non-zero integer. If m is non-zero in k, that is, $m \neq 0$ if* $\operatorname{char}(k) = 0$ *and $(m,p) = 1$ if* $\operatorname{char}(k) = p > 0$*, then*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Moreover, if $\operatorname{char}(k) = p > 0$*, then one of the following is true:*

(i) $E[p^e] = \{\mathcal{O}_E\}$ for all $e = 1, 2, \ldots$

(ii) $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1, 2, \ldots$

Proof. Suppose that m is non-zero in k. We have $|\ker([m])| = \deg_s([m])$ (cf.[Sil], III.4.10). By definition, we have $\ker([m]) = E[m] = E[m](\bar{k})$. By Proposition 73, we know that $[m]$ has degree m^2 and that $[m]$ is separable so that $\deg_s([m]) = \deg([m])$. We conclude that $|E[m]| = m^2$. Note that for any $d|m$, d is also non-zero in k and thus we also have $|E[d]| = d^2$ and $E[d]$ is a subgroup of $E[m]$. Applying Lemma 15 with $A = E[m]$ and $r = 2$ yields the desired result.

Suppose that $\operatorname{char}(k) = p > 0$ and let ϕ be the p-th power Frobenius morphism. Then we have

$$|E[p^e]| = \deg_s([p^e]) = \deg_s(\widehat{\phi} \circ \phi)^e = \deg_s(\widehat{\phi})^e \deg_s(\phi)^e$$

(cf.[Sil], III.4.10). By Proposition 74, ϕ is inseparable so that $\deg_s(\phi) = 1$. It follows that

$$|E[p^e]| = \deg_s(\widehat{\phi})^e.$$

We have $\deg(\widehat{\phi}) = \deg(\phi) = p$ by Proposition 74 (*iii*). There are now two cases. If $\widehat{\phi}$ is inseparable, then $\deg_s(\widehat{\phi}) = 1$ so that $E[p^e] = \{\mathcal{O}_E\}$ for all e. Otherwise, $\widehat{\phi}$ is separable so that $\deg_s(\widehat{\phi}) = \deg(\widehat{\phi}) = p$ and $|E[p^e]| = p^e$. By Lemma 15 applied with $A = E[p^e]$, $m = p^e$ and $r = 1$, we get $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ for all e. □

7.3 The Mordell-Weil Theorem

In this section we present and briefly sketch the proof of the Mordell-Weil Theorem. We do not provide all details since this proof was the subject of the previous paper [Lil] of the author. The statement of the theorem is the following:

Theorem 7.3.1. *Let k be a number field and let E/k be an elliptic curve. Then $E(k)$ is a finitely generated abelian group.*

The proof relies on two fundamental results, one is the existence of the Néron-Tate height on E/k and the other is known as the Weak Mordell-Weil Theorem. The statements are as follows:

Theorem 7.3.2 (Height Theorem)**.** *Let E/k be an elliptic curve. There exists an even function $\widehat{h} : E(\bar{k}) \longrightarrow \mathbb{R}$, known as the Néron-Tate (or canonical) height, that has the following properties:*

(i) For all $P, Q \in E(\bar{k})$, we have $\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$.

(ii) For all $P \in E(\bar{k})$ and for all $m \in \mathbb{Z}$, $\widehat{h}([m]P) = m^2\widehat{h}(P)$.

(iii) For any $P \in E(\bar{k})$, we have $\widehat{h}(P) \geq 0$. Moreover, for any positive integer M, the set $\{P \in E(k) : \widehat{h}(P) \leq M\}$ is finite.

Theorem 7.3.3 (Weak Mordell-Weil Theorem)**.** *For any integer $m \geq 2$, the group $E(k)/mE(k)$ is finite.*

Together these two results give a proof of the Mordell-Weil Theorem.

Proof of Theorem 7.3.1. Let $Q_1, \dots, Q_r$ be representatives of the quotient group $E(k)/mE(k)$ which is finite by Theorem 7.3.3. Let P be a point of $E(k)$. Then there exists P_1 in $E(k)$ and an index i_1 between 1 and r such that $P = mP_1 + Q_{i_1}$. Similarly for P_1, there exists P_2 in $E(k)$ and an index i_2 between 1 and r such that $P_1 = mP_2 + Q_{i_2}$. Proceeding inductively, at the n^{th} stage we obtain a element P_n of $E(k)$ and an index i_n between 1 and r such that $P_{n-1} = mP_n + Q_{i_n}$. We may then write P as a linear combination of the point P_n and the representatives $Q_1, \dots, Q_r$. If we can bound $\widehat{h}(P_n)$ by a constant, taking n large if necessary, we will be able to conclude that $E(k)$ is finitely generated by using property (iii) of Theorem 7.3.2. So our goal is to find a suitable bound. We have

$$\begin{aligned}\widehat{h}(P_n) &\overset{(ii)}{=} m^{-2}\widehat{h}([m]P_n) = m^{-2}\widehat{h}(P_{n-1} - Q_{i_n}) \\ &\overset{(i)}{=} m^{-2}(2\widehat{h}(P_{n-1}) + 2\widehat{h}(Q_{i_n}) - \widehat{h}(P_{n-1} + Q_{i_n})).\end{aligned}$$

Using the fact that $\widehat{h}$ takes non-negative values and setting $M := 2\max_i \widehat{h}(Q_i)$, we get

$$\widehat{h}(P_n) \leq m^{-2}(2\widehat{h}(P_{n-1}) + M).$$

Proceeding inductively, after n stages we obtain the bound

$$\widehat{h}(P_n) \leq \left(\frac{2}{m^2}\right)^n \widehat{h}(P) + \frac{M}{m^2}\sum_{i=0}^{n-1}\left(\frac{2}{m^2}\right)^i = \left(\frac{2}{m^2}\right)^n \widehat{h}(P) + M\frac{1-\left(\frac{2}{m^2}\right)^n}{m^2-2}.$$

Using the fact that $m \geq 2$, we get

$$\widehat{h}(P_n) \leq \left(\frac{2}{m^2}\right)^n \widehat{h}(P) + \frac{M}{2}$$

and we can pick n large enough so that $\left(\frac{2}{m^2}\right)^n \widehat{h}(P) \leq 1$. For such n we have

$$\widehat{h}(P_n) \leq 1 + \frac{M}{2}.$$

Every point in $E(k)$ is thus a linear combination of points in the set

$$\{Q_1, \ldots, Q_r\} \cup \{P \in E(k) : \widehat{h}(P) \leq 1 + M/2\},$$

which is finite by property (iii) of Theorem 7.3.2. We conclude that $E(k)$ is finitely generated. □

7.3.1 The Néron-Tate Height

We briefly outline the construction of the above mentioned height without dwelling too much on the details of the proofs. Everything here is done in Chapter VIII of [Sil] or in Chapter 1 of [Lil] by the author of the present paper. We start by defining a height in projective space.

Definition 32. Let k be a number field and let $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(k)$. We define the height of P with respect to k to be

$$H_k(P) = \prod_{v \in M_k} \max_{0 \leq i \leq n} |x_i|_v.$$

This seemingly infinite product is actually finite. The definition is independent of the choice of homogeneous coordinates by the product formula. Since we can always choose projective coordinates with at least one coordinate equal to 1, one easily sees that $H_k(P) \geq 1$. Finally, it is not difficult to see that if K/k is a finite extension, then $H_K(P) = H_k(P)^{[K:k]}$. Using this last fact, one defines a height on projective space that is independent of the number field k.

Definition 33. Let $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$. We define the absolute height of P by choosing a number field k such that $P \in \mathbb{P}^n(k)$ and setting

$$H(P) = H_k(P)^{1/[k:\mathbb{Q}]}.$$

For our purposes, it is more convenient to have a height that behaves additively, whence the following definition.

Definition 34. We define the logarithmic height to be the function $h : \mathbb{P}^n \longrightarrow \mathbb{R}$ defined by $h(P) = \log H(P)$.

The next task is to define heights on an elliptic curve E/k where k a number field. If $f \in \bar{k}(E)$, then consider the map $f : E \longrightarrow \mathbb{P}^1$ defined by

$$f(P) = \begin{cases} [f(P), 1] & \text{if f is regular at P,} \\ [1, 0] & \text{otherwise.} \end{cases}$$

This is a rational map and since both E and $\mathbb{P}^1$ are smooth curves it is a morphism of varieties.

Definition 35. Let E/k be an elliptic curve over a number field and $f \in \bar{k}(E)$. We define the height on E relative to f to be the function

$$h_f : E(\bar{k}) \longrightarrow \mathbb{R}, \qquad h_f(P) = h(f(P)).$$

Proposition 77. *Let E/k be an elliptic curve and let x, y be Weierstrass coordinates for E which is given by the equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in k$. A function $f \in \bar{k}(E) = \bar{k}(x, y)$ is even if and only if $f \in \bar{k}(x)$.

Proof. If $P \in E(\bar{k})$, then the inversion formula (cf. [Sil]) III.2.3 (a)) says that $-P$ is given in coordinates by $(x(P), -y(P) - a_1x(P) - a_3)$. In particular, x is an even function so that every function in $\bar{k}(x)$ is even. Conversely, let $f \in \bar{k}(E)$. Using the Weierstrass equation for E, one can write

$$f(x, y) = g(x) + h(x)y$$

for some $g, h \in \bar{k}(x)$. If furthermore f is even then we have

$$\begin{aligned} f(x, y) = f(x, -y - a_1x - a_3) &\implies g(x) + h(x)y = g(x) - h(x)(y + a_1x + a_3) \\ &\implies (2y + a_1x + a_3)h(x) = 0. \end{aligned}$$

This implies that either $h(x)$ is identically zero or $2y+a_1x+a_3$ is identically zero. The latter implies that $2 = a_1 = a_3 = 0$ which implies $\Delta = 0$. This contradicts the non-singularity of E so the only possibility is $h(x) = 0$. Consequently, we have $f(x, y) = g(x) \in \bar{k}(x)$. □

Lemma 16. *Let $f, g \in \bar{k}(E)$ be even functions. Then*

$$\deg(g)h_f = \deg(f)h_g + O(1).$$

Proof. Let $x, y \in k(E)$ be Weierstrass coordinates for E. Since f is even, we have $f \in \bar{k}(x)$ by Proposition 77. There exists therefore a rational function $r(X) \in \bar{k}(X)$ such that $f = r \circ x$. Since $\mathbb{P}^1$ is a smooth curve, r is a morphism of curves. Using ([Lil], Proposition 3.10) and taking logarithms we obtain

$$h_f = \deg(r)h_x + O(1).$$

We have $\deg(f) = \deg(x)\deg(r)$. We have $x^*(\bar{k}(X, Y)) = \bar{k}(x)$ and $[\bar{k}(x, y) : \bar{k}(x)] = 2$ by looking at the Weierstrass equation of E. Thus $\deg(x) = 2$ so that $\deg(f) = 2\deg(r)$. We find that $2h_f = \deg(f)h_x + O(1)$. By the same reasoning, we also have $2h_g = \deg(g)h_x + O(1)$. Finally,

$$2\deg(g)h_f - 2\deg(f)h_g = \deg(f)\deg(g)h_x - \deg(f)\deg(g)h_x + O(1) = O(1)$$

so that $\deg(g)h_f = \deg(f)h_g + O(1)$. □

Theorem 7.3.4. *Let E/k be an elliptic curve and let $f \in k(E)$ be an even function. For all $P, Q \in E(\bar{k})$ we have*

$$h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + O(1).$$

Proof. See Theorem 3.13 of [Lil] for the case $f = x$. For a general f, by Lemma 16 we have $2h_f = \deg(f)h_x + O(1)$. Thus multiplying the desired relation for x by $\deg(f)/2$ gives the general result. □

Corollary 38. *Let E/k be an elliptic curve over a number field and $f \in k(E)$ an even function.*

(i) For any point $Q \in E(\bar{k})$ we have

$$h_f(P + Q) \leq 2h_f(P) + O(1)$$

for all $P \in E(\bar{k})$, where the constant depends on E, f and Q.

(ii) Let m be any integer. Then for all $P \in E(\bar{k})$ we have

$$h_f([m]P) = m^2 h_f(P) + O(1)$$

where the constant depends on E, f and m.

(iii) For any integer M, the set $\{P \in E(k) \,:\, h_f(P) \leq M\}$ is finite.

Proof. To prove (i), we use the fact that the height on E is always non-negative and Theorem 7.3.4 in order to obtain

$$h_f(P + Q) \leq h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + O(1).$$

Bringing $2h_f(Q)$ into the big O yields the desired result.

To prove (ii), note that since f is supposed even we only need to prove this for m non-negative. The cases $m = 0$ and $m = 1$ are trivial and involve no constants. We proceed by induction. For m greater than 2, suppose that the result is true for n less than m. Using Theorem 7.3.4 with P and $[m-1]P$, we get

$$\begin{aligned} h_f([m]P) &= h_f([m-1]P + P) \\ &= -h_f([m-1]P - P) + 2h_f([m-1]P) + 2h_f(P) + O(1) \\ &= (-(m-2)^2 + 2(m-1)^2 + 2)h_f(P) + O(1) \\ &= m^2 h_f(P) + O(1) \end{aligned}$$

and this completes the proof of (ii).

By Proposition 3.12 of [Lil] we have that the set

$$\{P \in E(k) : h_x(P) \leq M\}$$

is finite for any M. By Lemma 16 there exists a constant C such that

$$|2h_f - \deg(f)h_x| \leq C.$$

Now, $h_f(P) \leq M$ implies $h_x(P) \leq (C+2M)/\deg(f)$. We thus have an inclusion of sets

$$\{P \in E(k) : h_f(P) \leq M\} \subset \{P \in E(k) : h_x(P) \leq (C + 2M)/\deg(f)\}$$

and the latter is finite. □

Theorem 7.3.5 (Tate)**.** *Let E/k be an elliptic curve, let $f \in k(E)$ be a non-constant even function and let $P \in E(\bar{k})$. Then the limit*

$$\frac{1}{\deg(f)} \lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

exists and is independent of f.

Proof. By Corollary 38, there exists a constant C such that for all $Q \in E(\bar{k})$, we have

$$|h_f([2]Q) - 4h_f(Q)| \leq C.$$

Let $N \geq M \geq 0$. Then we have

$$\begin{aligned} |4^{-N}h_f([2^N]P) - 4^{-M}h_f([2^M]P)| &= |\sum_{n=M}^{N-1} 4^{-n-1}h_f([2^{n+1}]P) - 4^{-n}h_f([2^n]P)| \\ &\leq \sum_{n=M}^{N-1} 4^{-n-1}|h_f([2]([2^n]P)) - 4h_f([2^n]P)| \\ &\leq C \sum_{n=M}^{N-1} 4^{-n-1}. \end{aligned}$$

We compute that

$$\sum_{n=M}^{N-1} 4^{-n-1} = \sum_{n=0}^{N} 4^{-n} - \sum_{n=0}^{M} 4^{-n} = \frac{4}{3}(1 - 4^{-N-1} - (1 - 4^{-M-1})) \leq 4^{-M}.$$

Therefore we have

$$|4^{-N}h_f([2^N]P) - 4^{-M}h_f([2^M]P)| \leq C4^{-M}. \qquad (7.3.5.1)$$

It follows that the sequence $\{4^{-N}h_f([2^N]P)\}_N$ is Cauchy and thus converges.

If $g \in k(E)$ is another non-constant even function, then from Lemma 16 we know that $\deg(f)h_g = \deg(g)h_f + O(1)$. Whence

$$\frac{4^{-N}h_f([2^N]P)}{\deg(f)} - \frac{4^{-N}h_g([2^N]P)}{\deg(g)} = O(4^{-N}) \overset{N\to\infty}{\longrightarrow} 0.$$

Consequently, the limit does not depend on f. □

Definition 36. Let E/k be an elliptic curve over a number field. The Néron-Tate height on E is the function $\widehat{h} : E(\bar{k}) \longrightarrow \mathbb{R}$ defined by

$$\widehat{h}(P) = \frac{1}{\deg(f)} \lim_{N \to \infty} 4^{-N} h_f([2^N]P)$$

where $f \in k(E)$ is any non-constant even function.

Proof of Theorem 7.3.2. Using Theorem 7.3.4, for any N we have

$$h_f([2^N](P+Q)) + h_f([2^N](P-Q)) = 2h_f([2^N]P) + 2h_f([2^N]Q) + O(1).$$

Dividing by $4^N \deg(f)$ and taking limits as $N \to \infty$, we obtain (i).

Using (i) with $\mathcal{O}_E$ we obtain

$$\widehat{h}(P)+\widehat{h}(-P)=2\widehat{h}(\mathcal{O}_E)+2\widehat{h}(P).$$

Since $f(\mathcal{O}_E)=[1,0]$ and $H([1,0])=1$ we see that $\widehat{h}(\mathcal{O}_E)=0$ and thus $\widehat{h}(P)=\widehat{h}(-P)$. This proves that $\widehat{h}$ is an even function.

Using Corollary 38 (ii), we see that

$$h_f([m]\circ[2^N]P)=m^2h_f([2^N]P)+O(1).$$

Dividing by $4^N\deg(f)$ and taking limits as $N\to\infty$, we obtain (ii).

If $P\in E(k)$ and $\widehat{h}(P)\leq M$, then for N large enough we must have $h_x([2^N]P)\leq 4^NC$. But only finitely many points satisfy this condition by Corollary 38 (iii). This proves (iii). □

We continue by proving some interesting facts concerning the canonical height.

Proposition 78. *Let $f\in k(E)$ be an even function. Then*

$$\deg(f)\widehat{h}=h_f+O(1)$$

where $O(1)$ depends on E and f.

Proof. By (7.3.5.1) there exists a constant C depending on f such that for $N\geq M\geq 0$ we have

$$|4^{-N}h_f([2^N]P)-4^{-M}h_f([2^M]P)|\leq C4^{-M}.$$

In particular, taking $M=0$ yields

$$|4^{-N}h_f([2^N]P)-h_f(P)|\leq C.$$

Taking the limit as $N\to\infty$ finally yields

$$|\deg(f)\widehat{h}(P)-h_f(P)|\leq C.$$

□

Definition 37. Let E/k be an elliptic curve. We define the canonical height pairing on E to be the pairing

$$\langle\cdot,\cdot\rangle : E(\bar{k})\times E(\bar{k})\longrightarrow\mathbb{R}$$

defined by $\langle P,Q\rangle=\widehat{h}(P+Q)-\widehat{P}-\widehat{Q}$.

Proposition 79. *The canonical height $\widehat{h}$ is a quadratic form on E, that is, it is an even function and the canonical height pairing is biadditive. Moreover, $\langle P,P\rangle\geq 0$ for all $P\in E(\bar{k})$ and*

$$\langle P,P\rangle=0 \textit{ if and only if } P \textit{ is a torsion point.}$$

Proof. Let $P \in E(\bar{k})$. Using Theorem 7.3.2 (i) with $\mathcal{O}_E$ yields $\widehat{h}(P) = \widehat{h}(-P)$ which shows that $\widehat{h}$ is an even function. Therefore in order to prove biadditivity, it suffices by symmetry to prove that

$$\langle P + R, Q \rangle = \langle P, Q \rangle + \langle R, Q \rangle \, .$$

Using 7.3.2 (i) multiple times, one easily proves this.

Using 7.3.2 (ii) we see that $\langle P, P \rangle = 2\widehat{h}(P)$. Since $h_f([2^N]P) \geq 0$ for all N and all P we see that also $\widehat{h}(P) \geq 0$.

Suppose that P is a torsion point on E. Then $[2^N]P$ takes on finitely many values as N varies. As a consequence, we have

$$\widehat{h}(P) = \lim_{N \to \infty} 4^{-N} h_f([2^N]P) = 0.$$

Conversely, suppose that $\langle P, P \rangle = 0$, that is, $\widehat{h}(P) = 0$. Let K/k be a finite extension such that $P \in E(K)$. By Theorem 7.3.2 (ii) we then have

$$\widehat{h}([m]P) = m^2 \widehat{h}(P) = 0$$

for all m. By Proposition 78 there is a constant C such that for all m we have

$$h_f([m]P) = |\deg(f)\widehat{h}([m]P) - h_f([m]P)| \leq C.$$

Therefore we have an inclusion of sets

$$\{[m]P \ : \ m \in \mathbb{N}\} \subset \{Q \in E(K) \ : \ h_f(Q) \leq C\}$$

and the latter is finite by Corollary 38 (iii). Therefore P must have finite order. □

Remark 48. As a consequence, $\widehat{h}$ is a positive definite quadratic form on $E(k)/E_{\mathrm{tors}}(K)$. An even more important consequence is that the existence of the Néron-Tate height is enough to show that $E_{\mathrm{tors}}(k)$ is a finite group.

We end our discussion of heights by showing that the canonical height is unique.

Proposition 80. *If* $\widehat{h}' : E(\bar{k}) \longrightarrow \mathbb{R}$ *is a function for which there exists an even function* $f \in k(E)$ *and an integer* $m \geq 2$ *such that*

$$\deg(f)\widehat{h}' = h_f + O(1) \qquad \textit{and} \qquad \widehat{h}' \circ [m] = m^2 \widehat{h}',$$

then $\widehat{h}' = \widehat{h}$.

Proof. Repeated applications of the second condition yields $\widehat{h}' \circ [m^N] = m^{2N}\widehat{h}'$ for all $N \in \mathbb{N}$. The first condition combined with Proposition 78 gives

$$\widehat{h}' - \widehat{h} = O(1).$$

For any $P \in E(\bar{k})$ we have

$$\widehat{h}'(P) = m^{-2N}\widehat{h}'([m^N]P) = m^{-2N}(\widehat{h}[m^N]P + O(1)) = \widehat{h}(P) + O(m^{-2N}).$$

This holds for all $N \in \mathbb{N}$ and taking the limit as $N \to \infty$ gives the desired equality $\widehat{h}'(P) = \widehat{h}(P)$. □

Remark 49. We point out that the Néron-Tate height pairing was discovered independently by Tate and Néron. What we saw above was the formulation due to Tate. However, this definition is very difficult to work with in practice. Néron developed a theory of local height pairings. For each $v \in M_k$ he defined a pairing $\langle \cdot, \cdot \rangle_v$ on certain divisors of E rational over k_v and obtained the global pairing by adding together the local pairings. The reader who is interested in Néron's local height theory is referred to the article of Gross [Gr3]. The reason that we make this remark is that all computations that are done for the global height pairing are in practice done for each local pairing.

7.3.2 The Weak Mordell-Weil Theorem

Let $m \geq 2$ be an integer. Let k be a number field and let $\bar{k}$ denote a fixed algebraic closure. We will use the notation $H^q(k, A)$ to mean $H^q(\mathrm{Gal}(\bar{k}/k), A)$ for any $\mathrm{Gal}(\bar{k}/k)$-module A.

We have the following short exact sequence of $\mathrm{Gal}(\bar{k}/k)$-modules:

$$0 \longrightarrow E[m] \longrightarrow E \xrightarrow{[m]} E \longrightarrow 0.$$

When we write E or $E[n]$ here we mean the points over $\bar{k}$. Taking the long exact sequence of cohomology we obtain an exact sequence

$$0 \longrightarrow E[m](k) \to E(k) \xrightarrow{[m]} E(k) \xrightarrow{\delta} H^1(k, E[m]) \\ \longrightarrow H^1(k, E) \xrightarrow{[m]} H^1(k, E) \longrightarrow \dots.$$

From this sequence we deduce the following short exact sequence

$$0 \longrightarrow E(k)/mE(k) \xrightarrow{\delta} H^1(k, E[m]) \longrightarrow H^1(k, E)[m] \longrightarrow 0.$$

Let $v \in M_k$ and denote by k_v the completion. Let $\bar{k}_v$ denote a fixed algebraic closure of k_v. Fix an extension of v to $\bar{k}$ which serves to fix an embedding $\bar{k} \hookrightarrow \bar{k}_v$. We have a restriction homomorphism

$$r_v : \mathrm{Gal}(\bar{k}_v/k_v) \longrightarrow \mathrm{Gal}(\bar{k}/k).$$

Using the same argument as above, we also have an exact sequence

$$0 \longrightarrow E(k_v)/mE(k_v) \xrightarrow{\delta} H^1(k_v, E[m]) \longrightarrow H^1(k_v, E)[m] \longrightarrow 0.$$

When we write E of $E[m]$ here we mean the points over $\bar{k}_v$. We get the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & E(k)/mE(k) \arrow[r, "\delta"] \arrow[d, "r_v"] & H^1(k, E[m]) \arrow[r] \arrow[d, "r_v"] & H^1(k, E)[m] \arrow[r] \arrow[d, "r_v"] & 0 \\
0 \arrow[r] & E(k_v)/mE(k_v) \arrow[r, "\delta"] & H^1(k_v, E[m]) \arrow[r] & H^1(k_v, E)[m] \arrow[r] & 0.
\end{tikzcd}$$

Definition 38. We define the m-Selmer group of E/k to be

$$\mathrm{Sel}_m(k,E) = \ker\left(H^1(k,E[m]) \longrightarrow \prod_{v\in M_k} H^1(k_v,E)\right)$$

and the Tate-Shafarevitch group of E/k to be

$$Ш(k,E) = \ker\left(H^1(k,E) \longrightarrow \prod_{v\in M_k} H^1(k_v,E)\right).$$

From the above diagram, one sees that the image of $E(k)/mE(k)$ via the connecting homomorphism δ lies in the m-Selmer group. Also, the image of the m-Selmer group lies in the $[m]$-torsion subgroup of $Ш(k,E)$. It is easy now to check that the following sequence is exact:

$$0 \longrightarrow E(k)/mE(k) \xrightarrow{\delta} \mathrm{Sel}_m(k,E) \longrightarrow Ш(k,E)[m] \longrightarrow 0.$$

One can prove that the m-Selmer group is always finite. As a consequence, $E(k)/mE(k)$ and $Ш(k,E)[m]$ are both finite. A full proof of Theorem 7.3.3 is the subject of Chapter 4 of [Lil] and uses the classical results of algebraic number theory, namely finiteness of the ideal class group and the S-unit theorem. It is conjectured that the Tate-Shafarevitch group is finite and a formula for the hypothetical order $|Ш(k,E)|$ appears in the conjecture of Birch and Swinnerton-Dyer.

7.3.3 The Regulator of an Elliptic Curve

Let E/k be an elliptic curve defined over the number field k. Let n be the rank of the Mordell-Weil group $E(k)$ so that $E(k) \cong E_{\mathrm{tors}}(k) \times \mathbb{Z}^n$. The free abelian group $E(k)/E_{\mathrm{tors}}(k)$ is a lattice in the real vector space $E(k) \otimes_{\mathbb{Z}} \mathbb{R}$. From Remark 48 the Néron-Tate height $\widehat{h}$ is a positive definite quadratic form on $E(k)/E_{\mathrm{tors}}(k)$. We want $\widehat{h}$ to extend to a positive definite quadratic form on the vector space $E(k) \otimes_{\mathbb{Z}} \mathbb{R}$. For this, we need the following lemma:

Lemma 17. *Let V be a real vector space of dimension n and let $L \subset V$ be a lattice. Let $q : V \longrightarrow \mathbb{R}$ be a quadratic form and suppose we have the following properties:*

(i) For all $P \in L$, we have $q(P) = 0$ if and only if $P = 0$.

(ii) For every constant C, the set $\{P \in L : q(P) \leq C\}$ is finite.

Then q is positive definite on V.

Proof. Corresponding to the Sylvester matrix decomposition, we may pick a basis for V such that q has signature (s,t). In other words, for every $x = (x_1,\dots,x_n) \in V$ expressed in this basis, we have

$$q(x) = \sum_{i=1}^{s} x_i^2 - \sum_{i=s+1}^{t} x_i^2.$$

Of course, $s+t \leq n$. We use this basis to identify V with $\mathbb{R}^n$. Consider the set

$$B(\epsilon,\delta) = \left\{x = (x_1,\dots,x_n) \in V \ : \ \sum_{i=1}^{s} x_i^2 \leq \epsilon \text{ and } \sum_{i=s+1}^{t} x_i^2 \leq \delta\right\}.$$

This is a measurable convex subset of $\mathbb{R}^n$ which is symmetric around the origin. Define $\lambda = \inf\{q(P) : P \in L, P \neq 0\}$. By (i) and (ii) we have $\lambda > 0$.

Suppose that q is not positive definite on V. Then $s < n$ and $t > 0$. By increasing δ, we can therefore increase the volume of $B(\lambda/2, \delta)$ in order to obtain $\mu(B(\lambda/2, \delta)) > 2^n v(L)$. For such a choice of δ, by Proposition 3, there exists a non-zero lattice point P in $B(\lambda/2, \delta)$. But

$$q(P) = \sum_{i=1}^{s} x_i^2 - \sum_{i=s+1}^{t} x_i^2 \leq \frac{\lambda}{2}$$

which contradicts the definition of λ. We conclude that q is indeed positive definite on V. □

Corollary 39. *Let E/k be an elliptic curve. The Néron-Tate height $\widehat{h}$ on E extends to a positive definite quadratic form on the finite-dimensional real vector space $E(k) \otimes_{\mathbb{Z}} \mathbb{R}$.*

Proof. We extend $\widehat{h}$ to $E(k) \otimes_{\mathbb{Z}} \mathbb{R}$ by $\widehat{h}(P \otimes x) = x^2 \widehat{h}(P)$. By the Mordell-Weil Theorem, $E(k)/E_{\text{tors}}(k)$ is a lattice in $E(k) \otimes_{\mathbb{Z}} \mathbb{R}$. Condition (i) of the previous lemma holds because of Proposition 79 and condition (ii) holds because of Theorem 7.3.2 (iii). □

Associated to E/k we have the following quantities: $E(k) \otimes_{\mathbb{Z}} \mathbb{R}$ a finite dimensional real vector space, $\widehat{h}$ a positive definite quadratic form on $E(k) \otimes_{\mathbb{Z}} \mathbb{R}$ and a lattice $E(k)/E_{\text{tors}}(k)$. In such a situation, an important invariant is the volume of the given lattice with respect to the quadratic form in question. We have seen this situation arise already when defining quantities attached to number fields. By Proposition 2 the discriminant d_k is a scaling of the volume of the lattice $\mathcal{O}_k$ in the finite-dimensional real vector space $k \otimes_{\mathbb{Q}} \mathbb{R}$ with respect to the inner product of $k_{\mathbb{R}}$. In defining the regulator of k, one considers the lattice $\lambda(U_k)$ in the finite-dimensional real vector space $\mathbb{R}X_k$ with respect to the euclidean inner product and take R_k to be a scaling of the volume of $\lambda(U_k)$. This leads to the following definition:

Definition 39. Let E/k be an elliptic curve. Let $P_1, \ldots, P_n$ be a $\mathbb{Z}$-basis of the lattice $E(k)/E_{\text{tors}}(k)$. We define the regulator of E to be the positive quantity

$$R(E/k) = \det(\langle P_i, P_j \rangle)/|E_{\text{tors}}(k)|^2.$$

As when defining the regulator of k or the discriminant of k, this definition does not depend on the choice of a basis.

Proposition 81. *Let E/k be an elliptic curve. Let $Q_1, \ldots, Q_n$ be a basis of a free subgroup A of $E(k)$ with finite index I. Then we have*

$$R(E/k) = \det(\langle Q_i, Q_j \rangle)/I^2.$$

Proof. The subgroup A is free and thus contains no torsion. It is therefore a subgroup of the free group $E(k)/E_{\text{tors}}(k)$. Therefore there exists a basis $P_1, \ldots, P_n$ of $E(k)/E_{\text{tors}}(k)$ and non-zero integers $a_1, \ldots, a_n$ such that $a_1P_1, \ldots, a_nP_n$ is a basis of A (cf. [Sam], § 1.5, Theorem 1). It follows that the index of A in $E(k)/E_{\text{tors}}(k)$ is given by $a_1 \ldots a_n$ and $I = a_1 \ldots a_n |E_{\text{tors}}(k)|$. Moreover, we have

$$\langle a_iP_i, a_jP_j \rangle = a_ia_j \langle P_i, P_j \rangle = \text{Diag}(a_1, \ldots, a_n) \langle P_i, P_j \rangle \text{Diag}(a_1, \ldots, a_n).$$

As a consequence, we have

$$\det(\langle a_i P_i, a_j P_j\rangle) = I^2 \det(\langle P_i, P_j\rangle)/|E_{\mathrm{tors}}(k)|^2 = I^2 R(E/k).$$

Since $\det(\langle Q_i, Q_j\rangle)/I^2$ is independent of the choice of basis we have proved the desired formula. □

Remark 50. In practice this formula is less rigid than the definition of the regulator and therefore often easier to use for computations.

7.4 The L-Function of an Elliptic Curve

Let E/k be an elliptic curve defined over the number field k. In this section we define the Hasse-Weil L-function $L(s, E/k)$ associated to E. Before doing that, we need a little more theory of elliptic curves.

7.4.1 More on Elliptic Curves

We introduce the ℓ-adic Weil pairing on the Tate module and then give some point counting results concerning elliptic curves over finite fields.

The Tate Module and the Weil Pairing

Let E/k is an elliptic curve over a perfect field and let $\ell \in \mathbb{Z}$ be a prime. The ℓ-adic Tate module of E is the group

$$T_\ell(E) = \varprojlim E[\ell^n]$$

where the inverse limit is taken with respect to the natural maps

$$[\ell] : E[\ell^{n+1}] \longrightarrow E[\ell^n].$$

Since each group $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, $T_\ell(E)$ naturally acquires the structure of a $\mathbb{Z}_\ell$-module. If ℓ is non-zero in k, then by Proposition 76, we have a group isomorphism

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

From now on we shall use ℓ to denote a prime that is non-zero in k and we write p for the characteristic of k (which may be zero). Also, since the multiplication-by-integer maps are defined over k, the Galois group $\mathrm{Gal}(\bar{k}/k)$ commutes with multiplication and therefore acts on $E[\ell^n]$. This gives an action of $\mathrm{Gal}(\bar{k}/k)$ on $T_\ell(E)$.

Let $\psi \in \mathrm{End}(E)$. Since ψ is an isogeny we have $\psi(P+Q) = \psi(P) + \psi(Q)$ for all $P, Q \in E$ (cf. [Sil], III.4.8). In particular, ψ maps $E[\ell^n]$ to $E[\ell^n]$ and the following diagram commutes:

$$\begin{tikzcd}
E[\ell^{n+1}] \arrow[r, "\psi"] \arrow[d, "{[\ell]}"'] & E[\ell^{n+1}] \arrow[d, "{[\ell]}"] \\
E[\ell^n] \arrow[r, "\psi"] & E[\ell^n].
\end{tikzcd}$$

As a consequence, we get a well-defined group homomorphism which commutes with the action of $\mathbb{Z}_\ell$:

$$\psi_\ell : T_\ell(E) \longrightarrow T_\ell(E), \qquad P \mapsto (\psi(P_n))_{n=1}^{\infty}.$$

This construction gives a ring homomorphism

$$\mathrm{End}(E) \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)), \qquad \psi \mapsto \psi_\ell.$$

This homomorphism is injective since $\psi_\ell = 0$ implies that $E[\ell^n] \subset \ker(\psi)$ for all n. But any non-zero isogeny is a finite map and in particular the kernel is finite. This forces $\psi = 0$. Choosing a basis for $T_\ell(E)$ as a free $\mathbb{Z}_\ell$-module of rank two, we get an injective homomorphism of rings $\mathrm{End}(E) \longrightarrow M_2(\mathbb{Z}_\ell)$.

For any integer m prime to p, there is a pairing, called the Weil pairing on E,

$$e_m : E[m] \times E[m] \longrightarrow \mu_m.$$

One can show that this is a bilinear, alternating, non-degenerate and $\mathrm{Gal}(\bar{k}/k)$ invariant pairing (cf. [Sil], III.8.1). Moreover, if $\psi : E_1 \longrightarrow E_2$ is an isogeny, then ψ and its dual isogeny $\widehat{\psi} : E_2 \longrightarrow E_1$ are adjoint with respect to this pairing (cf. [Sil], III.8.2). The definition of e_m relies on the following fact:

Proposition 82. *Let E/k be an elliptic curve and let $D = \sum n_P(P) \in \mathrm{Div}(E)$. Then D is a principal divisor if and only if*

$$\deg(D) = 0 \qquad \textit{and} \qquad \sum [n_P]P = \mathcal{O}_E.$$

Proof. Since principal divisors have degree zero we must have $D \in \mathrm{Div}^0(E)$. Next, we have

$$\begin{aligned} D \sim 0 \iff \sigma(D) = 0 &\iff \sigma\left(\sum n_P((P) - (\mathcal{O}_E))\right) = 0 \\ &\iff \sigma\left(\sum n_P \kappa(P)\right) = 0 \\ &\iff \sum [n_P]P = \mathcal{O}_E \end{aligned}$$

where in the second equivalence we used the fact that $\deg(D) = 0$ and in the last equivalence we used Definition 29. □

The pairing is constructed as follows: if $T \in E[m]$, then by Proposition 82 we can pick $f \in \bar{k}(E)$ such that $\mathrm{div}(f) = m(T) - m(\mathcal{O}_E)$. Next, consider the divisor

$$[m]^*(T) - [m]^*(\mathcal{O}_E) = \sum_{P \in [m]^{-1}E(\bar{k})} (P) - \sum_{R \in E[m]} (R) = \sum_{R \in E[m]} (T' + R) - (R)$$

where $T' \in E(\bar{k})$ is any point such that $[m]T' = T$. This is a divisor of degree zero and

$$\sum_{R \in E[m]} T' + R - R = [\#E[m]]T' = [m^2]T' = [m]T = 0$$

since $T \in E[m]$. By Proposition 82 there exists $g \in \bar{k}(E)$ such that

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(\mathcal{O}_E).$$

We have

$$\mathrm{div}(f \circ [m]) = \mathrm{div}([m]^* f) = [m]^* \mathrm{div}(f) = m([m]^*(T) - [m]^*(\mathcal{O}_E)) = \mathrm{div}(g^m).$$

Therefore $f \circ [m]$ and g^m differ by a constant $c \in \bar{k}$ so without loss of generality we may suppose that

$$f \circ [m] = g^m.$$

Now, let $S \in E[m]$. Then for any point $X \in E$ we have

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

so that $g(X+S)/g(X) \in \mu_m$. Consider the morphism

$$E \longrightarrow \mathbb{P}^1, \qquad X \longmapsto g(X+S)/g(X).$$

Since μ_m is finite, this map cannot be surjective and must therefore be constant. We conclude that the value of $g(X+S)/g(X)$ does not depend on the choice of X. We define

$$e_m(S,T) = \frac{g(X+S)}{g(X)}$$

where $X \in E$ and this is the e_m-Weil pairing.

Proposition 83. *There exists a bilinear, alternating, non-degenerate and Galois invariant pairing*

$$e : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu)$$

called the ℓ-adic Weil paring on the Tate module. Moreover, if $\psi : E_1 \longrightarrow E_2$ is an isogeny between elliptic curves and $\widehat{\psi} : E_2 \longrightarrow E_1$ its dual, then ψ_ℓ and $\widehat{\psi}_\ell$ are adjoint with respect to the above pairing.

Remark 51. Here $T_\ell(\mu)$ denotes the ℓ-adic Tate module of $\bar{k}^*$. It is the inverse limit

$$T_\ell(\mu) = \varprojlim \mu_{\ell^n}$$

taken with respect to the natural maps $[\ell] : \mu_{\ell^{n+1}} \longrightarrow \mu_{\ell^n}$.

Proof. In order to define the pairing e, one needs to check that the following diagram commutes:

$$\begin{tikzcd} E[\ell^{n+1}] \times E[\ell^{n+1}] \arrow[r, "e_{\ell^{n+1}}"] \arrow[d, "{[\ell \times \ell]}"'] & \mu_{\ell^{n+1}} \arrow[d, "{[\ell]}"] \\ E[\ell^n] \times E[\ell^n] \arrow[r, "e_{\ell^n}"] & \mu_{\ell^n} \end{tikzcd}$$

for all $n \geq 1$. This amounts to proving that

$$e_{\ell^{n+1}}(S,T)^\ell = e_{\ell^n}([\ell]S, [\ell]T)$$

for all $S, T \in E[\ell^{n+1}]$. This can achieved by using the properties of the Weil pairing (cf. [Sil], III.8.1). The fact that these diagrams commute give a well-defined pairing

$$e : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu)$$

by setting $e(S,T) = (e_{\ell^n}(S_n, T_n))_{n=1}^\infty$. One easily verifies that all the properties of e_m hold for e. □

Recall that we have an injective homomorphism of rings

$$\mathrm{End}(E) \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E)) \cong M_2(\mathbb{Z}_\ell)$$

upon choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$. Therefore, if $\psi : E \longrightarrow E$ is an isogeny, then we can compute $\det(\psi_\ell)$ and $\mathrm{tr}(\psi_\ell)$. These are both elements of $\mathbb{Z}_\ell$ and do not depend on the choice of basis. Amazingly, as this next result shows, these quantities do not depend on the prime ℓ.

Proposition 84. *Let $\psi \in \mathrm{End}(E)$ and let $\psi_\ell : T_\ell(E) \longrightarrow T_\ell(E)$ be the induced map on the Tate module of E. Then*

$$\det(\psi_\ell) = \deg(\psi) \qquad \text{and} \qquad \mathrm{tr}(\psi_\ell) = 1 + \deg(\psi) - \deg(1-\psi).$$

In particular, $\det(\psi_\ell)$ and $\mathrm{tr}(\psi_\ell)$ are in $\mathbb{Z}$ and do not depend on ℓ.

Proof. Choose a basis $\{v_1, v_2\}$ of $T_\ell(E)$ as a $\mathbb{Z}_\ell$-module and write

$$\psi_\ell(v_1) = av_1 + cv_2 \qquad \text{and} \qquad \psi_\ell(v_2) = bv_1 + dv_2$$

where $a, b, c, d \in \mathbb{Z}_\ell$. The matrix of ψ_ℓ relative to this basis is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Using the properties of the ℓ-adic Weil pairing, we have

$$\begin{aligned} e(v_1, v_2)^{\deg(\psi)} &= e([\deg(\psi)]v_1, v_2) = e(\widehat{\psi}_\ell \circ \psi_\ell(v_1), v_2) \\ &= e(\psi_\ell v_1, \psi_\ell v_2) = e(av_1 + cv_2, bv_1 + dv_2). \end{aligned}$$

The first equality uses bilinearity of e while the third one uses the fact that ψ_ℓ and $\widehat{\psi}_\ell$ are adjoint with respect to e. Using bilinearity and the fact that e is alternating, we see that

$$e(v_1, v_2)^{\deg(\psi)} = e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det(\psi_\ell)}.$$

We have shown that $e(v_1, v_2)^{\deg(\psi) - \det(\psi_\ell)} = 1$. By non-degeneracy of e, the latter implies $\deg(\psi) = \det(\psi_\ell)$. Finally, for any 2×2 matrix A one has the formula

$$\mathrm{tr}(A) = 1 + \det(A) - \det(1-A)$$

and the trace formula follows. □

Elliptic curves over finite fields

In order to define the local L-factors of elliptic curves we need a few results concerning elliptic curves defined over finite fields.

Theorem 7.4.1 (Hasse). *Let $E/\mathbb{F}_q$ be an elliptic curve defined over the finite field $\mathbb{F}_q$ of cardinality q. Then*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Proof. Choose a Weierstrass equation for E and let $\phi : E \longrightarrow E$ denote the q-th power Frobenius isogeny. By Remark 47 we have $\#E(\mathbb{F}_q) = \ker(1-\phi)$. By Proposition 75, the map $1-\phi$ is separable and therefore $\#E(\mathbb{F}_q) = \deg(1-\phi)$ (cf. [Sil], III.4.10 (c)). The degree map is a positive definite quadratic form on $\mathrm{End}(E)$ (cf. [Sil], III.6.3). By the Cauchy-Schwarz inequality, for any $\alpha, \beta \in \mathrm{End}(E)$ we have

$$|\deg(\alpha+\beta) - \deg(\alpha) - \deg(\beta)| \leq 2\sqrt{\deg(\alpha)\deg(\beta)}.$$

Applying this inequality with $\alpha = 1$ and $\beta = -\phi$, and using the fact that $\deg(1) = 1$ and $\deg(\phi) = q$ by Proposition 74 (*iii*), we obtain

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

□

Proposition 85. *Let $E/\mathbb{F}_q$ be an elliptic curve and denote by $\phi : E \longrightarrow E$ the q-th power Frobenius isogeny. We define $a = q + 1 - \#E(\mathbb{F}_q)$. Consider the polynomial $T^2 - aT + q \in \mathbb{Z}[T]$. The roots α and β of this polynomial are complex conjugates and satisfy $|\alpha| = |\beta| = \sqrt{q}$. Moreover, $\phi^2 - a\phi + q = 0$ in* $\operatorname{End}(E)$ *and we have the following formula: for all $n \geq 1$,*

$$\#E(\mathbb{F}_{q^n}) = (q^n + 1) - (\alpha^n + \beta^n).$$

Proof. Consider the homomorphism $\phi_\ell : T_\ell(E) \longrightarrow T_\ell(E)$. By Proposition 84 we have

$$\begin{aligned} \det(\phi_\ell) &= \deg(\phi) = q \\ \operatorname{tr}(\phi_\ell) &= 1 + \deg(\phi) - \deg(1 - \phi) = 1 + q - \#E(\mathbb{F}_q) = a. \end{aligned}$$

Therefore, taking the characteristic polynomial of ϕ_ℓ we get

$$\det(T - \phi_\ell) = T^2 - \operatorname{tr}(\phi_\ell)T + \det(\phi_\ell) = T^2 - aT + q.$$

Computing the discriminant of this polynomial, we get $a^2 - 4q$ which is non-positive by Theorem 7.4.1. As a consequence, α and β are either equal or complex conjugates. In either case, by comparing coefficients, we have $\alpha\beta = q$ so that $|\alpha| = |\beta| = \sqrt{q}$. This proves the first part.

By the Hamilton-Cayley Theorem, ϕ_ℓ is annihilated by its characteristic polynomial so that by Proposition 84 we have

$$\deg(\phi^2 - a\phi + q) = \det(\phi_\ell^2 - a\phi_\ell + q) = \det(0) = 0$$

which implies $\phi^2 - a\phi + q = 0$.

Finally, let $n \geq 1$. Putting ϕ_ℓ in normal Jordan form, we see that

$$\det(T - \phi_\ell^n) = (T - \alpha^n)(T - \beta^n).$$

By Remark 47 we have $\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n)$. Using Proposition 84 we have

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n) = \det(1 - \phi_\ell^n) = \det(\phi_\ell^n) + 1 - \operatorname{tr}(\phi_\ell^n) = q + 1 - \alpha^n - \beta^n$$

as desired. □

7.4.2 The L-function

We define the Hasse-Weil L-function of an elliptic curve in two steps. Then we state the conjectural functional equation of the completed L-function.

The Incomplete L-Function

Let k be a number field and let E/k be an elliptic curve. Let S be the set of places containing M_k^∞ and all finite places of bad reduction of E. For a place $v \notin S$, we let A_v be the associated ring of integers and π_v be a choice of uniformizer. We denote by $\mathbb{F}_v = A_v/\pi_v A_v$ the corresponding residue field which is finite of cardinality denoted by q_v. The fact that v does not belong to S means that there is a model for E with coefficients in A_v and $v(\Delta) = 0$ so that the reduced curve $\tilde{E}_v/\mathbb{F}_v$ is an elliptic curve. We define

$$a_v = 1 + q_v - \#E(\mathbb{F}_v)$$

and consider the characteristic polynomial of the q_v-th power Frobenius isogeny ϕ_{q_v} of $\tilde{E}_v$:

$$h_v(t) = \det(1 - \phi_{q_v} t) = 1 - a_v t + q_v t^2 = (1 - \alpha_v t)(1 - \bar{\alpha}_v t).$$

The elements α_v and $\bar{\alpha}_v$ are roots of the polynomial $t^2 - at + q$ and by Proposition 85 they are complex conjugates and $|\alpha_v| = |\bar{\alpha}_v| = \sqrt{q_v}$. The polynomial $h_v(t)$ is the reciprocal of the formal local L-factor of $\tilde{E}_v$:

$$L(\tilde{E}_v/\mathbb{F}_v, t) = h_v(t)^{-1}.$$

We substitute t by q_v^{-s} to get the local L-factor

$$L_v(E/k, s) = L(\tilde{E}_v/\mathbb{F}_v, q_v^{-s}) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}.$$

Remark 52. Note that we have

$$L_v(E/k, 1) = (1 - a_v q_v^{-1} + q_v^{-1})^{-1} = \frac{q_v}{\#\tilde{E}_v(\mathbb{F}_v)}.$$

Definition 40. We define the incomplete L-function of E to be

$$L_S(E/k, s) = \prod_{v \notin S} L_v(E/k, s).$$

Proposition 86. *Let E/k be an elliptic curve. The incomplete L-function $L_S(E/k, s)$ converges absolutely in the half-plane $\Re s > 3/2$.*

Proof. We will achieve this by comparison with the Dedekind zeta-function of k. For any $v \notin S$ we have the following estimate

$$|1 - \alpha_v q_v^{-s}| \geq |1 - |\alpha_v| q_v^{-\Re s}| = |1 - q_v^{1/2 - \Re s}|.$$

It follows that

$$|L_v(E/k, s)| = |(1 - \alpha_v q_v^{-s})(1 - \bar{\alpha}_v q_v^{-s})|^{-1} \leq |1 - q_v^{-(\Re s - 1/2)}|^{-2}$$

so that

$$|L_S(E/k, s)| \leq \prod_v |1 - q_v^{-(\Re s - 1/2)}|^{-2} = |\zeta_{k,S}(\Re s - 1/2)|^2.$$

Since $\zeta_{k,S}(s)$ converges absolutely in the half-plane $\Re s > 1$ we conclude that $L_S(E/k, s)$ converges absolutely in the half-plane $\Re s > 3/2$. □

The Completed L-Function

The general theory of L-functions suggest that they should admit a meromorphic continuation to the whole $\mathbb{C}$ and satisfy a functional equation. Before this is possible in the case of elliptic curves, we need to complete the L-function by adding in local factors at the primes of bad reduction and at the infinite places. Recall that S is the set of infinite places and finite places of bad reduction. For finite $v \in S$ we define the local L-factor as follows:

$$L_v(E/k,s) = \begin{cases} 1 & \text{if } E \text{ has additive reduction at } v \\ (1-q_v^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction at } v \\ (1+q_v^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction at } v. \end{cases}$$

Proposition 87. *Let v be a place of bad reduction of E. We have*

$$\tilde{E}_v^{ns}(\mathbb{F}_v) \cong \begin{cases} \mathbb{F}_v^+ & \textit{if } E \textit{ has additive reduction at } v \\ \mathbb{F}_v^* & \textit{if } E \textit{ has split multiplicative reduction at } v. \end{cases}$$

If E has non-split multiplicative reduction at v, let α_1 and α_2 denote the slopes of the tangent lines at the singular point of $\tilde{E}_v/\mathbb{F}_v$. Let $L = \mathbb{F}_v(\alpha_1, \alpha_2)$. Then

$$\tilde{E}_v^{ns}(\mathbb{F}_v) \cong \{\alpha \in L^* \ : \ N_{L/\mathbb{F}_v}(\alpha) = 1\}.$$

Proof. See [Sil], III.2.5 and Ex. 3.5. □

Proposition 88. *Let v be a finite place of k. Then*

$$L_v(E/k,1) = \frac{q_v}{\#\tilde{E}_v^{ns}(\mathbb{F}_v)}.$$

Proof. If v is a place of good reduction then this is Remark 52. If v is a place of additive reduction, then $L_v(E/k,1) = 1$ and $\#\tilde{E}_v^{ns}(\mathbb{F}_v) = \#\mathbb{F}_v^+ = q_v$ so the formula is correct. If the reduction at v is split multiplicative, then $L_v(E/k,1) = q_v/(q_v-1)$ and $\#\tilde{E}_v^{ns}(\mathbb{F}_v) = \#\mathbb{F}_v^* = q_v - 1$ so the formula is correct. Finally, if the reduction at v is non-split multiplicative, then $L_v(E/k,1) = q_v/(q_v+1)$. We have

$$\#\tilde{E}_v^{ns}(\mathbb{F}_v) = |\{\alpha \in L^* : \alpha^{q_v+1} = 1\}| = q_v + 1$$

since there are at most $q_v + 1$ distinct $q_v + 1$-th roots of unity and L contains them all. This proves the formula in this case. □

Definition 41. The Hasse-Weil L-function of E/k is

$$L(E/k,s) = \prod_{v\nmid\infty} L_v(s, E/k).$$

Definition 42. The completed L-function of E/k is

$$\Lambda(E/k,s) = ((2\pi)^{-s}\Gamma(s))^{[k:\mathbb{Q}]} L(s, E/k).$$

Before discussing the conjectured functional equation of Λ we define the two following quantities which measure bad reduction. These two quantities also appear in the statement of the Birch and Swinnerton-Dyer Conjecture.

Definition 43. The minimal discriminant for E/k, denoted by $\mathcal{D}(E/k)$, is the integral ideal of k defined by

$$\mathcal{D}(E/k) = \prod_{v \nmid \infty} \mathfrak{p}_v^{v(\Delta_v)}$$

where $\mathfrak{p}_v$ denotes the prime ideal of k associated to the finite place v and Δ_v denotes the discriminant of a minimal Weierstrass model of E for v.

Remark 53. Notice that if v is a prime of good reduction, then $v(\Delta_v) = 0$. Since there are only finitely many primes of bad reduction, the product defining the minimal discriminant is finite and contains only information about the primes of bad reduction. Note that a Weierstrass model for E/k is a global minimal Weierstrass model if and only if $\mathcal{D}(E/k)$ is principal generated by the discriminant Δ.

Definition 44. The conductor of E/k, denoted by $N(E/k)$, is the integral ideal of k defined by

$$N(E/k) = \prod_{v \nmid \infty} \mathfrak{p}_v^{f_v}$$

where

$$f_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v \\ 1 & \text{if } E \text{ has multiplicative reduction at } v \\ 2 + \delta_v & \text{if } E \text{ has additive reduction at } v, \end{cases}$$

where δ_v is a non-negative integer. We do not give its definition but only mention that it is zero whenever the characteristic of $\mathbb{F}_v$ is not 2 or 3.

Conjecture 7. *Let k be a number field and E/k and elliptic curve. The holomorphic function $\Lambda(E/k, s)$ on the right half-plane $\Re s > 3/2$ admits an analytic continuation to the entire complex plane and satisfies the functional equation*

$$\Lambda(E/k, s) = \pm A^{1-s} \Lambda(E/k, 2-s)$$

where $A = N(N(E/k))d_k^2$.

Remark 54. This conjecture has been proved in the case $k = \mathbb{Q}$ as a consequence of the Theorem of Wiles, Breuil, Conrad and Taylor otherwise known as the Modularity Theorem. It is generally not known to hold. The Birch and Swinnerton-Dyer Conjecture is a conjecture on the order of the L-function of E/k at the reflexion point $s = 1$ of the presumed functional equation.

7.4.3 Artin Formalism for L-Functions of Elliptic Curves

Let k be a number field, E/k and elliptic curve and $\ell \in \mathbb{Z}$ a prime. Since addition on E is defined over k the action of $\mathrm{Gal}(\bar{k}/k)$ on E commutes with addition and therefore the Galois group acts on $E[\ell^n]$ for all n. Consequently, the Galois group acts on the Tate module $T_\ell(E)$. Upon choosing a basis for the 2-dimensional $\mathbb{Q}_\ell$-vector space $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, this action gives an ℓ-adic Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Let v be a finite place of k and choose an extension of v to $\bar{k}$ so that we have an embedding $\bar{k} \hookrightarrow \bar{k}_v$ and therefore a restriction map

$$r_v : \mathrm{Gal}(\bar{k}_v/k_v) \longrightarrow \mathrm{Gal}(\bar{k}/k).$$

We then have a representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{k}_v/k_v) \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Denote by I_v the inertia group of v which is defined by the exact sequence

$$1 \longrightarrow I_v \longrightarrow \mathrm{Gal}(\bar{k}_v/k_v) \longrightarrow \mathrm{Gal}(\bar{\mathbb{F}}_v/\mathbb{F}_v) \longrightarrow 1.$$

Let ϕ_v denote a representative in $\mathrm{Gal}(\bar{k}_v/k_v)$ of the Frobenius element in the quotient group $\mathrm{Gal}(\bar{k}_v/k_v)/I_v = \mathrm{Gal}(k_v^{nr}/k_v)$. The action of ϕ_v on $V_\ell(E)$ depends on the choice of representative and to eliminate this dependency, we restrict our attention to the subrepresentation $V_\ell(E)^{I_v}$.

Proposition 89. *Let E/k be an elliptic curve and let v be a finite place of k. Suppose that E/k has good reduction at v. If $m \geq 1$ is an integer coprime to the characteristic of $\mathbb{F}_v$, then $E[m]$ is unramified at v meaning that the inertia group I_v acts trivially on $E[m]$. As a consequence, if $\ell \in \mathbb{Z}$ is a prime not equal to the characteristic of $\mathbb{F}_v$, then $T_\ell(E)$ is unramified at v.*

Proof. Let E/k_v be given by a minimal Weierstrass equation for v with discriminant Δ. Let K'/k_v be a finite extension such that $E[m] \subset E(K')$ and let w be the extension of v to L. Denote by A_w the ring of integers of w and by $\mathbb{F}_w$ the corresponding residual field. By our assumption that E/k has good reduction at v, we have $v(\Delta) = 0$. Since $w(\cdot) = ev(\cdot)$ where the non-zero integer e is the ramification index of K'/k_v, we see that $w(\Delta) = 0$ and consequently the Weierstrass equation for E is minimal for w and E has good reduction at w. By the theory of formal groups of elliptic curves (cf. [Sil], Chapter IV), one can show (cf. [Lil], Proposition 4.37) that the reduction map gives an injective homomorphism

$$E[m] \hookrightarrow \tilde{E}_w(\mathbb{F}_w). \tag{7.4.1.1}$$

Let $P \in E[m]$ and let $\sigma \in I_v$. We need to prove that $P^\sigma = P$. By definition of the inertia group, I_v acts trivially on $\mathbb{F}_w$ and therefore on $\tilde{E}_w(\mathbb{F}_w)$. Therefore,

$$\widetilde{P^\sigma - P} = \tilde{P}^\sigma - \tilde{P} = \mathcal{O}_{\tilde{E}_w}.$$

By (7.4.1.1), this implies that $P^\sigma = P$.

Let ℓ be a prime not equal to the characteristic of $\mathbb{F}_v$. Then for all n, $E[\ell^n]$ is unramified at v and since $T_\ell(E)$ is the inverse limit of these groups the same is true for $T_\ell(E)$. □

Let v be a good prime of k and choose ℓ such that $v \nmid \ell$. By Proposition 89, $V_\ell(E)^{I_v} = V_\ell(E)$ so that $\rho_{E,\ell}(\phi_v)$ is a 2-by-2 matrix with coefficients in $\mathbb{Q}_\ell$. The reduction map $E(\bar{k}) \longrightarrow \tilde{E}_v(\bar{\mathbb{F}}_v)$ is a homomorphism of groups (cf. [Lil], Appendix A). We therefore get a homomorphism of $\mathrm{Gal}(\bar{k}/k)$-modules $E[\ell^n] \longrightarrow \tilde{E}_v[\ell^n]$ where $\mathrm{Gal}(\bar{\mathbb{F}}_v/\mathbb{F}_v)$ is viewed as a $\mathrm{Gal}(\bar{k}/k)$-module. By (7.4.1.1) this map is injective and by comparing cardinalities we see that it is an isomorphism. It induces a reduction map $T_\ell(E) \longrightarrow T_\ell(\tilde{E}_v)$ which is an isomomorphism of $\mathrm{Gal}(\bar{k}/k)$-modules. Let $\sigma \in \mathrm{Gal}(\bar{k}_v/k_v)$ and denote by $\bar{\sigma}$

image of σ in $\mathrm{Gal}(\bar{\mathbb{F}}_v/\mathbb{F}_v)$. The action of $\bar{\phi}_v$ on $\tilde{E}_v$ is the same as the one of the q_v-th power Frobenius isogeny ϕ so that $\rho_{E,\ell}(\phi_v) = \phi_\ell$ and by Proposition 84, the characteristic polynomial of $\rho_{E,\ell}(\phi_v)$ is given by

$$P_v(X) = \det(1 - \rho_{E,\ell}(\phi_v)X|V_\ell(E)) = 1 - a_vX + q_vX^2 \in \mathbb{Z}[X]$$

so that the local factor $L_v(E/k, s)$ is equal to $P_v(q_v^{-s})^{-1}$. Let S denote the finite set of places consisting of the archimedean ones, and all places of bad reduction. Choose ℓ a prime that is divisible by a place in S. Then we have shown that

$$L_S(E/k, s) = \prod_{v \notin S} \det(1 - \rho_{E,\ell}(\phi_v)q_v^{-s} \mid V_\ell(E))^{-1}.$$

We point out the similarities in the construction of the incomplete L-function of an elliptic curve and the construction of Artin L-functions. Let K/k is a finite Galois extension with Galois group G and let S denotes the set of places containing the archimedean ones and all finite primes of k that ramify in K (the "bad" primes). Let (ρ, V) be a finite-dimensional complex representation of G. For any $v \notin S$, we consider the characteristic polynomial of a Frobenius element ϕ_w

$$g_v(t) = \det(1 - \rho(\phi_w)t).$$

Here w is any choice of a prime above v and the characteristic polynomial does not depend on this choice. Define the formal local Artin L-factor to be the reciprocal of this polynomial:

$$L(t, V, K/k, v) = g_v(t)^{-1}.$$

The the local Artin L-factor is defined by substituting t with $N(v)^{-s} = q_v^{-s}$:

$$L_v(s, V, K/k) = L(q_v^{-s}, V, K/k, v).$$

Finally, the incomplete Artin L-function is

$$L_S(s, V, K/k) = \prod_{v \notin S} \det(1 - \rho(\phi_w)q_v^{-s} \mid V)^{-1}.$$

We mention without proof that the analogy works all the way and one can prove the following:

Proposition 90. *Let E/k be an elliptic curve over a number field. Then we have the formula*

$$L(s, E/k) = \prod_{v \nmid \infty} \det(1 - \rho_{E,\ell}(\phi_v)q_v^{-s}|V_\ell(E)^{I_v})^{-1}$$

where ϕ_v denotes a representative of the Frobenius element in $\mathrm{Gal}(\bar{k}_v/k_v)/I_v$.

As a consequence, the L-function attached to an elliptic curve is similar in construction to an Artin L-function, the difference being that the representation in question is over $\mathbb{Q}_\ell$ and not $\mathbb{C}$ and that the represented group is infinite. Nevertheless, it is not suprising that the L-function of an elliptic curve shares properties similar to the ones of the Artin L-functions. This is illustrated in the following result that we mention without proof.

Proposition 91. *Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ and let k be a finite Galois extension of $\mathbb{Q}$. Let $\rho_{E,\ell}$ denote the ℓ-adic Galois representation* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(V_\ell(E))$ *and let $\tilde{\rho}_{E,\ell}$ denote its restriction to the subgroup* $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$. *Choosing an embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ we can view these representations as finite-dimensional complex representations. Let $\eta_i : \mathrm{Gal}(k/\mathbb{Q}) \longrightarrow \mathrm{GL}(W_i)$ be the irreducible finite-dimensional complex representations of* $\mathrm{Gal}(k/\mathbb{Q})$ *and denote again by η_i their inflation to* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Then we have the following Artin-type decomposition:*

$$L(E/k, s) = \prod_i L(s, \rho_{E,\ell} \otimes \eta_i)^{\dim(\eta_i)}$$

where where $L(s, \rho_{E,\ell} \otimes \eta_i)$ denotes the Euler product

$$\prod_p \det(1 - \rho_{E,\ell} \otimes \eta_i(\phi_p)p^{-s} | (V_\ell(E) \otimes W_i)^{I_p})^{-1}.$$

7.5 The Global Period of an Elliptic Curve

The purpose of this section is to define the global period of an elliptic curve defined over a number field k. This requires the notion of a measure on the adeles of k and of a measure on $E(k_v)$ for any place v of k. Our references here are [CF], Chapter X as well as [We1], Chapter I and II.

7.5.1 Adeles

Let k be a number field and denote as usual by M_k the set of non-equivalent normalized absolute values on k. For any place $v \in M_k$ we denote by k_v the completion of k at v. If v is a finite place, that is, a non-archimedean absolute value, then k_v is complete with finite residue field and therefore locally compact in the v-adic topology and the closed unit ball $\mathcal{O}_v$, that is, the ring of integers, is compact in this topology. Let S be any finite subset of M_k that contains the archimedean places and consider the subset of $\prod_{v \in M_k} k_v$ defined by

$$A_S = \prod_{v \in S} k_v \times \prod_{v \notin S} \mathcal{O}_v.$$

This set comes naturally with the product topology and is locally compact with respect to this topology. As a set we define the adeles of k as

$$A_k = \bigcup_S A_S$$

where the union is over all finite subsets of M_k that contain the archimedean places. We give the set A_k the final topology associated to this inductive limit, that is, we define a subset $U \subset A_k$ to be open if and only if $U \cap A_S$ is open in A_S for all S with respect to the product topology. We call A_k together with this topology the adeles of k. The A_S are open in A_k and each A_S is locally compact whence A_k is locally compact with respect to its topology. Moreover, A_k is a ring for the operations of addition and multiplication defined componentwise. Hence A_k is a locally compact topological ring.

An element $a \in A_k$ is an infinite vector $(a_v)_v$ in $\prod_{v \in M_k} k_v$ such that for all v, except for a finite number, we have $a_v \in \mathcal{O}_v$. A basis of open sets for A_k consists of products $\prod_{v \in M_k} U_v$ where U_v is open in k_v and for all but a finite number of v we have $U_v = \mathcal{O}_v$. Alternatively, one could have defined A_k to be the restricted topological product of the k_v with respect to the $\mathcal{O}_v$ (cf. [CF], Chapter II). Since k embeds in all its completions, k embeds diagonally in A_k. The image of the embedding consists of the principal adeles and we will naturally identify k with this image. On can prove that k is discrete in A_k and that the quotient A_k/k is compact in the quotient topology. Furthermore, one has the Strong Approximation Theorem. See [CF] for these results.

Each k_v^+ is a locally compact group and therefore has a left-invariant Haar measure which is unique up to scalar multiplication. Let $\mathrm{d}x_v$ denote the choice of a Haar measure for k_v^+ subject to the following normalization:

- If v is a real archimedean, then $k_v = \mathbb{R}$ and we take $\mathrm{d}x_v = \mathrm{d}x$ the Lebesgue measure.
- If v is complex archimedean, then $k_v = \mathbb{C}$ and we take $\mathrm{d}x_v$ to be the Lebesgue product measure on $\mathbb{R} \times i\mathbb{R}$.
- If v is non-archimedean, we normalize the measure $\mathrm{d}x_v$ by setting
$$\int_{\mathcal{O}_v} \mathrm{d}x = 1.$$

We define a measure $\mathrm{d}x$ on A_k to be the one for which a basis of measurable sets is the $\prod_{v \in M_k} M_v$ where $M_v \subset k_v$ has finite $\mathrm{d}x_v$-measure and $M_v = \mathcal{O}_v$ for almost all v and where
$$\int_{\prod M_v} \mathrm{d}x = \prod \int_{M_v} \mathrm{d}x_v.$$
Note that this product is convergent thanks to our normalizations of $\mathrm{d}x_v$ for v non-archimedean. The restriction of $\mathrm{d}x$ to A_S is the standard product measure. We will often denote the measure $\mathrm{d}x$ by $\bigotimes_{v \in M_k} \mathrm{d}x_v$. It is not difficult to check that this measure on A_k is invariant under additive translation by elements of k. We therefore get an induces measure $\mathrm{d}x$ on the compact quotient A_k/k.

Proposition 92. *We the above notations, we have*
$$\mu_k := \int_{A_k/k} \mathrm{d}x = 2^{-r_2} |d_k|^{1/2}.$$

Proof. Let S be the finite subset of M_k consisting of the archimedean places of k. Let r_1 be the number of real archimedean places and let r_2 be the number of complex archimedean places. Note that $k_S := \prod_{v \in S} k_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is the Minkowski space of k. As an $\mathbb{R}$-alegebra it is isomorphic to $\mathbb{R}^n$ where $n = [k : \mathbb{Q}]$. The field k diagonally embeds in k_S via the map $\sigma : (\sigma_1, \ldots, \sigma_{r_1+r_2})$ where $\sigma_i : k \hookrightarrow \mathbb{C}$ are the corresponding real or complex embeddings. Moreover, $\sigma : k \otimes_{\mathbb{Q}} \mathbb{R} \longrightarrow k_S$ is an isomorphism of $\mathbb{R}$-algebras. Note that $\mathcal{O}_k = A_S \cap k$ sits as a lattice in k_S. Let $\mathcal{O}'(S)$ denote the projection of $\mathcal{O}_k$ onto k_S. Note that $\mathcal{O}'(S) = \sigma(\mathcal{O}_k)$. Consider the map
$$A_S \hookrightarrow A_k \twoheadrightarrow A_k/k.$$

Let $x \in A_k$. Then for all but finitely many $v \notin S$ we have $x_v \in \mathcal{O}_v$. Let $v \in S$. Then by the strong approximation theorem, for all $\epsilon > 0$ there exists $\beta \in k$ such that $|x_w - \beta|_v \leq \epsilon$ for all $w \neq v$. In particular, $x - \beta \in \mathcal{O}_w$ for all $w \notin S$ so that $x - \beta \in A_S$. This proves that the above map is surjective. The kernel of this map is $\mathcal{O}_k$ so that we have an isomorphism $A_S/\mathcal{O}_k \cong A_k/k$. Let $\mathcal{F}$ denote a fundamental domain for the lattice $\sigma(\mathcal{O}_k)$ in k_S. Then $\mathcal{F}' = \mathcal{F} \times \prod_{v \nmid \infty} \mathcal{O}_v$ is a measurable set for the measure $\mathrm{d}x$ of representatives of the quotient $A_S/\mathcal{O}_k$ so that

$$\mu_k = \int_{A_S/\mathcal{O}_k} \mathrm{d}x = \int_{\mathcal{F}'} \mathrm{d}x = \int_{\mathcal{F}} \prod_{v \in S} \mathrm{d}x_v = v(\mathcal{O}_k) = 2^{-r_2}|d_k|^{1/2}$$

by Proposition 2. □

7.5.2 Measure on $E(k_v)$

Let k be a number field and let v be a finite place of k. Let E/k_v be an elliptic curve. Suppose that E is given by a minimal Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let ω_v denote the invariant differential

$$\omega_v = \frac{dx}{2y + a_1x + a_3} \in \Omega_E.$$

This differential is unique up to a unit of $\mathcal{O}_v$. One can associate to such a differential a left Haar measure $|\omega_v|$ on $E(k_v)$. We do not define this measure here and refer the reader to [We1]. However, we will show how one may compute the integral

$$\int_{E(k_v)} |\omega_v|$$

under certain conditions on v.

Denote by $\tilde{E}_v/\mathbb{F}_v$ the reduced curve obtained by reducing the coefficients of the above Weierstrass equation modulo $\pi_v\mathcal{O}_v$. This curve may be singular and we denote by $\tilde{E}_v^{ns}$ the smooth part of $\tilde{E}_v$. Note that if E has good reduction at v, then $\tilde{E}_v^{ns} = \tilde{E}_v$ is an elliptic curve. In either case, one can check that the chord-and-tangent process still works on $\tilde{E}_v^{ns}$ and thus that $\tilde{E}_v^{ns}$ is an algebraic group. Denote by ρ the reduction map $E(k_v) \longrightarrow \tilde{E}_v(\mathbb{F}_v)$ and define $E_0(k_v) = \rho^{-1}(\tilde{E}_v^{ns}(\mathbb{F}_v))$ and $E_1(k_v) = \rho^{-1}(\mathcal{O}_{\tilde{E}_v})$. There is an exact sequence of abelian groups

$$0 \longrightarrow E_1(k_v) \longrightarrow E_0(k_v) \xrightarrow{\rho} \tilde{E}_v^{ns}(\mathbb{F}_v) \longrightarrow 0$$

(cf. [Sil], VII.2.1). Moreover, one can prove that $E_0(k_v)$ is a subgroup of finite index in $E(k_v)$ (cf. [Sil], VII.6.2).

We have

$$E_1(k_v) = \{(x, y) \in E(k_v) \mid v(x) < 0 \text{ and } v(y) < 0\} \cup \{\mathcal{O}_E\}$$

and if $(x, y) \in E_1(k_v)$, then $2v(y) = 3v(x)$ (cf. [Lil], Proposition 4.32). Thus for some $m \geq 1$ we have $2v(y) = 3v(x) = -6m$ which implies that $v(x) = -2m$ and $v(y) = -3m$. For each $m \geq 1$ we let

$$E_m(k_v) = \{(x, y) \in E(k_v) \mid v(x) \leq -2m \text{ and } v(y) \leq -3m\} \cup \{\mathcal{O}_E\}.$$

Let $z = -x/y$. Then z is a uniformizing parameter at $\mathcal{O}_E$ and we can get expansions

- $x(z) = z^{-2} - a_1 z^{-1} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \ldots$
- $y(z) = -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + a_3 + (a_4 + a_1 a_3) z + \ldots$
- $\omega_v = (1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + a_3) z^3 + \ldots) dz = P(z) dz$

with coefficients in $\mathcal{O}_v$ and we can define a formal group law

$$F(z_1, z_2) = z_1 + z_2 + \ldots \in \mathcal{O}_v[[z_1, z_2]]$$

by $z(P+Q) = F(z(P), z(Q))$ (cf. [Sil], IV.1). The completeness of $\mathcal{O}_v$ ensures that these expansions converge for $z \in \pi_v \mathcal{O}_v$ and we denote by $\hat{E}(\pi_v \mathcal{O}_v)$ the set $\pi_v \mathcal{O}_v$ with the group structure given by the formal law F. This is an abstract group and one can prove that

$$\psi : \hat{E}(\pi_v \mathcal{O}_v) \longrightarrow E_1(k_v), \qquad z \longmapsto (x(z), y(z))$$

is an isomorphism of groups (cf. [Sil], VII.2.2) under which the subgroups $\hat{E}(\pi_v^m \mathcal{O}_v)$ correspond to the subgroups $E_m(k_v)$ for all $m \geq 1$.

For any $n \geq 1$, we claim that we have an isomorphism

$$\hat{E}(\pi_v^n \mathcal{O}_v) / \hat{E}(\pi_v^{n+1} \mathcal{O}_v) \cong \pi_v^n \mathcal{O}_v / \pi_v^{n+1} \mathcal{O}_v$$

induced by the identity map. As sets, these two groups are equal and we therefore only need to prove that it is a homomorphism of group. Let $z_1, z_2 \in \pi_v^n \mathcal{O}_v$. Then

$$\begin{aligned} z_1 \oplus_F z_2 = F(z_1, z_2) &= z_1 + z_2 + \text{(higher order terms)} \\ &\equiv z_1 + z_2 \mod \pi_v^{2n} \\ &\equiv z_1 + z_2 \mod \pi_v^{n+1} \end{aligned}$$

and therefore it is a homomorphism.

On the other hand, we have an isomorphism

$$\mathcal{O}_v / \pi_v \mathcal{O}_v \xrightarrow{\sim} \pi_v^n \mathcal{O}_v / \pi_v^{n+1} \mathcal{O}_v$$

defined by $\alpha \mapsto \pi_v^n \alpha$. We conclude that the quotient groups

$$\hat{E}(\pi_v^n \mathcal{O}_v) / \hat{E}(\pi^{n+1} \mathcal{O}_v)$$

are isomorphic to $\mathbb{F}_v^+$ for all $n \geq 1$. We therefore have a filtration

$$E(k_v) \supset E_0(k_v) \supset E_1(k_v) \subset E_2(k_v) \supset \ldots$$

with

$$\begin{cases} E(k_v)/E_0(k_v) & \text{finite,} \\ E_0(k_v)/E_1(k_v) \cong \tilde{E}_v(\mathbb{F}_v) & \\ E_m(k_v)/E_{m+1}(k_v) \cong \mathbb{F}_v^+ & \text{for all } m \geq 1. \end{cases}$$

Giving $E(k_v)$ the filtration topology makes it into a topological group.

Theorem 7.5.1 (Tate)**.** *Let E be an elliptic curve over k_v where v is a finite place of k and choose a minimal Weierstrass model for E. Let ω_v be an invariant differential, defined over $\mathcal{O}_v$, which does not vanish modulo $\pi_v\mathcal{O}_v$ and let $\mathrm{d}x_v$ be the Haar measure on k_v^+ which gives $\mathcal{O}_v$ volume 1. Then*

$$\int_{E(k_v)} |\omega_v| = \frac{[E(k_v) : E_0(k_v)]}{L_v(E/k, 1)}.$$

Proof. Assume that E is given by the minimal Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and take ω_v to be the invariant differential

$$\frac{dx}{2y + a_1x + a_3} \in \Omega_E.$$

Let $\log_{\hat{E}}$ denote the formal logarithm associated to $\hat{E}(\pi_v\mathcal{O}_v)$, that is, the formal power series

$$\log_{\hat{E}}(z) = \int P(z)dz \in k_v[[z]].$$

(cf. [Sil], IV.6). The logarithm induces a homomorphism of groups

$$\log_{\hat{E}} : \hat{E}(\pi_v\mathcal{O}_v) \longrightarrow k_v^+$$

and for an integer m that is large enough, it induces an isomorphism

$$\log_{\hat{E}} : \hat{E}(\pi_v^m\mathcal{O}_v) \xrightarrow{\sim} \pi_v^m\mathcal{O}_v$$

(cf. [Sil], IV.6.4).

The above tells us that $E(k_v)$ contains a finite index subgroup $E_m(k_v)$ which is isomorphic via $\log_{\hat{E}}$ to $\pi_v^m\mathcal{O}_v$ for some $m \geq 1$. The group $\pi_v^m\mathcal{O}_v$ comes equipped with the v-adic topology and is compact with respect to this topology. The map $\log_{\hat{E}}$ is an isomorphism of topological groups, that is, an isomorphism of groups and a homeomorphism.

Pull-back $\mathrm{d}x_v$ to $\hat{E}(\pi_v\mathcal{O}_v)$ via $\log_{\hat{E}}$. This gives

$$\log_{\hat{E}}^*(\mathrm{d}x_v)(z) = \mathrm{d}\log_{\hat{E}}(z) = |P(z)|_v\mathrm{d}z.$$

Note that $P(z) = 1 + O(z)$ so that if $z \in \pi_v\mathcal{O}_v$, then by the ultrametric property of the valuation v we have $|P(z)|_v = 1$.

We can now compute that

$$\int_{E_m(k_v)} |\omega_v| = \int_{\hat{E}(\pi_v^m\mathcal{O}_v)} |P(z)|_v\mathrm{d}z = \int_{\pi_v^m\mathcal{O}_v} \mathrm{d}x_v = q_v^{-m}.$$

We then have

$$\int_{E_1(k_v)} |\omega_v| = q_v^{m-1}\int_{E_m(k_v)} |\omega|_v = \frac{1}{q_v}.$$

Using the fact that $E_0(k_v)$ is the disjoint union of $\#\tilde{E}_v^{ns}(\mathbb{F}_v)$ copies of $E_1(k_v)$ together with the translation-invariance of our measure, we see that

$$\int_{E_0(k_v)} |\omega_v| = \frac{\#\tilde{E}_v^{ns}(\mathbb{F}_v)}{q_v} = L_v(E/k,1)^{-1}$$

where in the last equality we used Proposition 88. Using now that $E_0(k_v)$ is a subgroup of finite index in $E(k_v)$ together with the translation-invariance of our measure we get

$$\int_{E(k_v)} |\omega_v| = \frac{[E(k_v):E_0(k_v)]}{L_v(E/k,1)}.$$

□

7.5.3 The Global Period

Let k be a number field and let E/k be an elliptic curve. Let ω be an invariant differential on E/k. It gives an invariant differential ω_v on E/k_v for all v. Let $\mathrm{d}x = \otimes_v \mathrm{d}x_v$ denote a measure on A_k subject to the normalization

$$\int_{A_k/k} \mathrm{d}x = 1.$$

This can by achieved, by letting $\mathrm{d}x_v$ denote the normalized Haar measures on k_v^+ for all finite places and by taking the standard measures $\mathrm{d}x_v$ for v archimedean introduced in Section 7.6.1 and rescale them by real number c_v such that

$$\prod_{v\in M_k^\infty} c_v = 2^{r_2}|d_k|^{-1/2}$$

by Proposition 92.

Definition 45. The global period of E/k is

$$P(E/k) = P(\omega) = \prod_{v\nmid\infty}\left(L_v(E/k,1)\int_{E(k_v)}|\omega_v|\right)\cdot\prod_{v|\infty}\int_{E(k_v)}|\omega_v|.$$

Remark 55. The above product is well-defined. In fact, for almost all prime v, the differential ω_v satisfies the conditions of Theorem 7.5.1 in that ω_v is defined over $\mathcal{O}_v$ and does not vanish module $\pi_v\mathcal{O}_v$. For those v we have

$$L_v(E/k,1)\int_{E(k_v)}|\omega_v| = [E(k_v):E_0(k_v)].$$

For all but finitely many v we have $E(k_v) = E_0(k_v)$ so that only finitely many terms in the above product are not 1.

Proposition 93. *The global period is independent of the choice of a differential ω on E/k.*

Proof. If ω' is another differential on E/k, then there exists $\alpha \in k^*$ such that $\omega' = \alpha\omega$. But then

$$P(\omega') = P(\omega)\prod_{v\in M_k}|\alpha|_v$$

which is $P(\omega)$ by the product formula. □

7.6 Statement of the Conjecture

We now have all ingredients in hand to state the conjecture of Birch and Swinnerton-Dyer.

Conjecture 8 (BSD)**.** *Let E/k be an elliptic curve over a number field and assume that $L(E/k,s)$ has a meromorphic continuation to a neighborhood of the point $s=1$.*

(1) If n is the rank of the finitely generated abelian group $E(k)$, then

$$\mathrm{ord}_{s=1}(L(E/k,s))=n.$$

(2) Let $c(E/k)=P(E/k)\cdot R(E/k)\cdot \#Ш(k,E)$. Then

$$L(E/k,s)\sim c(E/k)(s-1)^n, \text{ as } s\to 1.$$

Bibliography

[Ar1] E. Artin, *Über eine neue Art von L-Reihen.* Abh. Math. Sem. Hamburg 3, 1923.

[Ar2] E. Artin, *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren.* Abh. Math. Sem. Hamburg 8, 1930.

[Ar3] E. Artin, *Die gruppentheoretische Struktur der Diskriminante algebraischer Zahlkörper.* J. Reine Angew. Math. 164, 1931.

[BS] Z. I. Borevich, I. R. Shafarevich *Number Theory.* Academic Press, 1966.

[BSD] B. Birch, P. Swinnerton-Dyer *Notes on Elliptic Curves II.* J. Reine. Angew. Math 165, 1965.

[CF] J.W.S. Cassels, A. Fröhlich *Algebraic Number Theory.* Thompson Book Company, 1967.

[Cog] J.W. Cogdell, *On Artin L-functions*, people.math.osu.edu/cogdell, 2006.

[Coh] P.M. Cohn, *Algebraic Numbers and Algebraic Functions.* Springer, 1991.

[Cox] D.A. Cox, *Primes of the form $x^2 + ny^2$.* Wiley-Interscience, 1989.

[Das] S. Dasgupta, *Stark's Conjectures.* http://people.ucsc.edu/ sdasgup2/, 1999.

[Dir] P. G. L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthÃďlt*, Abhand. Ak. Wiss. Berlin 48, 1837.

[Lil] D. Lilienfeldt, *The Mordell-Weil Theorem.* Unpublished, 2015.

[Gr1] B. Gross, *Heegner Points on $X_0(N)$*, In Rankin, R.A. (ed): Modular forms. Chicester: Ellis Horwood, 1984.

[Gr2] B. Gross, *Lectures on the Conjecture of Birch and Swinnerton-Dyer*, 2009.

[Gr3] B. Gross, *Local Heights on Curves*, In *Arithmetic Geometry*, Ch. XIV, Springer-Verlag, 1984.

[GZ] B. Gross, D. Zagier, *Heegner Points and Derivatives of L-series*, Inv. Math. 84, 1986.

[Hon] T. Honda, *Invariant differentials and L-functions. Reciprocity law for quadratic fields and elliptic curves over* $\mathbb{Q}$, Rendiconti del Seminario Matematico della Università di Padova tome 49, 1973.

[Lan] S. Lang, *Algebraic Number Theory.* Springer GTM 110, 1994.

[Mor] L. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge. Phil. Soc. 21, 1922.

[Mos] P. Mostert, *Stark's Conjectures.* www.mth.uct.ac.za/academics/, 2008.

[Ro1] J. Rotman, *Advanced Modern Algebra.* Prentice Hall, 2003.

[Ro2] J. Rotman, *Introduction to Homological Algebra.* Universitext, 2009.

[Sam] P. Samuel, *Algebraic Theory of Numbers.* Dover, 2008.

[Se1] J. P. Serre, *Linear representations of finite groups.* Springer GTM 42, 1977.

[Se2] J. P. Serre, *Local fields.* Springer GTM 67, 1979.

[Sie] C.L. Siegel, *Über die Fourierschen Koeffizienten von Modulformen.* Nachr. Akad. Wiss. Göttingen, 1970.

[Sil] J.H. Silverman, *The arithmetic of elliptic curves.* Springer, 1986.

[Sny] N. Snyder, *Artin L-functions: A Historical Approach.* math.columbia.edu/nsnyder, 2002.

[StI] H. M. Stark, *L-Functions at s=1. I. L-Functions for Quadratic Forms.* Advances in Math. 7, 1971.

[StII] H. M. Stark, *L-Functions at s=1. II. Artin L-Functions with Rational Characters.* Advances in Math. 17, 1975.

[StIII] H. M. Stark, *L-Functions at s=1. III. Totally Real Fields and Hilbert's Twelfth Problem.* Advances in Math. 22, 1976.

[StIV] H. M. Stark, *L-Functions at s=1. IV. First Derivatives at s=0.* Advances in Math. 35, 1980.

[Ta1] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s=0.* Birkhäuser, 1984.

[Ta2] J. Tate, *Algorithm for determining the Type of a Singular Fiber on an Elliptic Pencil*, in *Modular functions in one variable IV*, Springer, 1975.

[We1] A. Weil, *Adeles and algebraic groups*, Progress in Mathematics Vol. 23, Birkhäuser, 1982.

[We2] A. Weil, *L'Arithmétique sur les courbes algÃl'briques*, Acta Mathematica 52, 1929.